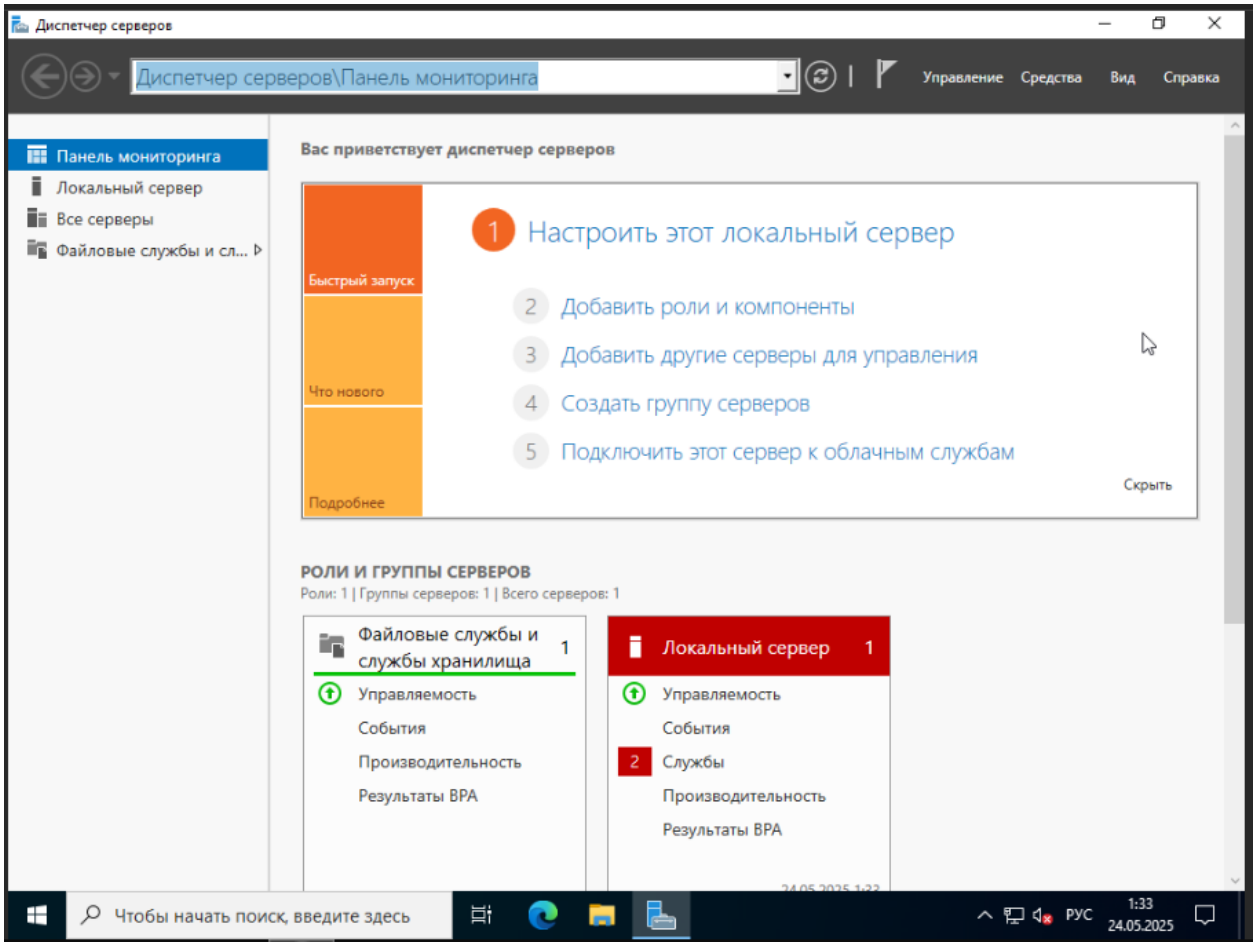
На сервере у вас будет примерно 4 адаптера:

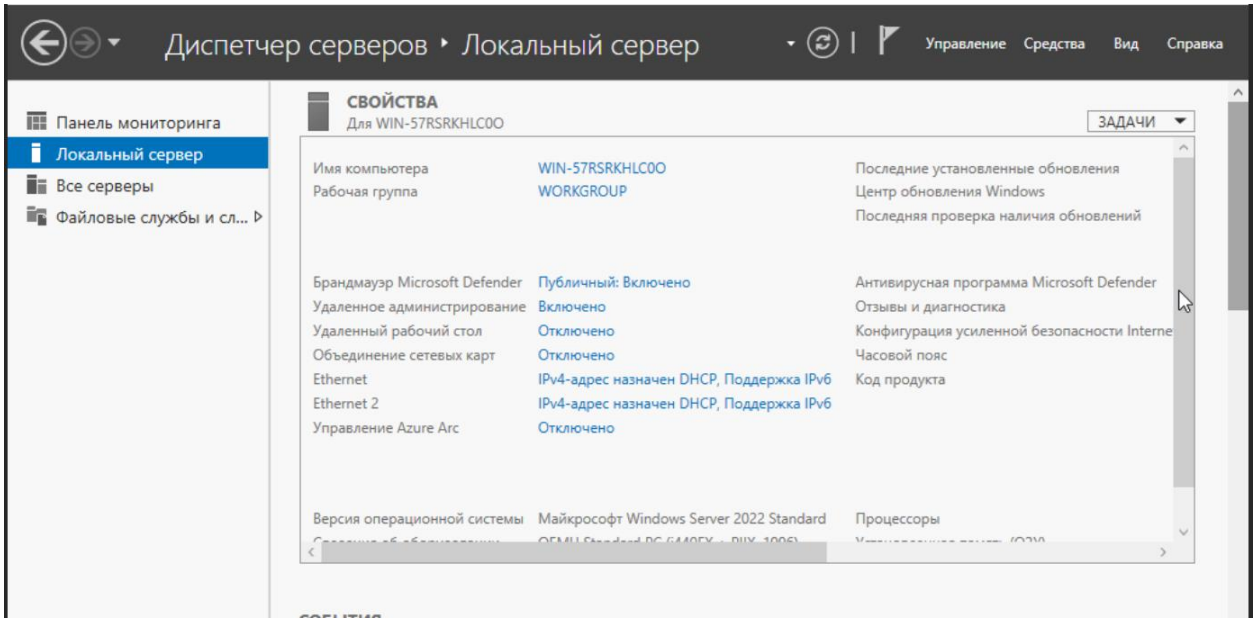
1. Для доступа в интернет
2. Для локальной сети
3. Для ЦО это 172 в методичке
4. Для впн он создаста сам после настройки впн

ВСЕ IP ВЗЯТЫ ИЗ ТЗ ДЕМОЭКЗАМЕНА, поэтому берите как у меня или ставьте в соотвествии с ТЗ ну или свои как хотите.

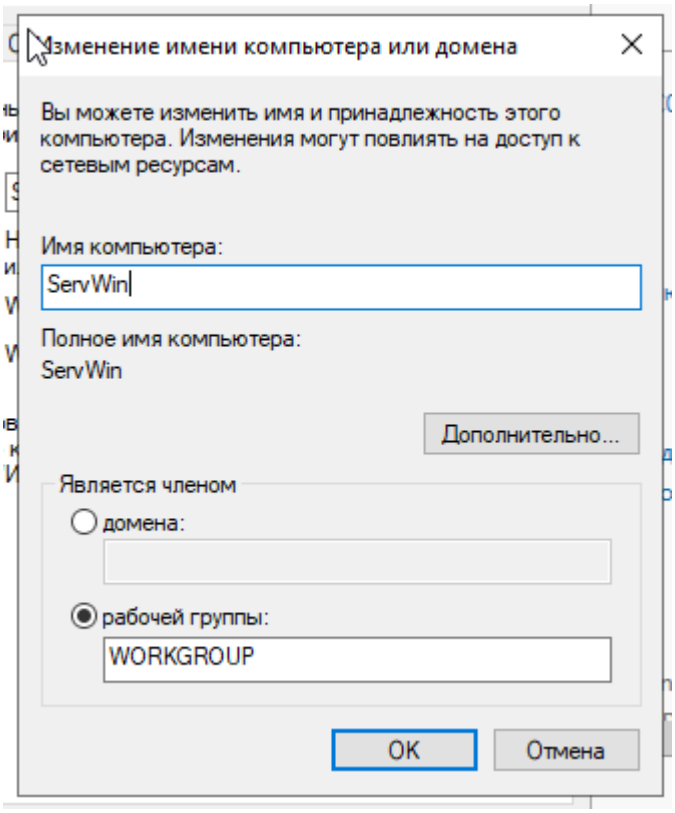
При первом запуске необходимо открыть вкладку «Локальный сервер».



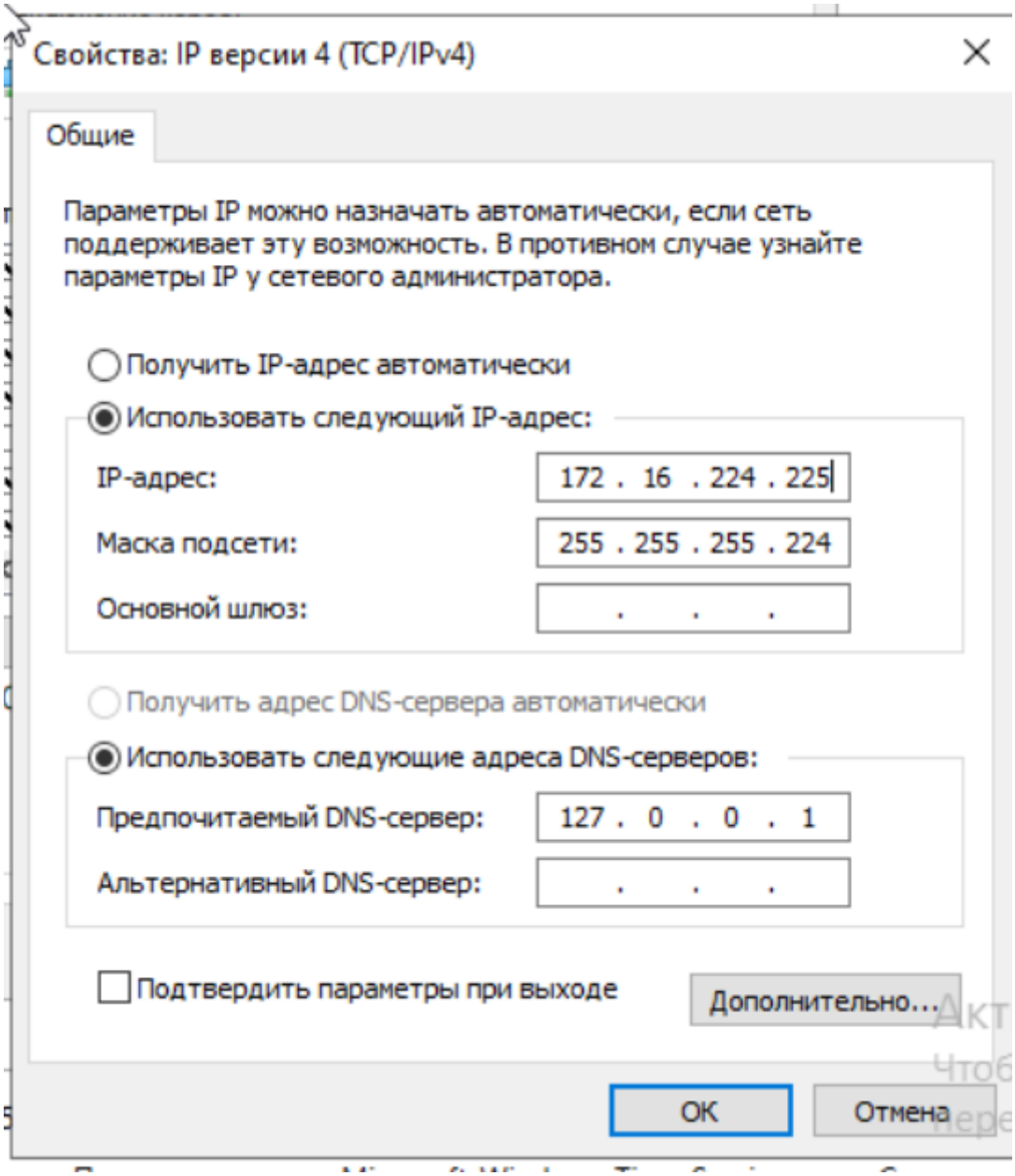
Далее необходимо изменить имя компьютера на более понятное, поэтому клацаем на имя сервера и откроется меню изменения имени сервера.



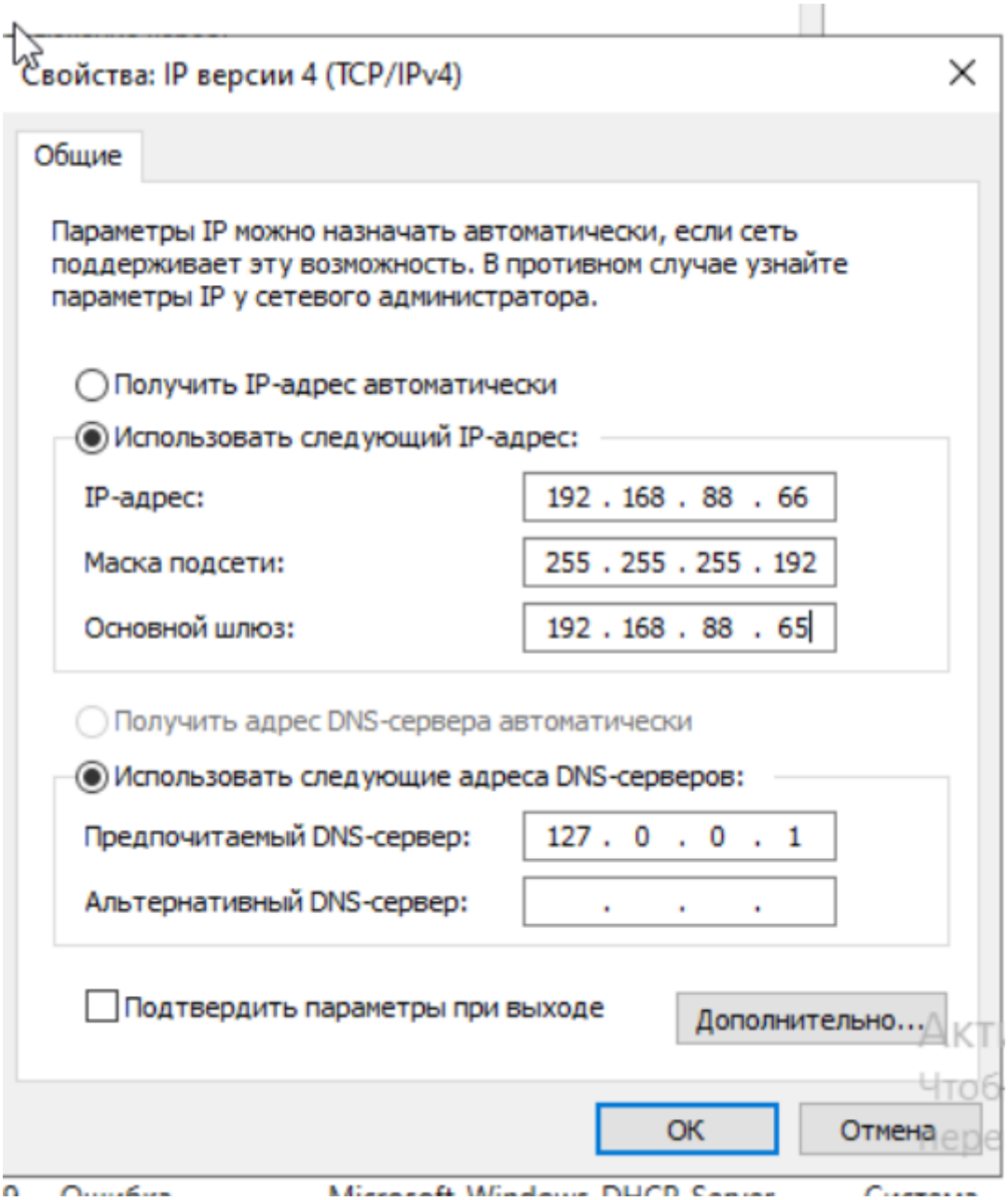
Вот тут изменяем только имя компьютера на то которое нравится или как показано ниже



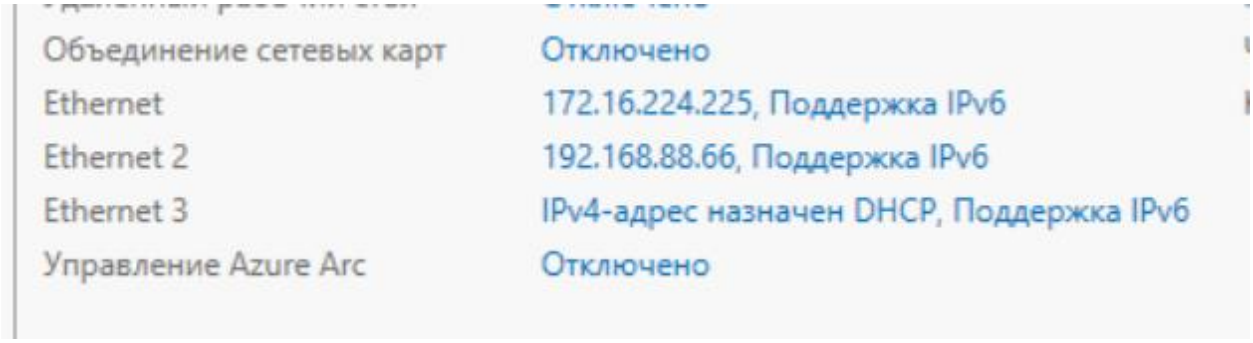
Далее на той же вкладке «Локальный сервер» необходимо указать статический ip. ВАЖНО ВНИМАТЕЛЬНО СМОТРИТЕ КУДА НАСТРАИВАЕТЕ СТАТИКУ, ибо если настроите статику на нат, то сервер не увидит клиентов, а клиенты сервер. ВНИМАТЕЛЬНО ставьте локальные сегменты, чтобы они бли одинаковы. НИЖЕ показан адрес для ЦО про который говорилось выше.



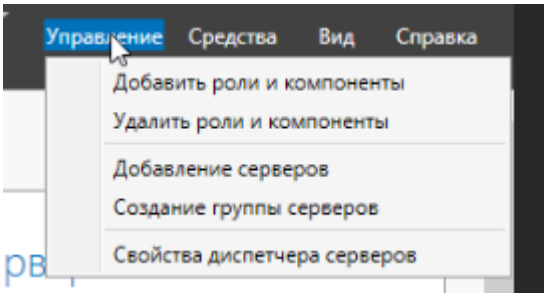
Далее необходимо настроить статику для локальной сети 1 фелиала.



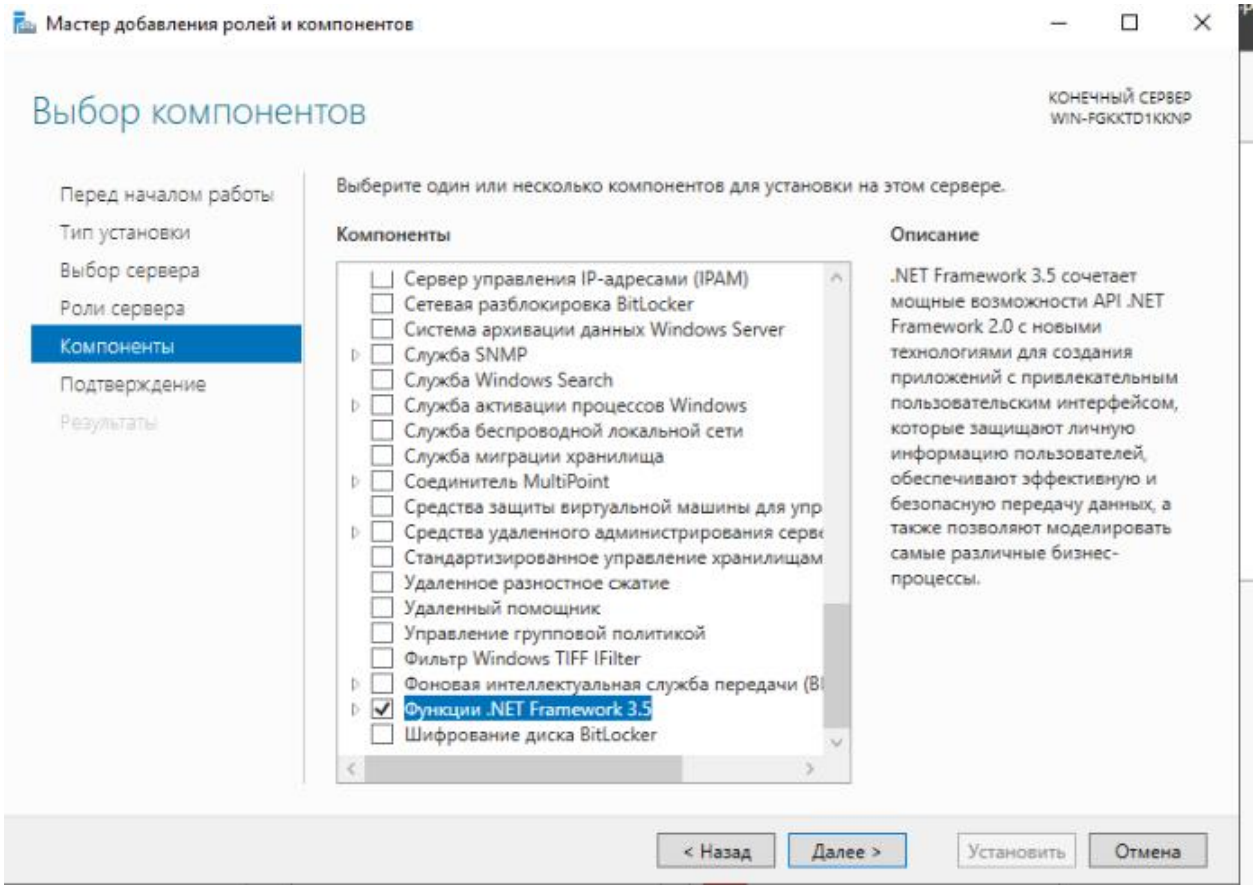
Ниже представлены измененые сетевые адаптеры, самый нижний используется для доступа в интернет.

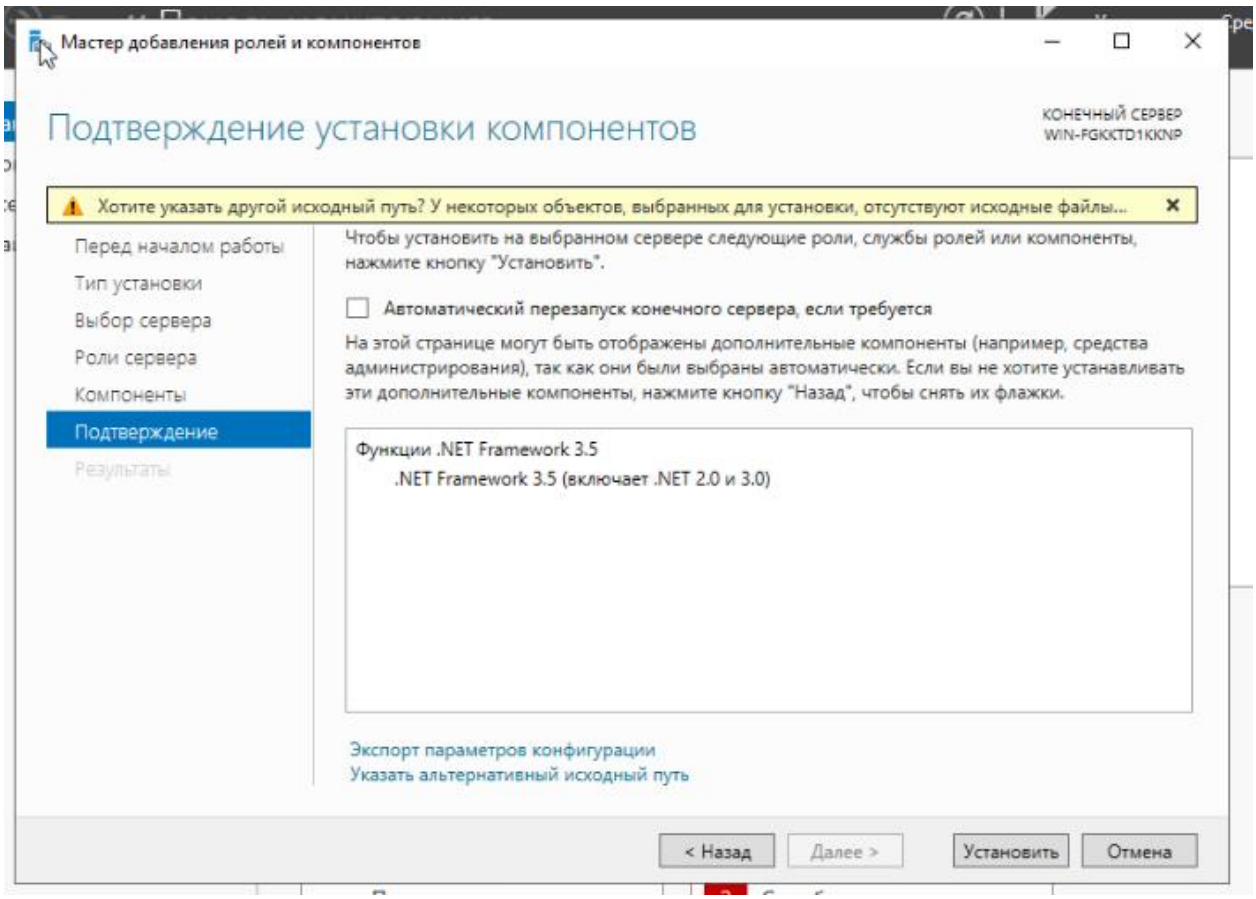


Дале в левом верхнем углу необходимо выпрать пункты «Управление» «Добавить роли и компоненты»

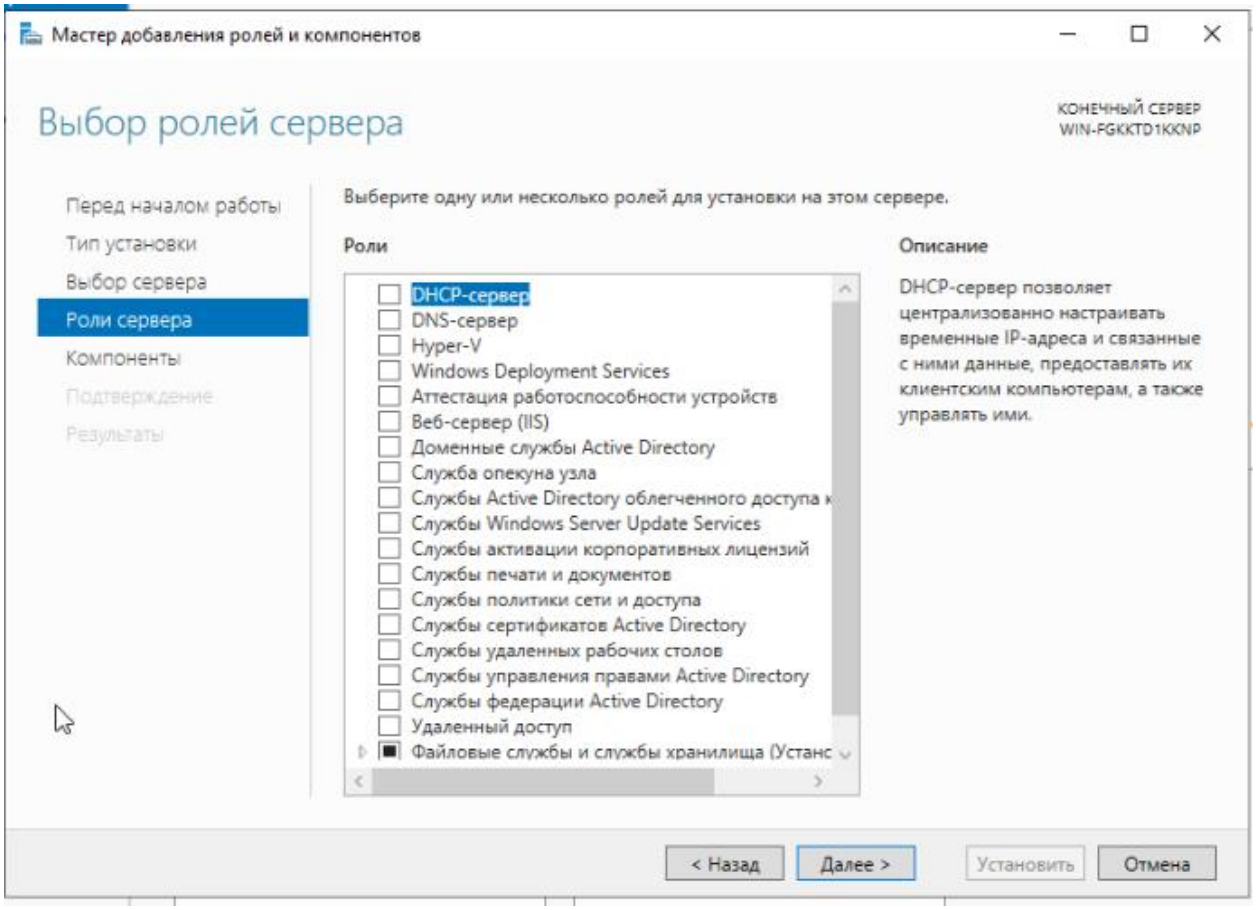


Далее на всякий случай был устоновлен компонент .NET Framework для, mySQL, Но внимательно смотрите возможно mySQL уже устоновлен на сервер и клиента. ВАЖНО Если какие то скриншоты не указаны значит там необходимо нажимать далее или Установить

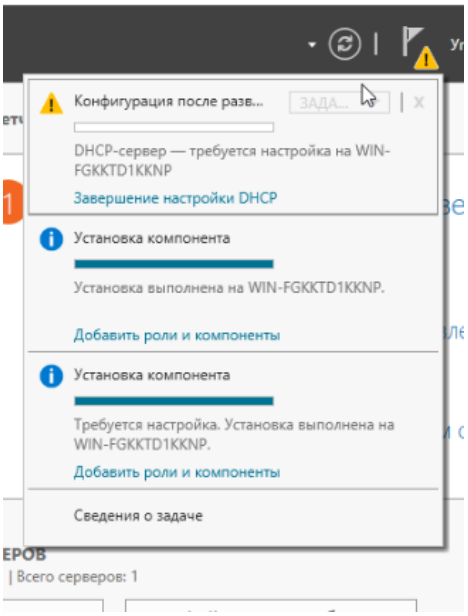




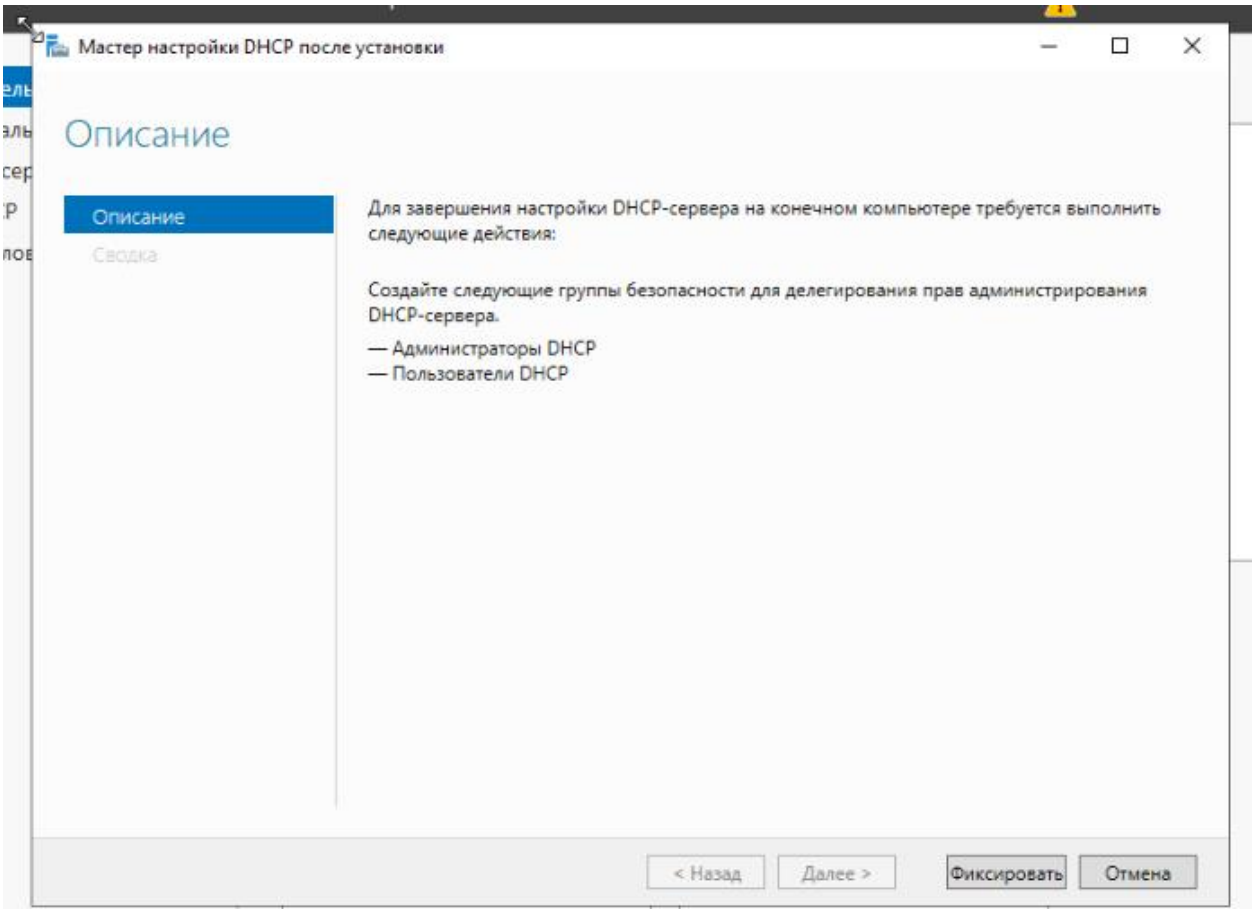
После .NET Framework необходимо установить Роль сервера DHCP



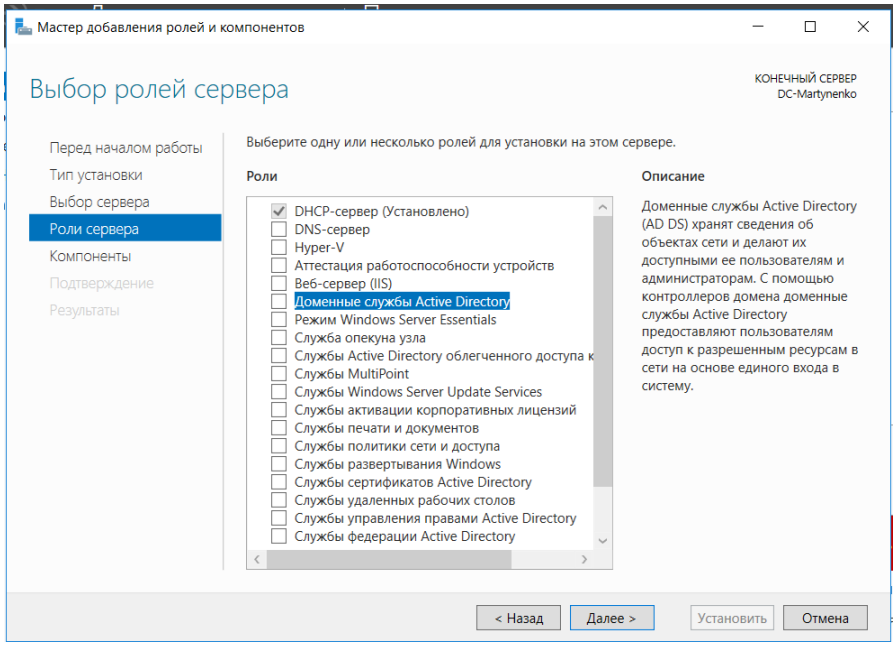
После установки в левом верхнем углу необходимо нажать на влажок с желтым треугольником и «Завершение» DHCP.



