

Инструкция по установке и обновлению
криптографического программного обеспечения для
абонентов РУП «Национальный центр электронных услуг»
с импортом сертификата, выдаваемым Республиканским
удостоверяющим центром ГосСУОК, с помощью
объединённого инсталлятора AvPKISetup

Листов 39

Аннотация

В настоящей инструкции описан порядок установки и обновления криптографического программного обеспечения «Программный комплекс «Комплект Абонента АВЕСТ» AvUSK» с установкой сертификата, выдаваемого Республиканским удостоверяющим центром ГосСУОК, с помощью объединенного инсталлятора AvPKISetup. Данный комплект предназначен для абонентов РУП «Национальный центр электронных услуг» (далее РУП «НЦЭУ») и распространяется в рамках оказания услуг РУП «НЦЭУ».

СОДЕРЖАНИЕ

| | |
|--|----|
| 1. Системные требования | 4 |
| 2. Установка программного обеспечения с помощью объединенного инсталлятора AvPKISetup на компьютер, где ранее не было установлено ПО АВЕСТ | 7 |
| 3. Обновление программного обеспечения с помощью объединенного инсталлятора AvPKISetup | 12 |
| 4. Удаление криптографического программного обеспечения с помощью объединенного инсталлятора | 17 |
| Приложение 1. Установка сертификатов с помощью объединенного инсталлятора AvPKISetup..... | 20 |
| Приложение 2. Способы получения/обновления списков отозванных сертификатов | 24 |
| Приложение 3. Импорт личного сертификата в персональный менеджер сертификатов Авест | 27 |
| Приложение 4. Импорт атрибутивного сертификата в формате *.асг в персональный менеджер сертификатов Авест | 35 |
| 5. Перечень сокращений | 39 |

1. Системные требования

1) Работа инсталлятора AvPKISetup рассчитана на выполнение под управлением одной из следующих ОС:

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

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

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

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

2) Пользователь для установки и запуска программного обеспечения должен иметь права в операционной системе Windows не ниже «PowerUser».

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

В ОС Windows XP, Windows 2003 Server:

1. Перейти в меню «Start» - «Control Panel» («Пуск» - «Панель управления»), в зависимости от параметров просмотра элементов в панели управления (классический вид или по категориям) выбрать «Regional and Language Options» («Язык и региональные стандарты») или «Date, Time, Language and Regional Options» - «Regional and Language Options» («Дата, время, язык и региональные стандарты» - «Язык и региональные стандарты»).

2. На вкладке «Regional options» («Региональные параметры») в поле «Standards and formats» («Языковые стандарты и форматы») выбрать русский язык, в поле «Location» («Расположение») указать Беларусь, на вкладке «Advanced» («Дополнительно») в поле «Language for non-Unicode programs» («Язык для программ, не поддерживающих Юникод») выбрать русский язык.

3. Выполнить перезагрузку.

4. Проверить отображение кодировки.

В ОС Windows 7, Windows 2008 Server:

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

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

3. Выполнить перезагрузку.

4. Проверить отображение кодировки.

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

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

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

3. Выполнить перезагрузку.

4. Проверить отображение кодировки.

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

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

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

3. Выполнить перезагрузку.

4. Проверить отображение кодировки.

4) AvPKISetup предназначен для запуска и выполнения на компьютере (сервере), имеющем следующие минимальные технические характеристики:

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

5) Файлы, содержащие личный ключ подписи/шифрования, должны находиться на электронном устройстве AvBign 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.

2. Установка программного обеспечения с помощью объединенного инсталлятора AvPKISetup на компьютер, где ранее не было установлено ПО АВЕСТ

Комплект абонента AvУСК совместно с сертификатом, сконфигурированный для установки и обновления с помощью объединенного инсталлятора AvPKISetup, передается пользователям способом, который определяется удостоверяющим центром, выдающим сертификат.

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.*

*Внимание!!! Объединенный инсталлятор AvPKISetup сможет проимпортировать сертификаты только в формате *.p7b. Сертификаты, сохраненные в других форматах, например, атрибутный сертификат в формате *.acr, импортируется в персональный менеджер сертификатов вручную (см. Приложение 4. Импорт атрибутного сертификата в формате *.acr в персональный менеджер сертификатов Авест).*

Перед установкой необходимо извлечь комплект абонента из архива AvPKISetup(big).zip.

Для начала установки ПО нужно 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).

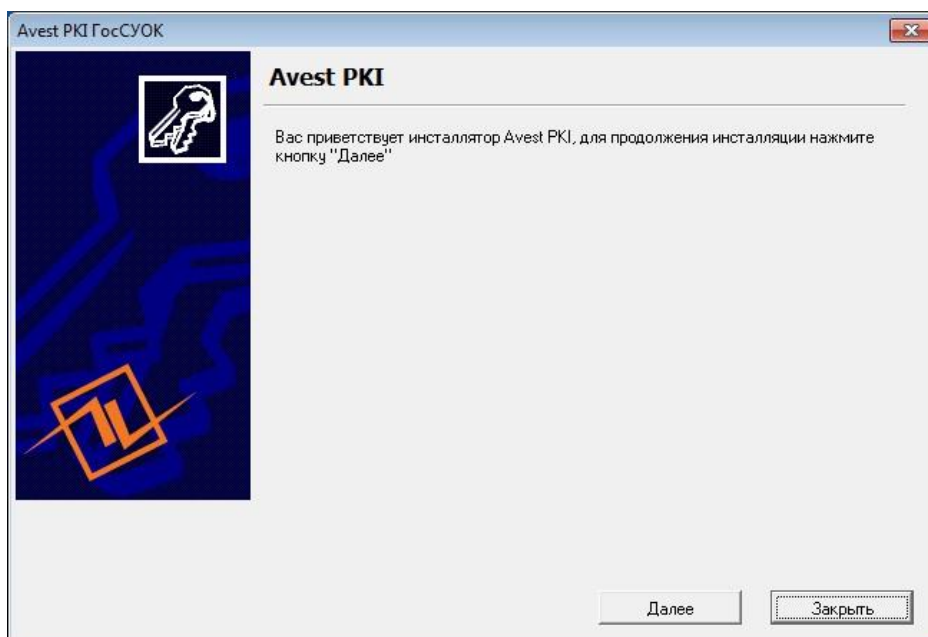


Рисунок 1. Окно мастера установки Avest PKI

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

В появившемся окне представлен список устанавливаемых на компьютер компонентов, отмеченных флажками. В колонке «Инсталлируемая версия» отображается версия устанавливаемого продукта. В списке устанавливаемых компонентов будет указана версия устанавливаемого криптопровайдера Avest CSP Bign, версия устанавливаемого персонального менеджера сертификатов, версия программного комплекса AvJCEProv, версия плагина AvCMXWebP, а также версия драйвера для носителя AvBign (см. Рисунок 2. Выбор компонентов).

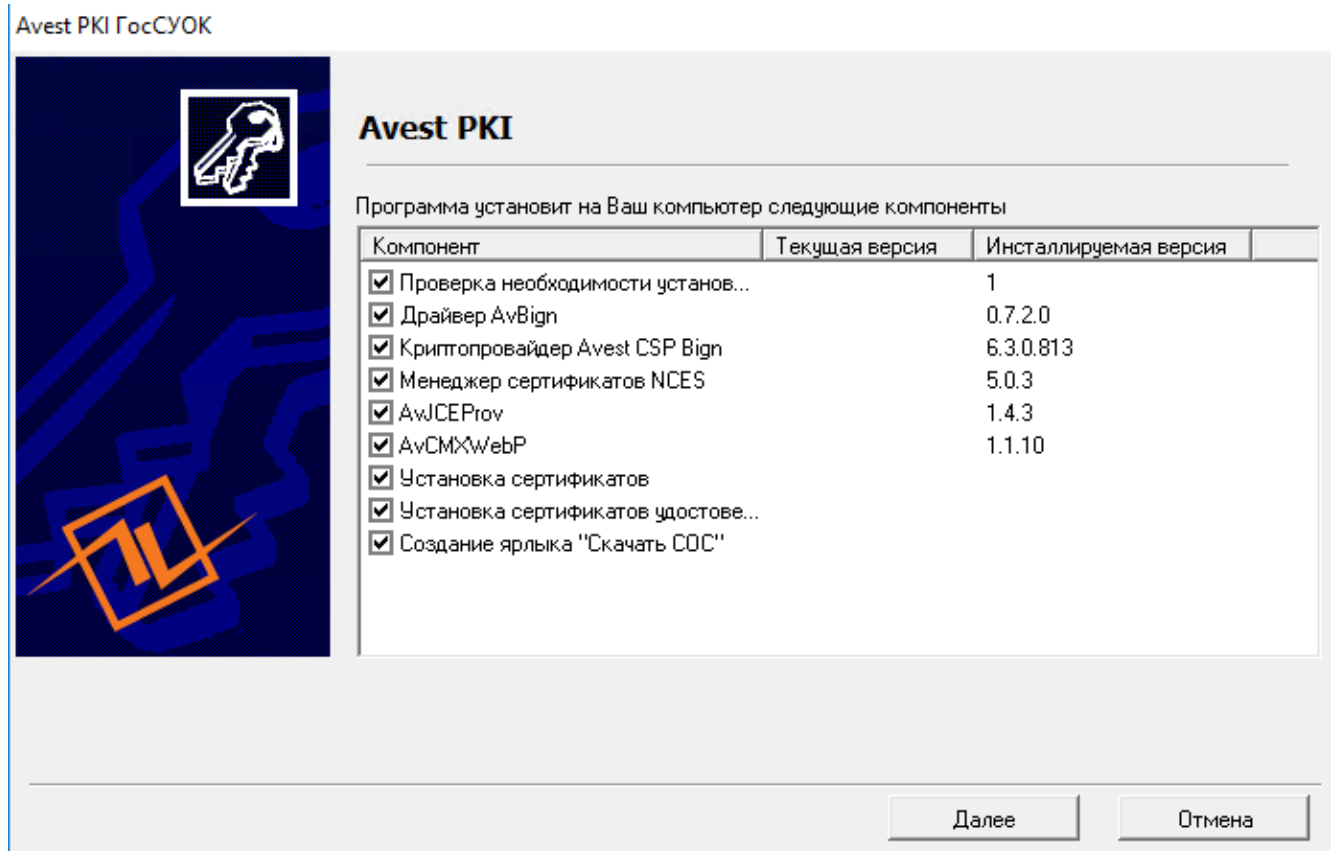


Рисунок 2. Выбор компонентов

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 (см. Рисунок 3 Предупреждение о перезагрузке).

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

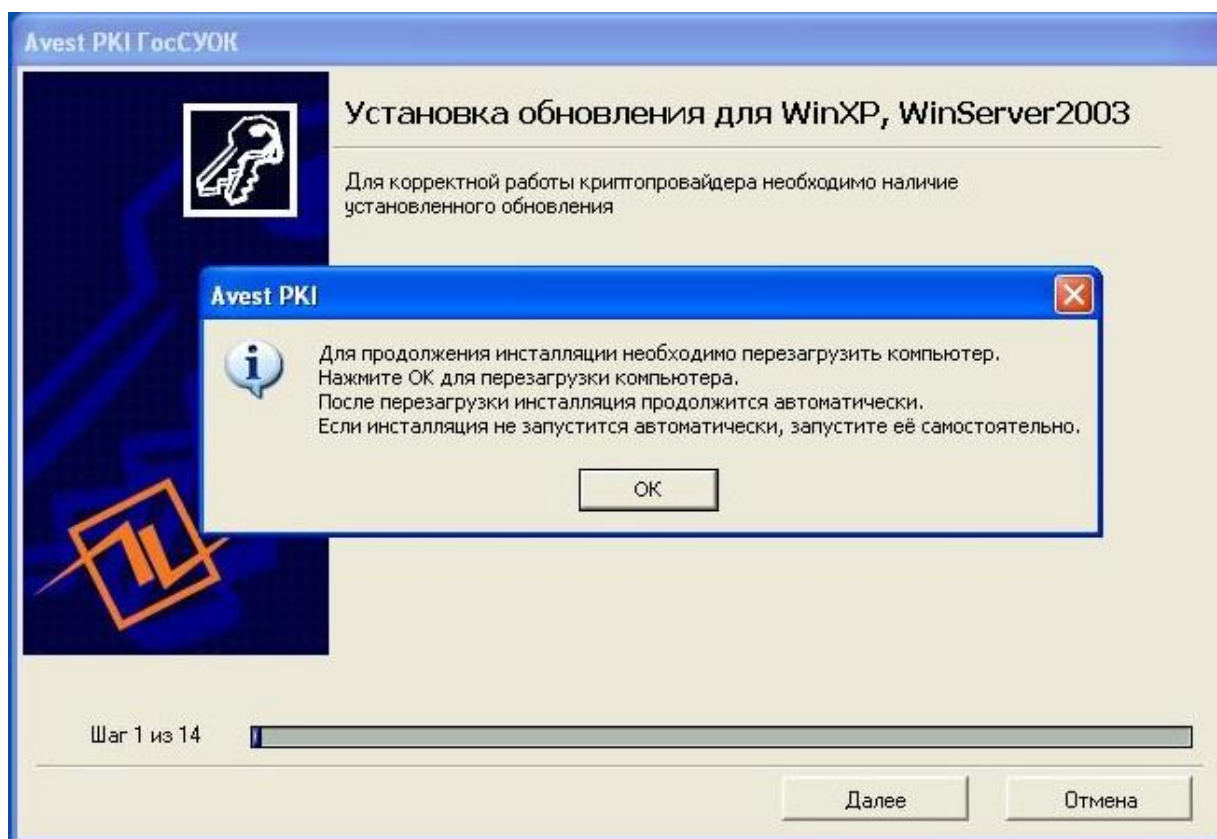


Рисунок 3 Предупреждение о перезагрузке

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).

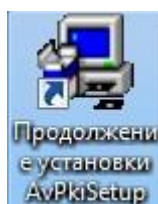


Рисунок 4 Ярлык «Продолжение установки AvPKISetup»

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,,
- веб плагина AvCMXWebP,
- программного комплекса AvJCEProv,
- персонального менеджера сертификатов AvPCM_ncesBign,
- импорт сертификата в личный справочник и импорт атрибутивного сертификата, *если соответствующие сертификаты были помещены в папку*

data в формате *.p7b (см. Приложение 1. Установка сертификатов с помощью объединенного инсталлятора AvPKISetup),

- установка сертификатов удостоверяющих центров.

На шаге «Установка сертификатов удостоверяющих центров» будет выведено предупреждение операционной системы Windows о добавлении сертификатов корневых удостоверяющих центров в корневое хранилище, в этих сообщениях указаны атрибуты помещаемых сертификатов. Если они соответствуют данным сертификатов ваших корневых УЦ, то нужно нажать «Да» в двух уведомлениях (см. Рисунок 5 Предупреждение системы безопасности).

