2021 г.

Установка программного обеспечения в режиме ограниченных прав

Оглавление

Сведения об учётной записи

Учётная запись — хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.

Перед установкой программного обеспечения необходимо определить следующее:

- входит ли компьютер в домен
- тип учетной записи (администратор/пользователь)

Как определить, входит ли компьютер в домен?

1. Откройте компонент «Система», нажав кнопку «Пуск» и выбрав пункты «Панель управления» → «Система и безопасность» → «Система» или кликнув правой клавишей мыши по ярлыку «Мой компьютер», выберите «Свойства».
2. В разделе «Имя компьютера, имя домена и параметры рабочей группы» будет соответствующая надпись «Рабочая группа» или «Домен», после чего будет следовать имя (См. Рисунок 1 Определение домена).

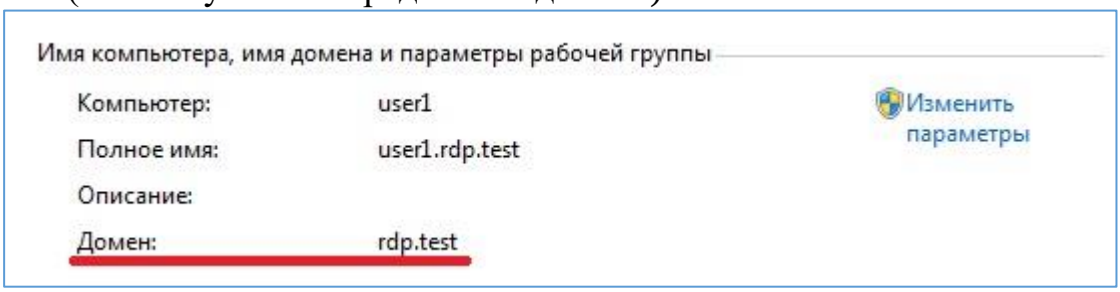

Рисунок 1 Определение домена

Как определить тип учетной записи?

Нужно зайти в «Панель управления» → «Учетные записи пользователей» → «Управление учетными записями пользователей». Откроется окно с основными учетными записями (См. Рисунок 2 Тип учетной записи).

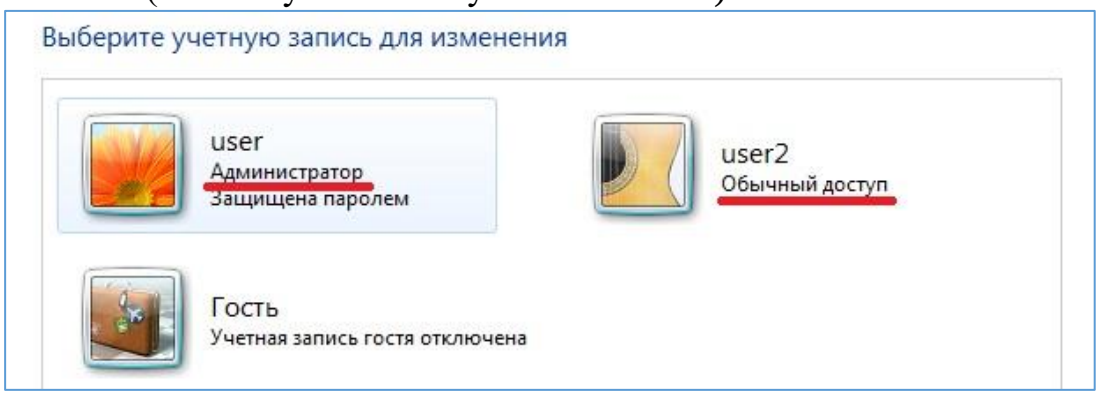

Рисунок 2 Тип учетной записи

Установка ПО

Компьютер входит в домен

Если *компьютер входит в домен*, то возможность изменения его параметров пользователем, скорее всего, будет ограничена. Установка программного обеспечения производится администратором домена, согласно документу «Инструкция по обновлению». При установке ПО с правами администратора домена импорт сертификата в личный справочник проводить не нужно.

После того, как все программы из комплекта AvPKISetup установлены, нужно войти под учетной записью пользователя и проимпортировать личный сертификат вручную, средствами менеджера (см. Приложение 1.2 Импорт сертификатов средствами персонального менеджера) и установить доверие сертификатам корневых удостоверяющих центров (см. Приложение 1.3 Установка сертификатов корневых удостоверяющих центров в домене.).

Компьютер не входит в домен

Если *компьютер не входит в домен* и учетная запись с правами «**Пользователь**» (обычный доступ), установка программного обеспечения производится под учетной записью администратора, согласно документу «Инструкция по обновлению». При установке ПО с правами администратора импорт сертификата в личный справочник проводить не нужно.

Далее необходимо осуществить вход под учетной записью пользователя и произвести импорт сертификата, а также установку сертификатов корневых удостоверяющих центров. (см. Приложение 1.1 Импорт сертификата с помощью AvPKISetup)

Если *компьютер не входит в домен* и учетная запись с правами «**Администратор**», то просто следуйте инструкциям по установке из документа «Инструкция по обновлению».

Приложение 1.1 Импорт сертификата с помощью AvPKISetup

Для импорта сертификатов необходимо войти под учетной записью пользователя и запустить файл AvPKISetup2.exe. На шаге, где программа предлагает выбрать компоненты для установки, оставить галочку в пункте «Установка сертификатов» и нажать «Далее». (См. Рисунок 3 Выбор компонентов)

