Инструкция по установке комплекта абонента с сертификатом ГосСУОК с помощью объединённого инсталлятора AvPKISetup2

Содержание

Системные требования

Криптопровайдер AvCSP предназначен для работы на ПЭВМ (ЭВМ), функционирующей под управлением одной из следующих ОС MS Windows:

- Windows 2003 Server (x32, x64) SP2 с установленным обновлением KB2836198
- Windows XP SP3 (x32) с установленным обновлением KB2836198
- Windows 7 (x32, x64)
- Windows 8 (x32, x64)
- Windows 8.1 (x32, x64)
- Windows 2008 R1 Server (x32, x64)
- Windows 2008 R2 Server (x64)
- Windows 2012 Server (x64)
- Windows 2012 R2 Server (x64)
- Windows 2016 Server (x64)
- Windows 10 (build 10240, 10586, 14393, 15063) (x32, x64).

Внимание! Для корректной работы криптопровайдера на операционных системах Windows XP, Windows Server 2003 необходимо перед установкой программного обеспечения установить обновление **KB2836198**, соответствующее разрядности и языку ОС.

Требуется наличие Microsoft Internet Explorer 6.0 или выше.

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

Файлы, содержащие личный ключ подписи/шифрования, а также другие необходимые параметры, должны находиться на электронных устройствах 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 на компьютер, на котором уже присутствует более ранняя его версия

В случае наличия на компьютере более ранней версии криптографического программного обеспечения необходимо осуществить его удаление.

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 Avest PKI следует нажать кнопку «Далее» (Рисунок 1).

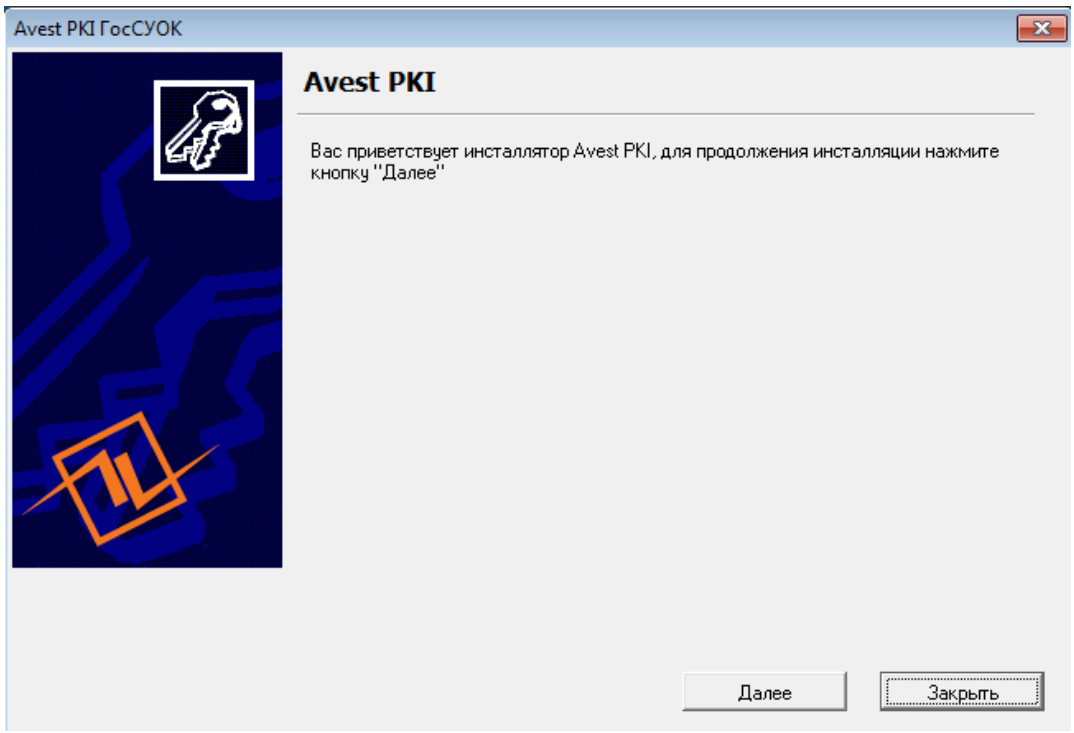

Рисунок 1 − Окно мастера установки Avest PKI

В следующем окне следует выбрать режим «Удаление» и нажать кнопку «Далее» (Рисунок 2).

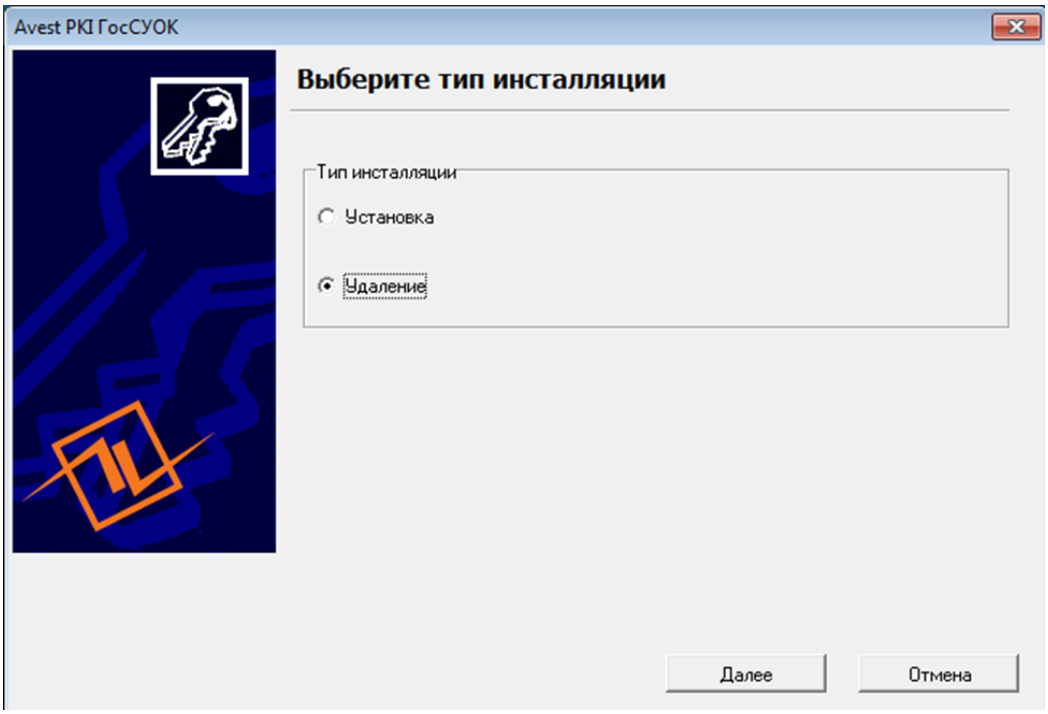

Рисунок 2 − Выбор типа инсталляции

Далее программа выведет список удаляемых компонентов, нажмите кнопку «Далее» (Рисунок 3).

