2021г.

Инструкция по обновлению комплекта абонента

Обновление комплекта абонента с сертификатом ГосСУОК с помощью объединённого инсталлятора AvPKIsetup

Оглавление

Аннотация **2**

Системные требования **3**

Обновление комплекта абонента **4**

Удаление криптографического программного обеспечения с помощью объединенного инсталлятора **8**

Приложение 1. Установка сертификатов в процессе обновления комплекта абонента **12**

Приложение 2. Импорт сертификата, если программное обеспечение уже установлено на компьютер **19**

Приложение 3. Способы получения/обновления списков отзыва сертификатов СОС: **25**

Аннотация

В настоящей инструкции описан порядок обновления криптографического программного обеспечения «Комплект абонента AvUCK» с сертификатом ГосСУОК с помощью объединенного инсталлятора AvPKISetup.

Системные требования

1) Работа инсталлятора AvPKISetup рассчитана на выполнение под управлением 32-х и 64-х битных операционных систем:

- Windows Server 2003 с установленным Service Pack 2 с обновлением **KB2836198 –** снята с поддержки Microsoft в 2015 году**,**
- Windows XP с установленным Service Pack 3 с обновлением **KB2836198** – снята с поддержки Microsoft в 2015 году,
- Windows 7 – снята с поддержки Microsoft в 2020 году,
- Windows Server 2008 R1,
- Windows Server 2008 R2,
- Windows Server 2012,
- Windows Server 2012 R2,
- Windows Server 2016,
- Windows Server 2019,
- Windows 8,
- Windows 8.1,
- Windows 10 (build 10240, 10586, 14393, 15063).

ВНИМАНИЕ! В операционных системах ОС Windows, снятых Microsoft с технической поддержки, не гарантируется корректная работа криптопровайдера при работе с браузером Internet Explorer, установленным по умолчанию.

2) Требуется наличие **Microsoft Internet Explorer 8.0** или выше.

3) Пользователь для установки и запуска должен иметь права в операционной системе **Windows** не ниже «**PowerUser**».

4) Необходимо **установить поддержку русского языка** для программ, не поддерживающих Юникод. Для этого

1. Перейти в меню Start - Control Panel - Region and Language (Пуск-Панель управления-Язык и региональные стандарты).
2. На вкладке Formats - Форматы выбрать русский язык, на вкладке Location - Текущее расположение выбрать Беларусь, на вкладке Administrative – Дополнительно выбрать русский язык для программ, не поддерживающих Юникод.
3. Выполнить перезагрузку.
4. Проверить отображение кодировки.

5) Файлы, содержащие личный ключ подписи/шифрования, а также другие необходимые параметры, должны находиться на электронных устройствах **AvToken, AvPass** в защищенном виде.

6) На время установки антивирусное программное обеспечение (в том числе встроенное в ОС, например, Windows Defender) рекомендуется отключать, т.к.

некоторые антивирусные программы могут создавать препятствие записи значений в реестр Windows и установке компонентов программ в системные папки.

Обновление комплекта абонента

Комплект абонента AvUCK сконфигурирован для установки и обновления программного обеспечения с помощью AvPKISetup. Каждое окно объединенного инсталлятора AvPKISetup снабжено пояснительными надписями, которые следует внимательно читать.

В любой момент установку можно прервать, нажав кнопку «**Отмена**».

Во время установки или обновления ПО с помощью данного инсталлятора может быть проимпортирован личный сертификат в персональный справочник, а также атрибутный сертификат. Для этого файл сертификата или сертификатов в формате *.p7b необходимо поместить в папку Data.

Для начала обновления ПО необходимо запустить файл **AvPKISetup2.exe**.

В окне мастера установки следует нажать кнопку «**Далее**», чтобы начать установку ПО на компьютер (*Рисунок 1*).

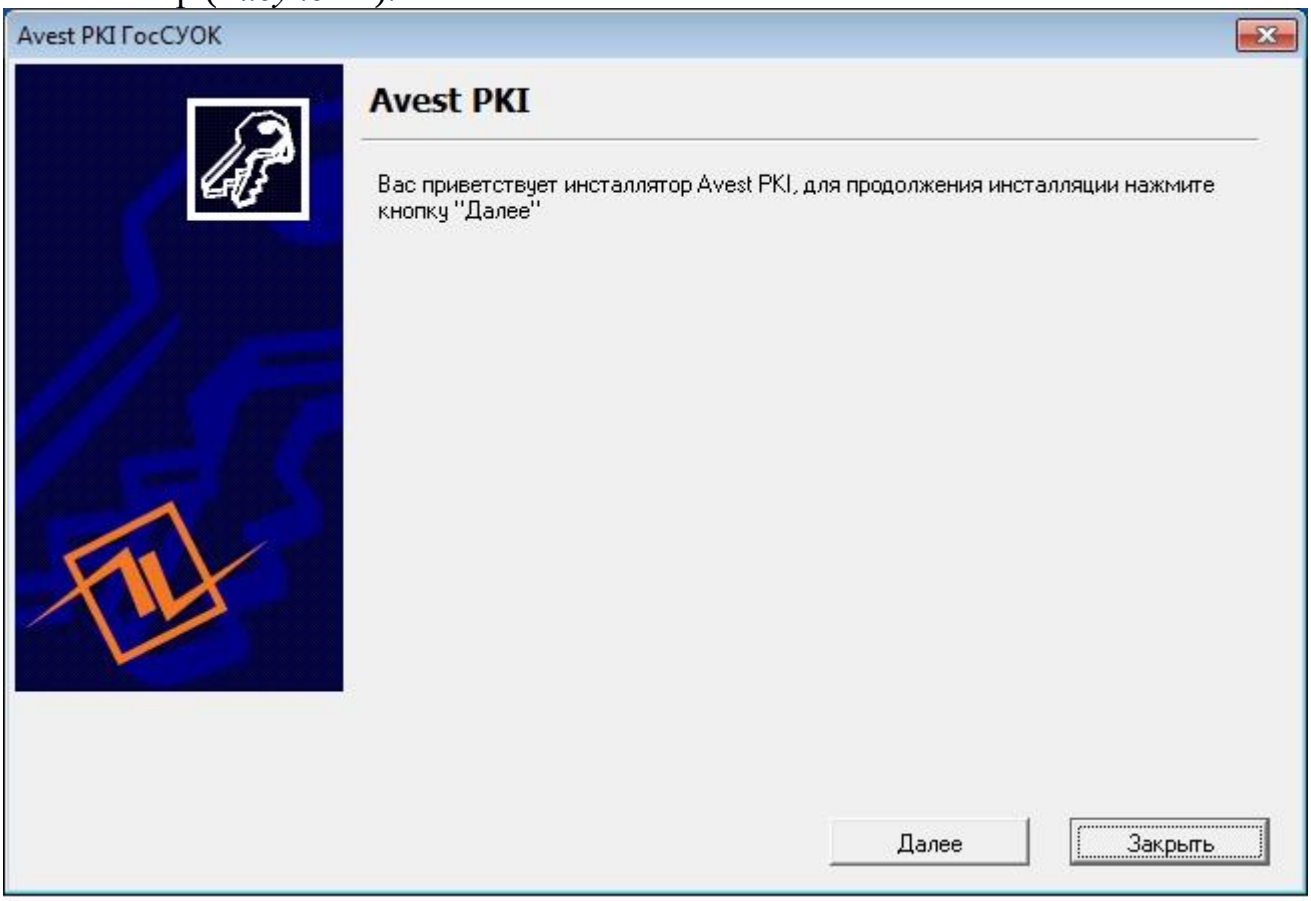


Рисунок 1. Окно мастера установки Avest PKI

В следующем окне следует выбрать режим **Установка** и нажать кнопку «**Далее**».

В появившемся окне представлен список устанавливаемых на компьютер компонентов, отмеченный флажками. В колонке «**Инсталлируемая версия**»

отображается версия устанавливаемого продукта. В списке устанавливаемых компонентов будет указана версия устанавливаемого криптопровайдера Avest CSP Bel, версия устанавливаемого Персонального менеджера сертификатов, AvJCEProv, плагина AvCMXWebP. **Если будет производиться импорт сертификата, компонент «Установка сертификата» также будет отмечен флажком.* Будут установлены сертификаты удостоверяющих центров. (См. *Рисунок 2. Выбор компонентов)*.

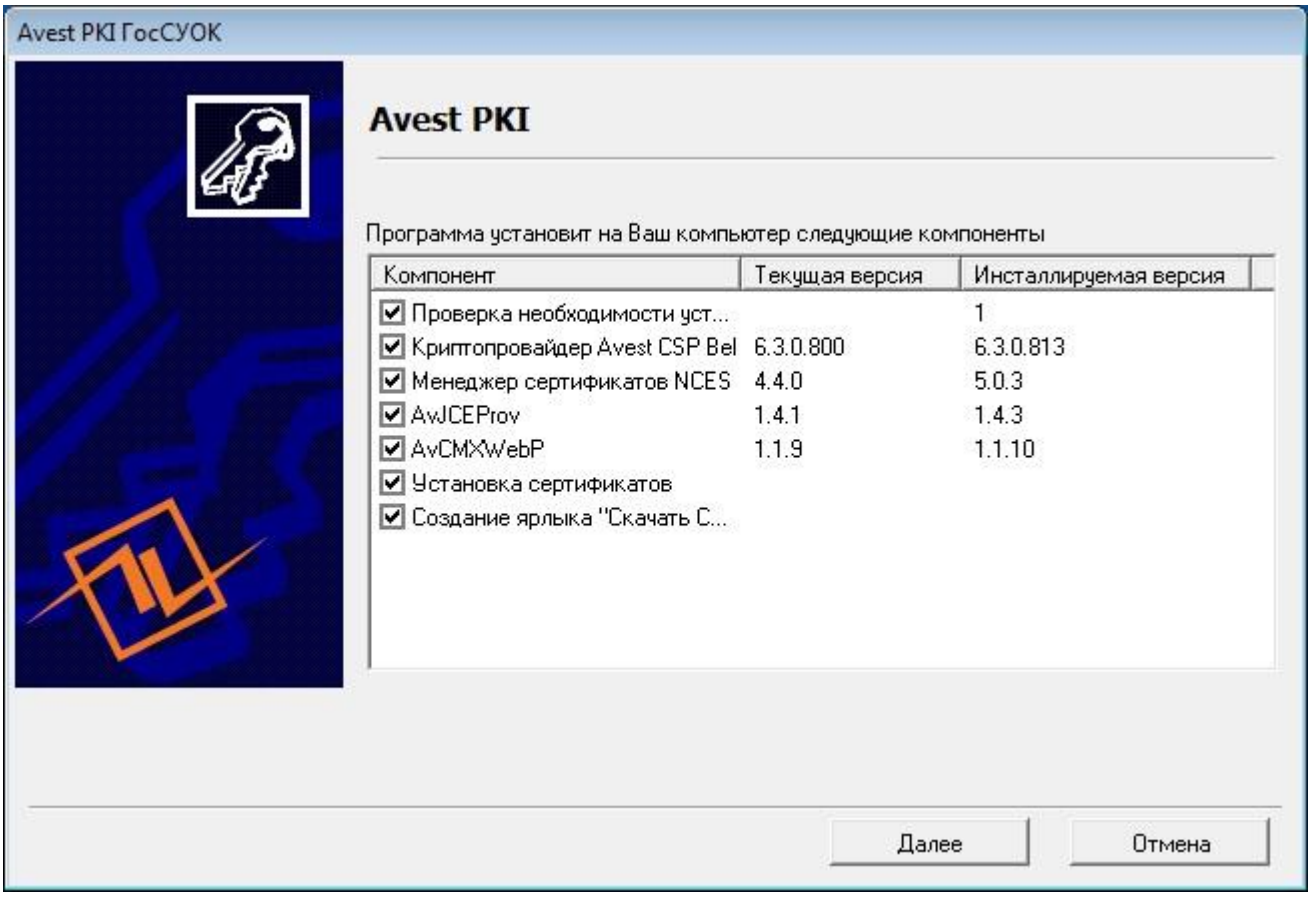


Рисунок 2. Выбор компонентов

Для корректной работы криптопровайдера на операционных системах **Windows XP Service Pack 3** и **Windows Server 2003** обязательно должно быть установлено обновление **KB2836198**. Эта процедура требует перезагрузки компьютера (*Рисунок 3 Предупреждение о перезагрузке*).

