

Инструкция по установке

Установка программного обеспечения для Национального центра
электронных услуг с помощью AvPKISetup

Оглавление

Аннотация.....	2
Системные требования.....	3
Установка комплекта абонента.....	3
Установка на компьютер, на котором уже присутствуют более ранние версии криптографического ПО ЗАО Авест	8
Удаление криптографического программного обеспечения с помощью объединенного инсталлятора.....	10
Приложение 1. Установка поддержки русского языка для программ, не поддерживающих Юникод	13
Приложение 2. Установка сертификатов	13
Приложение 3. Способы получения/обновления списков отзыва сертификатов СОС:	19

Аннотация

В настоящей инструкции описан порядок установки криптографического программного обеспечения с помощью объединенного инсталлятора AvPKISetup.

Системные требования

Комплекс AvPKISetup рассчитан на выполнение под управлением 32-х и 64-х битных операционных систем:

- **Windows Server 2003** с установленным Service Pack 2,
- **Windows Server 2008 R1,**
- **Windows Server 2008 R2,**
- **Windows Server 2012,**
- **Windows Server 2012 R2,**
- **Windows Server 2016,**
- **Windows Server 2019,**
- **Windows XP** с установленным Service Pack 3,
- **Windows 7,**
- **Windows 8,**
- **Windows 8.1,**
- **Windows 10.**

Требуется наличие **Microsoft Internet Explorer 6.0** или выше.

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

Необходимо **установить поддержку русского языка** для программ, не поддерживающих Юникод. См. **Приложение 1. Установка поддержки русского языка для программ, не поддерживающих Юникод**

Файлы, содержащие личный ключ подписи/шифрования, а также другие необходимые параметры, должны находиться на электронном устройстве **AvToken**, **AvPass** в защищенном виде.

ВНИМАНИЕ! 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.

Установка комплекта абонента

Программное обеспечение AvPKISetup передается пользователям на диске, флеш-носителе или иным способом (порядок определяется Удостоверяющим центром, выдающим ПО).

Каждое окно объединенного инсталлятора снабжено пояснительными надписями, которые следует внимательно читать.

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

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

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

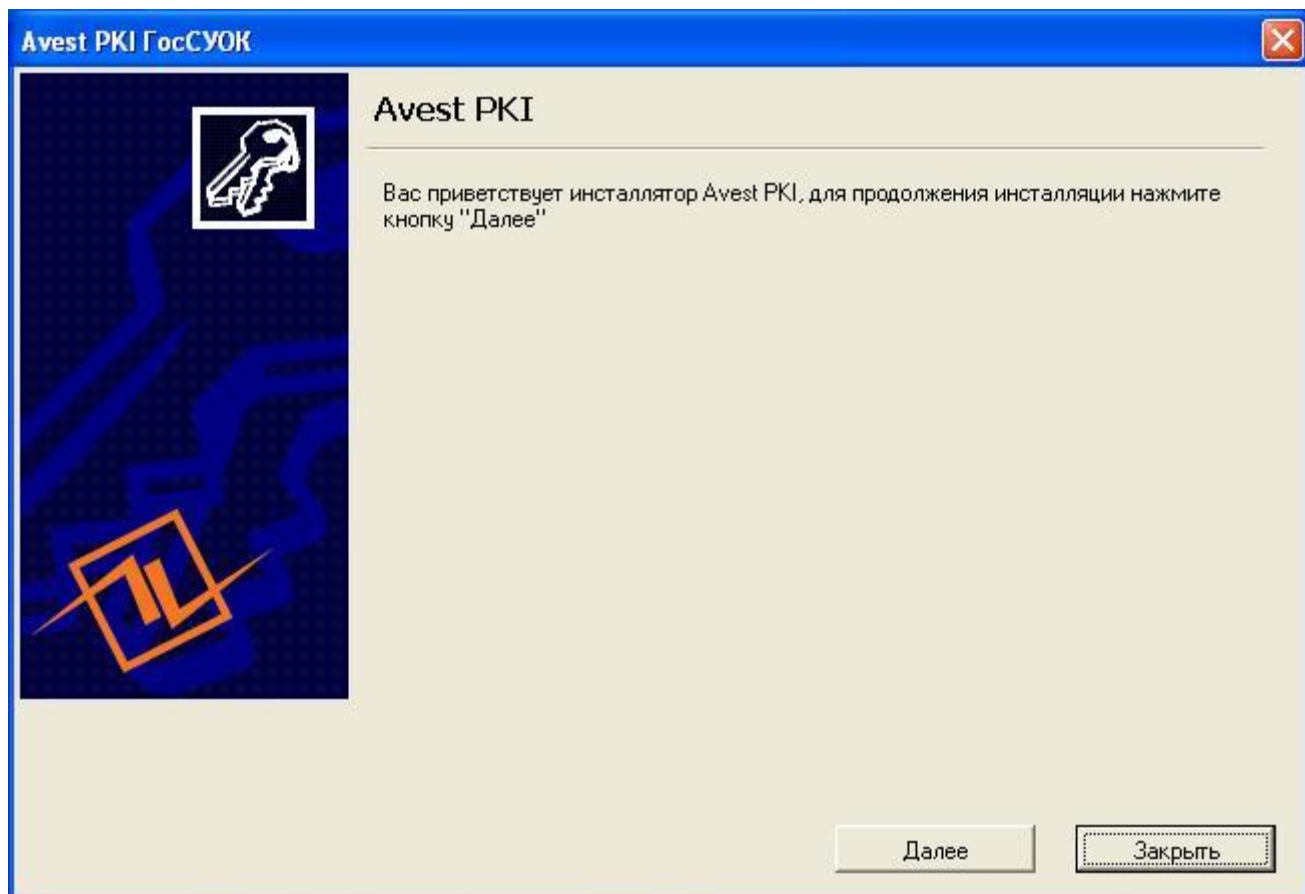


Рисунок 1 Окно мастера установки Avest PKI

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 Bing 6.3.0.800 (или выше), версия устанавливаемого менеджера сертификатов, а также версия драйвера для носителя AvBign (см. *Рисунок 2 Выбор компонентов*).

Для корректной работы криптопровайдера на операционных системах Windows XP и Windows Server 2003 будет установлено обновление **KB2836198**. Эта процедура обязательно требует перезагрузки компьютера (см. *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.