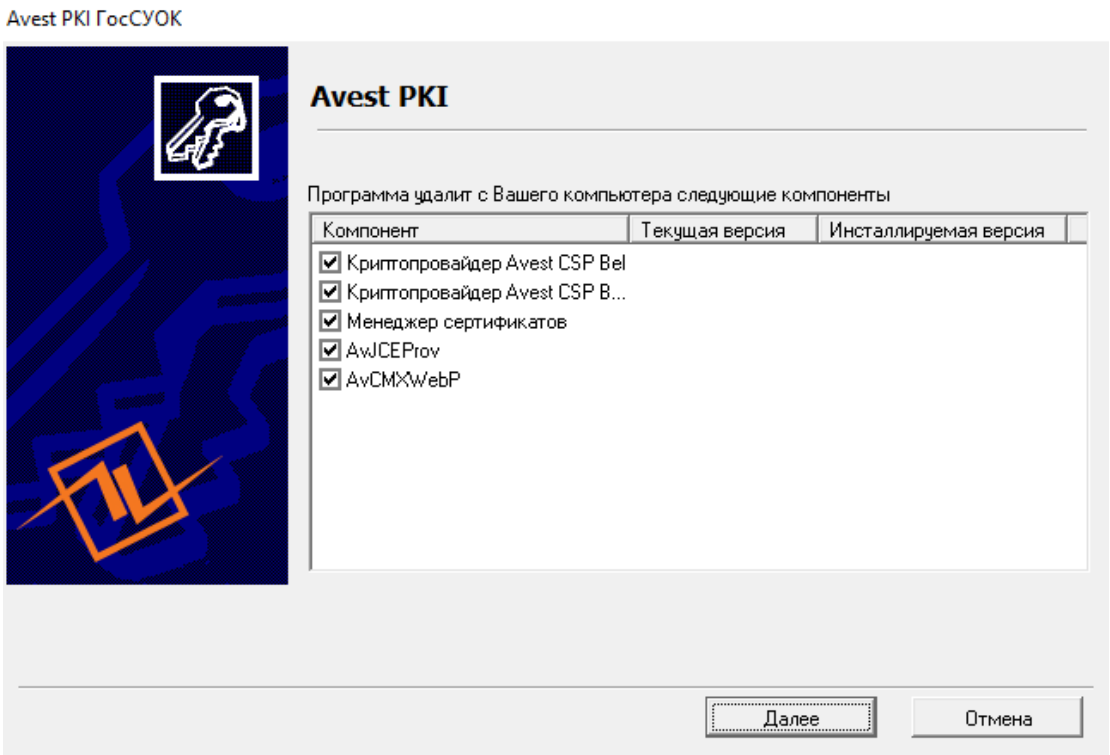

Рисунок 3 − Список удаляемых компонентов

В следующем окне отображается результат работы мастера установки «AvPKISetup». В столбце «Компонент» отображается, что именно было удалено; в столбце «Состояние» – статус удаления компонентов (Рисунок 4).

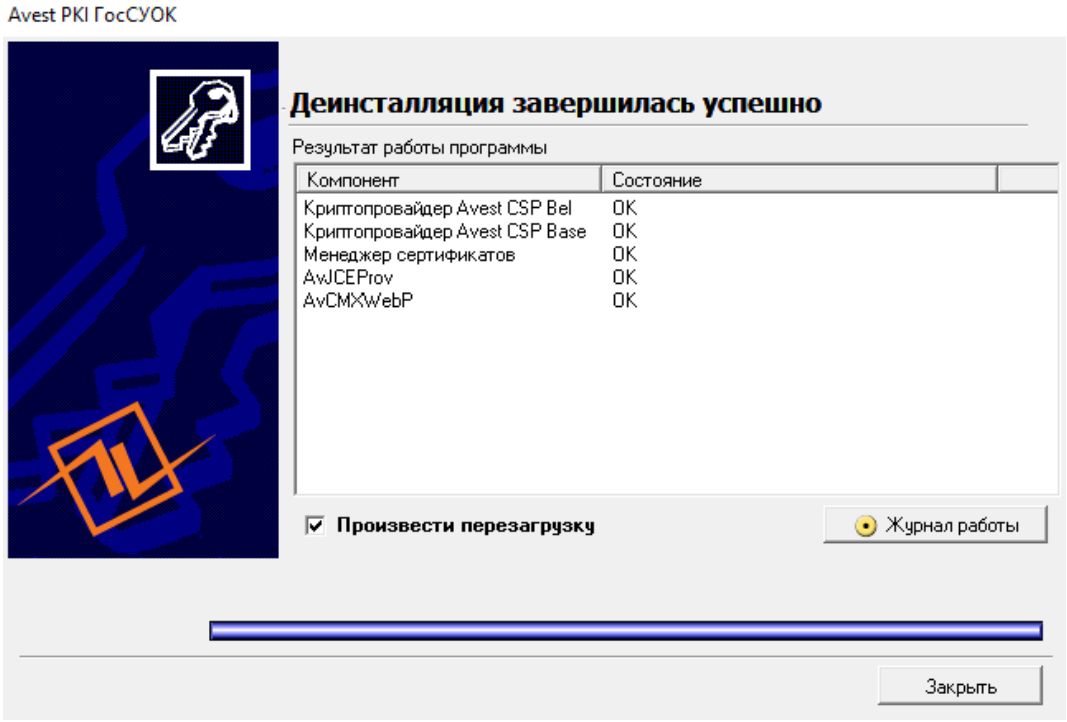

Рисунок 4 − Результат работы программы

В этом же окне возможно отказаться от перезагрузки путем снятия галочки. Если отметка о перезагрузке была снята, появится окно с предупреждением о необходимости перезагрузки (Рисунок 5).

Внимание! Для дальнейшей корректной установки Комплекта абонента рекомендуется перегрузить компьютер.

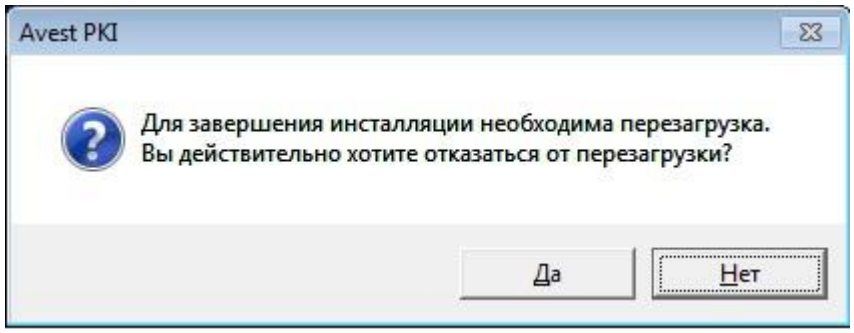

Рисунок 5 − Предупреждение о необходимости перезагрузки

После перезагрузки компьютера необходимо произвести **установку** Комплекта абонента, как описано в разделе **«Первичная установка Комплекта абонента на компьютер».**

Первичная установка Комплекта абонента на компьютер

Комплект абонента AvUCK совместно с сертификатом, сконфигурированный для установки с помощью AvPKISetup, передается пользователям на диске, флеш-носителе, через Облачное хранилище сертификатов или иным способом (порядок определяется Республиканским удостоверяющим центром, выдающим ПО).

Каждое окно объединенного инсталлятора AvPKISetup 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 (Рисунок 6).

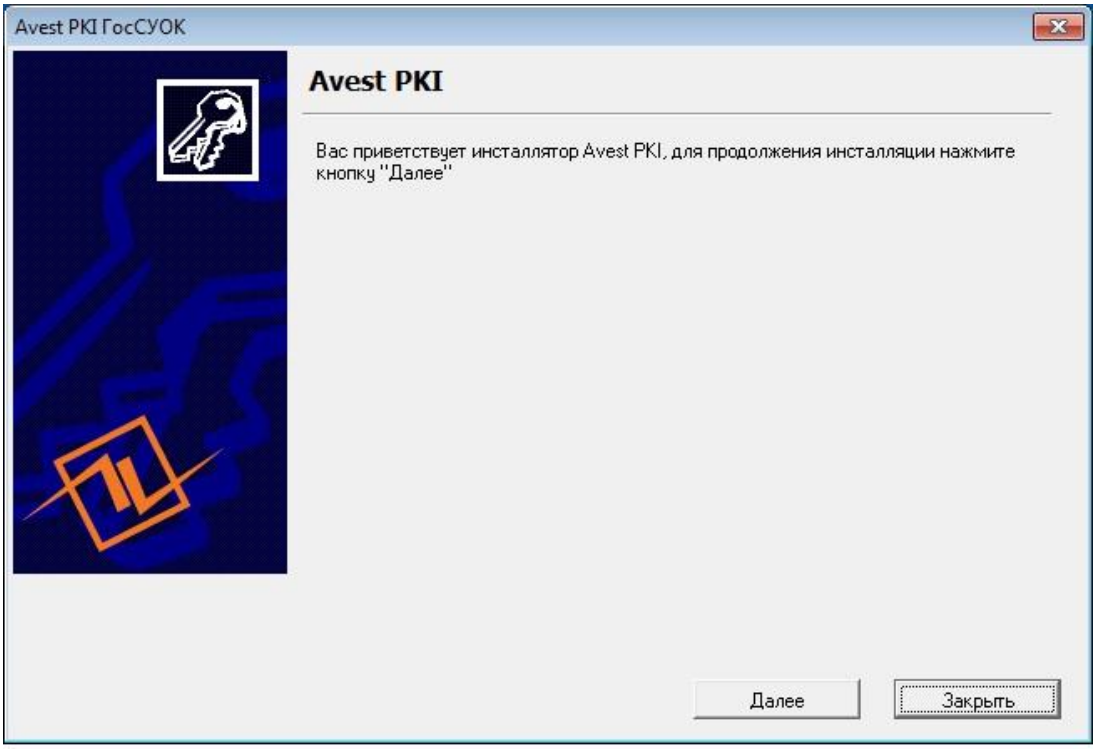

Рисунок 6 − Окно мастера установки Avest PKI

В появившемся окне представлен список устанавливаемых на компьютер компонентов, отмеченный флажками. В колонке «**Инсталлируемая версия**» отображается версия устанавливаемого криптопровайдера Avest CSP Bel, Персонального менеджера сертификатов, AvJCEProv, плагина AvCMXWebP и иных компонентов (Рисунок 7).