Если мастер установки AvPKISetup обнаруживает, что это обновление отсутствует, выдаёт собщение об этом и предлагает нажать «Далее».

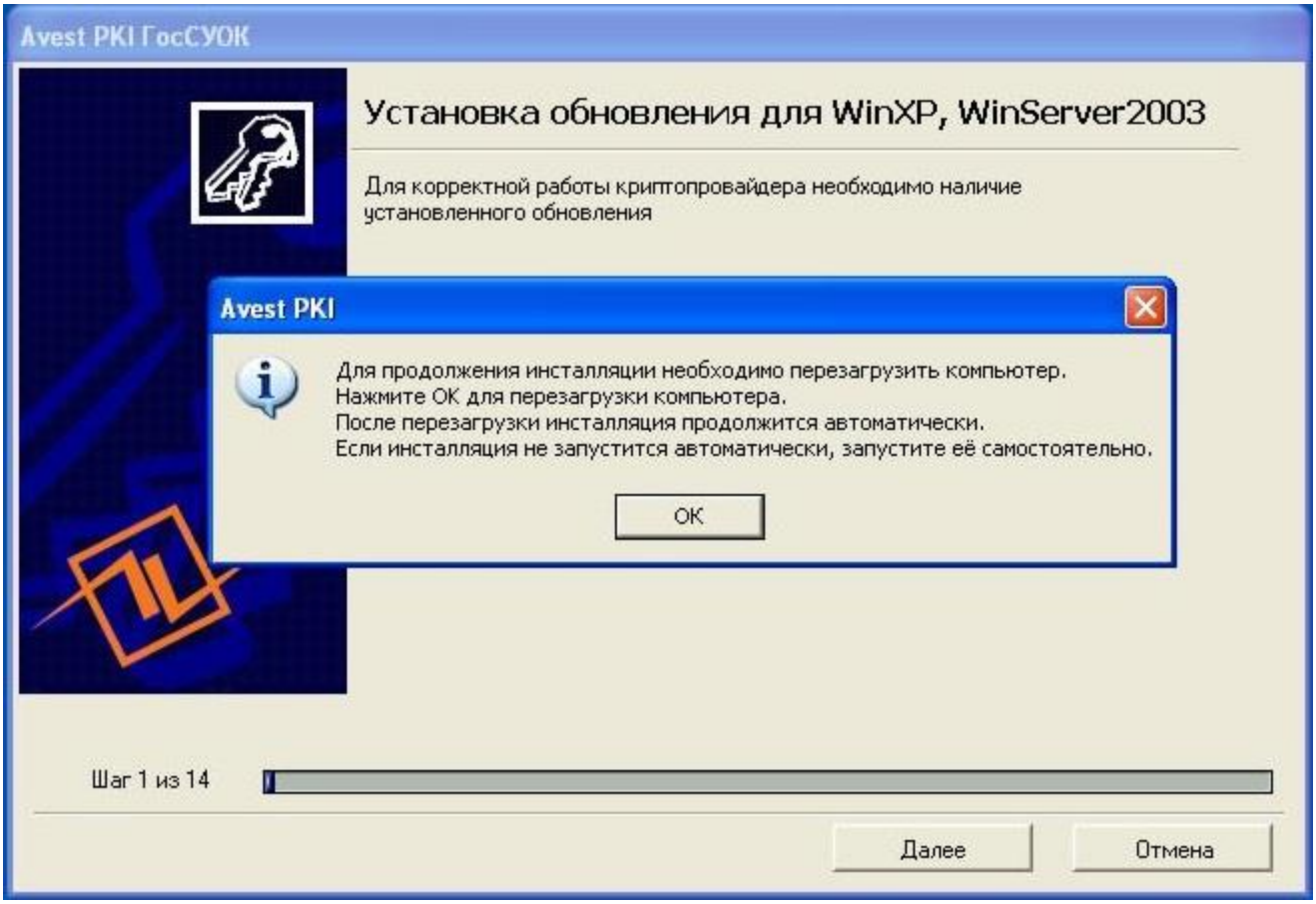


Рисунок 3 Предупреждение о перезагрузке

Если по каким-то причинам AvPKISetup после перезагрузки не запустится сам, то его нужно снова запустить, открыв появившийся на рабочем столе ярлык «Продолжение установки AvPKISetup», как это показано на *Рисунок 4 Ярлык «Продолжение установки AvPKISetup* (ярлык после успешной установки удалится с рабочего стола самостоятельно).

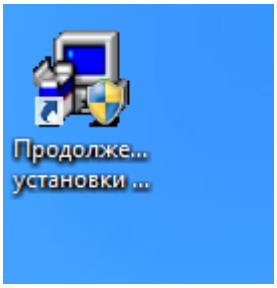


Рисунок 4 Ярлык «Продолжение установки AvPKISetup»

Следующий шаг мастера установки – сбор случайных данных. Для их сбора нужно подвигать мышью в окне установки, пока индикатор сбора случайных данных не достигнет отметки 100%.

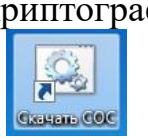
Далее произойдет установка или обновление:

- криптопровайдера Avest CSP Bel (после установки будет выполнена перезагрузка компьютера),
- веб плагина AvCMXWebP,
- программного комплекса AvJCEProv,
- персонального менеджера сертификатов AvPCM,

- импорт сертификата в Личный справочник и импорт атрибутного сертификата, *если сертификат был помещен в папку data* (см. Приложение 1. Установка сертификатов),
- установка доверия сертификатам Корневых удостоверяющих центров.

Перед установкой сертификатов корневых удостоверяющих центров на экране возникает «Предупреждение системы безопасности» Windows о добавлении сертификата в список доверенных УЦ, в этом сообщении всегда указываются атрибуты помещаемого сертификата. Нужно сравнить имя сертификата корневого УЦ с именем, указанным в бумажной карточке открытого ключа, а значения поля «Отпечаток» со значениями, изображенными на рисунке. Если всё соответствует, то нажать кнопку «Да» (См. Рисунок *15* Предупреждение системы безопасности)

Мастер установки произведет все действия автоматически.

Для получения/обновления списков отзыва сертификатов (СОС) на рабочем столе во время установки криптографического программного обеспечения будет создан ярлык «Скачать СОС». 

Перед завершением инсталляции программа выведет окно о результате работы. В графе «**Состояние**» можно увидеть, произошла ли установка того или иного компонента.

Более подробная информация находится в «**Журнале работы**», который доступен при нажатии соответствующей кнопки.

Для завершения работы AvPKISetup нужно нажать кнопку «**Закрыть**» (*Рисунок 5. Завершение установки*).

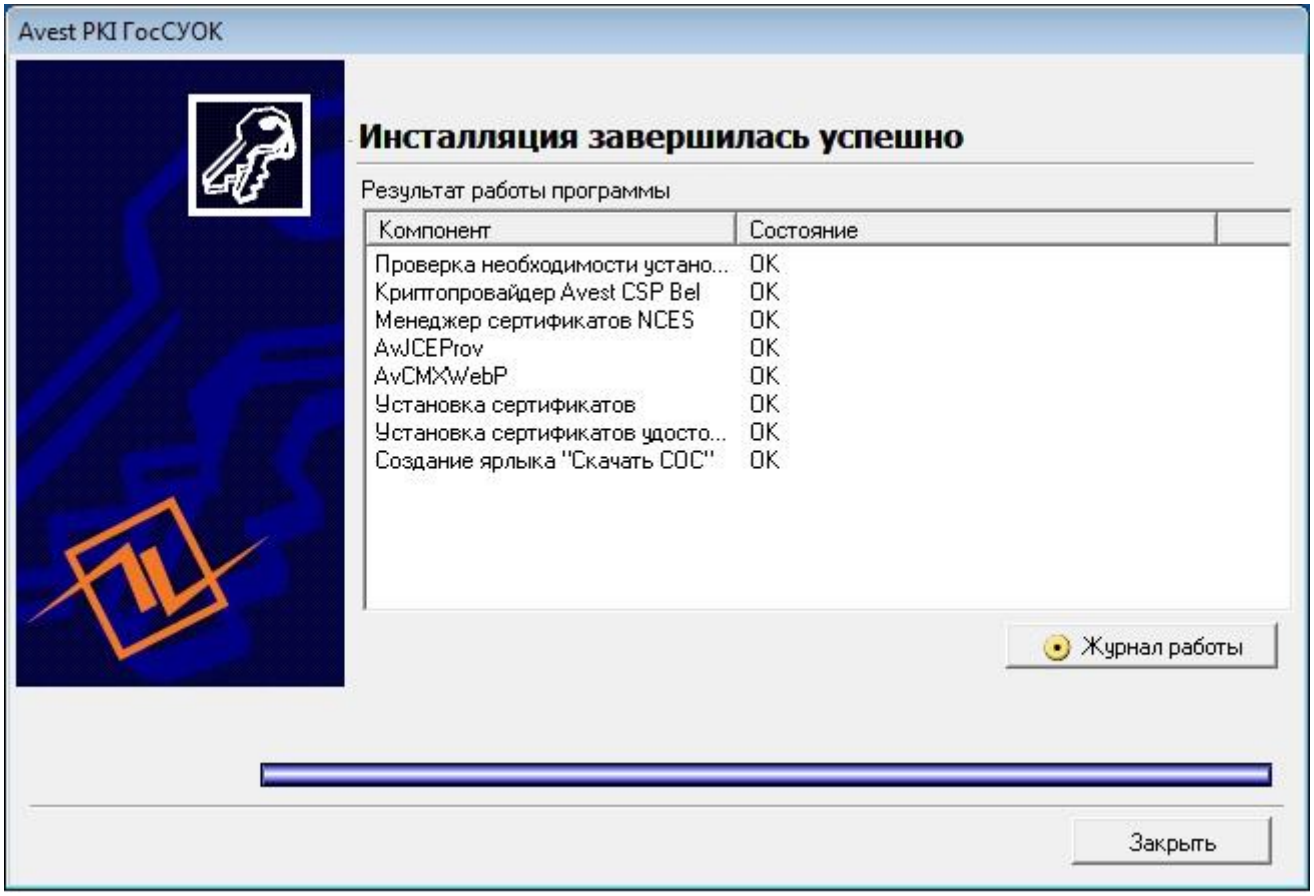


Рисунок 5. Завершение установки

Обновление комплекта абонента завершено.

Сертификат ГосСУОК может быть использован в различных информационных системах, например:

- подписание электронных деклараций, работа на сайте portal.nalog.gov.by;
- подписание ЭСЧФ, работа на сайте vat.gov.by;
- работа на сайте portal.gov.by;
- работа на сайте portal2.ssf.gov.by;
- и в прочих государственных сервисах, уточняйте, пожалуйста, есть ли такая возможность, у владельца сервиса.

Удаление криптографического программного обеспечения с помощью объединенного инсталлятора

Для того, чтобы корректно удалить криптографическое программное обеспечение, необходимо использовать объединенный инсталлятор AvPKISetup. Для начала удаления ПО необходимо запустить файл **AvPKISetup2.exe**.

В окне мастера установки следует нажать кнопку «Далее», В следующем окне следует выбрать режим «**Удаление»** и нажать кнопку «Далее» (см. *Рисунок 6 Выбор типа инсталляции*).