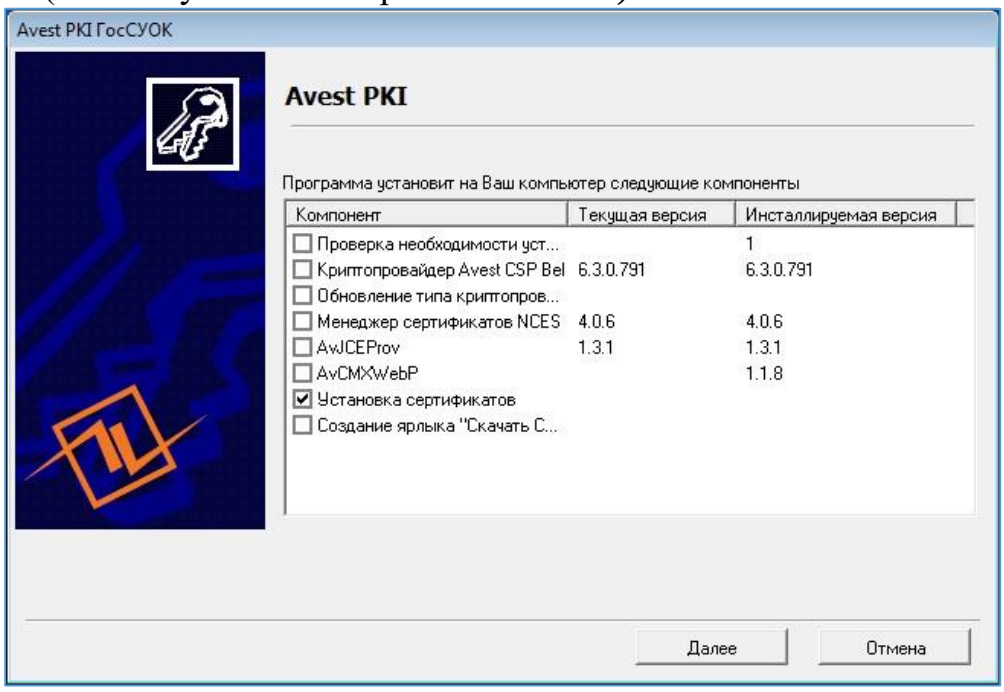

Рисунок 3 Выбор компонентов

На шаге «Установка сертификатов» открывается окно Мастера импорта и происходит установка сертификатов в системные справочники Windows. 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 (см. Рисунок 4 Импортируемые сертификаты).

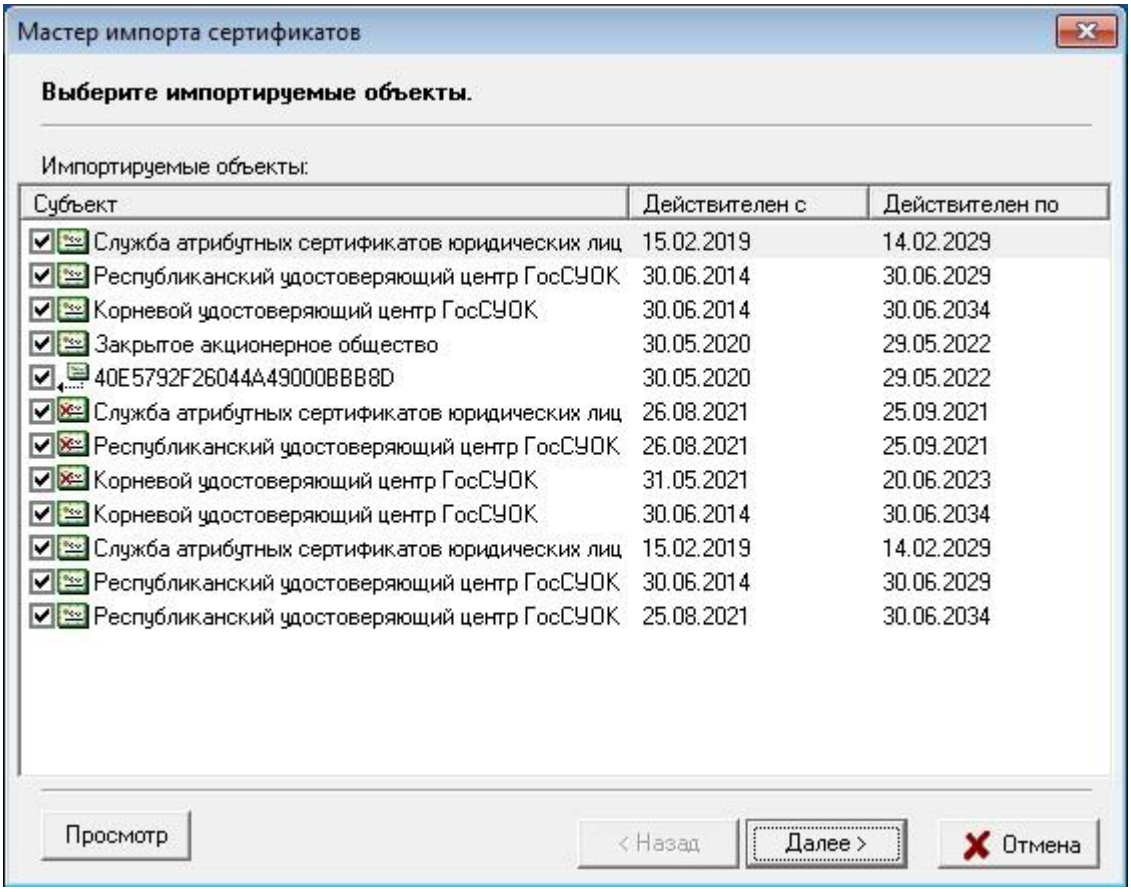

Рисунок 4 Импортируемые сертификаты

Мастер импорта уведомит о количестве импортированных сертификатов (см. Рисунок 5 Уведомление о количестве импортируемых сертификатов).