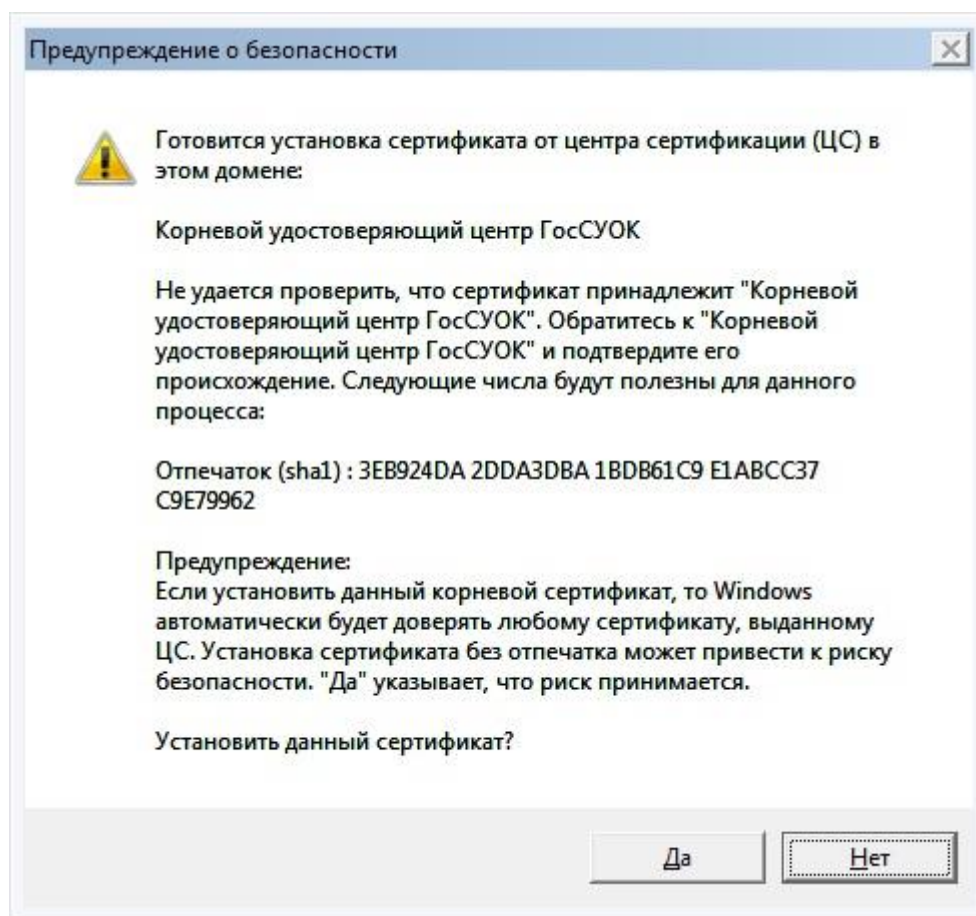
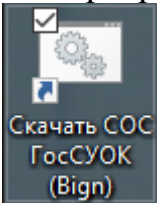


Рисунок 5 Предупреждение системы безопасности

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

ярлык «Скачать СОС ГосСУОК (Bign)» .

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 6. Завершение установки).

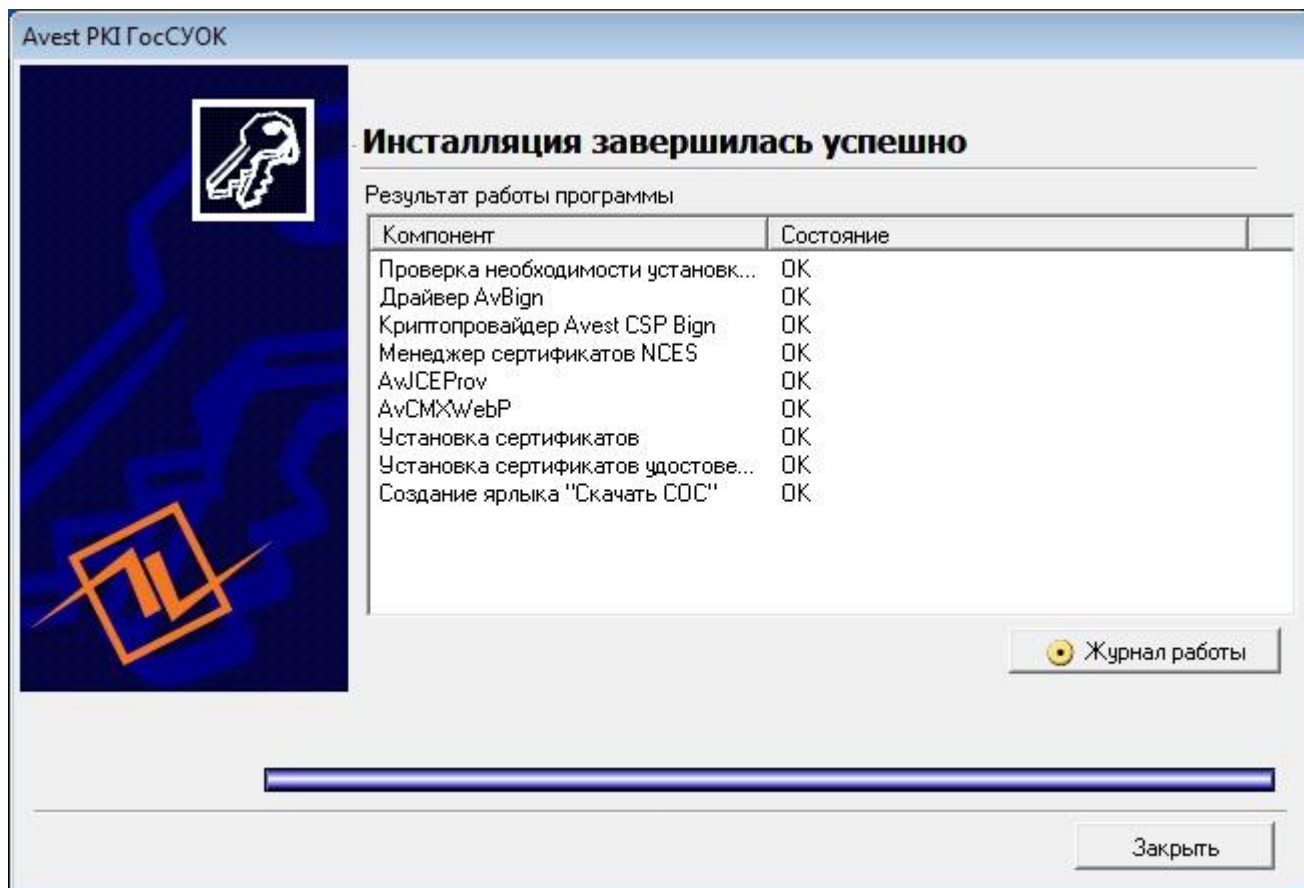


Рисунок 6. Завершение установки

Установка комплекта абонента завершена.

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 portal2.ssf.gov.by;
- и в прочих государственных сервисах. Уточняйте, пожалуйста, есть ли такая возможность, у владельца сервиса.

3. Обновление программного обеспечения с помощью объединенного инсталлятора AvPKISetup

Комплект абонента AvUСK совместно с сертификатом, сконфигурированный для установки и обновления с помощью объединенного инсталлятора AvPKISetup, передается пользователям способом, который определяется удостоверяющим центром, выдающим сертификат.

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

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.*

*Внимание!!! Объединенный инсталлятор AvPKISetup сможет проимпортировать сертификаты только в формате *.p7b. Сертификаты, сохраненные в других форматах, например, атрибутный сертификат в формате *.acg, импортируется в персональный менеджер сертификатов вручную (см. Приложение 4. Импорт атрибутного сертификата в формате *.acg в персональный менеджер сертификатов Авест).*

Для начала обновления ПО необходимо запустить файл AvPKISetup2.exe.

В окне мастера установки следует нажать кнопку «Далее», чтобы начать установку ПО на компьютер (см. Рисунок 7. Окно мастера установки Avest PKI).

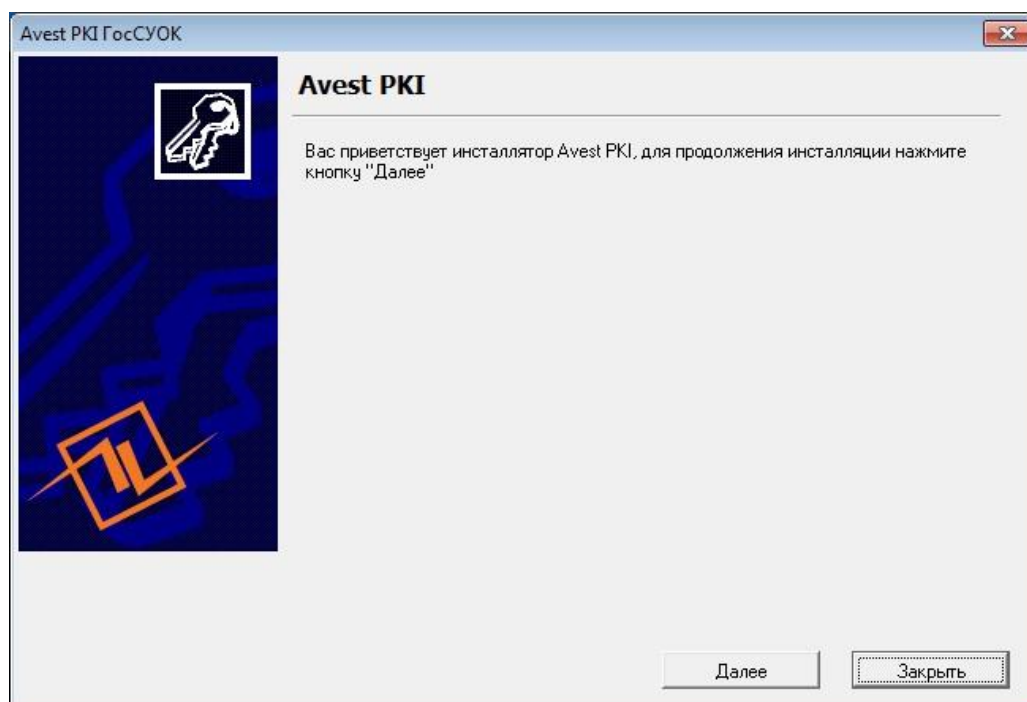


Рисунок 7. Окно мастера установки Avest PKI

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

В появившемся окне представлен список устанавливаемых на компьютер компонентов, отмеченных флажками. В колонке «Инсталлируемая версия» отображается версия устанавливаемого продукта. В колонке «Текущая версия» будут указаны:

- версия текущего криптопровайдера Avest CSP Bign, которая будет заменена на версию 6.3.0.813 (или выше),
- версия установленного менеджера сертификатов, которая будет заменена на 5.0.3 (или выше),
- версия программного комплекса AvJCEProv, которая будет заменена на версию 1.4.3 (или выше),
- версия программного средства «Веб плагин AvCMXWebP», которая будет заменена на версию 1.1.10 (или выше),
- версия драйвера для носителя AvBign, которая будет заменена на версию 0.7.2.0 (или выше).

Если будет производиться импорт сертификата, компонент «Установка сертификата» также будет отмечен флажком. Также будут установлены сертификаты удостоверяющих центров (см. Рисунок 8. Обновление компонентов).

Avest PKI ГосСУОК

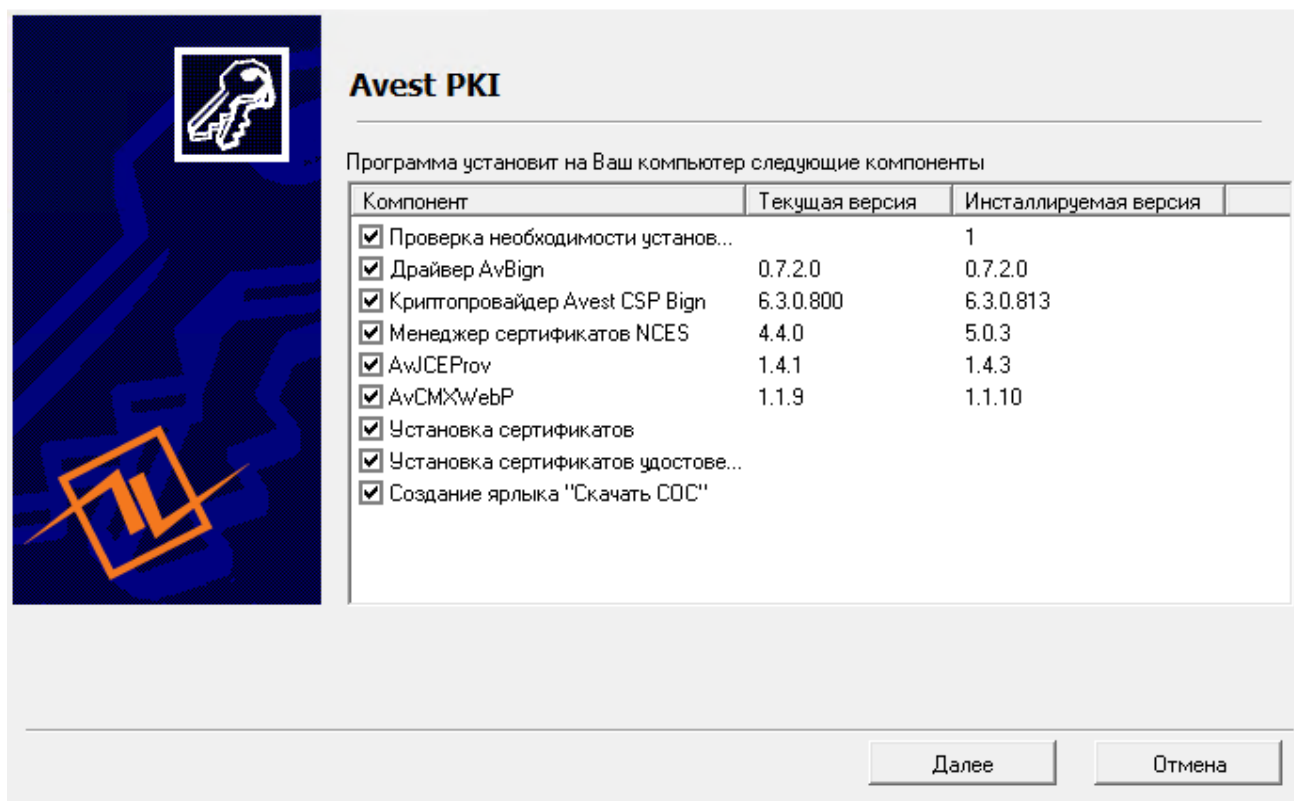


Рисунок 8. Обновление компонентов

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

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 (см. Рисунок 9 Предупреждение о перезагрузке).