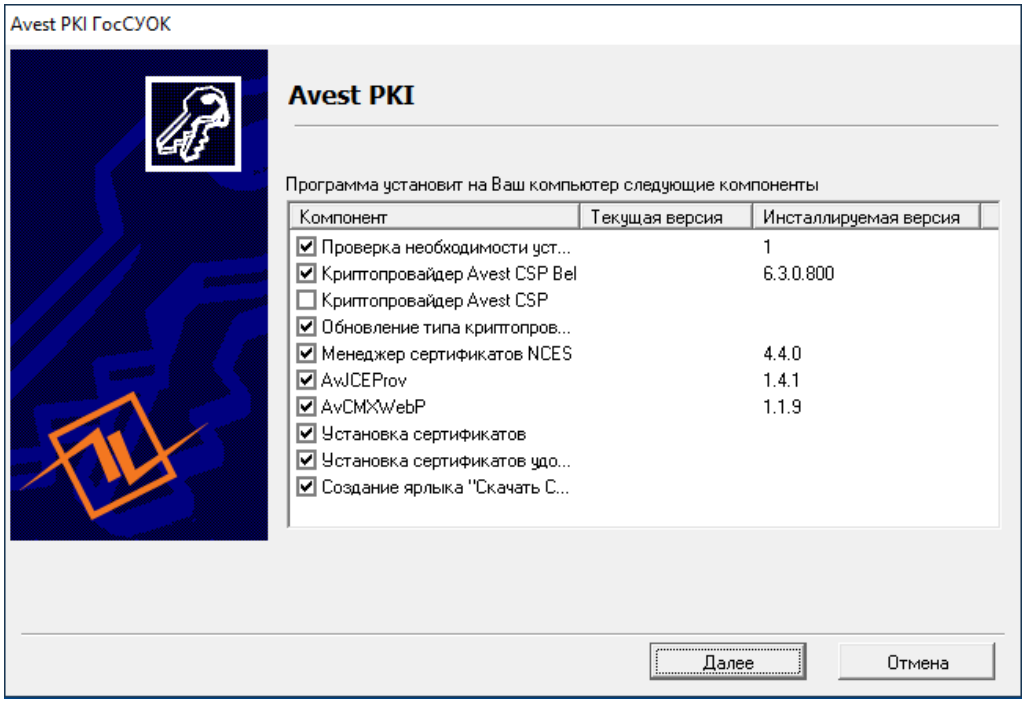

Рисунок 7 − Выбор компонентов

Следующий шаг мастера установки – сбор случайных данных. Для их сбора необходимо подвигать мышью в окне установки, пока индикатор сбора случайных данных не достигнет отметки **100%** (Рисунок 8).

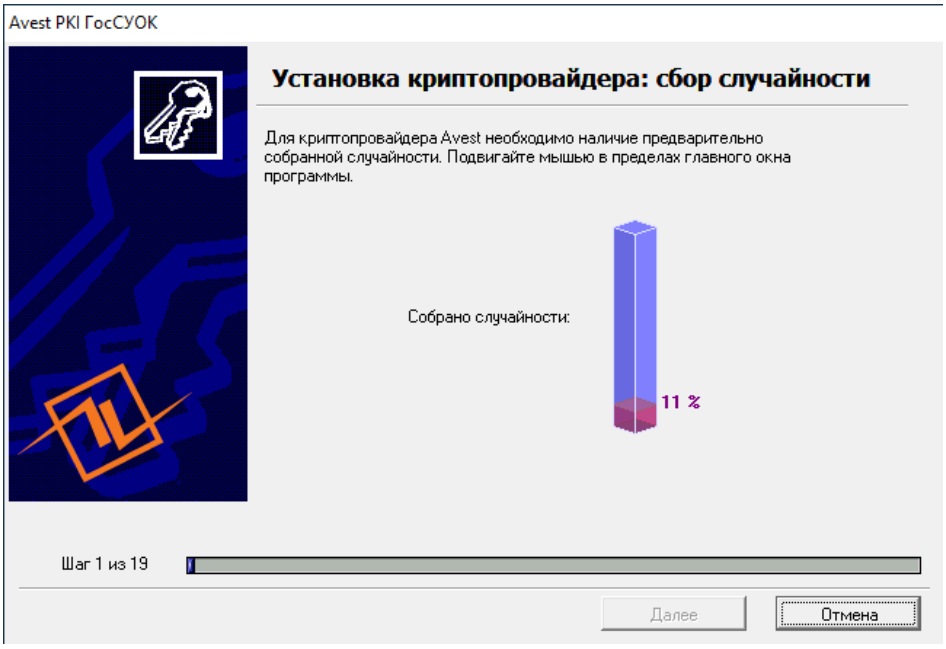

Рисунок 8 − Сбор случайности

После шага «Установка криптопровайдера: сбор случайности» требуется перезагрузка компьютера. В окне о необходимости произвести перезагрузку компьютера нажать «ОК» (Рисунок 9).

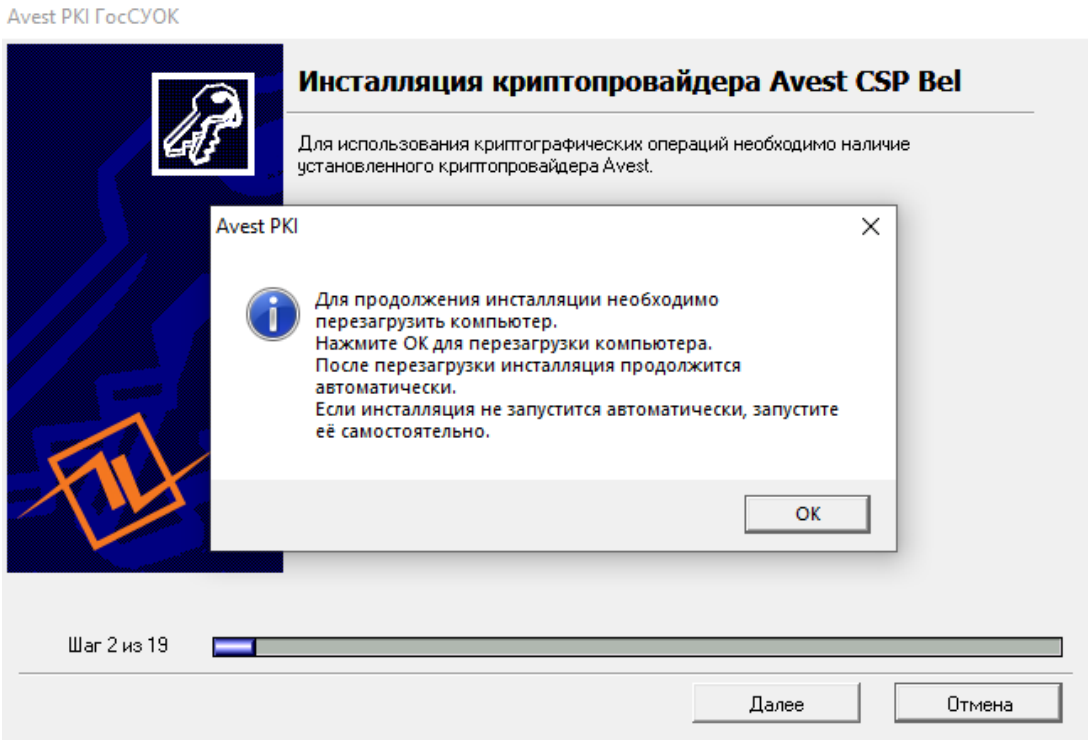

Рисунок 9 − Необходимость перезагрузки компьютера

Если по каким-то причинам AvPKISetup после **перезагрузки не запустится сам**, то его необходимо запустить вручную, открыв появившийся на рабочем столе **ярлык «Продолжение установки AvPKISetup»,** как это показано на Рисунке 10 (ярлык после успешной установки удалится с рабочего стола самостоятельно).