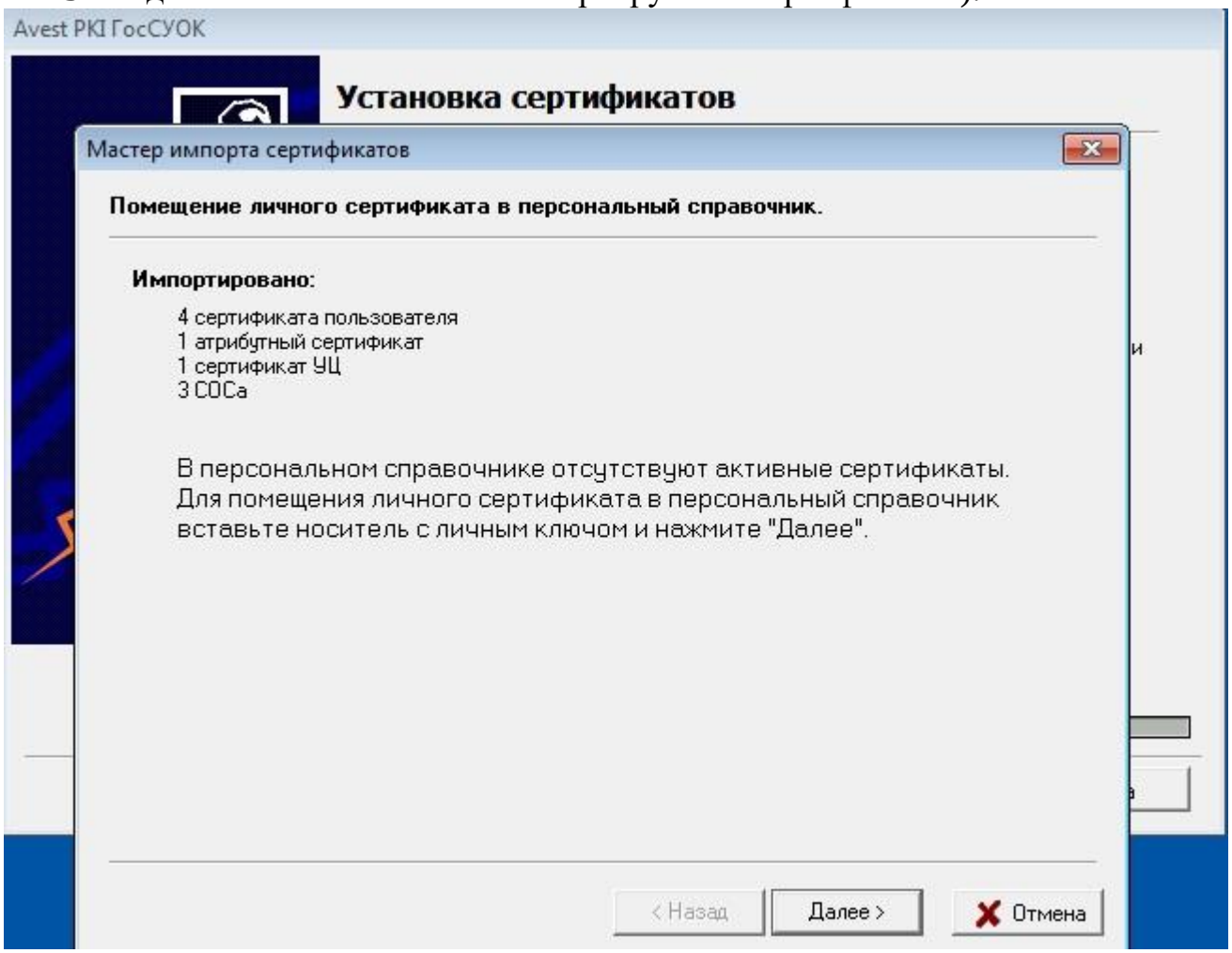

Рисунок 5 Уведомление о количестве импортируемых сертификатов

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 6 Выбор контейнера).

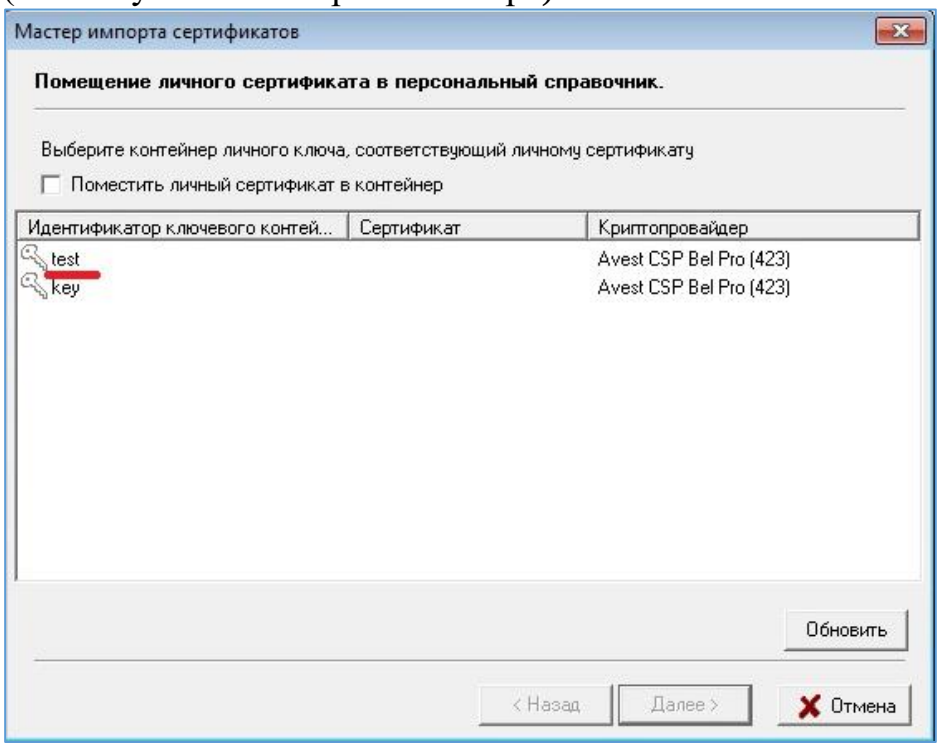

Рисунок 6 Выбор контейнера

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 7 Сертификаты корневых удостоверяющих центров).