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

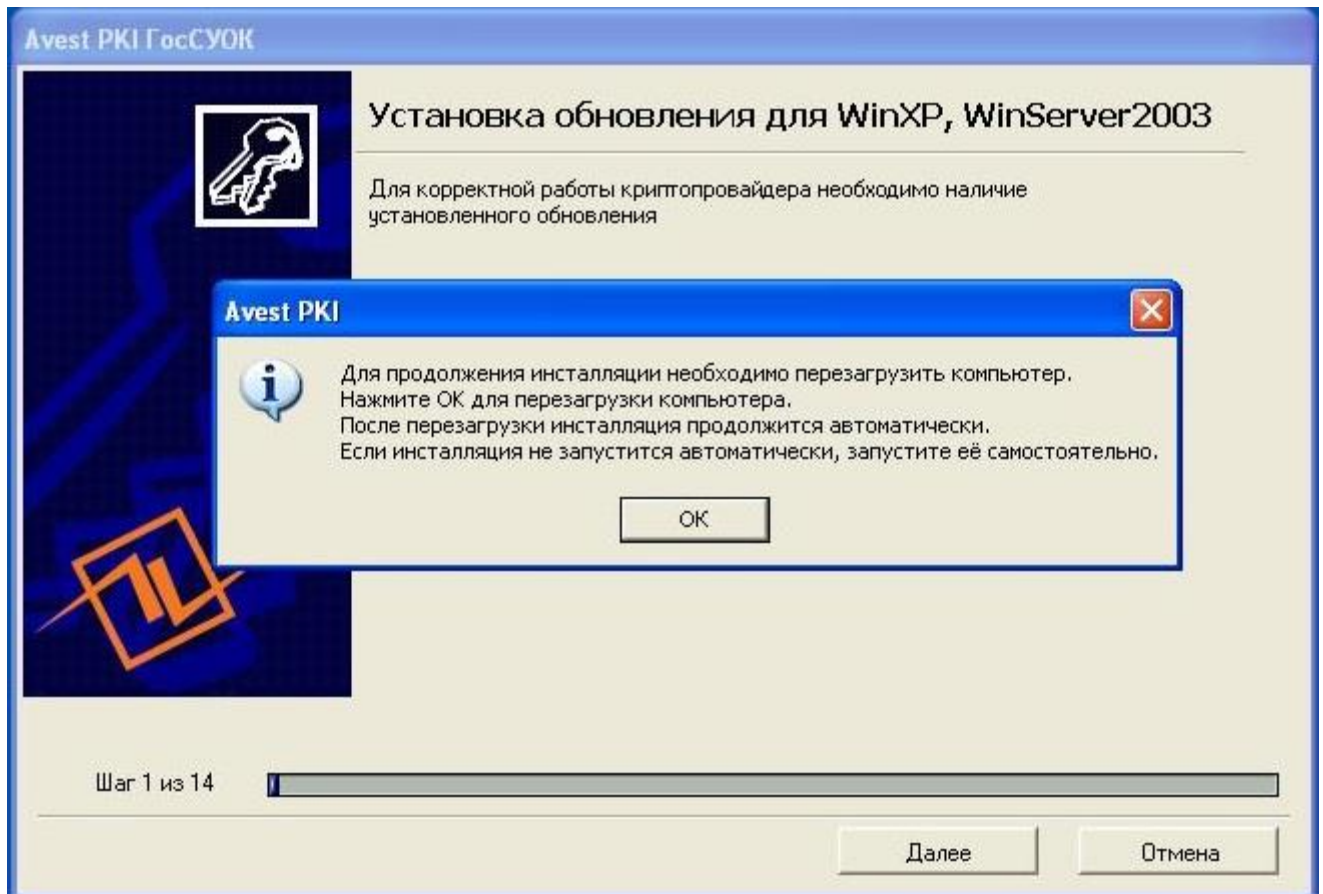


Рисунок 9 Предупреждение о перезагрузке

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 10 Ярлык «Продолжение установки AvPKISetup» (ярлык после успешной установки удалится с рабочего стола самостоятельно).

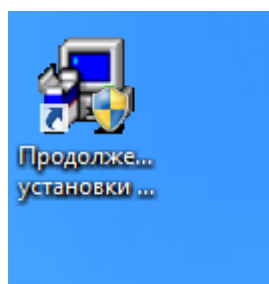


Рисунок 10 Ярлык «Продолжение установки AvPKISetup»

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 или обновление:

- криптопровайдера Avest CSP Bign (после установки будет выполнена перезагрузка компьютера),
- веб плагина AvCMXWebP,
- программного комплекса AvJCEProv,
- персонального менеджера сертификатов AvPCM_ncesBign,
- импорт сертификата в личный справочник и импорт атрибутного сертификата, *если соответствующие сертификаты были помещены в папку data в формате *.p7b (см. Приложение 1. Установка сертификатов с помощью объединенного инсталлятора AvPKISetup),*
- установка сертификатов удостоверяющих центров.

На шаге «Установка сертификатов удостоверяющих центров» будут выведены предупреждения операционной системы Windows о добавлении сертификатов корневых удостоверяющих центров в корневое хранилище, в этом сообщении указаны атрибуты помещаемых сертификатов. Если они соответствуют данным сертификатов ваших корневых УЦ, то нужно нажать «Да» в двух уведомлениях (см. Рисунок 11 Предупреждение системы безопасности).

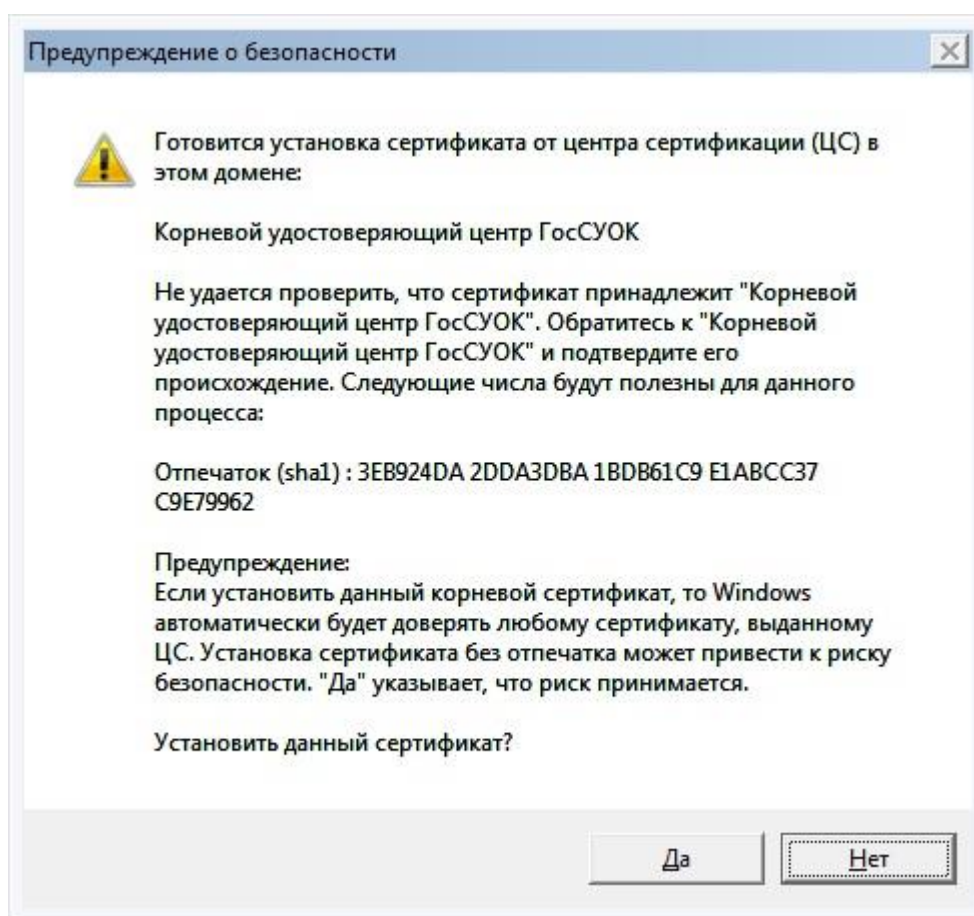
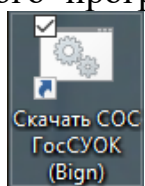


Рисунок 11 Предупреждение системы безопасности

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



ярлык «Скачать СОС ГосСУОК (Bign)».

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 «Заккрыть» (см. Рисунок 12 Завершение установки).

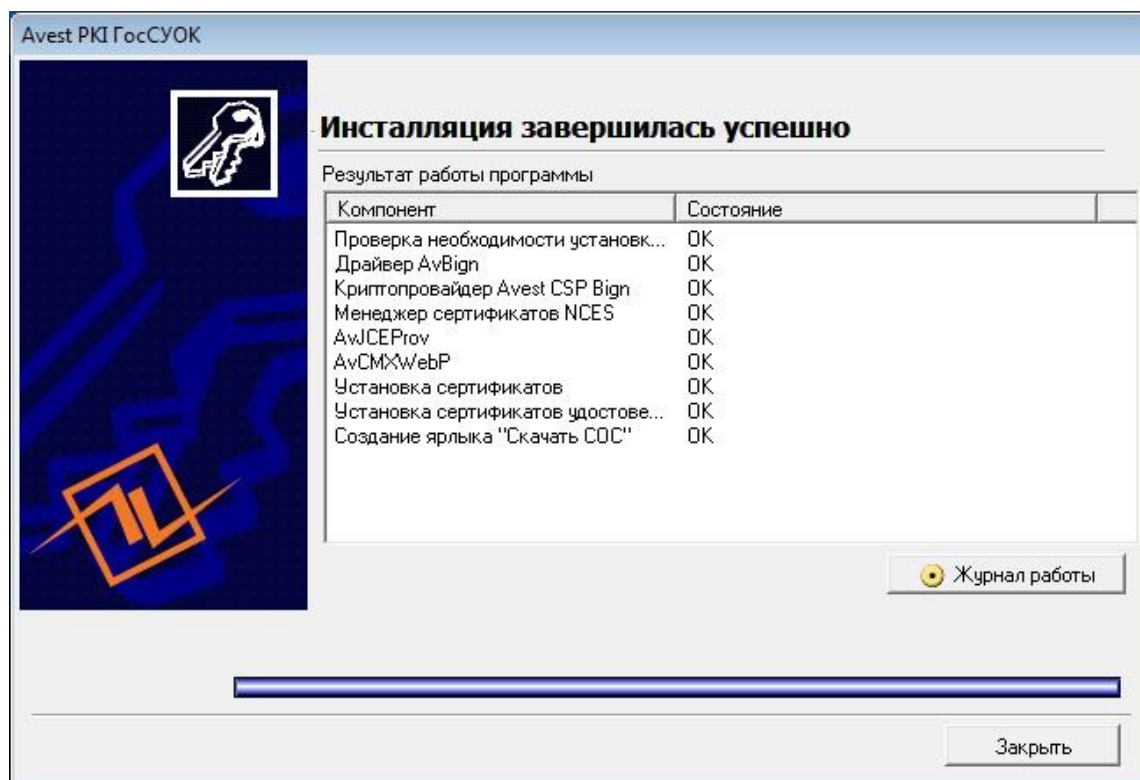


Рисунок 12 Завершение установки

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.

4. Удаление криптографического программного обеспечения с помощью объединенного инсталлятора

Для того, чтобы корректно удалить криптографическое программное обеспечение, нужно 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 13 Выбор типа инсталляции).

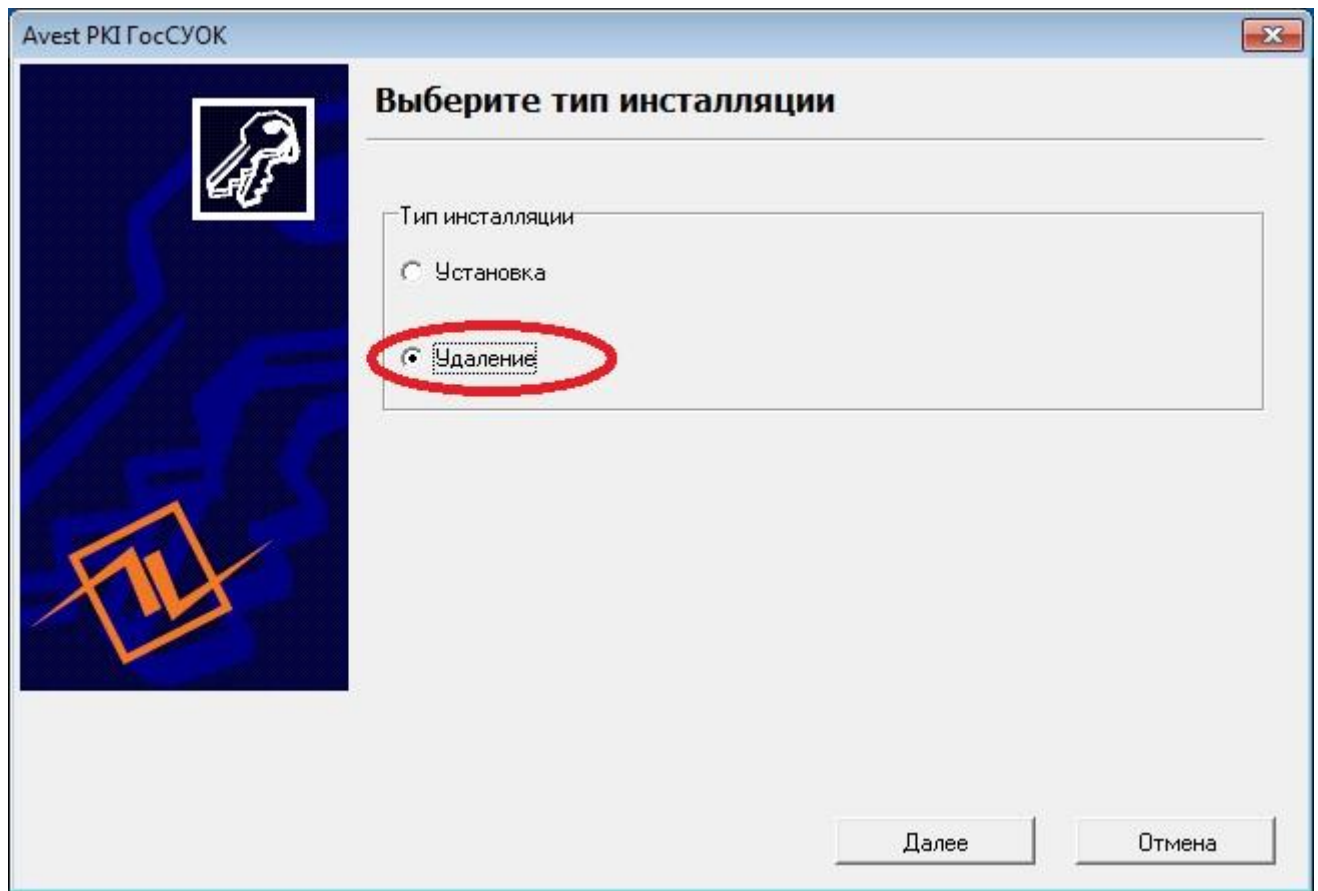


Рисунок 13 Выбор типа инсталляции

В следующем окне программа выводит список удаляемых компонентов. Необходимо выбрать те компоненты, которые надо удалить, и нажать кнопку «Далее» (см. Рисунок 14 Список удаляемых компонентов).