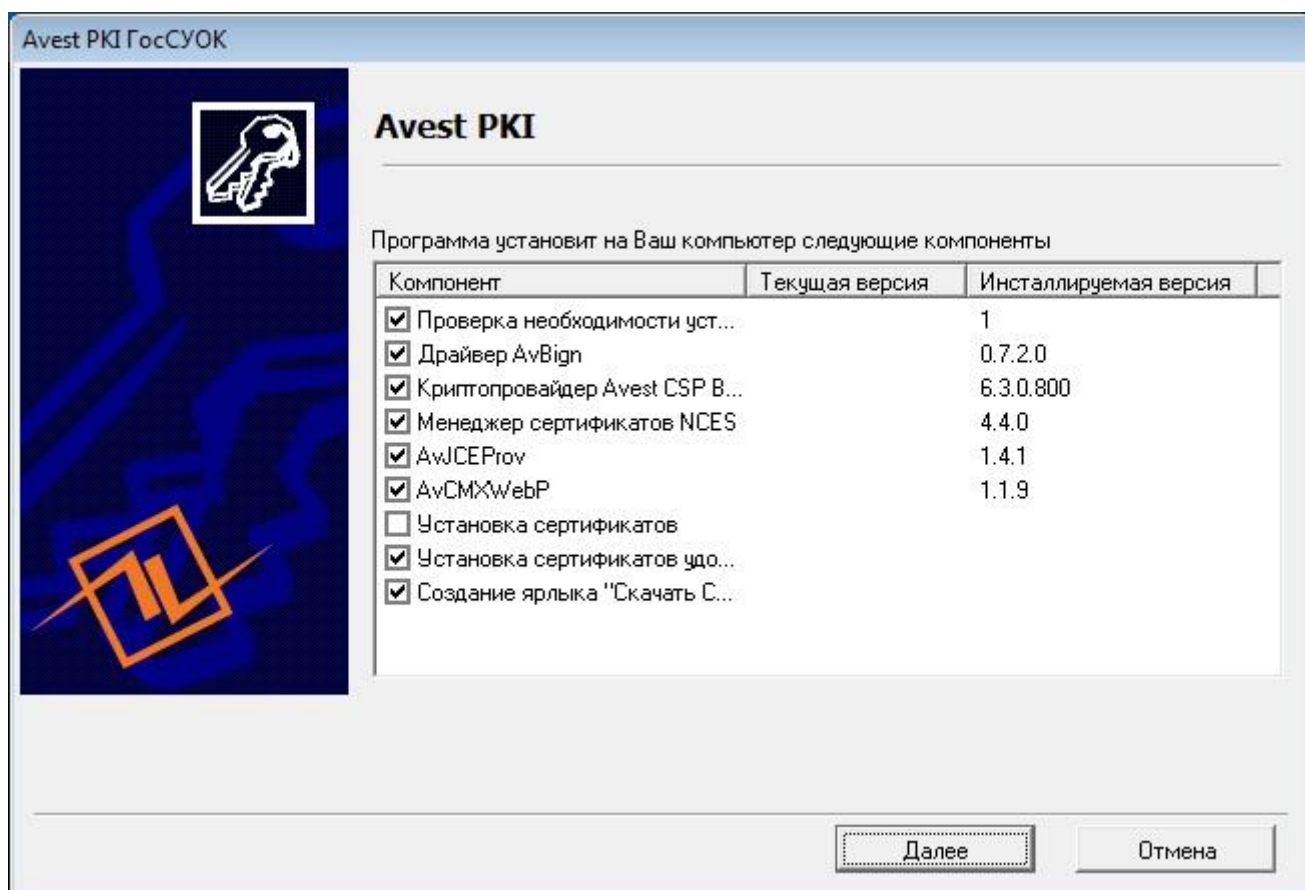


Рисунок 2 Выбор компонентов

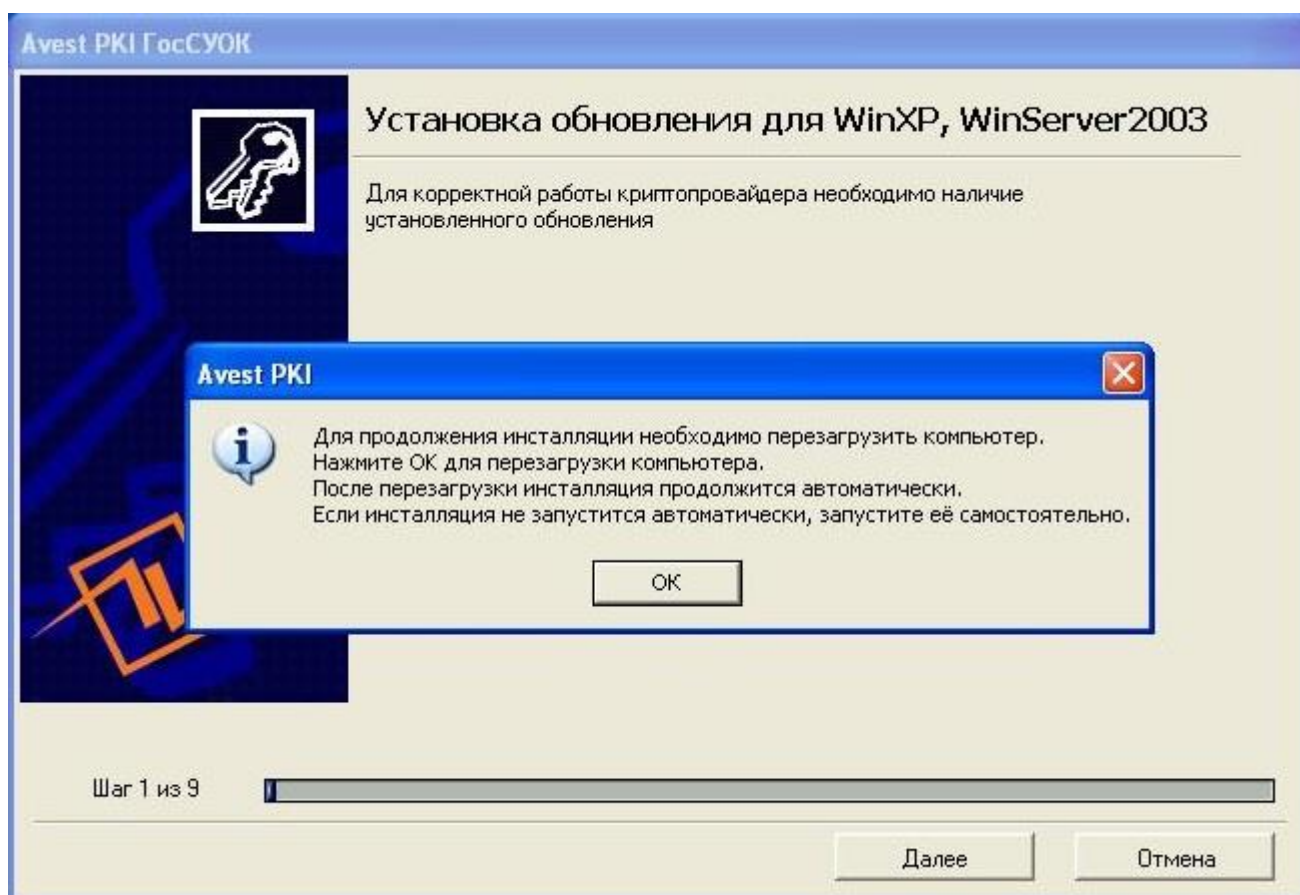


Рисунок 3 Предупреждение о перезагрузке

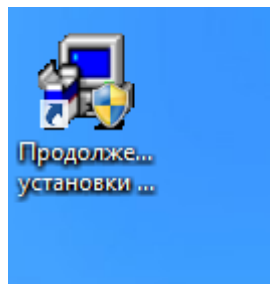


Рисунок 4 Ярлык "Продолжение установки AvPKISetup"

Далее будет установлен драйвер для носителя AvBign. 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 криптопровайдера Avest CSP Bign, персонального менеджера сертификатов AvPCM nces_Bign, веб плагина AvCMXWebP, импорт сертификата в Личный справочник и/или импорт атрибутного сертификата, установка доверия сертификатам Корневых удостоверяющих центров (См. Приложение 1. **Установка поддержки** русского языка для программ, не поддерживающих Юникод

Русифицировать ОС не требуется. Достаточно установить поддержку русского языка для программ, не поддерживающих Юникод.

Решение:

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.

Приложение 2. Установка сертификатов). Мастер установки произведет все действия автоматически.

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 «Закреть» (см.

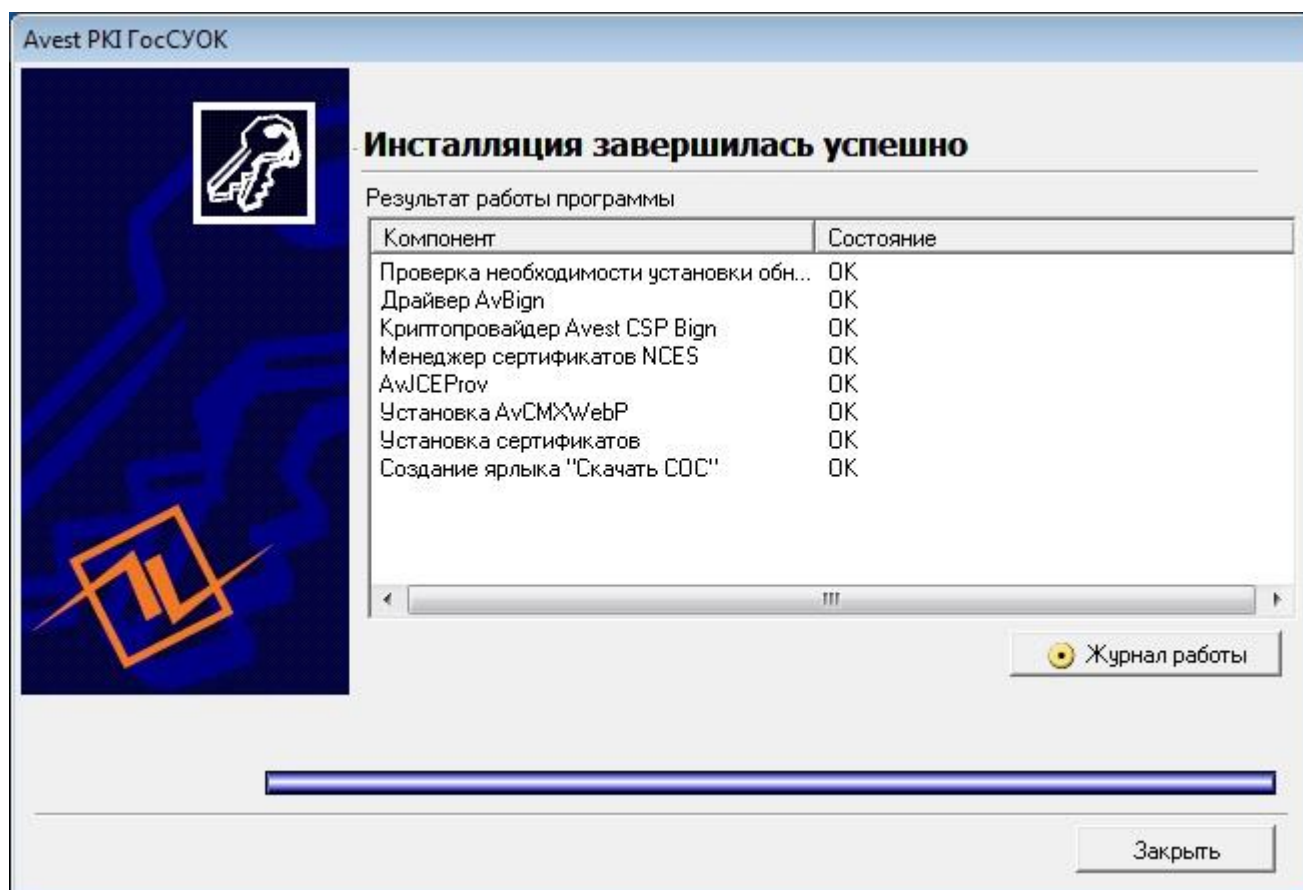


Рисунок 5 Завершение установки).