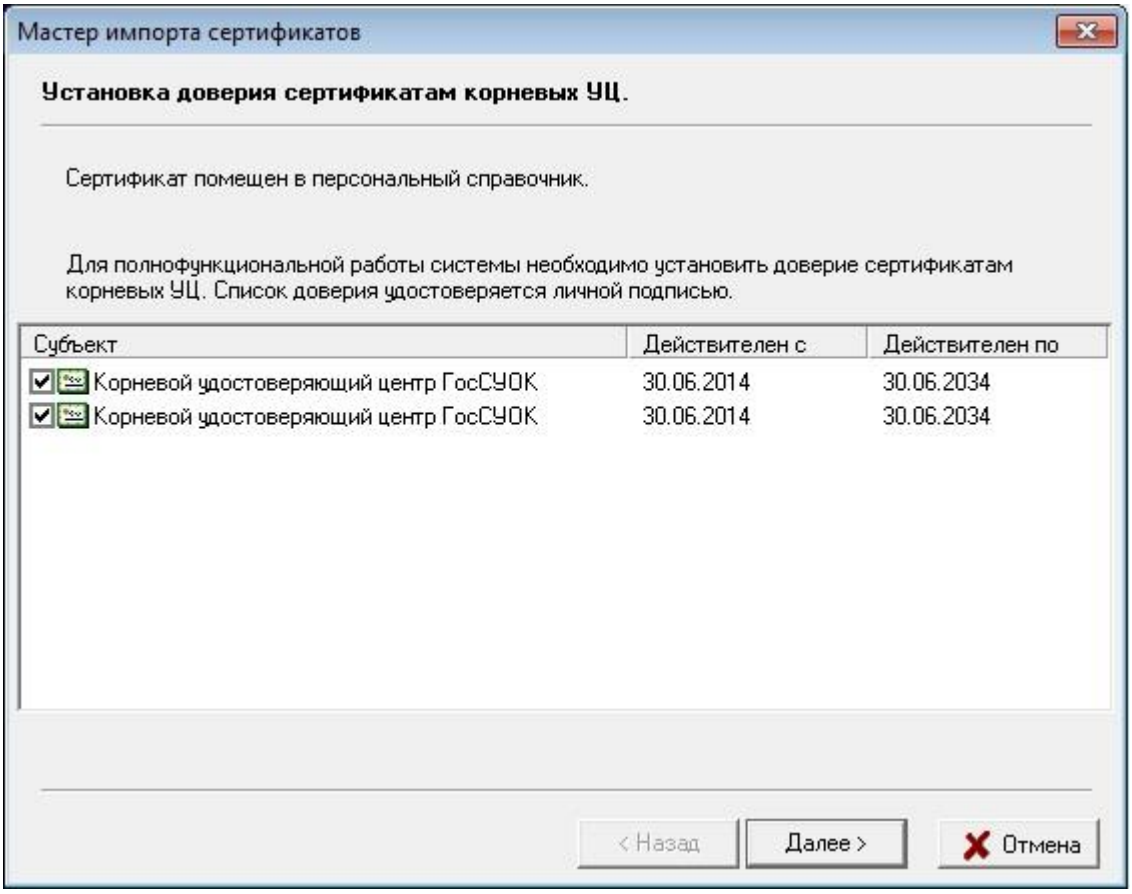

Рисунок 7 Сертификаты корневых удостоверяющих центров

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 8 Предупреждение системы безопасности).

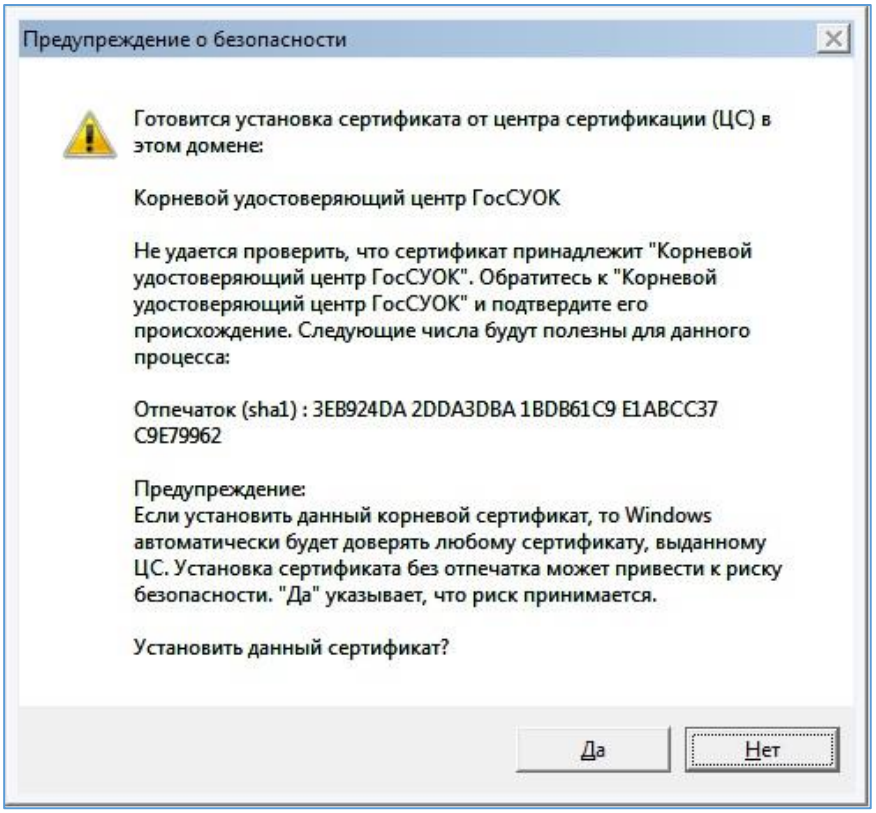

Рисунок 8 Предупреждение системы безопасности

На следующем шаге мастер импорта уведомит о сертификатах, которым было установлено доверие. Нажмите кнопку «Закрыть». (См. Рисунок 9 Завершение работы мастера импорта сертификатов)