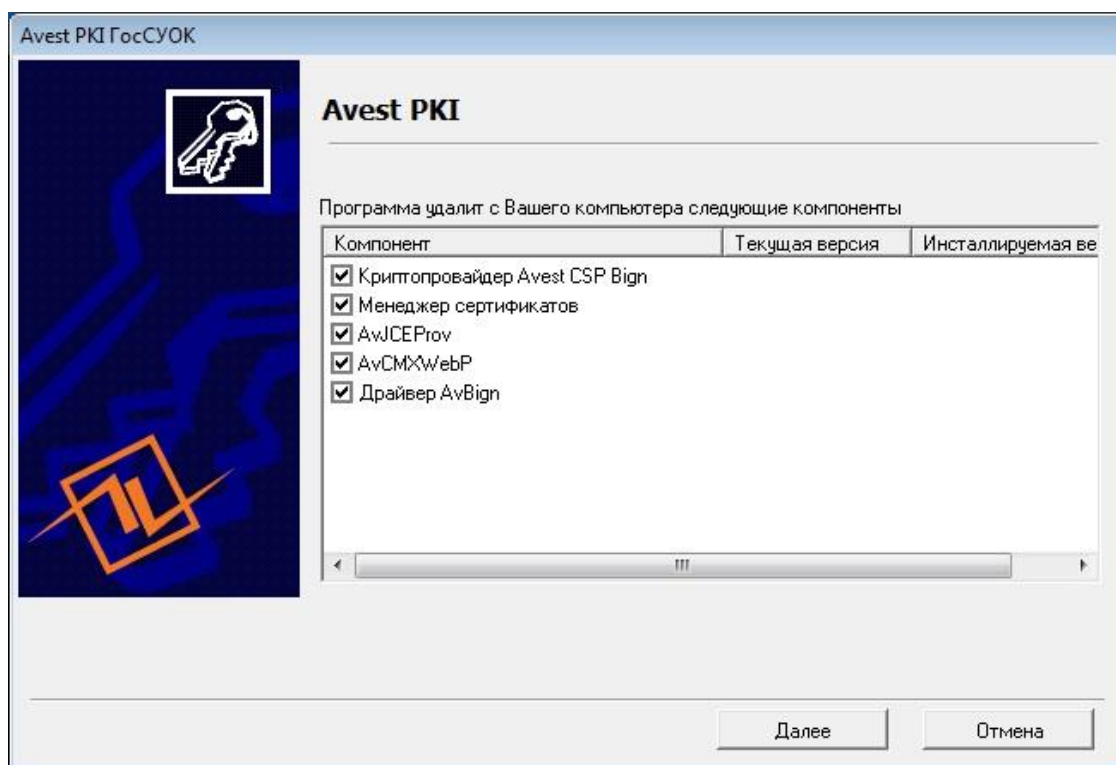


Рисунок 14 Список удаляемых компонентов

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 15 Результат работы программы).

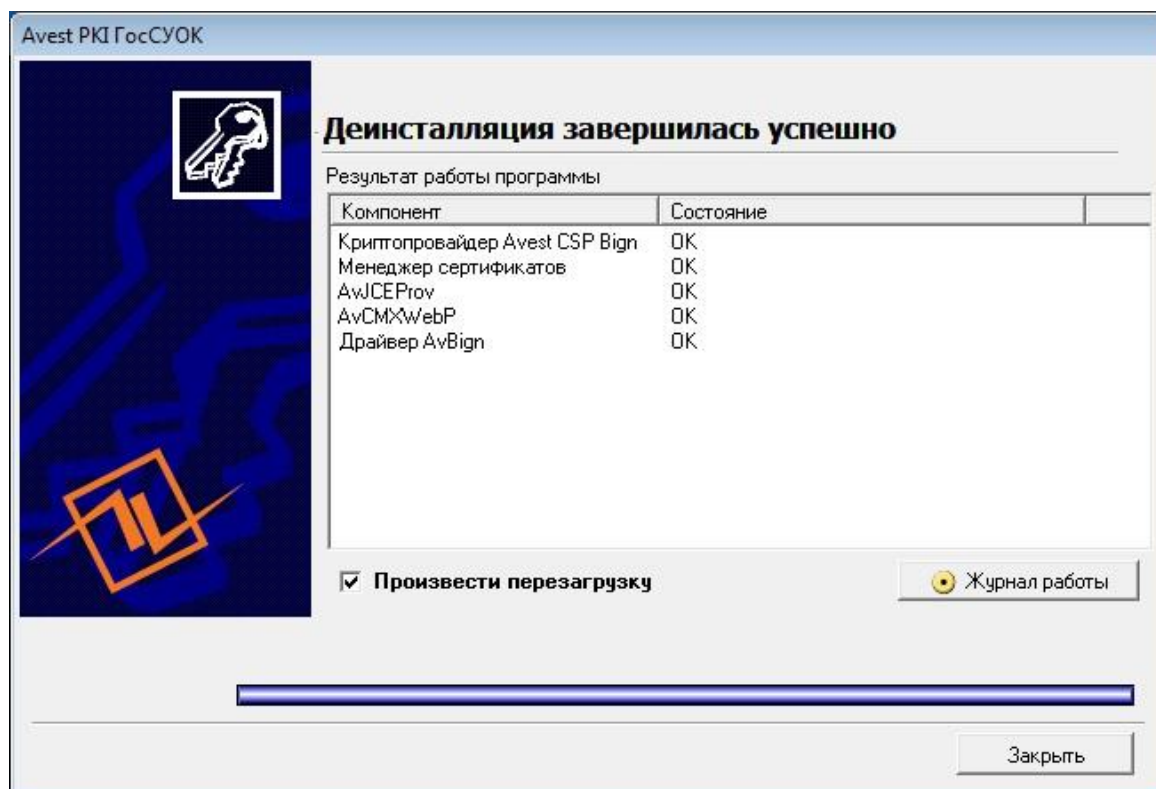


Рисунок 15 Результат работы программы

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 16 Предупреждение о необходимости перезагрузки).

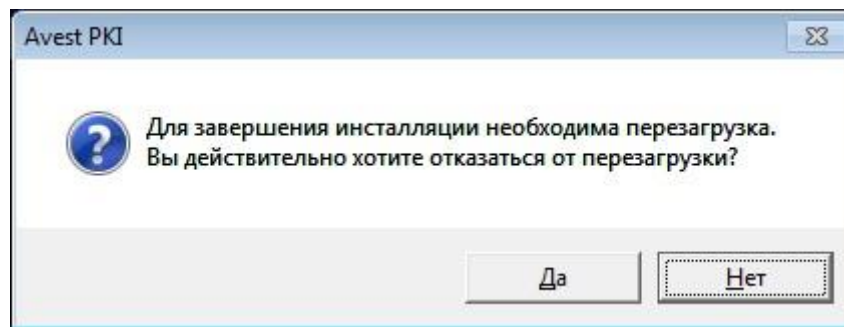


Рисунок 16 Предупреждение о необходимости перезагрузки

Также можно более подробно посмотреть результат работы мастера установки AvPKISetup, нажав кнопку «Журнал работы» (см. Рисунок 17 Журнал работы).

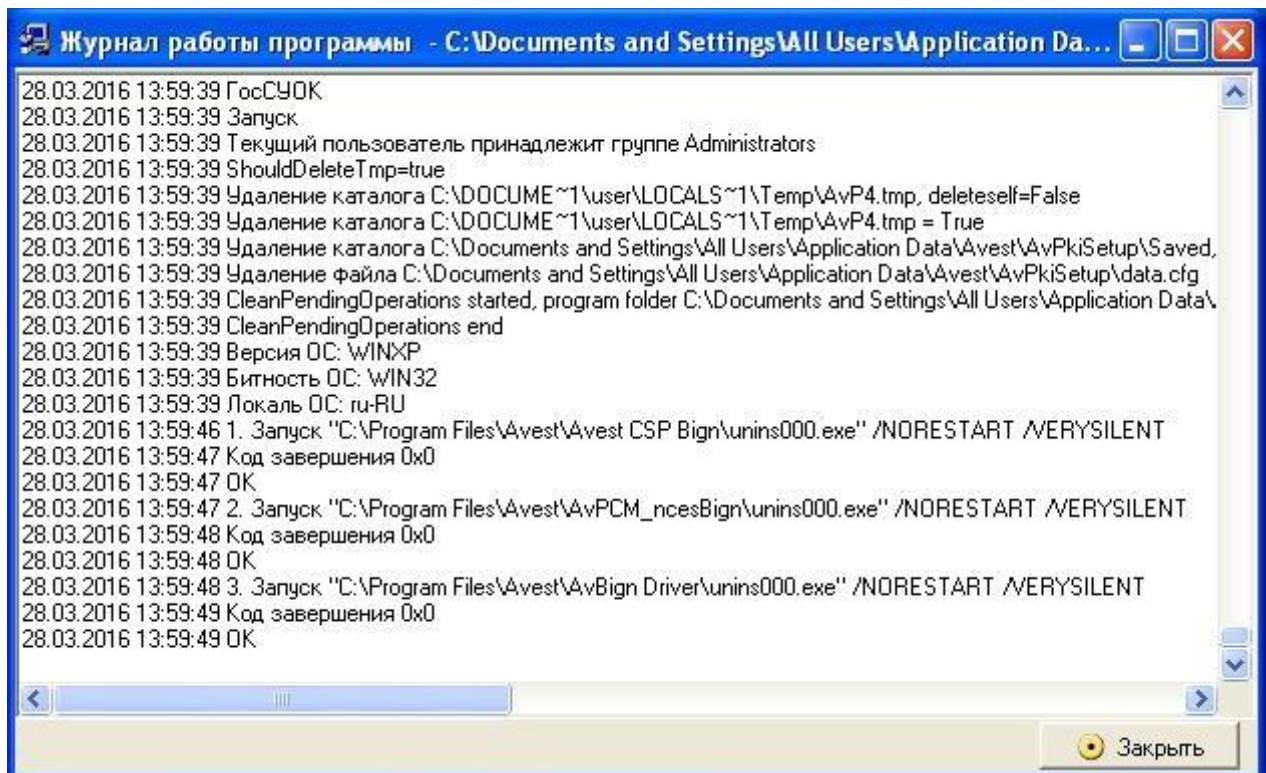


Рисунок 17 Журнал работы

Приложение 1. Установка сертификатов с помощью объединенного инсталлятора AvPKISetup

На шаге «Установка сертификатов», если сертификат был помещен в папку *data* в формате *.p7b, открывается окно мастера импорта сертификатов и происходит установка сертификатов в системные справочники Windows (см. Рисунок 18 Импортируемые сертификаты). Галочками отмечены сертификаты, которые будут проимпортированы и которые отсутствуют в системном справочнике. Нужно нажать кнопку «Далее». Если в списке импортируемых объектов сертификаты повторяются, оставьте галочки по умолчанию, как предлагает мастер импорта сертификатов.

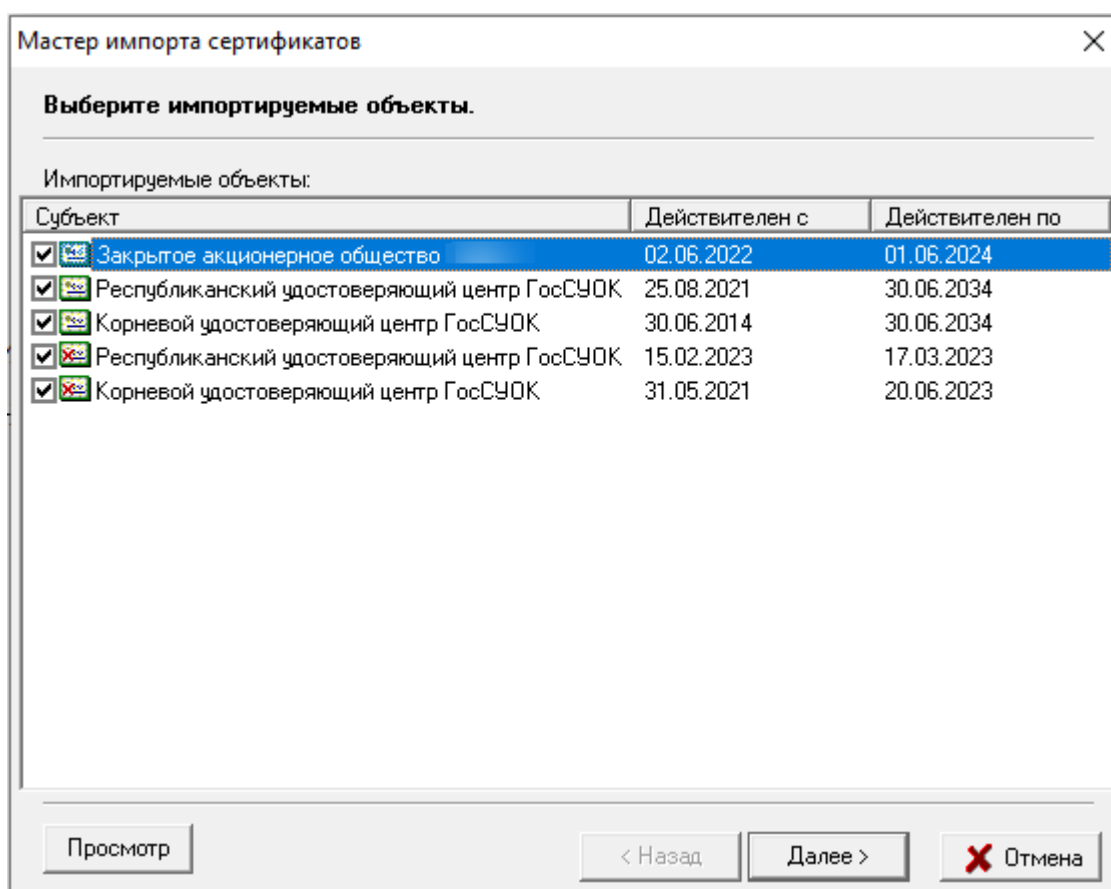


Рисунок 18 Импортируемые сертификаты

Мастер импорта уведомит о количестве импортированных сертификатов (см. Рисунок 19 Уведомление о количестве импортируемых сертификатов).

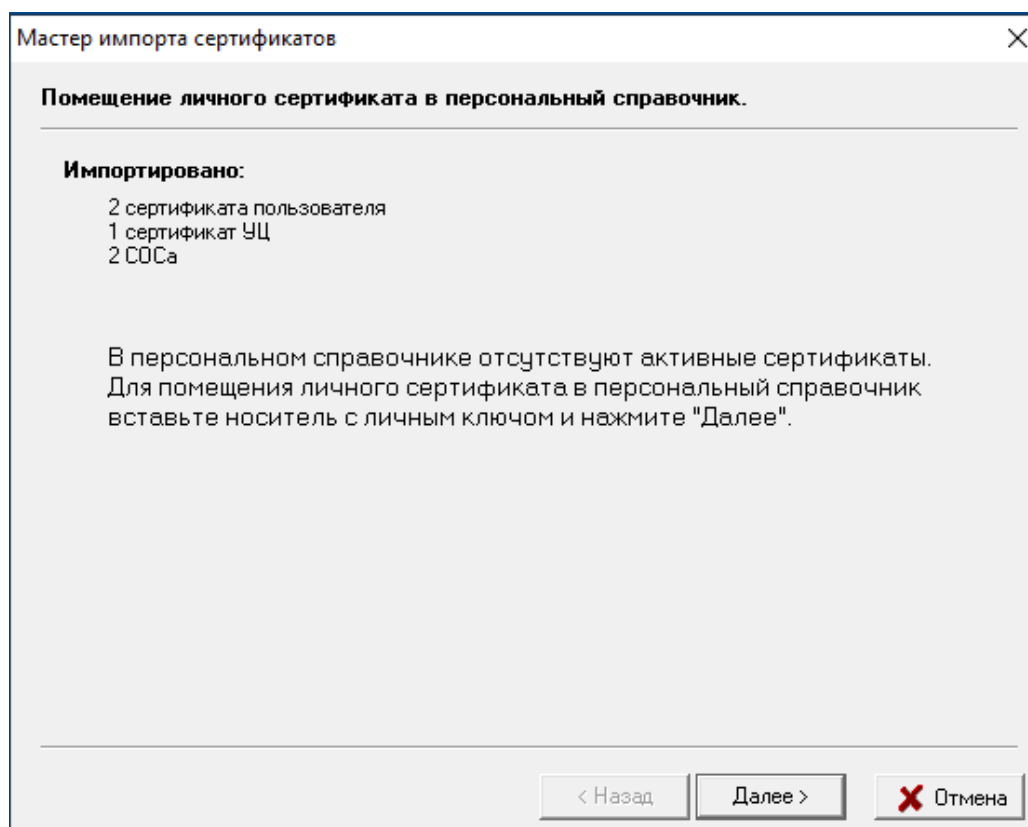


Рисунок 19 Уведомление о количестве импортируемых сертификатов

Для установки личного сертификата надо вставить носитель AvBign, 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 AvBign. Если на носителе записано более одного контейнера, то в списке нужно выбрать тот, который соответствует вашему личному сертификату. Определить это можно, например, по дате генерации контейнера с личным ключом (по умолчанию контейнер с личным ключом создается с именем «[Наименование организации владельца открытого ключа]_дд_мм_гг_чч_мм», где «дд_мм_гг_чч_мм» – это время генерации ключей). После того, как соответствующий контейнер выбран, нужно нажать на кнопку «Далее» (см. Рисунок 20 Выбор контейнера).

