**Установка Застава 6**

Установку проводить под пользователем **с правами администратора компьютера**.

Вначале Необходимо определиться, какую конфигурацию устанавливать. Если у клиента необходимо подключить к сети минфина более двух компьютеров ( при наличии сервера не менее windows server 2012 c двумя сетевыми платами ), то необходимо настроить маршрутизацию на сервере.

**Оглавление**

[Создание клиента на TPN-сервере 1](#_Toc106877683)

[Необходимые ресурсы и компоненты для установки у клиента 1](#_Toc106877684)

[Установка КриптоПро 2](#_Toc106877685)

[Создание носителя с закрытыми ключами 5](#_Toc106877686)

[Копирование ключей с виртуального диска в реестр. 5](#_Toc106877687)

[Установить заставу. 9](#_Toc106877688)

[Настройка и активация Застава 6 10](#_Toc106877689)

[Настройка маршрутизации на сервере 15](#_Toc106877690)

**Создание и получение сертификатов для установки**

Изготовление осуществляется службой технической поддержки проекта. Для этого необходимо обратиться по контактам: (Телефон:  8 (843) 253 53 16, email: [zastava@vrca.ru](mailto:zastava@vrca.ru), чат в Tелеграмм: <https://t.me/+Q6WB5gQE9MEwZTYy>) , и сообщить название организации, используемый в текущее время сертификат ПО Застава (Посмотреть можно запустив на работающей старой версии панель Заставы – Управление – Сертификаты и определить Название сертификата с суффиксом FC), IP адрес сети ГИСТ назначенный на рабочее место ПО Застава.

**Необходимые ресурсы и компоненты для установки у клиента**

***Установочные файлы (размещены на ресурсе https://minfin.tatarstan.ru/soft):***

КриптоПро (CSPSetup-4.0.R4.9963.exe)

Застава клиент 6.7 zastava64-v6.70.21575)

Пакет Microsot Visual C++ (vc\_redist.x64.exe)

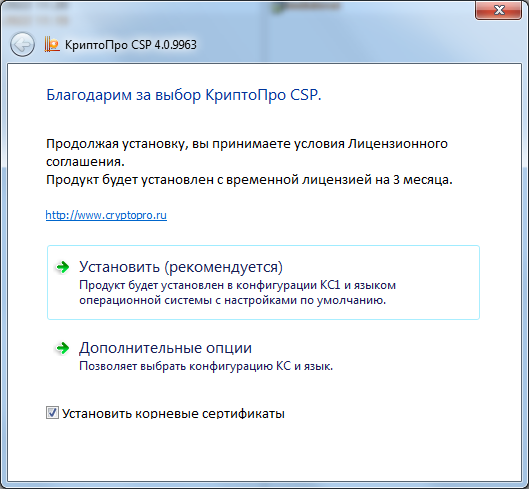
Корневой сертификат (rootca-minfin-gost2012.cer)

Сертификат клиента с закрытыми ключами и лицензия Крипто (предоставляется техподдежкой)

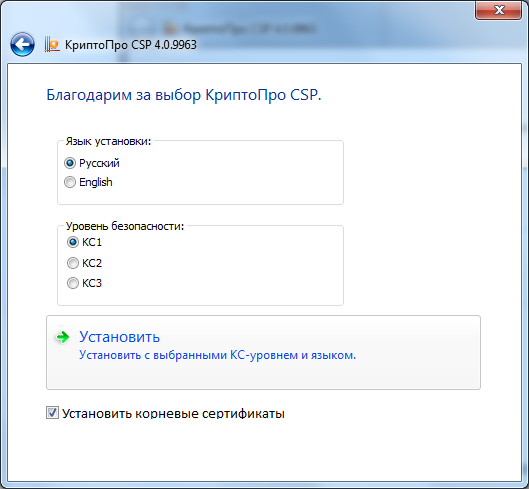
**Установка КриптоПро**

Запустить установку КриптоПро ( файл CSPSetup-4.0.R4.9963.exe ) и выбрать установку с дополнительными опциями

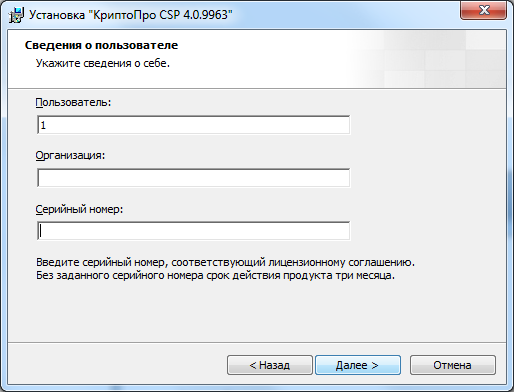
Если на компьютере имеется КриптоПро версии 5.0.12000 то для успешной установки достаточно будет доустановить Криптопровайдер уровня ядра и установить Застава Клиент v6.70 (версия v6.5 умеет работать только с КриптоПро 4).



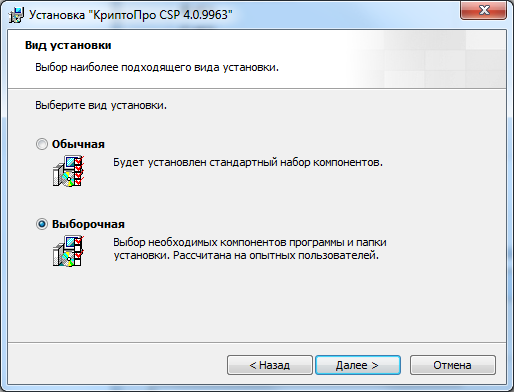
Выбрать «Дополнительные опции»



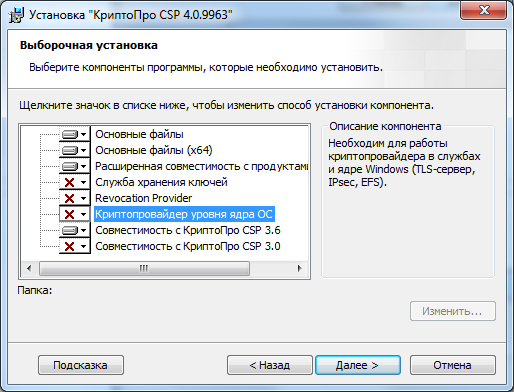
Выбрать «Установить»



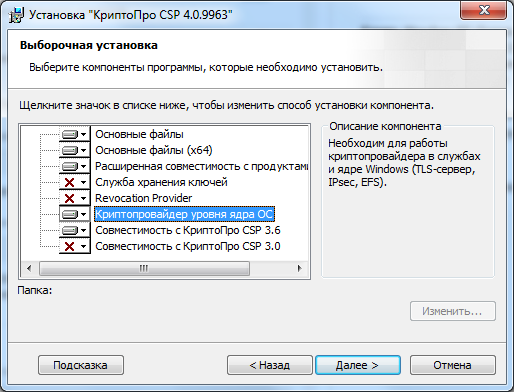
Ввести серийный номер ( если не сервере, то серверный ) и нажать «Далее»



Выбрать выборочную установку



Если не отмечен к установке «Криптопровайдер уровня ядра ОС», то выбрать «Данный компонент будет установлен на локальный жесткий диск»



Далее установка по умолчанию.

## 

## **Создание носителя с закрытыми ключами**

Так как КриптоПро использует при копировании ключей конкретный носитель, то используем виртуальный диск.