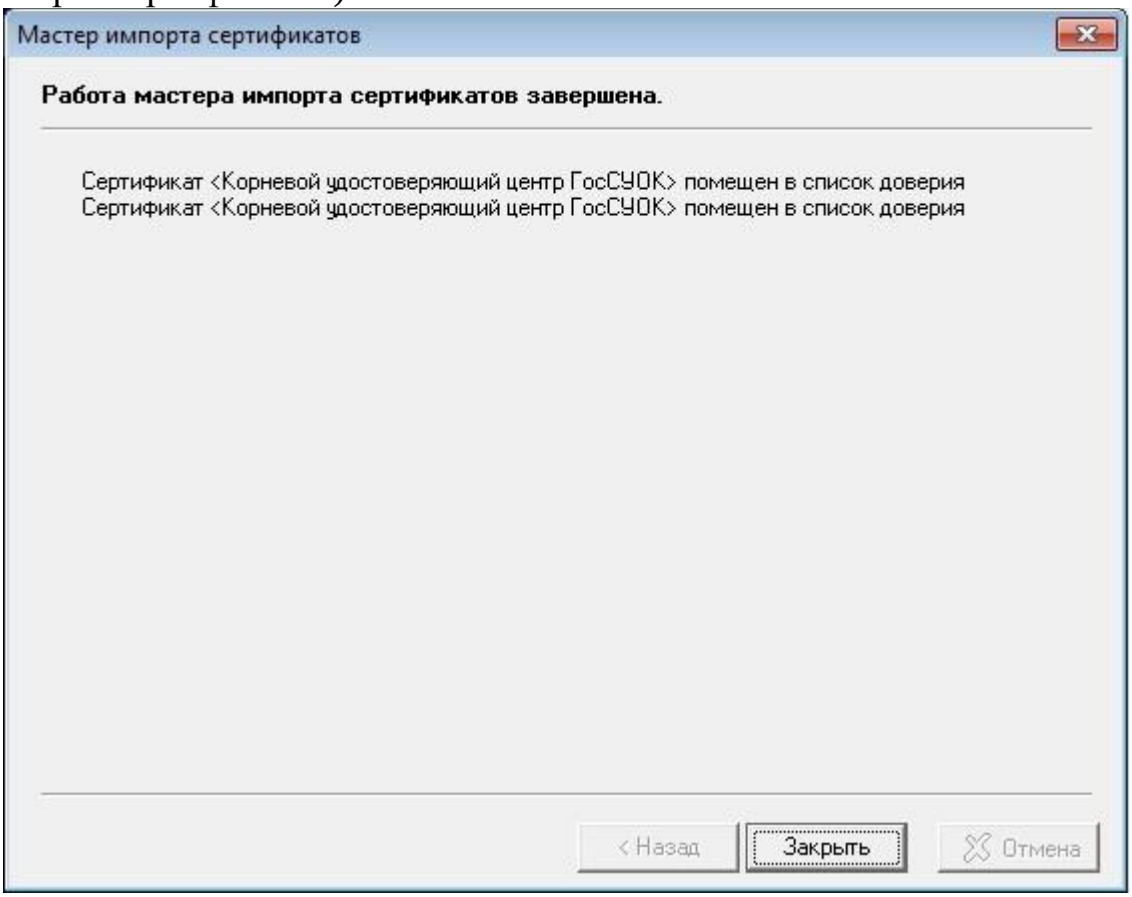

Рисунок 9 Завершение работы мастера импорта сертификатов

Приложение 1.2 Импорт сертификатов средствами персонального менеджера

Менеджер сертификатов по умолчанию устанавливается в папку:

- C:\Program Files(x86)\Avest\AvPCM_nces (для 64-х разрядных ОС);
- C:\Program Files\Avest\AvPCM_nces (для 32-х разрядных ОС).

Запуск осуществляется через исполняемый файл «MngCert.exe», который находится в этой папке. Запустить менеджер также можно с помощью ярлыка на рабочем столе или через меню «Пуск» → «Программы» → «Авест» → «Авест для НЦЭУ».

Для установки личного сертификата надо запустить менеджер сертификатов без авторизации (в окне «Авторизация пользователя» установить галочку «Войти в систему без авторизации» и нажать «ОК»). Вызвать меню «Файл» → «Импорт сертификатов» (см. Рисунок 10 Импорт сертификата). В окне импорта указать файл, содержащий личный сертификат пользователя (это может быть цепочка сертификатов с расширением *.p7b или отдельный сертификат с расширением *.cer).

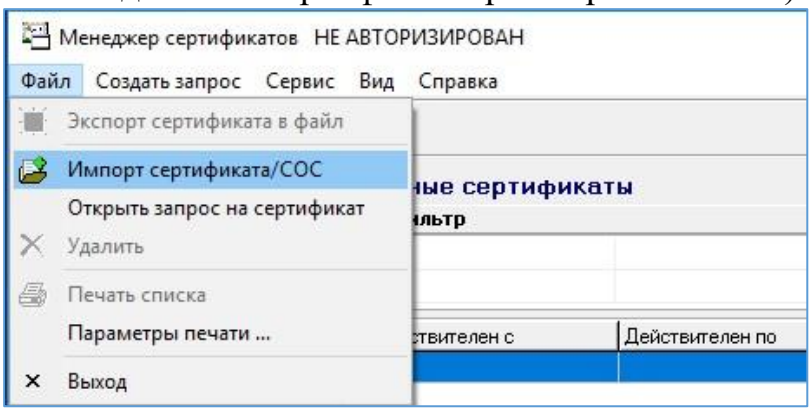

Рисунок 10 Импорт сертификата

Программа отобразит импортируемые объекты (см. Рисунок 11 Импортируемые объекты) и на следующем шаге предложит вставить носитель с личным ключом.