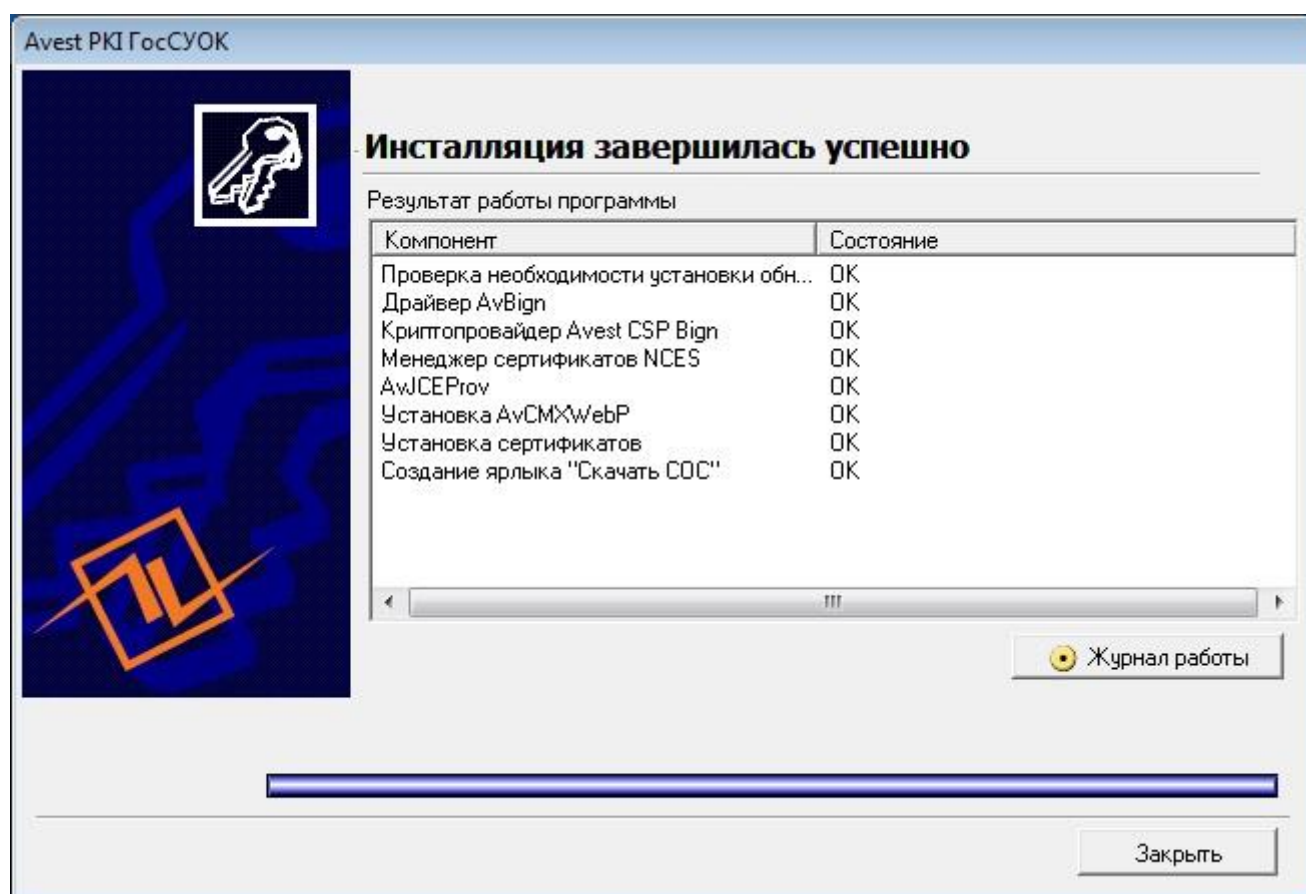


Рисунок 5 Завершение установки

Установка на компьютер, на котором уже присутствуют более ранние версии криптографического ПО ЗАО Авест

Вариантов и комбинаций предустановленного криптографического ПО может быть несколько, поэтому версии ПО, указанные в этом разделе, могут не совпадать с установленными на компьютере.

Обновление программного обеспечения с помощью объединенного инсталлятора AvPKISetup будет происходить аналогично установке без обновления, описанной выше с небольшими отличиями, о которых рассказано ниже:

В списке устанавливаемых компонентов будет указана версия текущего криптопровайдера, которая будет заменена на версию 6.3.0.791 (или выше), версия установленного менеджера сертификатов, которая будет заменена на 4.0.6 (или выше) (см. *Рисунок 6 Обновление компонентов*)

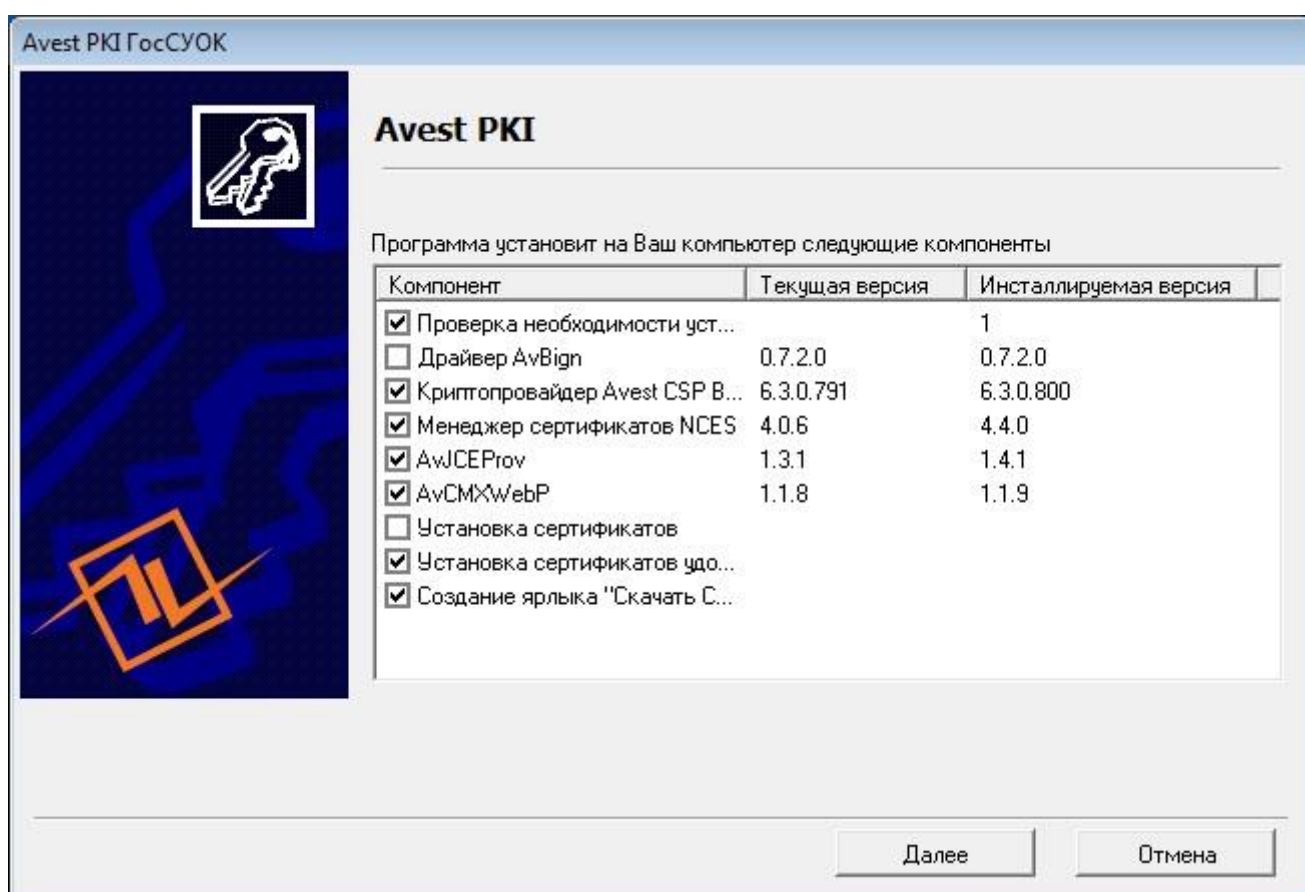


Рисунок 6 Обновление компонентов

После того, как кнопка «Далее» будет нажата, мастер установки AvPKISetup выдаст сообщение о том, что он удалит текущую версию криптопровайдера и

проинсталлирует новую версию. Эта процедура обязательно требует перезагрузки компьютера (см. *Рисунок 7 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 8 Ярлык «Продолжение установки AvPKISetup»*. Ярлык после успешной установки удалится с рабочего стола самостоятельно.