Необходимо скопировать папку с ключами клиента в папку на локальном диске (например, c:\zastava).

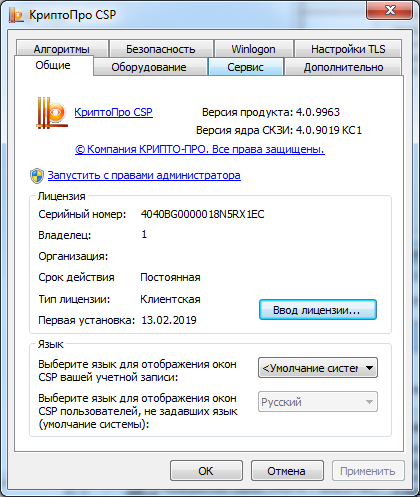
Запустить командную строку ( CMD ) от имени администратора.

В командном окне ввести subst j: c:\zastava ( j: - любая свободная буква диска)

## 

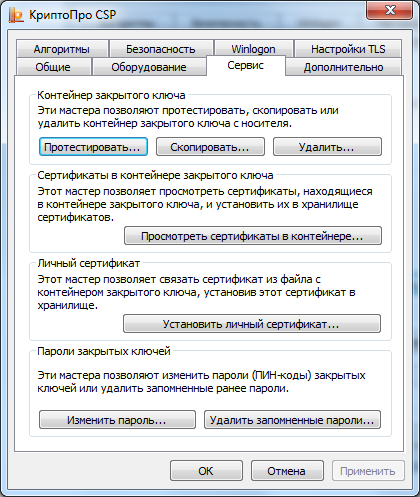
## **Копирование ключей с виртуального диска в реестр.**

Запустить КриптПро ( с правами администратора )

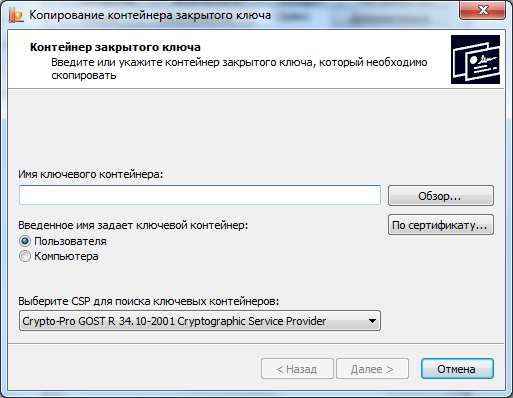


Если запустили КриптоПро из Панели управления – выбрать «Запустить с правами администратора»

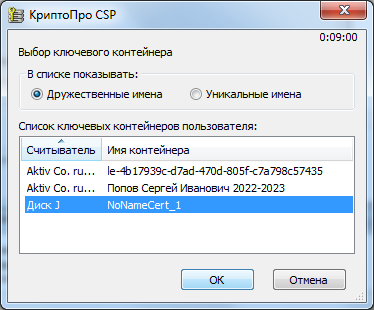
Далее выбрать вкладку «Сервис»



Выбрать «Скопировать»



«Обзор»

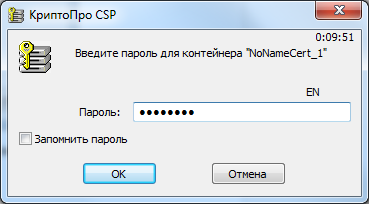


Выбрать ранее созданный контейнер на виртуальном диске. ( что-бы не запутаться вынуть все токены )

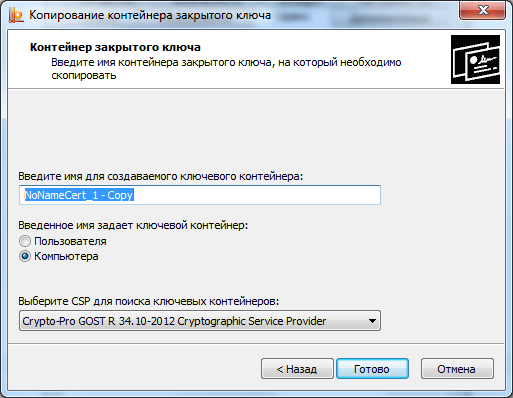


Ключевой контейнер должен быть для **Компьютера** ( недоступно, если запустили не с правами администратора )

Нажать «Далее»

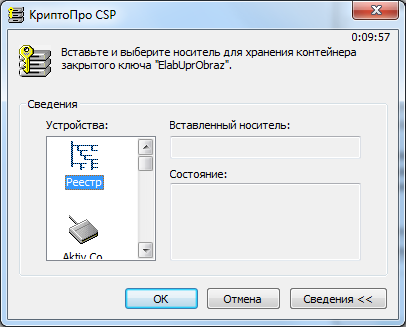


Ввести пароль P@ssCenter

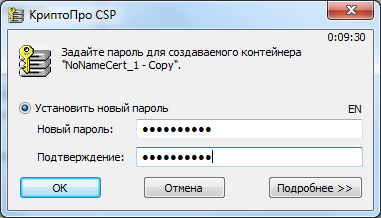


Дать имя создаваемого ключевого контейнера ( без пробелов )

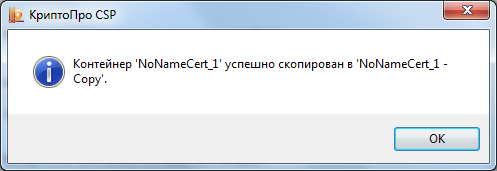
«Готово»



Выбрать «Реестр»



Задать пароль для нового контейнера ( P@ssCenter )



После установки контейнера удалить виртуальный диск из командного окна запушенного от имени админситратора

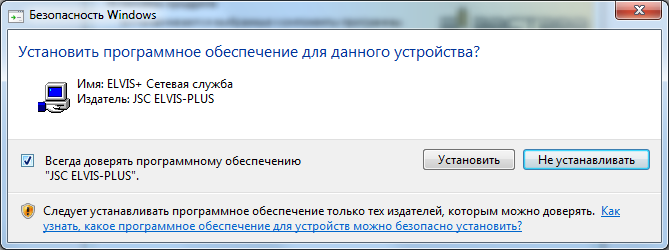
Subst j: /d

# **Установка Заставы.**

Запустить установку Заставы – файл zastavaclient64-v6.7.21575.exe

Установку производить по умолчанию.

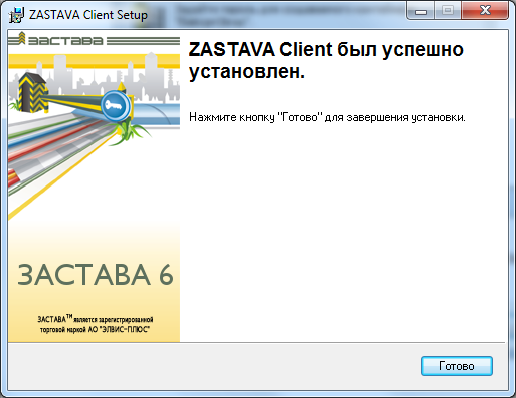
В случае появления окна



Выбрать «Установить»

Во время установки может появиться ошибка с упоминанием .dll файла. В этом случае завершить установку Заставы. Удалить программу ( если установилась ) через панель управления.

Установить Microsoft Visual C++ ( файл vc\_redist.x64.exe ). Затем повторить установку Заставы.