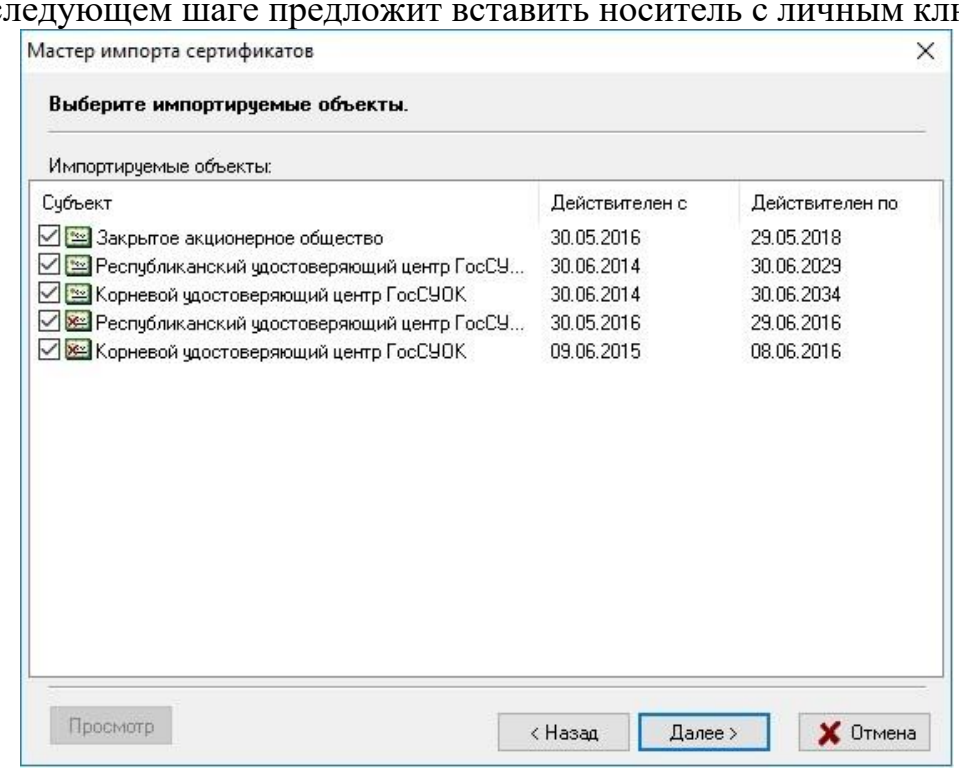

Рисунок 11 Импортируемые объекты

Для помещения личного сертификата в справочник личных сертификатов необходимо выбрать контейнер личного ключа, соответствующий личному сертификату. В появившемся окне ввести пароль.

На следующем шаге будет установлено доверие сертификату корневого удостоверяющего центра, который входит в цепочку сертификатов *.p7b. На экране возникает «Предупреждение системы безопасности» Windows, в котором необходимо нажать «Да» (см. Рисунок 8 Предупреждение системы безопасности).

Внимание! Если при установке доверия сертификату КУЦ откроется уведомление «Отказано в доступе», которое будет обозначать отсутствие прав пользователя производить данную процедуру, то для установки сертификатов КУЦ следуйте инструкции, описанной в

После завершения помещения сертификата в «Личные» программа выдаст соответствующее сообщение.

Для импорта сертификатов других корневых удостоверяющих центров, необходимо войти в персональный менеджер сертификатов с авторизацией или без авторизации, если установлен менеджер версии 3.6.0 и выше.

Для входа с авторизацией нужно выбрать действующий сертификат в окне «Авторизация пользователя» и ввести пароль. Чтобы войти без авторизации, надо в окне «Авторизация пользователя» отметить «Войти в систему без авторизации» и нажать «ОК». В менеджере сертификатов вызвать меню «Файл» → «Импорт сертификата», выбрать соответствующий файл с диска из папки data и проимпортировать его. Повторить импорт для всех корневых сертификатов, находящихся на диске.

В настоящее время для успешной работы со всеми системами требуется импорт сертификата Корневого удостоверяющего центра ГосСУОК (kuc_gos.cer.)

Далее выбрать пункт «Сетевой справочник». В отобразившемся списке сертификатов нужно выбрать сертификат корневого УЦ, который необходимо поместить в справочник доверенных УЦ.

Правой клавишей мыши вызвать контекстное меню, выбрать пункт «Поместить сертификат в справочник доверенных УЦ» (см. Рисунок 12 Помещение сертификата в справочник доверенных УЦ) Повторить помещение в доверенные УЦ для остальных проимпортированных корневых сертификатов.