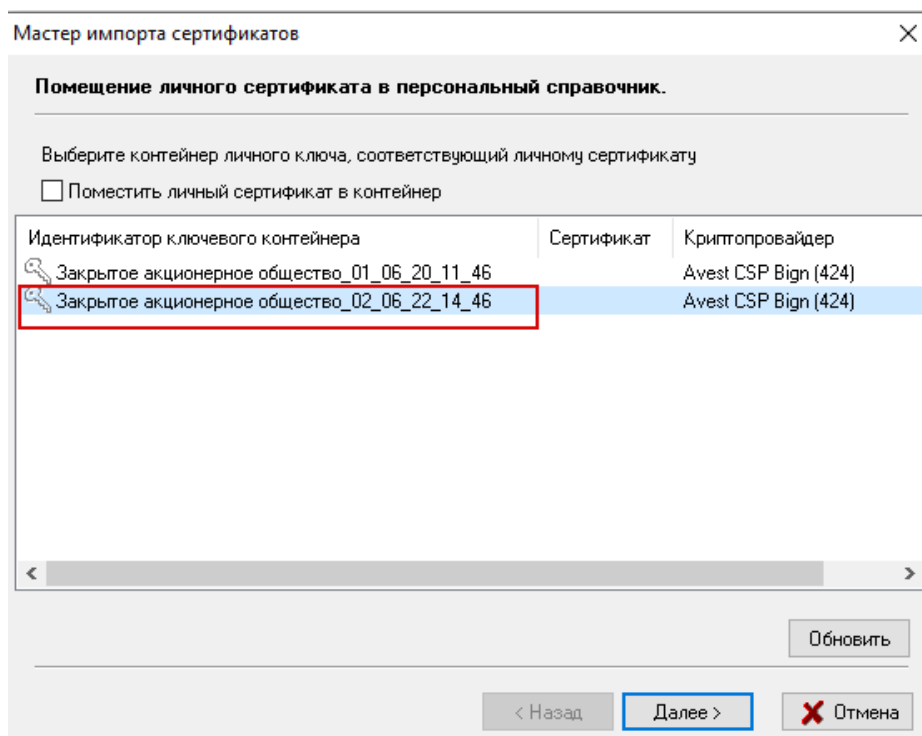


Рисунок 20 Выбор контейнера

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 21 Сертификаты корневых удостоверяющих центров).

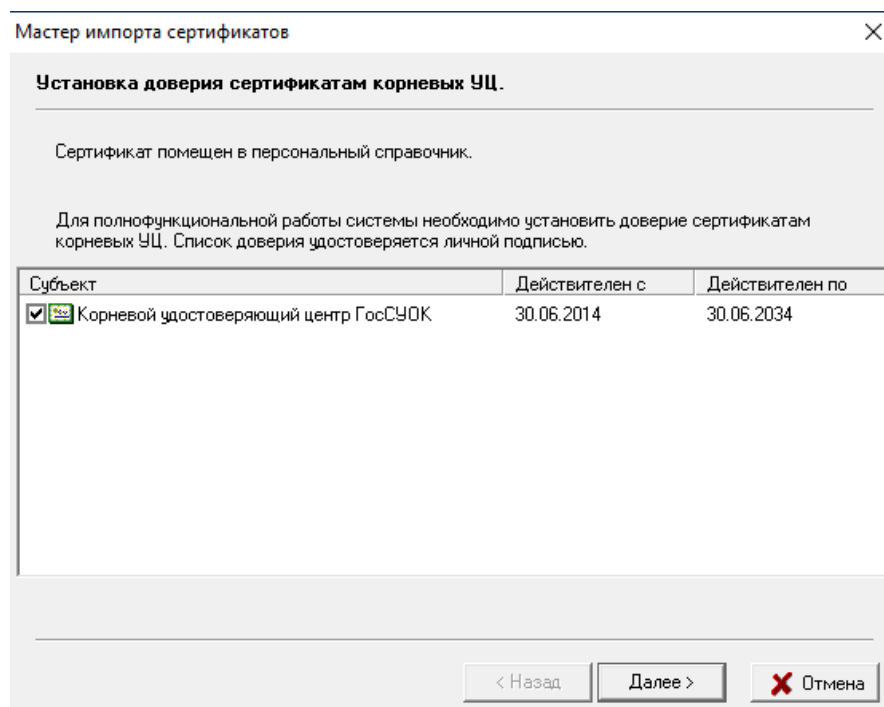


Рисунок 21 Сертификаты корневых удостоверяющих центров

На этом шаге 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 сертификата вашего корневого УЦ, то нужно нажать «Да» (см. Рисунок 22 Предупреждение системы безопасности).

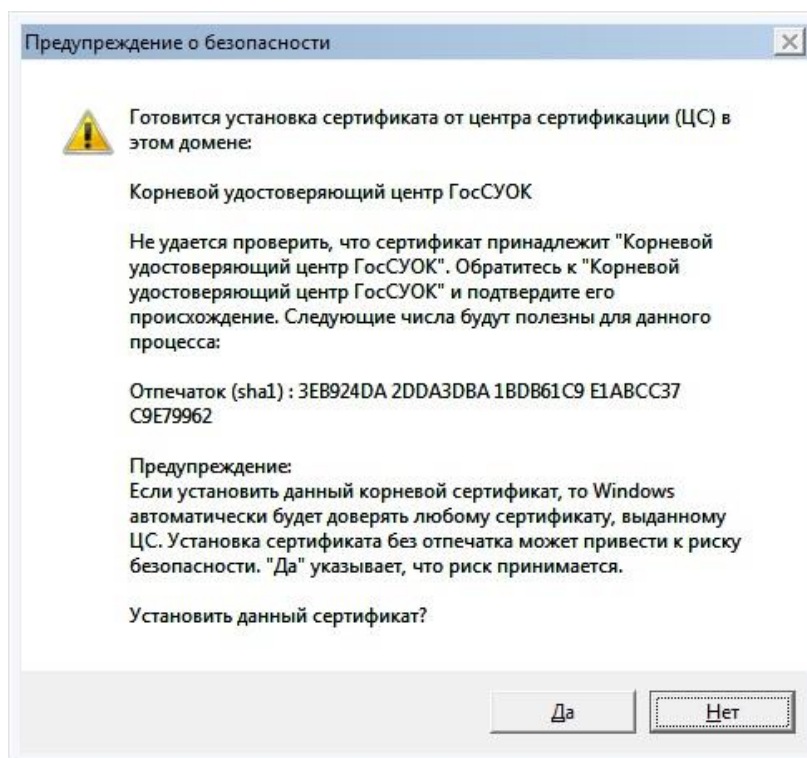


Рисунок 22 Предупреждение системы безопасности

На следующем шаге мастер импорта сертификатов уведомит о сертификатах, которым было установлено доверие, нажать кнопку «Закреть» (см. Рисунок 23 Завершение работы мастера импорта сертификатов).

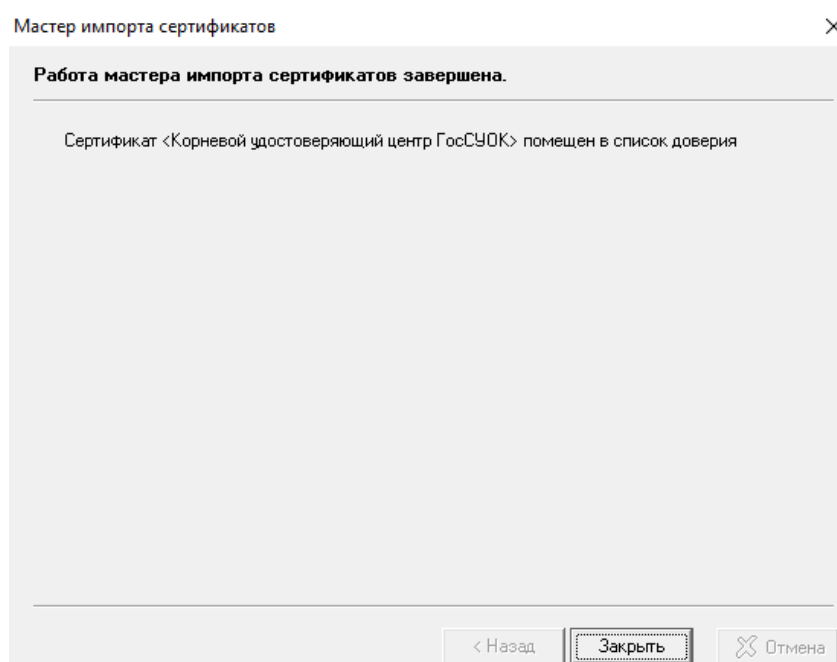


Рисунок 23 Завершение работы мастера импорта сертификатов

Приложение 2. Способы получения/обновления списков отозванных сертификатов

1) Через персональный менеджер сертификатов Авест для ГосСУОК.

Для того, чтобы запустить обновление СОС (а также проимпортировать недостающие сертификаты удостоверяющих центров и службы атрибутивных сертификатов), 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_ncesBign\`, если ОС 64-разрядная, или `c:\Program Files\Avest\AvPCM_ncesBign\`, если ОС 32-разрядная. Для этого нужно добавить секцию `HttpProху` с актуальными значениями для подключения:

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

В строке `ProxyServer=` указывается адрес прокси сервера.

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

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

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

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

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

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

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

```
ReadTimeOut=180
```

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

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 ГосСУОК (Bign)», нажав на который можно получить актуальные СОС.

Или зайти по пути c:\Program Files (x86)\Avest\AvPCM_ncesBign (c:\Program Files\Avest\AvPCM_ncesBign) и запустить файл get_crl.bat.