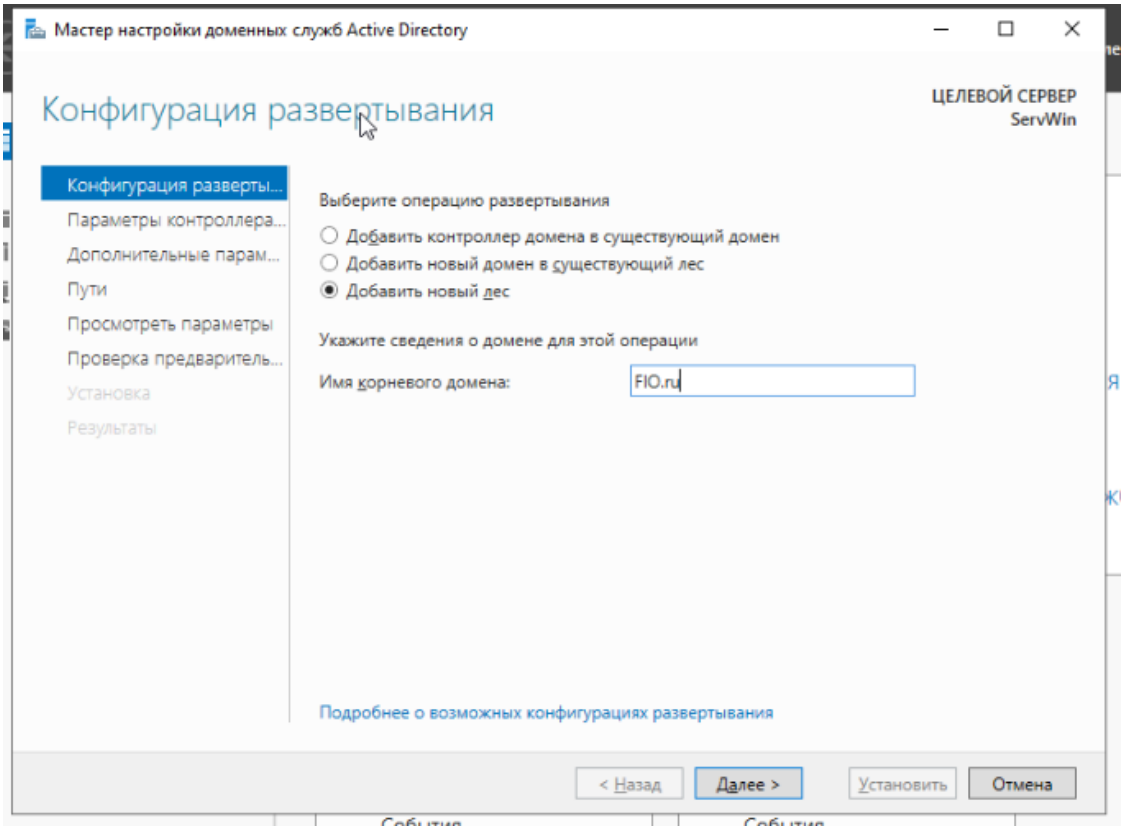
В открывшемся окне необходимо нажать «Фиксировать» затем «Далее» и закрыть.



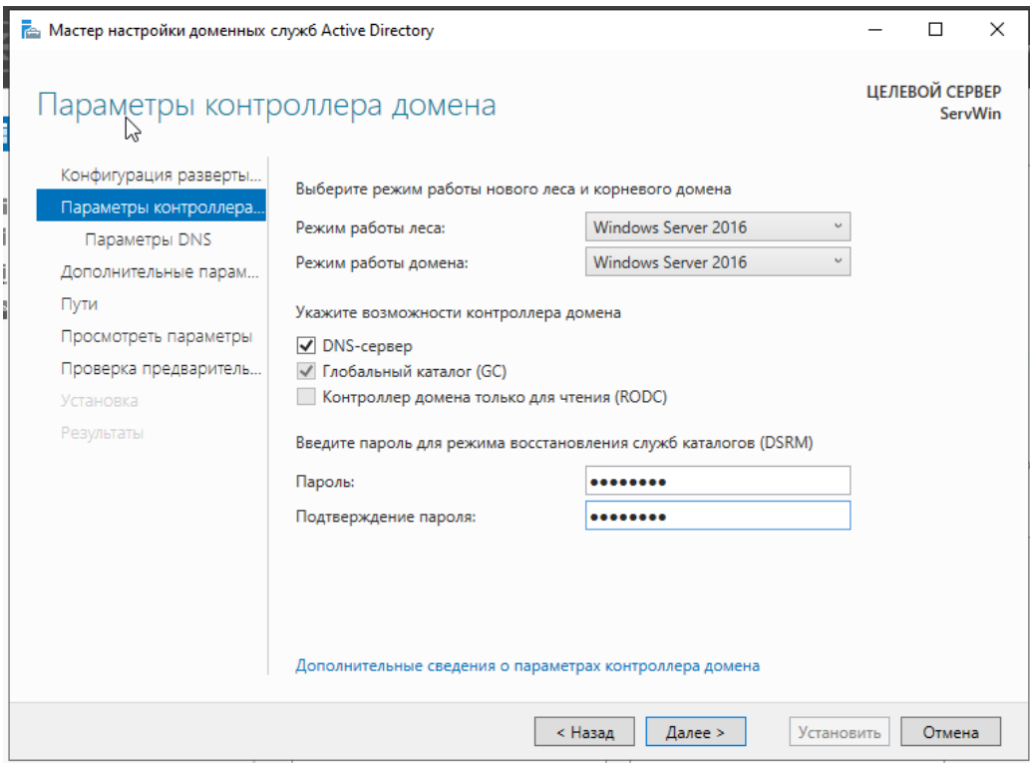
Далее так же через «Управление»-«Добавить новые роли и компоненты» необходимо выбрать роль сервера «Доменные службы Active Directory».



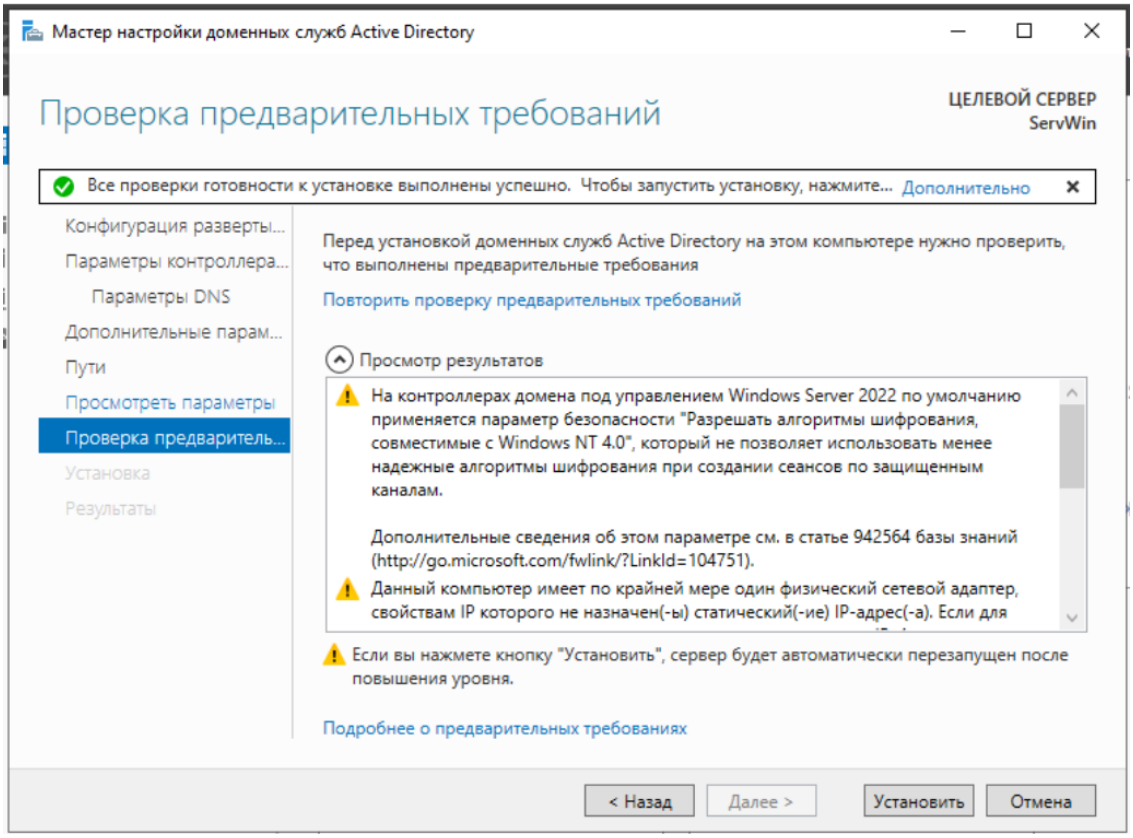
После устанвоки необходимо нажать в левом верънем углу на флажок с желтым треугольником и продолжаем установку АД. В открывшемся окне необходимо выбрать «новый лес» и Указать имя домена через точку. Примеры: Slava.ru, Lubit.com, Antona.local и так далее, после указания нажать далее.

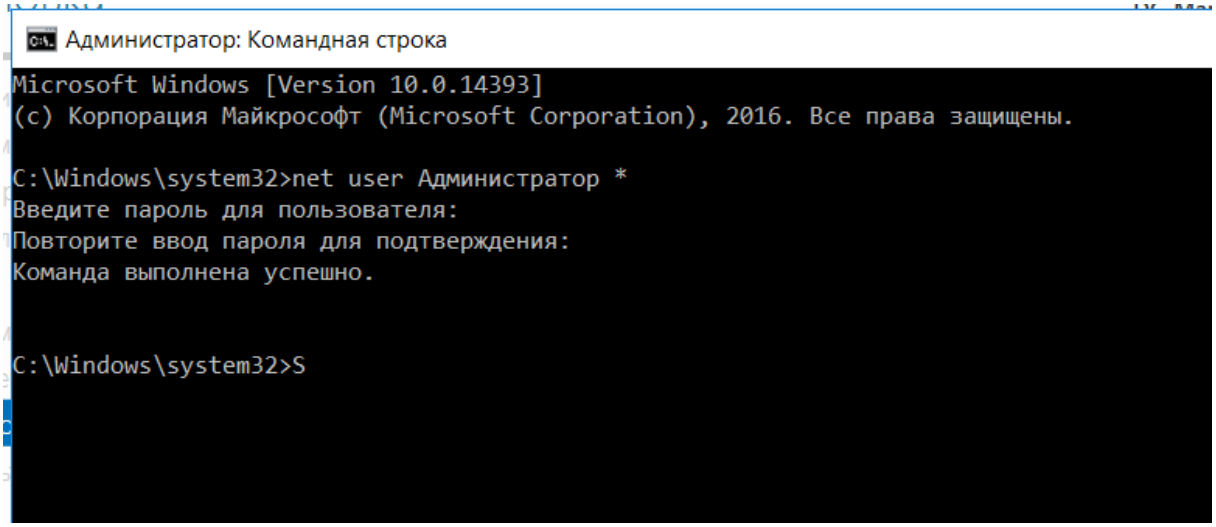


Далее необходимо просто указать пароль и далее

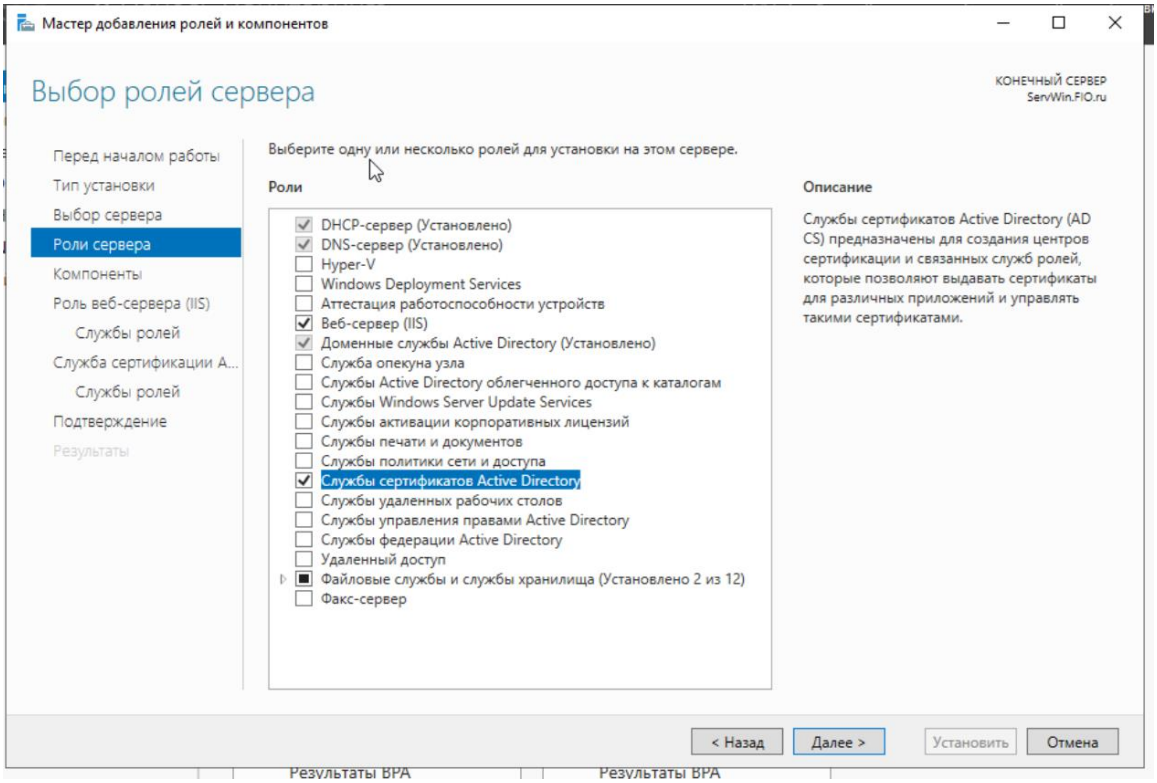


Затем прокликивыаем все окна, далее запустится проверка. ЕСЛИ ПРОВЕРКА ВЫДАЕТ ОШИБКУ значит запускаем от имени администратора командную строку и командой «net user Администратор *» меняем пароль админа на P@SSw0rd. После того как проверка пройдена необходимо нажать «Установить». После установки сервер автоматически перегрузится, для более быстрой перезагрузки можно перезагрузить сервер в ручную.

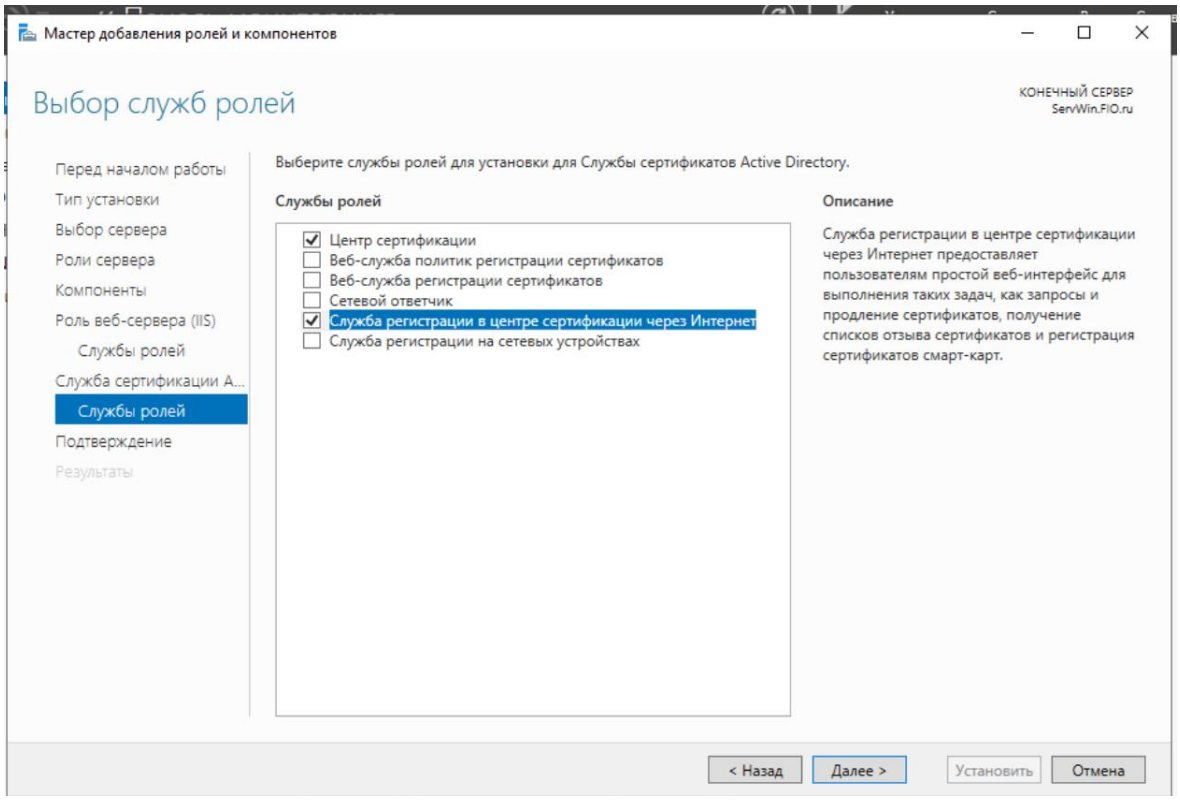

Мастер настройки доменных служб Active Directory
Проверка предварительных требований
ЦЕЛЕВОЙ СЕРВЕР
ServWin
Все проверки готовности к установке выполнены успешно. Чтобы запустить установку, нажмите...
Дополнительно
Конфигурация разверты...
Параметры контроллера...
Параметры DNS
Дополнительные парам...
Пути
Просмотреть параметры
Проверка предваритель...
Установка
Результаты
Перед установкой доменных служб Active Directory на этом компьютере нужно проверить, что выполнены предварительные требования
Повторить проверку предварительных требований
Просмотр результатов
На контроллерах домена под управлением Windows Server 2022 по умолчанию применяется параметр безопасности "Разрешать алгоритмы шифрования, совместимые с Windows NT 4.0", который не позволяет использовать менее надежные алгоритмы шифрования при создании сеансов по защищенным каналам.
Дополнительные сведения об этом параметре см. в статье 942564 базы знаний (http://go.microsoft.com/fwlink/?LinkId=104751).
Данный компьютер имеет по крайней мере один физический сетевой адаптер, свойствам IP которого не назначен(-ы) статический(-ие) IP-адрес(-а). Если для
Если вы нажмете кнопку "Установить", сервер будет автоматически перезапущен после повышения уровня.
Подробнее о предварительных требованиях
< Назад
Далее >
Установить
Отмена


Администратор: Командная строка
Microsoft Windows [Version 10.0.14393]
(c) Корпорация Майкрософт (Microsoft Corporation), 2016. Все права защищены.
C:\Windows\system32>net user Администратор *
Введите пароль для пользователя:
Повторите ввод пароля для подтверждения:
Команда выполнена успешно.
C:\Windows\system32>S

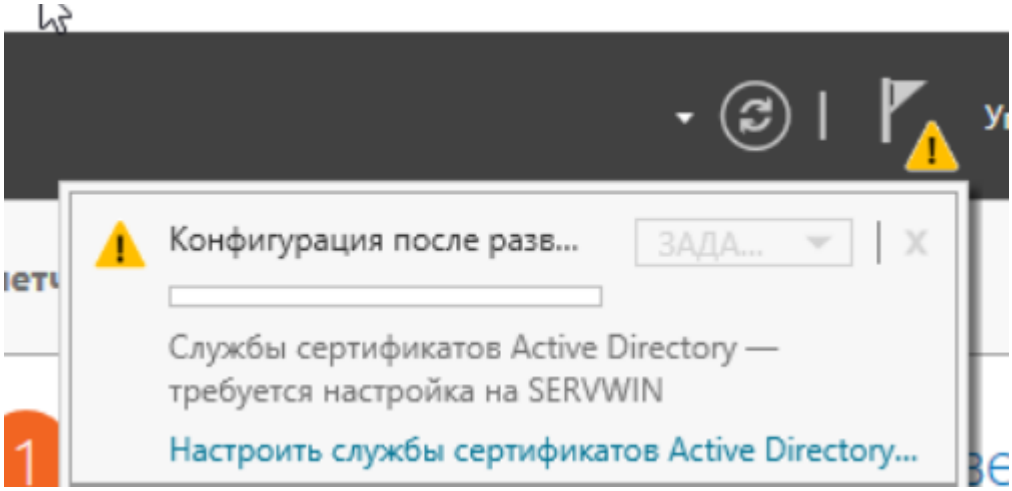
Далее необходимо установить роль «Службы сертификатов Active Directory»



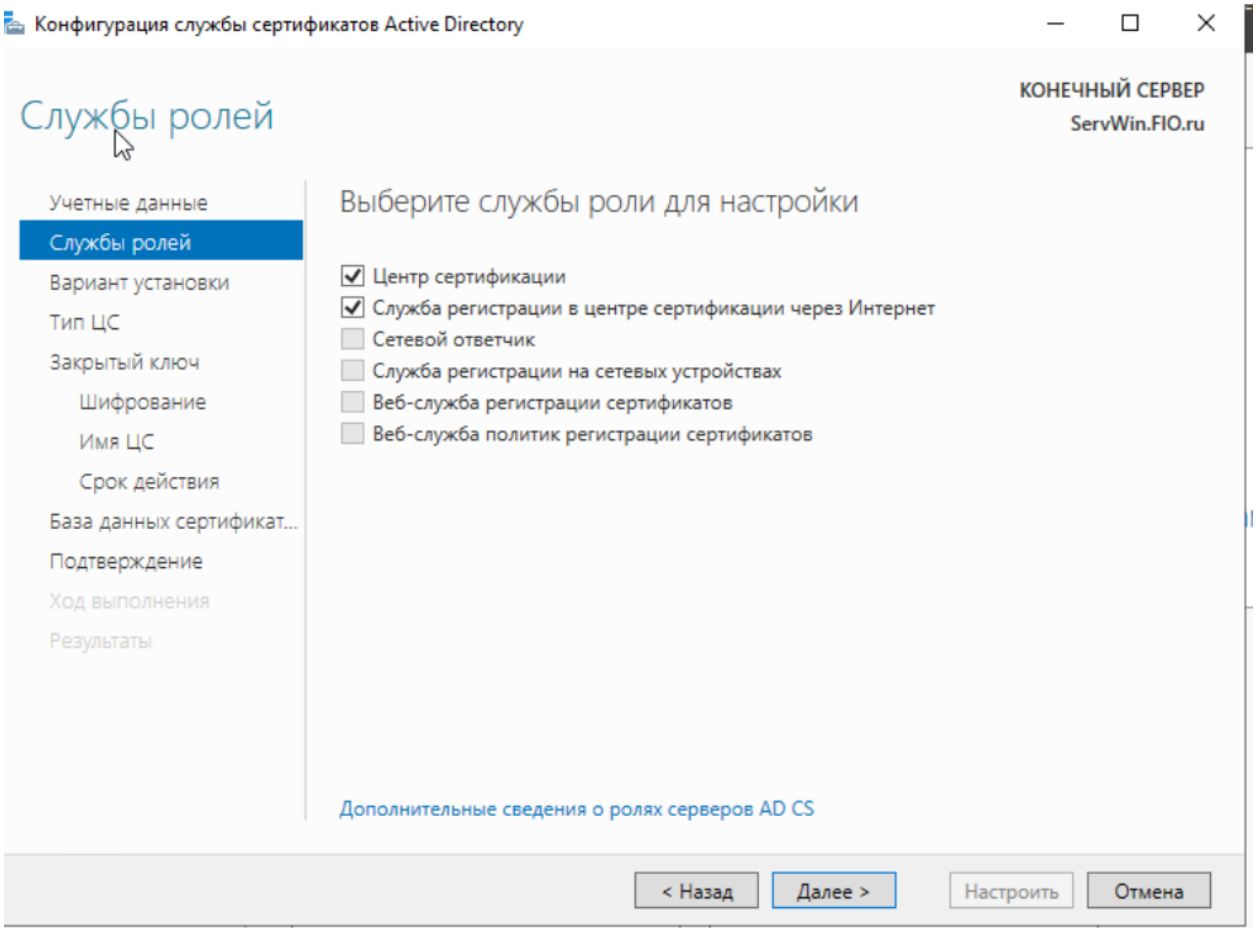
Далее в службы ролей необходимо выбрать пункты «Центр сертификации» и «Службы регистрации в центре сертификации через Интернет»

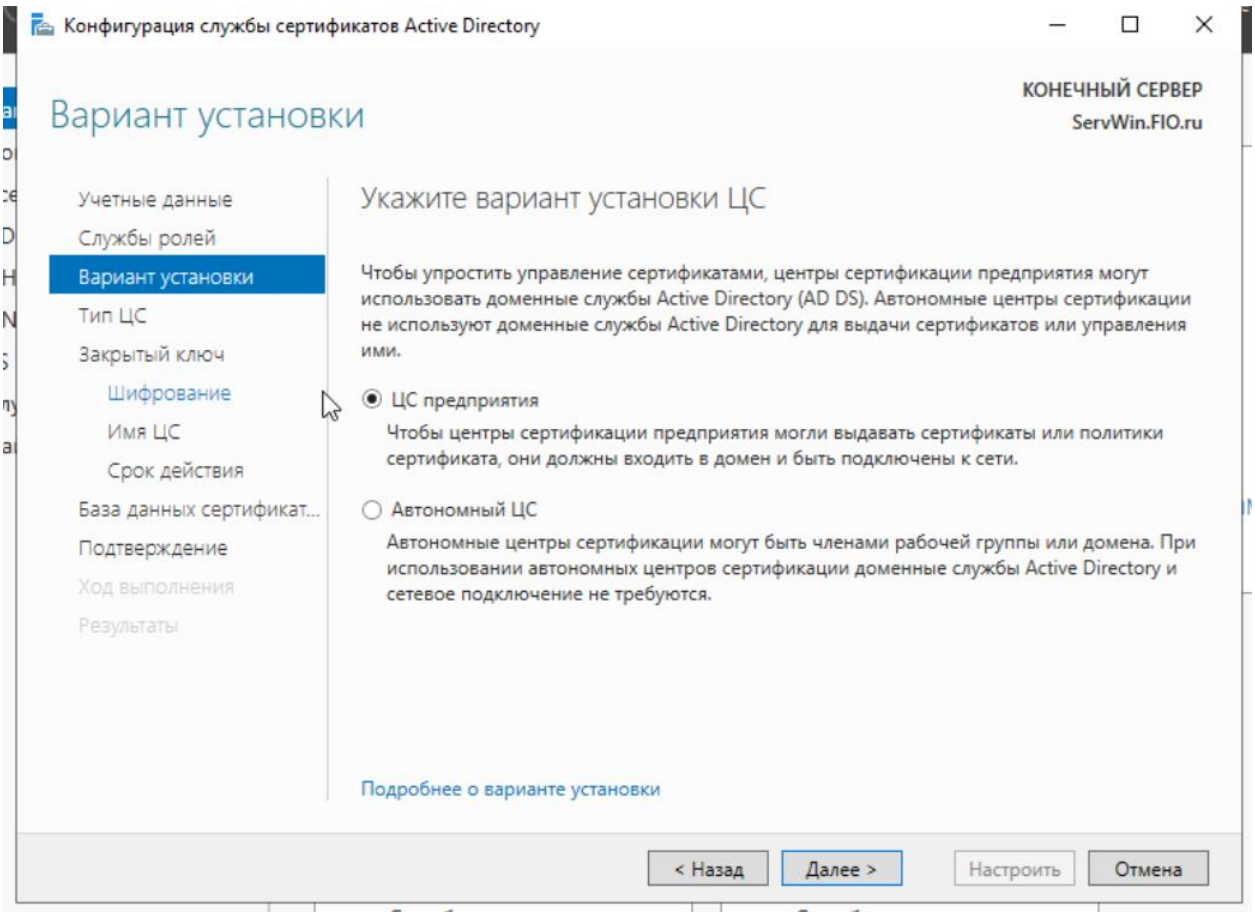


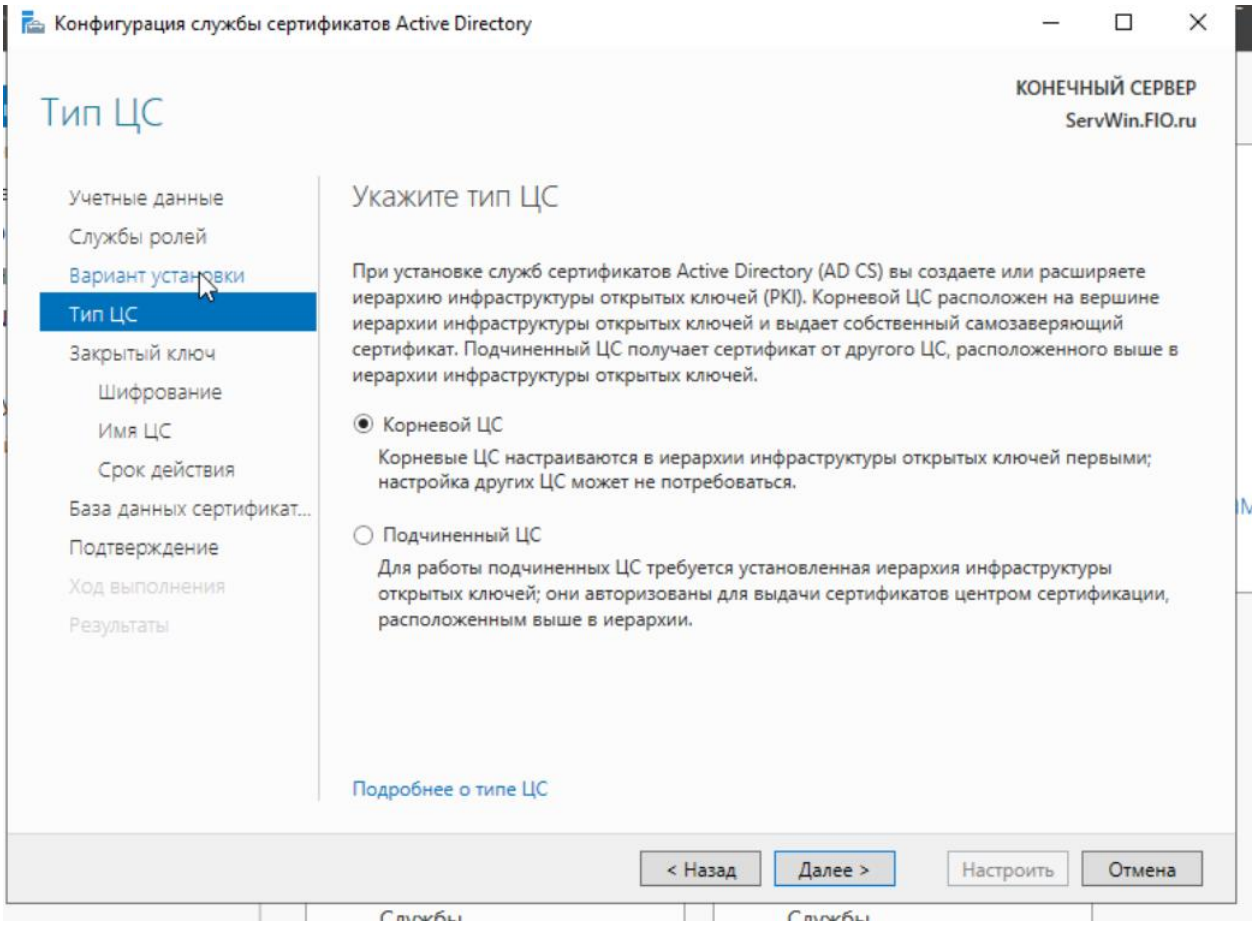
Далее необходимо нажать на флажок с желтым треугольником и выбрать «Настроить службы сертивикатов AD»