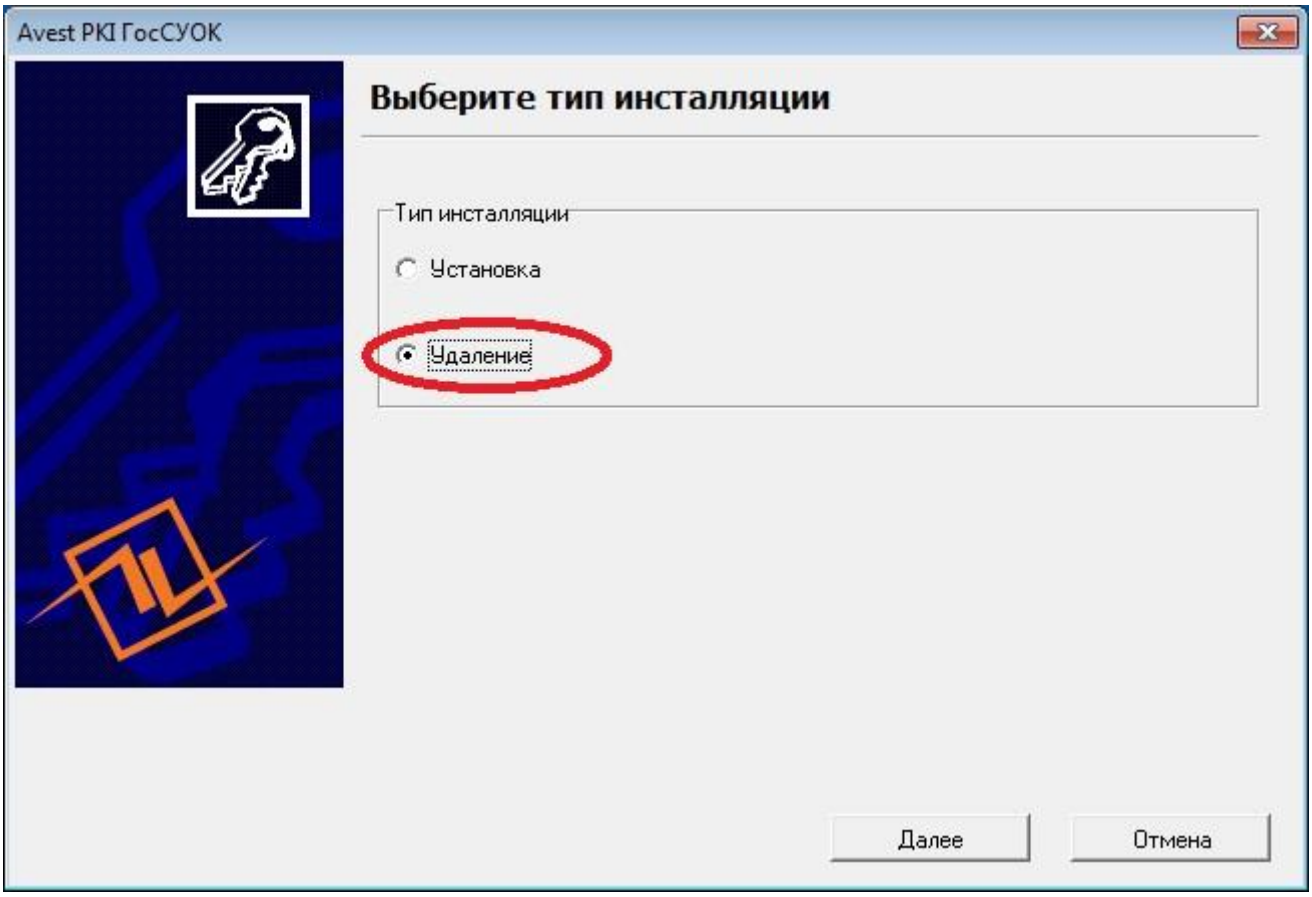


Рисунок 6 Выбор типа инсталляции

В следующем окне программа выводит список удаляемых компонентов. Необходимо выбрать те компоненты, которые надо удалить, и нажать кнопку «Далее» (см. *Рисунок 7 Список удаляемых компонентов*).

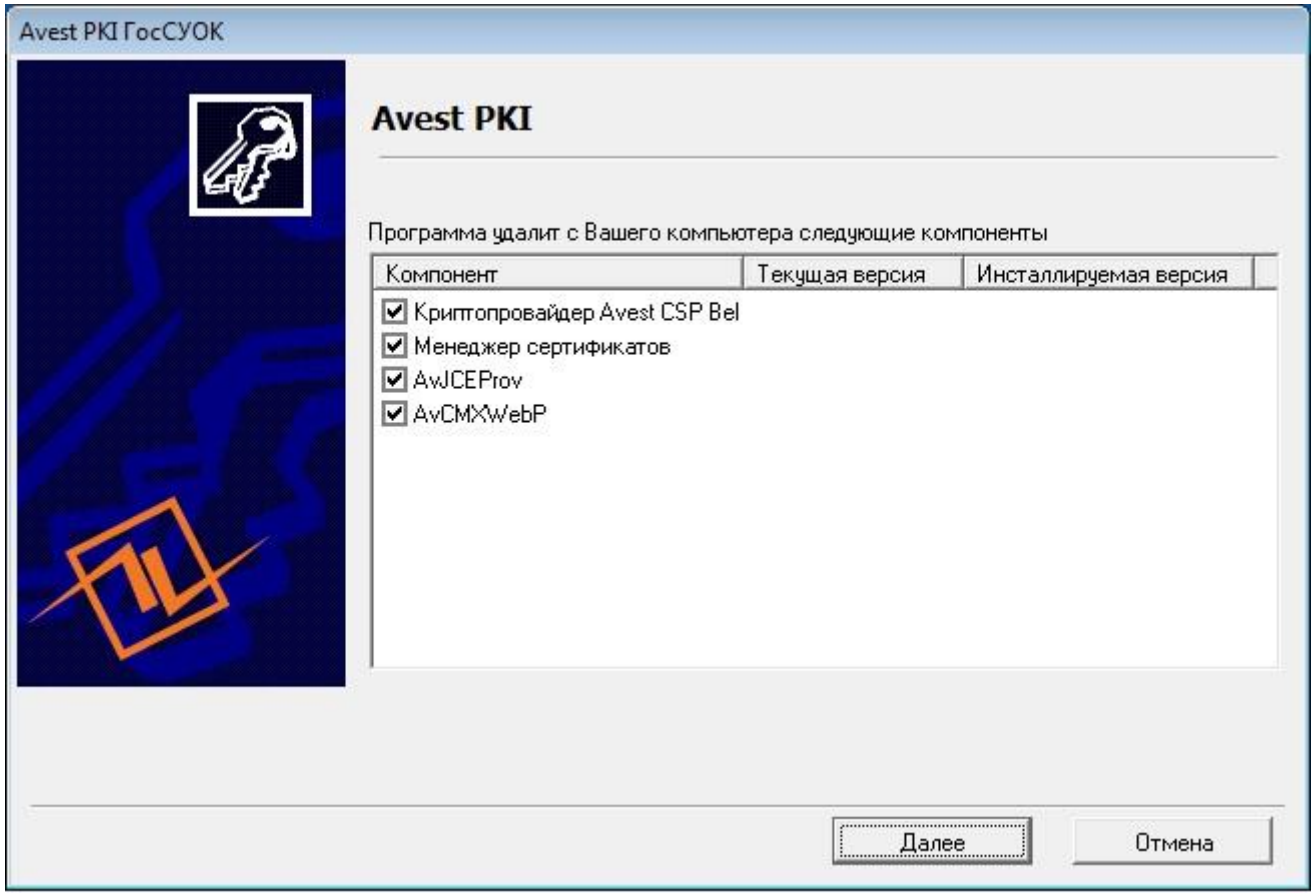


Рисунок 7 Список удаляемых компонентов

В следующем окне отображается результат работы мастера установки «AvPKISetup». В столбце «Компонент» отображается что именно было удалено, в столбце «Состояние» отображается статус удаления компонентов (см. *Рисунок 8 Результат работы программы*).

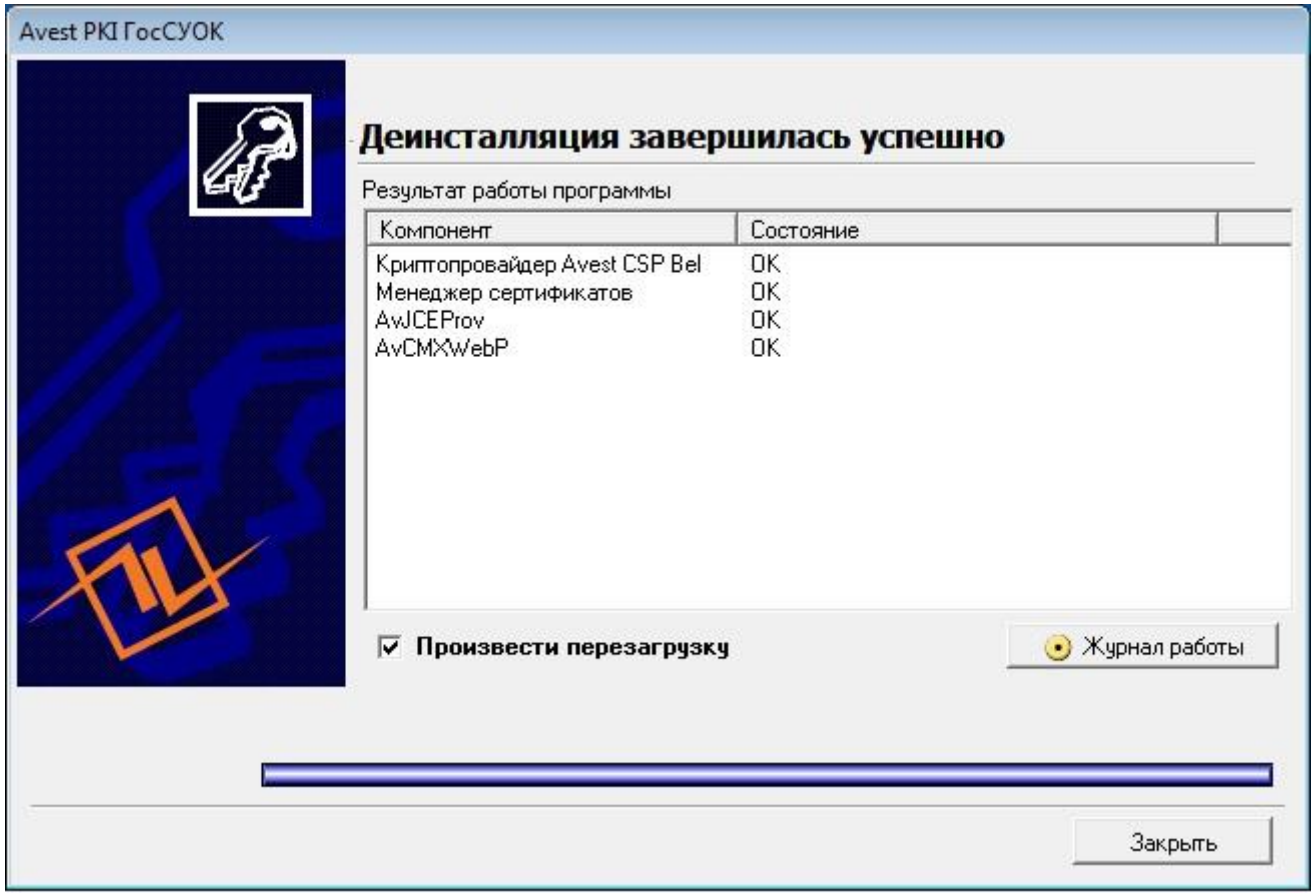


Рисунок 8 Результат работы программы

В этом же окне возможно отказаться от перезагрузки путем снятия галочки. Если отметка о перезагрузке была снята, появится окно с предупреждением о необходимости перезагрузки (см. *Рисунок 9 Предупреждение о необходимости перезагрузки)*.