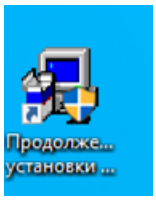

Рисунок 10 − Ярлык «Продолжение установки AvPKISetup»

Далее произойдет установка:

- ✓ криптопровайдера Avest CSP Bel,
- ✓ обновление криптопровайдера Avest CSP,
- ✓ веб плагина AvCMXWebP,
- ✓ программного комплекса AvJCEProv,
- ✓ персонального менеджера сертификатов AvPCM,
- ✓ импорт сертификата в Личный справочник,
- ✓ импорт атрибутного сертификата в формате *.p7b

Замечание: особенности установки атрибутного сертификата **формата *.acr** описаны в **Приложении 1**,

- ✓ установка доверия сертификатам Корневых удостоверяющих центров.

На шаге «Установка сертификатов» открывается окно Мастера импорта и происходит установка сертификатов в **системные справочники Windows** (см. Рисунок 11).

Внимание! Галочками отмечены сертификаты, которые **будут проимпортированы** и которые **отсутствуют** в системном справочнике. У каждого пользователя сертификаты, отмеченные галочками в поле «Импортируемые объекты», могут отличаться.

Рекомендация: обратите внимание на дату действия личного сертификата. Это поможет избежать ошибок на этапе выбора контейнера (Рисунок 13).

Оставьте галочки по умолчанию, как предлагает Мастер импорта, нажмите кнопку «Далее».

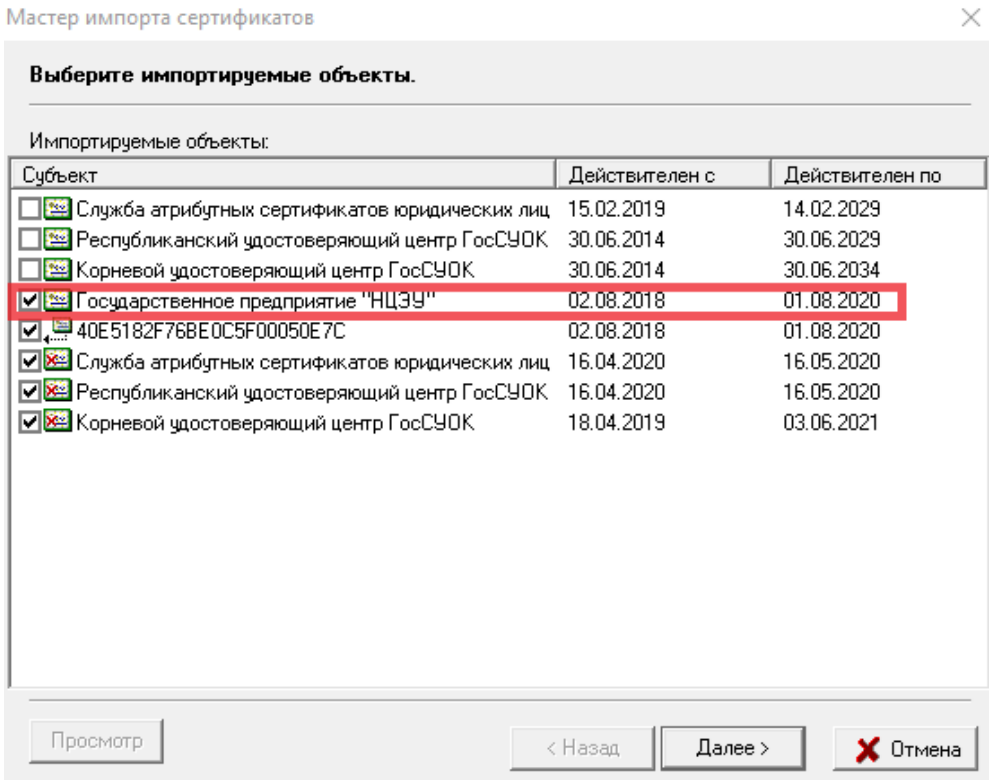

Рисунок 11 – Импортируемые сертификаты

Мастер импорта уведомит о количестве импортированных сертификатов (Рисунок 12).

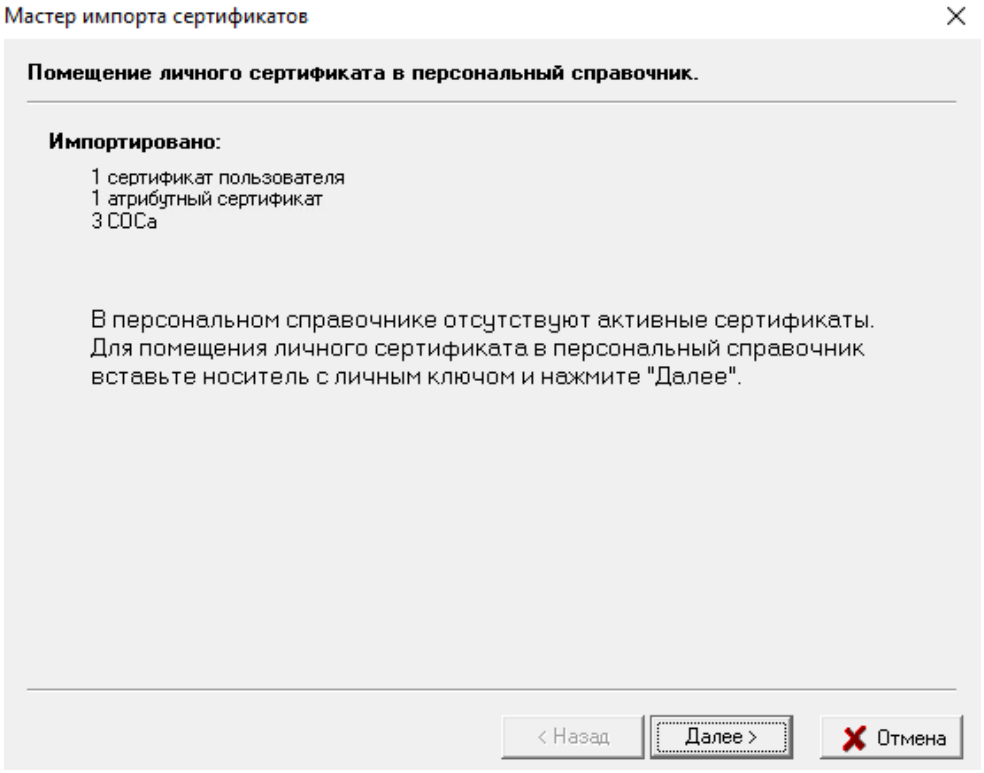

Рисунок 12 − Уведомление о количестве импортируемых сертификатов

Для установки личного сертификата необходимо вставить в USB-разъем компьютера носитель **AvPass (AvToken)**, на котором записан личный ключ, и нажать кнопку «Далее».

Внимание! Из компьютера необходимо извлечь все ключи от иных инфраструктур (ключи систем (севисов) банка и т.д.).

