

Установка и обновление криптографического
программного обеспечения для абонентов РУП
«Национальный центр электронных услуг» с
помощью объединённого инсталлятора AvPKISetup
в режиме ограниченных прав учетной записи
пользователя

Листов 13

Аннотация

В настоящей инструкции описаны особенности 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 в режиме ограниченных прав учетной записи пользователя. Данный комплект предназначен для абонентов РУП «Национальный центр электронных услуг» (далее РУП «НЦЭУ») и распространяется в рамках оказания услуг РУП «НЦЭУ».

Оглавление

1. Сведения об учётной записи.....	4
1.1 Как определить, входит ли компьютер в домен?	4
1.2 Как определить тип учётной записи?.....	5
2. Установка ПО	6
2.1 Компьютер входит в домен.....	6
2.2 Компьютер не входит в домен.....	6
Приложение 1 Импорт сертификатов средствами персонального менеджера.....	7
Приложение 2 Установка сертификатов корневых удостоверяющих центров в домене	11
3. Перечень сокращений	13

1. 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)

1.1 Как определить, входит ли компьютер в домен?

Информация о том, входит ли ваш компьютер в домен или принадлежит к рабочей группе, будет указана в сведениях о системе. Как это выглядит, например, на ОС Windows 7 см. Рисунок 1 Определение домена на ОС Windows 7.

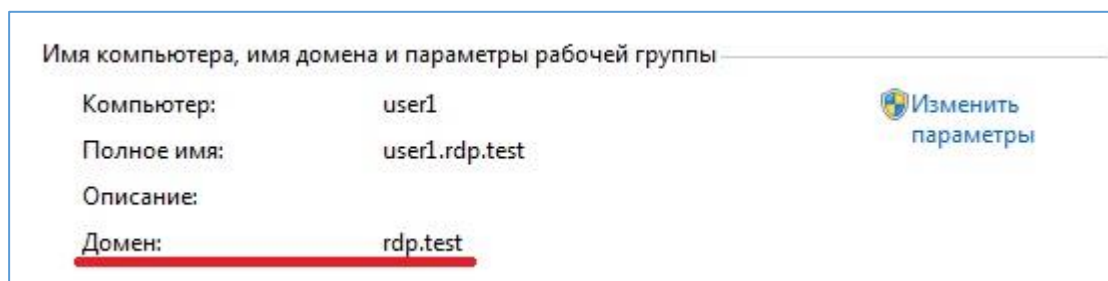


Рисунок 1 Определение домена на ОС Windows 7

Чтобы просмотреть эти сведения нужно:

- В ОС **Windows XP, Windows 2003 Server**:
 1. Перейти в меню «Пуск» - «Панель управления», в зависимости от параметров просмотра элементов в панели управления (классический вид или по категориям) выбрать «Система» или «Производительность и обслуживание» - «Система». Другой способ - кликнуть правой клавишей мыши по ярлыку «Мой компьютер», выбрать «Свойства».
 2. Открыть вкладку «Имя компьютера».
- В ОС **Windows 7, Windows 2008 Server**:
 1. Перейти в меню «Пуск» - «Панель управления», в зависимости от параметров отображения элементов в панели управления (категория или значки) выбрать «Система» или «Система и безопасность» - «Система». Другой способ - кликнуть правой клавишей мыши по ярлыку «Компьютер», выбрать «Свойства».
 2. Найти нужную информацию в разделе «Имя компьютера, имя домена и параметры рабочей группы».
- В ОС **Windows 8, Windows 8.1, Windows 2012 Server**:

1. Навести курсор мыши на правый верхний или нижний угол рабочего стола. В открывшейся боковой панели выбрать пункт «Параметры». В списке параметров выбрать пункт «Сведения о компьютере». Другой способ - нажать клавиши Windows+X, чтобы отобразить список команд и параметров, щелкнуть пункт «Система».
 2. Найти нужную информацию в разделе «Имя компьютера, имя домена и параметры рабочей группы».
- В ОС **Windows 10, Windows 2016 Server, Windows 2019 Server**:
 1. Нажать правой клавишей мыши по кнопке «Пуск», в списке параметров выбрать «Система», справа в разделе «Сопутствующие параметры» выбрать «Дополнительные параметры системы».
 2. Открыть вкладку «Имя компьютера».

1.2 Как определить тип учетной записи?