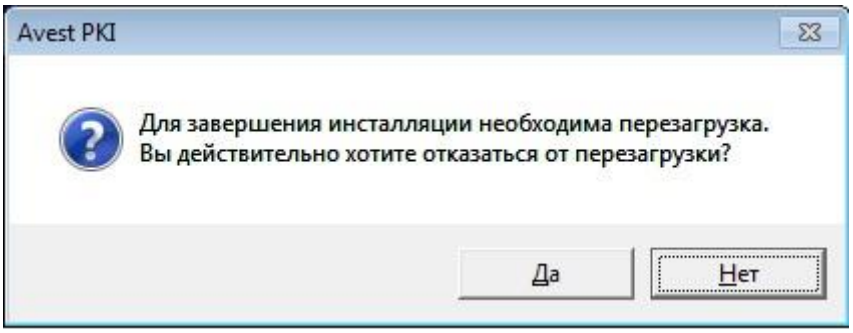


Рисунок 9 Предупреждение о необходимости перезагрузки

Также можно более подробно просмотреть результат работы мастера установки AvPKISetup, нажав кнопку «Журнал работы» (см. *Рисунок 10 Журнал работы*).

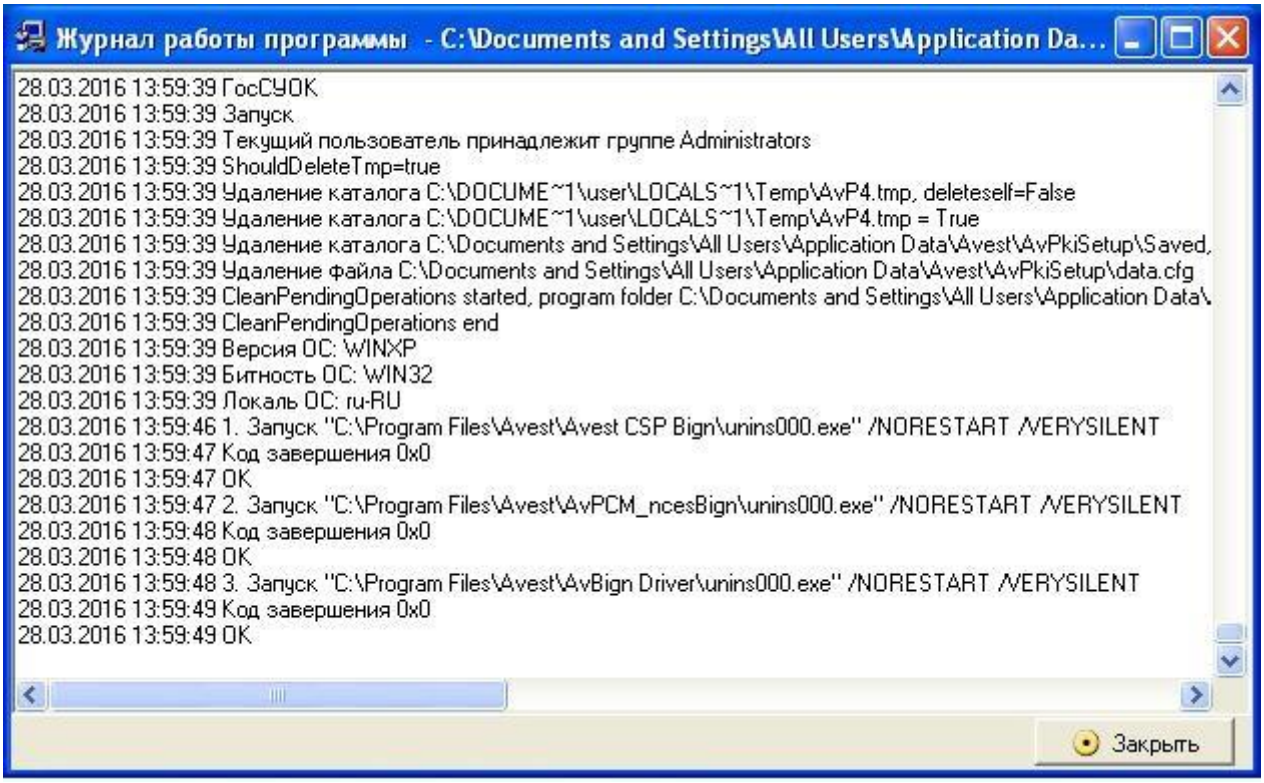


Рисунок 10 Журнал работы

Приложение 1. Установка сертификатов в процессе обновления комплекта абонента

На шаге «Установка сертификатов», *если сертификат был помещен в папку data*, открывается окно Мастера импорта и происходит установка сертификатов в системные справочники Windows (см. *Рисунок 11 Импортируемые сертификаты*). Галочками отмечены сертификаты, которые будут проимпортированы и которые отсутствуют в системном справочнике. Необходимо нажать кнопку «Далее». Если в списке импортируемых объектов сертификаты повторяются, оставьте галочки по умолчанию, как предлагает Мастер импорта.

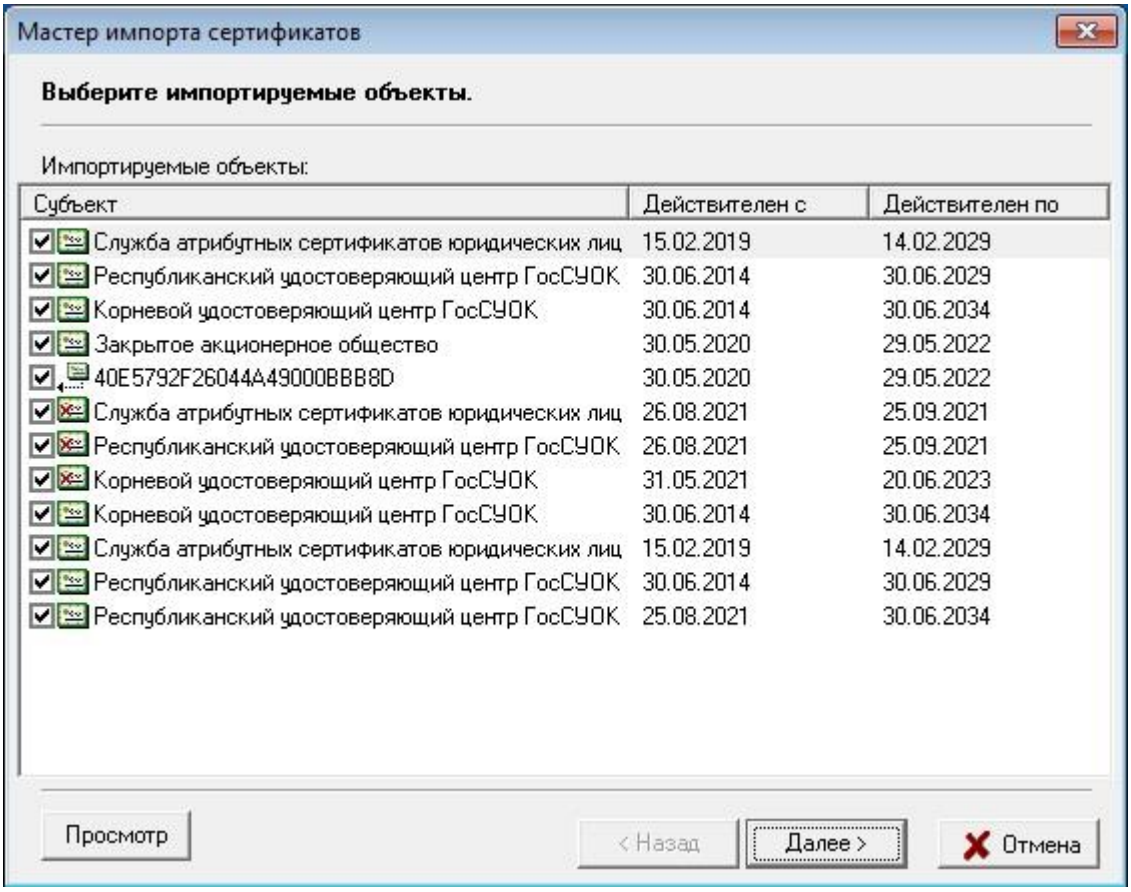


Рисунок 11 Импортируемые сертификаты

Мастер импорта уведомит о количестве импортированных сертификатов (см. *Рисунок 12 Уведомление о количестве импортируемых сертификатов*).

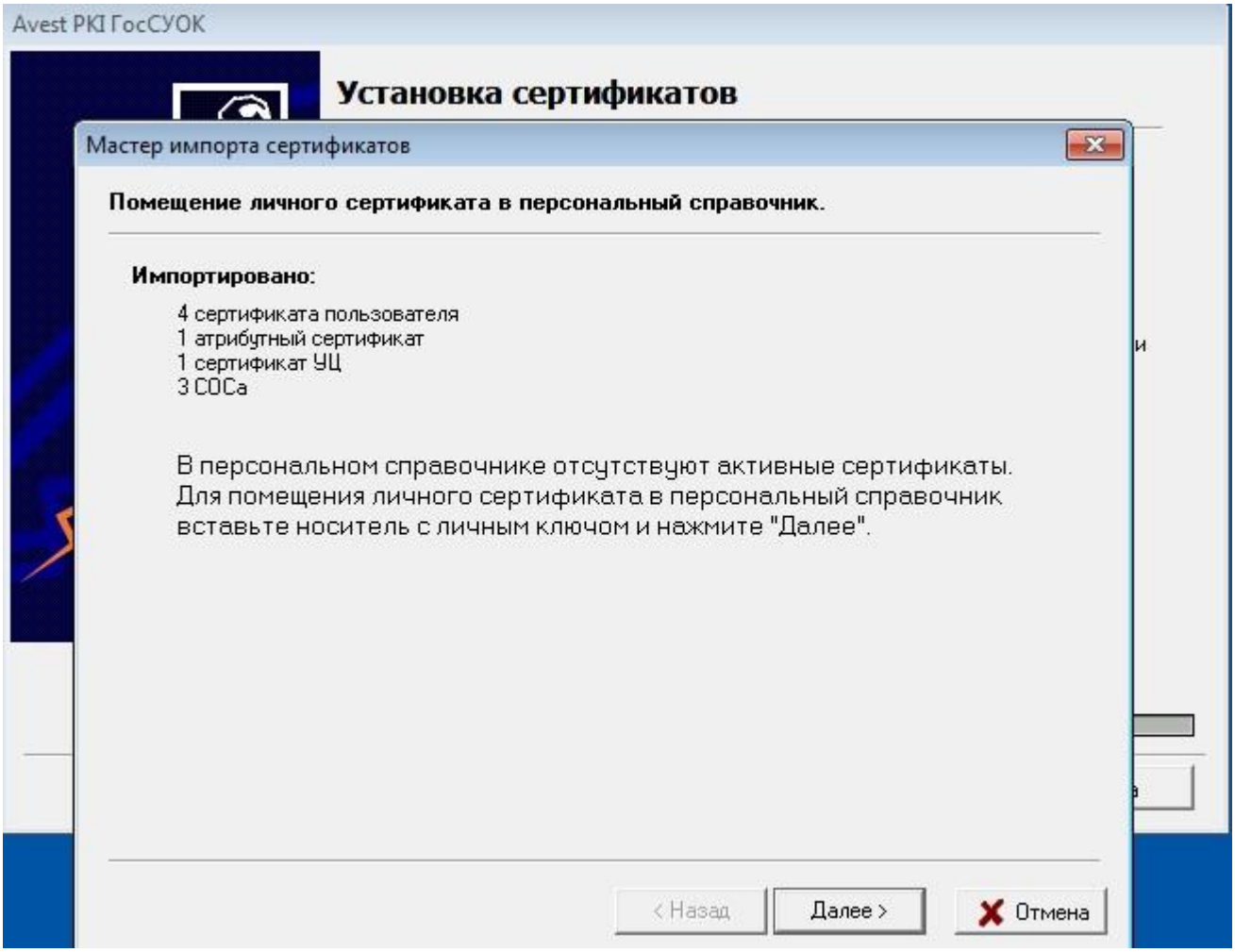


Рисунок 12 Уведомление о количестве импортируемых сертификатов

Для установки личного сертификата надо вставить носитель **AvToken** (**AvPass**), на котором записан личный ключ, в USB-разъем компьютера и нажать кнопку «Далее». В окне выбора контейнера отобразятся все контейнеры с личными ключами, записанные на носителе **AvToken** (**AvPass**). Если на носителе записано более одного контейнера, то в списке нужно выбрать тот, который соответствует Вашему личному сертификату. Определить это можно, например, по дате регистрации в УЦ предприятия. После того, как соответствующий контейнер выбран, нужно нажать на кнопку «Далее» (см. *Рисунок 13 Выбор контейнера*).