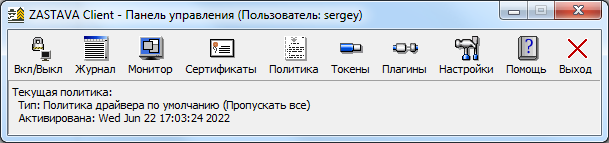
Если не установится ( или установится с ошибками ), связаться с администраторами.

# 

# **Настройка и активация Застава 6**

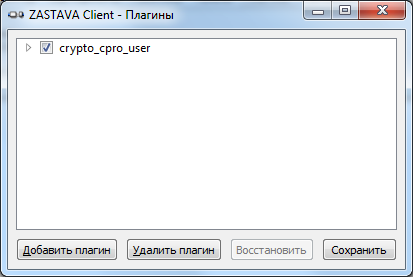
Запустить Заставу ( из меню программ ELVIS+ -> ZASTAVA Client -> VPN Agent

или из трея – значок с замком )



Главное окно ZASTAVA Client

Выбрать «Плагины»

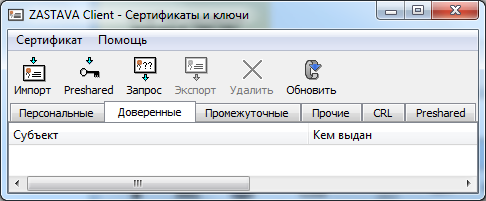


Убедиться, что плагин КриптоПро подключен. Картинка должна быть аналогична скриншоту.

Закрыть.

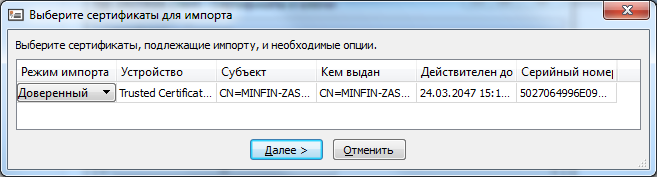
В главном окне ZASTAVA Client выбрать «Сертификаты»



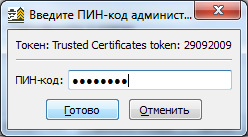


Выбрать вкладку «Доверенные» и затем «Импорт»

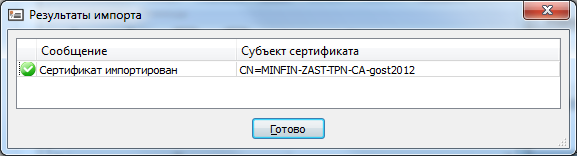
Выбрать файл корневого сертификата – rootca-minfin-gost2012.cer



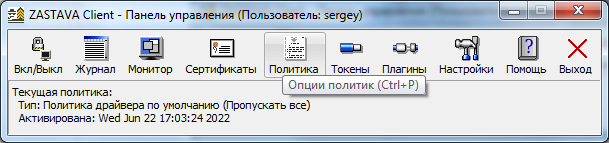
«Далее»

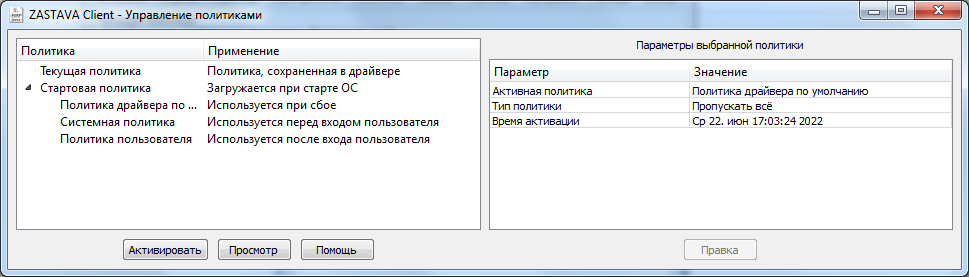


Ввести ПИН-код ( 12345678 )

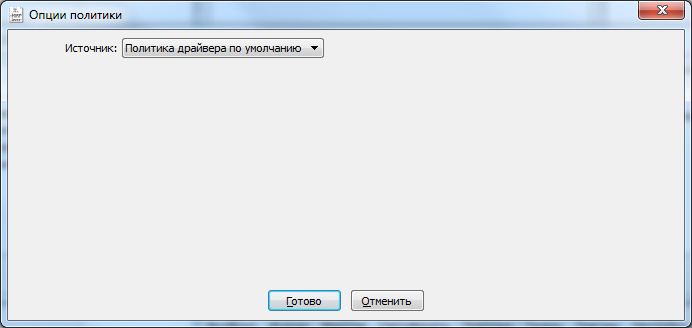


Снова в главном окне ZASTAVA Client выбираем «Политика»

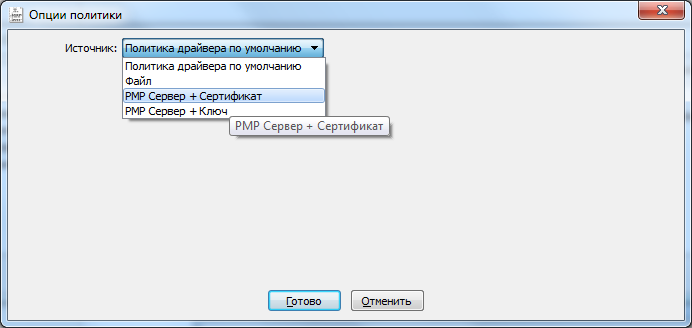




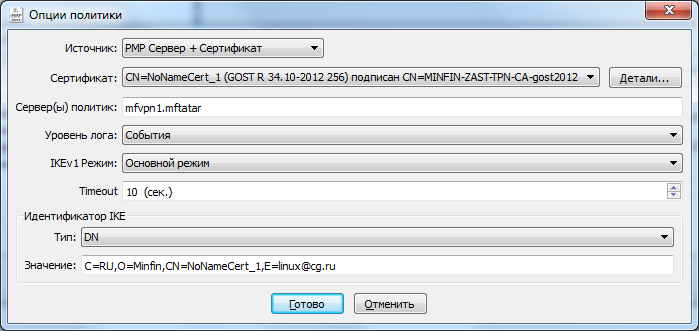
Дважды щелкаем на «Системная политика»



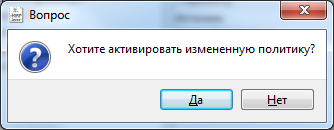
Жмем по ниспадающему списку



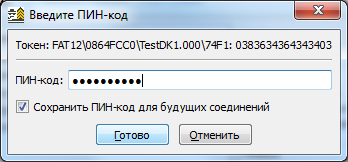
Выбирать «PMP Сервер+Сертификат»



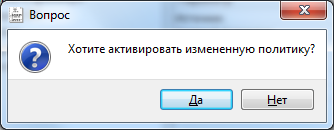
Выбрать сертификат и заполнить поле «Сервер(ы) политик». Далее «Готово»



«Да»



Ввести ПИН-код ( P@ssCenter )