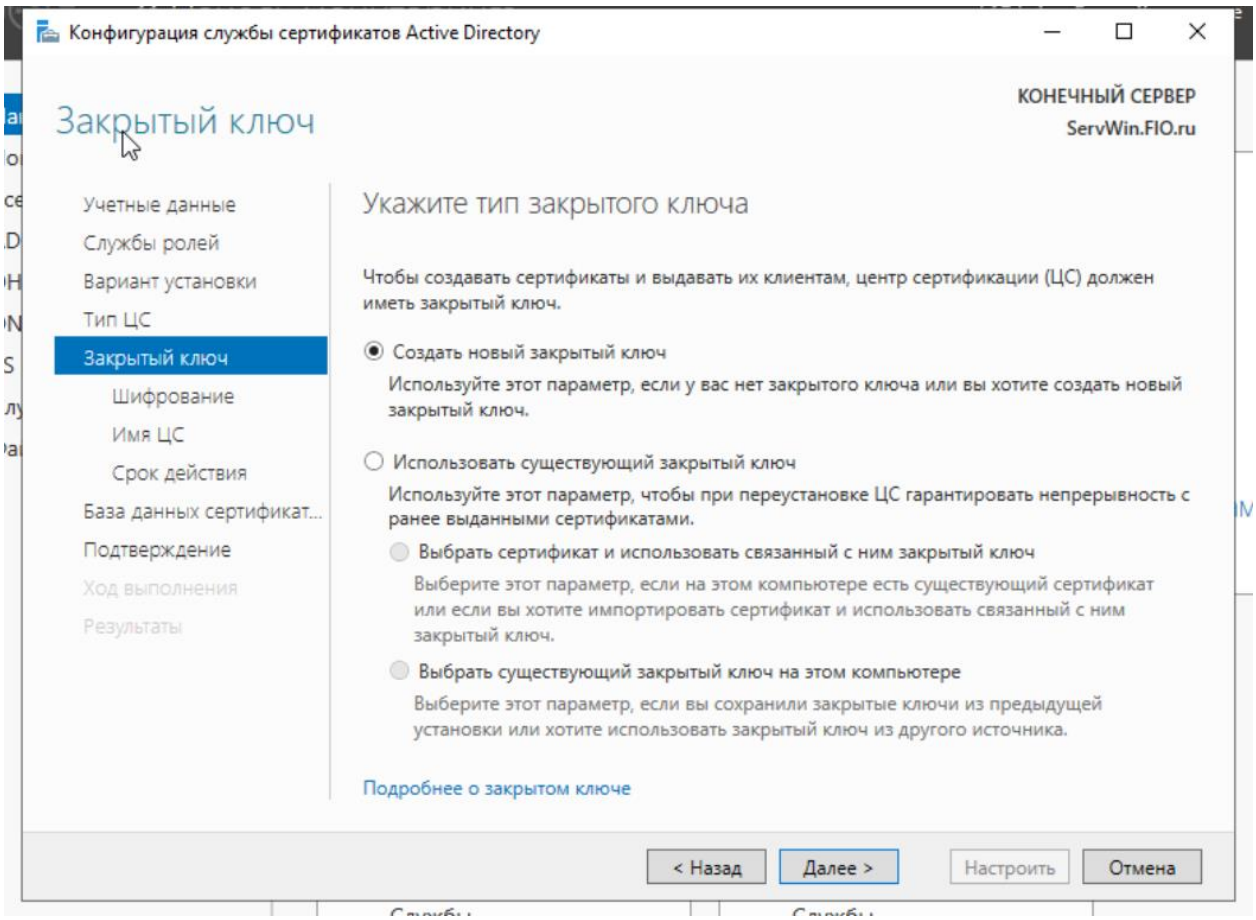


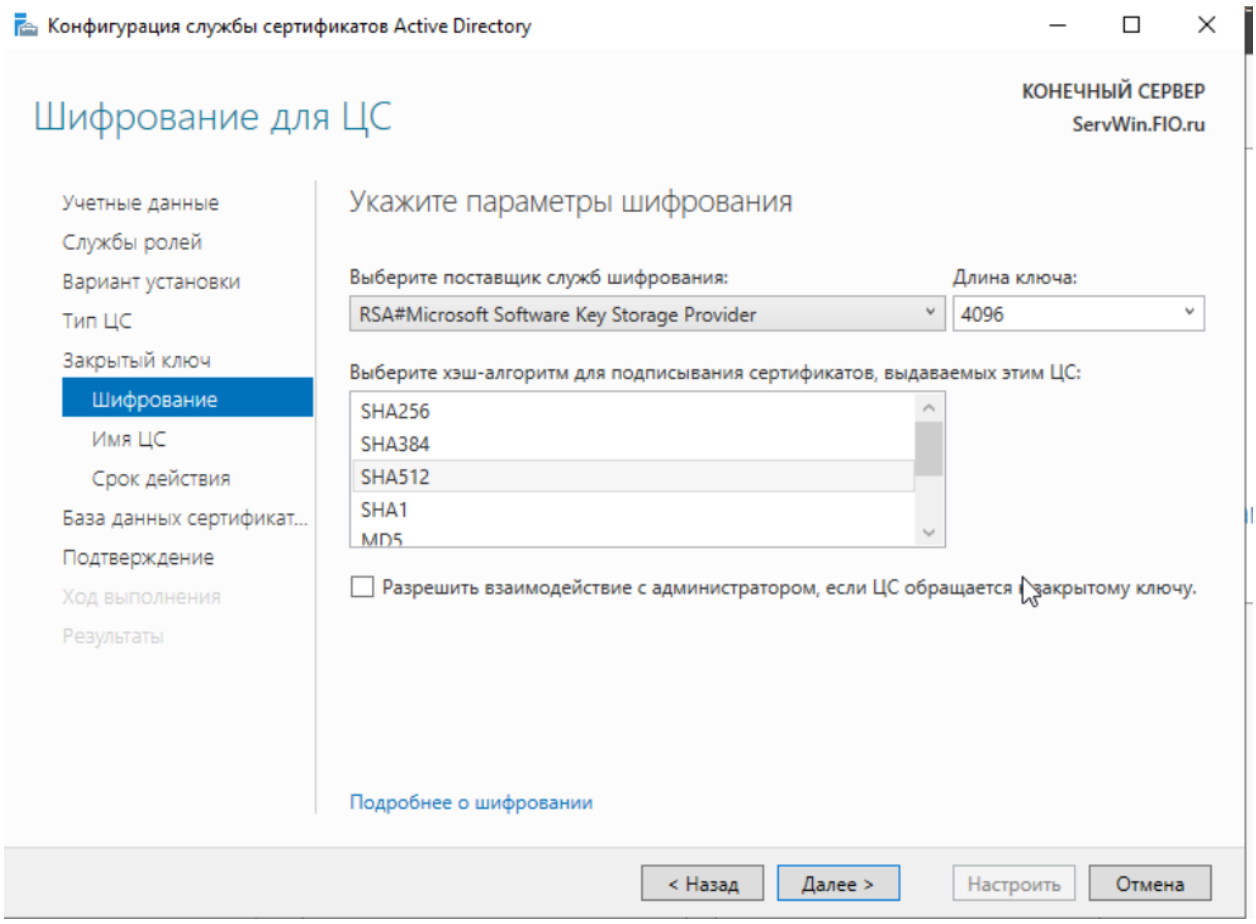
Далее необходимо указывать так же как показано ниже на скриншотах.

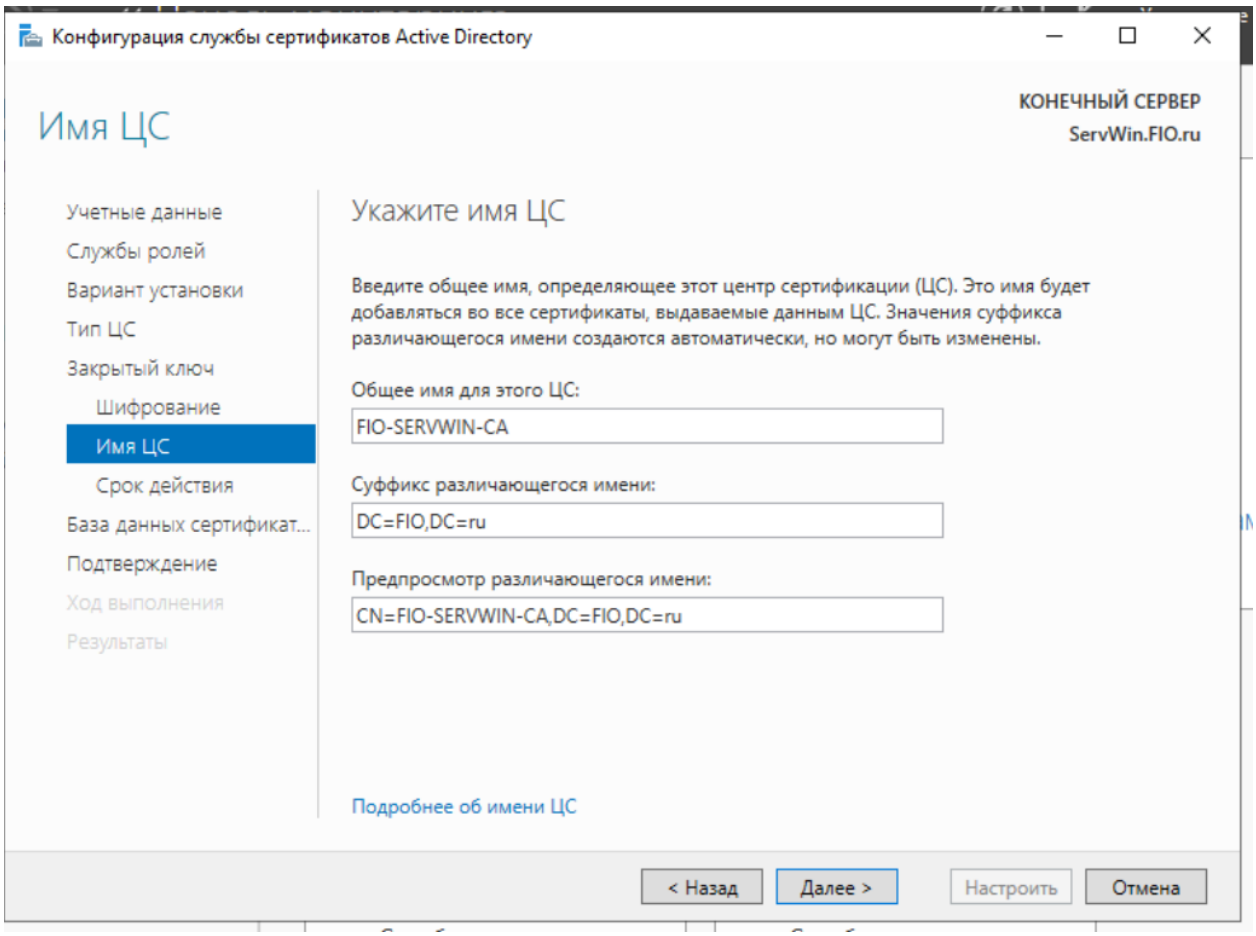


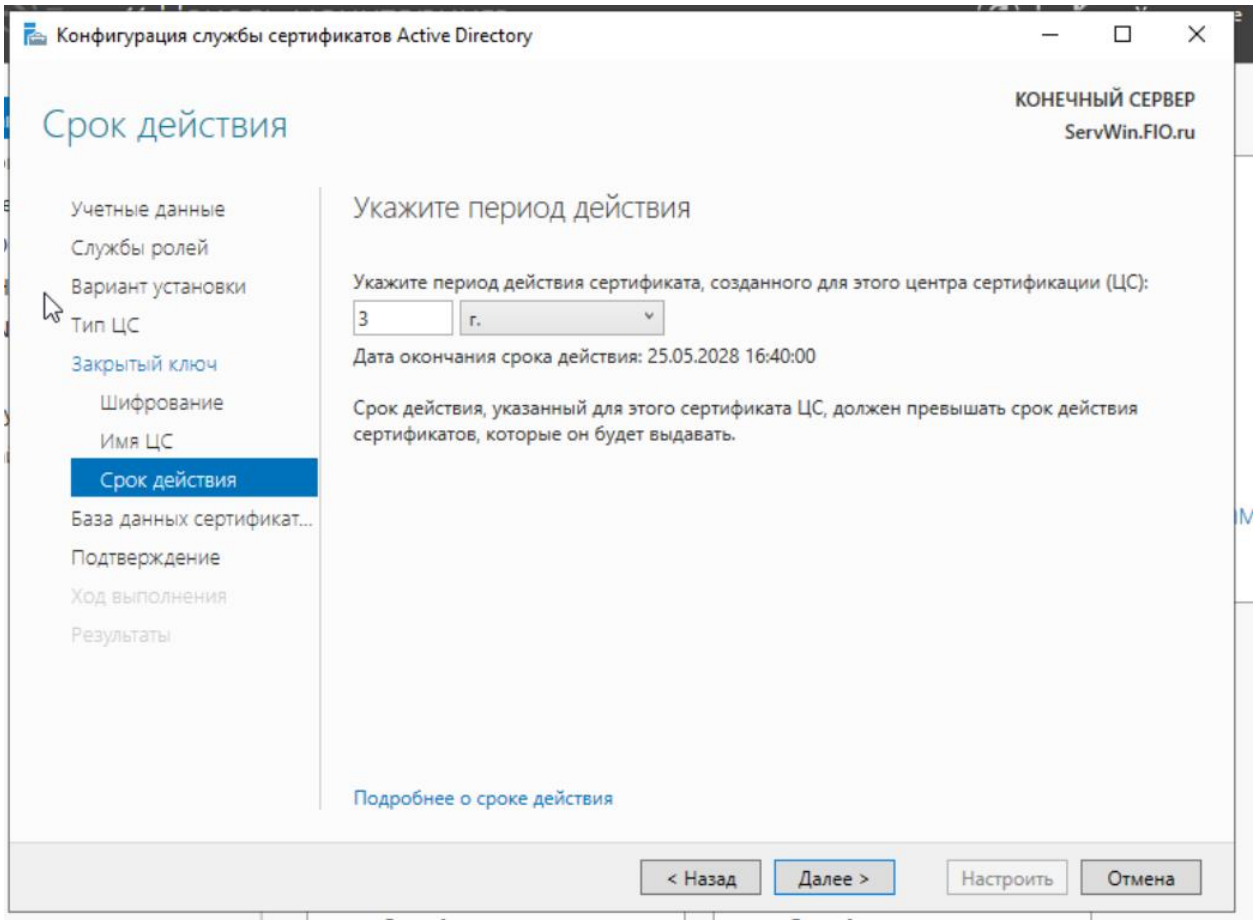

Конфигурация службы сертификатов Active Directory
Вариант установки
КОНЕЧНЫЙ СЕРВЕР
ServWin.FIO.ru
Учетные данные
Службы ролей
Вариант установки
Тип ЦС
Закрытый ключ
Шифрование
Имя ЦС
Срок действия
База данных сертификат...
Подтверждение
Ход выполнения
Результаты
Укажите вариант установки ЦС
Чтобы упростить управление сертификатами, центры сертификации предприятия могут использовать доменные службы Active Directory (AD DS). Автономные центры сертификации не используют доменные службы Active Directory для выдачи сертификатов или управления ими.
ЦС предприятия
Чтобы центры сертификации предприятия могли выдавать сертификаты или политики сертификата, они должны входить в домен и быть подключены к сети.
Автономный ЦС
Автономные центры сертификации могут быть членами рабочей группы или домена. При использовании автономных центров сертификации доменные службы Active Directory и сетевое подключение не требуются.
Подробнее о варианте установки
< Назад
Далее >
Настроить
Отмена

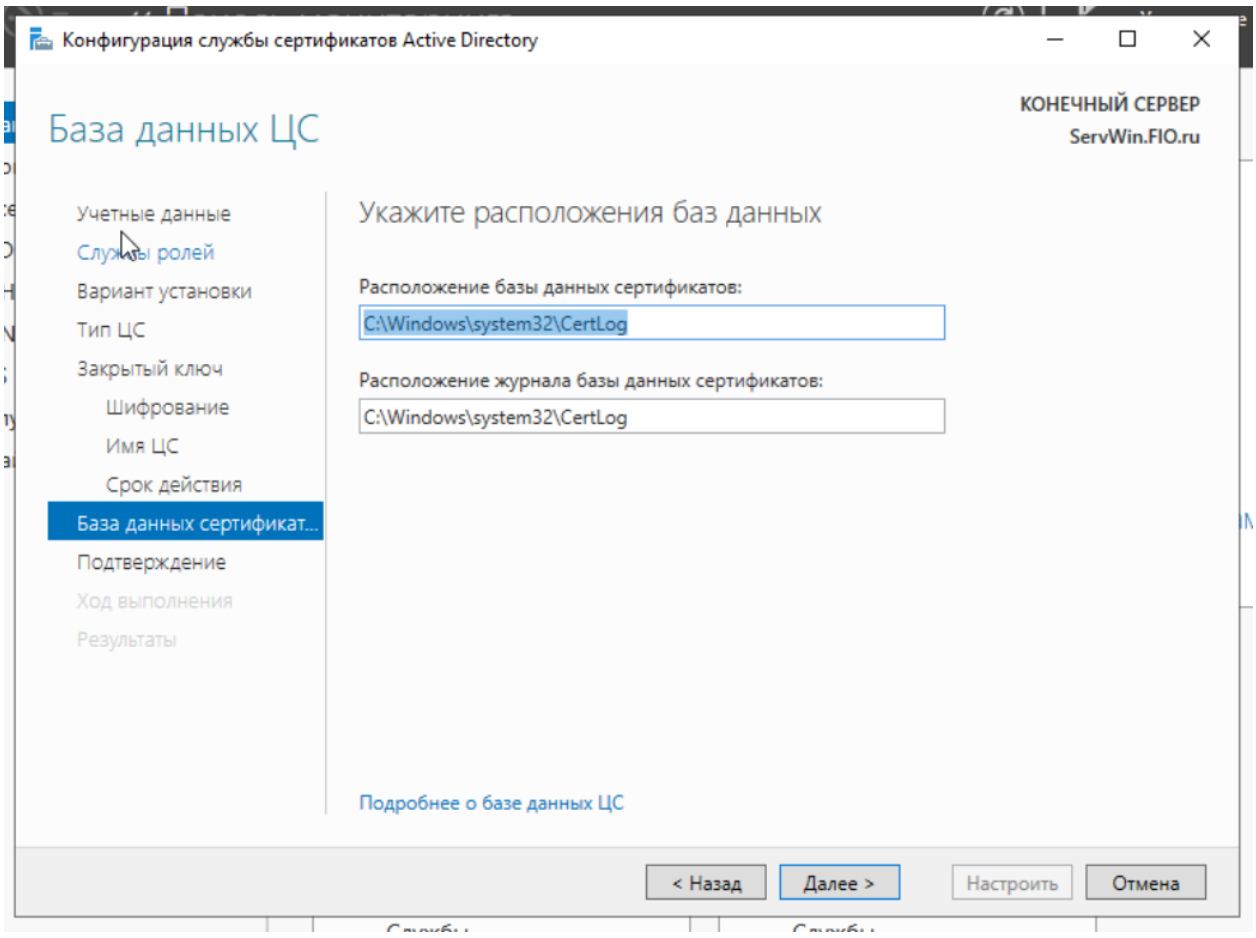

Конфигурация службы сертификатов Active Directory
Тип ЦС
КОНЕЧНЫЙ СЕРВЕР
ServWin.FIO.ru
Учетные данные
Службы ролей
Вариант установки
Тип ЦС
Закрытый ключ
Шифрование
Имя ЦС
Срок действия
База данных сертификат...
Подтверждение
Ход выполнения
Результаты
Укажите тип ЦС
При установке служб сертификатов Active Directory (AD CS) вы создаете или расширяете иерархию инфраструктуры открытых ключей (PKI). Корневой ЦС расположен на вершине иерархии инфраструктуры открытых ключей и выдает собственный самозаверяющий сертификат. Подчиненный ЦС получает сертификат от другого ЦС, расположенного выше в иерархии инфраструктуры открытых ключей.
Корневой ЦС
Корневые ЦС настраиваются в иерархии инфраструктуры открытых ключей первыми; настройка других ЦС может не потребоваться.
Подчиненный ЦС
Для работы подчиненных ЦС требуется установленная иерархия инфраструктуры открытых ключей; они авторизованы для выдачи сертификатов центром сертификации, расположенным выше в иерархии.
Подробнее о типе ЦС
< Назад
Далее >
Настроить
Отмена


Конфигурация службы сертификатов Active Directory
Закрытый ключ
КОНЕЧНЫЙ СЕРВЕР
ServWin.FIO.ru
Учетные данные
Службы ролей
Вариант установки
Тип ЦС
Закрытый ключ
Шифрование
Имя ЦС
Срок действия
База данных сертификат...
Подтверждение
Ход выполнения
Результаты
Укажите тип закрытого ключа
Чтобы создавать сертификаты и выдавать их клиентам, центр сертификации (ЦС) должен иметь закрытый ключ.
Создать новый закрытый ключ
Используйте этот параметр, если у вас нет закрытого ключа или вы хотите создать новый закрытый ключ.
Использовать существующий закрытый ключ
Используйте этот параметр, чтобы при переустановке ЦС гарантировать непрерывность с ранее выданными сертификатами.
Выбрать сертификат и использовать связанный с ним закрытый ключ
Выберите этот параметр, если на этом компьютере есть существующий сертификат или если вы хотите импортировать сертификат и использовать связанный с ним закрытый ключ.
Выбрать существующий закрытый ключ на этом компьютере
Выберите этот параметр, если вы сохранили закрытые ключи из предыдущей установки или хотите использовать закрытый ключ из другого источника.
Подробнее о закрытом ключе
< Назад
Далее >
Настроить
Отмена

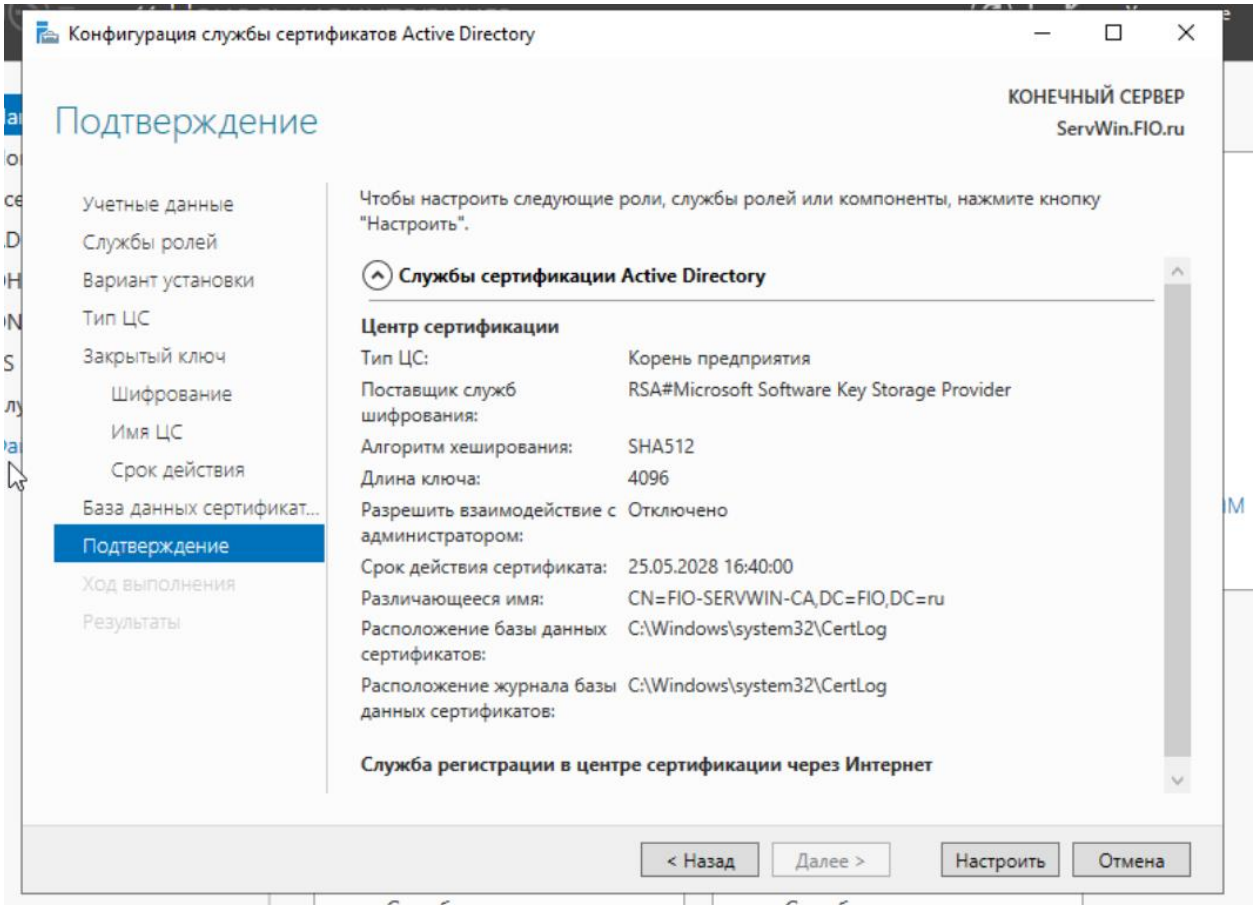

Конфигурация службы сертификатов Active Directory
Шифрование для ЦС
КОНЕЧНЫЙ СЕРВЕР
ServWin.FIO.ru
Учетные данные
Службы ролей
Вариант установки
Тип ЦС
Закрытый ключ
Шифрование
Имя ЦС
Срок действия
База данных сертификат...
Подтверждение
Ход выполнения
Результаты
Укажите параметры шифрования
Выберите поставщик служб шифрования:
RSA#Microsoft Software Key Storage Provider
Длина ключа:
4096
Выберите хэш-алгоритм для подписывания сертификатов, выдаваемых этим ЦС:
SHA256
SHA384
SHA512
SHA1
MD5
Разрешить взаимодействие с администратором, если ЦС обращается к закрытому ключу.
Подробнее о шифровании
< Назад
Далее >
Настроить
Отмена


Конфигурация службы сертификатов Active Directory
Имя ЦС
КОНЕЧНЫЙ СЕРВЕР
ServWin.FIO.ru
Учетные данные
Службы ролей
Вариант установки
Тип ЦС
Закрытый ключ
Шифрование
Имя ЦС
Срок действия
База данных сертификат...
Подтверждение
Ход выполнения
Результаты
Укажите имя ЦС
Введите общее имя, определяющее этот центр сертификации (ЦС). Это имя будет добавляться во все сертификаты, выдаваемые данным ЦС. Значения суффикса различающегося имени создаются автоматически, но могут быть изменены.
Общее имя для этого ЦС:
FIO-SERVWIN-CA
Суффикс различающегося имени:
DC=FIO,DC=ru
Предпросмотр различающегося имени:
CN=FIO-SERVWIN-CA,DC=FIO,DC=ru
Подробнее об имени ЦС
< Назад
Далее >
Настроить
Отмена

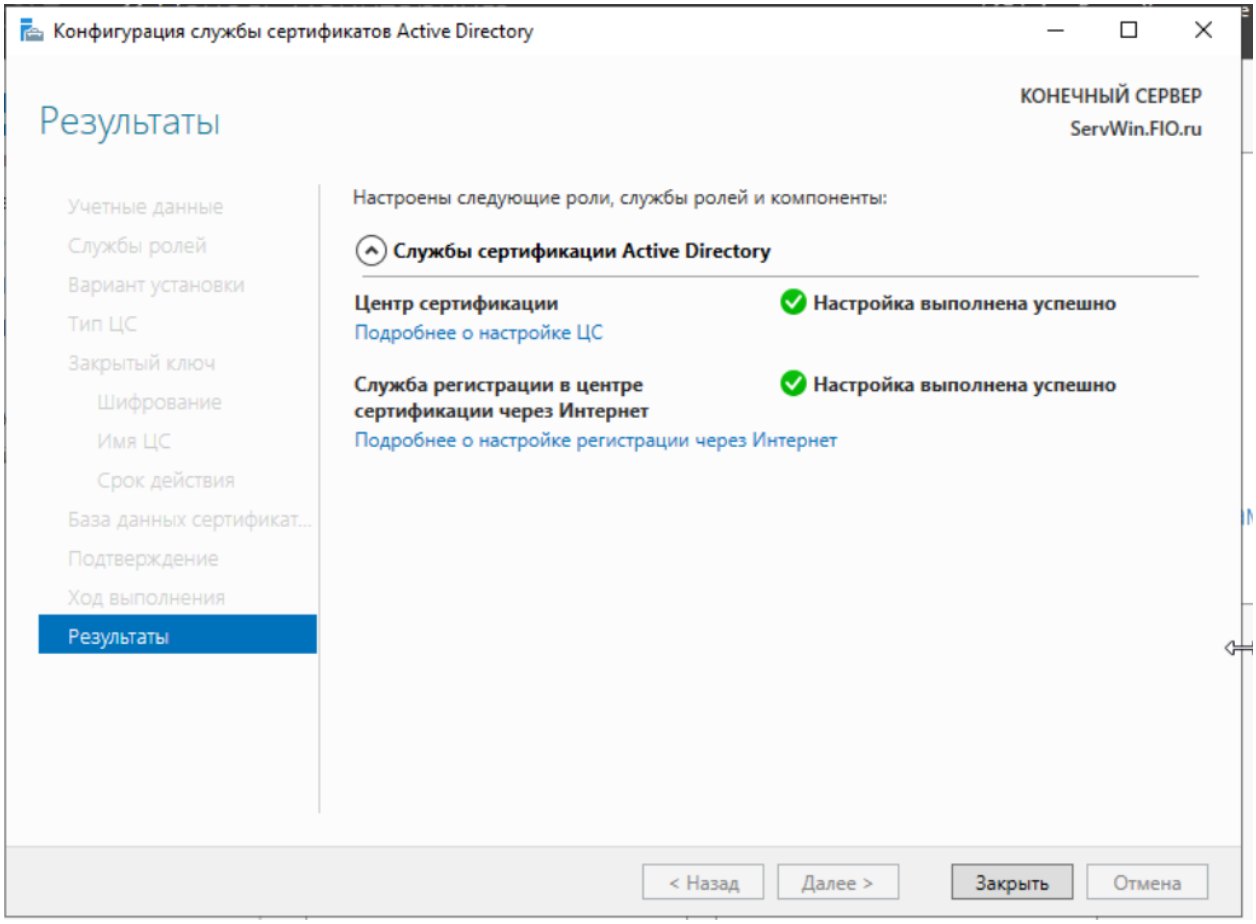

Конфигурация службы сертификатов Active Directory
Срок действия
КОНЕЧНЫЙ СЕРВЕР
ServWin.FIO.ru
Учетные данные
Службы ролей
Вариант установки
Тип ЦС
Закрытый ключ
Шифрование
Имя ЦС
Срок действия
База данных сертификат...
Подтверждение
Ход выполнения
Результаты
Укажите период действия
Укажите период действия сертификата, созданного для этого центра сертификации (ЦС):
3
г.
Дата окончания срока действия: 25.05.2028 16:40:00
Срок действия, указанный для этого сертификата ЦС, должен превышать срок действия сертификатов, которые он будет выдавать.
Подробнее о сроке действия
< Назад
Далее >
Настроить
Отмена



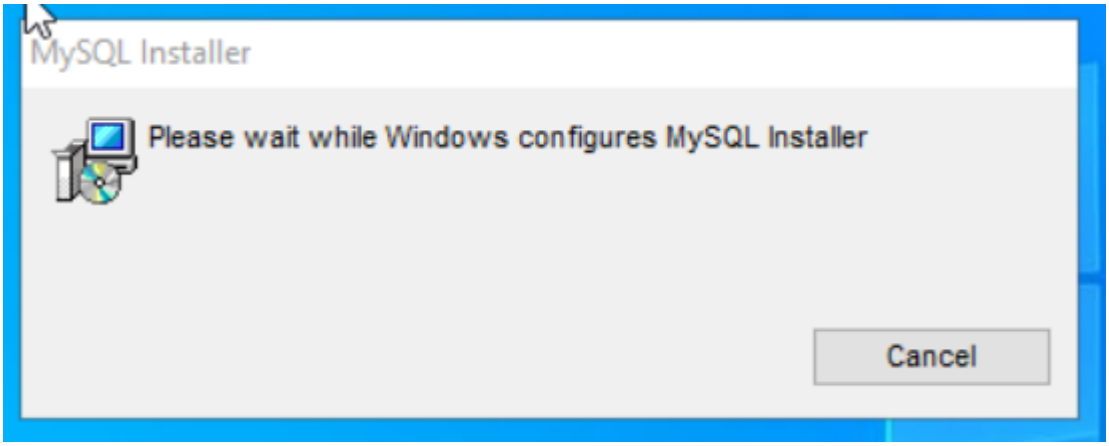
Далее необходимо нажать кнопку «Настроить»