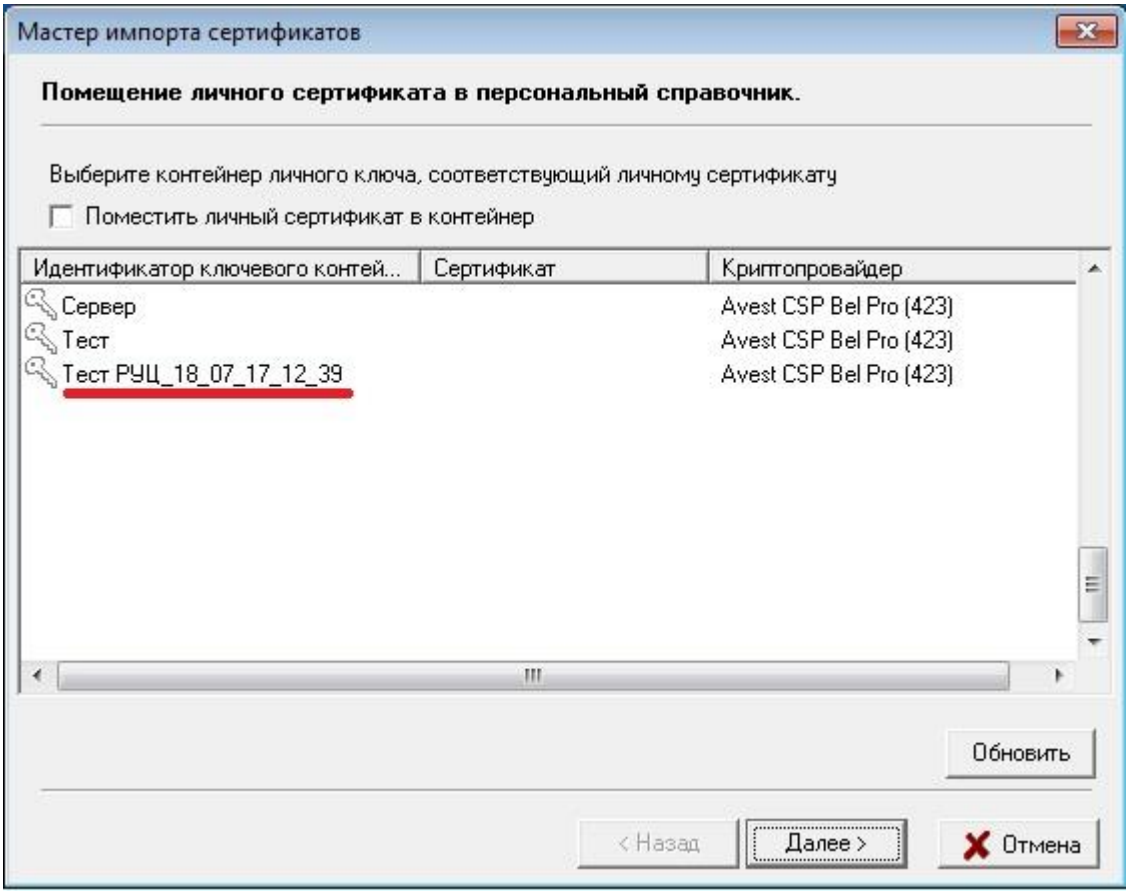


Рисунок 13 Выбор контейнера

В появившемся окне криптопровайдера нужно ввести пароль, который был задан при создании личных ключей, и нажать кнопку «ОК».

На следующем шаге будет установлено доверие сертификатам Корневых удостоверяющих центров (см. *Рисунок 14 Сертификаты корневых удостоверяющих центров*).

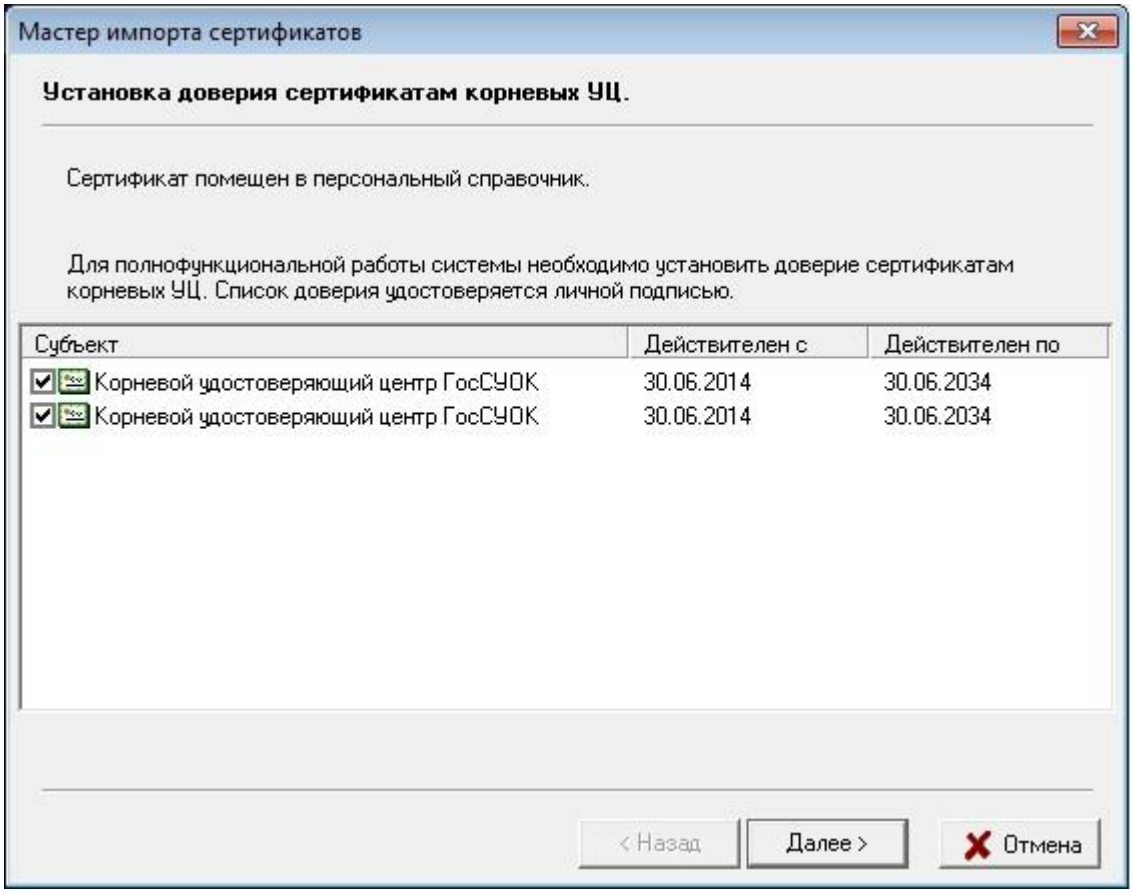


Рисунок 14 Сертификаты корневых удостоверяющих центров

Перед установкой сертификатов корневых удостоверяющих центров на экране возникает «Предупреждение системы безопасности» Windows о добавлении сертификата в список доверенных УЦ, в этом сообщении всегда указываются атрибуты помещаемого сертификата. Нужно сравнить имя сертификата корневого УЦ с именем, указанным в бумажной карточке открытого ключа, а значения поля «Отпечаток» со значениями, изображенными на рисунке. Если всё соответствует, то нажать кнопку «Да» (см. *Рисунок 15 Предупреждение системы безопасности*).

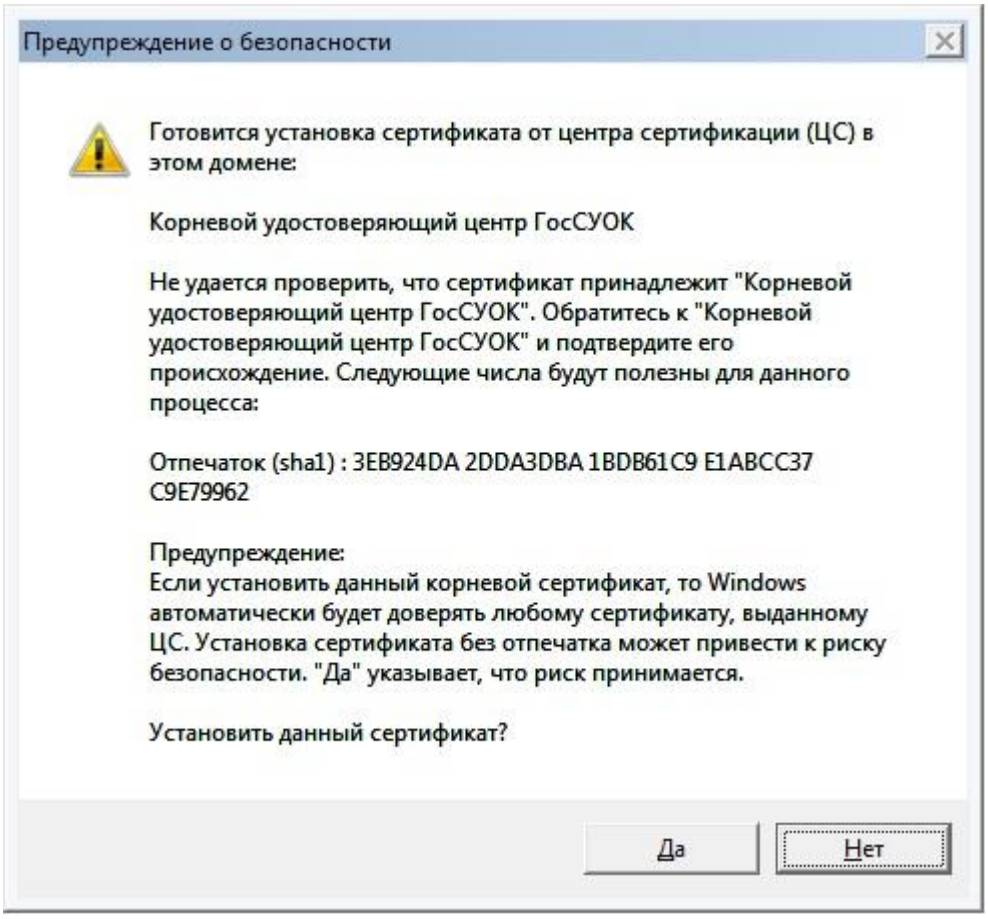


Рисунок 15 Предупреждение системы безопасности

На следующем шаге Мастер импорта уведомит о сертификатах, которым было установлено доверие. Нажмите кнопку «Закрыть». (См. *Рисунок 16 Завершение работы мастера импорта сертификатов)*