Открыть «Панель управления» → «Учетные записи пользователей» → «Управление учетными записями пользователей». Откроется окно с основными учетными записями. Если под вашим именем пользователя указано Администратор, значит, учетная запись имеет тип «Администратор». В противном случае это стандартный тип учетной записи пользователя с ограниченными правами (см. Рисунок 2 Тип учетной записи).

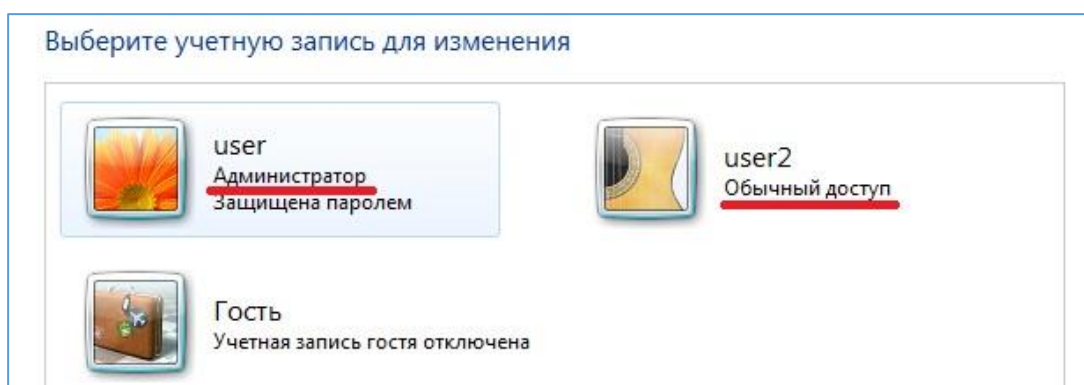


Рисунок 2 Тип учетной записи

2. Установка ПО

2.1 Компьютер входит в домен

Если компьютер входит в домен, то возможность изменения его параметров для учетной записи пользователя (не администратора), скорее всего, будет ограничена. Установка и обновление программного обеспечения производится администратором домена согласно документу *«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»*. При установке ПО с правами администратора домена импорт сертификата в личный справочник проводить не нужно.

После того, как все программы из комплекта абонента AvPKISetup установлены, нужно войти под учетной записью пользователя и проимпортировать личный сертификат вручную средствами менеджера сертификатов (см. Приложение 1 Импорт сертификатов средствами персонального менеджера) и установить доверие сертификатам корневых удостоверяющих центров (см. Приложение 2 Установка сертификатов корневых удостоверяющих центров в домене).

2.2 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 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»*. При установке ПО под учетной записью 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 Импорт сертификатов средствами персонального менеджера)

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

Приложение 1 Импорт сертификатов средствами персонального менеджера

Менеджер сертификатов по умолчанию устанавливается в папку:

- C:\Program Files(x86)\Avest\AvPCM_ncesBign (для 64-х разрядных ОС);
- C:\Program Files\Avest\AvPCM_ncesBign (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 для НЦЭУ (Bign)».

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 сертификата/СОС» (см. Рисунок 3 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).

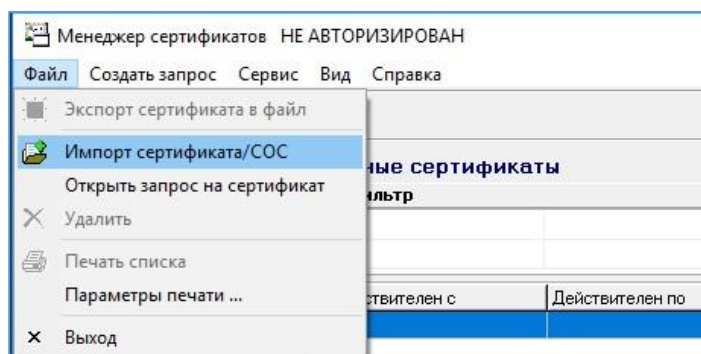


Рисунок 3 Импорт сертификата

Программа отобразит импортируемые объекты (см. Рисунок 4 Импортируемые объекты) и на следующем шаге предложит вставить носитель с личным ключом.