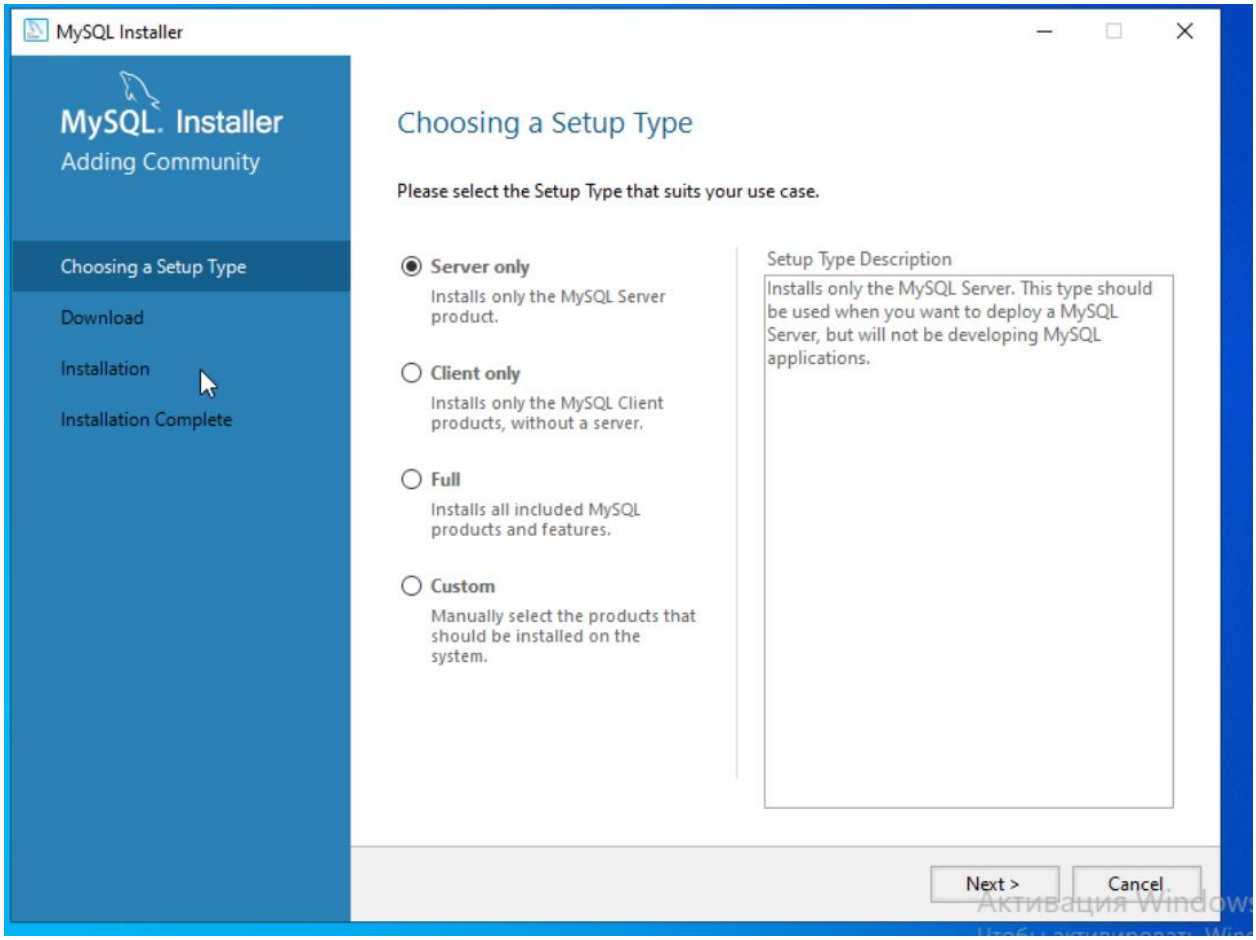


Далее настройка выполнена успешно

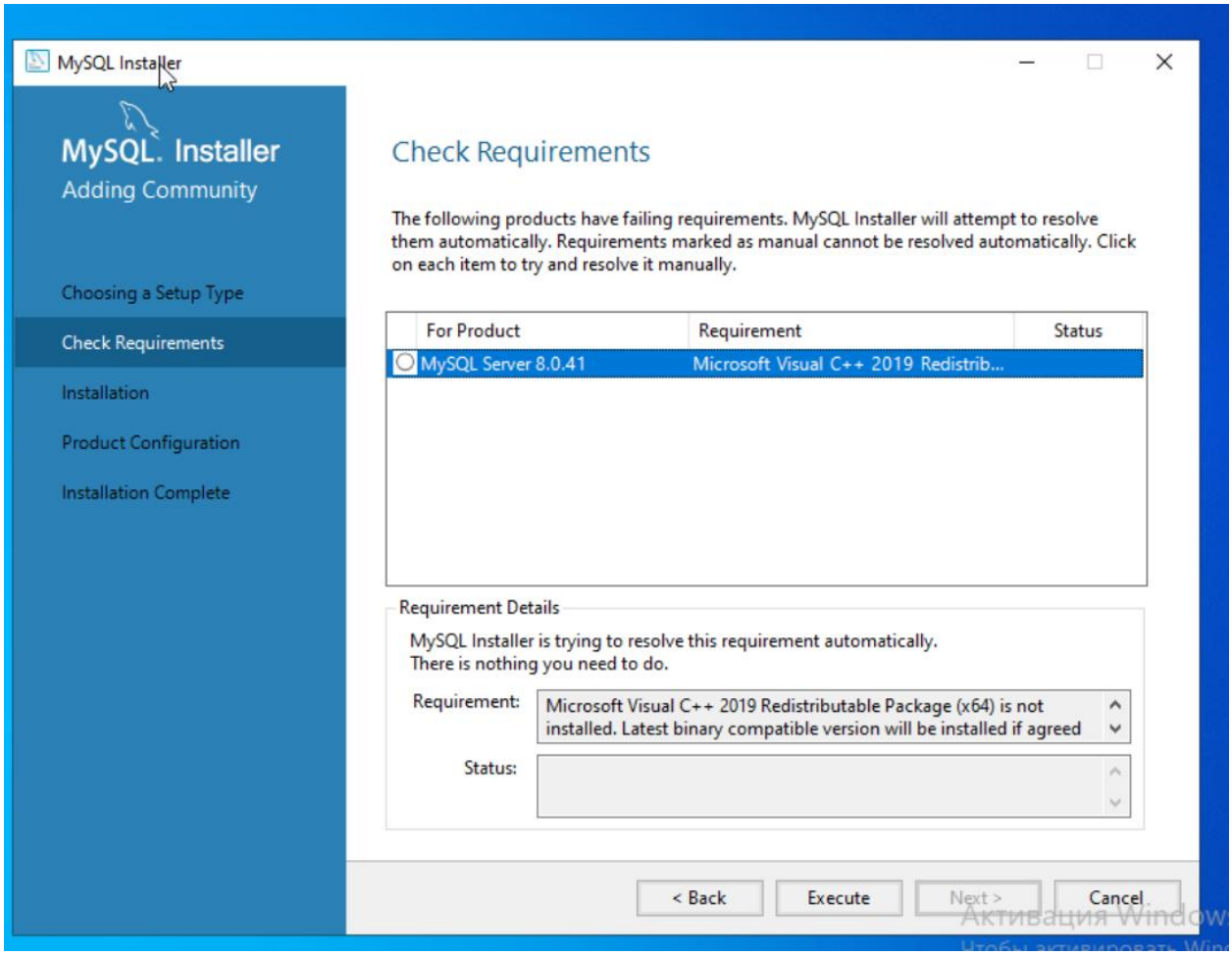


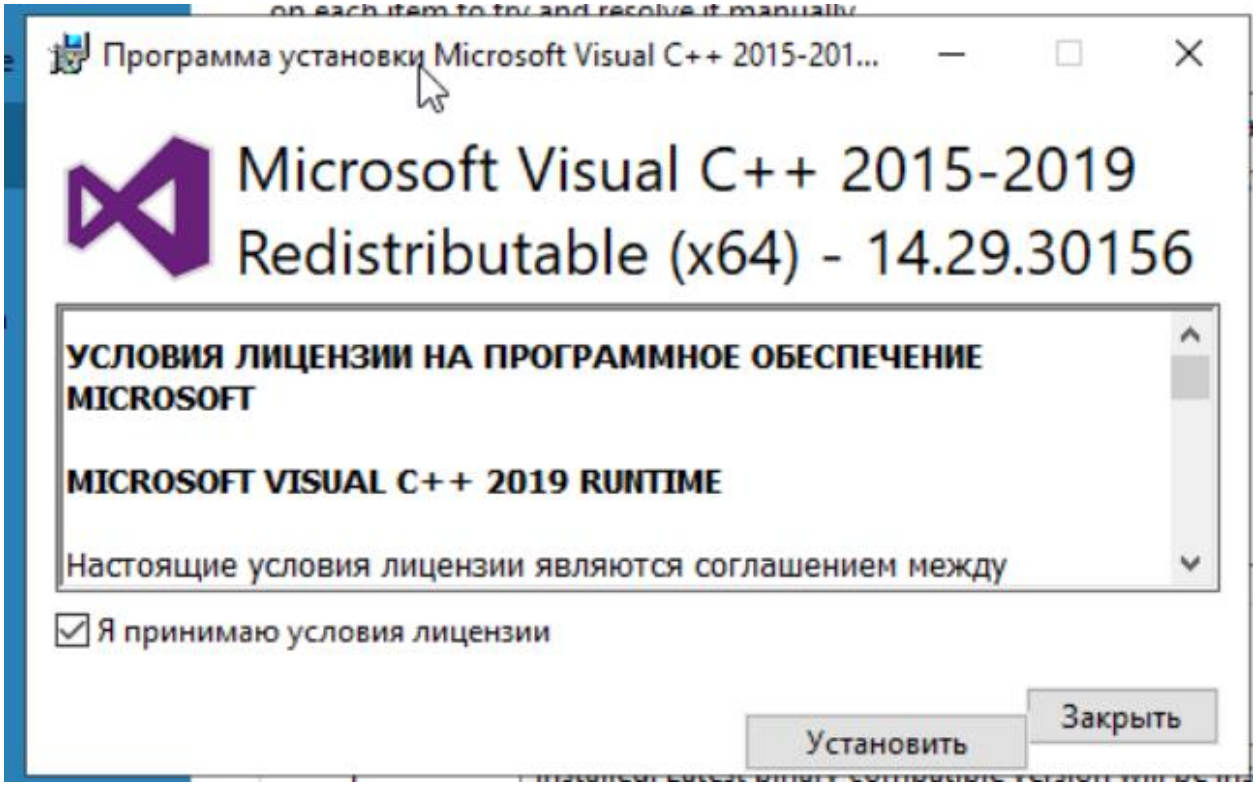
Ниже представлена устанвока MySQL, в целом mysql уже установлен, но если вдруг его не будет на сервере или на клиенте Open то в целом установка происходит по принципу «Далее, далее, далее» Если где то что то будет не указано вводите как указано ниже на скриншотах

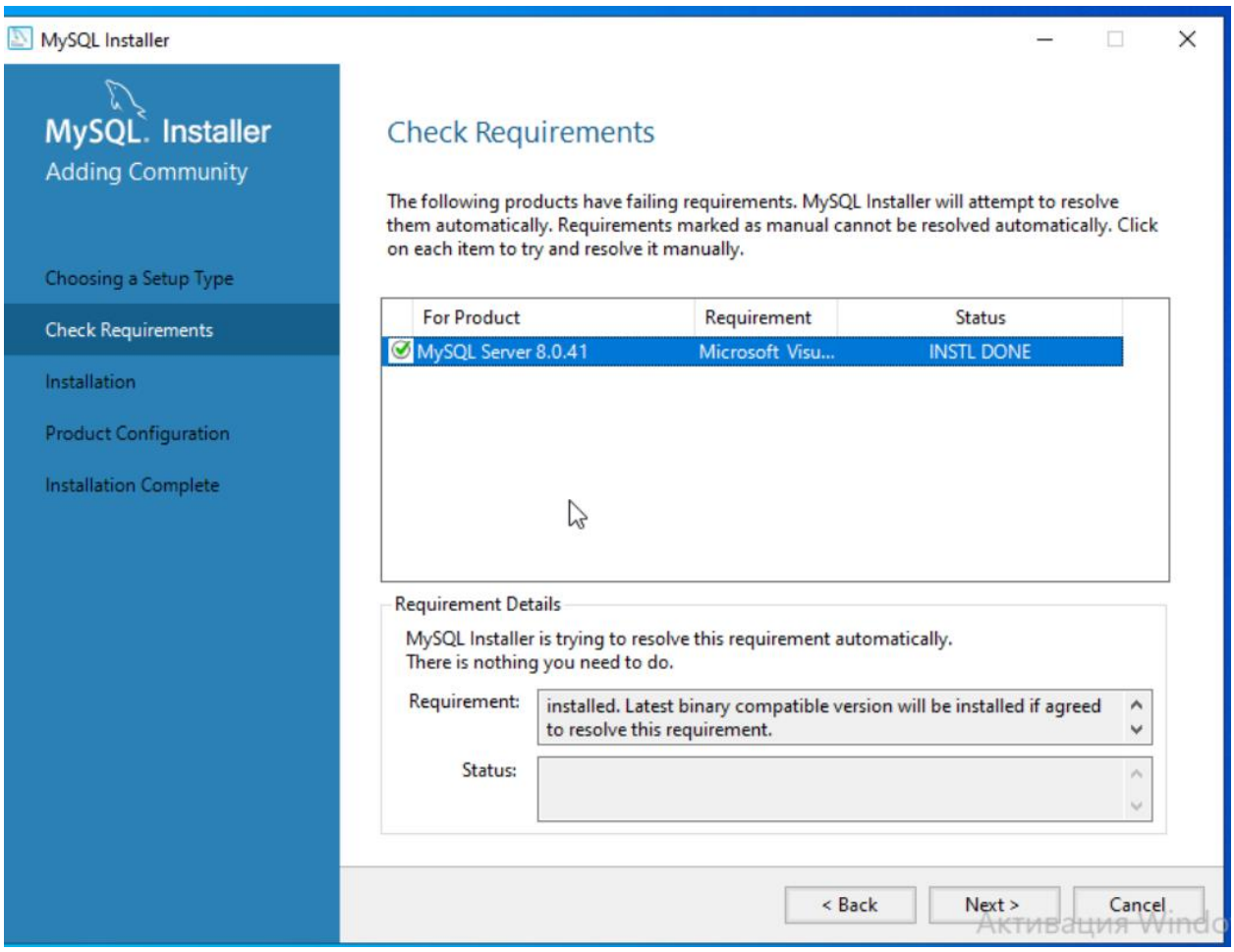


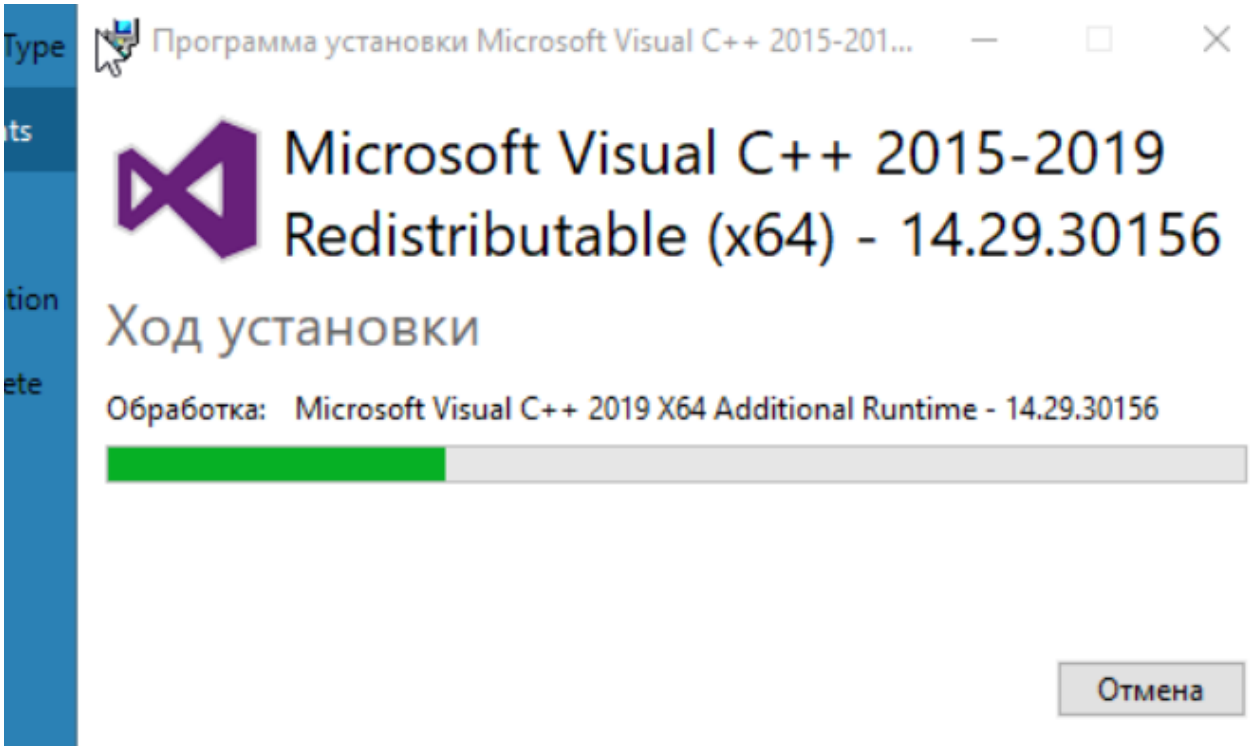


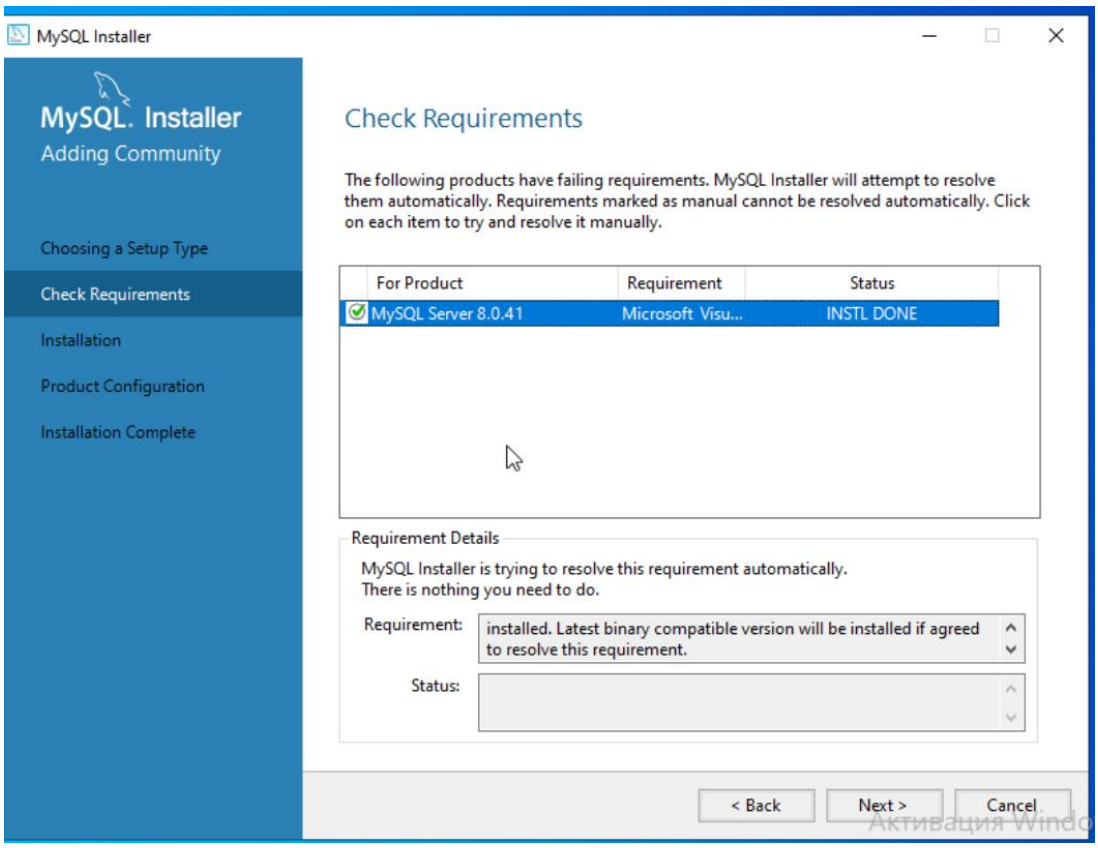
Здесь необходимо нажать «Execute» затем «далее»



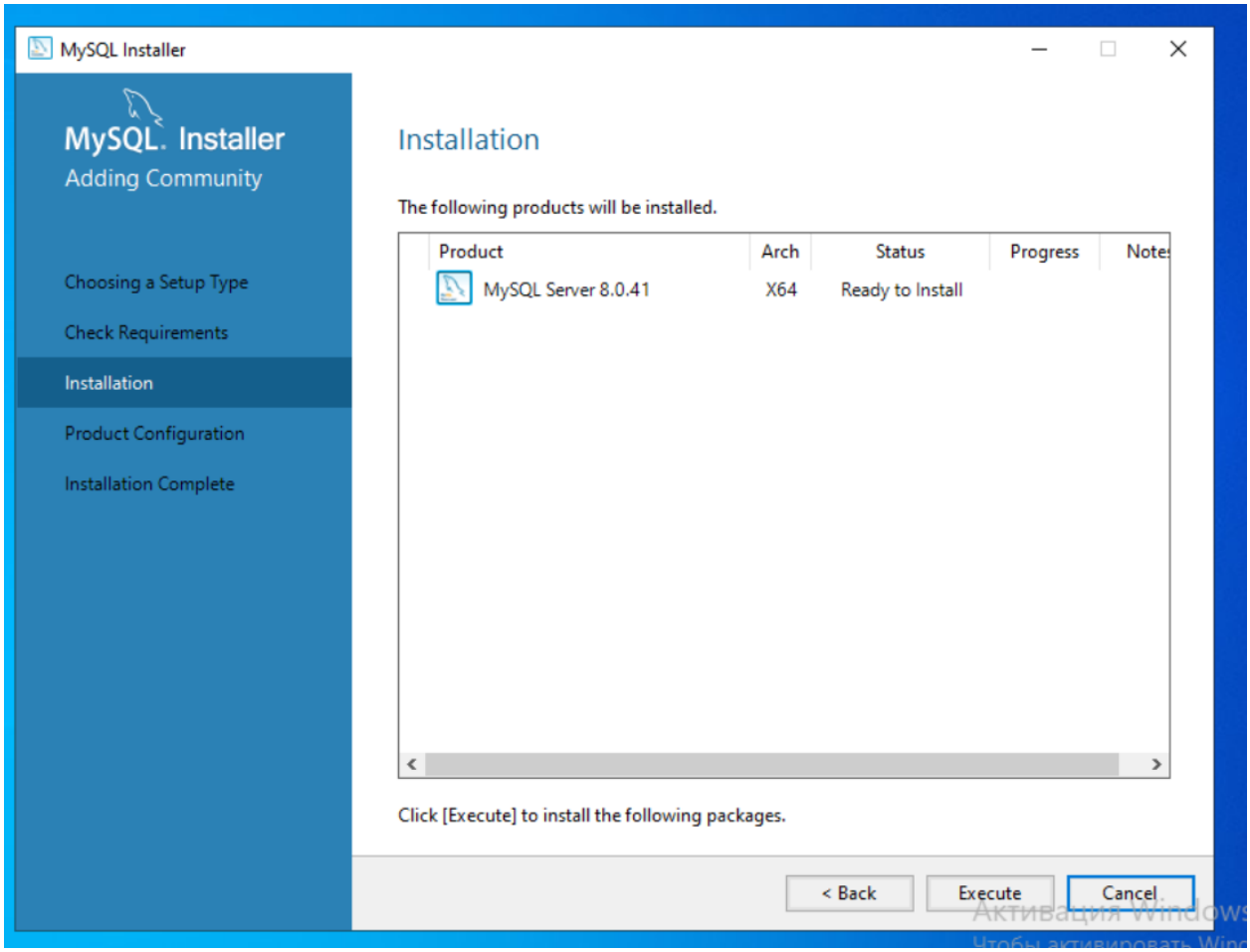


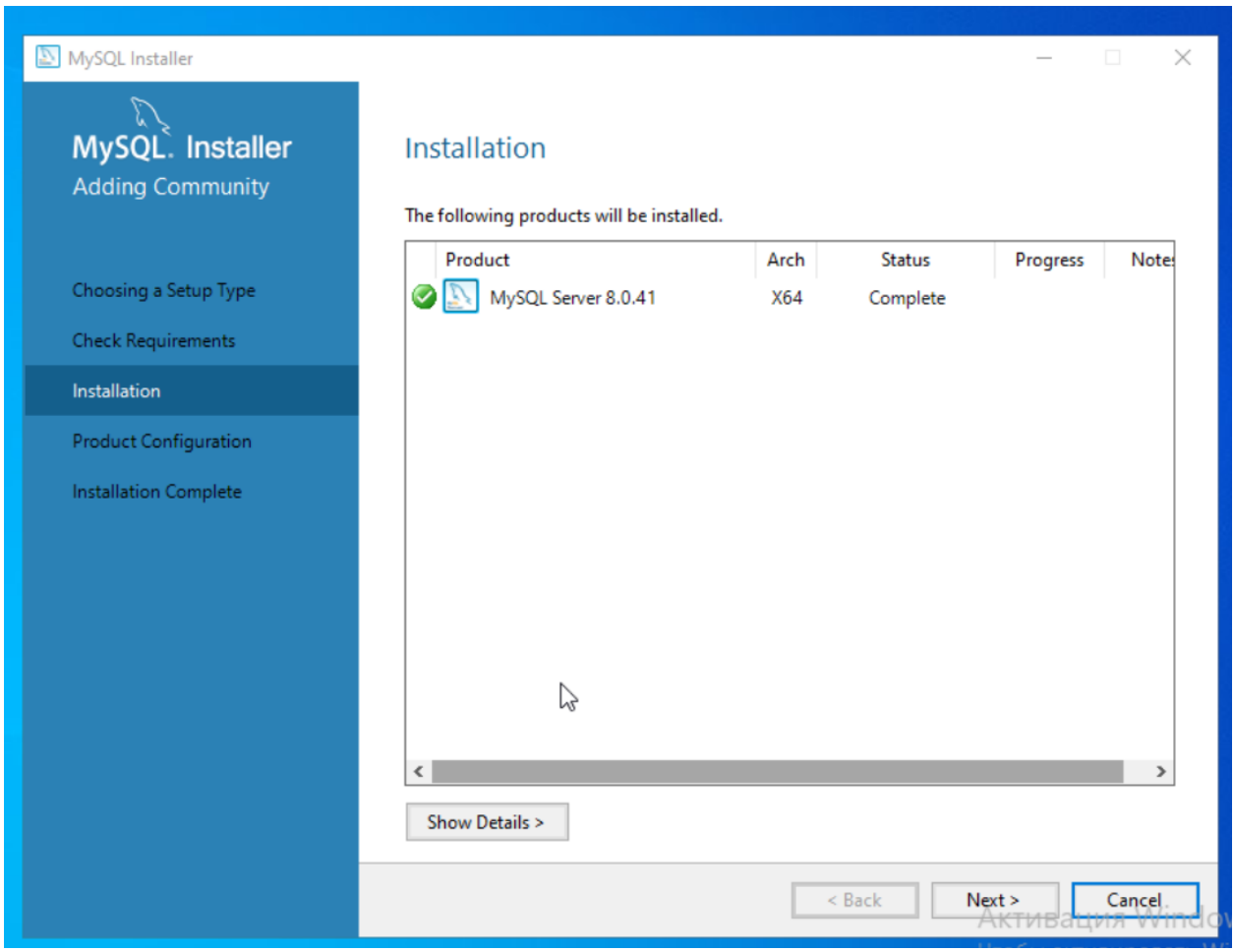

MySQL Installer
MySQL. Installer
Adding Community
Choosing a Setup Type
Check Requirements
Installation
Product Configuration
Installation Complete
Check Requirements
The following products have failing requirements. MySQL Installer will attempt to resolve them automatically. Requirements marked as manual cannot be resolved automatically. Click on each item to try and resolve it manually.
For Product
Requirement
Status
MySQL Server 8.0.41
Microsoft Visu...
INSTL DONE
Requirement Details
MySQL Installer is trying to resolve this requirement automatically.
There is nothing you need to do.
Requirement:
installed. Latest binary compatible version will be installed if agreed to resolve this requirement.
Status:
< Back
Next >
Cancel

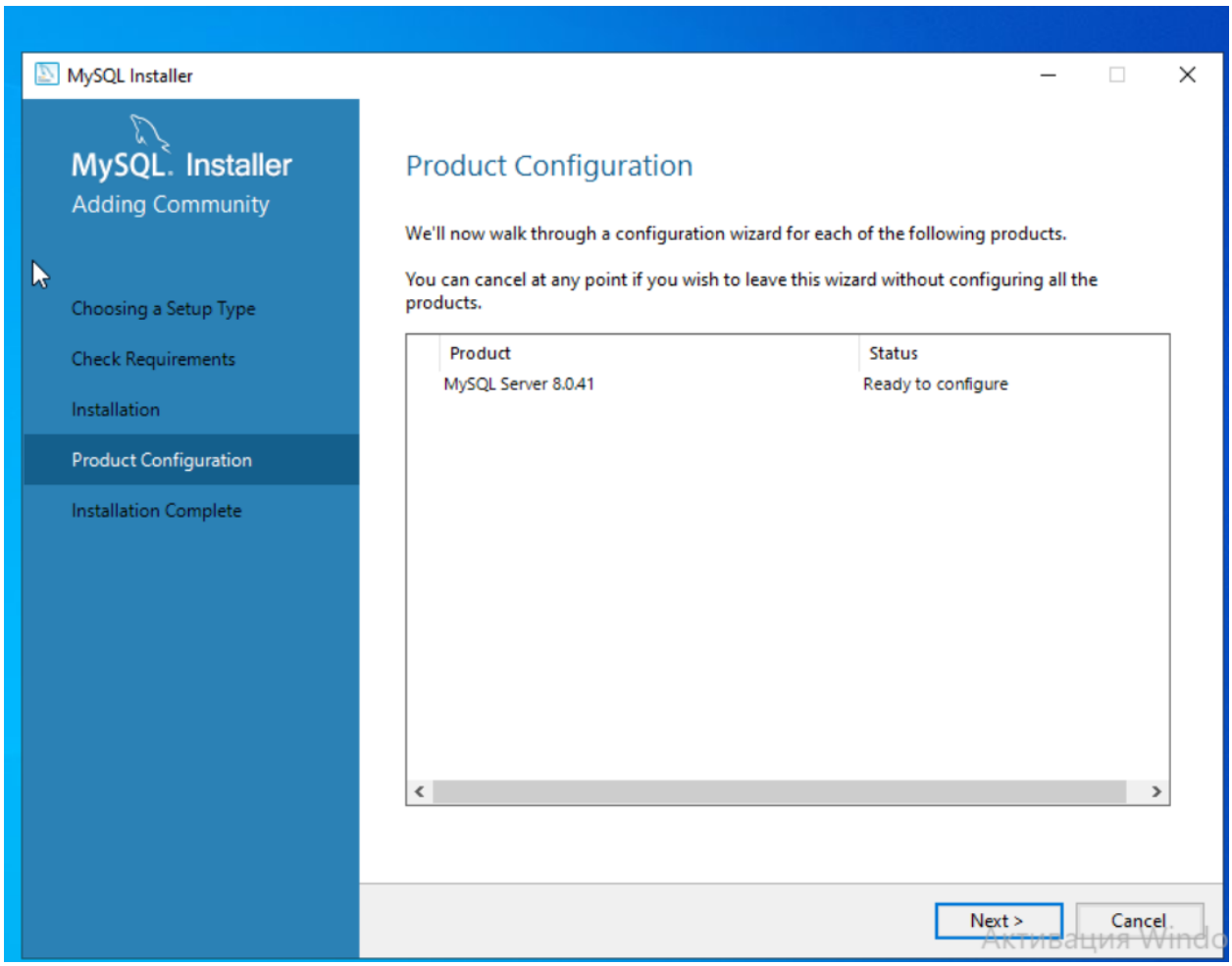

Программа установки Microsoft Visual C++ 2015-201...
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.29.30156
Ход установки
Обработка: Microsoft Visual C++ 2019 X64 Additional Runtime - 14.29.30156
Отмена

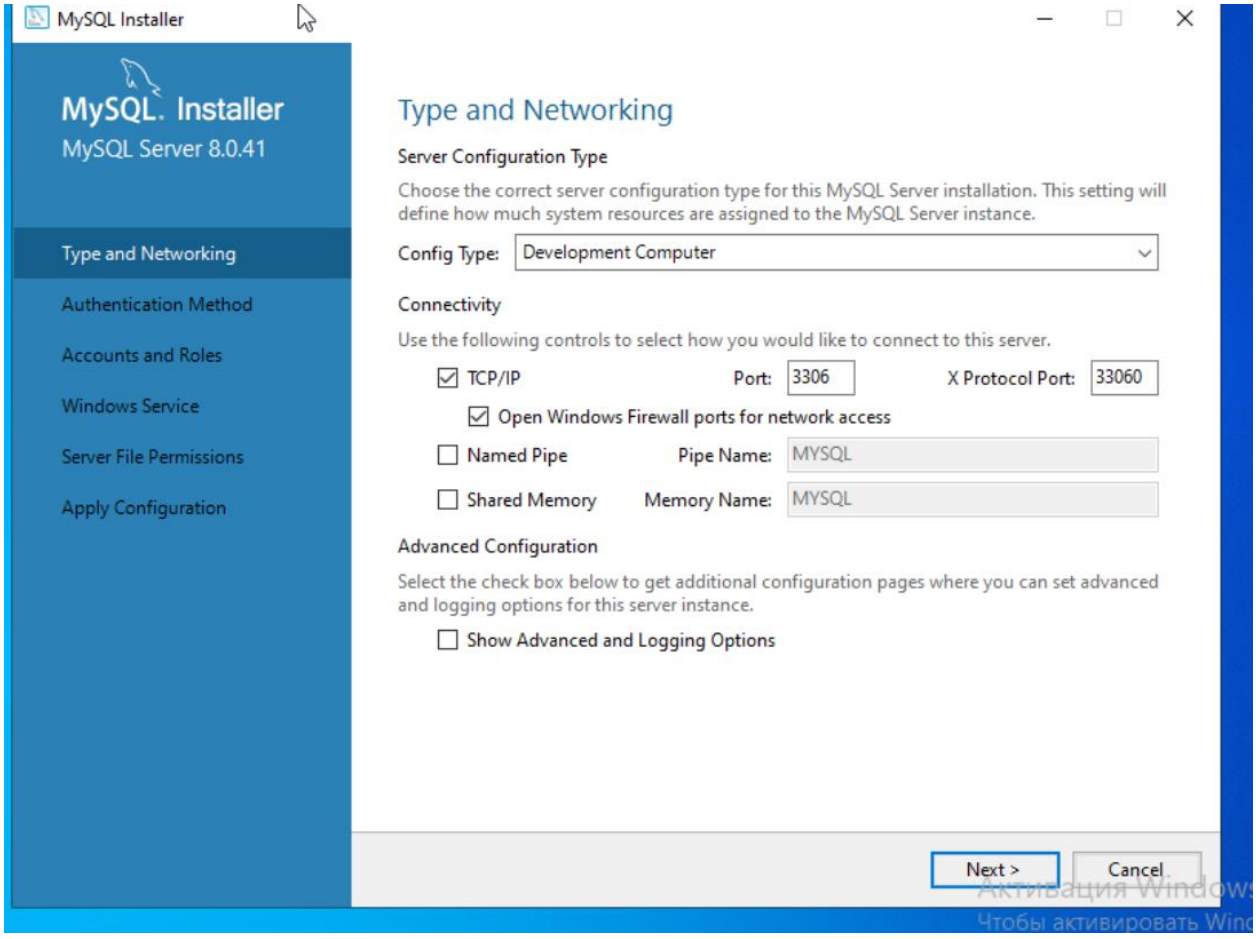


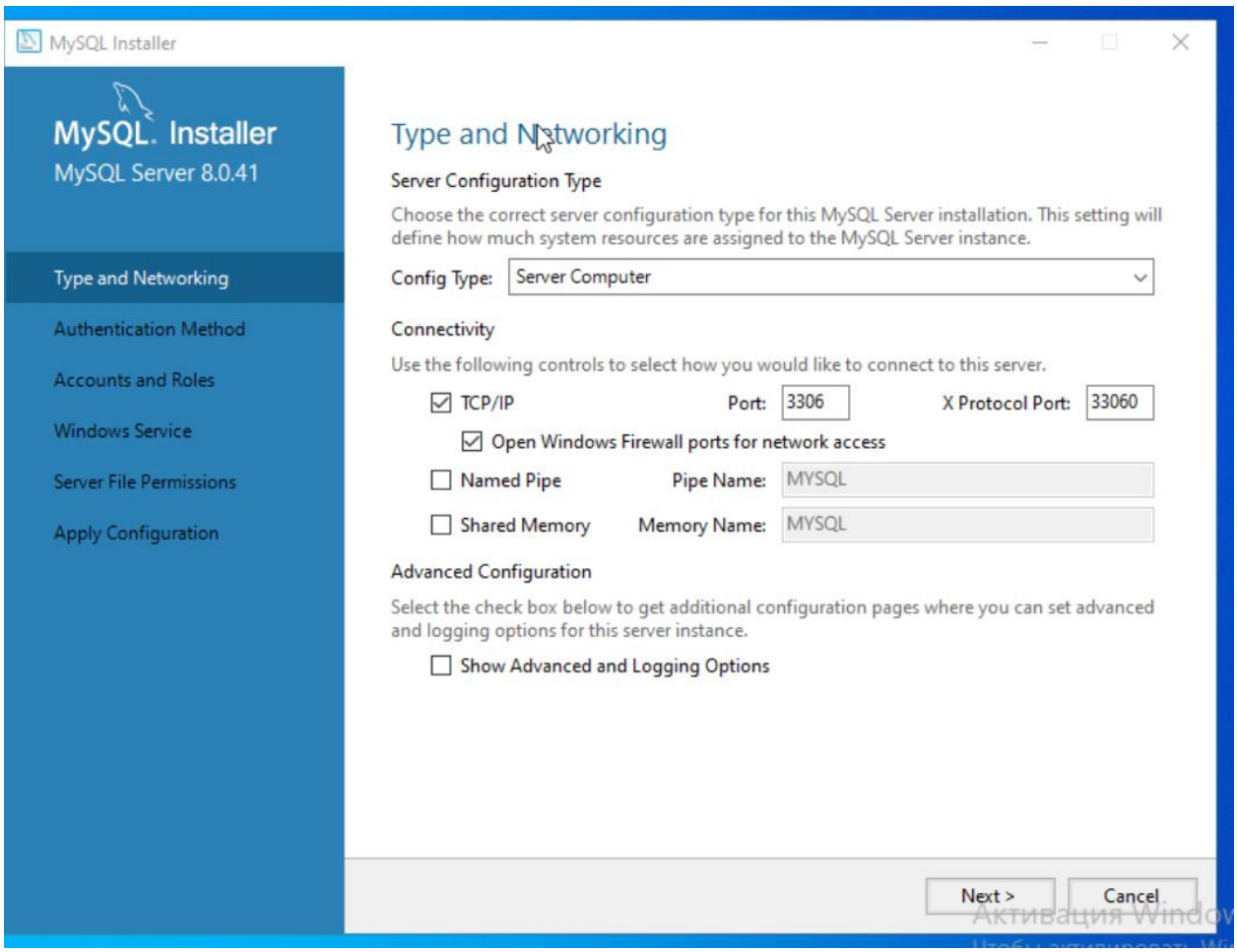
Здесь необходимо нажать «Execute» затем «далее»