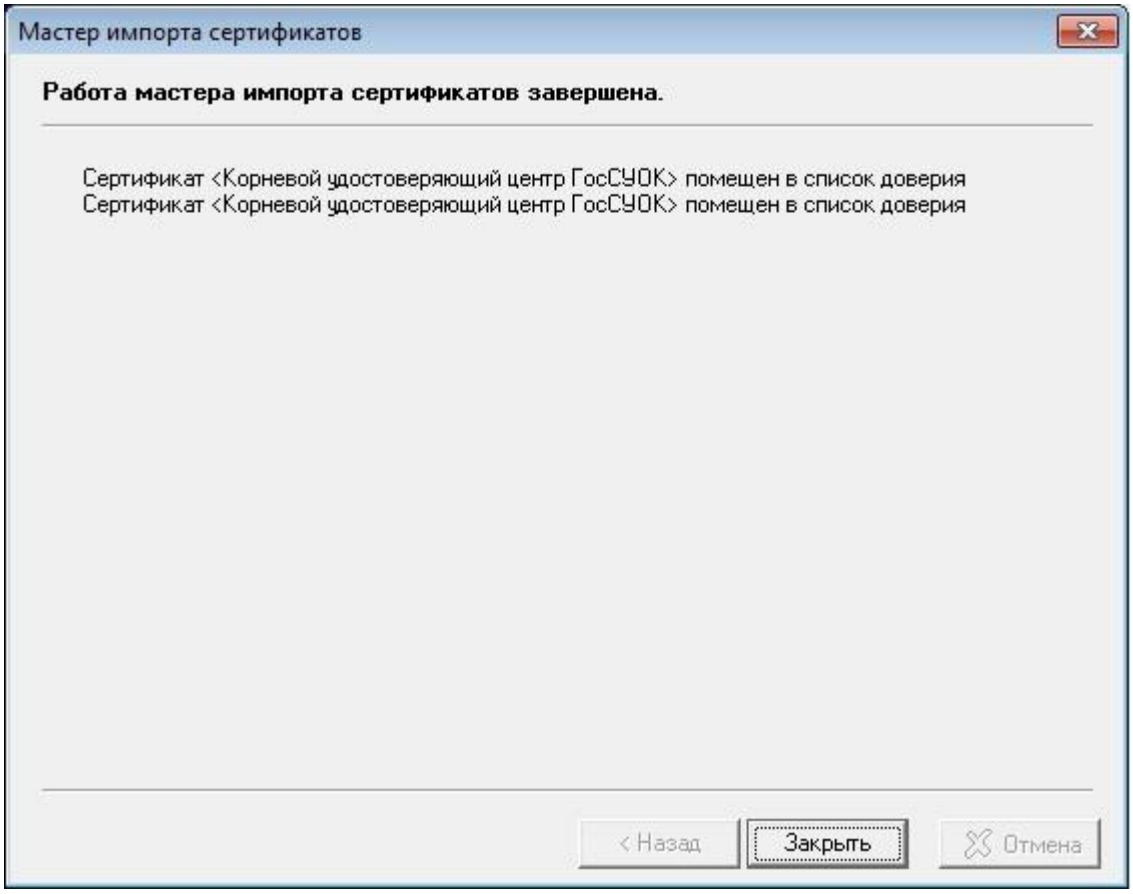


Рисунок 16 Завершение работы мастера импорта сертификатов

Приложение 2. Импорт сертификата, если программное обеспечение уже установлено на компьютер

В случае когда программное обеспечение Авест на компьютере было ранее установлено и необходимо проимпортировать только личный сертификат, надо из меню Пуск – Все программы – Авест для НЦЭУ запустить Персональный менеджер сертификатов Авест для ГосСУОК без авторизации. (См. Рисунок *17* Запуск менеджера без авторизации)

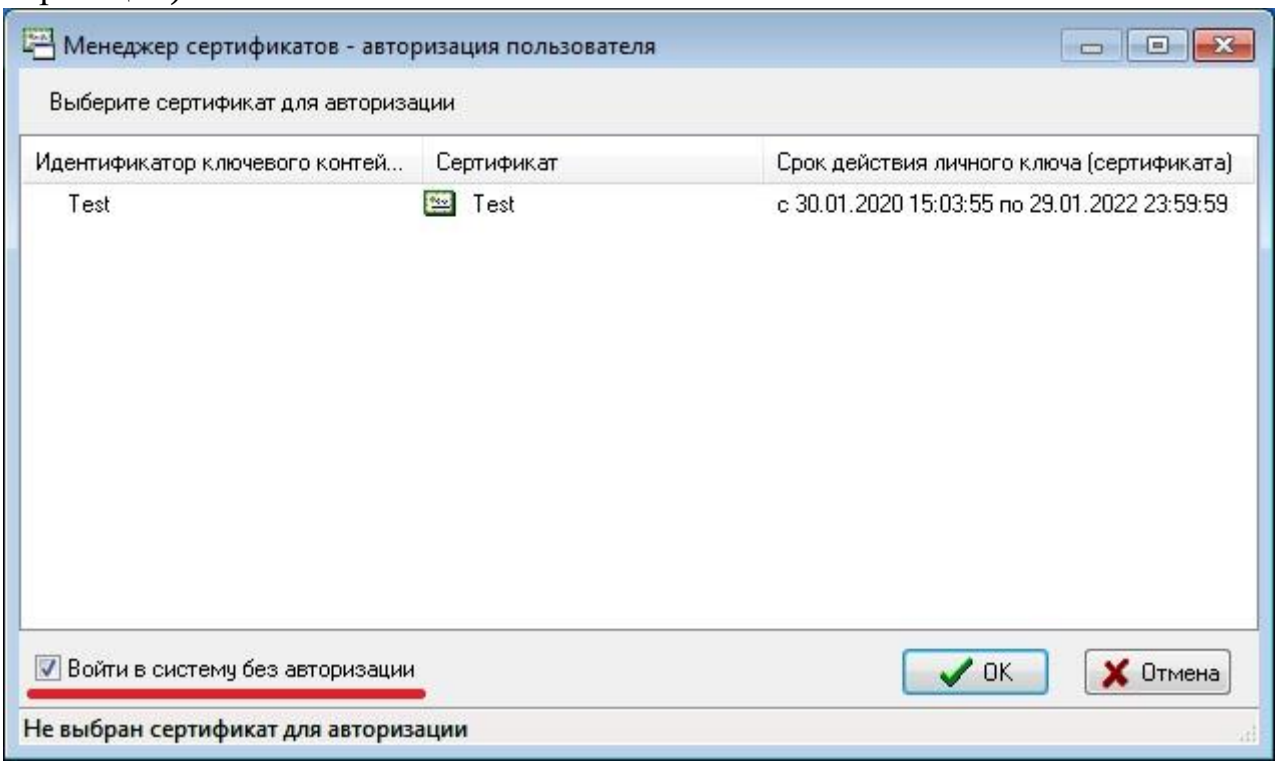


Рисунок 17 Запуск менеджера без авторизации

Выбрать пунк меню Файл – Импорт сертификатов/СОС. (См. Рисунок *18* Импорт сертификата)

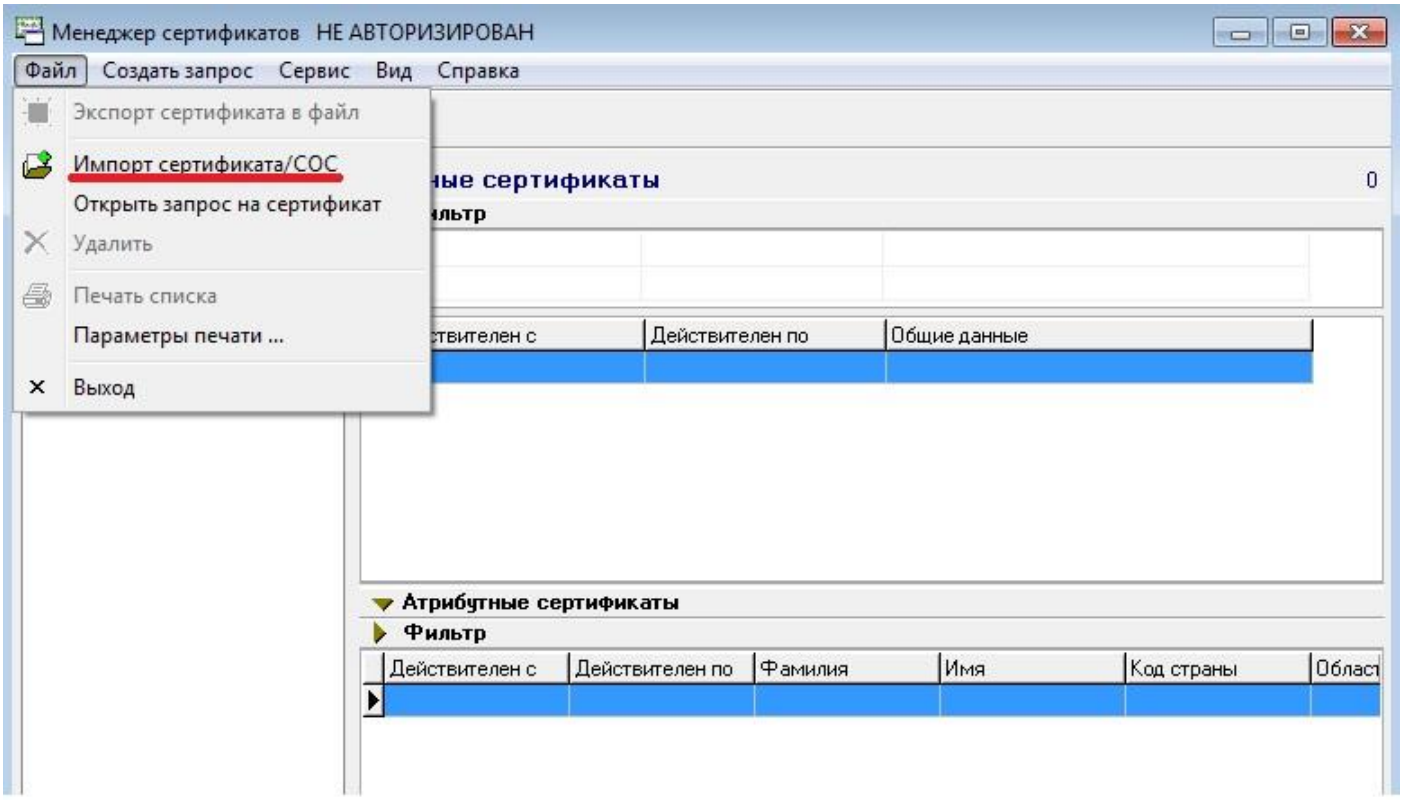


Рисунок 18 Импорт сертификата

В диалоговом окне мастера импорта сертификатов, нажав кнопку Обзор, указать имя каталога, из которого будет производиться импорт личного сертификата, цепочки сопутствующих сертификатов Удостоверяющих центров и СОС, выпущенных УЦ. (См. Рисунок *19* Выбор импортируемого файла)

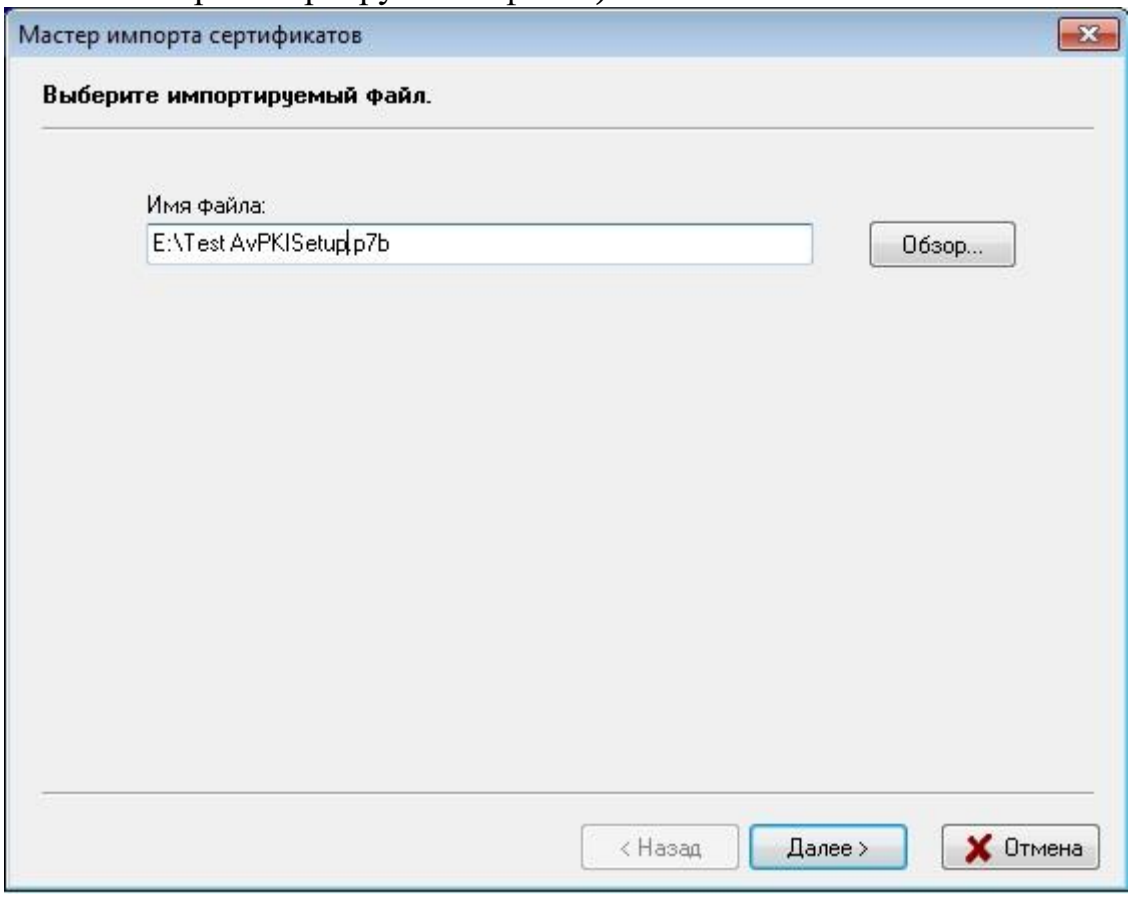


Рисунок 19 Выбор импортируемого файла

В появившемся окне в виде таблицы будут отражены все объекты, которые входят в импортируемый файл. (См. Рисунок *20* Информация об импортируемых объектах)