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

```
set PX_USER=--proxy-user=  
set PX_PASS=--proxy-password=  
set http_proxy=  
set https_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» («Программы») – «Авест для НЦЭУ (Bign)» запустить «Персональный менеджер сертификатов Авест для ГосСУОК (Bign)» с авторизацией или без авторизации,

- в менеджере выбрать пункт меню «Файл» – «Импорт сертификата/СОС» (см. *Рисунок 25 Импорт сертификата*), указать путь к скачанному файлу СОС в формате *.crl и проимпортировать его, следуя указаниям мастера импорта сертификатов.

4) 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, если ОС 64-разрядная, или c:\Program Files\Avest\AvPCM_ncesBign, если ОС 32-разрядная. Если выход в интернет осуществляется через прокси, настройки get_crl.bat описаны выше.

2) Скачать актуальный СОС с сайта nces.by и проимпортировать через персональный менеджер сертификатов Авест для ГосСУОК (Bign).

Для этого

- из папки «Пуск» – «Все программы» («Программы») – «Авест для НЦЭУ (Bign)» запустить «Персональный менеджер сертификатов Авест для ГосСУОК (Bign)» с авторизацией или без авторизации,

- в менеджере выбрать пункт меню «Файл» – «Импорт сертификата/СОС» (см. *Рисунок 25 Импорт сертификата*), указать путь к скачанному файлу СОС в формате *.crl и проимпортировать его, следуя указаниям мастера импорта сертификатов.

Приложение 3. Импорт личного сертификата в персональный менеджер сертификатов Авест

В случае, когда программное обеспечение Авест на компьютере было ранее установлено и необходимо проимпортировать только личный сертификат, надо из меню «Пуск» – «Все программы» («Программы») – «Авест для НЦЭУ (Bign)» запустить «Персональный менеджер сертификатов Авест для ГосСУОК (Bign)» без авторизации (см. Рисунок 24 Запуск менеджера без авторизации).

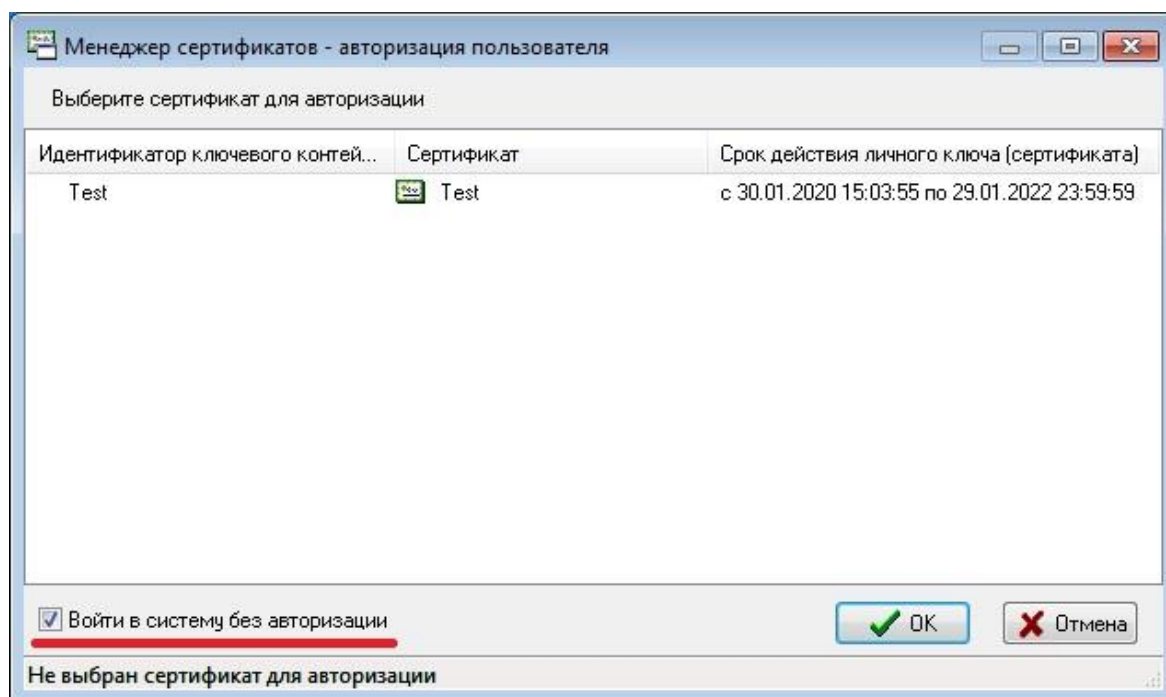


Рисунок 24 Запуск менеджера без авторизации

Далее выбрать пункт меню «Файл» – «Импорт сертификата/СОС» (см. Рисунок 25 Импорт сертификата).

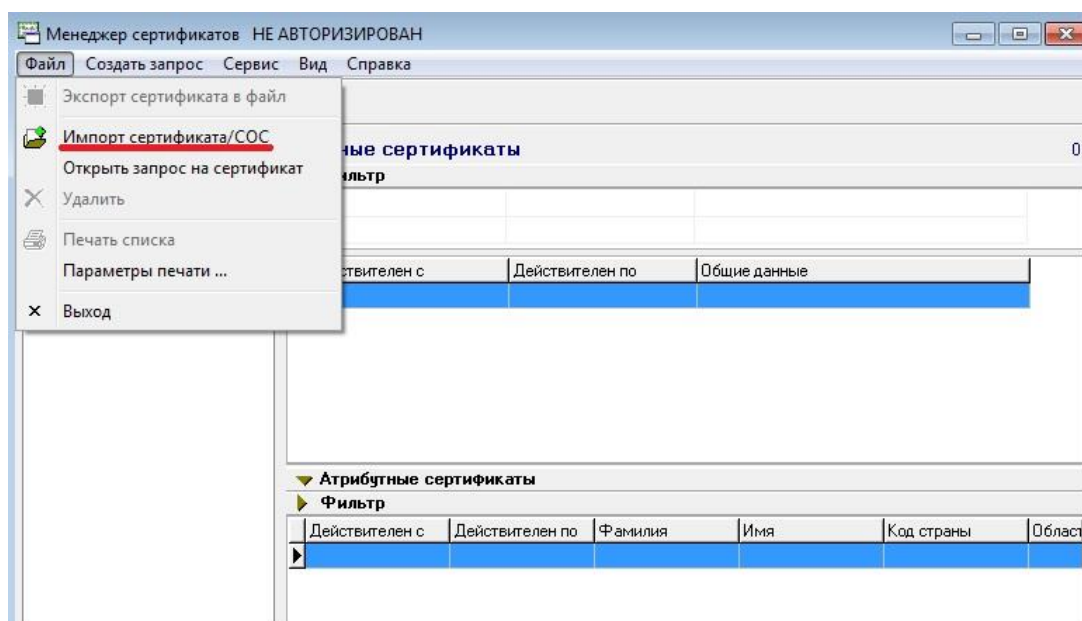


Рисунок 25 Импорт сертификата

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 26 Выбор импортируемого файла).

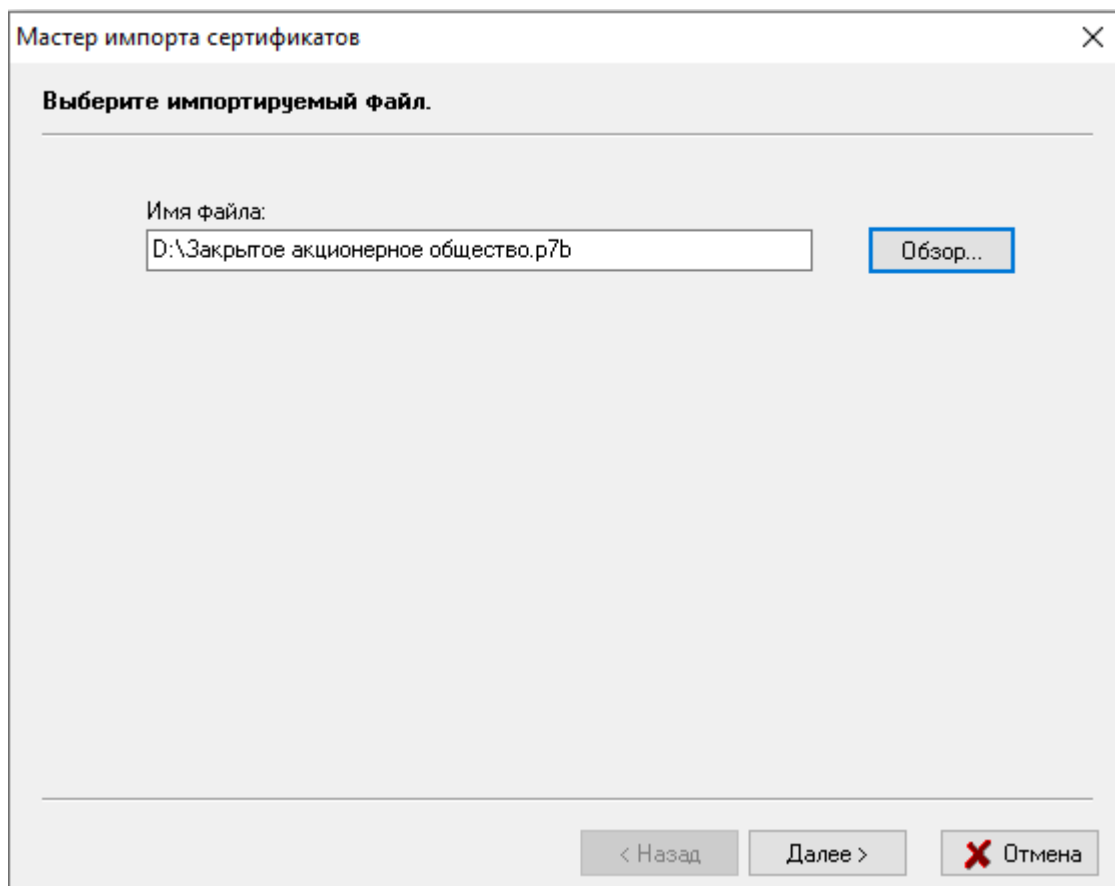


Рисунок 26 Выбор импортируемого файла

В появившемся окне в виде таблицы будут отражены все объекты, которые входят в импортируемый файл (см. Рисунок 27 Информация об импортируемых объектах).

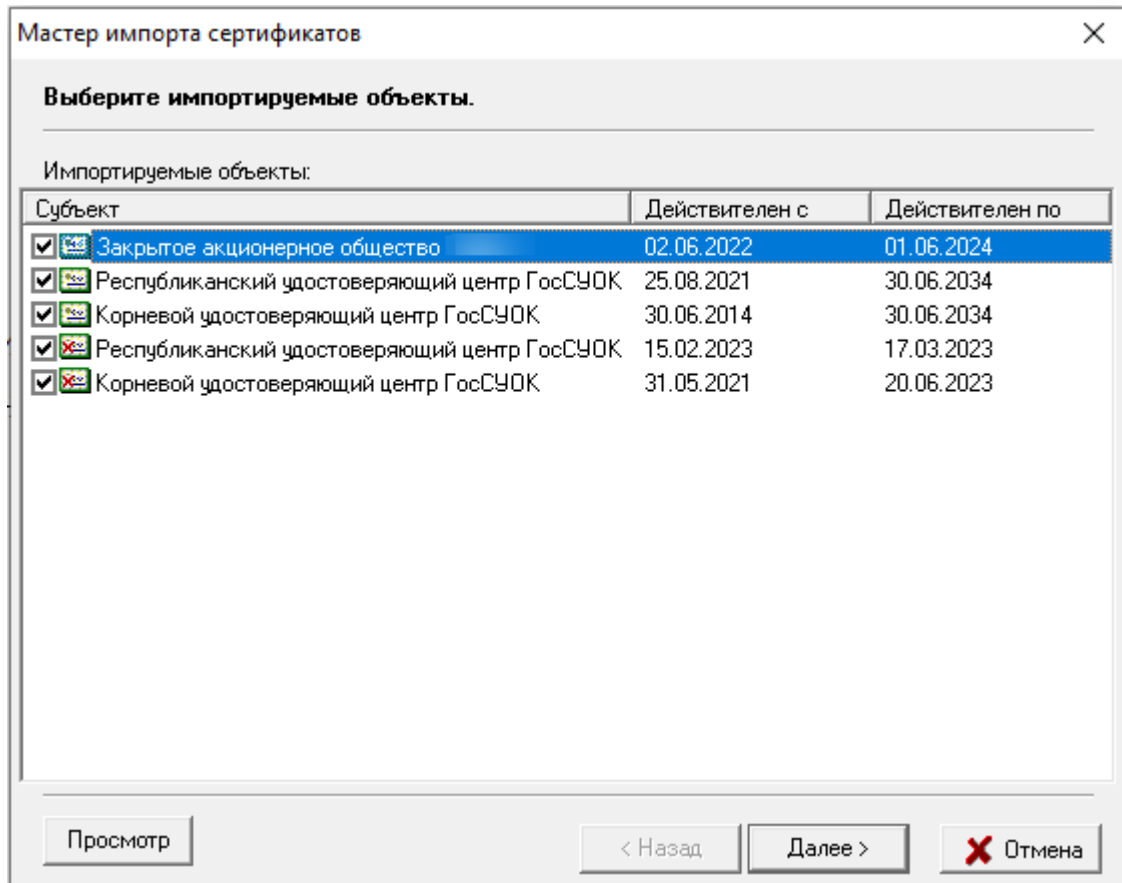


Рисунок 27 Информация об импортируемых объектах

В следующем окне содержится информация о количестве импортированных объектов и предложено поместить личный сертификат в персональный справочник (см. Рисунок 28 Уведомление о количестве импортируемых сертификатов).

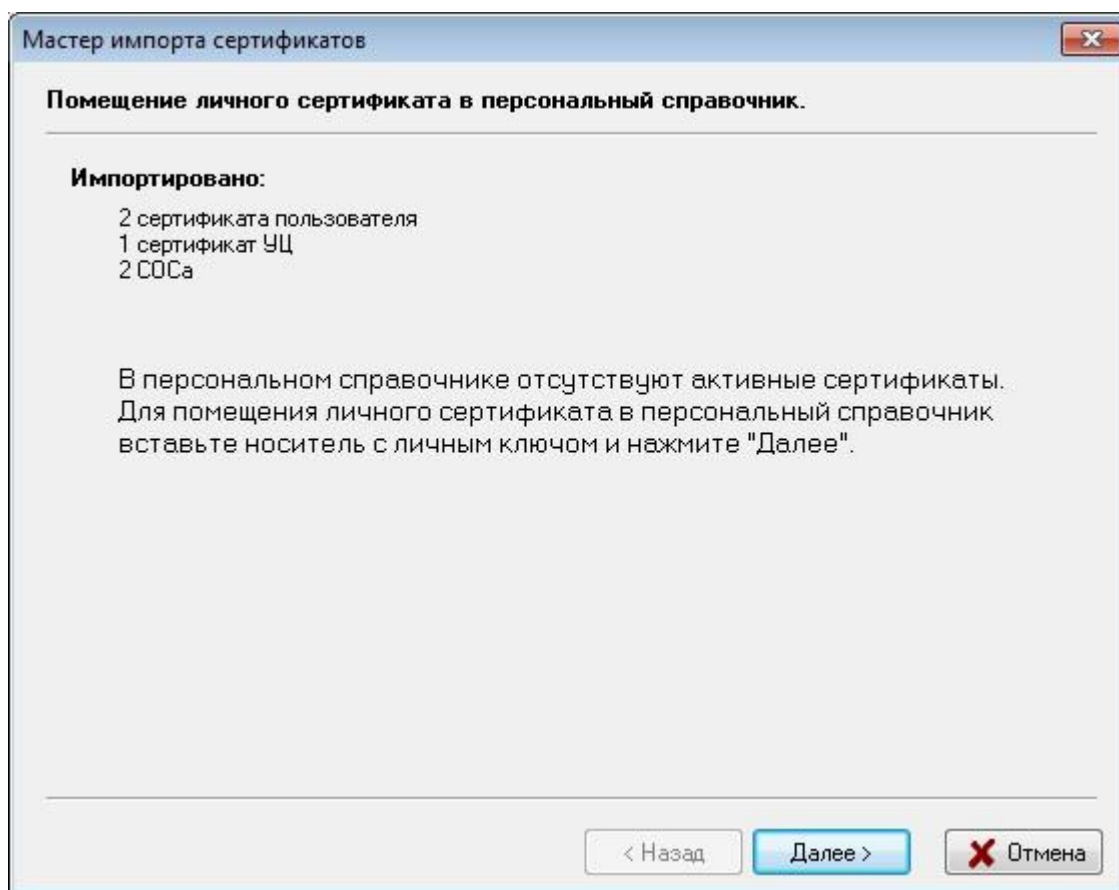


Рисунок 28 Уведомление о количестве импортируемых сертификатов