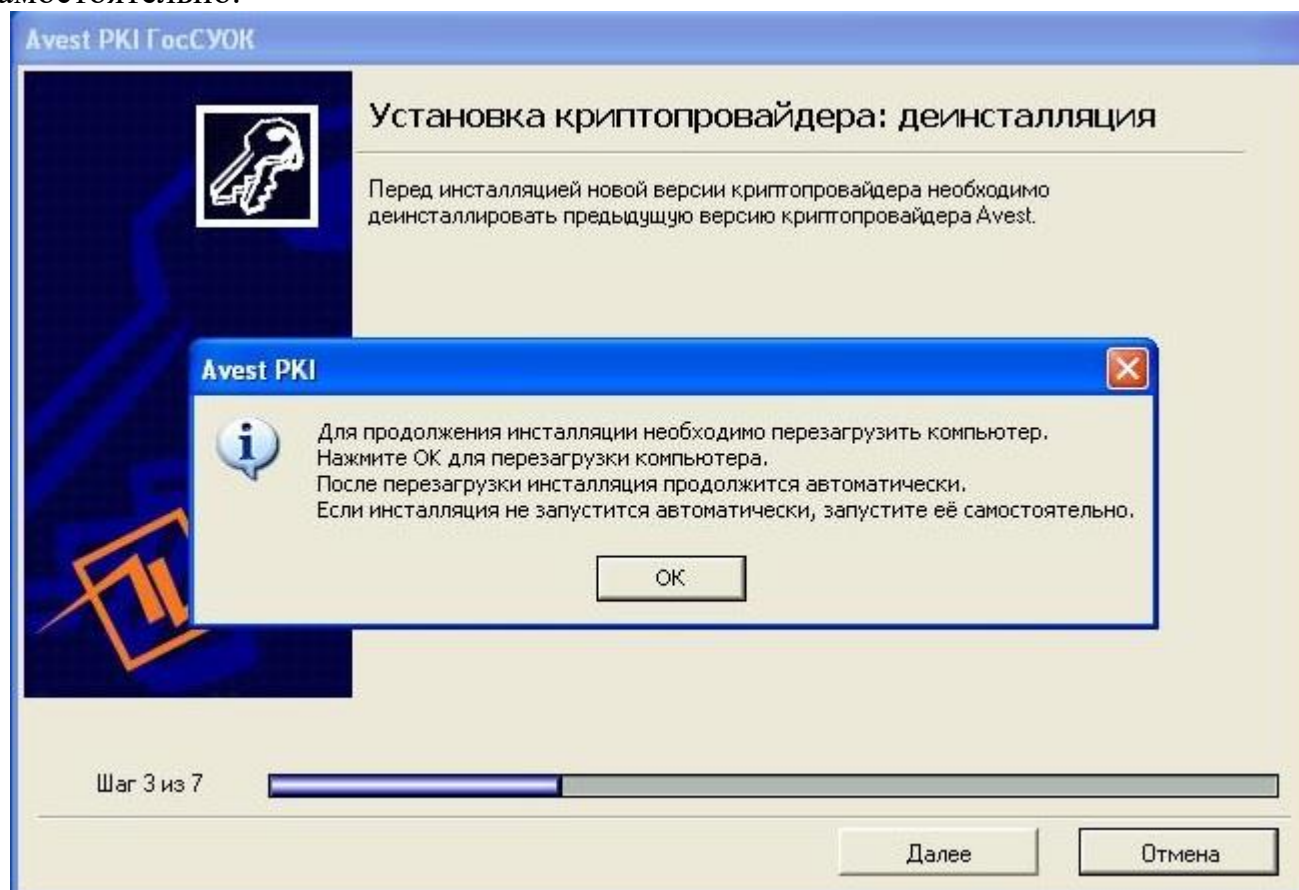


Рисунок 7 Предупреждение о перезагрузке.

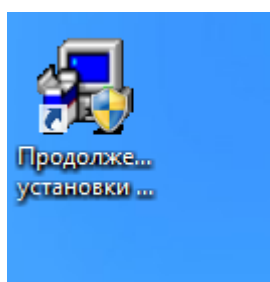


Рисунок 8 Ярлык «Продолжение установки AvPKISetup».

Далее установка проходит аналогичным способом, описанным выше в данном руководстве.

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 9 Выбор типа инсталляции*.Рисунок 9 Выбор типа инсталляции.)

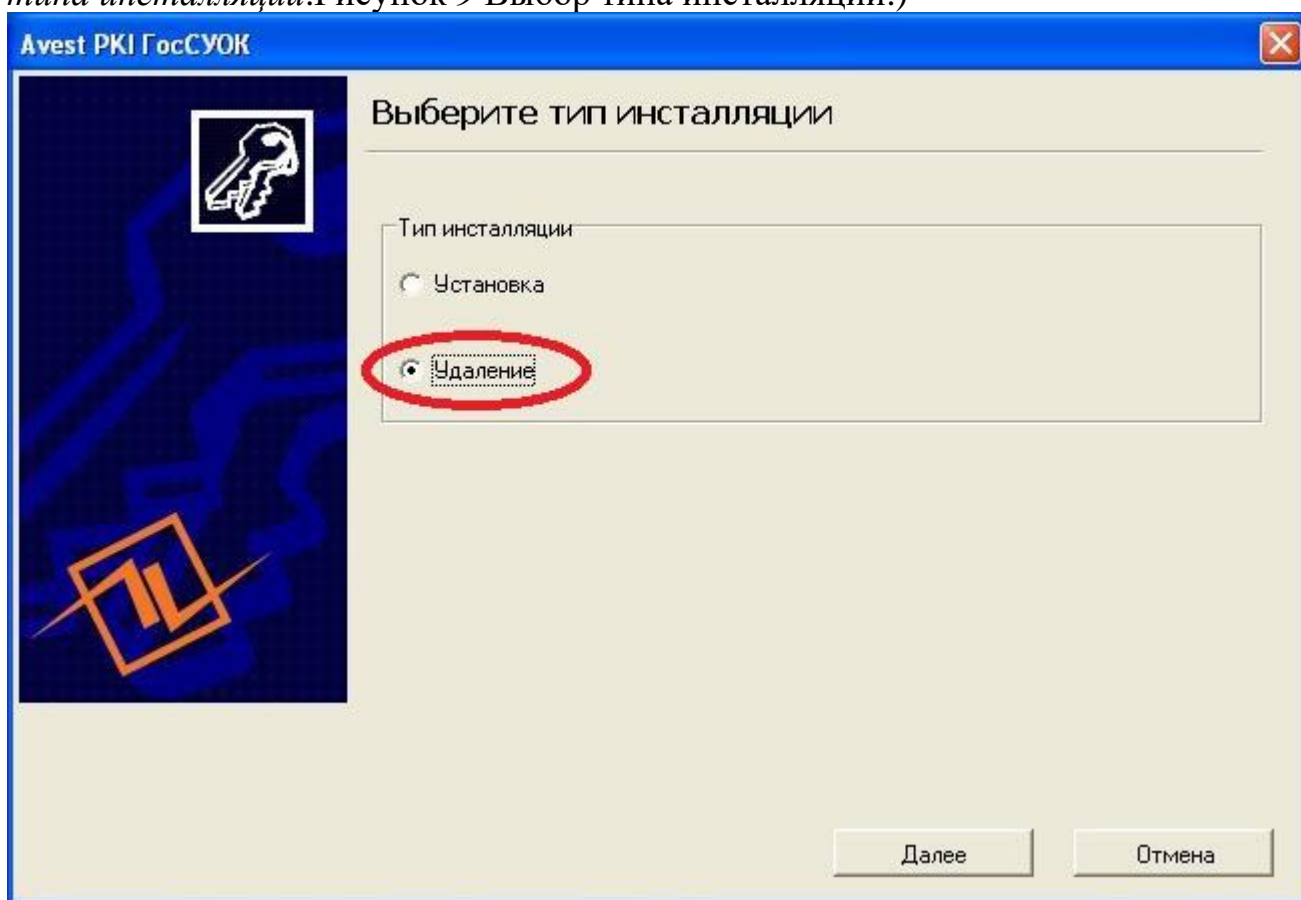


Рисунок 9 Выбор типа инсталляции.