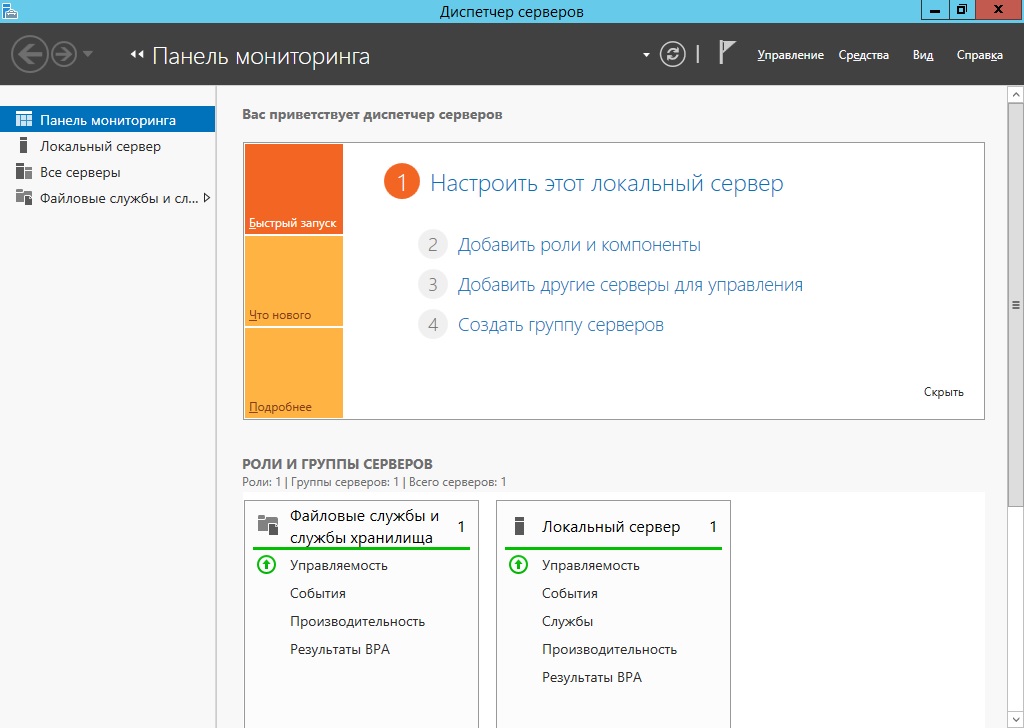
«Да»

При успешной активации значок в трее станет зеленым

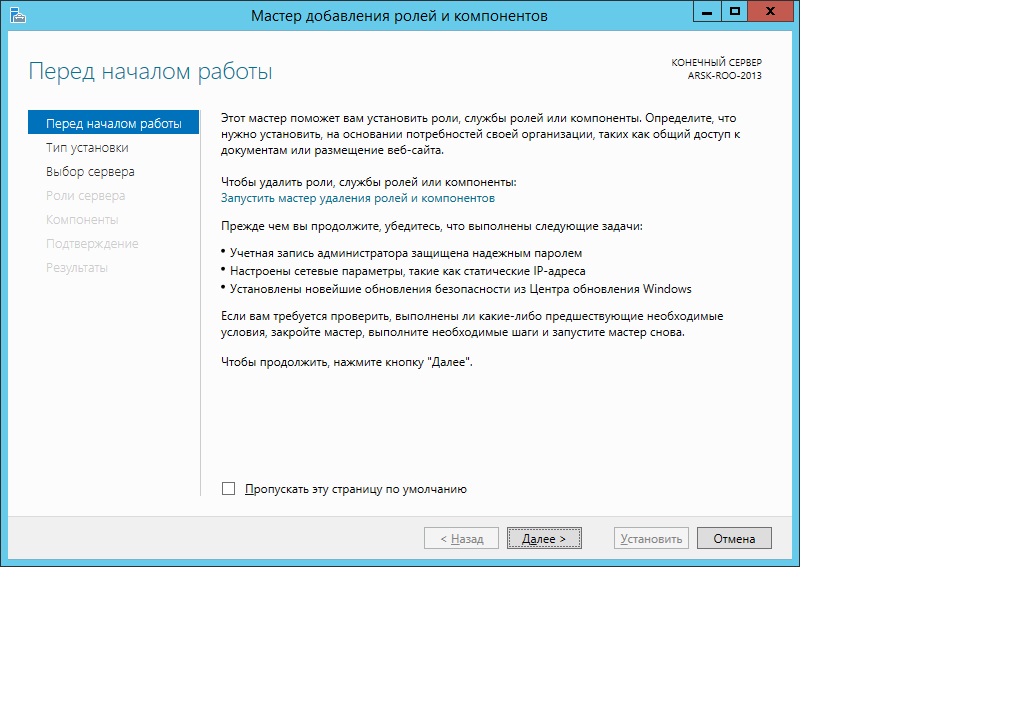
Проверить доступность серверов АЦК и Барс.

# **Настройка маршрутизации на сервере (необходимо если ПО Застава-Клиент используется для защиты сегмента локальной сети)**