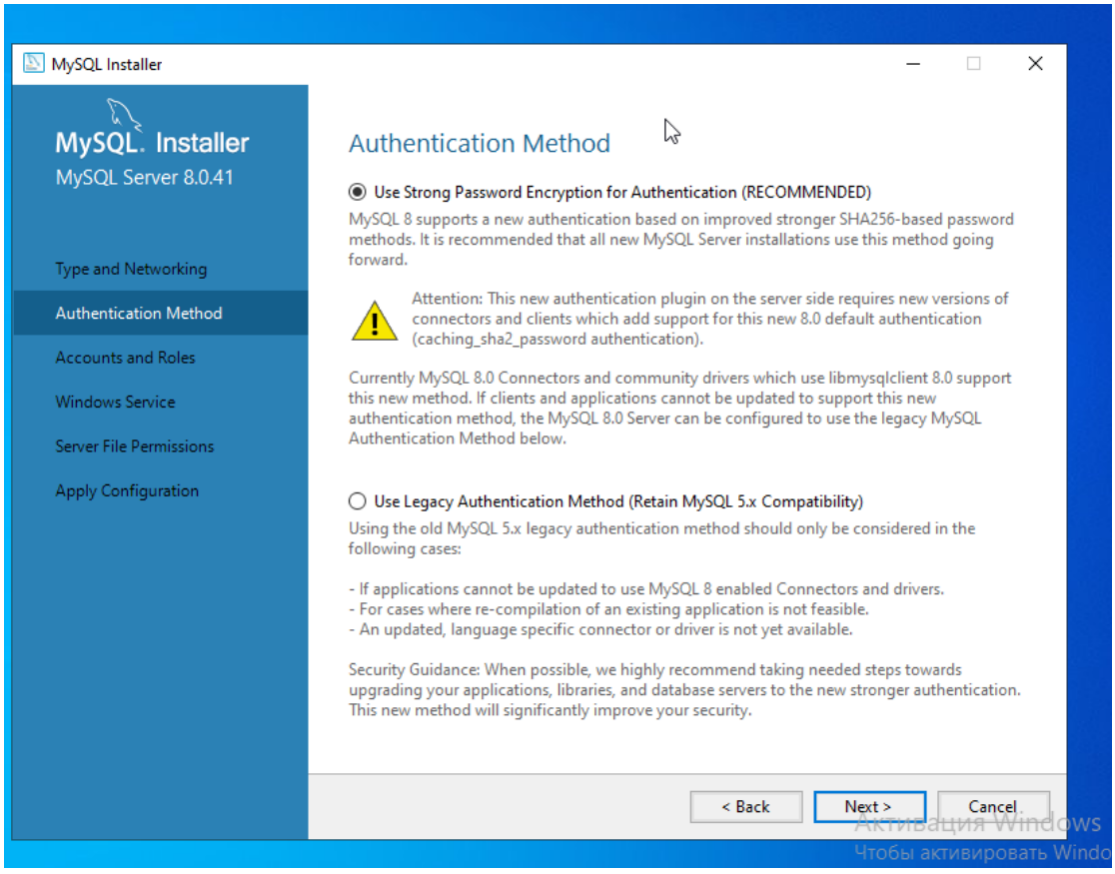



MySQL Installer
MySQL. Installer
Adding Community
Choosing a Setup Type
Check Requirements
Installation
Product Configuration
Installation Complete
Installation
The following products will be installed.
Product
Arch
Status
Progress
Note
MySQL Server 8.0.41
X64
Complete
Show Details >
< Back
Next >
Cancel

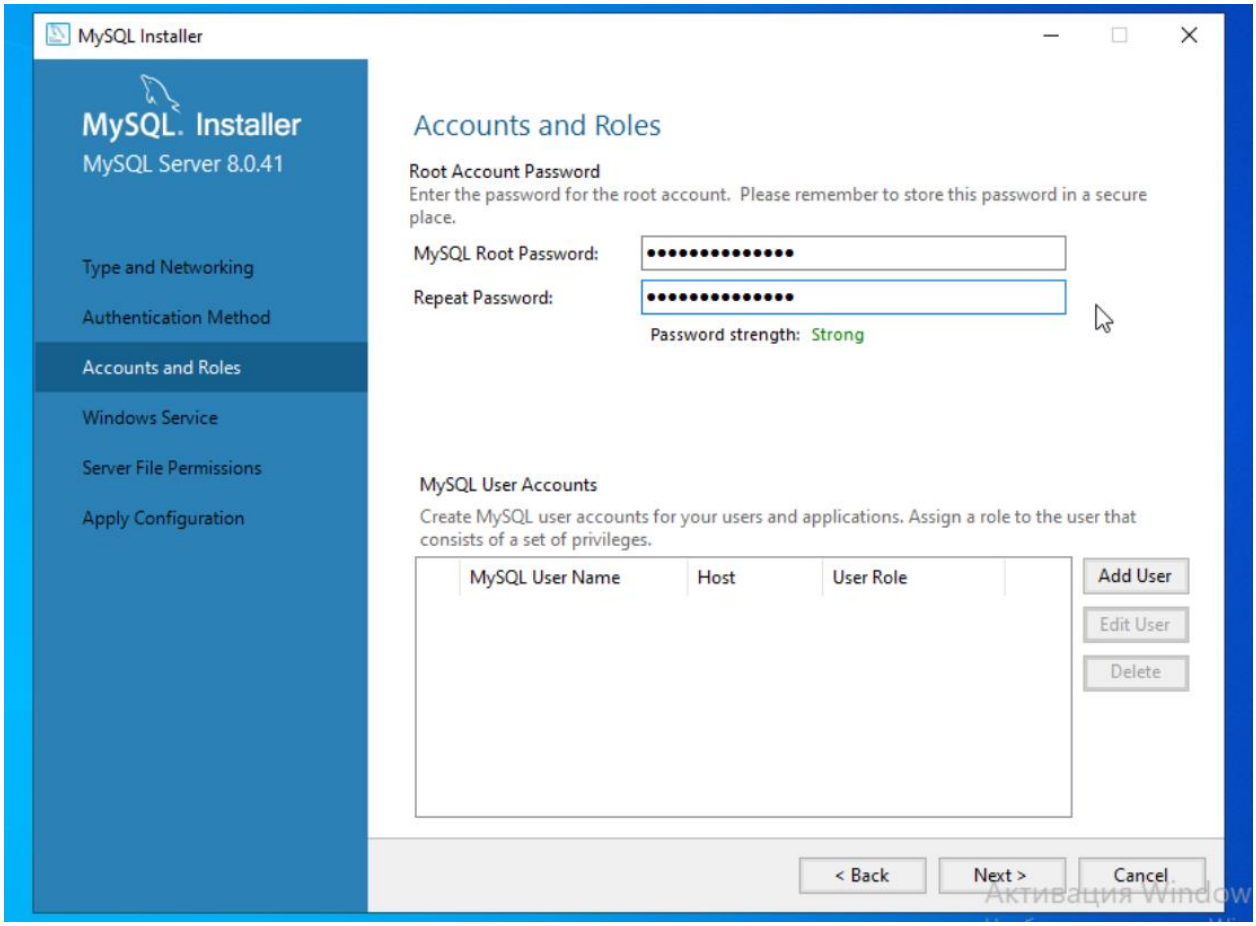

MySQL Installer
MySQL. Installer
Adding Community
Choosing a Setup Type
Check Requirements
Installation
Product Configuration
Installation Complete
Product Configuration
We'll now walk through a configuration wizard for each of the following products.
You can cancel at any point if you wish to leave this wizard without configuring all the products.
Product
Status
MySQL Server 8.0.41
Ready to configure
Next >
Cancel

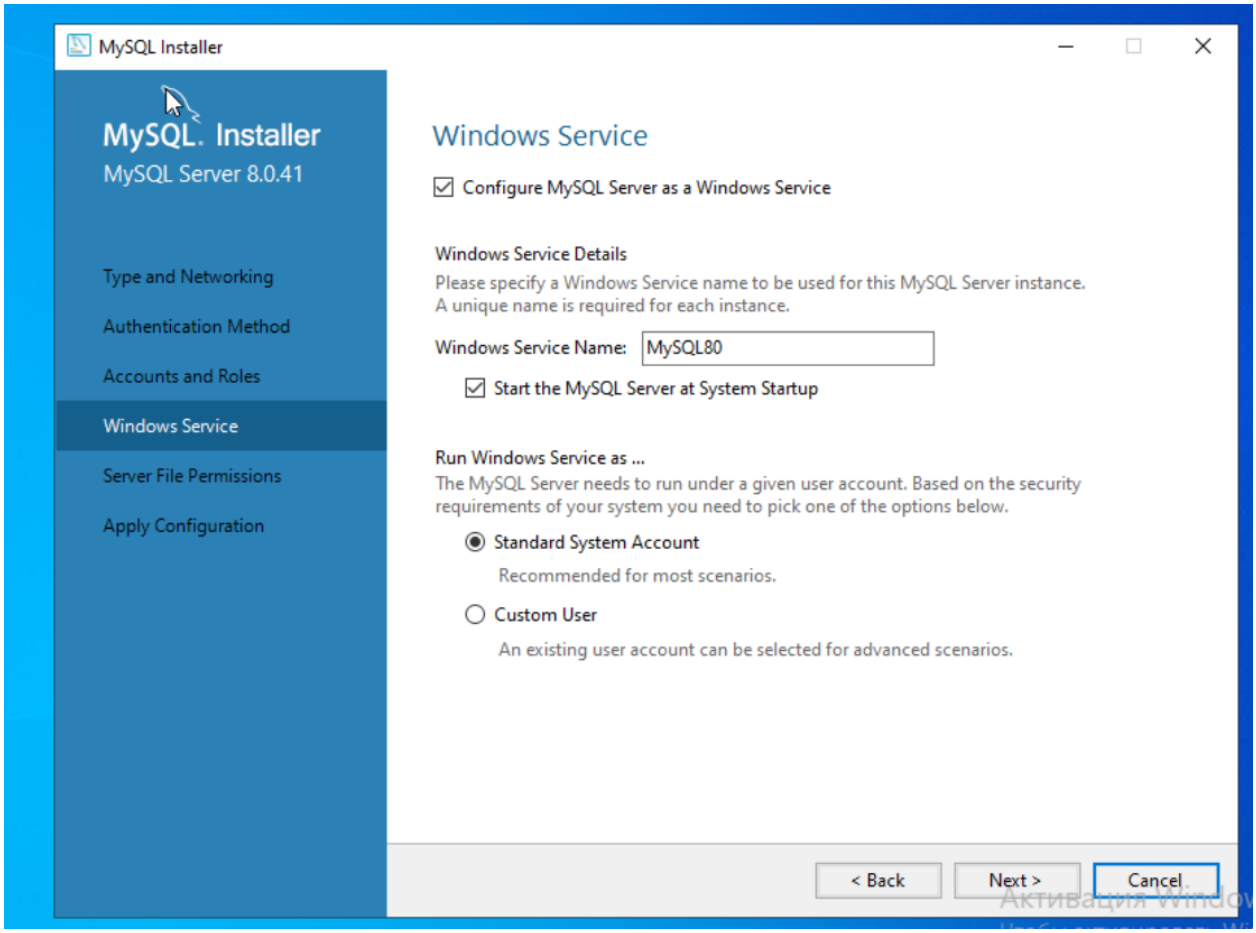

MySQL Installer
MySQL. Installer
MySQL Server 8.0.41
Type and Networking
Authentication Method
Accounts and Roles
Windows Service
Server File Permissions
Apply Configuration
Type and Networking
Server Configuration Type
Choose the correct server configuration type for this MySQL Server installation. This setting will define how much system resources are assigned to the MySQL Server instance.
Config Type: Development Computer
Connectivity
Use the following controls to select how you would like to connect to this server.
TCP/IP
Port: 3306
X Protocol Port: 33060
Open Windows Firewall ports for network access
Named Pipe
Pipe Name: MYSQL
Shared Memory
Memory Name: MYSQL
Advanced Configuration
Select the check box below to get additional configuration pages where you can set advanced and logging options for this server instance.
Show Advanced and Logging Options
Next >
Cancel

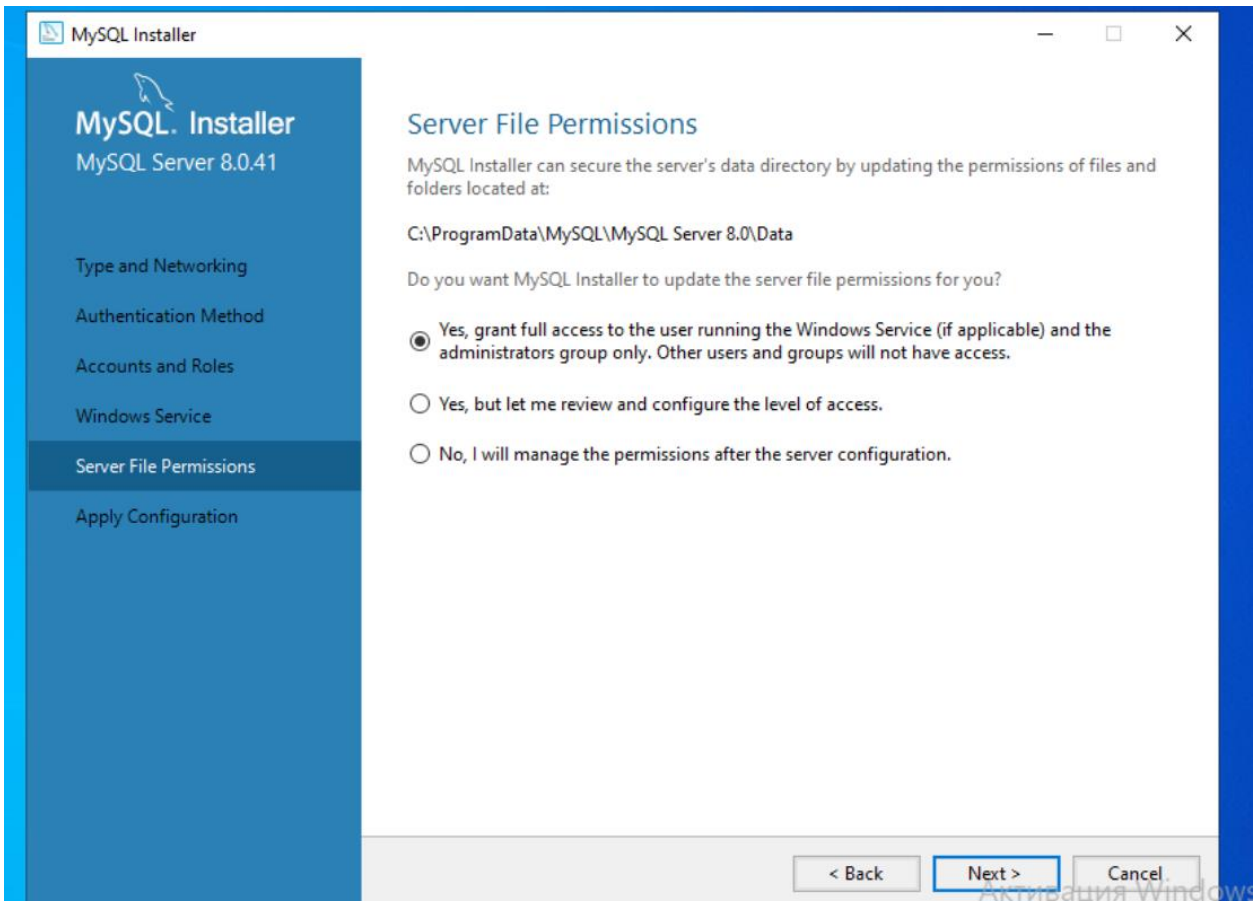

MySQL Installer
MySQL. Installer
MySQL Server 8.0.41
Type and Networking
Authentication Method
Accounts and Roles
Windows Service
Server File Permissions
Apply Configuration
Type and Networking
Server Configuration Type
Choose the correct server configuration type for this MySQL Server installation. This setting will define how much system resources are assigned to the MySQL Server instance.
Config Type: Server Computer
Connectivity
Use the following controls to select how you would like to connect to this server.
TCP/IP
Port: 3306
X Protocol Port: 33060
Open Windows Firewall ports for network access
Named Pipe
Pipe Name: MYSQL
Shared Memory
Memory Name: MYSQL
Advanced Configuration
Select the check box below to get additional configuration pages where you can set advanced and logging options for this server instance.
Show Advanced and Logging Options
Next >
Cancel

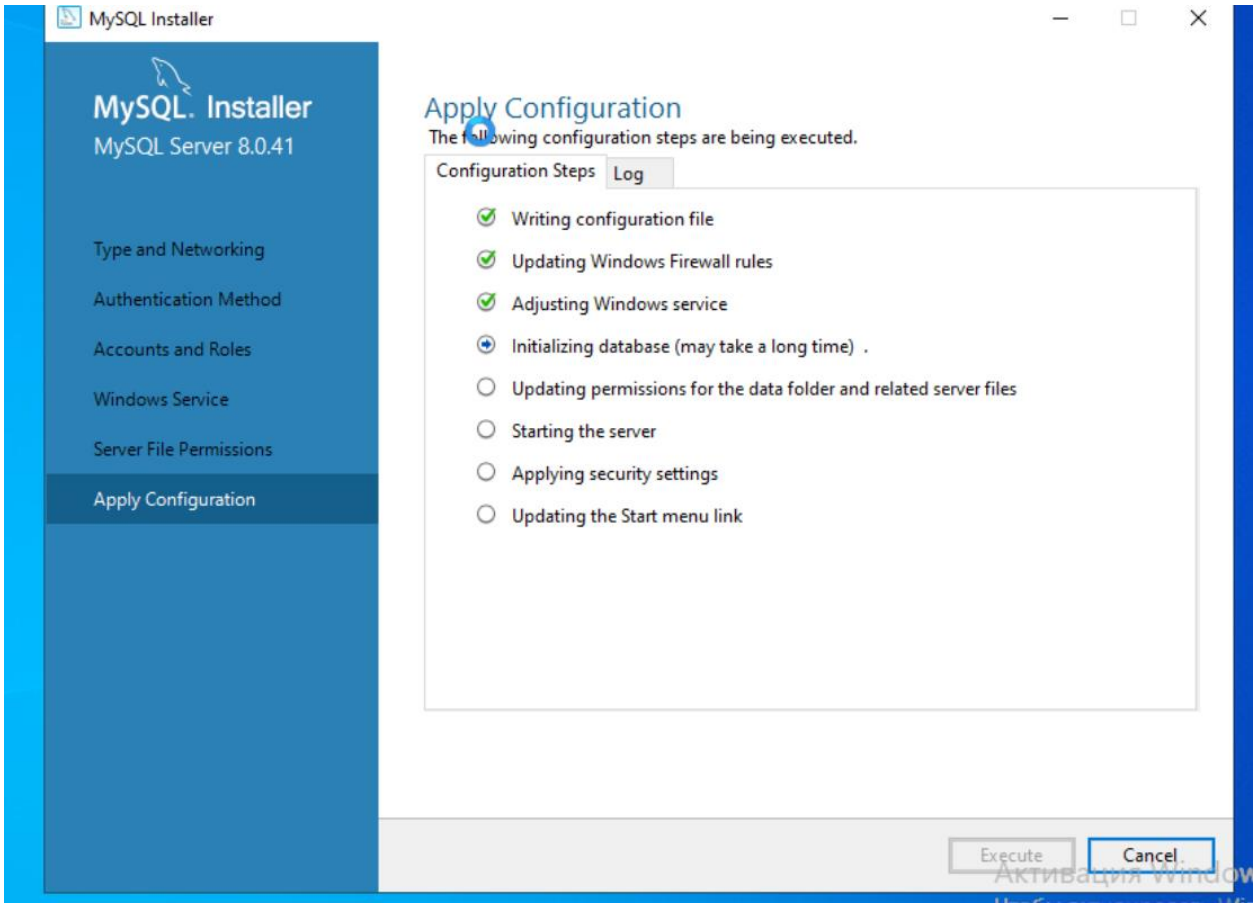

MySQL Installer
MySQL. Installer
MySQL Server 8.0.41
Type and Networking
Authentication Method
Accounts and Roles
Windows Service
Server File Permissions
Apply Configuration
Authentication Method
Use Strong Password Encryption for Authentication (RECOMMENDED)
MySQL 8 supports a new authentication based on improved stronger SHA256-based password methods. It is recommended that all new MySQL Server installations use this method going forward.
Attention: This new authentication plugin on the server side requires new versions of connectors and clients which add support for this new 8.0 default authentication (caching_sha2_password authentication).
Currently MySQL 8.0 Connectors and community drivers which use libmysqlclient 8.0 support this new method. If clients and applications cannot be updated to support this new authentication method, the MySQL 8.0 Server can be configured to use the legacy MySQL Authentication Method below.
Use Legacy Authentication Method (Retain MySQL 5.x Compatibility)
Using the old MySQL 5.x legacy authentication method should only be considered in the following cases:
- If applications cannot be updated to use MySQL 8 enabled Connectors and drivers.
- For cases where re-compilation of an existing application is not feasible.
- An updated, language specific connector or driver is not yet available.
Security Guidance: When possible, we highly recommend taking needed steps towards upgrading your applications, libraries, and database servers to the new stronger authentication. This new method will significantly improve your security.
< Back
Next >
Cancel

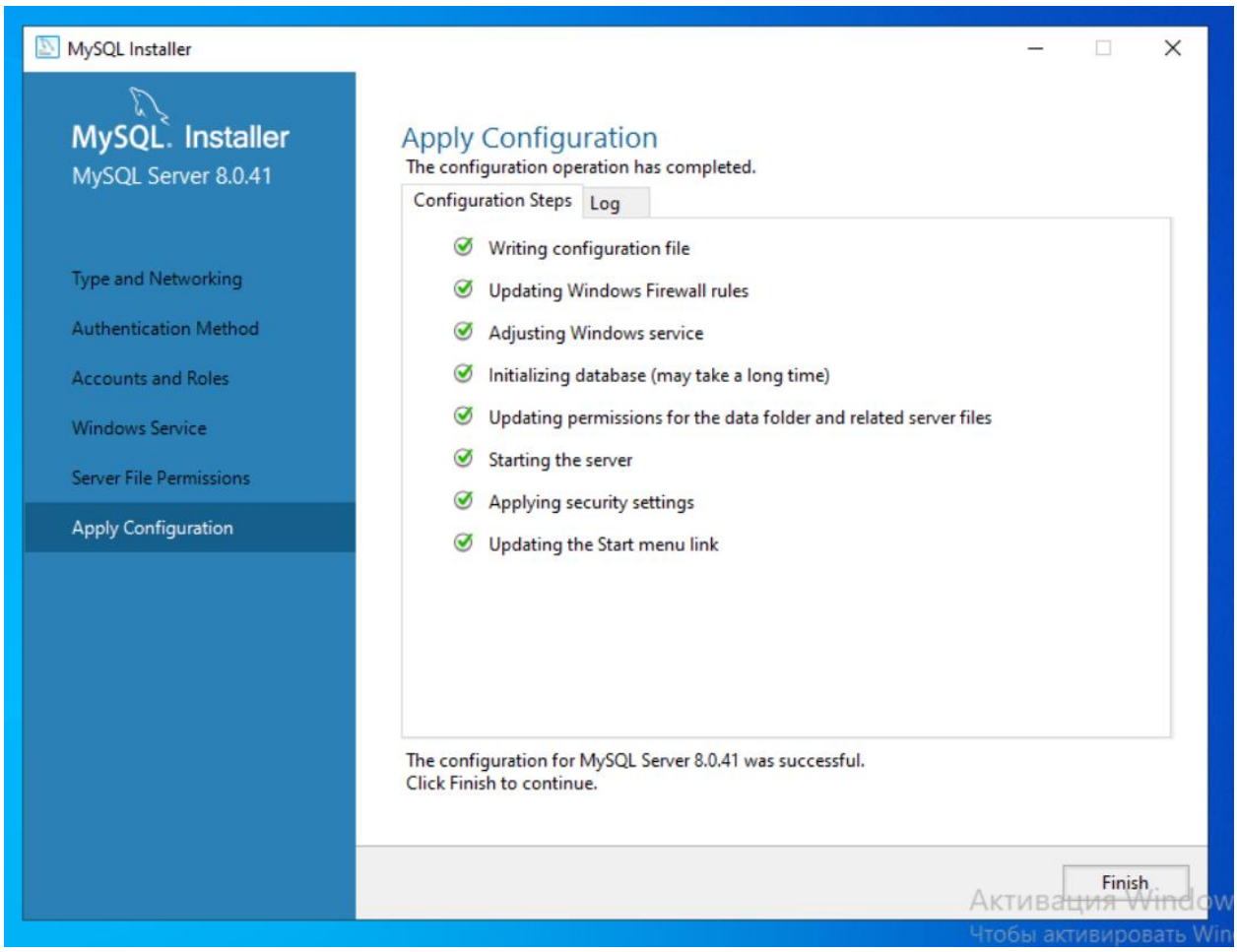
Здесь необходиму казать пароль желательно надежный и нажать next.

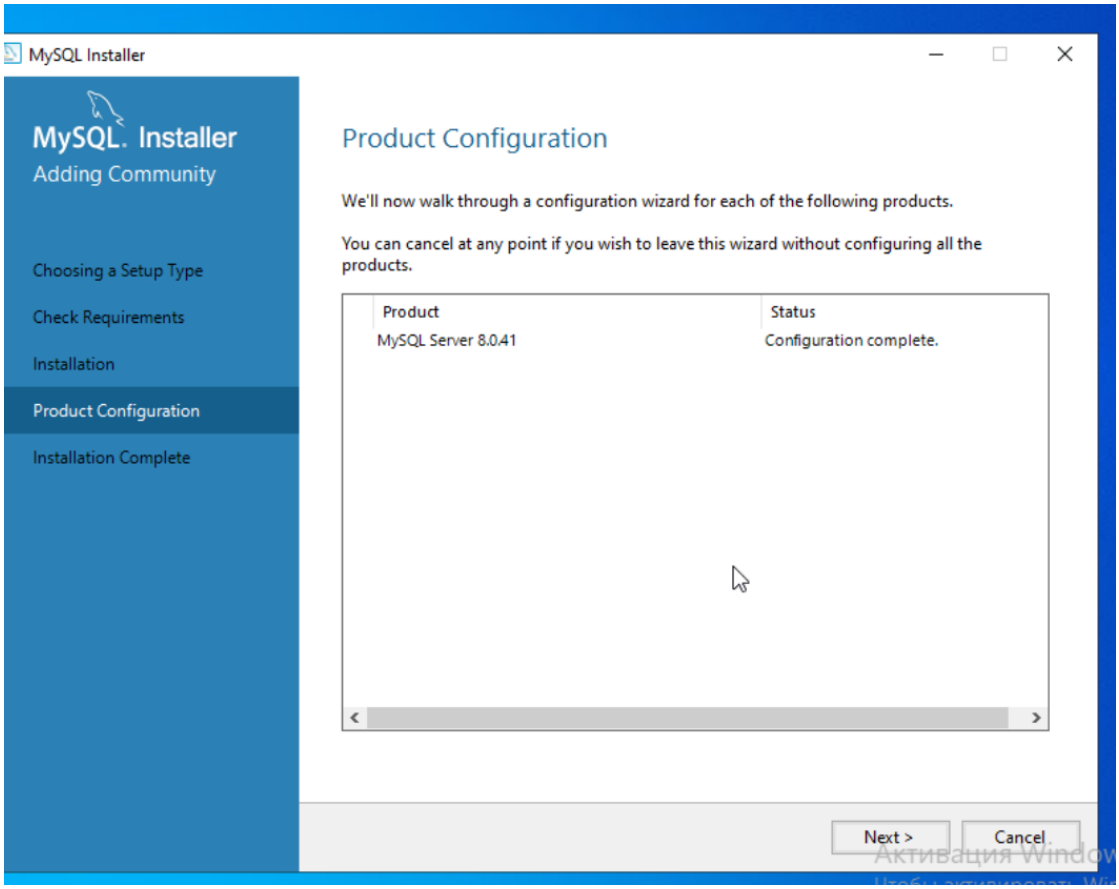




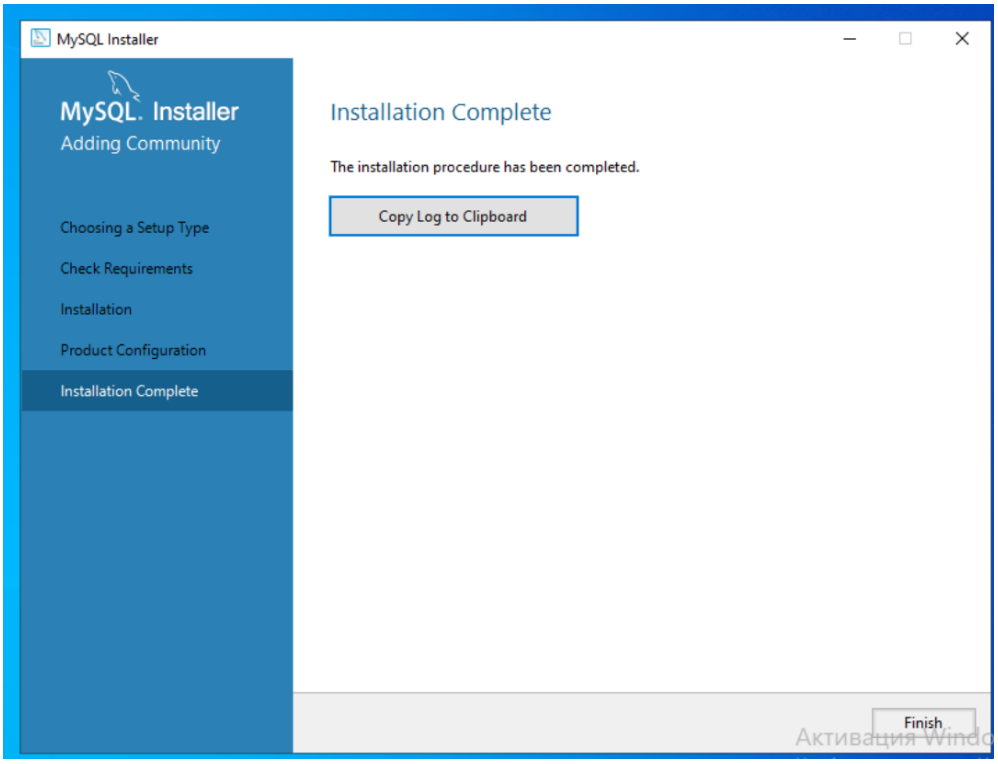

MySQL Installer
MySQL. Installer
MySQL Server 8.0.41
Type and Networking
Authentication Method
Accounts and Roles
Windows Service
Server File Permissions
Apply Configuration
Server File Permissions
MySQL Installer can secure the server's data directory by updating the permissions of files and folders located at:
C:\ProgramData\MySQL\MySQL Server 8.0\Data
Do you want MySQL Installer to update the server file permissions for you?
Yes, grant full access to the user running the Windows Service (if applicable) and the administrators group only. Other users and groups will not have access.
Yes, but let me review and configure the level of access.
No, I will manage the permissions after the server configuration.
< Back
Next >
Cancel


MySQL Installer
MySQL. Installer
MySQL Server 8.0.41
Type and Networking
Authentication Method
Accounts and Roles
Windows Service
Server File Permissions
Apply Configuration
Apply Configuration
The following configuration steps are being executed.
Configuration Steps
Log
Writing configuration file
Updating Windows Firewall rules
Adjusting Windows service
Initializing database (may take a long time) .
Updating permissions for the data folder and related server files
Starting the server
Applying security settings
Updating the Start menu link
Execute
Cancel

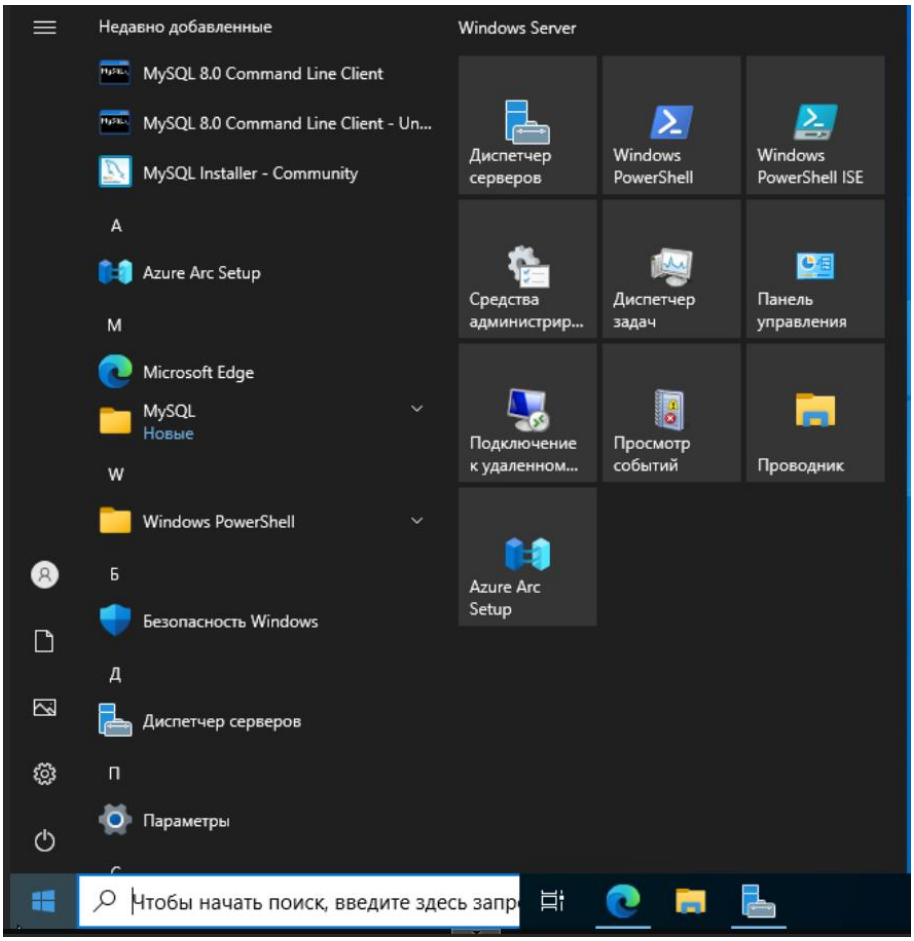

MySQL Installer
MySQL. Installer
MySQL Server 8.0.41
Type and Networking
Authentication Method
Accounts and Roles
Windows Service
Server File Permissions
Apply Configuration
Apply Configuration
The configuration operation has completed.
Configuration Steps
Log
Writing configuration file
Updating Windows Firewall rules
Adjusting Windows service
Initializing database (may take a long time)
Updating permissions for the data folder and related server files
Starting the server
Applying security settings
Updating the Start menu link
The configuration for MySQL Server 8.0.41 was successful.
Click Finish to continue.
Finish
Активация Windows
Чтобы активировать Win


MySQL Installer
MySQL. Installer
Adding Community
Choosing a Setup Type
Check Requirements
Installation
Product Configuration
Installation Complete
Product Configuration
We'll now walk through a configuration wizard for each of the following products.
You can cancel at any point if you wish to leave this wizard without configuring all the products.
Product
Status
MySQL Server 8.0.41
Configuration complete.
Next >
Cancel
Активация Windows

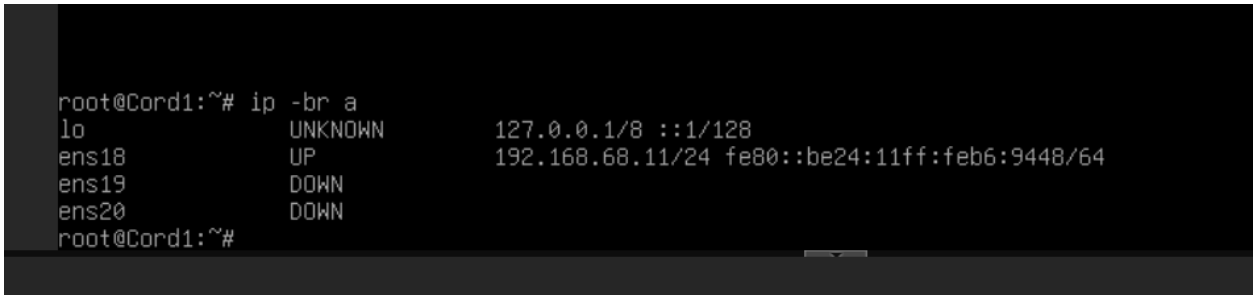
Все вы установили MySQL.