В следующем окне программа выводит список удаляемых компонентов. Необходимо выбрать те компоненты, которые надо удалить, и нажать кнопку «Далее» (см. *Рисунок 10 Список удаляемых компонентов*.).

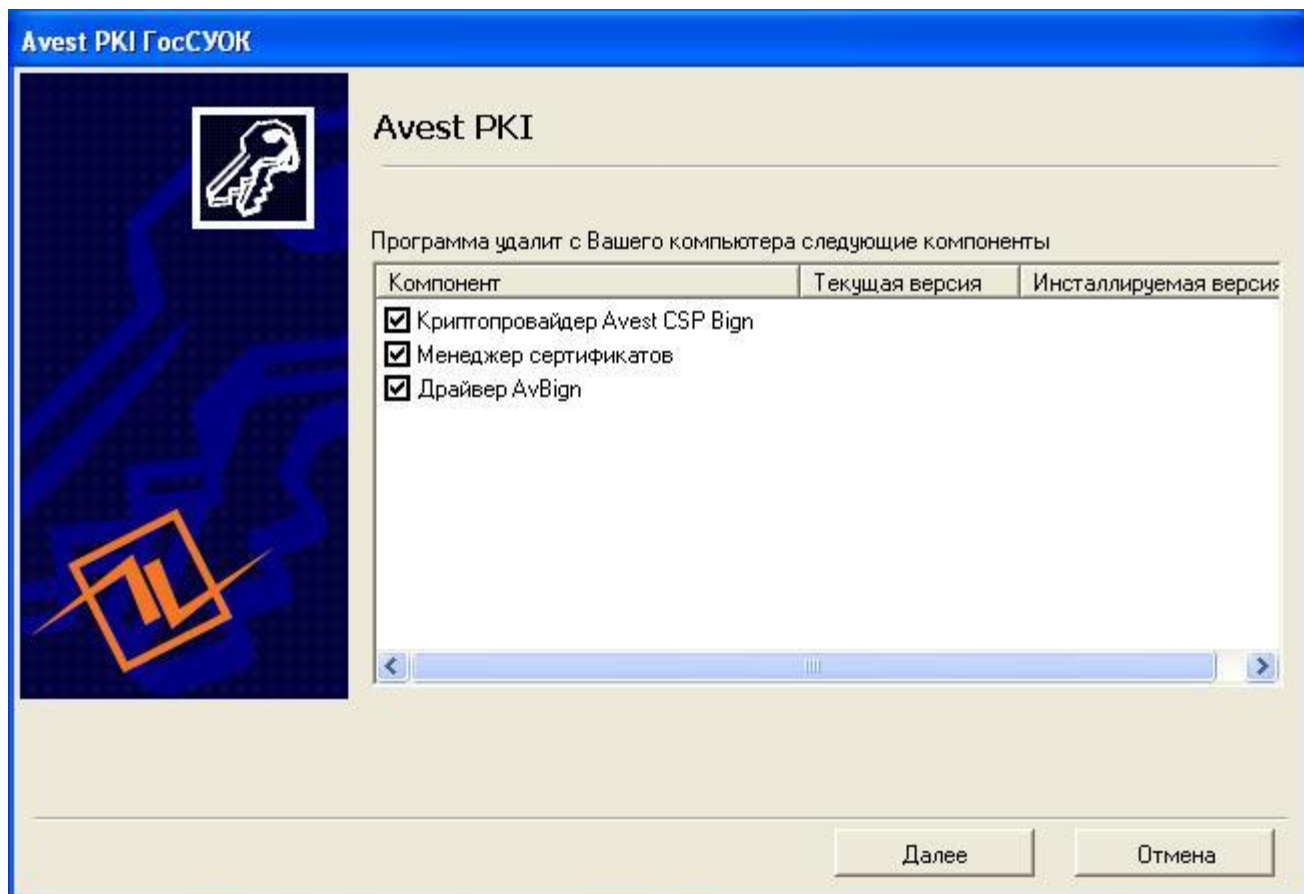


Рисунок 10 Список удаляемых компонентов.

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 11 Результат работы программы.*)

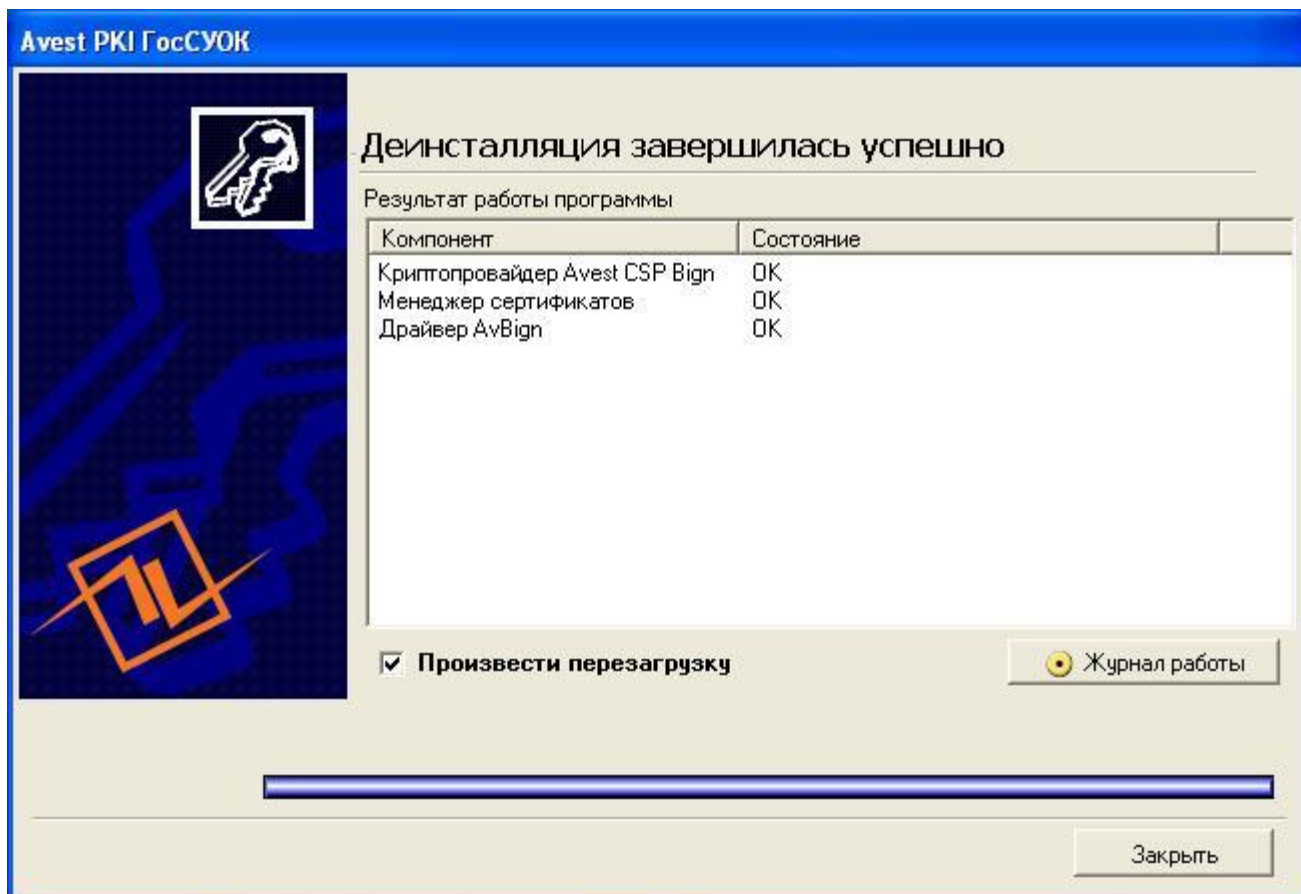


Рисунок 11 Результат работы программы.

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 12 Предупреждение о необходимости перезагрузки.*).

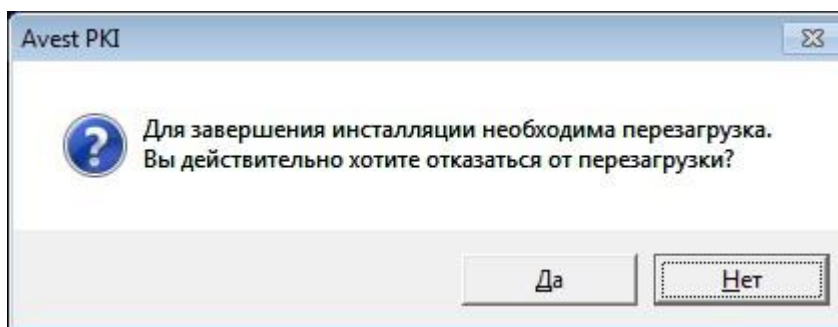


Рисунок 12 Предупреждение о необходимости перезагрузки.