Для установки личного сертификата надо вставить носитель AvBign, 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 AvBign. Если на носителе записано более одного контейнера, то в списке нужно выбрать тот, который соответствует вашему личному сертификату. Определить это можно, например, по дате генерации контейнера с личным ключом (по умолчанию контейнер с личным ключом создается с именем «[Наименование организации владельца открытого ключа]_дд_мм_гг_чч_мм», где «дд_мм_гг_чч_мм» – это время генерации ключей). После того, как соответствующий контейнер выбран, нужно нажать на кнопку «Далее» (см. Рисунок 29 Выбор контейнера личного ключа, соответствующего личному сертификату).

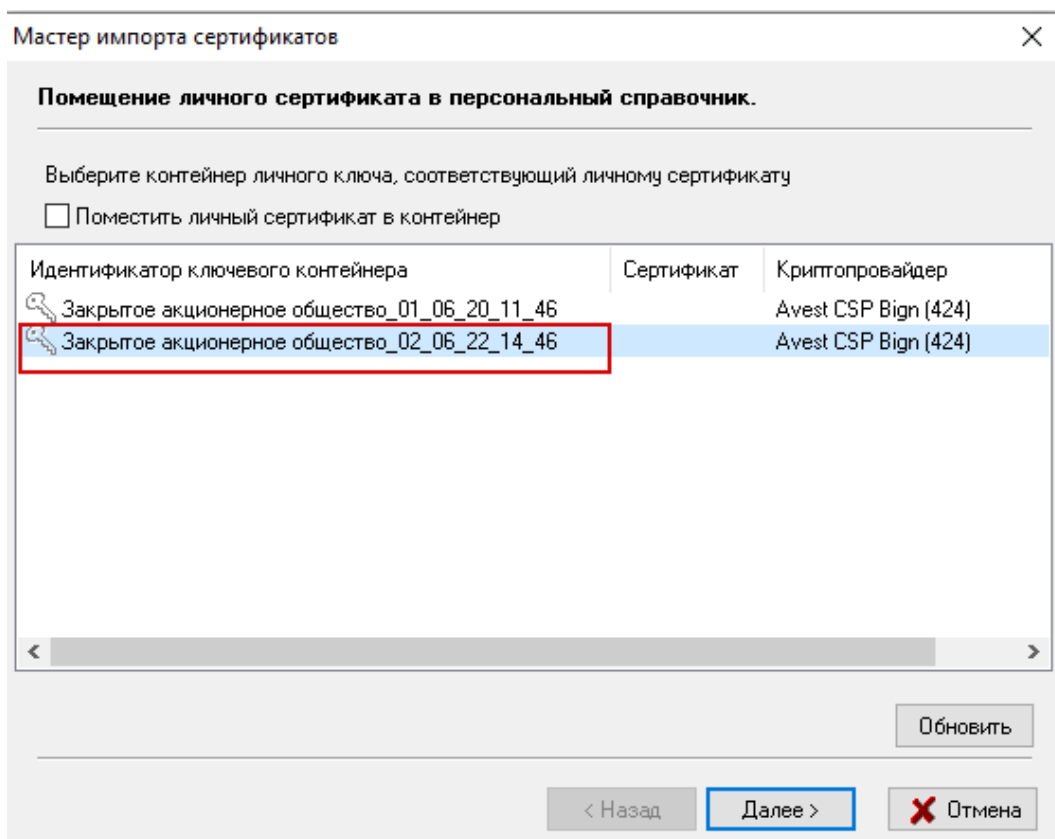


Рисунок 29 Выбор контейнера личного ключа, соответствующего личному сертификату

Затем для доступа к ключевому контейнеру в окне «Контейнер личных ключей» нужно ввести пароль, который вы вводили при генерации личных ключей (см. Рисунок 30 Ввод пароля доступа к контейнеру личного ключа).

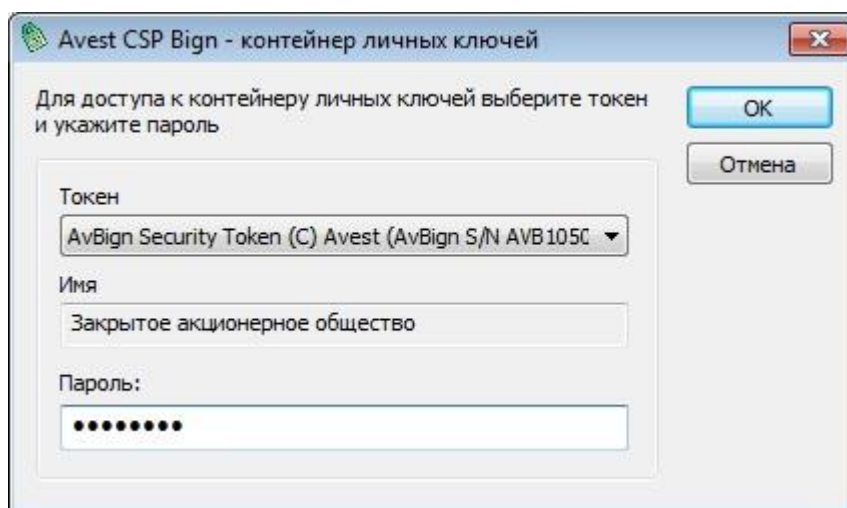


Рисунок 30 Ввод пароля доступа к контейнеру личного ключа

Для полноценной работы программы необходимо установить доверие к корневому сертификату УЦ. Для этого в следующем окне надо включить флажок «Установить доверие сертификату корневого УЦ» (см. Рисунок 31 Установка доверия сертификату корневого УЦ).

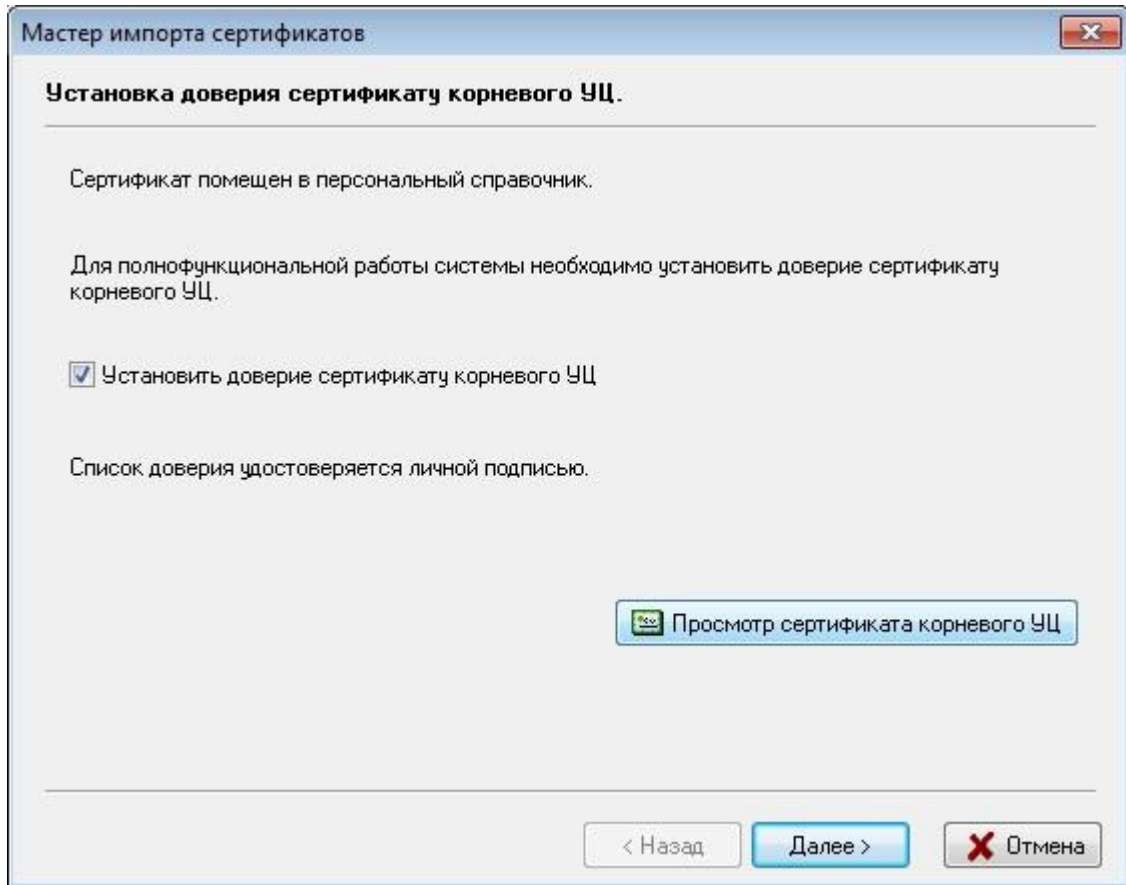


Рисунок 31 Установка доверия сертификату корневого УЦ

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 32 Предупреждение системы безопасности).

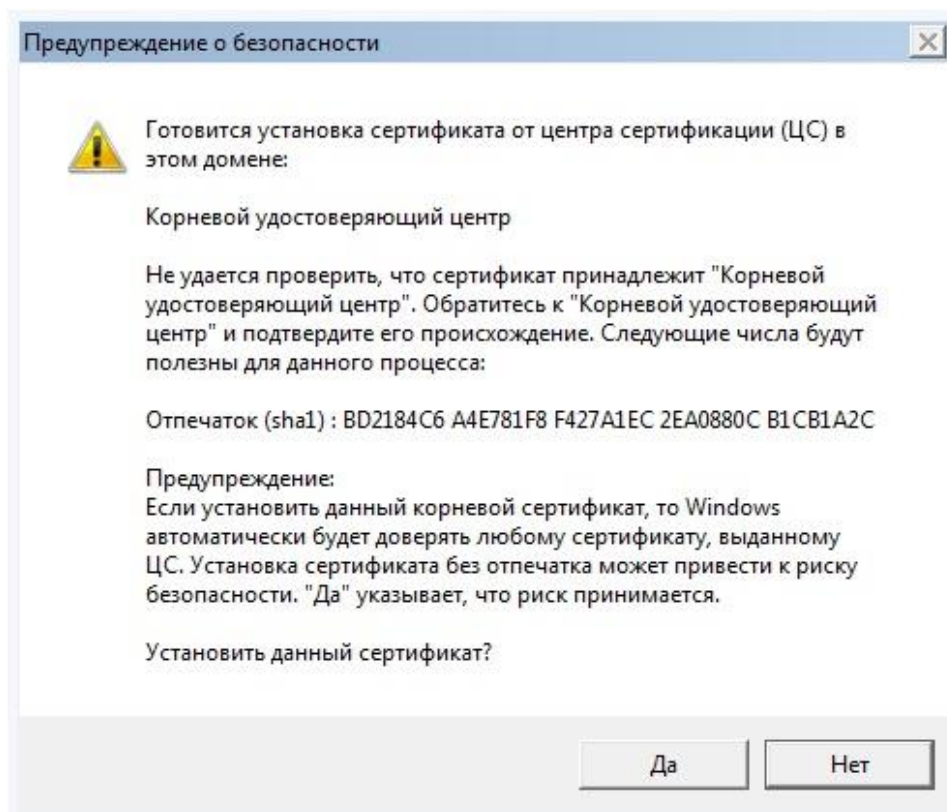


Рисунок 32 Предупреждение системы безопасности

После этого будет выведено сообщение о том, что корневой сертификат УЦ помещен в список доверия и мастер импорта сертификатов завершил работу, нужно нажать «Заккрыть» (см. Рисунок 33 Завершение работы мастера импорта сертификатов).

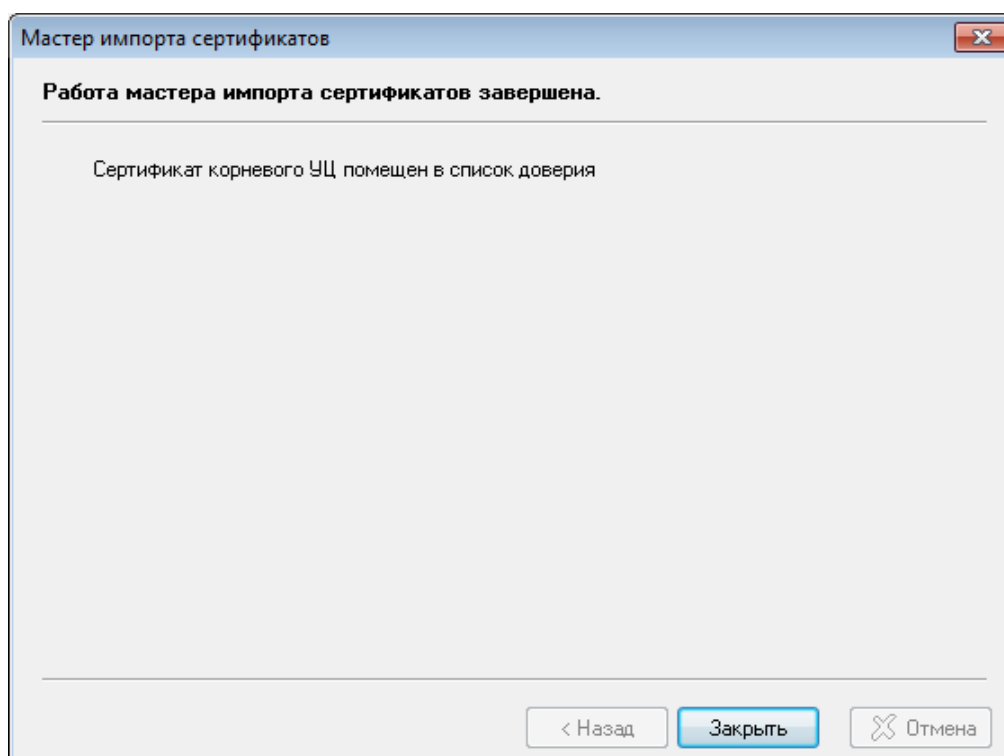


Рисунок 33 Завершение работы мастера импорта сертификатов

После успешного импорта личный сертификат появится в личном справочнике, он будет обведен красной рамкой, в окне заголовка менеджера будет отображаться общее имя (общие данные) личного сертификата (см. Рисунок 34. Сертификат в личном справочнике).

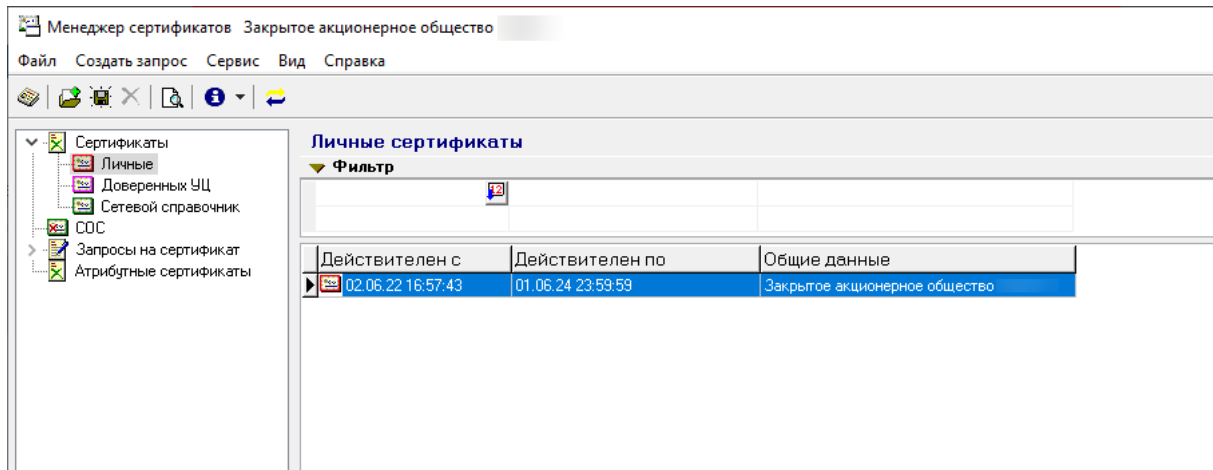


Рисунок 34. Сертификат в личном справочнике

Приложение 4. Импорт атрибутного сертификата в формате *.асг в персональный менеджер сертификатов Авест

В случае, если атрибутный сертификат сохранен в формате *.асг, объединенный инсталлятор AvPKISetup его не проимпортирует, и такой сертификат импортируется вручную. Установка атрибутного сертификата происходит после установки программного обеспечения Авест и импорта личного сертификата.

1. Запустить «Персональный менеджер сертификатов Авест для ГосСУОК (Bign)» («Пуск» – «Все программы» – «Авест для НЦЭУ (Bign)» или запустить на рабочем столе ярлык «Персональный менеджер сертификатов Авест для ГосСУОК (Bign)»).
2. Поставить галочку в пункте «Войти в систему без авторизации», нажать «ОК» (см. Рисунок 35 Запуск менеджера без авторизации).

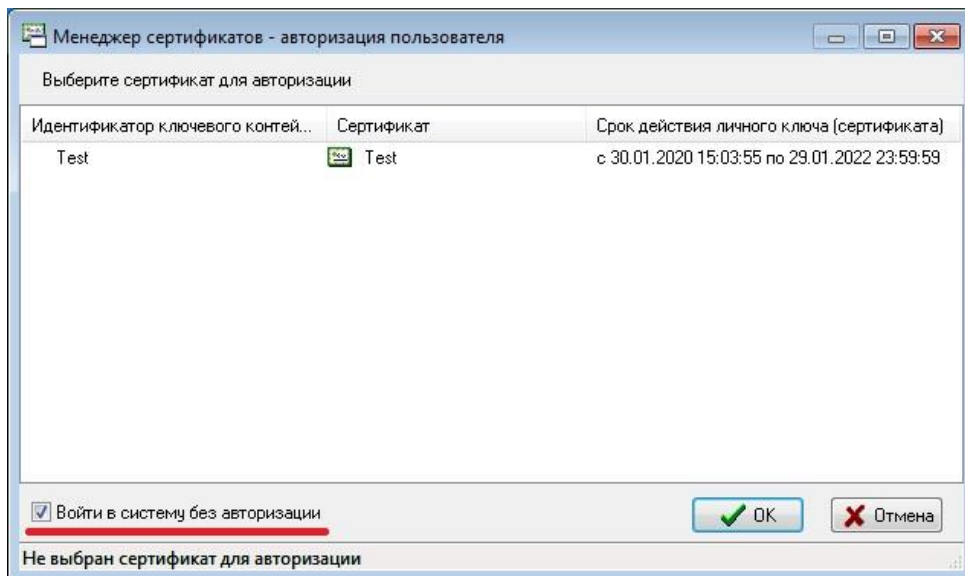


Рисунок 35 Запуск менеджера без авторизации

3. Далее выбрать пункт меню «Файл» – «Импорт сертификата/СОС» (см. Рисунок 36 Импорт сертификата).

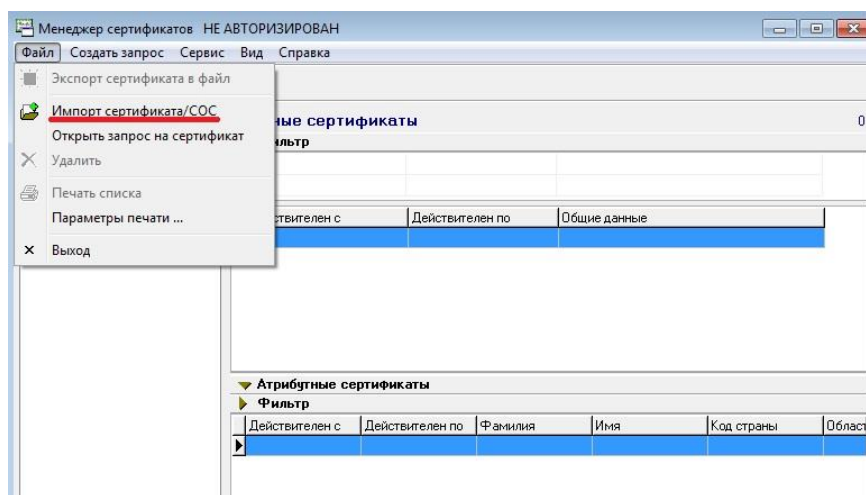


Рисунок 36 Импорт сертификата