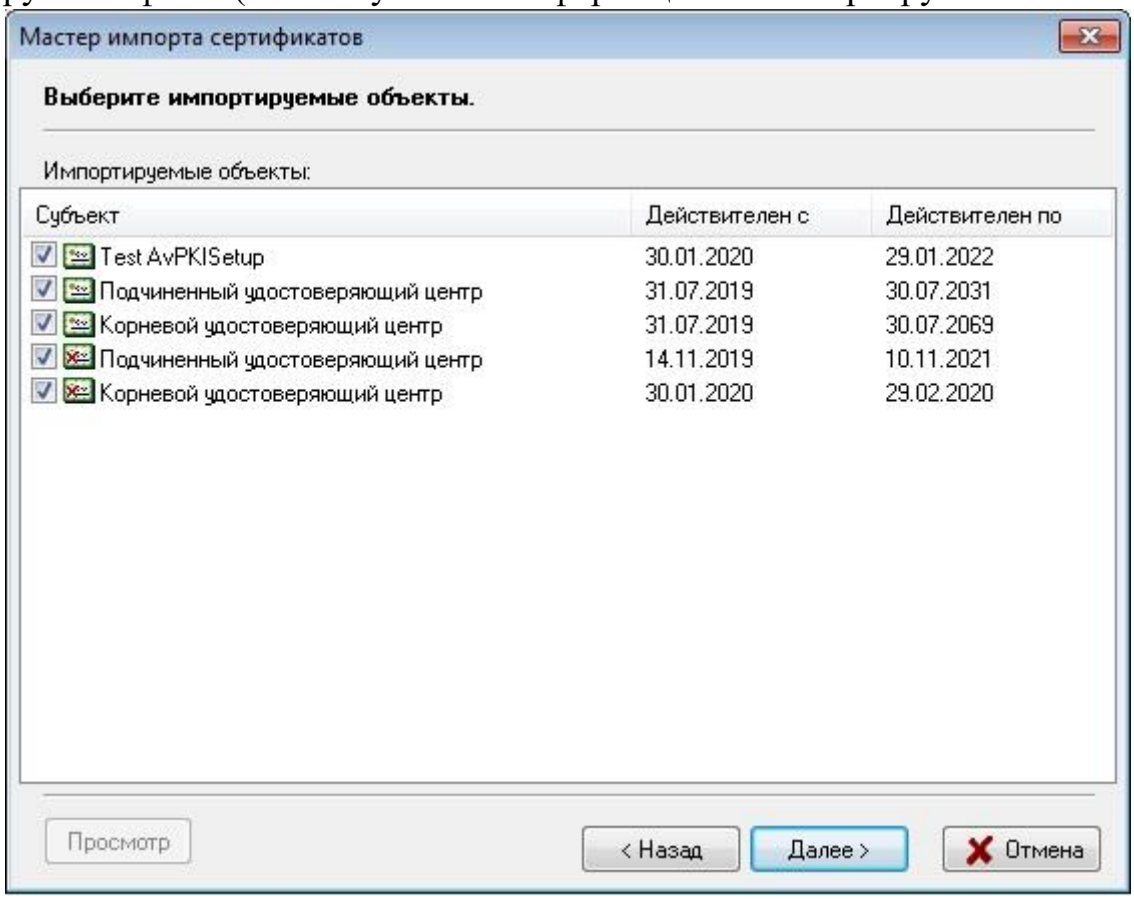


Рисунок 20 Информация об импортируемых объектах

В следующем окне содержится информация о количестве импортированных объектов и предложено поместить личный сертификат в персональный справочник. (См. Рисунок *21* Уведомление о количестве импортируемых сертификатов)

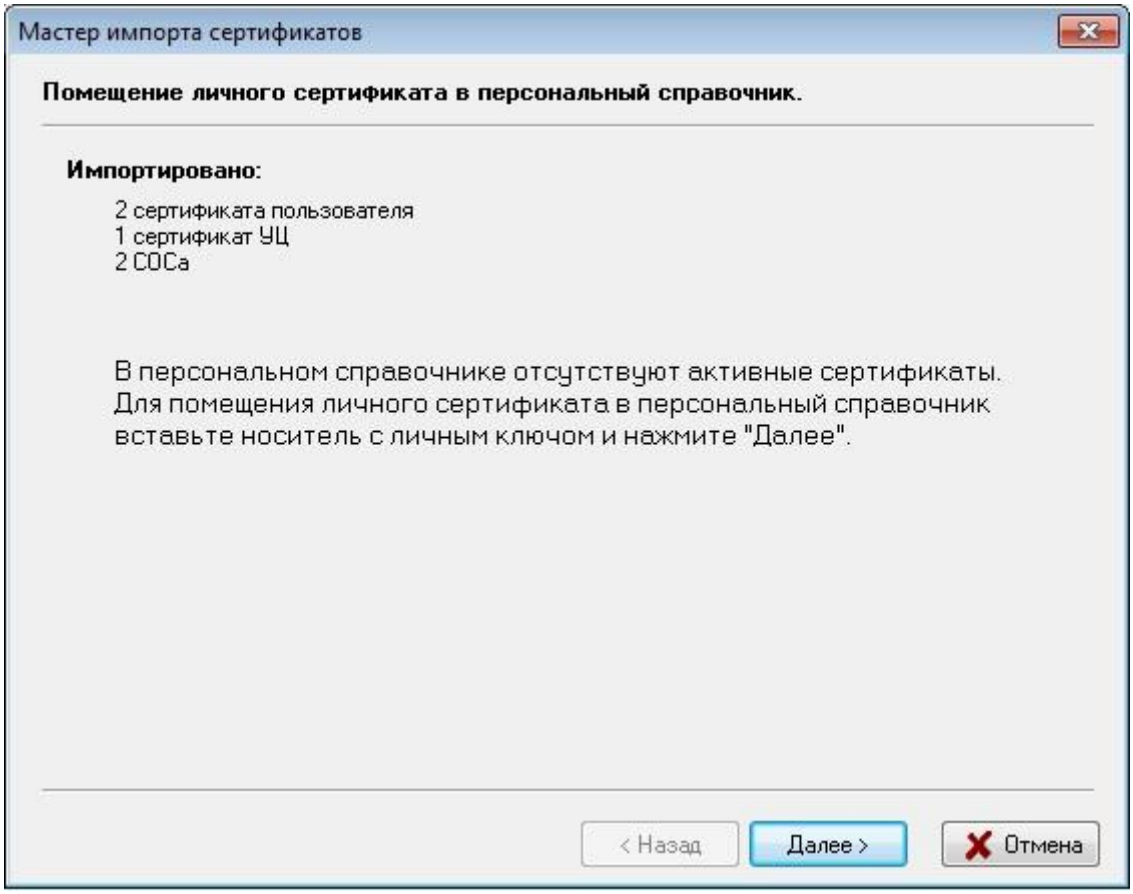


Рисунок 21 Уведомление о количестве импортируемых сертификатов

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 необходимо из данного списка выбрать контейнер личного ключа, который соответствует личному сертификату и нажать кнопку «Далее». (См. Рисунок *22* Выбор контейнера личного ключа, соответствующего личному сертификату)

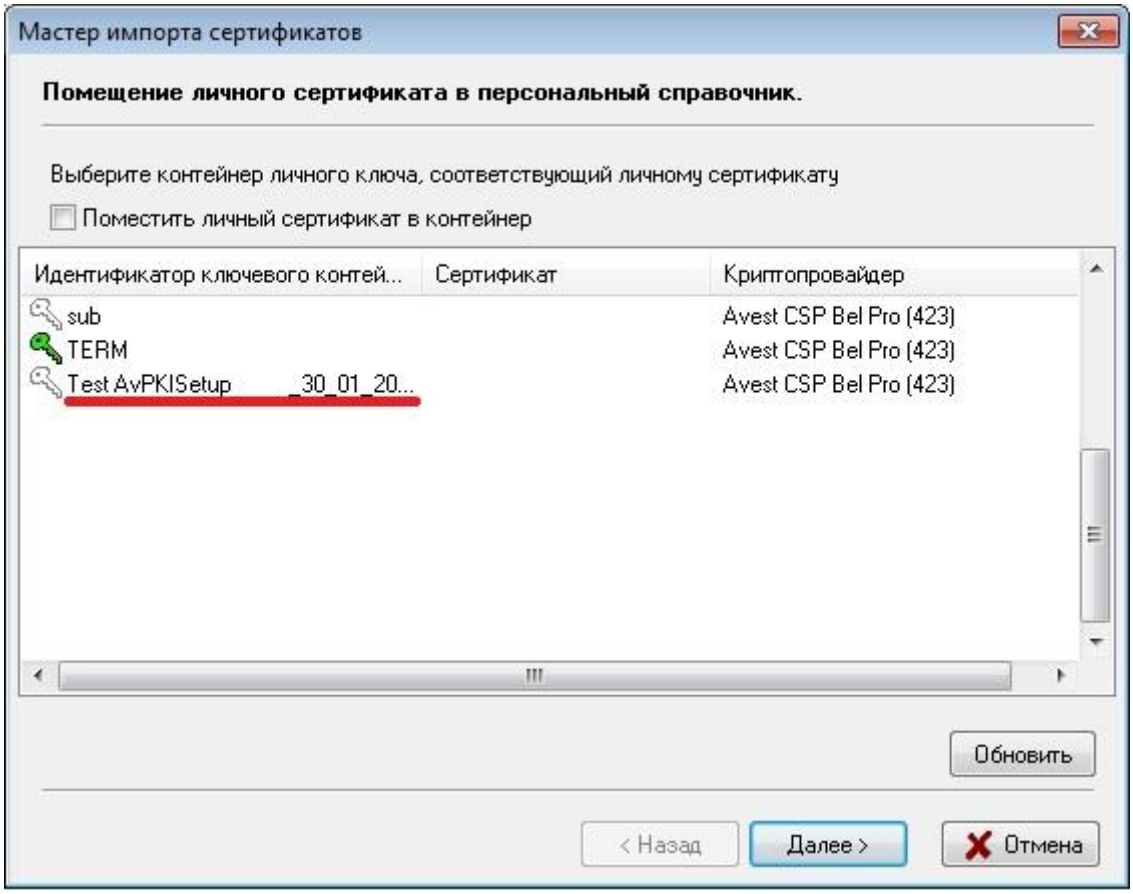


Рисунок 22 Выбор контейнера личного ключа, соответствующего личному сертификату

Затем для доступа к ключевому контейнеру в окне «Контейнер личных ключей» необходимо ввести пароль, который Вы вводили при генерации личных ключей. (См. Рисунок *23* Ввод пароля доступа к контейнеру личного ключа)