Также можно более подробно просмотреть результат работы мастера установки AvPKISetup, нажав кнопку «Журнал работы» (см. *Рисунок 13 Журнал работы.*).

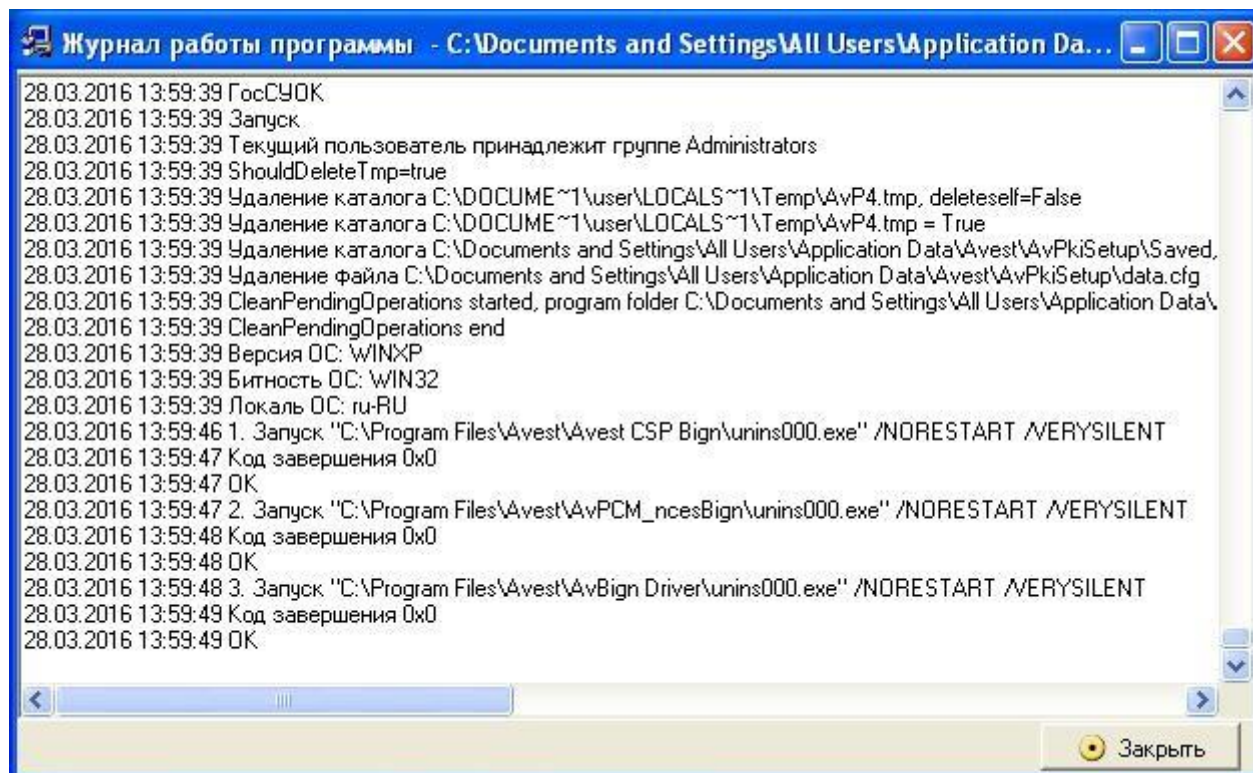


Рисунок 13 Журнал работы.

Приложение 1. Установка поддержки русского языка для программ, не поддерживающих Юникод

Русифицировать ОС не требуется. Достаточно установить поддержку русского языка для программ, не поддерживающих Юникод.

Решение:

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.

Приложение 2. Установка сертификатов

На шаге Установка сертификатов открывается окно Мастера импорта и происходит установка сертификатов в системные справочники Windows (см. Рисунок 14 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.

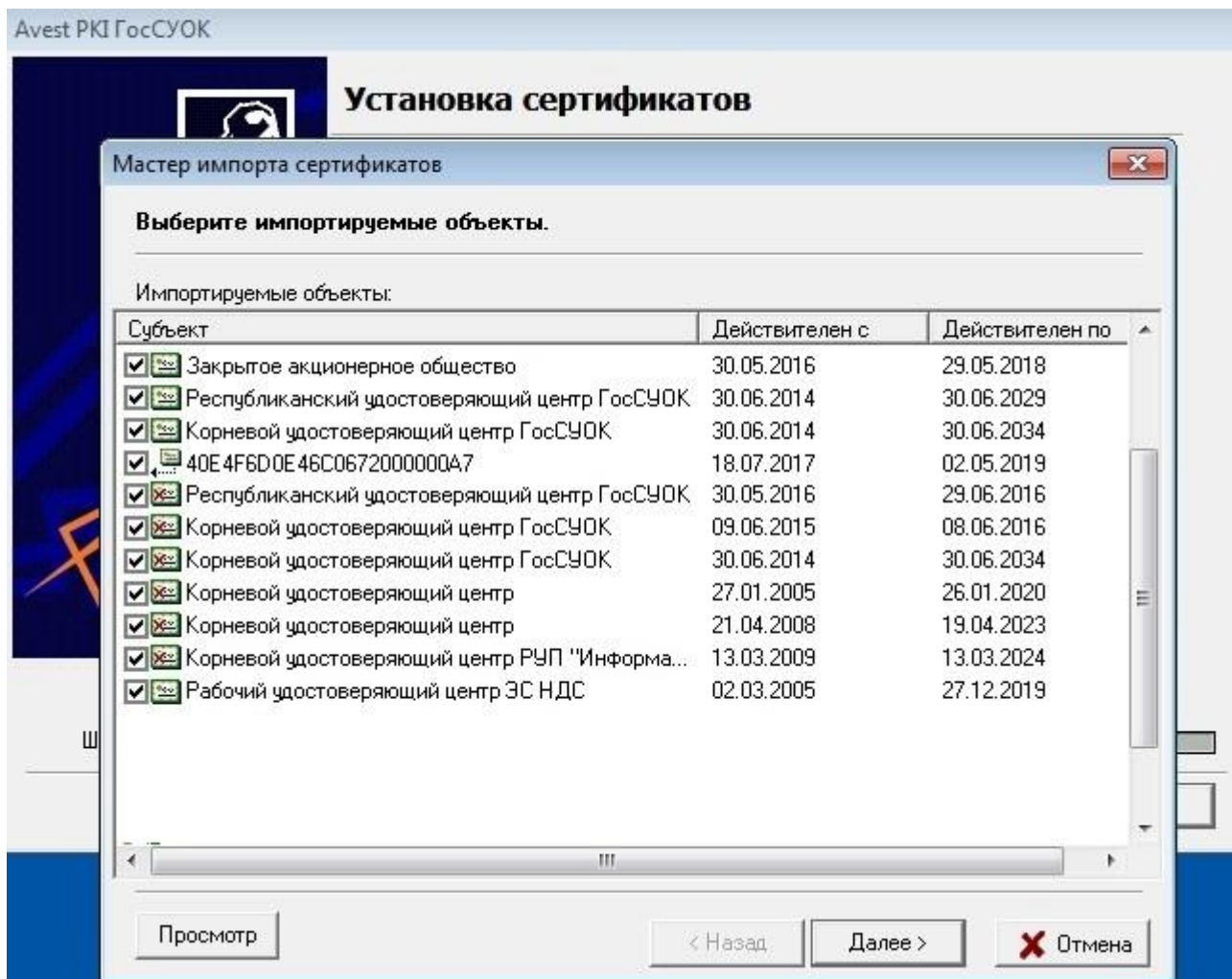


Рисунок 14 Импортируемые сертификаты

Мастер импорта уведомит о количестве импортированных сертификатов (см. *Рисунок 15 Уведомление о количестве импортируемых сертификатов*).