В окне выбора контейнера отобразятся все контейнеры с личными ключами, записанные на носителе **AvPass (AvToken)**. Если на носителе записано более одного контейнера, то в списке необходимо выбрать тот, который соответствует Вашему личному сертификату (контейнер с наименованием юридического лица, ИП или ФИО физического лица). Определить это можно, например, по дате регистрации в Регистрационном центре (Рисунок 13).

Обязательно необходимо установить галочку на пункте «Поместить личный сертификат в контейнер».

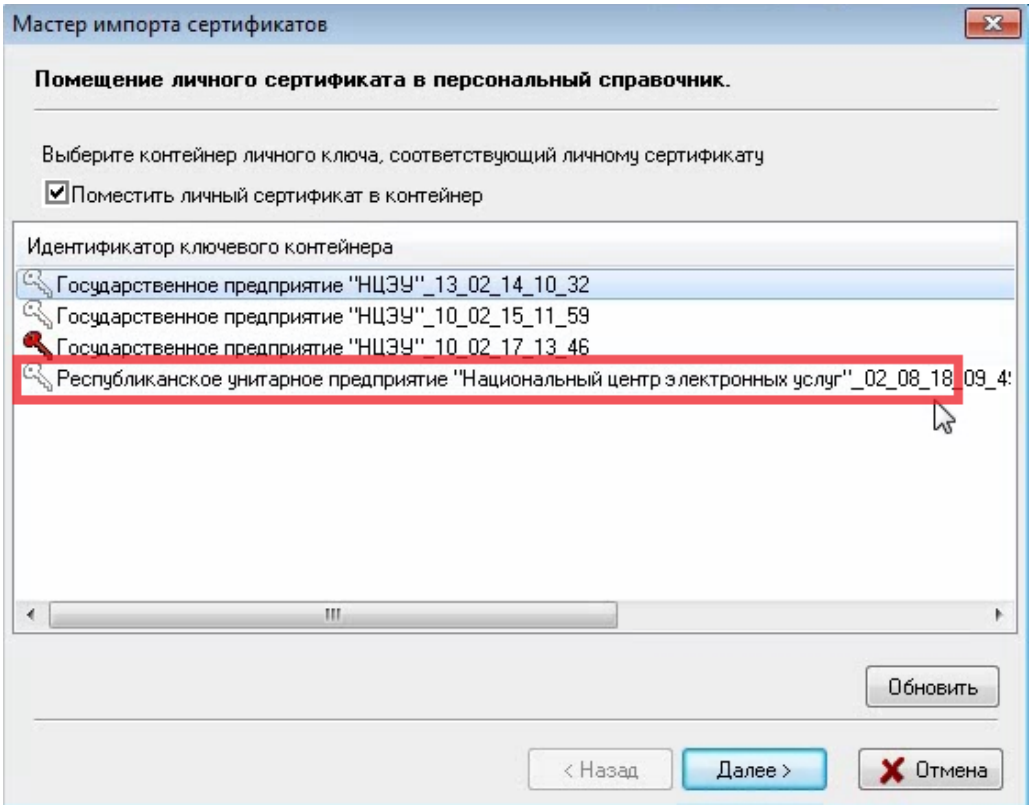

Рисунок 13 − Выбор контейнера

После того, как соответствующий контейнер выбран, необходимо нажать на кнопку «Далее».

В появившемся окне криптопровайдера необходимо ввести пароль, который был задан при создании личных ключей, и нажать кнопку «ОК» (Рисунок 14).

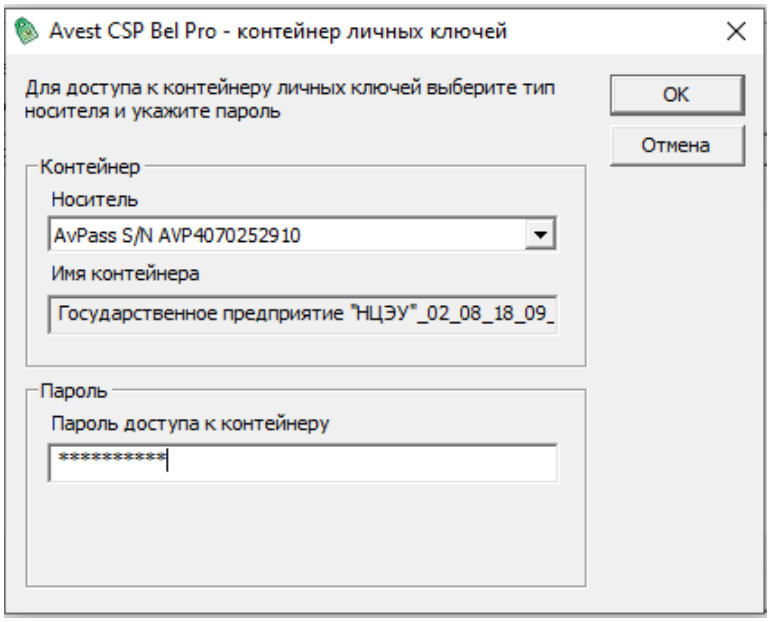

Рисунок 14 − Пароль доступа к контейнеру

На следующем шаге будет установлено доверие сертификатам Корневых удостоверяющих центров (Рисунок 15).

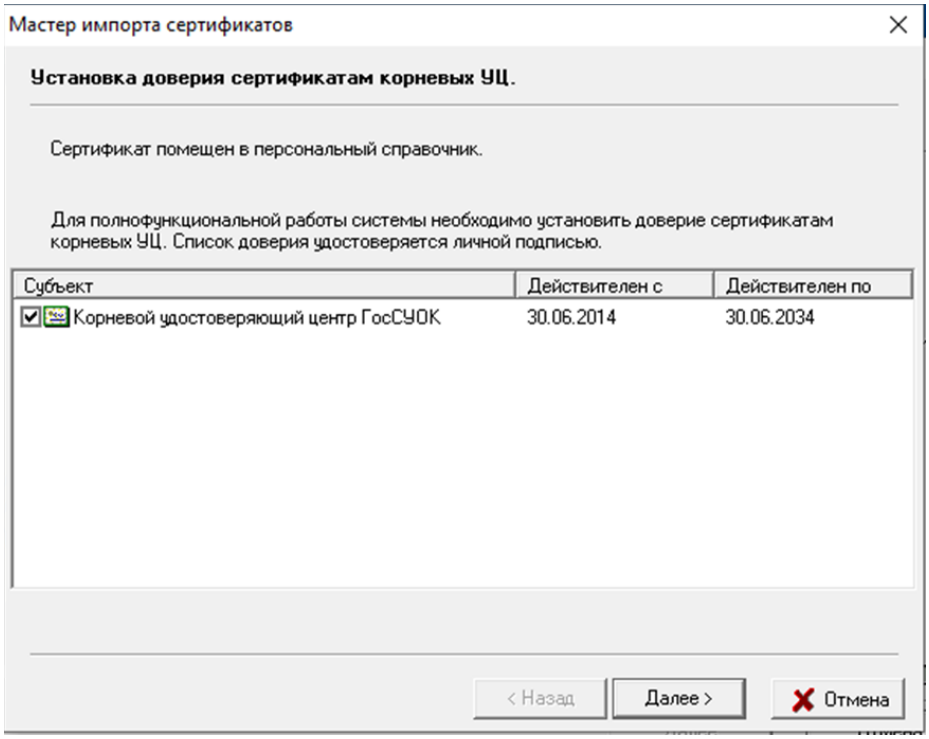

Рисунок 15 − Сертификаты корневых удостоверяющих центров

Перед установкой сертификатов корневых удостоверяющих центров на экране возникает «Предупреждение системы безопасности» Windows о добавлении сертификата в список доверенных УЦ, нажмите кнопку «Да» (Рисунок 16).