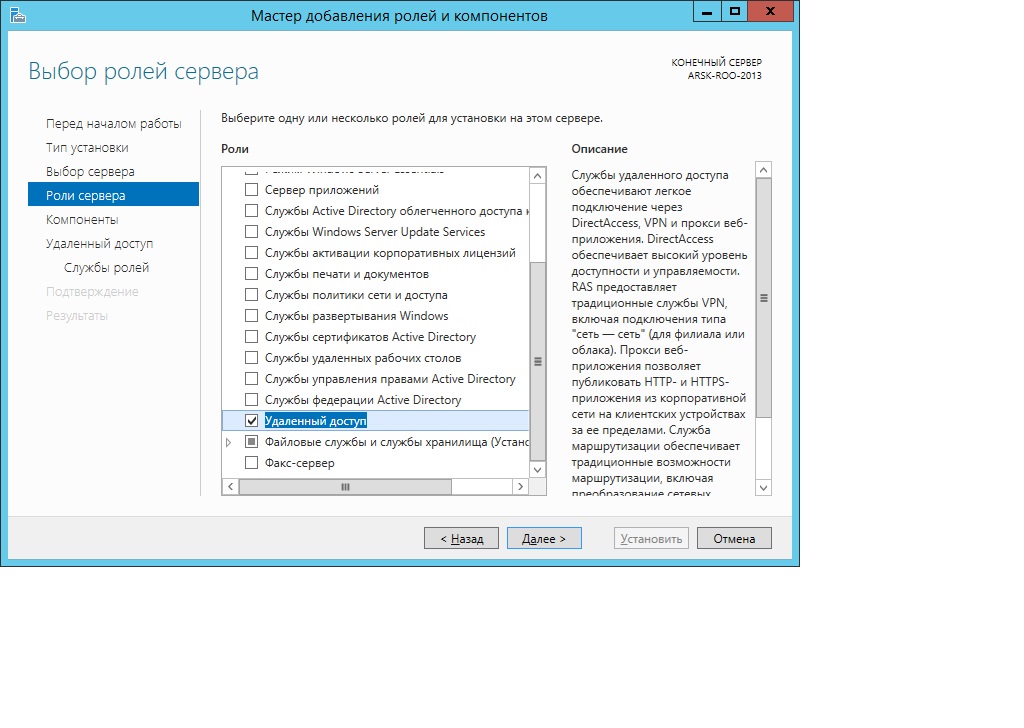
На примере windows server 2016



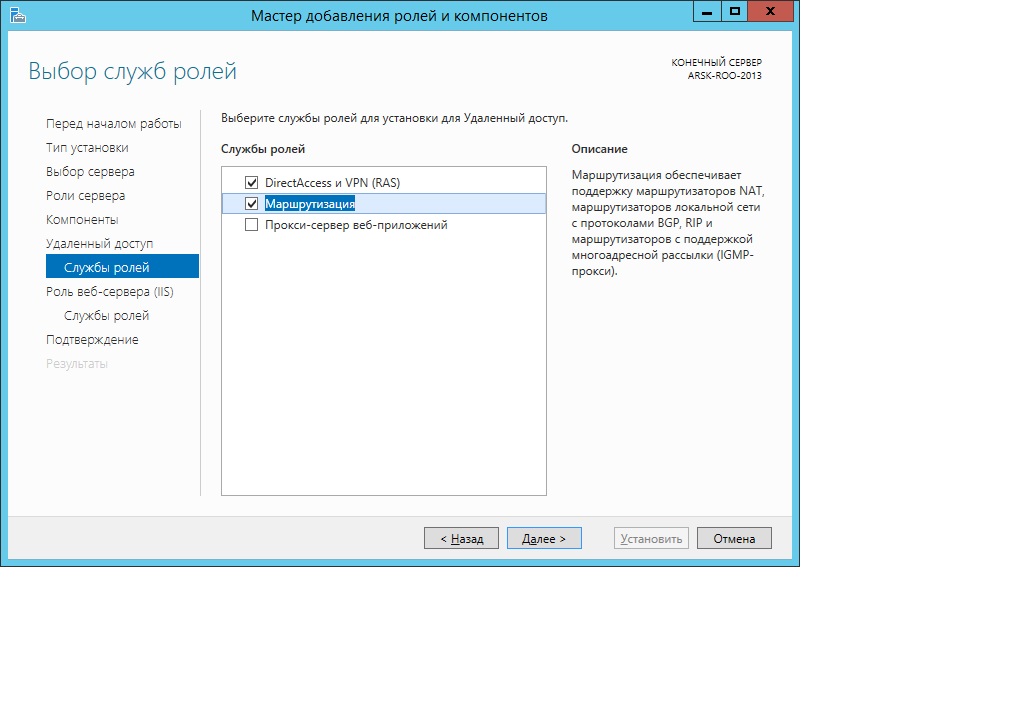
«Добавить роли и компоненты»



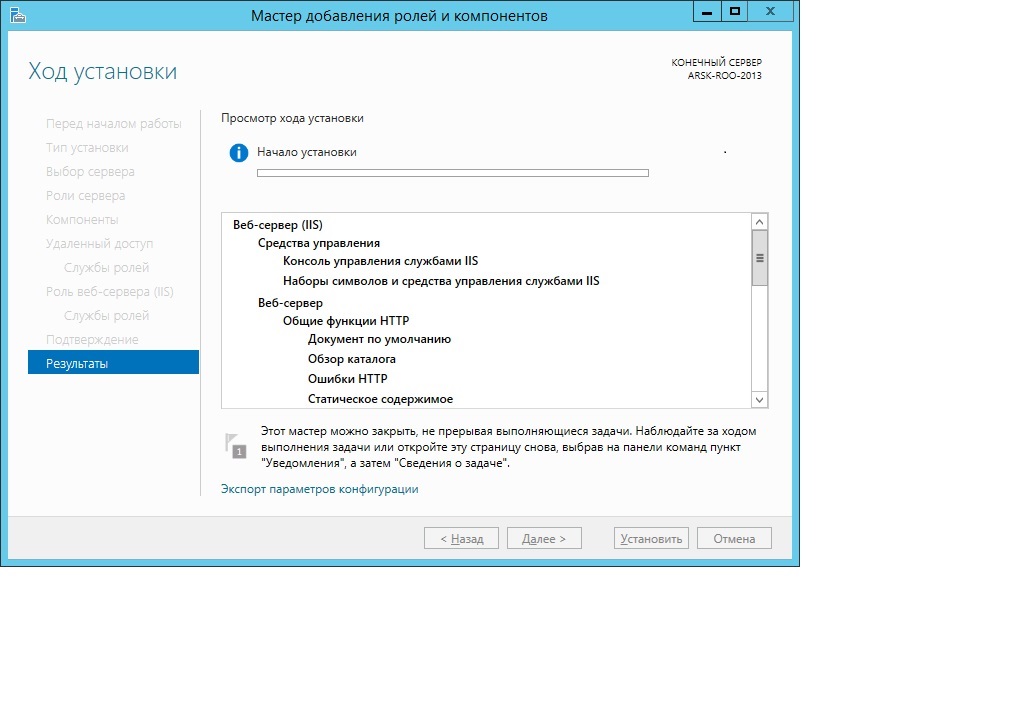
«Далее»



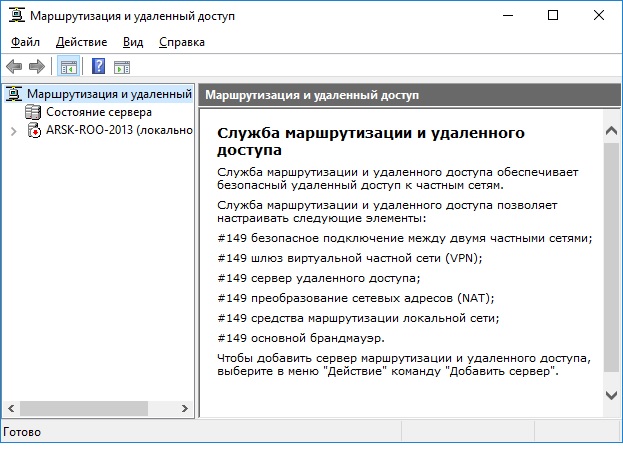
Отметить «Удаленный доступ». Далее до следующего окна:



Отметить «Маршрутизация» ( «DirectAccess и VPN (RAS)» отметится автоматически )