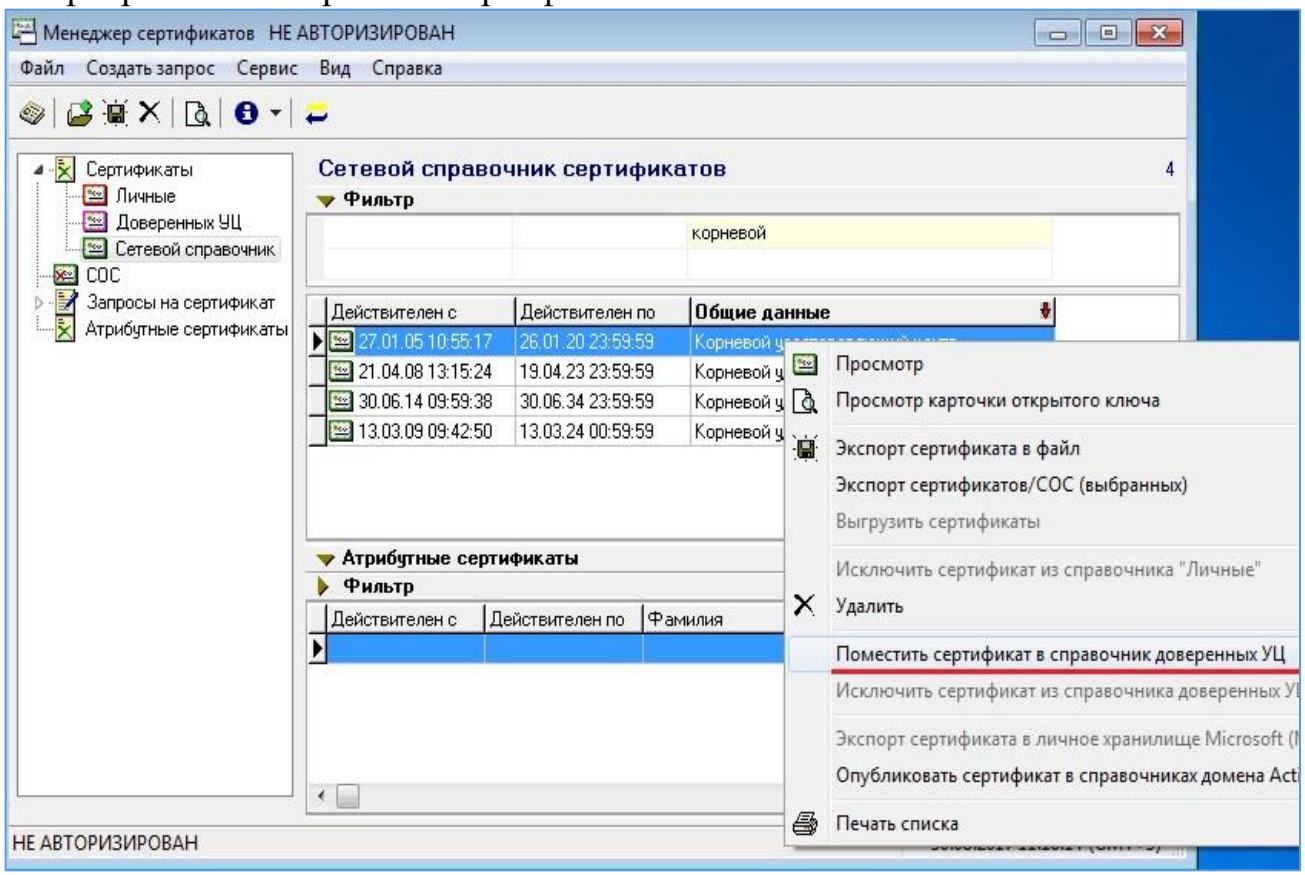

Рисунок 12 Помещение сертификата в справочник доверенных УЦ

Также аналогично необходимо проимпортировать сертификаты промежуточных центров сертификации, которые будут помещены в «Сетевой справочник».

В настоящее время для успешной работы со всеми системами требуется импорт трех промежуточных сертификатов:

- ruc.cer — Республиканский удостоверяющий центр ГосСУОК,
- ruc_old.cer — Республиканский удостоверяющий центр ГосСУОК,
- cas_ruc.cer — Служба атрибутных сертификатов.

Внимание! Если при установке доверия сертификату КУЦ откроется уведомление «Отказано в доступе», которое будет обозначать отсутствие прав пользователя производить данную процедуру, то для установки сертификатов КУЦ следуйте инструкции, описанной в

Приложение 1.3 Установка сертификатов корневых удостоверяющих центров в домене.

Приложение 1.3 Установка сертификатов корневых удостоверяющих центров в домене.

Внимание! Для выполнения этой процедуры необходимо быть, как минимум, членом группы «Администраторы домена».

Чтобы добавить сертификаты в хранилище доверенных корневых центров сертификации домена, выполните следующие действия:

1. Откройте «Пуск» → «Администрирование» →«Управление групповой политикой».
2. В дереве консоли откройте узел «Объекты групповой политики» в лесу и домене, содержащем изменяемый объект групповой политики «Политика домена по умолчанию».
3. Щелкните правой кнопкой мыши на объекте групповой политики «Политика домена по умолчанию» и выберите команду «Изменить».
4. В консоли управления групповой политикой перейдите в раздел «Конфигурация компьютера», «Политики», «Параметры Windows», «Настройка безопасности» и щелкните «Политики открытого ключа» (см. Рисунок 13 Политики открытого ключа).