Установленый mySQL

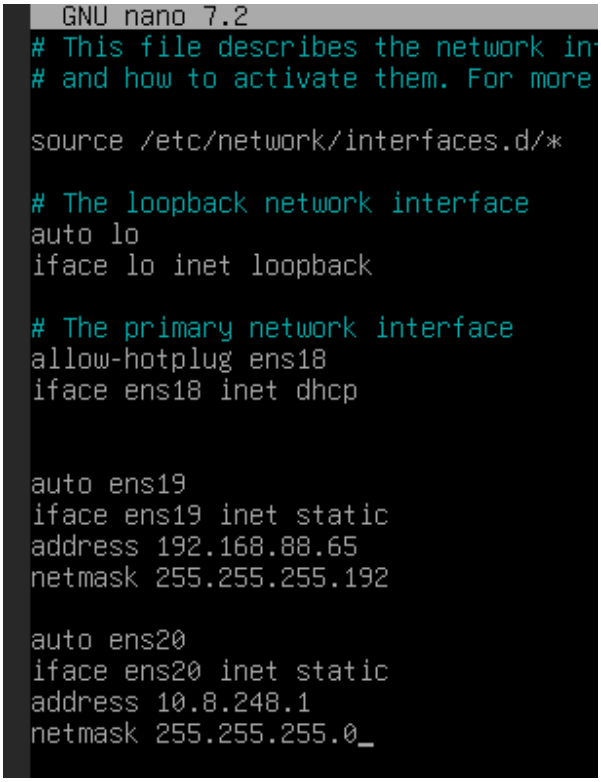


Далее был запущен линукс Cord1. Командой «ip -br a» были проверены сетевые адаптеры



Далее командой nano был открыт конфиграционный файл

Ниже показан конфиграционный файл адаптеров. Адаптер ens19 находится в 1 сети с сервером виндовс, ens20 с Cord2 в 1 сети



Далее необходимо перезапустить службу сети и проверить конфигурацию адаптеров. Если адрес не пришел и не включились адаптеры скорее всего где то ошиблись в конфиге

```
root@Cord1:~# systemctl restart networking
root@Cord1:~# ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens18            UP             192.168.68.11/24 fe80::be24:11ff:feb6:9448/64
ens19            UP             192.168.88.65/26 fe80::be24:11ff:fe69:8137/64
ens20            UP             10.8.248.1/24 fe80::be24:11ff:feff:ea7f/64
root@Cord1:~# _
```

Ниже представлен конфиграционный файл для виртуалки Cord2

```
  GNU nano 7.2
# This file describes the network in
# and how to activate them. For more

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens18
iface ens18 inet dhcp


auto ens19
iface ens19 inet static
address 10.10.20.129
netmask 255.255.255.128

auto ens20
iface ens20 inet static
address 10.8.248.2
netmask 255.255.255.0
```

Далее точно так же необходимо перезапусти службы интернета.

```
root@Cord2:~# systemctl restart networking
root@Cord2:~# ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens18            UP             192.168.68.22/24 fe80::be24:11ff:fe2e:d29c/64
ens19            UP             10.10.20.129/25 fe80::be24:11ff:fe21:393e/64
ens20            UP             10.8.248.2/24 fe80::be24:11ff:fea5:d476/64
root@Cord2:~# _
```

После настроек проверьте подключение между кордами, если пинги не идут тогда:

1. Ошибка в адресе, маске или файле конфигурации
2. Адаптеры не в одной сети

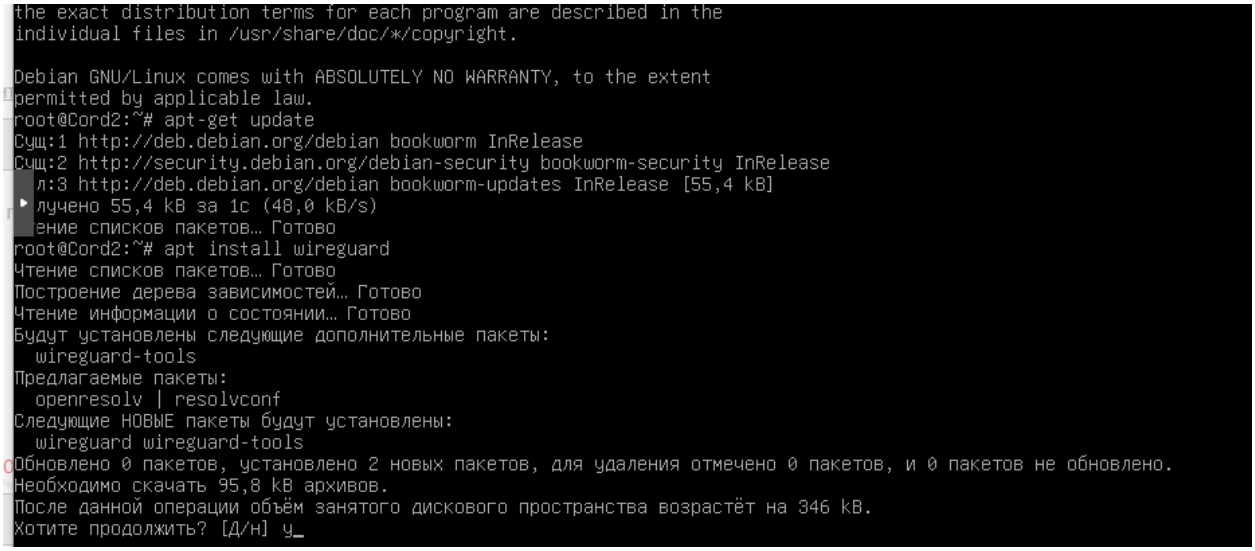
```
root@Cord2:~# ping 10.8.248.1
PING 10.8.248.1 (10.8.248.1) 56(84) bytes of data.
64 bytes from 10.8.248.1: icmp_seq=1 ttl=64 time=0.650 ms
64 bytes from 10.8.248.1: icmp_seq=2 ttl=64 time=0.289 ms
64 bytes from 10.8.248.1: icmp_seq=3 ttl=64 time=0.246 ms
64 bytes from 10.8.248.1: icmp_seq=4 ttl=64 time=0.267 ms
^C
--- 10.8.248.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
rtt min/avg/max/mdev = 0.246/0.363/0.650/0.166 ms
root@Cord2:~#
```

```
root@Cord1:~# ping 10.8.248.2
PING 10.8.248.2 (10.8.248.2) 56(84) bytes of data.
64 bytes from 10.8.248.2: icmp_seq=1 ttl=64 time=0.404 ms
64 bytes from 10.8.248.2: icmp_seq=2 ttl=64 time=0.260 ms
64 bytes from 10.8.248.2: icmp_seq=3 ttl=64 time=0.258 ms
^C
--- 10.8.248.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2039ms
rtt min/avg/max/mdev = 0.258/0.307/0.404/0.068 ms
root@Cord1:~#
```

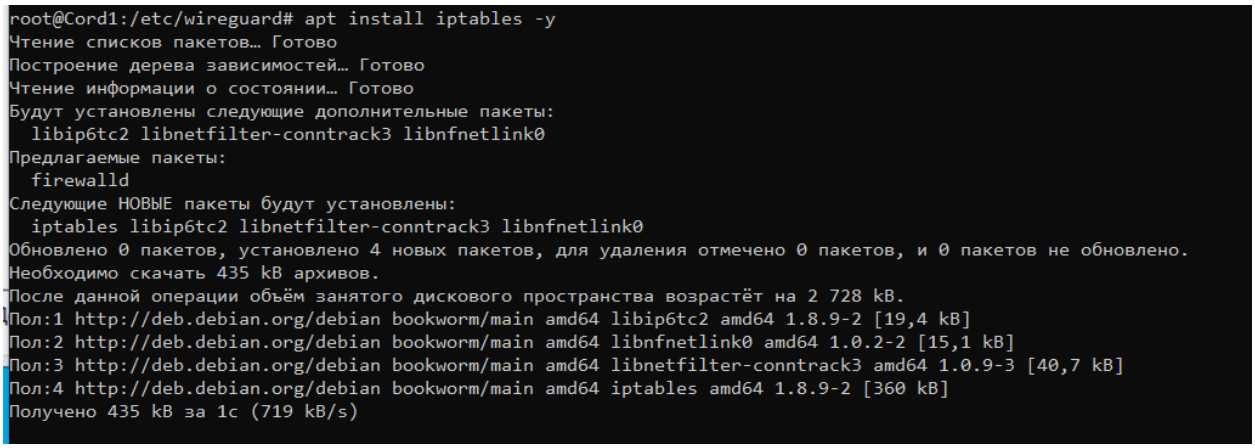
Так же с Cord1 был пропингован виндовс сервер

```
root@Cord1:~# ping 192.168.88.66
PING 192.168.88.66 (192.168.88.66) 56(84) bytes of data.
64 bytes from 192.168.88.66: icmp_seq=1 ttl=128 time=0.759 ms
64 bytes from 192.168.88.66: icmp_seq=2 ttl=128 time=0.262 ms
64 bytes from 192.168.88.66: icmp_seq=3 ttl=128 time=0.368 ms
64 bytes from 192.168.88.66: icmp_seq=4 ttl=128 time=0.340 ms
64 bytes from 192.168.88.66: icmp_seq=5 ttl=128 time=0.361 ms
64 bytes from 192.168.88.66: icmp_seq=6 ttl=128 time=0.346 ms
64 bytes from 192.168.88.66: icmp_seq=7 ttl=128 time=0.307 ms
^C
--- 192.168.88.66 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6100ms
rtt min/avg/max/mdev = 0.262/0.391/0.759/0.153 ms
root@Cord1:~#
```

Если wireguard не установлен на дебиан, тогда установите его командой «apt install wireguard»



Так же скачайте iptables, в дальнейшем они понядабятся для настроен нат и маршрутизации.



ВНИМАНИЕ СЕЙЧАС БУДЕТ НАСТРОИВАТЬСЯ ВПН МЕЖДУ Net2-Coord и Net2-Client

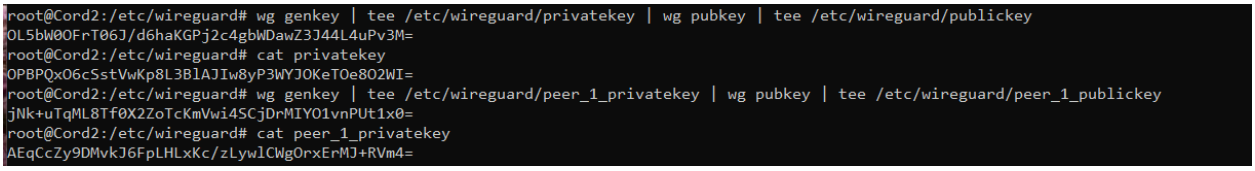
Перейдем на cord2

Сначала командой «cd /etc/wireguard» необходимо перейти в дерикторию ваер гуард

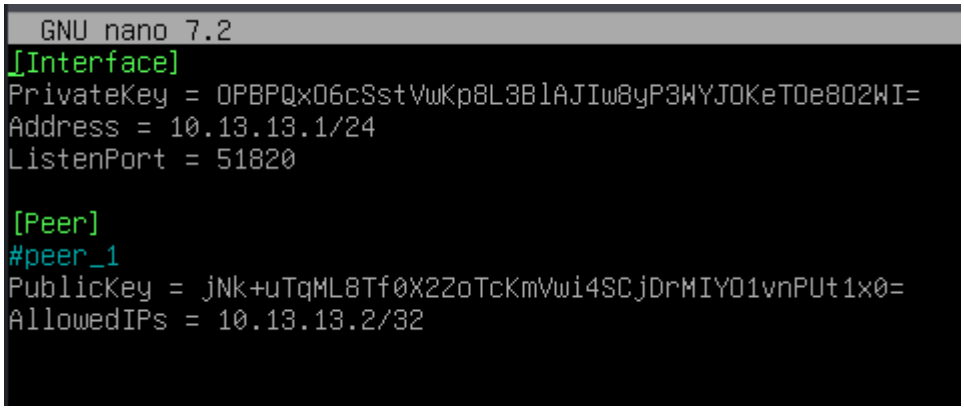
Затем необходимо сгененрировать открытый и закрытый ключ сервера командой:

«wg genkey | tee /etc/wireguard/privatekey | wg pubkey | tee /etc/wireguard/publickey» После данной комады атоматиески выводится ПУБЛИЧНЫЙ ключ, затем командой «cat privatekey» выводится закрытый ключ.

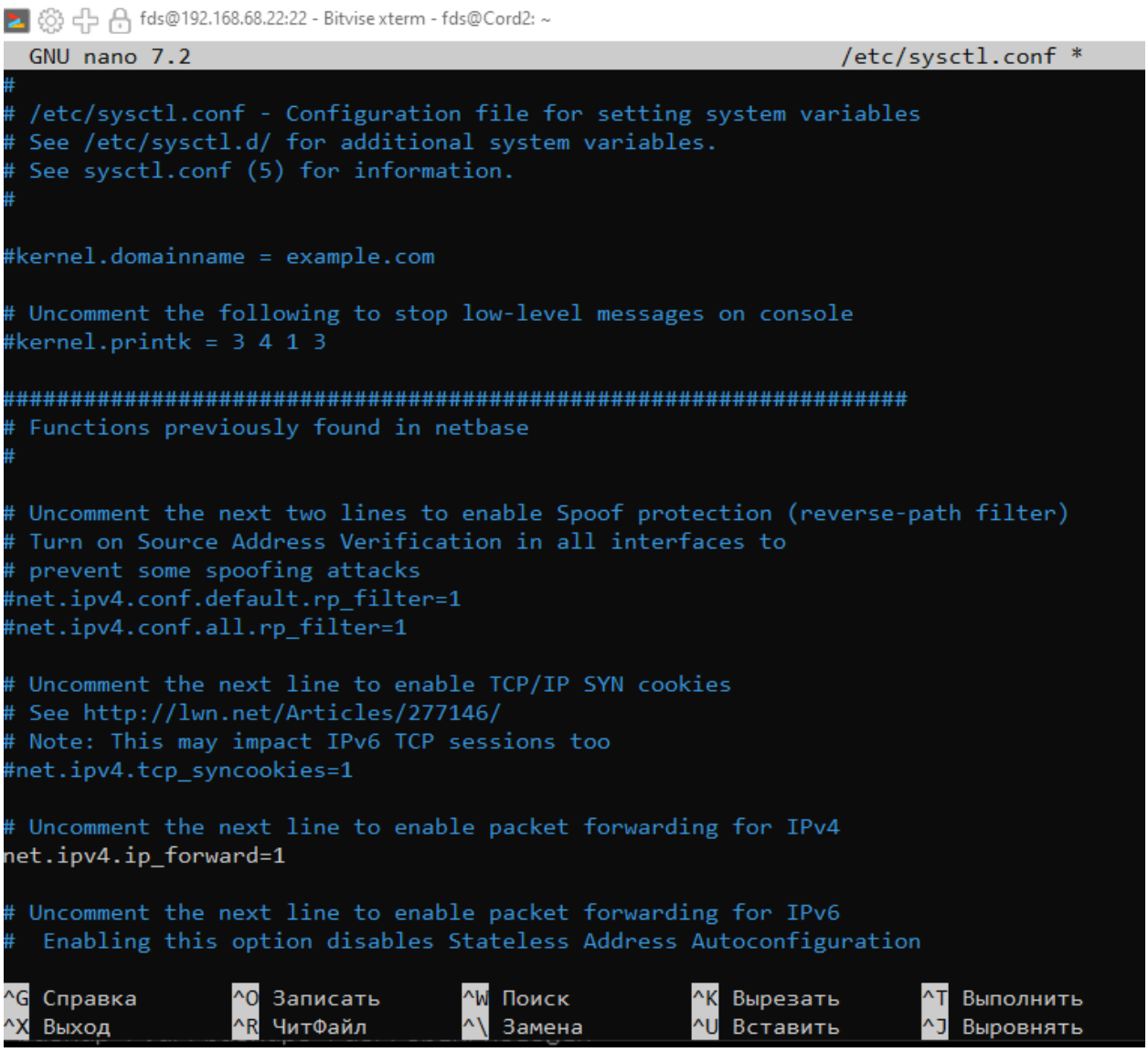
Далее необзодимо сгененрирвоать открытый и закрытый ключ клиента командой: «wg genkey | tee /etc/wireguard/peer_1_privatekey | wg pubkey | tee /etc/wireguard/peer_1_publickey». Так же после ввода команды отображатся публичный ключ и командой «cat peer_1_privatekey» приватный ключ.



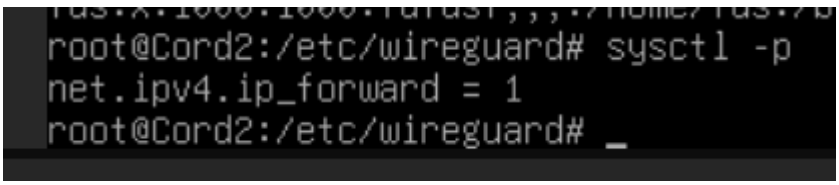
После командой nano создаем файл wg0.conf и внем прописывамся следующие строки. Далее комбинациями ctrl+s ctr+x сохраняем содержимое и выходим из файла



Затем командой «nano /etc/sysctl.conf» открываем файл и ищем строчку net.ipv4.ip_forward=1, ее необходимо расскоментировать, так же может стоять значение 0 его необхожимо заменить на значение 1.



Затем командой sysctl -p необходимо сохранить изменения



Далее командами «wg-quick up wg0» и «systemctl enable wg-quick@wg0» был включен тунель на адаптер wg0 и включен в автозагрузку.

```
root@Cord2:~# systemctl enable wg-quick@wg0
Created symlink /etc/systemd/system/multi-user.target.wants/wg-quick@wg0.service → /lib/systemd/system/wg-quick@.service.
root@Cord2:~#
```

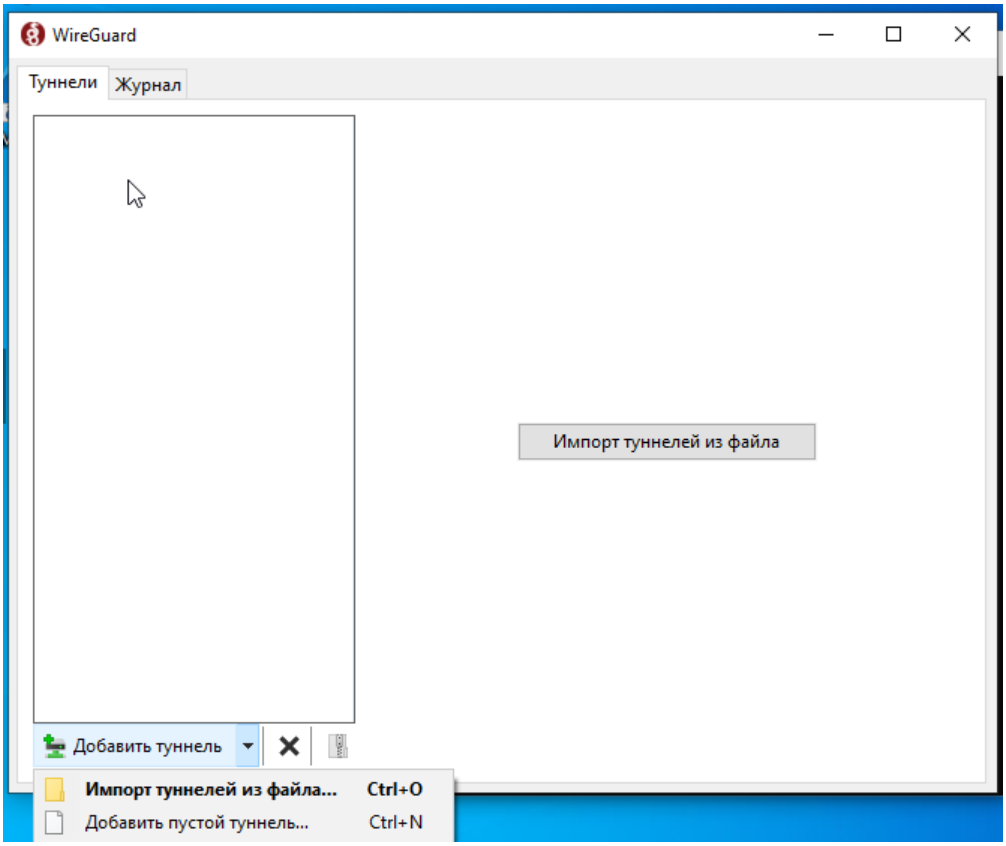
```
root@Cord2:/etc/wireguard# wg-quick up wg0
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.13.13.1/24 dev wg0
[#] ip link set mtu 1420 up dev wg0
[#] iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o ens19 -j MASQUERADE
```

Здесь я чисто для проверки перезапускал адаптер и проверял его статус.

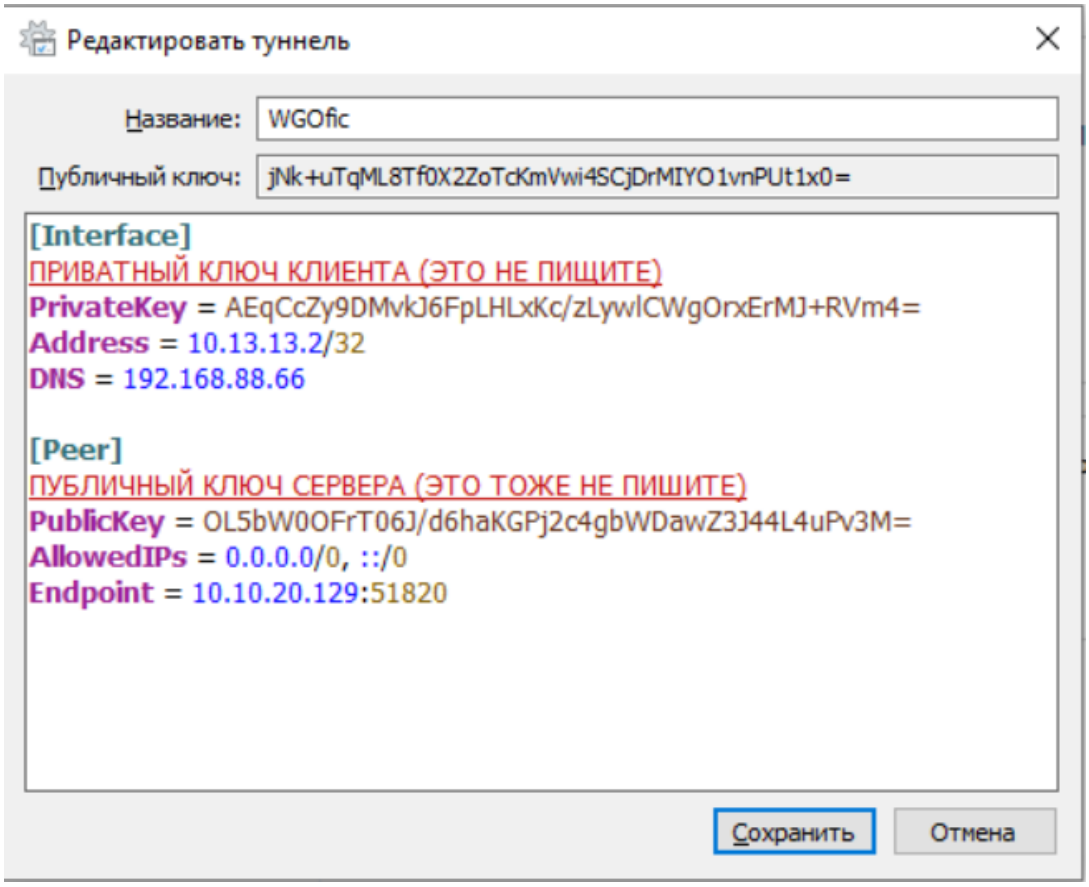
```
root@Cord2:/etc/wireguard# systemctl restart wg-quick@wg0
root@Cord2:/etc/wireguard# systemctl status wg-quick@wg0
● wg-quick@wg0.service - WireGuard via wg-quick(8) for wg0
     Loaded: loaded (/lib/systemd/system/wg-quick@.service; disabled; preset: enabled)
     Active: active (exited) since Wed 2025-05-28 21:56:36 MSK; 2s ago
       Docs: man:wg-quick(8)
             man:wg(8)
             https://www.wireguard.com/
             https://www.wireguard.com/quickstart/
             https://git.zx2c4.com/wireguard-tools/about/src/man/wg-quick.8
             https://git.zx2c4.com/wireguard-tools/about/src/man/wg.8
    Process: 712 ExecStart=/usr/bin/wg-quick up wg0 (code=exited, status=0/SUCCESS)
   Main PID: 712 (code=exited, status=0/SUCCESS)
        CPU: 36ms

мая 28 21:56:36 Cord2 systemd[1]: Starting wg-quick@wg0.service - WireGuard via wg-quick(8) for wg0...
мая 28 21:56:36 Cord2 wg-quick[712]: [#] ip link add wg0 type wireguard
мая 28 21:56:36 Cord2 wg-quick[712]: [#] wg setconf wg0 /dev/fd/63
мая 28 21:56:36 Cord2 wg-quick[712]: [#] ip -4 address add 10.0.1.1/24 dev wg0
мая 28 21:56:36 Cord2 wg-quick[712]: [#] ip link set mtu 1420 up dev wg0
мая 28 21:56:36 Cord2 wg-quick[712]: [#] iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o ens19 -j MASQUERADE
мая 28 21:56:36 Cord2 systemd[1]: Finished wg-quick@wg0.service - WireGuard via wg-quick(8) for wg0.
root@Cord2:/etc/wireguard#
```

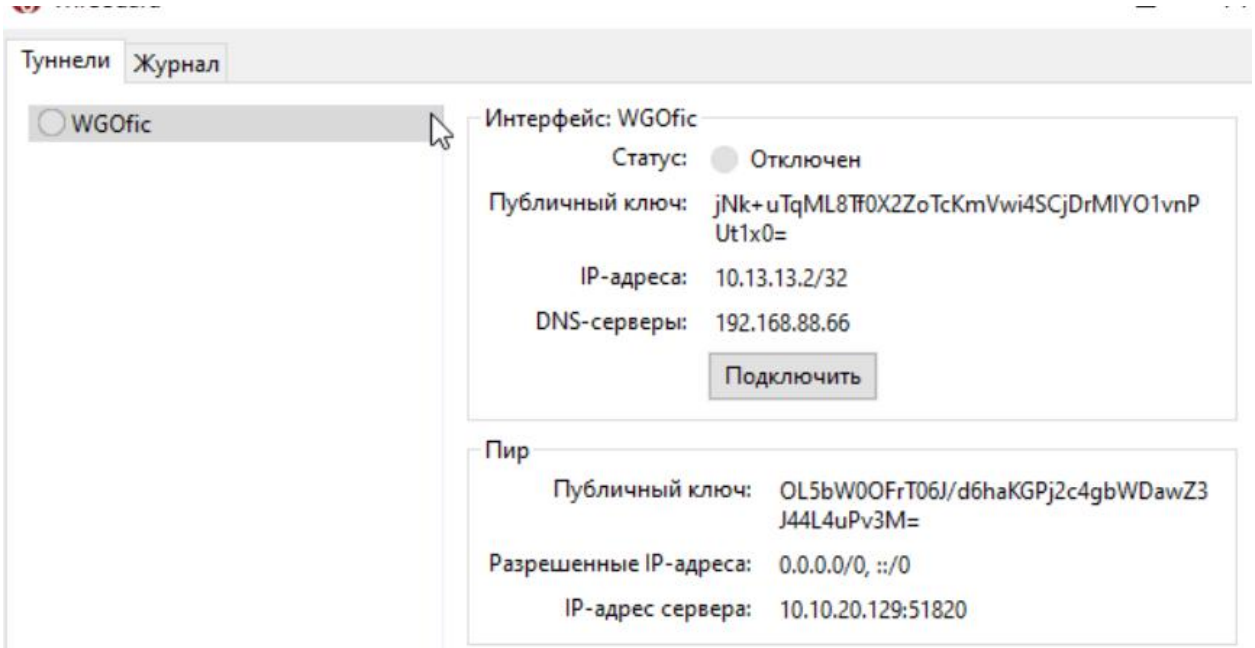
Далее необзодимо перейти на Net2-Client и нажать на стрелочку у «Добавить туннель» затем «Добавить пустой тунелль»

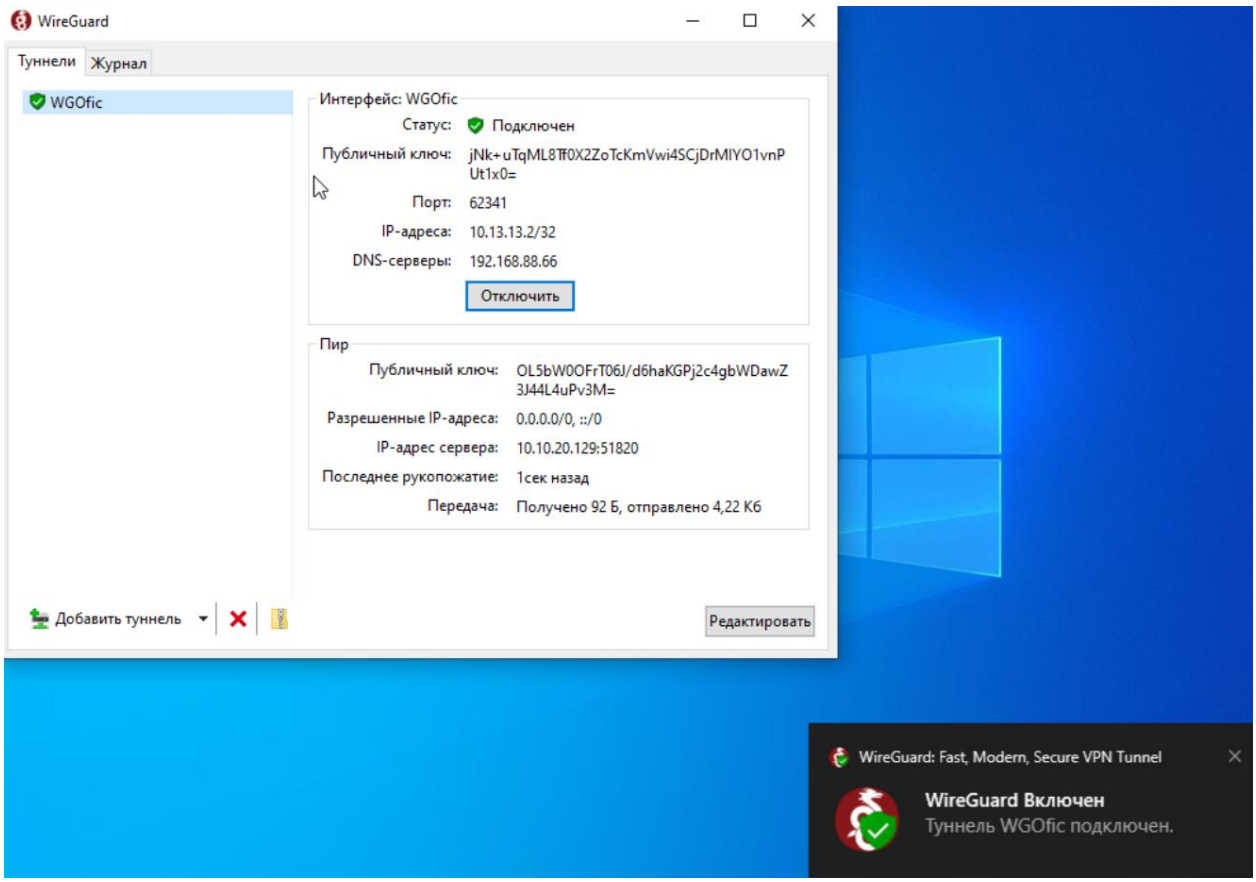


В открывшемся окне необходимо указать ПРИВАТНЫЙ КЛЮЧ КЛИЕНТА И СЕРВЕРА КОТОЫРЙ МЫ СОЗДАВАЛИ НА LINUX