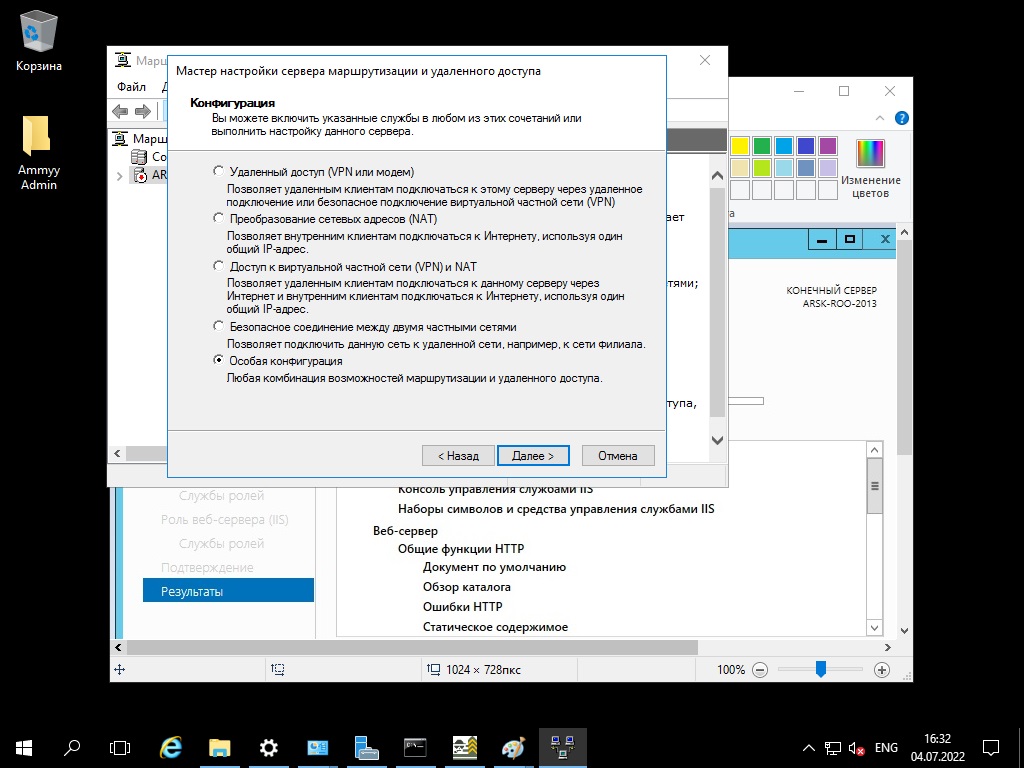


Дождаться установки компонентов

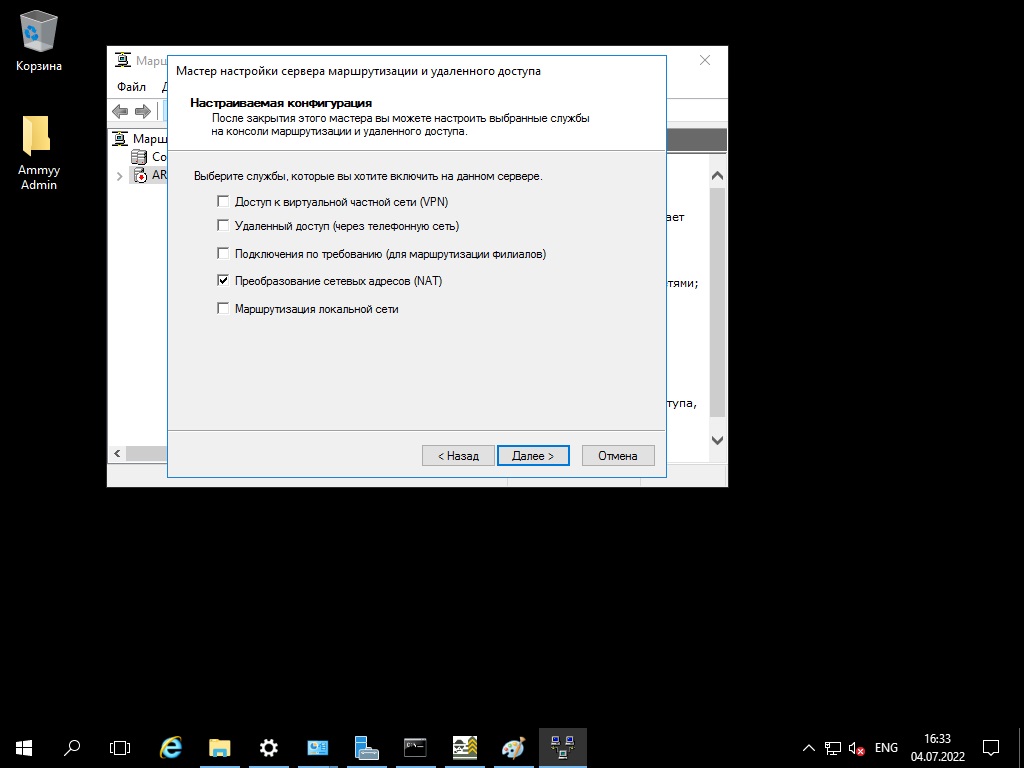


В панели управления ( Администрирование ) запустить «Маршрутизация и удаленный доступ»

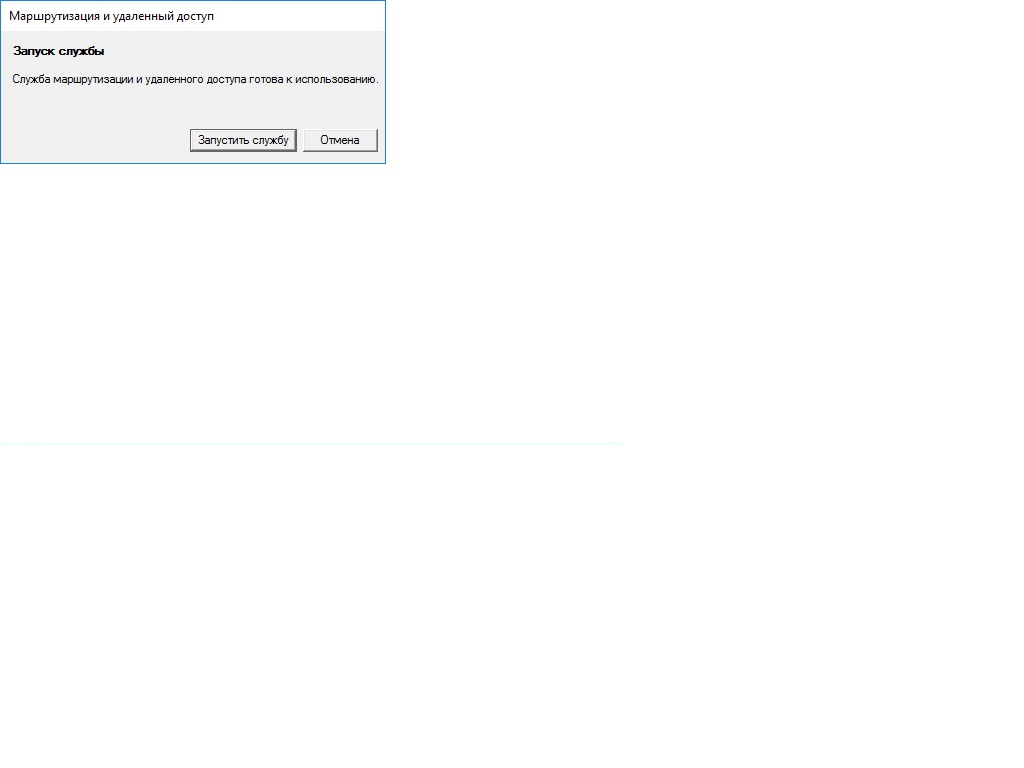
По правой кнопке мыши на сервере запустить «Настроить и включить маршрутизацию и удаленный доступ»