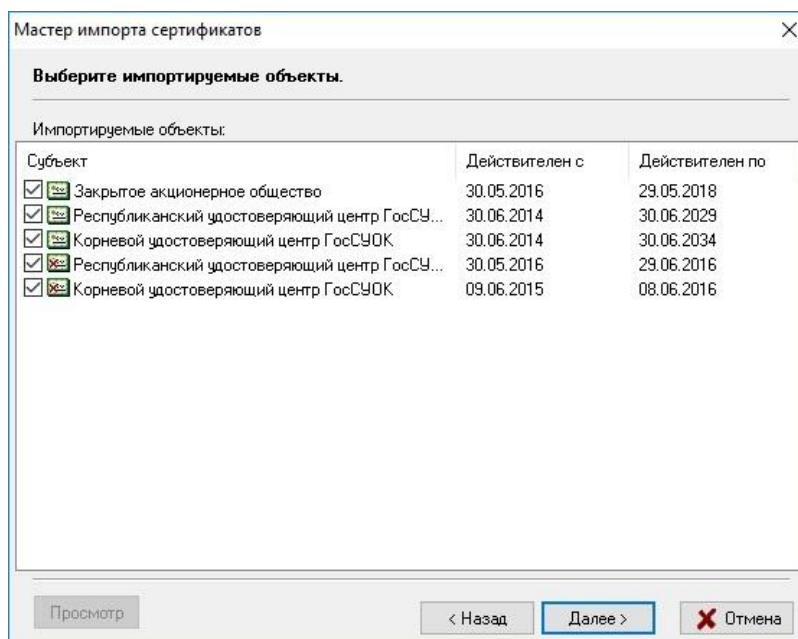


Рисунок 4 Импортируемые объекты

Для установки личного сертификата надо вставить носитель, 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. 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». В появившемся окне ввести пароль.

На следующем шаге будет установлено доверие сертификату корневого удостоверяющего центра, который входит в цепочку сертификатов *.p7b. На экране возникнет «Предупреждение системы безопасности» Windows, в котором нужно нажать «Да» (см. Рисунок 5 Предупреждение системы безопасности).

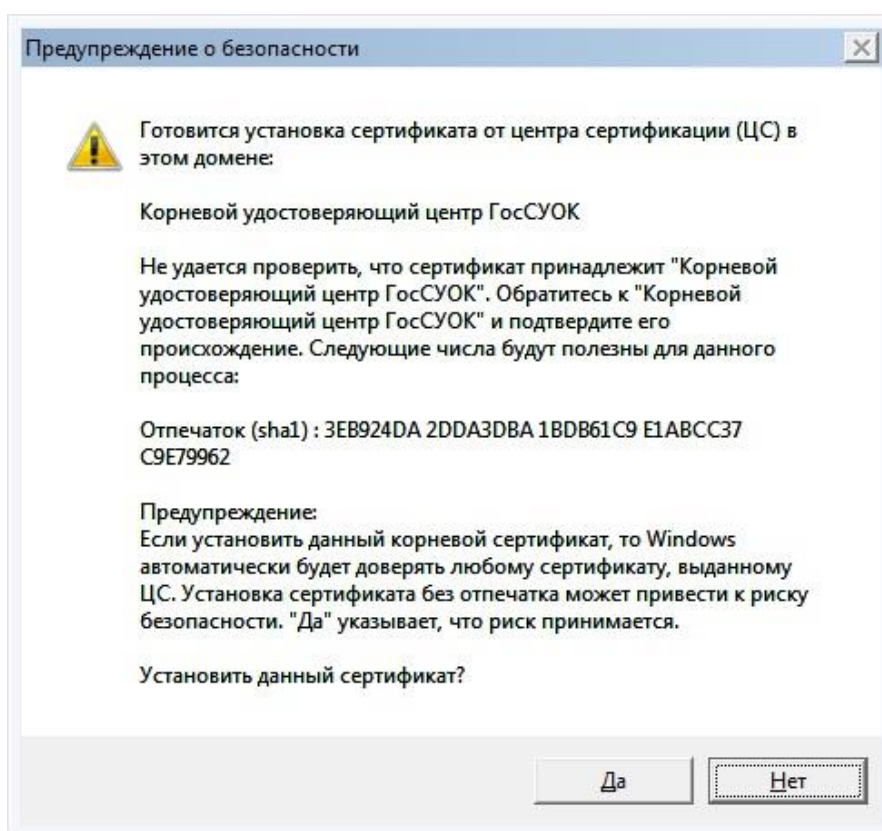


Рисунок 5 Предупреждение системы безопасности

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 Приложение 2 Установка сертификатов корневых удостоверяющих центров в домене

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

Если файл личного сертификата был сохранен с расширением *.cer, то он не включает сертификаты издателей и их СОСы, и их нужно проимпортировать. Сделать это можно двумя способами:

1. Войти в персональный менеджер сертификатов без авторизации (в окне «Авторизация пользователя» отметить «Войти в систему без авторизации» и нажать «ОК»). В менеджере сертификатов вызвать меню «Сервис» – «Обновление СОС и сертификатов УЦ» и нажать «Далее». Интернет при этом должен быть включён.