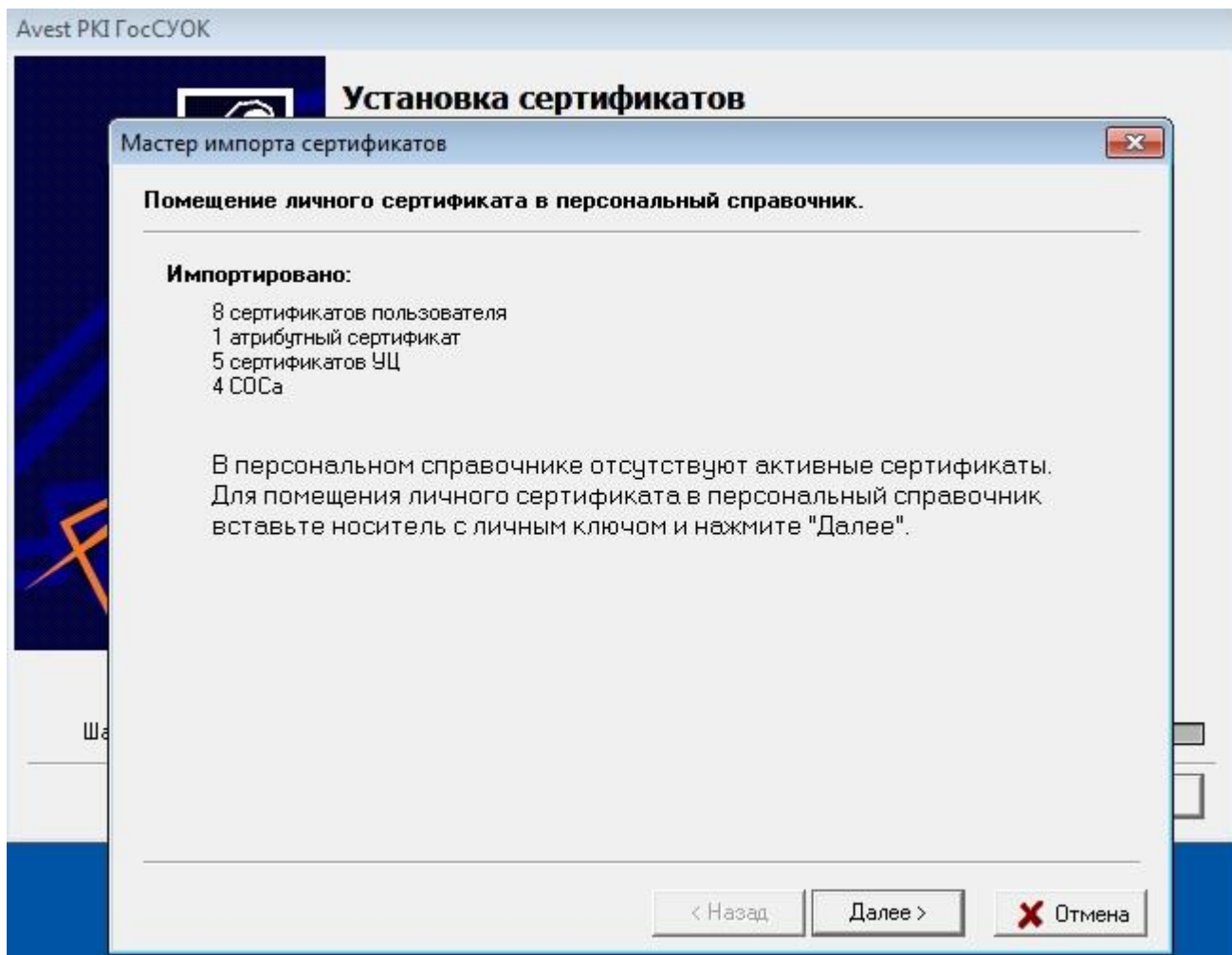


Рисунок 15 Уведомление о количестве импортируемых сертификатов

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 16 Выбор контейнера*).

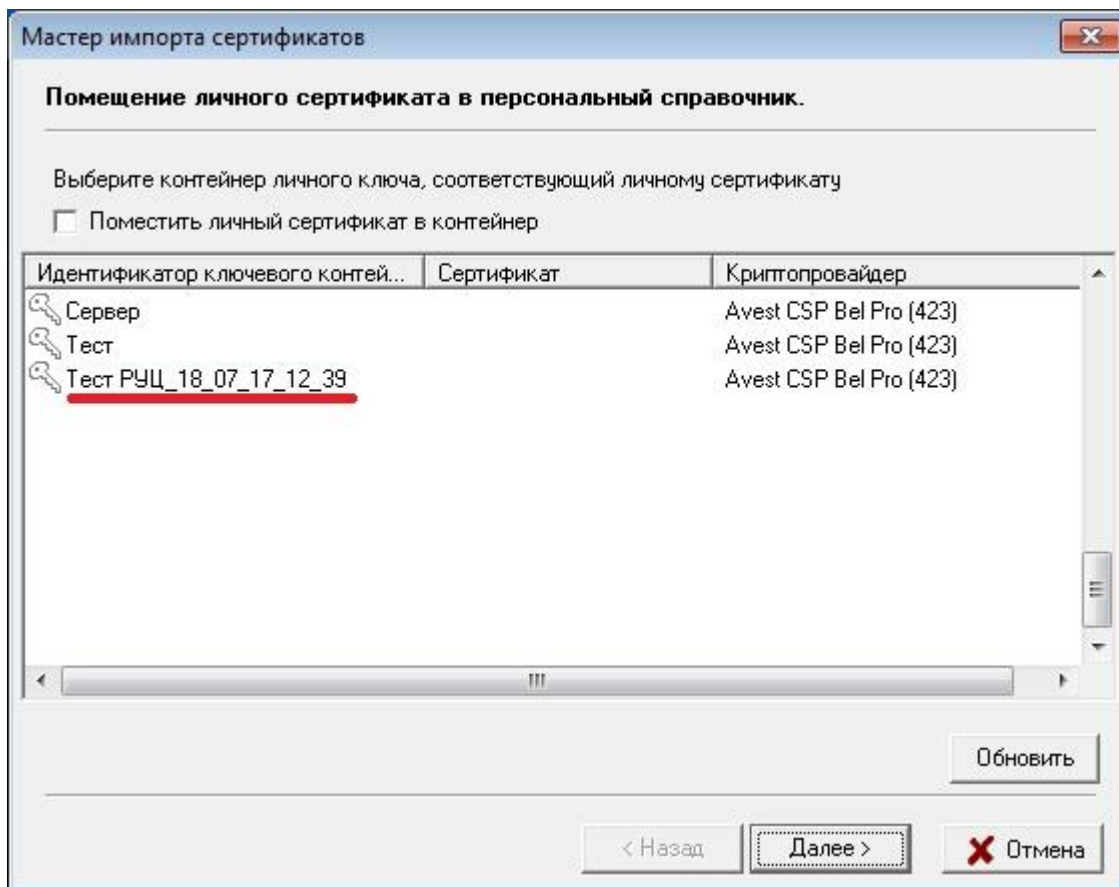


Рисунок 16 Выбор контейнера

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 17 Сертификаты корневых удостоверяющих центров*).

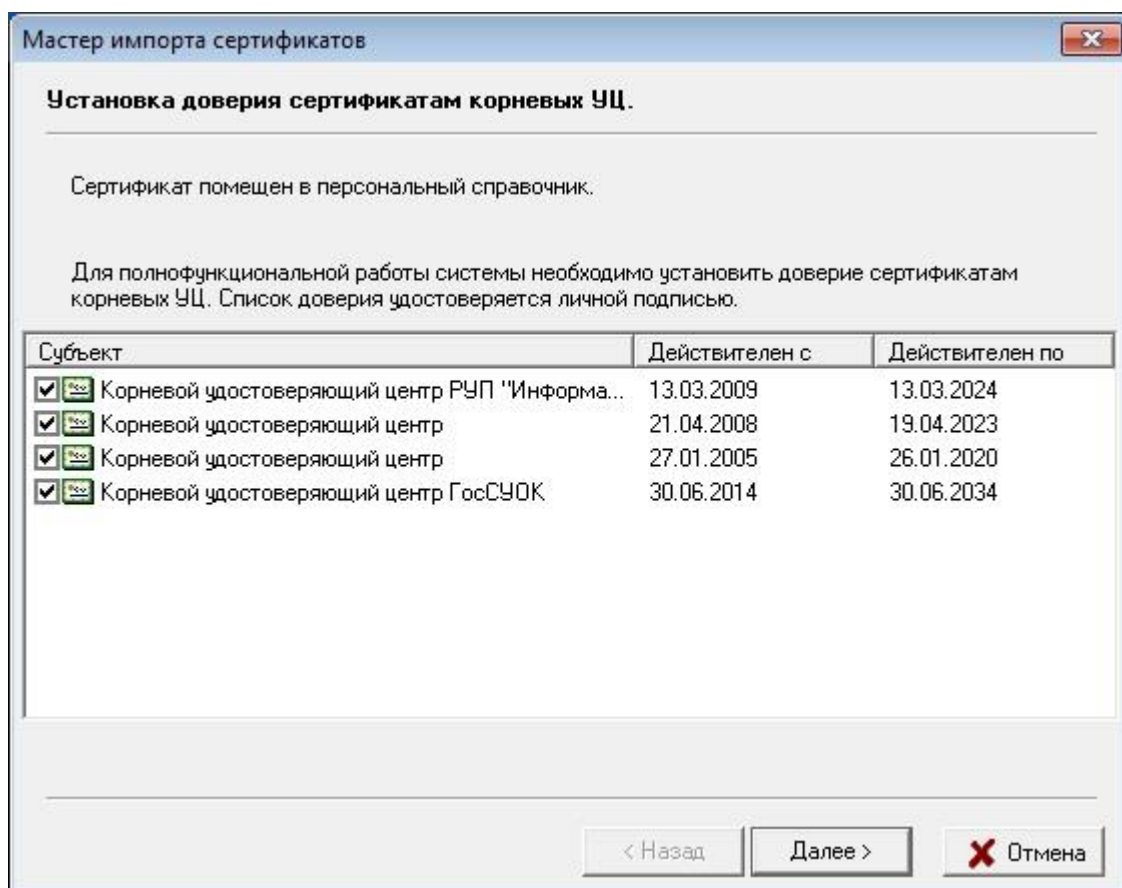


Рисунок 17 Сертификаты корневых удостоверяющих центров

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 18 Предупреждение системы безопасности*).