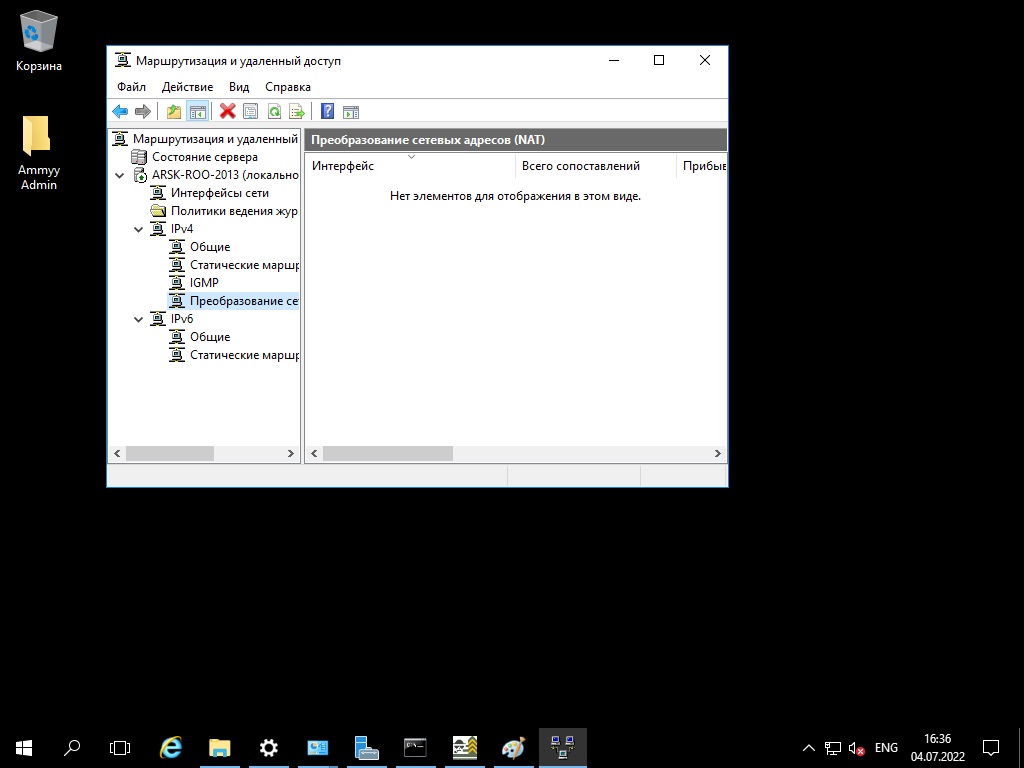
Выбрать «Особая конфигурация»



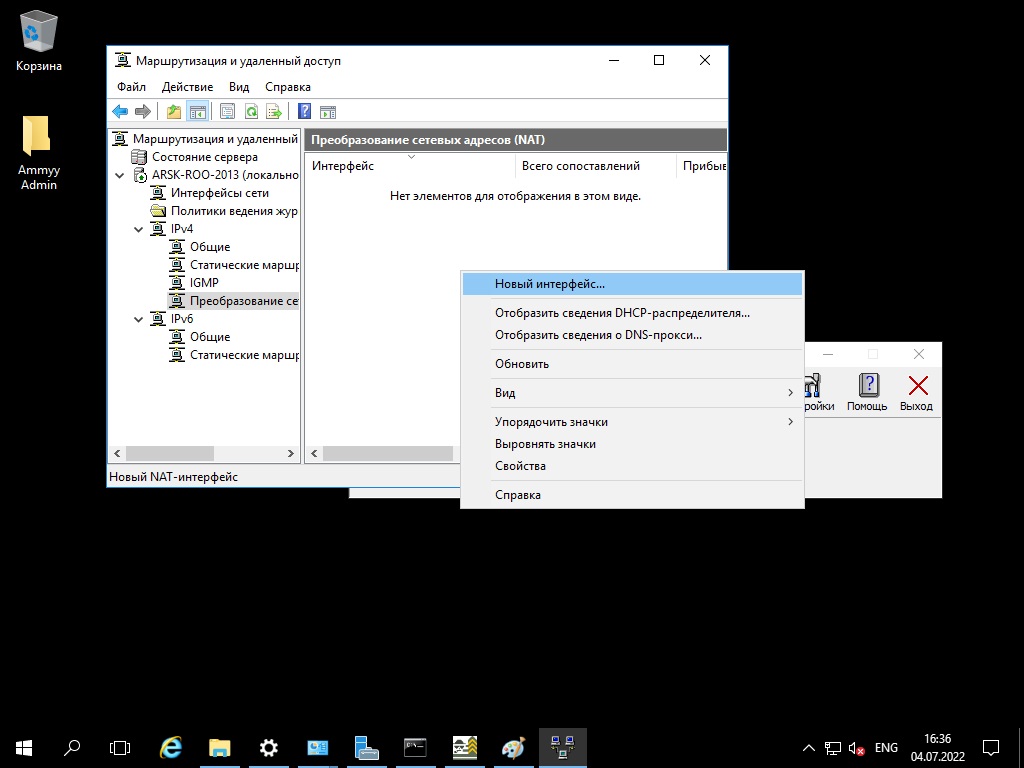
В мастере настройки выбрать «Преобразование сетевых адресов (NAT)»



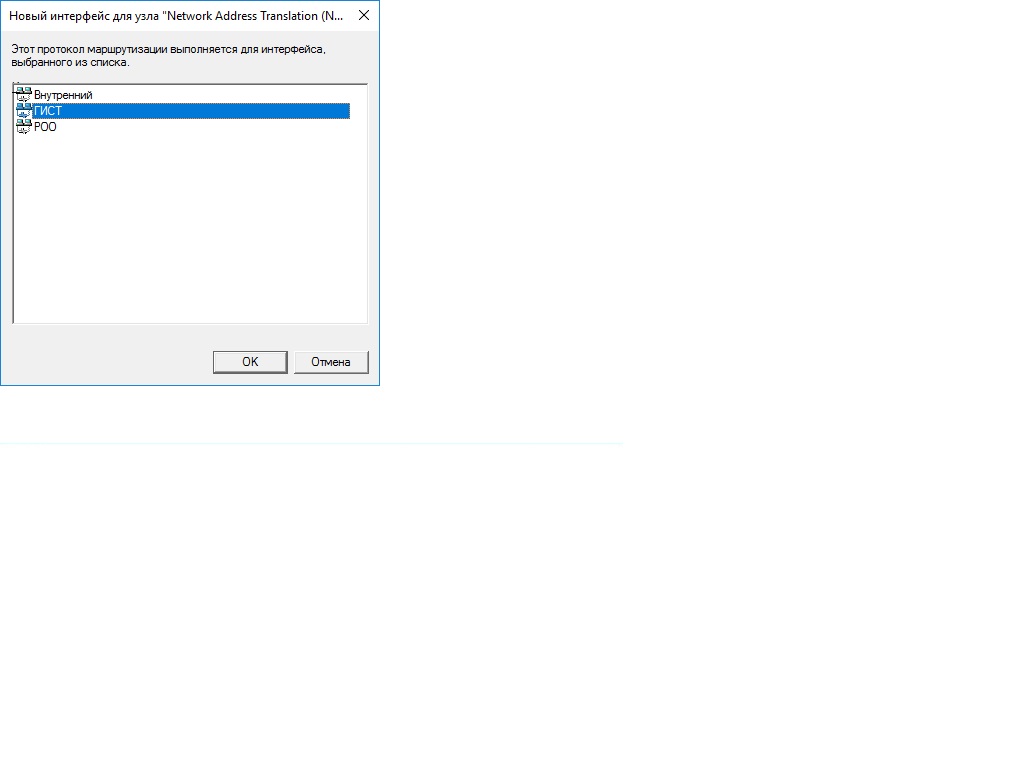
При появлении окна выбрать «Запустить службу»