2. Войти в персональный менеджер сертификатов без авторизации (в окне «Авторизация пользователя» отметить «Войти в систему без авторизации» и нажать «ОК»). В менеджере сертификатов вызвать меню «Файл» → «Импорт сертификата», выбрать соответствующий файл сертификата из папки data комплекта абонента AvPKISetup и проимпортировать его, следуя указаниям мастера импорта сертификатов.

В настоящее время для успешной работы со всеми информационными системами требуется импорт сертификатов Корневых удостоверяющих центров (ruc1.cer и ruc2.cer), а также пяти промежуточных сертификатов:

- ruc1.cer — старый сертификат Республиканского удостоверяющего центра ГосСУОК,
- ruc2.cer — обновленный сертификат Республиканского удостоверяющего центра ГосСУОК,
- ruc3.cer — обновленный сертификат Республиканского удостоверяющего центра ГосСУОК, выпущенный в 2024 году,
- cas_ruc2.cer — сертификат Службы атрибутивных сертификатов,
- cas_ruc3.cer — сертификат Службы атрибутивных сертификатов, выпущенный в 2024 году.

После импорта сертификатов издателей необходимо установить доверие сертификатам Корневого удостоверяющего центра ГосСУОК и BY Root CA NCES 2. Для этого в менеджере сертификатов выбрать пункт «Сетевой справочник», в отобразившемся списке сертификатов выбрать сертификат Корневого удостоверяющего центра ГосСУОК, правой клавишей мыши вызвать контекстное меню, выбрать пункт «Поместить сертификат в справочник доверенных УЦ» (см. Рисунок 6 Помещение сертификата в справочник доверенных УЦ). Аналогично установить доверие сертификату BY Root CA NCES 2.