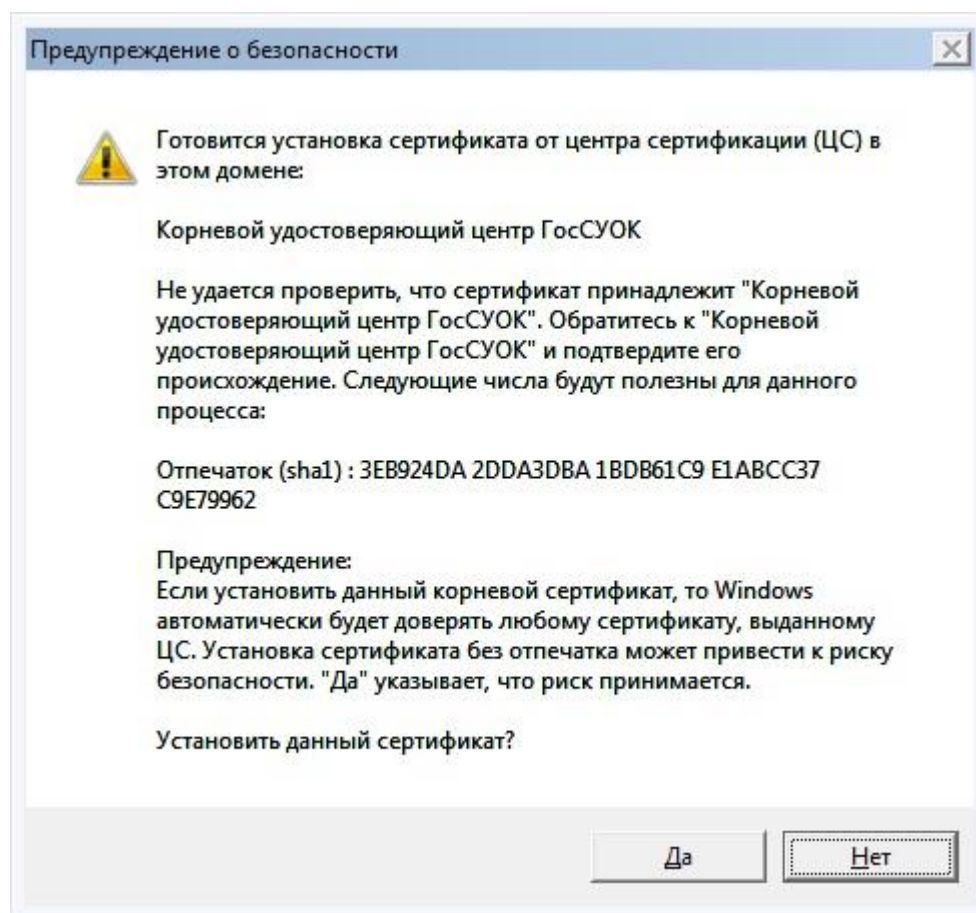


Рисунок 18 Предупреждение системы безопасности

На следующем шаге мастер импорта уведомит о сертификатах, которым было установлено доверие. Нажмите кнопку «Заккрыть». (См. *Рисунок 19 Завершение работы мастера импорта сертификатов*)

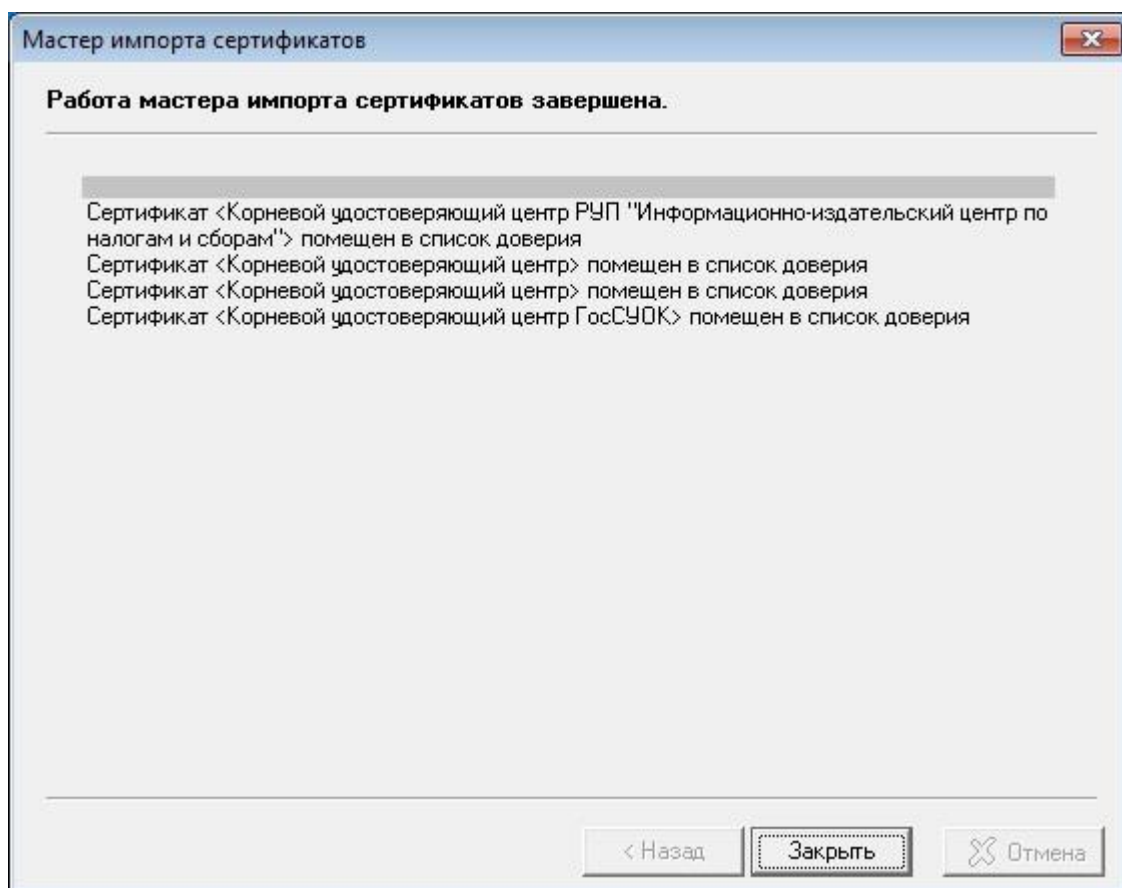


Рисунок 19 Завершение работы мастера импорта сертификатов

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

Для того, чтобы запустить обновление СОС, в персональном менеджере сертификатов нужно выбрать меню «Сервис» – «Контроль точек распределения СОС» или «Обновление СОС и сертификатов УЦ», если установлена версия менеджера 3.6.0 и выше. Интернет при этом должен быть включён.

Если у вас интернет через прокси или если требуется автоматизировать процесс получения СОС, можно воспользоваться заранее сконфигурированным файлом-«батником» **get_crl.bat**, который поставляется вместе с ПО на диске:

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.

*** Внимание!** Если выход в интернет осуществляется через прокси, необходимо:

1. в файле **get_crl.bat**

который находится в `c:\Program Files (x86)\Avest\AvPCM_ncesBign\` - ОС 64-разрядная или

c:\Program Files \Avest\AvPCM_ncesBign\ - ОС 32-разрядная)

раскомментировать строки (удалить слово «rem»):

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

и указать данные пользователя и адрес прокси.

2. Зайти по пути c:\Program Files (x86)\Avest\AvPCM_ncesBign или c:\Program Files \Avest\AvPCM_ncesBign\ и запустить файл **get_crl.bat**

(при использовании прокси предварительно надо внести необходимые данные, как описано выше).

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_ncesBign\ - ОС 64-разрядная или c:\Program Files \Avest\AvPCM_ncesBign\ - ОС 32-разрядная). Если выход в интернет осуществляется через прокси, настройки **get_crl.bat** описаны выше.
- 2) Скачать СОС с сайта nces.by и проимпортировать через Персональный менеджер сертификатов Авест для ГосСУОК (Bign). Для этого
 - из папки Пуск – Все программы -Авест для НЦЭУ (Bign) запустить Персональный менеджер сертификатов Авест для ГосСУОК с авторизацией или без авторизации,
 - в менеджере выбрать пункт меню Файл – Импорт сертификата/СОС и

проимпортировать списки отзыва сертификатов.