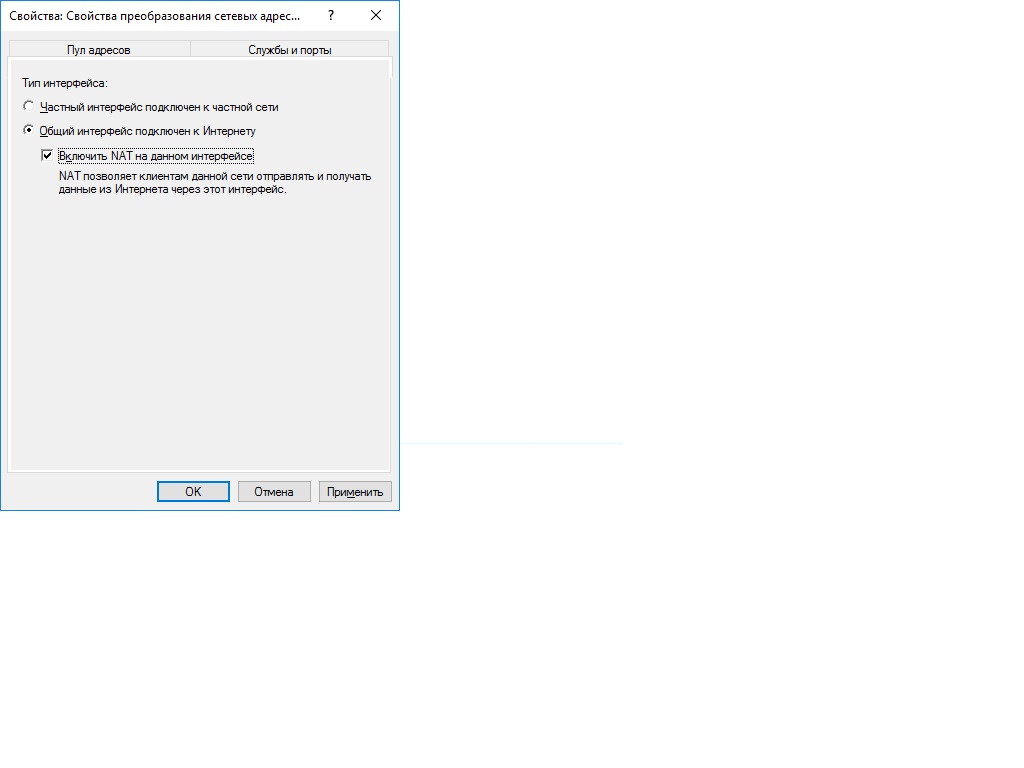
После запуска службы маршрутизации в конфигурации IPv4 ( Преобразование сетевых адресов ) в правой стороне окна по правой кнопке мыши выбрать



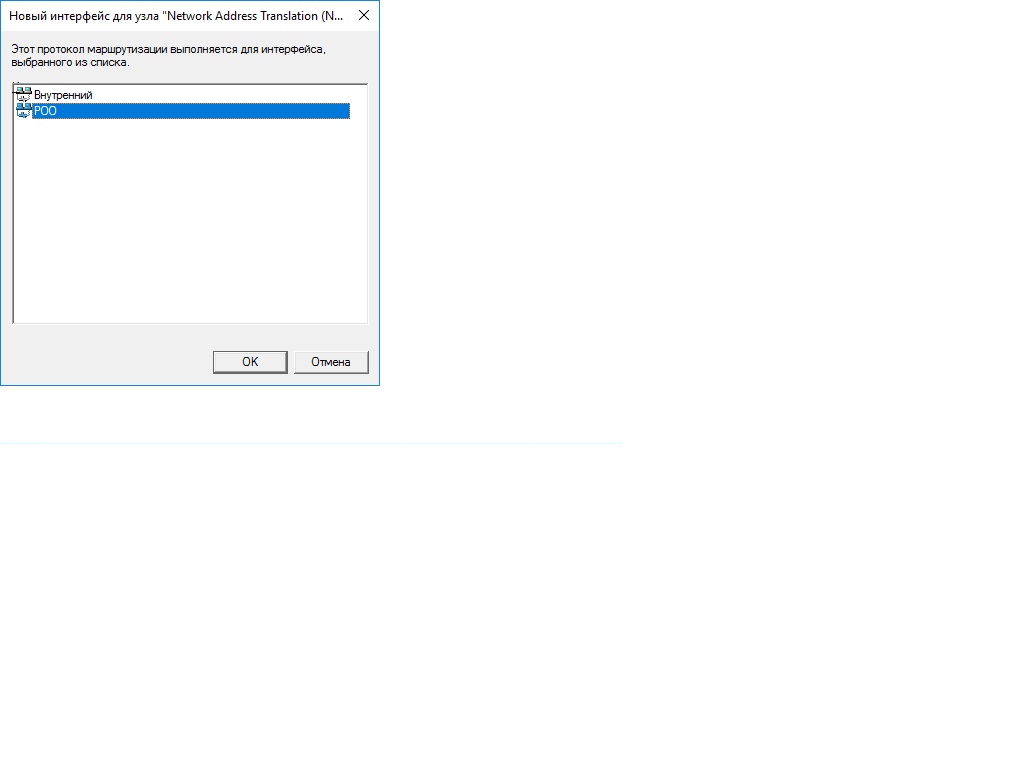
«Новый интерфейс»



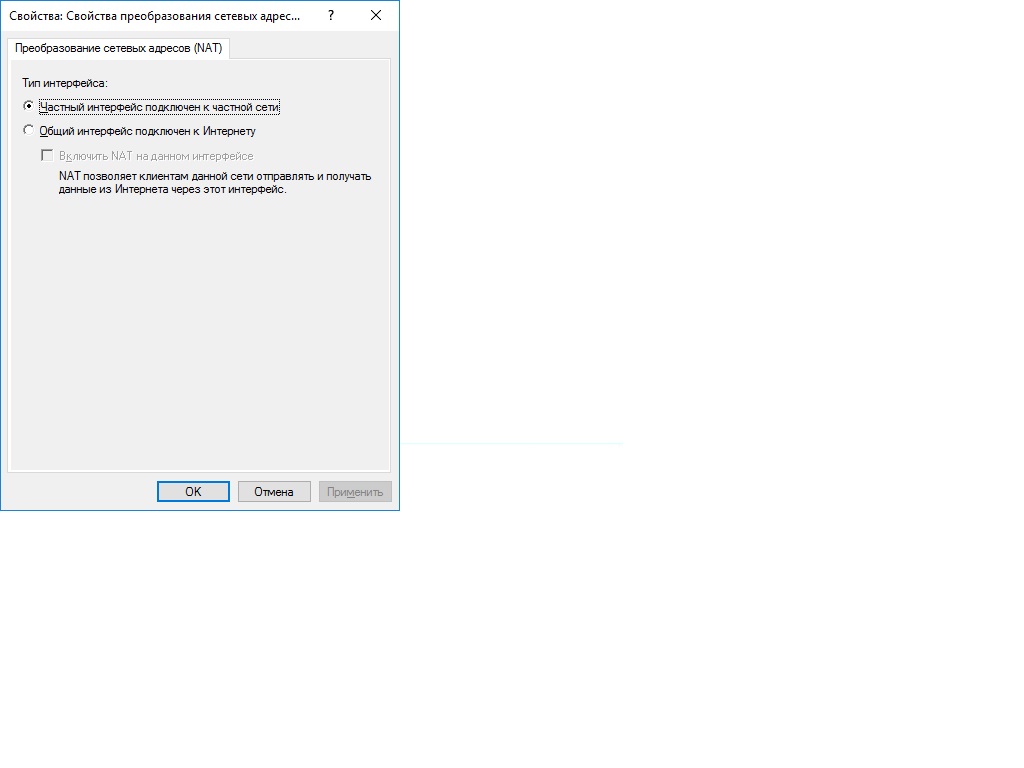
Выбрать сетевой интерфейс, подключенный к ГИСТ



Отметить как на примере



Добавить второй интерфейс ( подключенный к локальной сети )



Оставить по умолчанию ( как на примере )

Проверить доступность серверов с компьютеров в локальной сети.