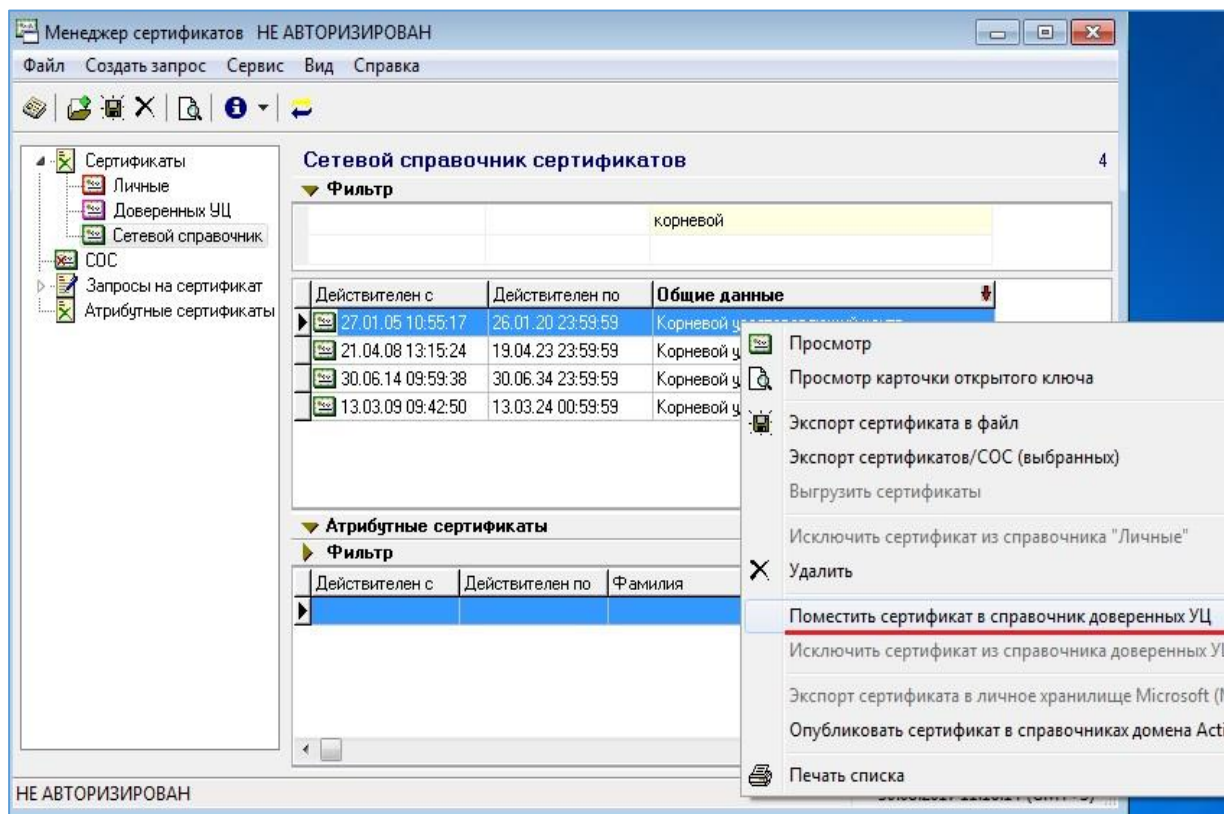


Рисунок 6 Помещение сертификата в справочник доверенных УЦ

Внимание! Если при установке доверия сертификатам Корневого удостоверяющего центра ГосСУОК и ВУ Root CA NCES 2 откроется уведомление «Отказано в доступе», которое будет обозначать отсутствие прав пользователя производить данную процедуру, то для установки доверия сертификатам КУЦ следуйте инструкции, описанной в Приложении 2 Установка сертификатов корневых удостоверяющих центров в домене

Приложение 2 Установка сертификатов корневых удостоверяющих центров в домене

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

Данная инструкция является примером того, как можно поместить сертификат КУЦ в справочник Доверенных корневых центров сертификации, используя средства ОС Microsoft, процедура может отличаться в зависимости от настроек домена, от версии ОС и других факторов. Более детальную информацию об особенностях работы с сертификатами КУЦ в домене нужно уточнять у официальных производителей ОС.

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 в лесу и домене узел «Объекты групповой политики», содержащий 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 7 Политики открытого ключа).

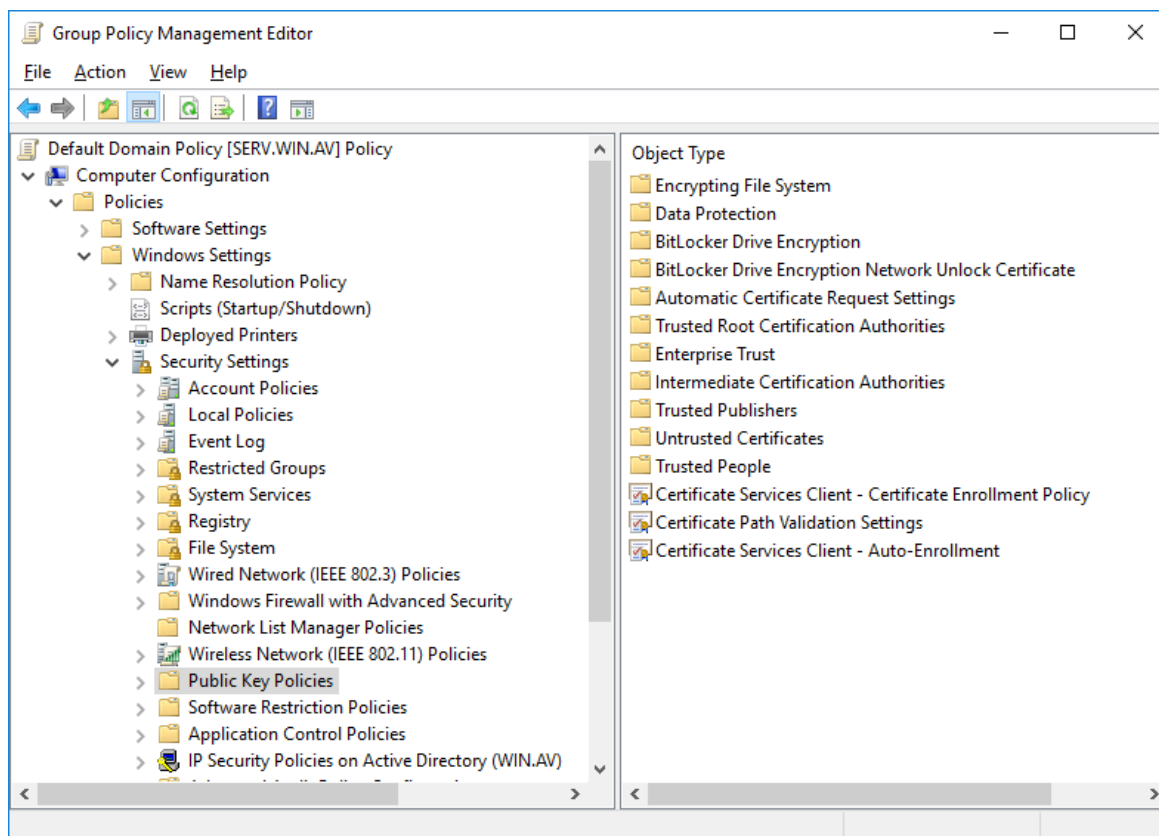


Рисунок 7 Политики открытого ключа

5. Щелкните правой кнопкой мыши хранилище «Доверенные корневые центры сертификации».