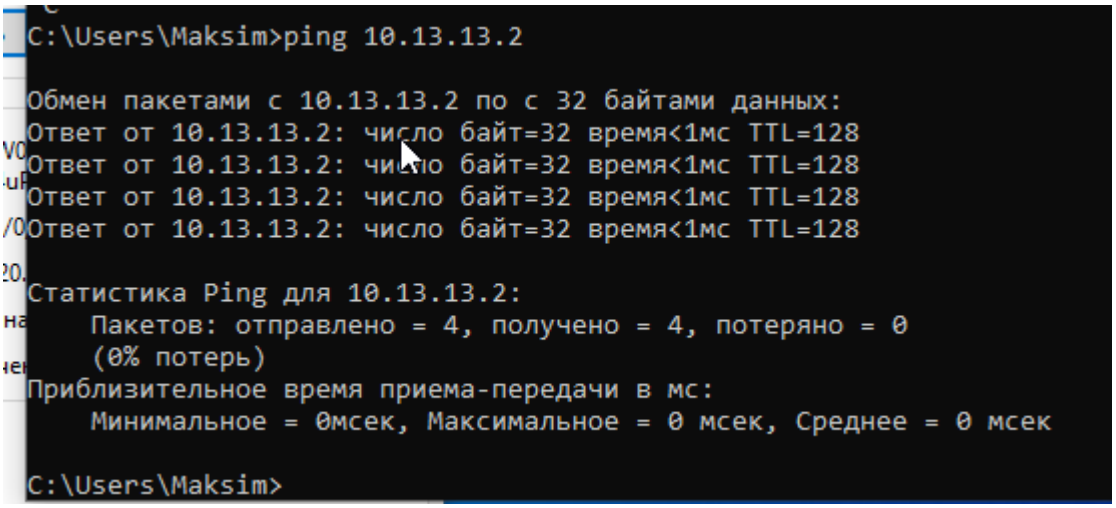
Затем после нажатия кнопки «Сохранить» тунель автоматически появится в списке и при нажатии «Подключить» произойдет подключение к серверу

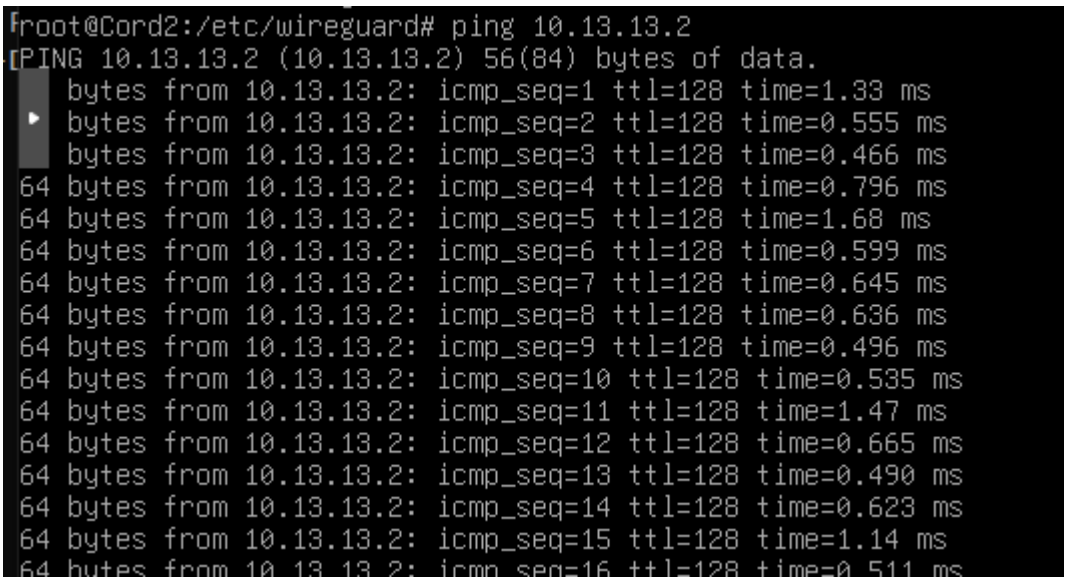




Далее для проверки корд2 и клиент обменялись пингами ЕСЛИ у вас не идут пинги тогда:

1. Адаптеры на котором работает впн находятся в разных сетях
2. Вы намудрили с открытми и закрытыми ключами перепутав их местами




root@Cord2:/etc/wireguard# ping 10.13.13.2
PING 10.13.13.2 (10.13.13.2) 56(84) bytes of data.
bytes from 10.13.13.2: icmp_seq=1 ttl=128 time=1.33 ms
bytes from 10.13.13.2: icmp_seq=2 ttl=128 time=0.555 ms
bytes from 10.13.13.2: icmp_seq=3 ttl=128 time=0.466 ms
64 bytes from 10.13.13.2: icmp_seq=4 ttl=128 time=0.796 ms
64 bytes from 10.13.13.2: icmp_seq=5 ttl=128 time=1.68 ms
64 bytes from 10.13.13.2: icmp_seq=6 ttl=128 time=0.599 ms
64 bytes from 10.13.13.2: icmp_seq=7 ttl=128 time=0.645 ms
64 bytes from 10.13.13.2: icmp_seq=8 ttl=128 time=0.636 ms
64 bytes from 10.13.13.2: icmp_seq=9 ttl=128 time=0.496 ms
64 bytes from 10.13.13.2: icmp_seq=10 ttl=128 time=0.535 ms
64 bytes from 10.13.13.2: icmp_seq=11 ttl=128 time=1.47 ms
64 bytes from 10.13.13.2: icmp_seq=12 ttl=128 time=0.665 ms
64 bytes from 10.13.13.2: icmp_seq=13 ttl=128 time=0.490 ms
64 bytes from 10.13.13.2: icmp_seq=14 ttl=128 time=0.623 ms
64 bytes from 10.13.13.2: icmp_seq=15 ttl=128 time=1.14 ms

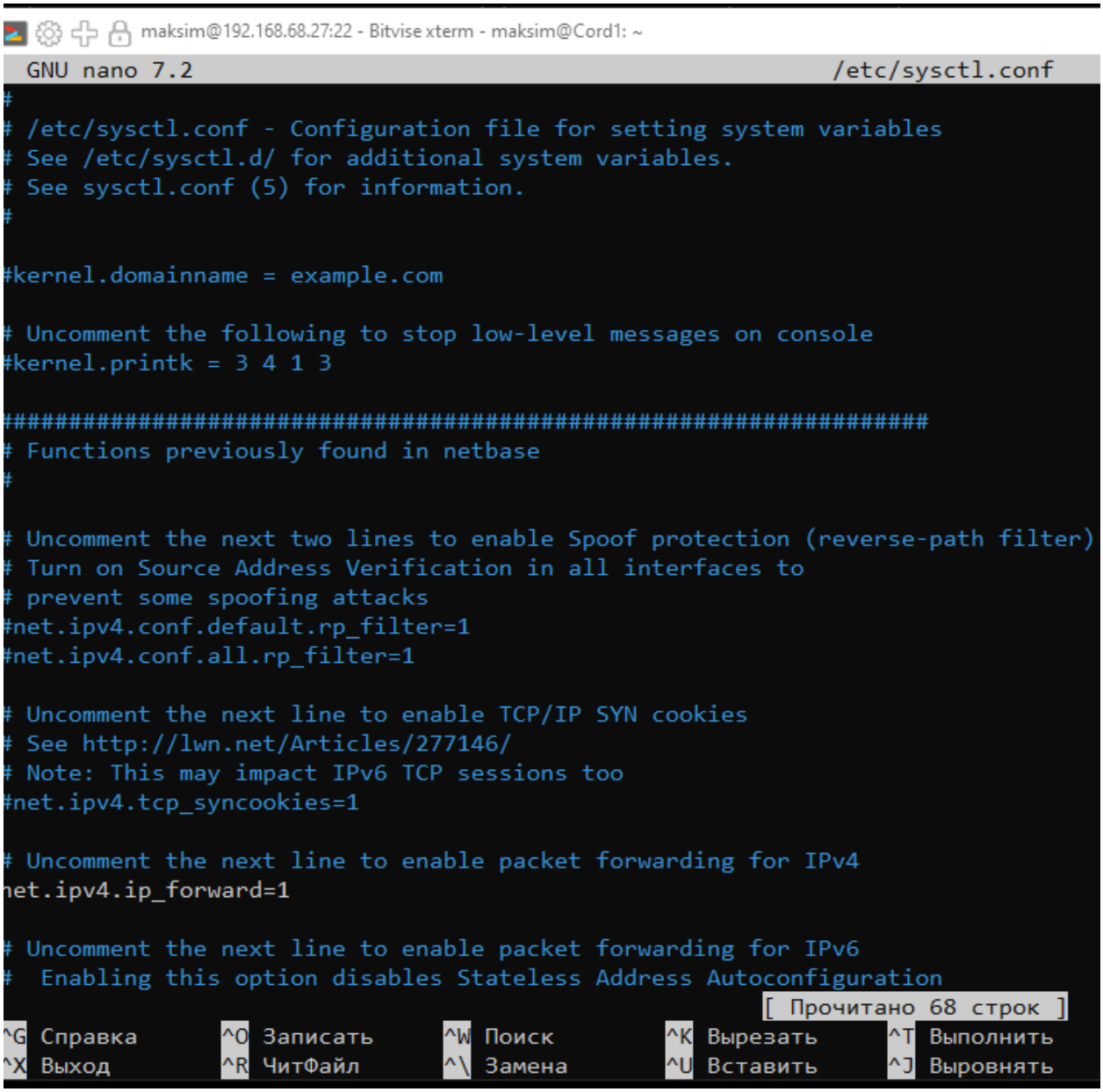
ДАЛЕЕ НАСТРАИВАЕТСЯ ВПН МЕЖДУ Net1-AdminCA И Net1-Coord.

ПРОЦЕСС СОЗДАНИЯ ТУНЕЛЯ ИНДЕТИЧЕН ПОЭТОМУ РАСПИСЫВАТЬ Я ЕГО НЕ БУДУ

```
root@Cord1:/etc/wireguard# wg genkey | tee /etc/wireguard/privatekey | wg pubkey | tee /etc/wireguard/publickey
7As0aOJMbzwrvYeDFTHhH1qliP4LyDl4yjiAUWMlv0M=
root@Cord1:/etc/wireguard# cat privatekey
yOeWTPb4FEBExT1+GT25+n7nAP2GEopE0T1EXJrwXV0=
root@Cord1:/etc/wireguard#
root@Cord1:/etc/wireguard#
root@Cord1:/etc/wireguard# wg genkey | tee /etc/wireguard/peer_1_privatekey | wg pubkey | tee /etc/wireguard/peer_1_publickey
IAkk0eRD+x60nL3g4s4+dVpshiUhR4DNHY7E/D3bXUo=
root@Cord1:/etc/wireguard# cat peer_1_privatekey
0Bb6Gq/l4pQtYXtfIjWE10hE6Lx47ItmhU/ycuOLjm4=
root@Cord1:/etc/wireguard#
```

```
  GNU nano 7.2
[Interface]
#Секретный ключ сервера
PrivateKey = yOeWTPb4FEBExT1+GT25+n7nAP2GEopE0T1EXJrwXV0=
Address = 10.11.12.1/24
ListenPort = 51820

[Peer]
#peer_1 публичный ключ клиента
PublicKey = IAkk0eRD+x60nL3g4s4+dVpshiUhR4DNHY7E/D3bXUo=
AllowedIPs = 10.11.12.2/32
```

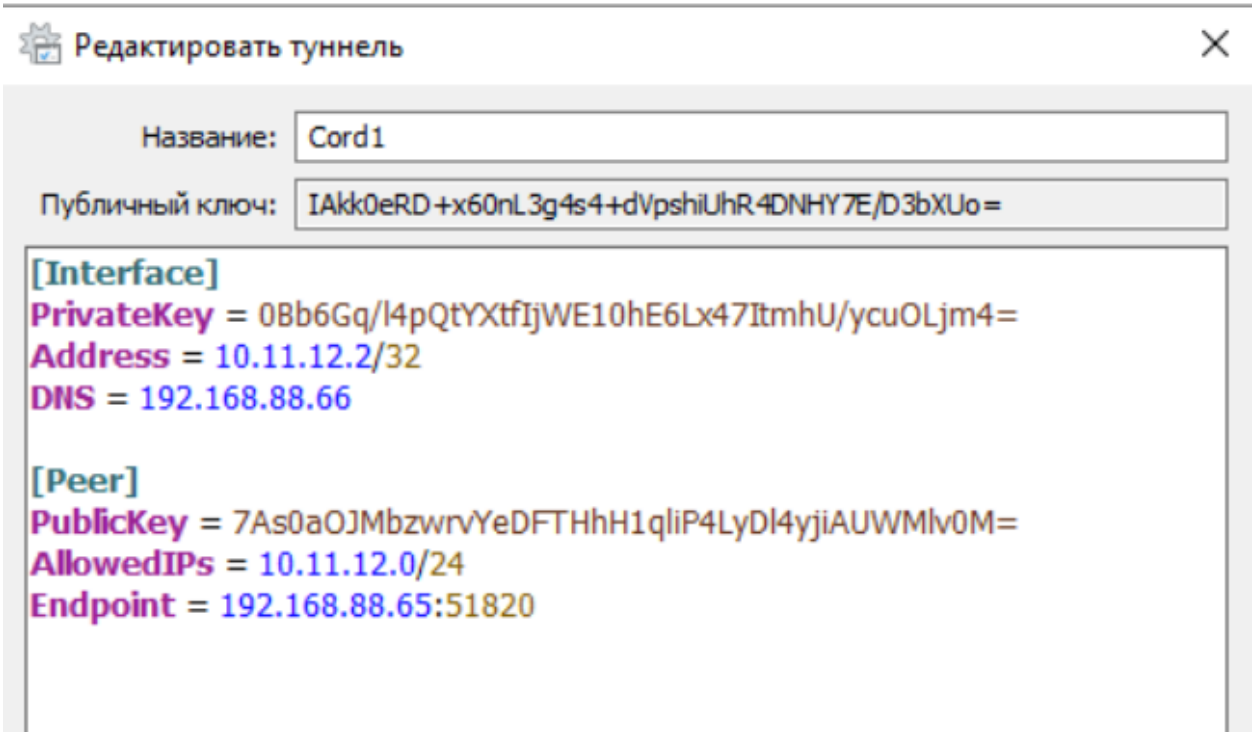



```
root@Cord1:/etc/wireguard# wg-quick up wg0
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.11.12.1/24 dev wg0
[#] ip link set mtu 1420 up dev wg0
[#] iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o ens19 -j MASQUERADE
/usr/bin/wg-quick: line 295: iptables: command not found
[#] ip link delete dev wg0
root@Cord1:/etc/wireguard# systemctl enable wg-quick@wg0
Created symlink /etc/systemd/system/multi-user.target.wants/wg-quick@wg0.service → /lib/systemd/system/wg-quick@.service.
root@Cord1:/etc/wireguard#
```

```
root@Cord1:/etc/wireguard# systemctl start wg-quick@wg0
```

Тут стоит сказать пару слов, собственно зачем мы качаем iptables, на данном рисунке настраиваются политики чтобы когда включался впн на сервере клиенты не теряли его внутри локальной сети и локальный трафик не уходил за предели сетки, и только выходной и входной трафик попадает в впн тунель.

```
root@Cord1:/etc/wireguard# sudo iptables -A FORWARD -i ens19 -o wg0 -j ACCEPT
root@Cord1:/etc/wireguard# sudo iptables -A FORWARD -i wg0 -o ens19 -j ACCEPT
root@Cord1:/etc/wireguard# sudo iptables -t nat -A POSTROUTING -o ens19 -j MASQUERADE
root@Cord1:/etc/wireguard# sudo iptables -t nat -A POSTROUTING -s 192.168.88.0/24 -d 192.168.88.0/24 -j RETURN
root@Cord1:/etc/wireguard#
```



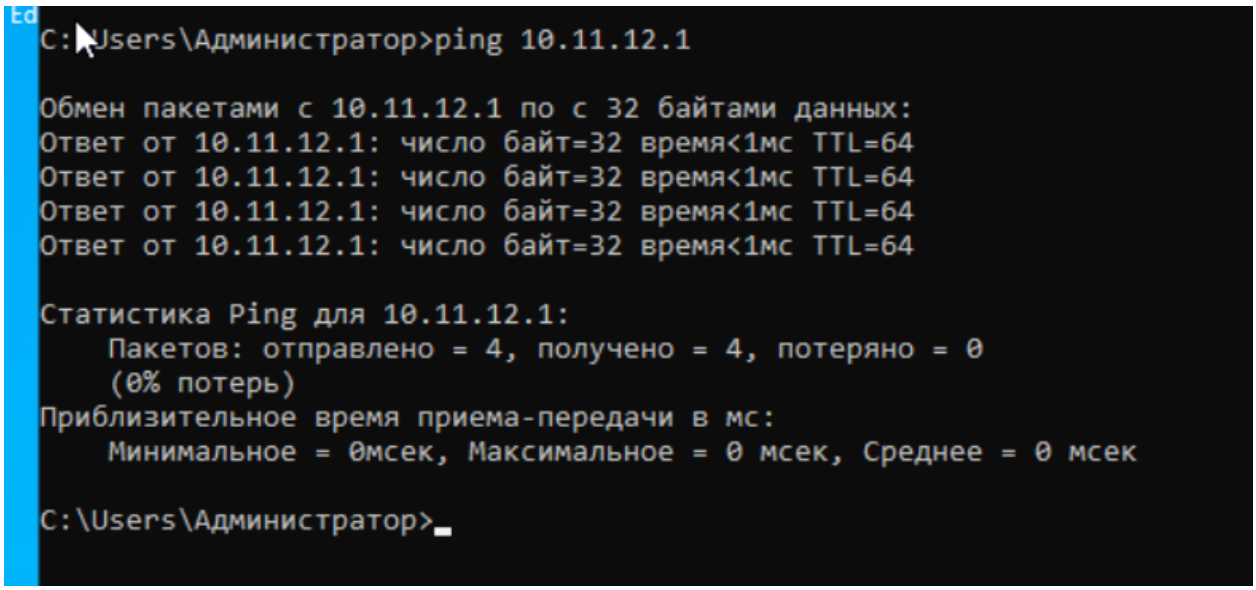
Так же чтобы ранее настроеные правила в линукс работали необходимо у сервера прописать маршруты для внутреней сетки

```
C:\Users\Администратор>route -p add 192.168.88.0 mask 255.255.255.0 192.168.88.66
 OK

C:\Users\Администратор>
```


Далее впн был проверен

```
root@Cord1:/etc/wireguard# ping 10.11.12.2
PING 10.11.12.2 (10.11.12.2) 56(84) bytes of data.
64 bytes from 10.11.12.2: icmp_seq=1 ttl=128 time=0.514 ms
64 bytes from 10.11.12.2: icmp_seq=2 ttl=128 time=0.393 ms
64 bytes from 10.11.12.2: icmp_seq=3 ttl=128 time=0.425 ms
```


C:\Users\Администратор>ping 10.11.12.1
Обмен пакетами с 10.11.12.1 по с 32 байтами данных:
Ответ от 10.11.12.1: число байт=32 время<1мс TTL=64
Ответ от 10.11.12.1: число байт=32 время<1мс TTL=64
Ответ от 10.11.12.1: число байт=32 время<1мс TTL=64
Ответ от 10.11.12.1: число байт=32 время<1мс TTL=64
Статистика Ping для 10.11.12.1:
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потерь)
Приблизительное время приема-передачи в мс:
Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
C:\Users\Администратор>

НАСТРОЙКА МАРШРУТИЗАЦИИ МЕЖДУ КОРДАМИ

Вспоминаем циско и то как писали маршруты, это необходимо для того чтобы каждый корд знал какая есть сетка у его соседа и в случае чего понимал куда ему гнать траффик, командами ниже мы сообщаем координаторам трафик из какой сети гнать на какой адрес и в какой адаптер

```
root@Cord2:~# sudo ip route add 10.11.12.0/24 via 10.8.248.1 dev ens20
root@Cord2:~#
```

```
root@Cord2:/etc/wireguard# ip route add 192.168.88.0/24 via 10.8.248.1 dev ens20
```

```
root@Cord1:~# sudo ip route add 10.10.20.128/25 via 10.8.248.2 dev ens20
```

```
root@Cord1:~# sudo ip route add 10.13.13.0/24 via 10.8.248.2 dev ens20
root@Cord1:~#
```

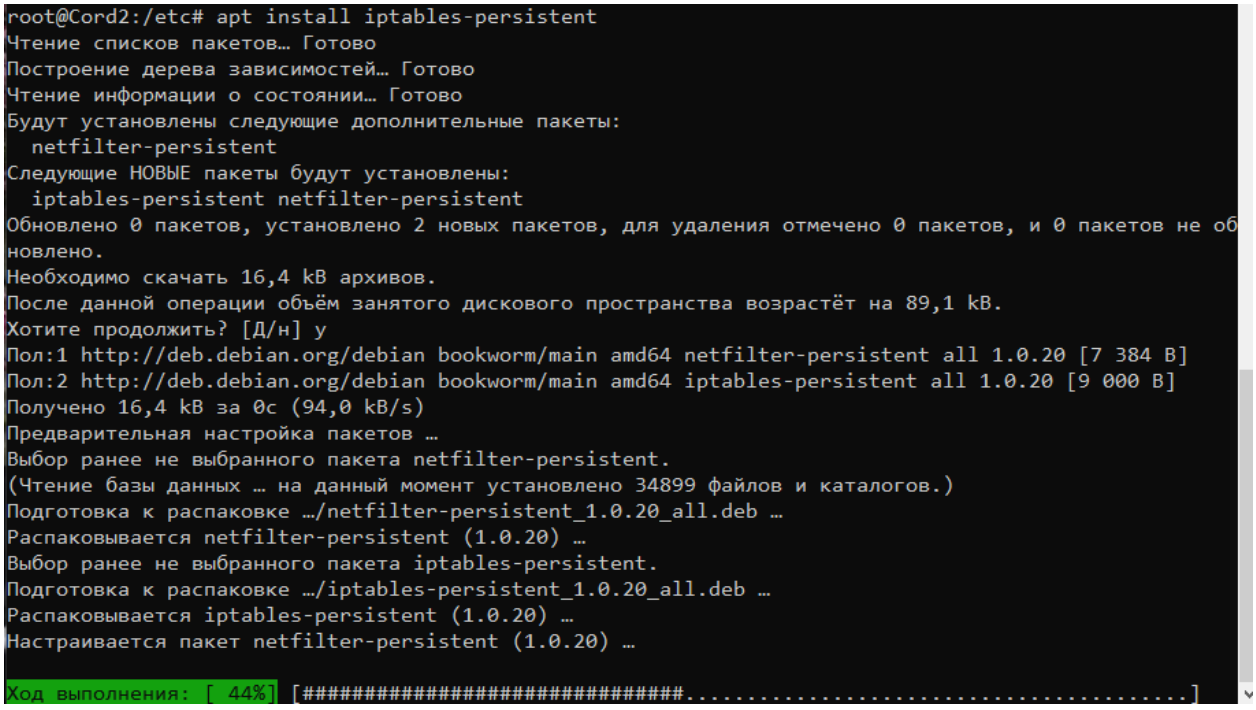
Пути корд1

```
default via 192.168.68.1 dev ens18
10.8.248.0/24 dev ens20 proto kernel scope link src 10.8.248.1
10.10.20.128/25 via 10.8.248.2 dev ens20
10.11.12.0/24 dev wg0 proto kernel scope link src 10.11.12.1
10.13.13.0/24 via 10.8.248.2 dev ens20
192.168.68.0/24 dev ens18 proto kernel scope link src 192.168.68.27
192.168.88.64/26 dev ens19 proto kernel scope link src 192.168.88.65
root@Cord1:~#
```

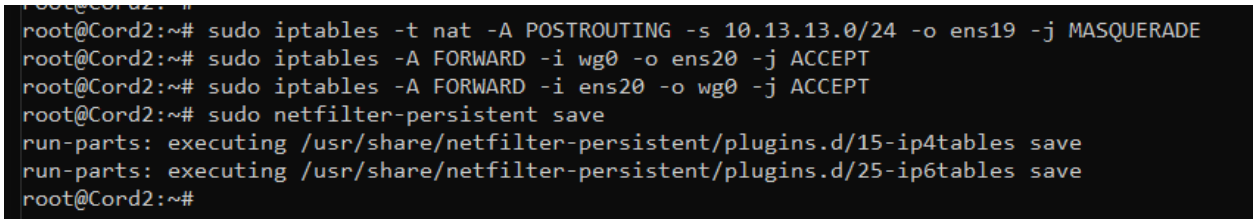
Пути корд2

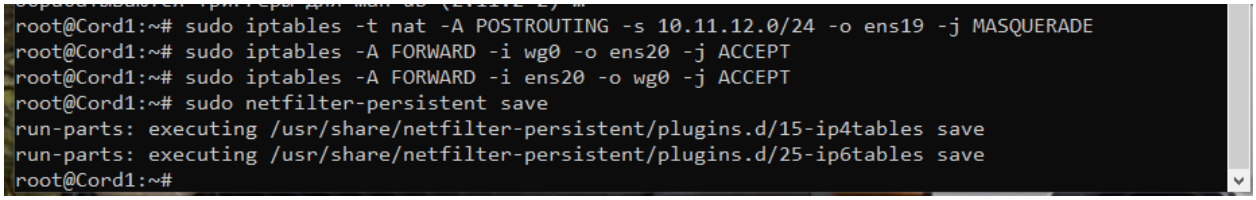
```
root@Cord2:/etc/wireguard# ip route
default via 192.168.68.1 dev ens18
10.8.248.0/24 dev ens20 proto kernel scope link src 10.8.248.2
10.10.20.128/25 dev ens19 proto kernel scope link src 10.10.20.129
10.11.12.0/24 via 10.8.248.1 dev ens20
10.13.13.0/24 dev wg0 proto kernel scope link src 10.13.13.1
192.168.68.0/24 dev ens18 proto kernel scope link src 192.168.68.24
192.168.88.0/24 via 10.8.248.1 dev ens20
root@Cord2:/etc/wireguard#
```

Для сохранения правил iptables установим «iptables-persistent»



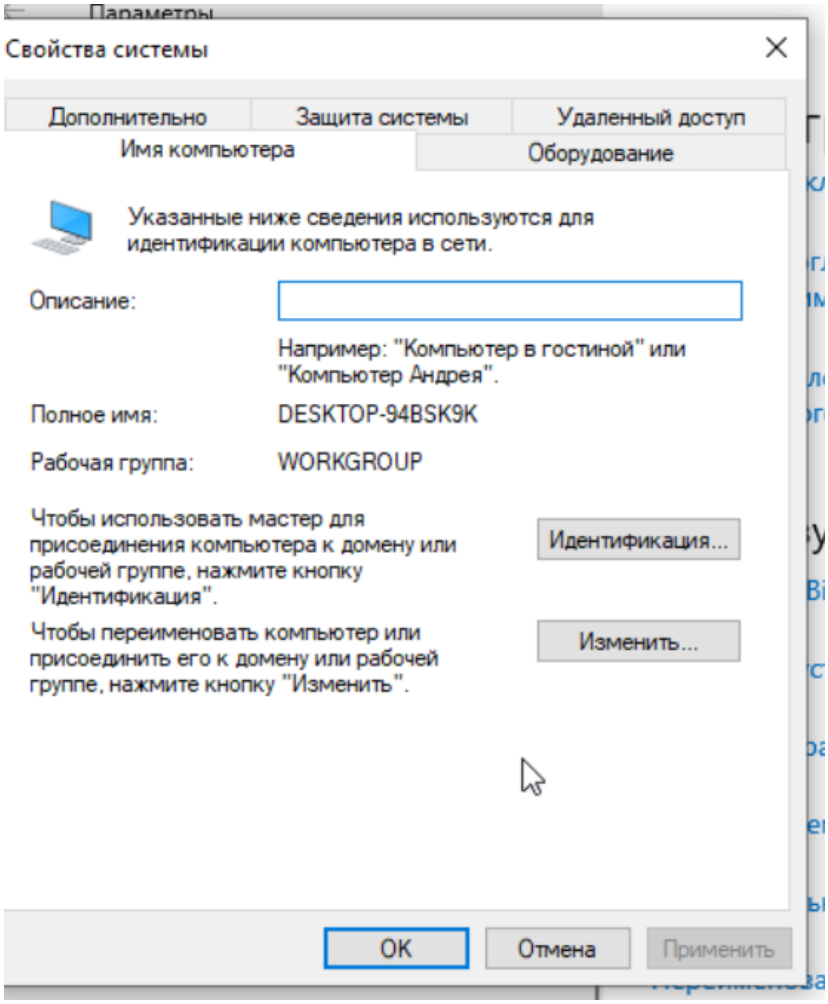
Далее натроены маршрутизации для впн и сохранены

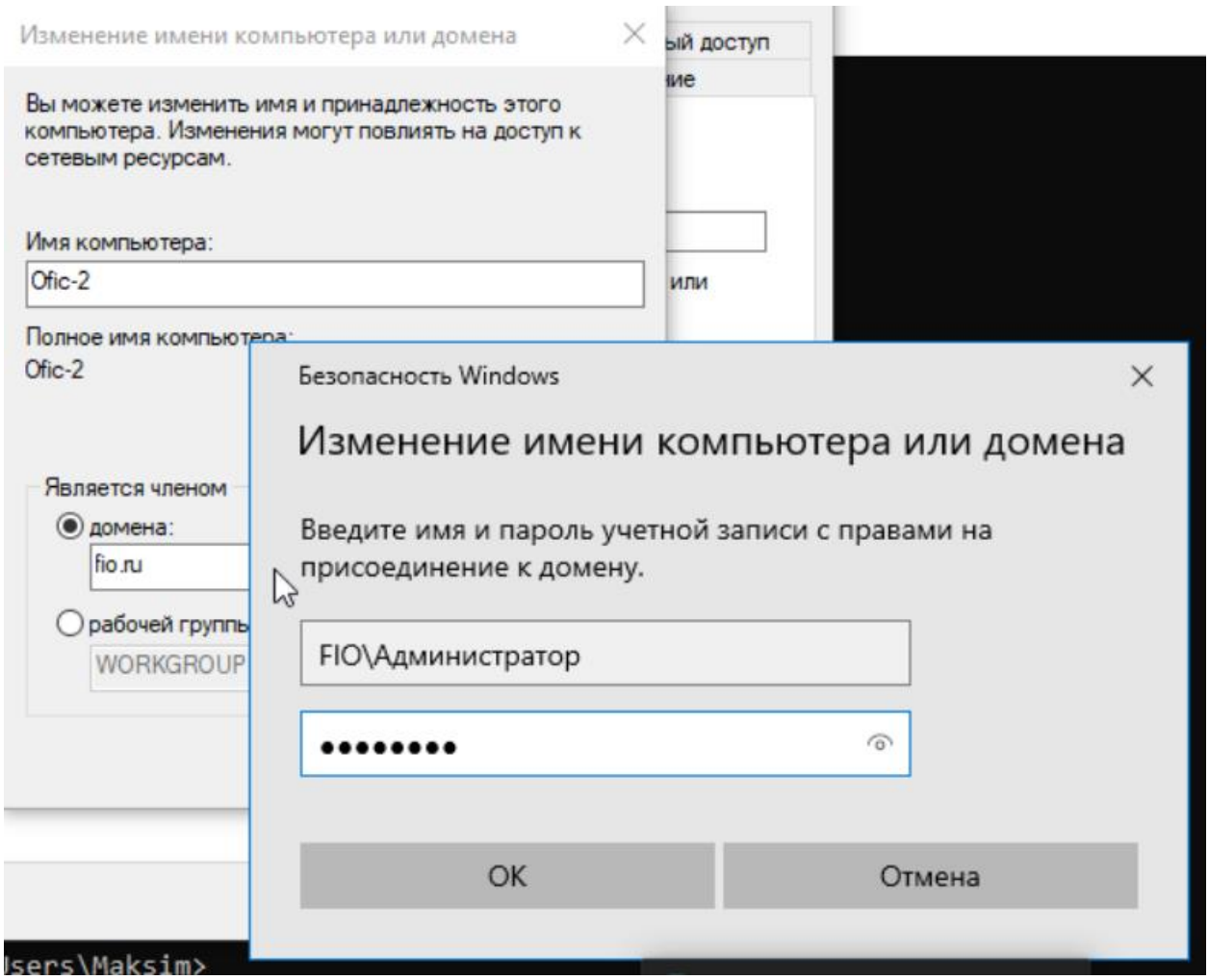


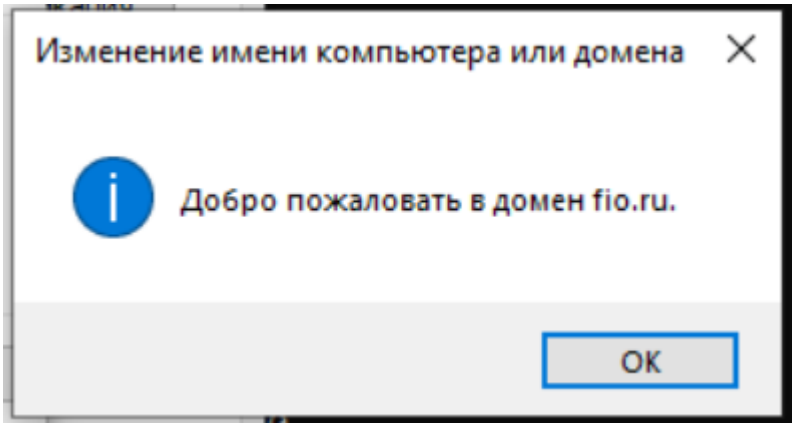


Далее нобохидомо перейти попути «Пуск»>«Параметры»>«Система»>«О программе»>«Переименовать этот ПК для опытных пользователей». Тогда откроется окно где необходимо указать имя пк и домен. Если впн имаршрутизация настроена верно тогда клиент войдет в домен без проблем, главное указать верные данные админа. Данное действие выполняется на Net2-client

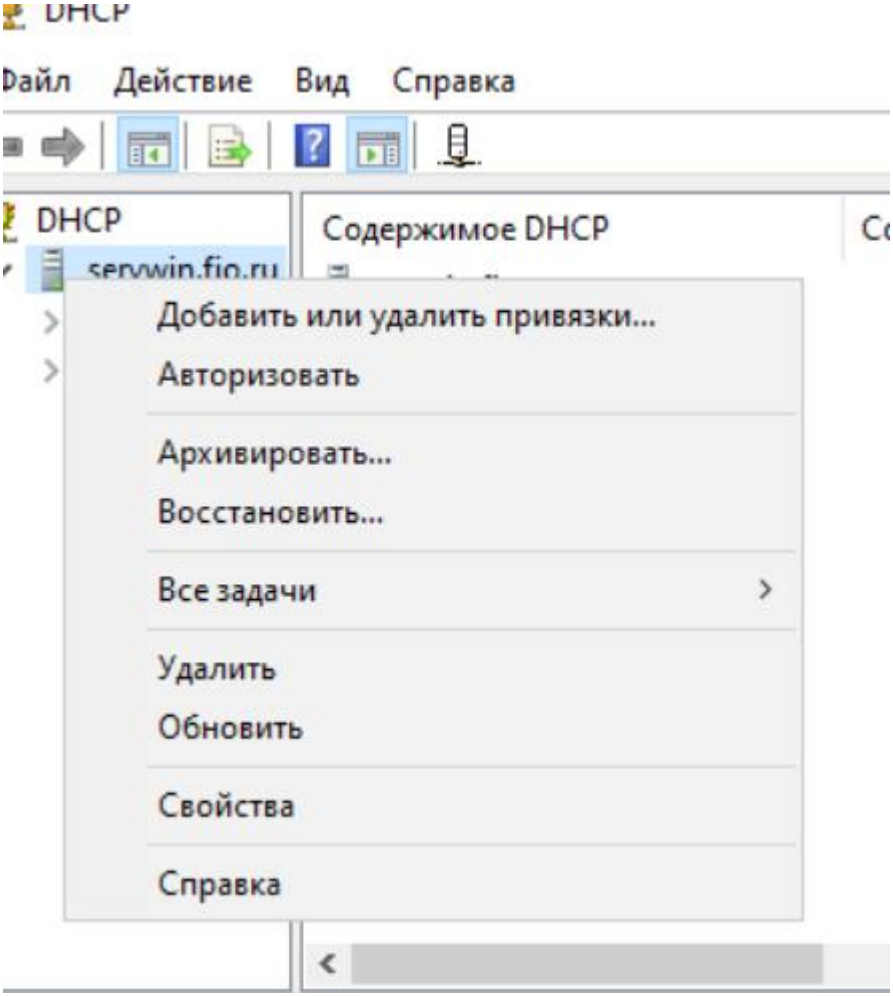
Откроется окно и надо нажать изменить и указать имя пк и его домен