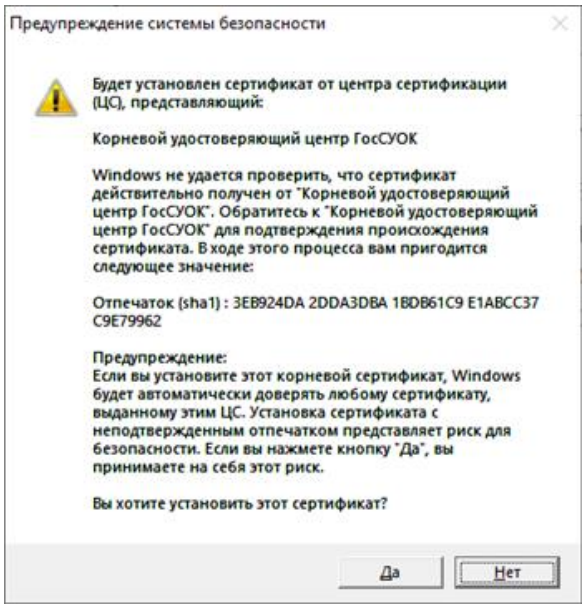

Рисунок 16 − Предупреждение системы безопасности

На следующем шаге Мастер импорта уведомит о сертификатах, которым было установлено доверие. Нажмите кнопку «Закрыть». (Рисунок 17).

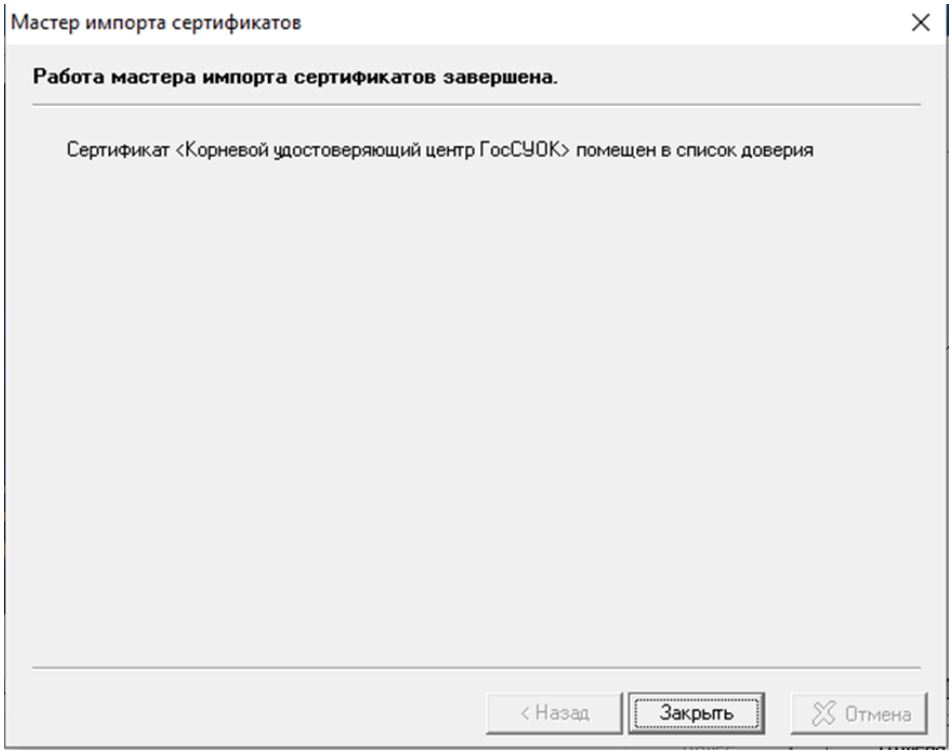

Рисунок 17 − Завершение работы мастера импорта сертификатов

После завершения процесса установки комплекта абонента с сертификатом ГосСУОК с помощью объединённого инсталлятора AvPKISetup2 нажмите «Закрыть» (Рисунок 18).

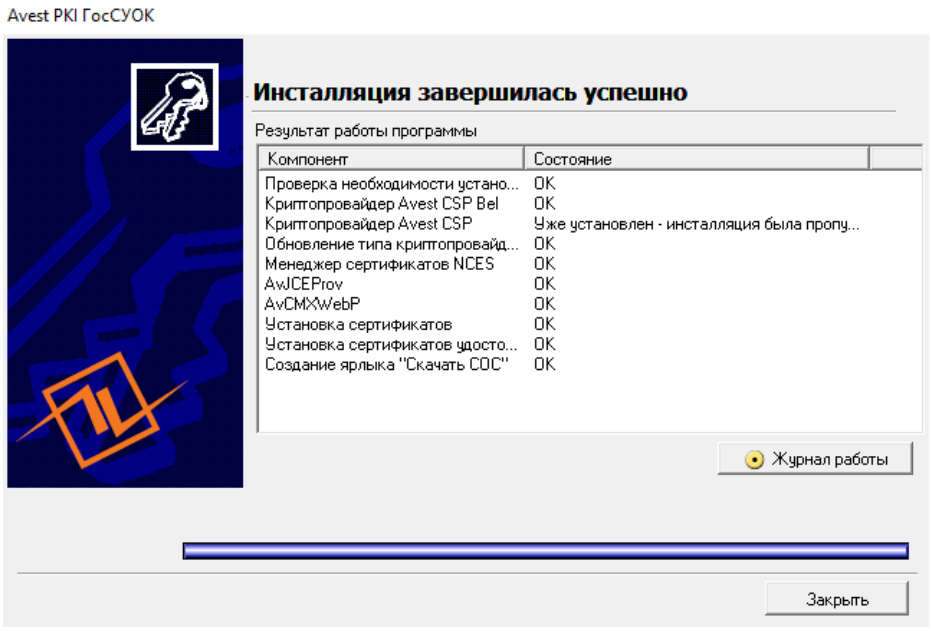

Рисунок 18 − Результат работы программы

Приложение 1. Особенности установки атрибутного сертификата формата *.acr

В разделе **«Первичная установка Комплекта абонента на компьютер»** описан процесс установки Комплекта абонента с атрибутным сертификатом формата *.p7b. В случае, если на диск, флеш-носитель, Облачное хранилище сертификатов записан атрибутный сертификат формата *.acr, атрибутный сертификат в процессе установки Комплекта абонента **не будет установлен** в Персональный менеджер сертификатов Авест для ГосСУОК. Для того, чтобы его установить, необходимо после установки в соответствии с инструкцией Комплекта абонента, проимпортировать атрибутный сертификат вручную.

Инструкция по установке базового атрибутного сертификата в формате «*.acr»

Для установки атрибутного сертификата (далее – АС) необходимо:

1) запустить Персональный менеджер сертификатов Авест для ГосСУОК, установленный ранее;

2) выбрать сертификат открытого ключа для авторизации и нажать кнопку «ОК» (Рисунок 1);

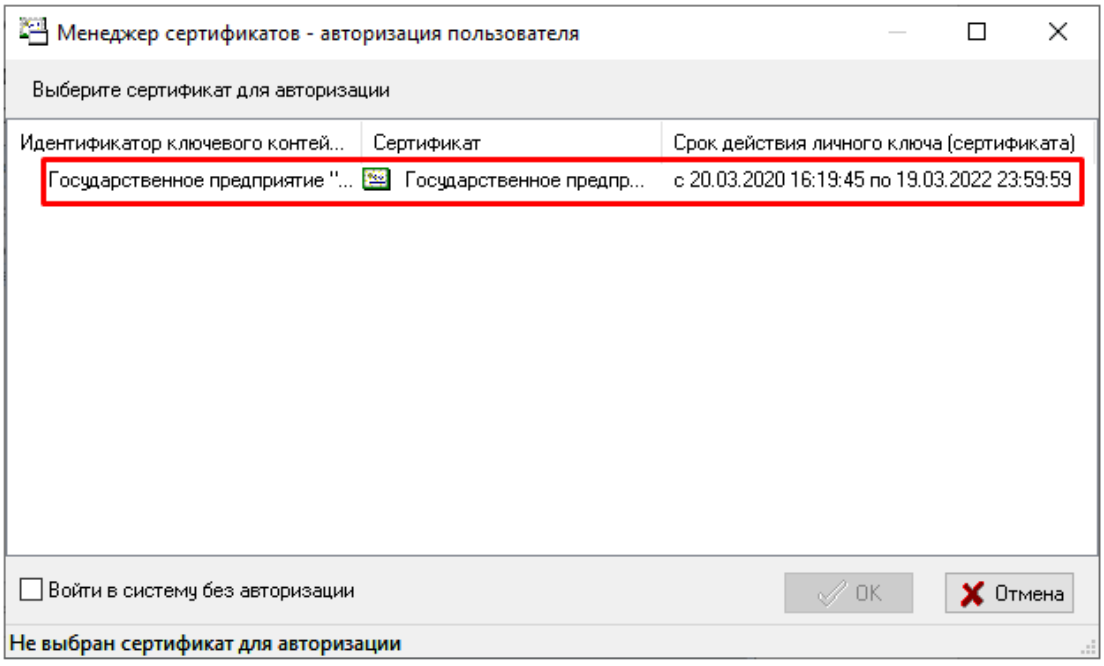

Рисунок 1 – Окно выбора сертификата

3) ввести пароль к личному ключу (пароль доступа к контейнеру) и нажать кнопку «ОК» (Рисунок 2);