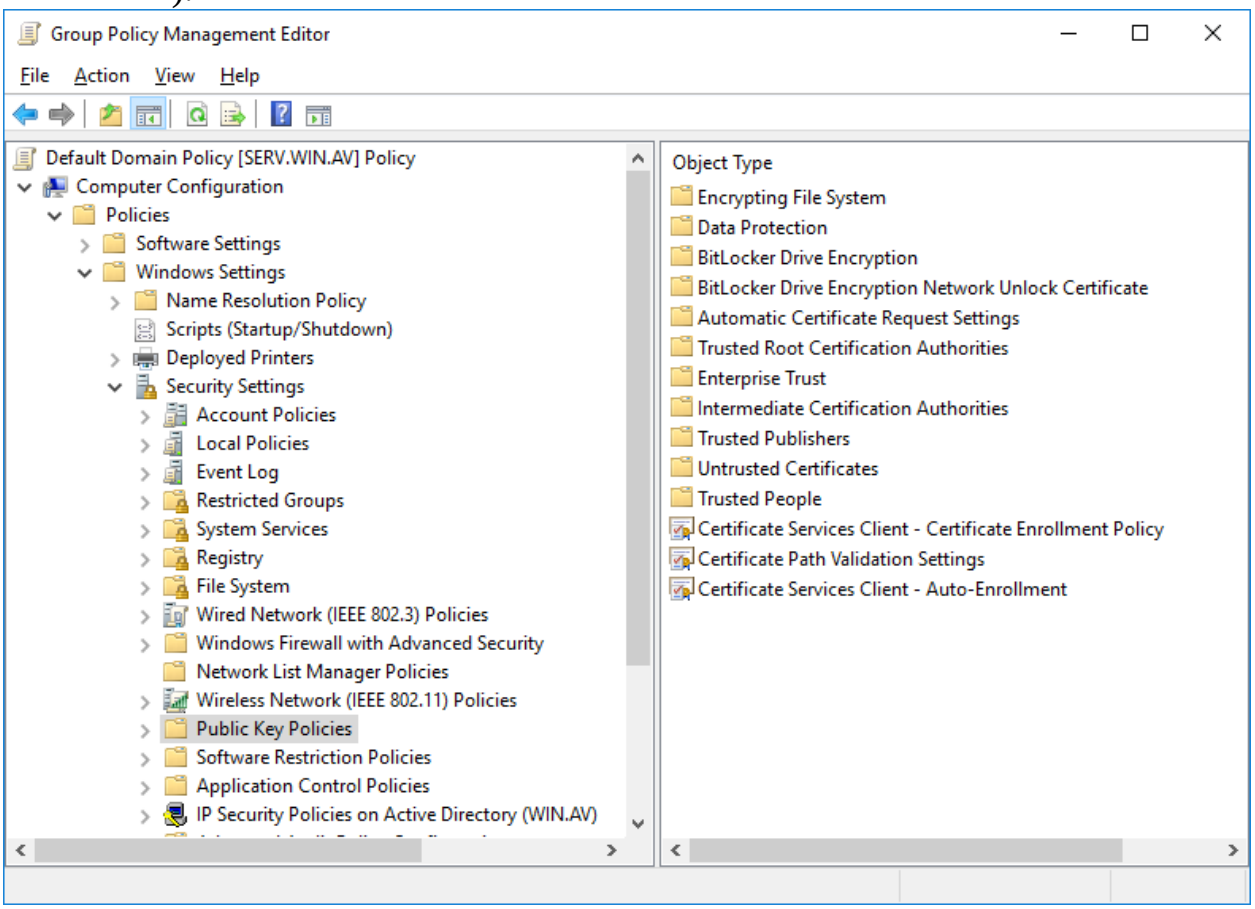

Рисунок 13 Политики открытого ключа

5. Щелкните правой кнопкой мыши хранилище «Доверенные корневые центры сертификации».
6. Нажмите кнопку «Импорт» и выполните импорт Всех Корневых сертификатов УЦ с диска из папки data. В настоящее время для успешной работы со всеми системами требуется импорт сертификата Корневого удостоверяющего центра ГосСУОК (kuc_gos.cer).

Снова выберите пункт «Политики открытого ключа».

1. Откройте «Параметры подтверждения пути сертификата», а затем щелкните вкладку «Хранилища».
2. Установите флажок «Определить параметры политики».
3. В группе «Хранилища сертификатов» отдельных пользователей установите флажки «Разрешить использование корневых ЦС, которым доверяет пользователь, для проверки сертификатов» и «Разрешить пользователям доверять сертификатам одноранговой групп» в группе флажков «Хранилища сертификатов отдельных пользователей».
4. В группе «Хранилища корневых сертификатов» определите корневые центры сертификации, которым могут доверять клиентские компьютеры, а затем нажмите кнопку «ОК», чтобы применить новые параметры (см. Рисунок 14 Применение параметров). На этом добавление сертификатов завершено.

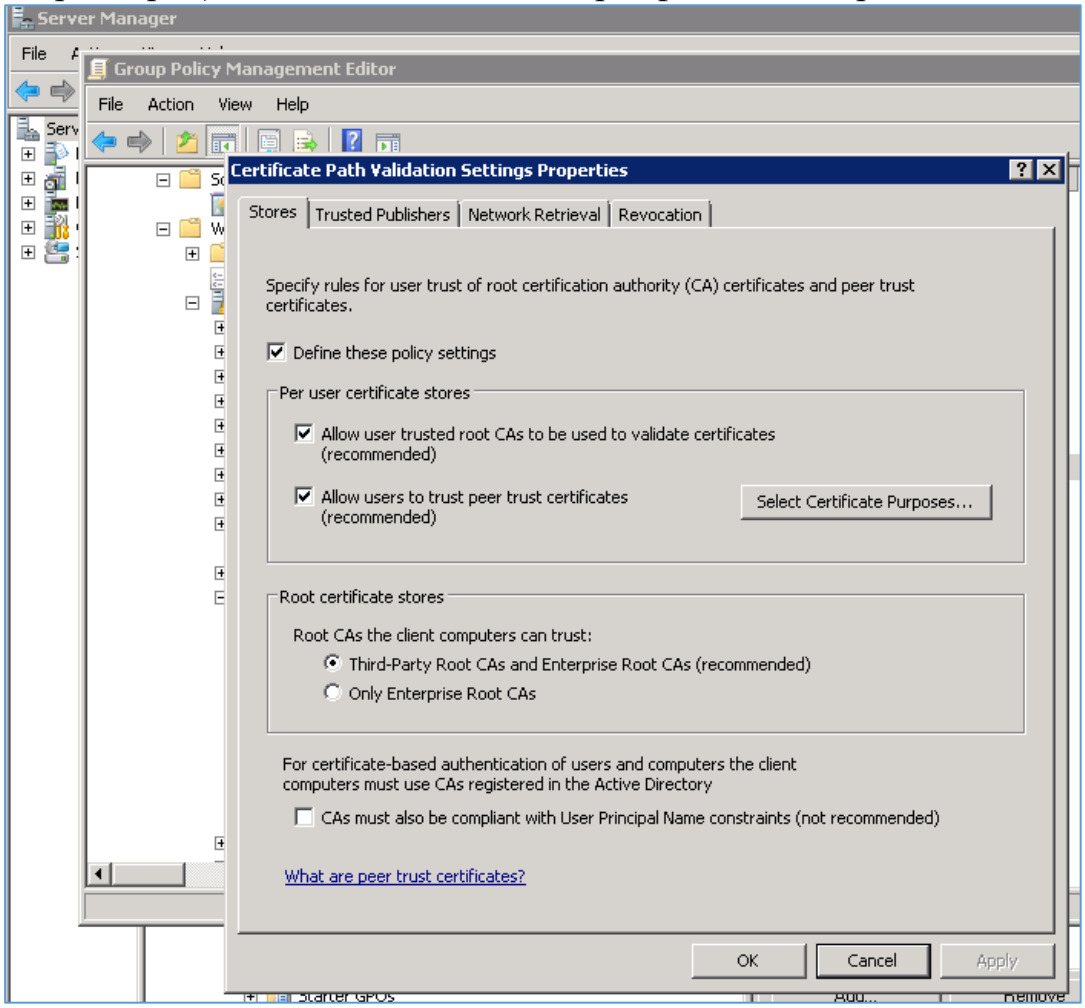

Рисунок 14 Применение параметров