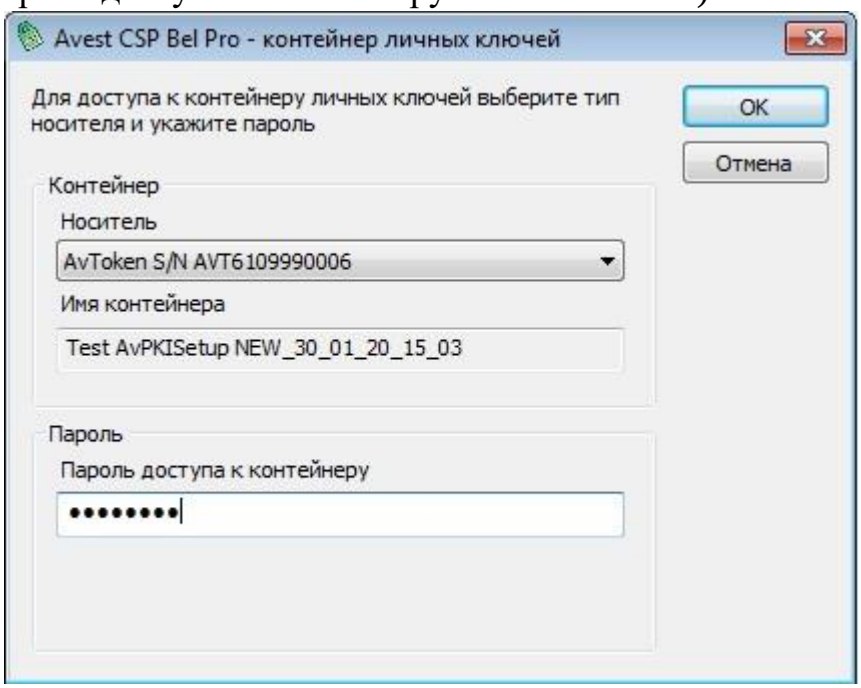


Рисунок 23 Ввод пароля доступа к контейнеру личного ключа

Для полнофункциональной работы программы необходимо установить доверие к корневому сертификату УЦ. Для этого в следующем окне надо включить

флажок «Установить доверие сертификату корневого УЦ». (См. Рисунок *24* Установка доверия сертификату корневого УЦ)

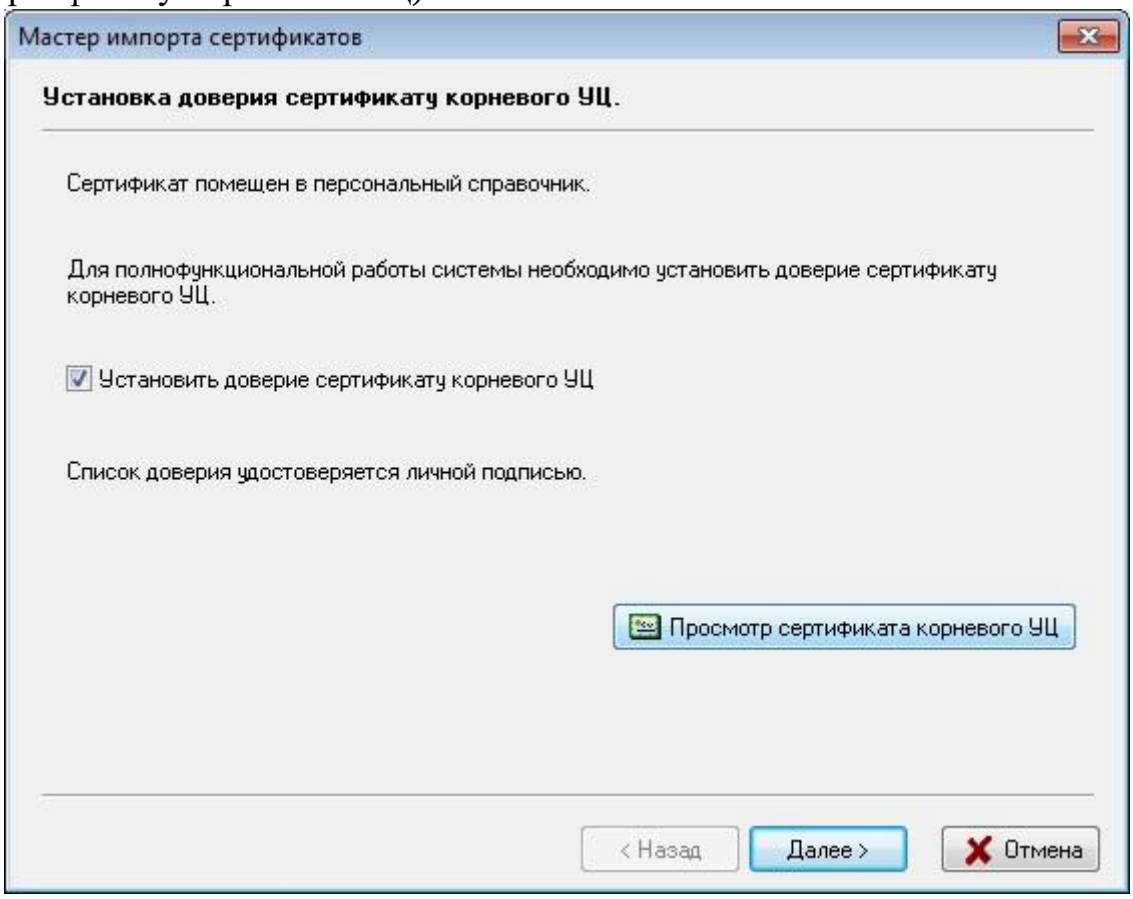


Рисунок 24 Установка доверия сертификату корневого УЦ

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 *25* Предупреждение системы безопасности)

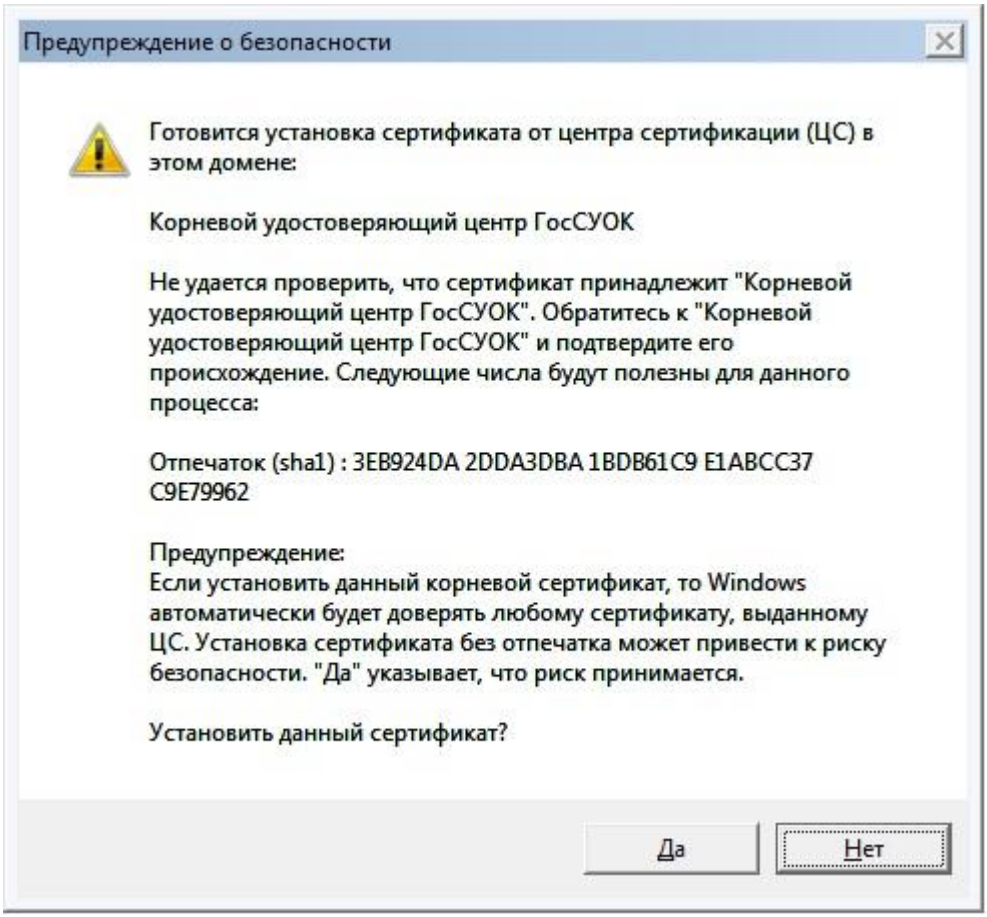


Рисунок 25 Предупреждение системы безопасности

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

Приложение 3. Способы получения/обновления списков отзыва сертификатов СОС

1) Через Персональный менеджер сертификатов Авест для ГосСУОК.

Для того, чтобы запустить обновление СОС, в персональном менеджере сертификатов нужно выбрать меню «Сервис» – «Обновление СОС и сертификатов УЦ» - нажать «Далее». Интернет при этом должен быть включён.

* **Внимание!** Если выход в интернет осуществляется через прокси, необходимо задать настройки прокси в конфигурационном файле *AvCmMsg.ini*, который находится в `c:\Program Files (x86)\Avest\AvPCM_nces\` - ОС 64-разрядная или `c:\Program Files \Avest\AvPCM_nces\` - ОС 32-разрядная. Для этого необходимо добавить секцию HttpProxy в следующем виде:

```
[HttpProxy]
ProxyServer=
ProxyPort=
ProxyUsername=
ProxyPassword=
BasicAuthentication=FALSE
ReadTimeOut=
```

2) С помощью файла-«батника» get_crl.bat.

Для получения/обновления списков отзыва сертификатов (СОС) с помощью **get_crl.bat** на рабочем столе при установке криптографического программного обеспечения создается ярлык «Скачать СОС», нажав на который можно получить актуальные СОС.

Или зайти по пути `c:\Program Files (x86)\Avest\AvPCM_nces` или `c:\Program Files \Avest\AvPCM_nces\` и запустить файл **get_crl.bat.**

* **Внимание!** Если выход в интернет осуществляется через прокси, необходимо в файле **get_crl.bat,** который находится в `c:\Program Files (x86)\Avest\AvPCM_nces\` - ОС 64-разрядная или `c:\Program Files \Avest\AvPCM_nces\` - ОС 32-разрядная, раскомментировать строки (удалить слово «rem»):

```
set PX_USER
set PX_PASS
set http_proxy
```

и указать данные пользователя и адрес прокси.

3)Скачать СОС с сайта nces.by и проимпортировать через Персональный менеджер сертификатов Авест для ГосСУОК. Для этого

- из папки Пуск – Все программы -Авест для НЦЭУ запустить Персональный менеджер сертификатов Авест для ГосСУОК с авторизацией или без авторизации,
- в менеджере выбрать пункт меню Файл – Импорт сертификата/СОС, указать путь к скачанному файлу СОС в формате *.crl и проимпортировать его, следуя указаниям.

Скачивание СОС на ОС Windows XP

На ОС Windows XP не скачиваются СОС, размещённые по URL с https. Это связано с тем, что Windows XP не поддерживает SNI (стандарт, позволяющий сделать HTTPS намного более масштабируемым).

Решение:

1) Для получения/обновления списков отзыва сертификатов (СОС) можно использовать **get_crl.bat,** который находится в `c:\Program Files (x86)\Avest\AvPCM_nces\` - ОС 64-разрядная или `c:\Program Files \Avest\AvPCM_nces\` - ОС 32-разрядная). Если выход в интернет осуществляется через прокси, настройки **get_crl.bat** описаны выше.
2) Скачать истекший СОС с сайта nces.by и проимпортировать через Персональный менеджер сертификатов Авест для ГосСУОК. Для этого
   - из папки Пуск – Все программы -Авест для НЦЭУ запустить Персональный менеджер сертификатов Авест для ГосСУОК с авторизацией или без авторизации,
   - в менеджере выбрать пункт меню Файл – Импорт сертификата/СОС (см. Рисунок *18* Импорт сертификата), указать путь к скачанному файлу СОС в формате *.crl и проимпортировать его, следуя указаниям.