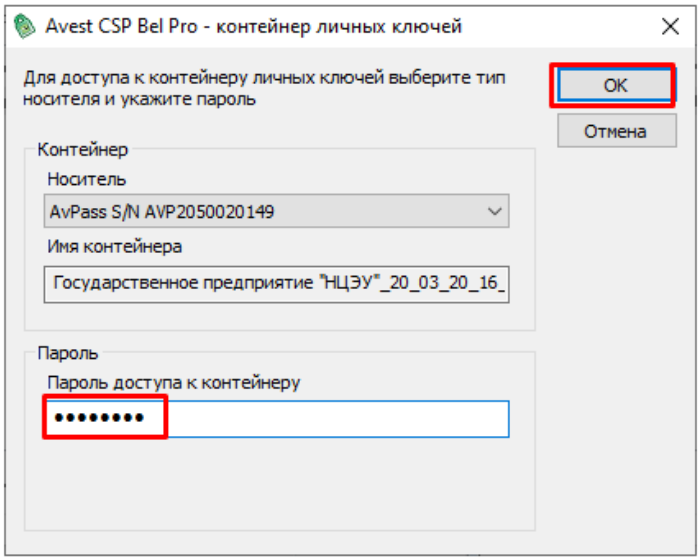

Рисунок 2 – Окно ввода пароля для доступа к контейнеру

4) В открывшемся Персональном менеджере сертификатов Авест для ГосСУОК провести процедуру импорта АС:

- выбрать меню «Файл» → «Импорт сертификата/СОС» (Рисунок 3);

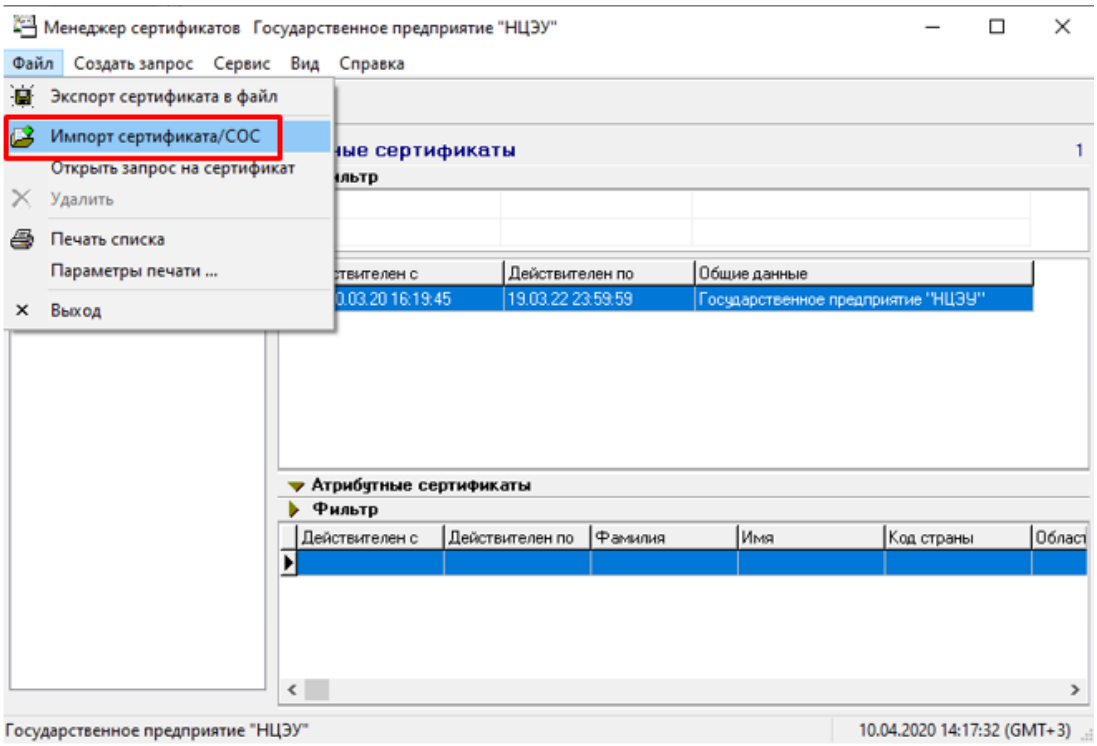

Рисунок 3 – Меню «Файл» менеджера сертификатов

- выбрать импортируемый файл и нажать кнопку «Далее» (Рисунок 4);

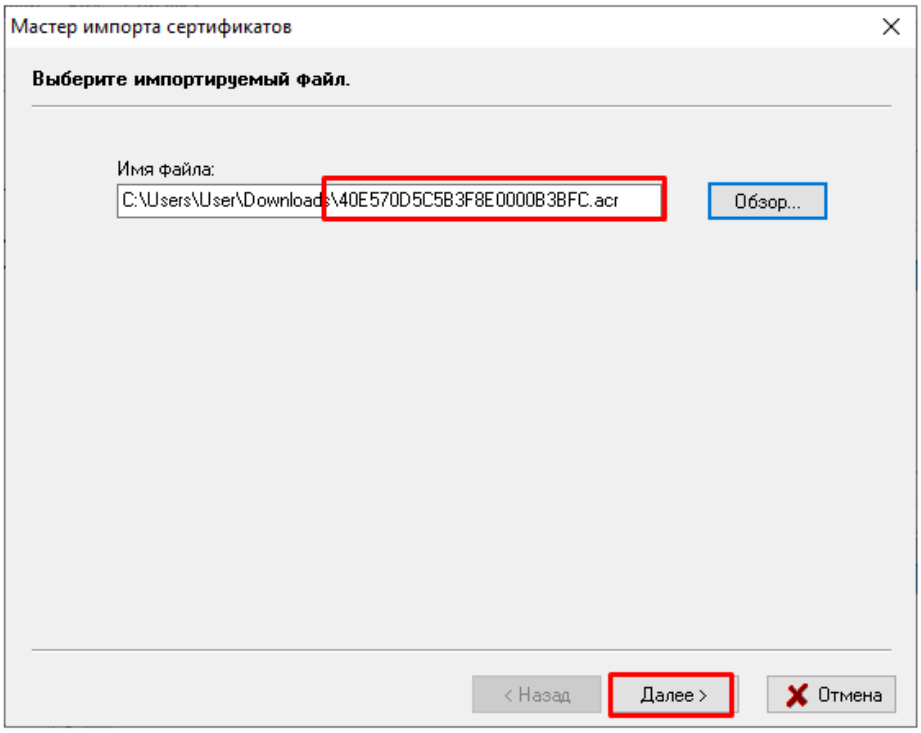

Рисунок 4 – Окно выбора импортируемого файла

- в открывшемся окне нажать кнопку «Далее» (Рисунок 5);