4. В диалоговом окне мастера импорта сертификатов на шаге «Выберите импортируемый файл», нажав кнопку «Обзор», выбрать импортируемый файл атрибутного сертификата, нажать «Открыть», затем «Далее» (см. Рисунок 37 Выбор импортируемого файла).

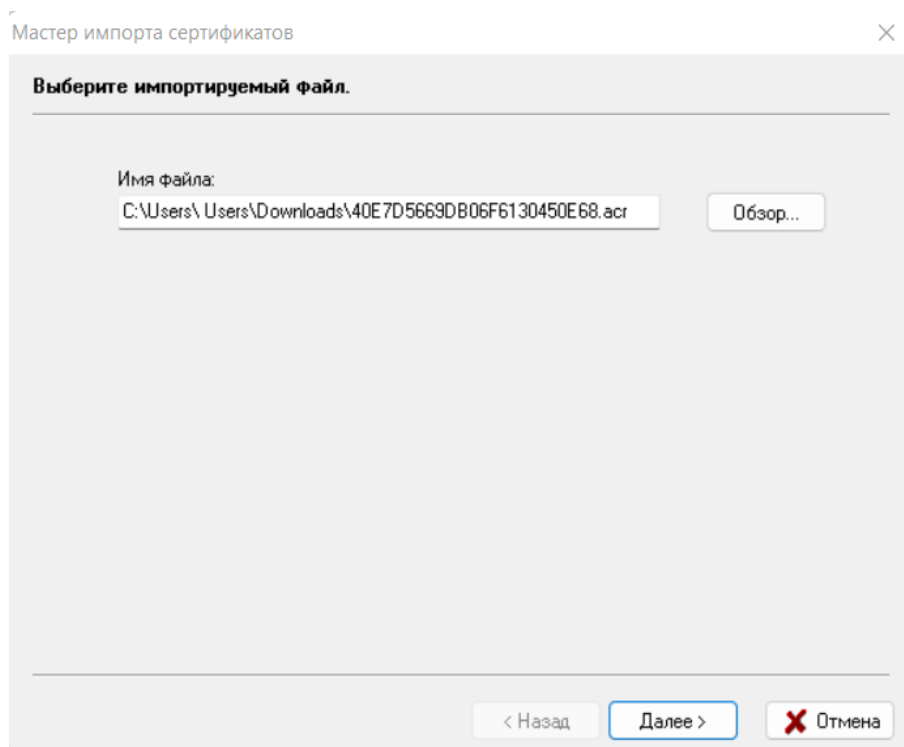


Рисунок 37 Выбор импортируемого файла

5. В следующем окне мастера импорта сертификатов на шаге «Выберите импортируемые объекты» отобразится импортируемый атрибутный сертификат. Если атрибутный сертификат еще не присутствует в справочнике, напротив него будет установлена галочка, и здесь нужно нажать «Далее» (см. Рисунок 38 Импортируемые объекты). Если галочка не стоит, значит данный сертификат уже был установлен и импорт его не требуется.

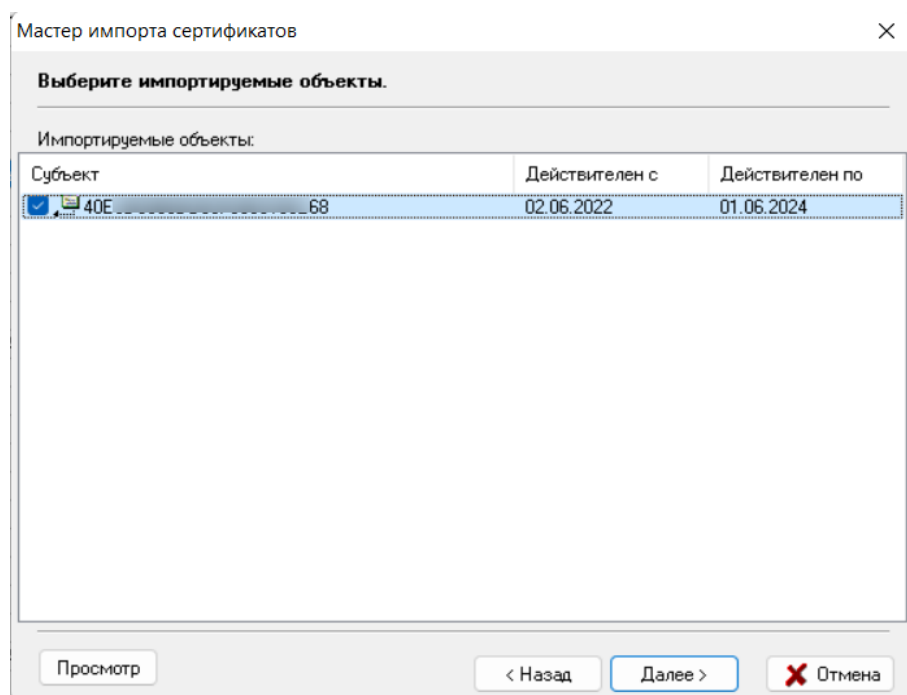


Рисунок 38 Импортируемые объекты

6. В финальном окне мастера импорта сертификатов появится информация, что атрибутный сертификат был проимпортирован (или не проимпортирован, если он уже присутствует в справочнике), нужно нажать «ОК» (см. Рисунок 39 Завершение работы мастера импорта сертификатов).

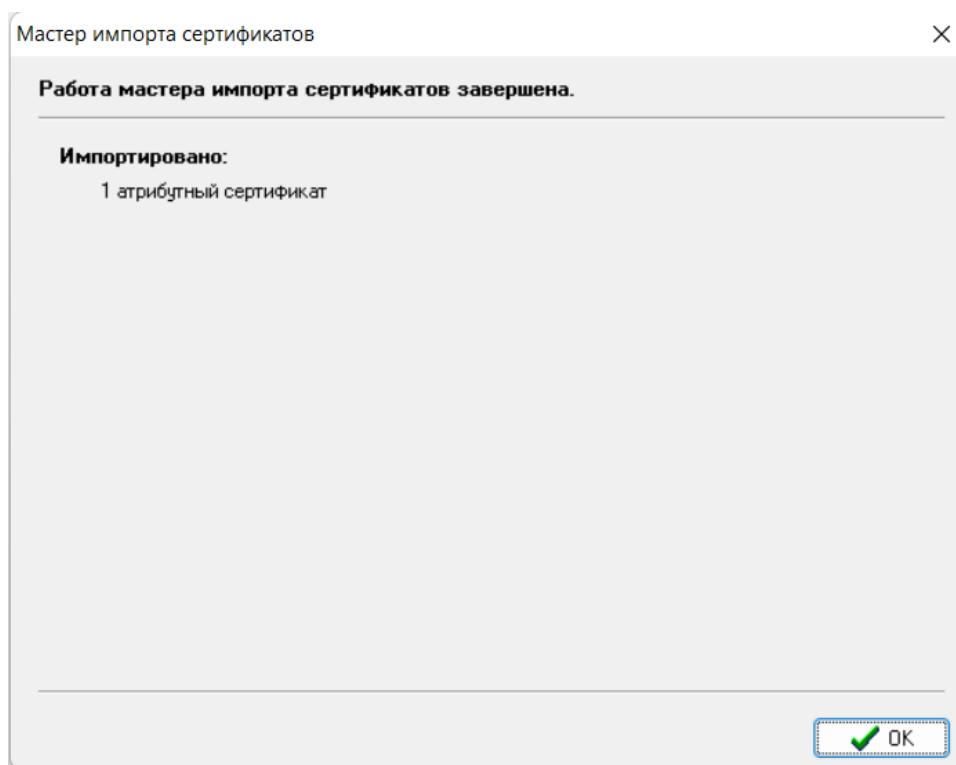


Рисунок 39 Завершение работы мастера импорта сертификатов

7. После импорта атрибутный сертификат будет отображаться в нижней части главного окна после выбора соответствующего личного сертификата в верхней части окна (см. Рисунок 40. Отображение атрибутного сертификата).

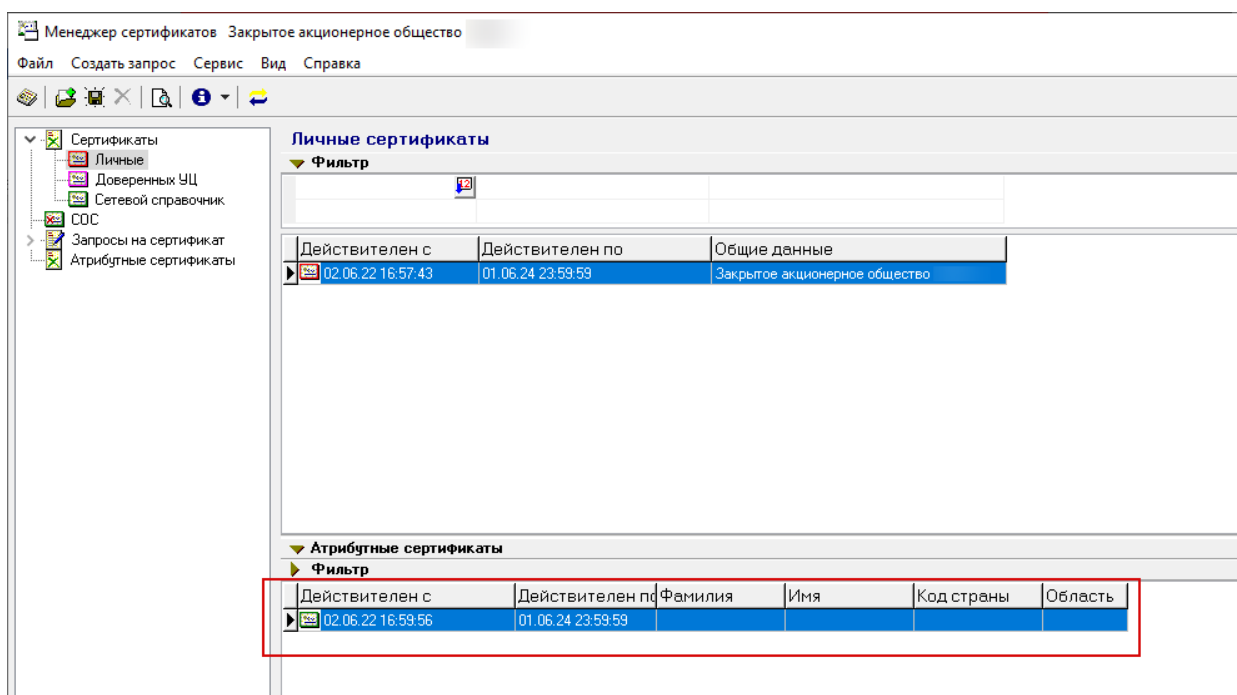


Рисунок 40. Отображение атрибутного сертификата

Поскольку атрибутный сертификат в формате *.acg не включает сертификат издателя и СОС, следующим шагом будет импорт сертификатов и СОС служб атрибутных сертификатов.

Сделать это можно вручную:

1. Сертификаты служб атрибутных сертификатов находятся в папке data, входящей в состав комплекта абонента AvPKISetup (файлы cas_ruc2.cer и cas_ruc3.cer), также файлы сертификатов служб атрибутных сертификатов можно скачать по ссылкам:
https://nces.by/wp-content/uploads/certificates/pki/cas_ruc2.cer
https://nces.by/wp-content/uploads/certificates/pki/cas_ruc3.cer
2. Скачать файлы СОС служб атрибутных сертификатов по ссылкам:
https://nces.by/wp-content/uploads/certificates/pki/cas_ruc2.crl
https://nces.by/wp-content/uploads/certificates/pki/cas_ruc3.crl
3. Запустить «Персональный менеджер сертификатов Авест для ГосСУОК (Bign)» с авторизацией или без авторизации.
4. В менеджере выбрать пункт меню «Файл» – «Импорт сертификата/СОС» (см. *Рисунок 25 Импорт сертификата*), указать путь к файлу сертификата службы атрибутных сертификатов cas_ruc2.cer и проимпортировать его, следуя указаниям мастера импорта сертификатов. Затем аналогично проимпортировать cas_ruc3.cer, cas_ruc2.crl, cas_ruc3.crl.

Также сертификат и СОС службы атрибутных сертификатов можно проимпортировать с помощью пункта «Сервис» – «Обновление СОС и сертификатов УЦ» в меню программы «Персональный менеджер сертификатов Авест для ГосСУОК (Bign)», как это описано в пункте 1 Приложение 2. Способы получения/обновления списков отозванных сертификатов.

5. Перечень сокращений

ГосСУОК – Государственная система управления открытыми ключами;

ОС – операционная система;

ПО – программное обеспечение;

СОС – список отозванных сертификатов;

УЦ – удостоверяющий центр;

ЭСЧФ – электронный счет-фактура.