6. Нажмите кнопку «Импорт» и выполните импорт сертификатов корневых удостоверяющих центров kus1.cer и kus2.cer (находятся в папке data).

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 группы» 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 8 Применение параметров). На этом добавление сертификатов завершено.

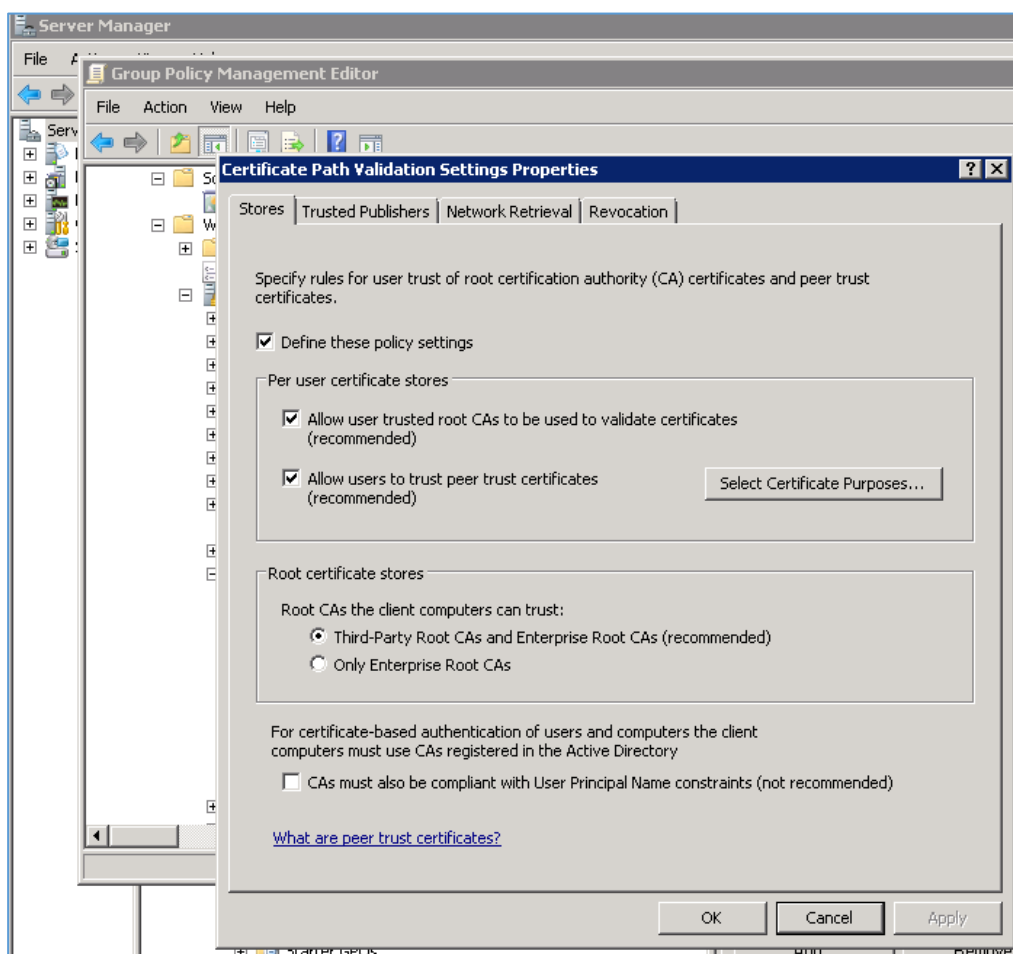


Рисунок 8 Применение параметров

3. Перечень сокращений

ГосСУОК – Государственная система управления открытыми ключами;

КУЦ – корневой удостоверяющий центр

ОС – операционная система;

ПО – программное обеспечение;

РУП «НЦЭУ» – Республиканское унитарное предприятие «Национальный центр электронных услуг»;

СОС – список отозванных сертификатов;

УЦ – удостоверяющий центр.