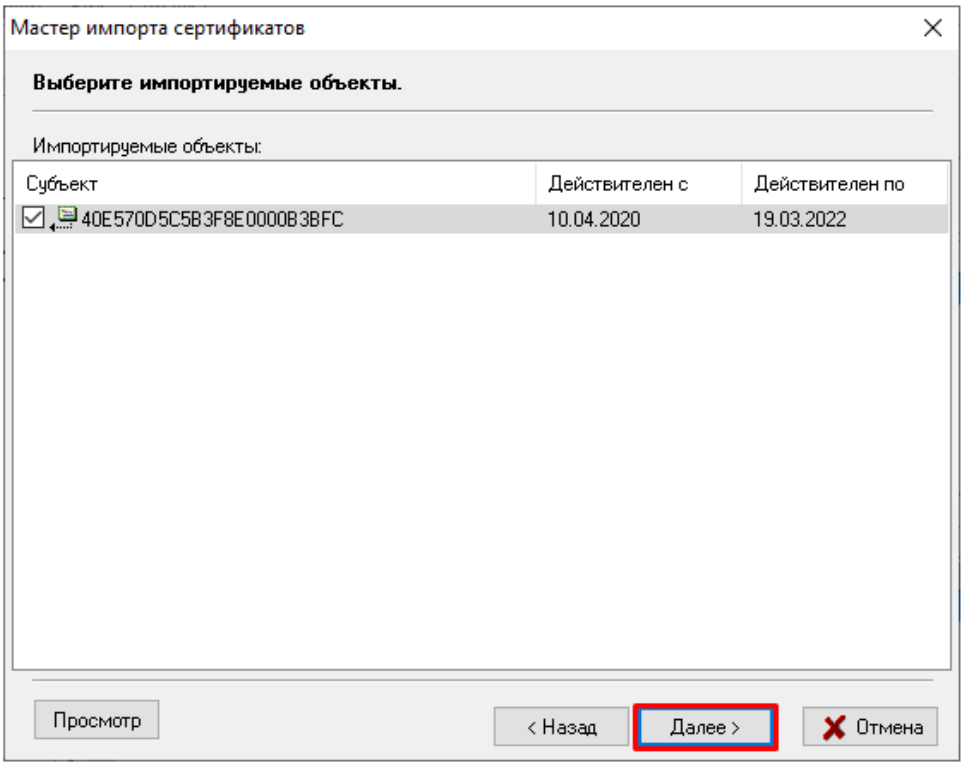

Рисунок 5 – Окно импортируемых объектов

Процесс завершения процедуры импорта АС отражается в отчете работы мастера импорта сертификатов (пример отчета на скриншоте ниже) и нажать кнопку «ОК» (Рисунок 6):

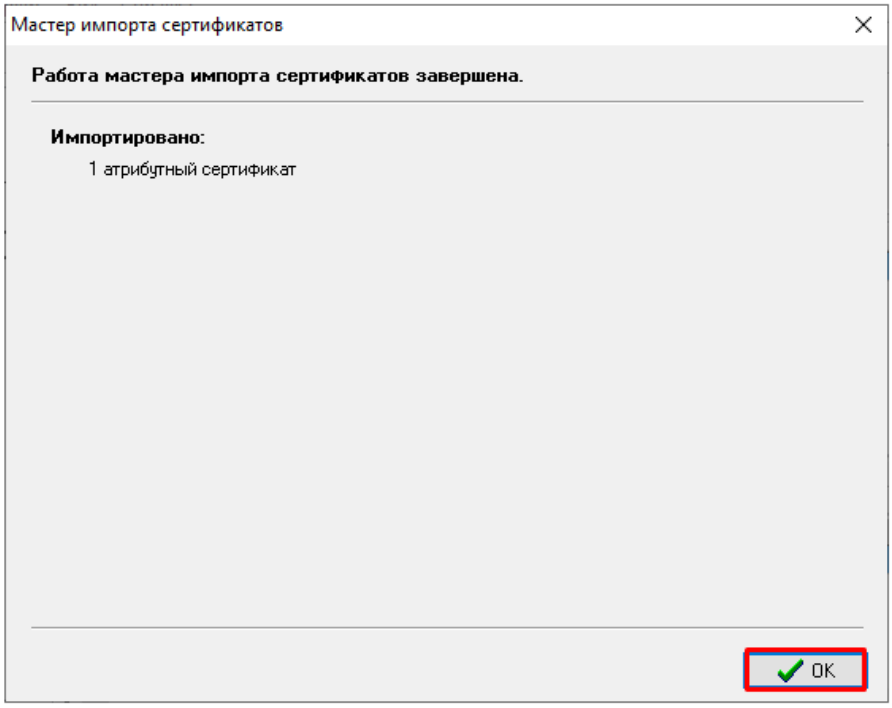

Рисунок 6 – Отчет мастера импорта сертификатов

Проимпортированный АС находится в Персональном менеджере сертификатов Авест для ГосСУОК (Рисунок 7):

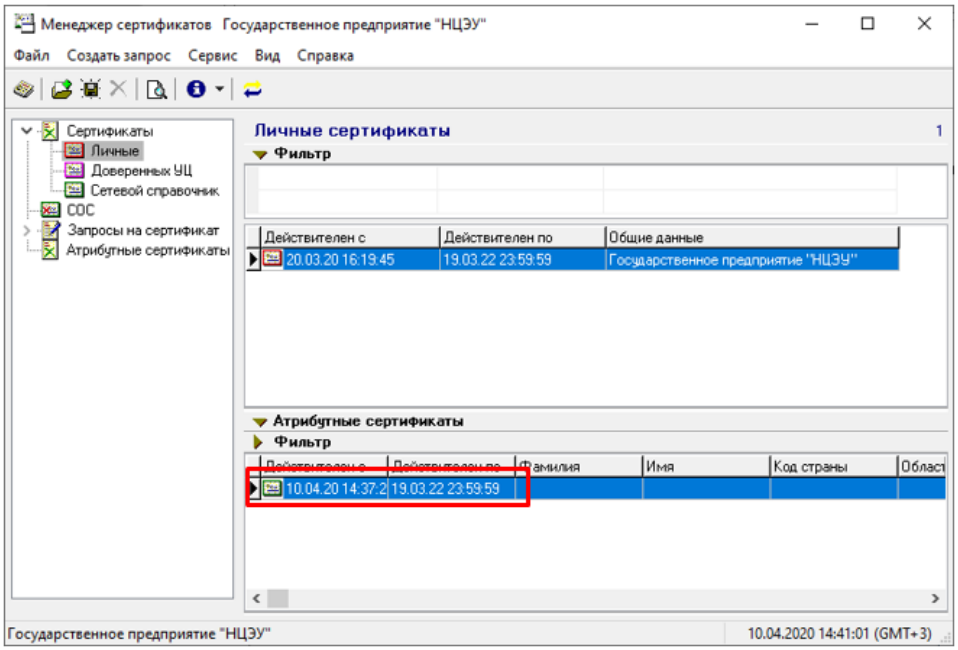

Рисунок 7 – Окно менеджера сертификатов

Приложение 2. Особенности работы атрибутного сертификата (в том числе в формате *.acr) для работы с системами ФСЗН

Для работы с системами ФСЗН кроме импорта атрибутного сертификата ФСЗН (см. Приложение 1) необходимо проимпортировать/ обновить списки отозванных сертификатов (далее – СОС) службы атрибутных сертификатов.

Для этого:

1. Скачайте сертификат службы атрибутных сертификатов юридического лица и список отозванных сертификатов для центра атрибутных сертификатов РУЦ на компьютер.

2. Запустите Персональный менеджер сертификатов Авест для ГосСУОК, для этого нажмите «Пуск» → «Все программы» → «Авест для НЦЭУ» → «Персональный менеджер сертификатов Авест для ГосСУОК» → выберите Ваш личный сертификат, авторизуйтесь → Введите пароль → нажмите «ОК».

3. Проимпортируйте скачанные сертификаты. Выберите в меню сверху «Файл» → «Импорт сертификатов/СОС» → «Обзор…» – укажите путь к скачанному файлу **atrib-cert-ul.cer** и проимпортируйте его, следуя указаниям (везде «Далее»). Далее таким же образом проимпортируйте файл **cas_ruc.crl**.

4. В Персональном менеджере сертификатов Авест для ГосСУОК выберите вкладку «Атрибутные сертификаты», дважды нажмите на Ваш атрибутный сертификат. В поле «Сведения о атрибутном сертификате» должна содержаться информация «Сертификат действителен».