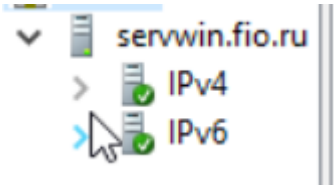

Изменение имени компьютера или домена
Вы можете изменить имя и принадлежность этого компьютера. Изменения могут повлиять на доступ к сетевым ресурсам.
Имя компьютера:
Ofic-2
Полное имя компьютера:
Ofic-2
Является членом
домена:
fio.ru
рабочей группы:
WORKGROUP
Безопасность Windows
Изменение имени компьютера или домена
Введите имя и пароль учетной записи с правами на присоединение к домену.
FIO\Администратор
OK
Отмена


Изменение имени компьютера или домена
Добро пожаловать в домен fio.ru.
OK

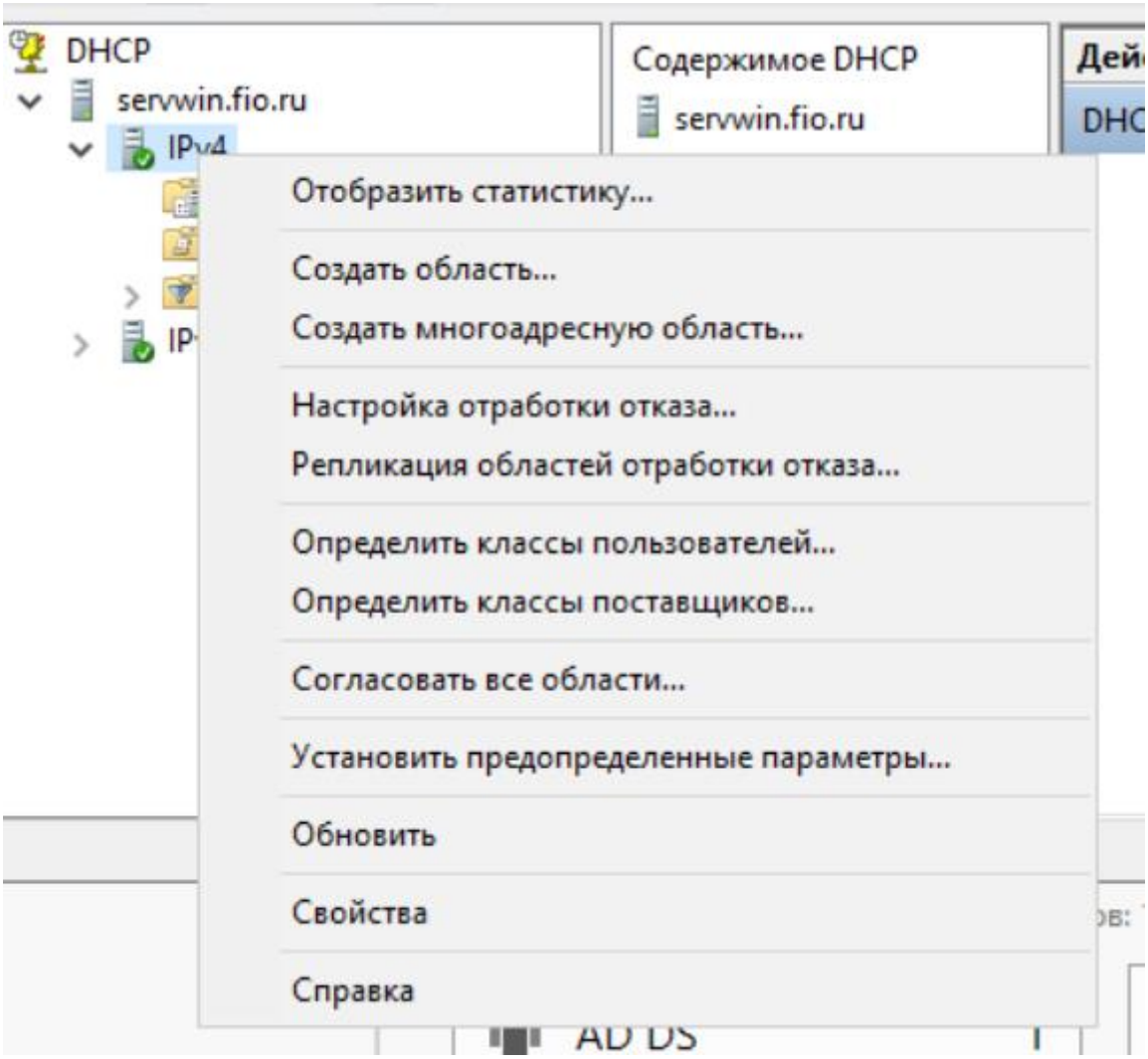
Далее необходимо перейти в «Средства» затем в «DHCP» и пкм необходимо нажать «Авторизовать»

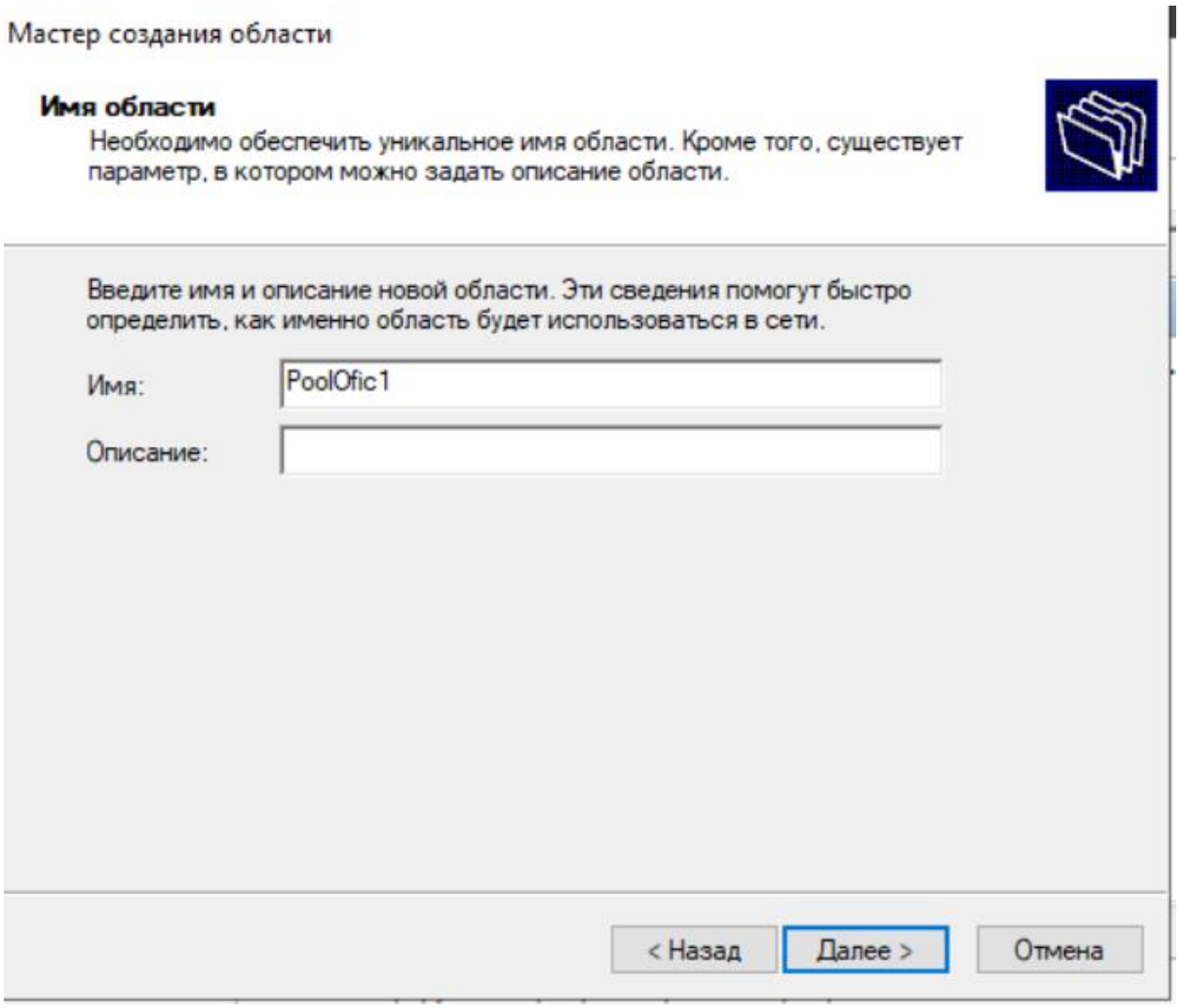


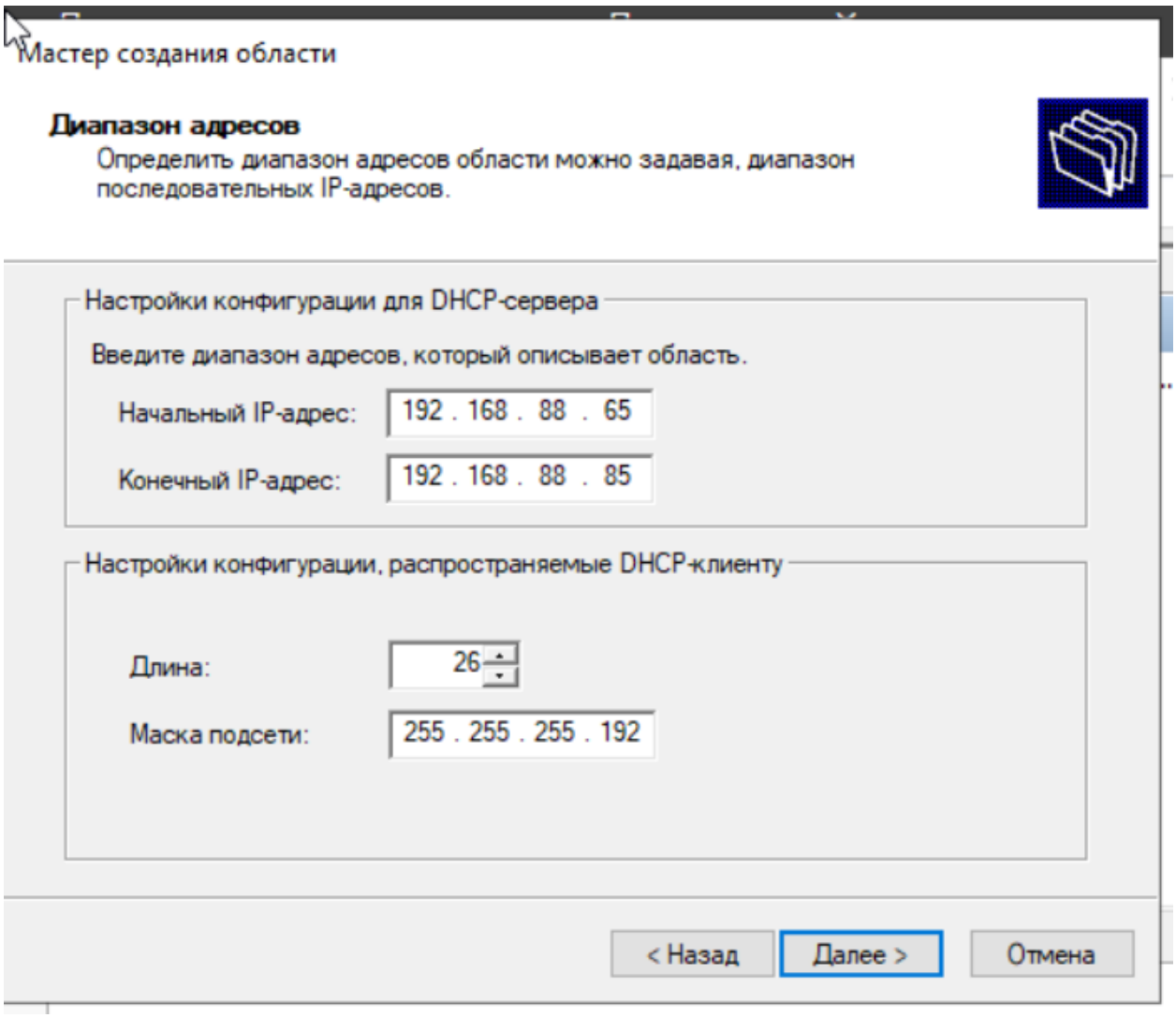
Должно загорется зеленым

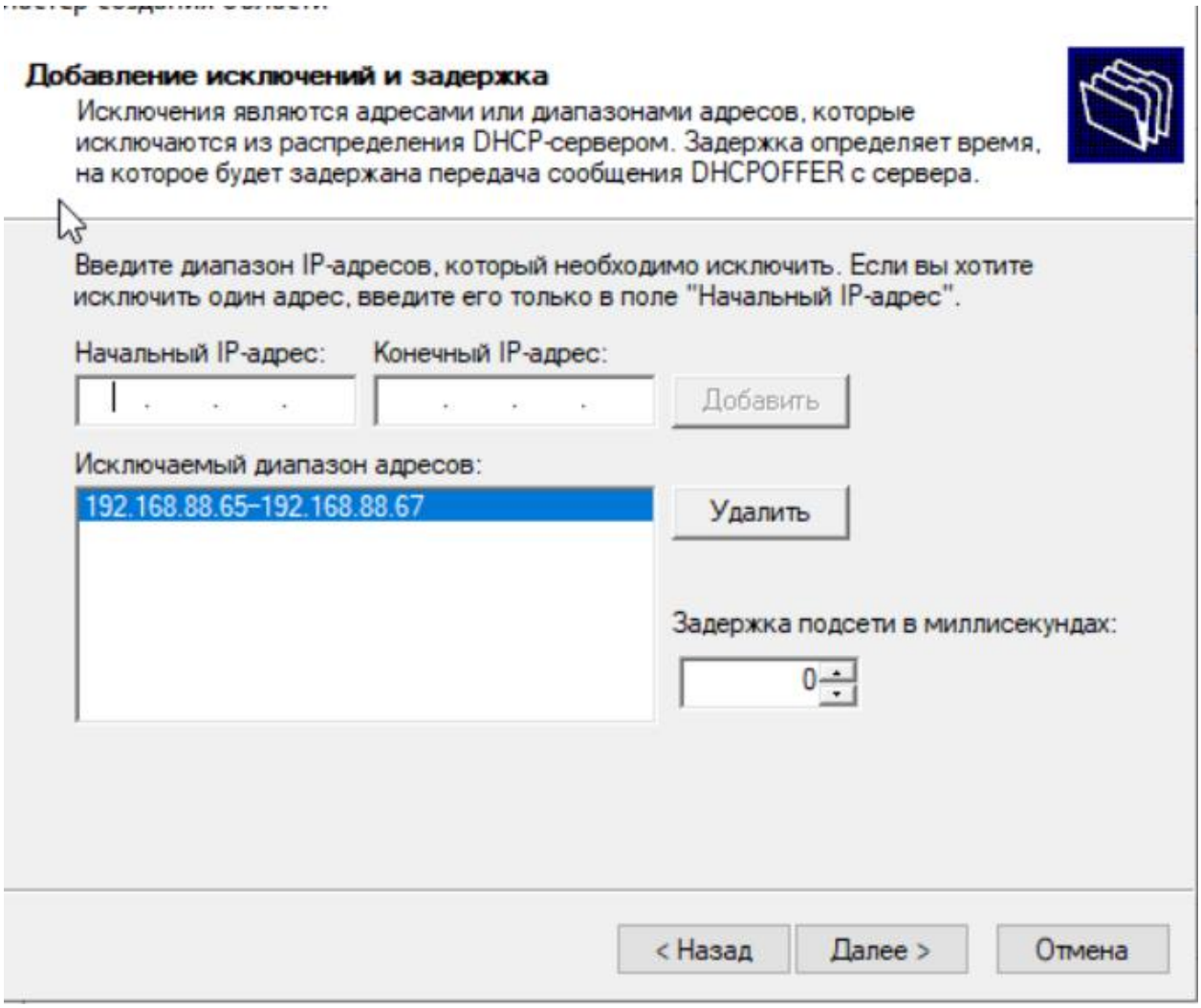


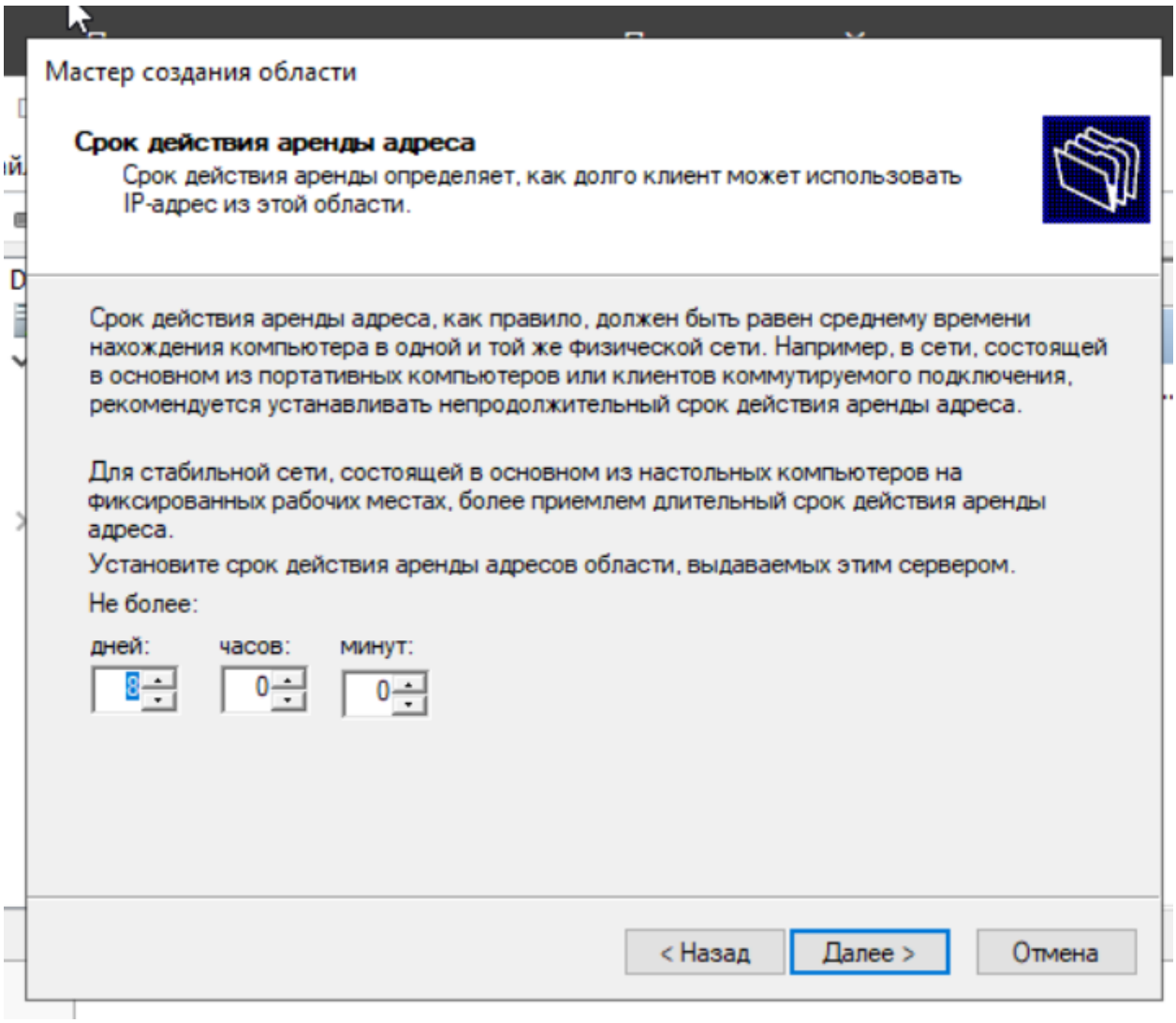
Затем выбрать «Создать область» после чего откроется матер и необходимо указать так как у меня, если до этого все повторяли если нет то указать свои ip адреса

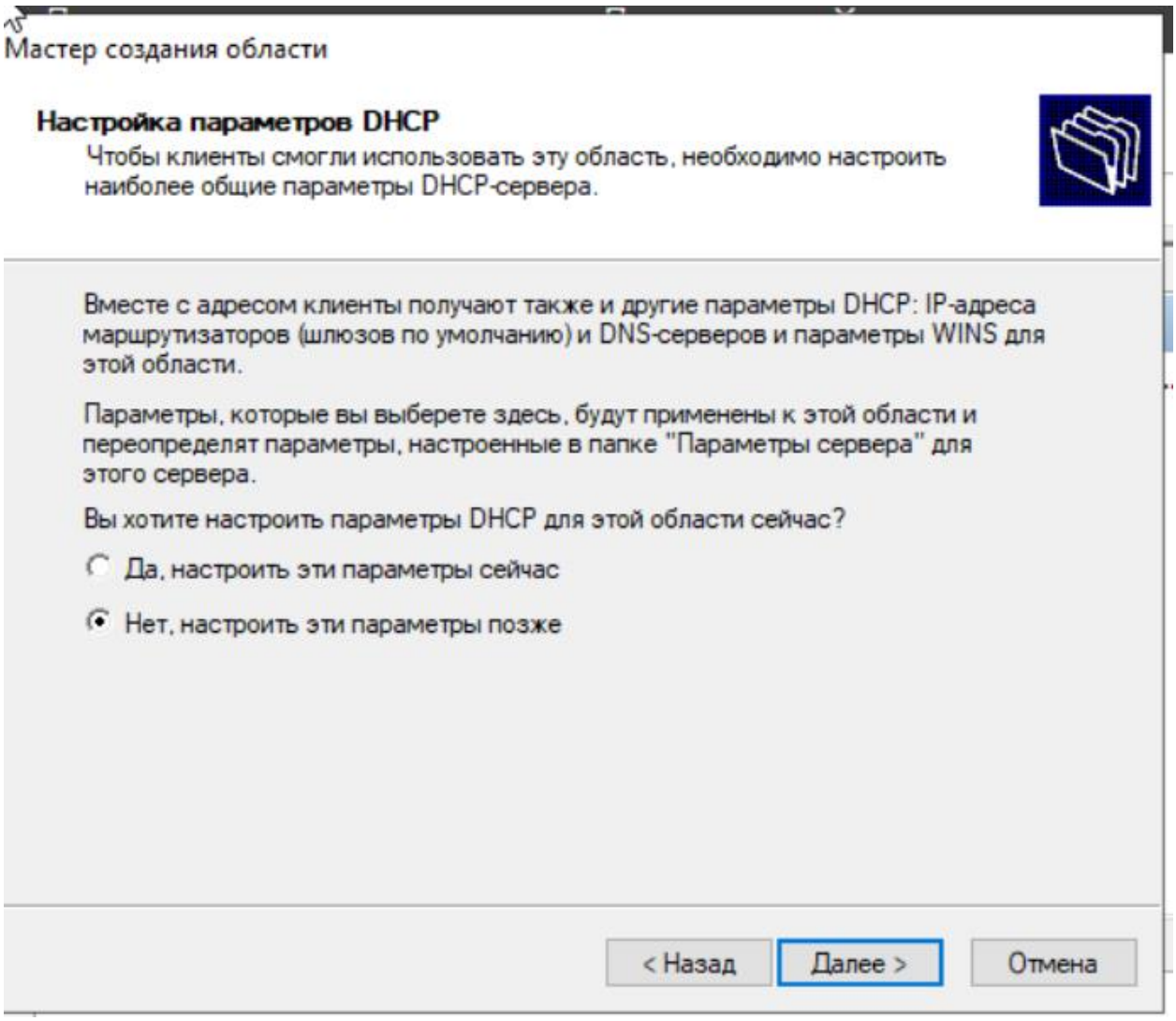


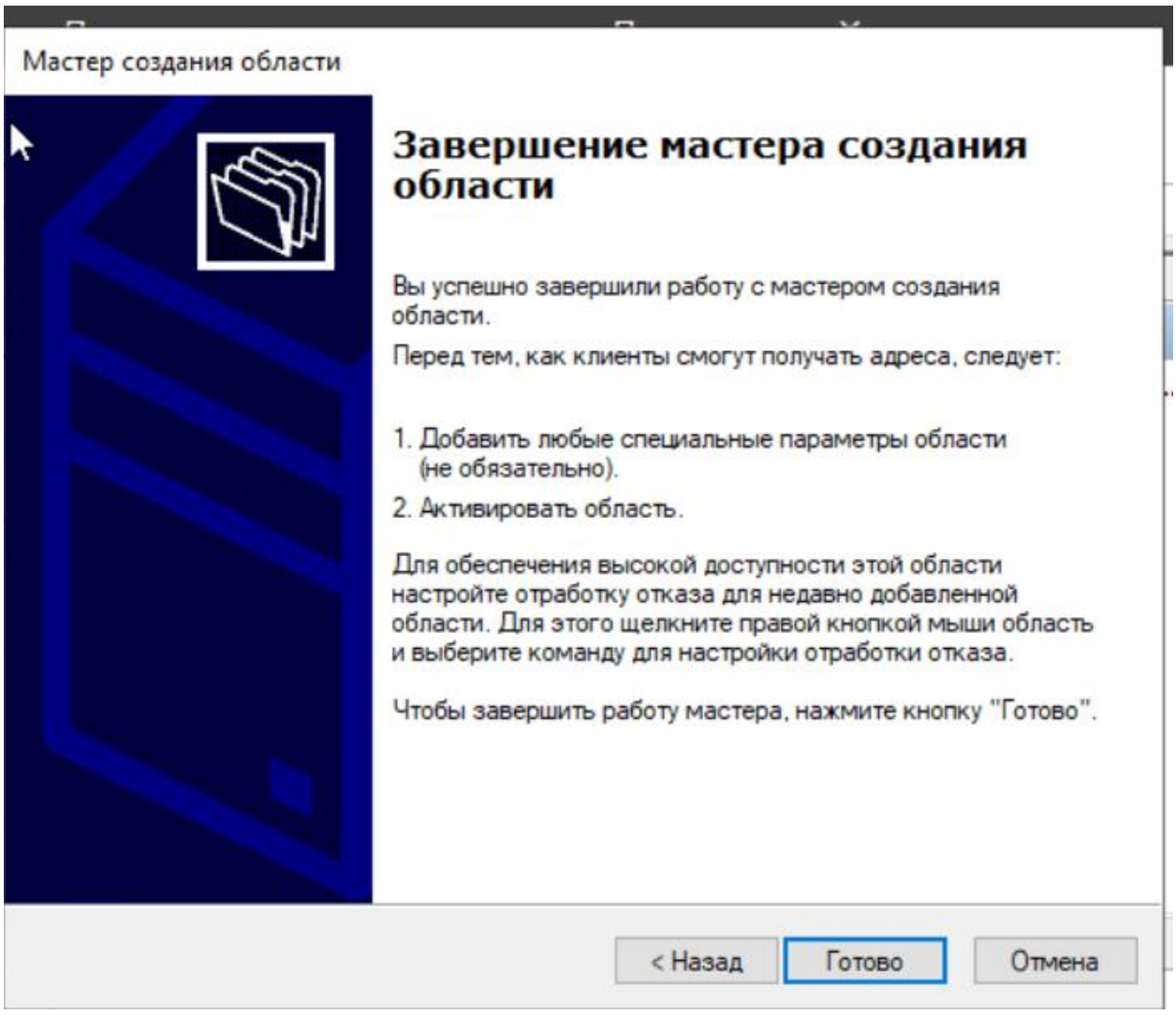

Мастер создания области
Имя области
Необходимо обеспечить уникальное имя области. Кроме того, существует параметр, в котором можно задать описание области.
Введите имя и описание новой области. Эти сведения помогут быстро определить, как именно область будет использоваться в сети.
Имя:
PoolOfic1
Описание:
< Назад
Далее >
Отмена


Мастер создания области
Диапазон адресов
Определить диапазон адресов области можно задавая, диапазон последовательных IP-адресов.
Настройки конфигурации для DHCP-сервера
Введите диапазон адресов, который описывает область.
Начальный IP-адрес: 192 . 168 . 88 . 65
Конечный IP-адрес: 192 . 168 . 88 . 85
Настройки конфигурации, распространяемые DHCP-клиенту
Длина: 26
Маска подсети: 255 . 255 . 255 . 192
< Назад
Далее >
Отмена

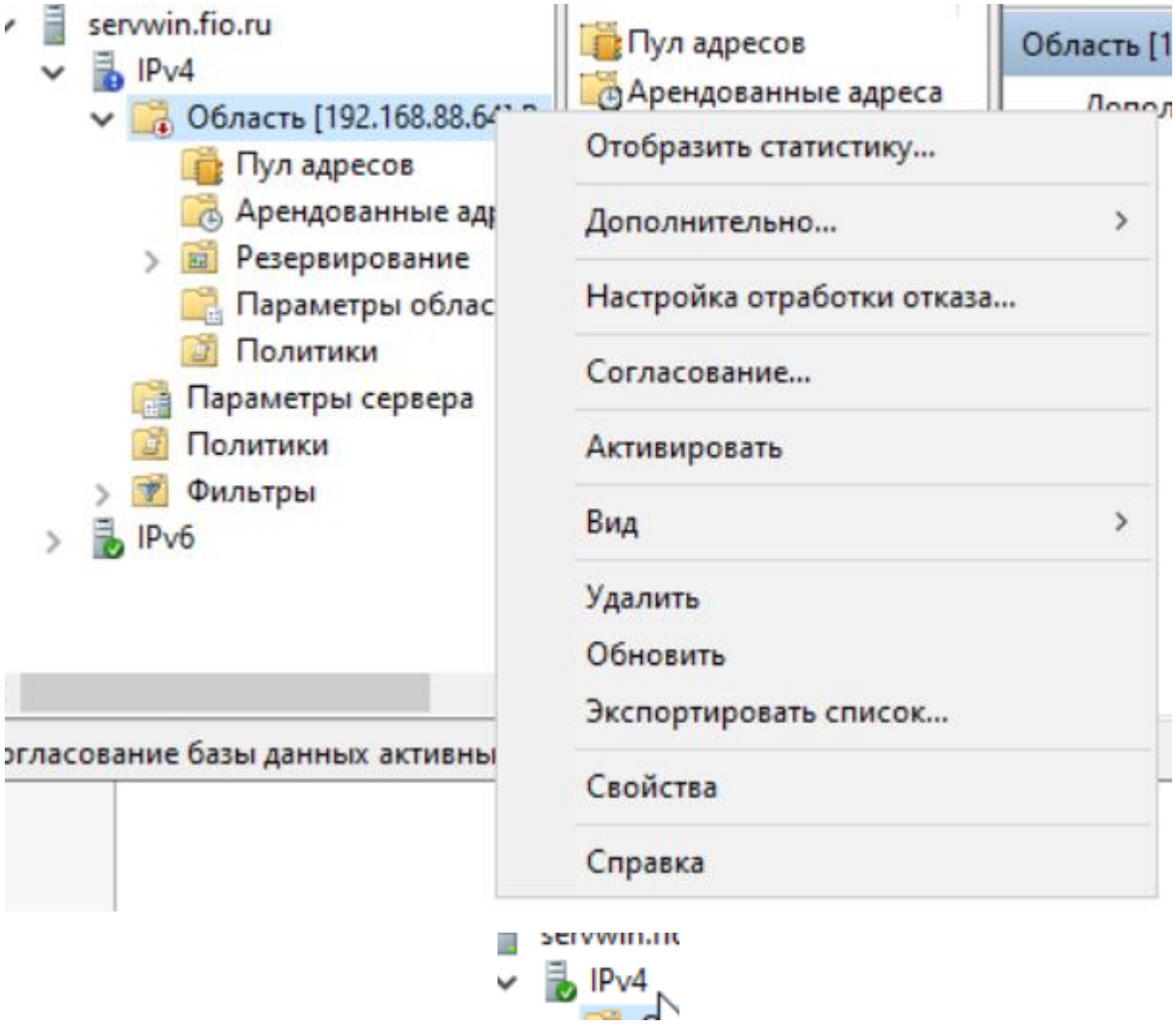

Добавление исключений и задержка
Исключения являются адресами или диапазонами адресов, которые исключаются из распределения DHCP-сервером. Задержка определяет время, на которое будет задержана передача сообщения DHCPOFFER с сервера.
Введите диапазон IP-адресов, который необходимо исключить. Если вы хотите исключить один адрес, введите его только в поле "Начальный IP-адрес".
Начальный IP-адрес:
Конечный IP-адрес:
Добавить
Исключаемый диапазон адресов:
192.168.88.65–192.168.88.67
Удалить
Задержка подсети в миллисекундах:
0
< Назад
Далее >
Отмена


Мастер создания области
Срок действия аренды адреса
Срок действия аренды определяет, как долго клиент может использовать IP-адрес из этой области.
Срок действия аренды адреса, как правило, должен быть равен среднему времени нахождения компьютера в одной и той же физической сети. Например, в сети, состоящей в основном из портативных компьютеров или клиентов коммутируемого подключения, рекомендуется устанавливать непродолжительный срок действия аренды адреса.
Для стабильной сети, состоящей в основном из настольных компьютеров на фиксированных рабочих местах, более приемлем длительный срок действия аренды адреса.
Установите срок действия аренды адресов области, выдаваемых этим сервером.
Не более:
дней:
часов:
минут:
8
0
0
< Назад
Далее >
Отмена

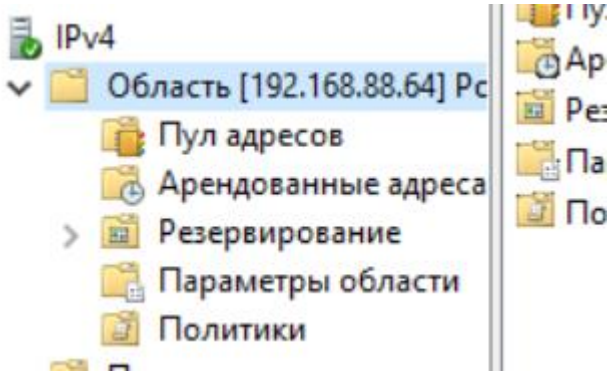

Мастер создания области
Настройка параметров DHCP
Чтобы клиенты смогли использовать эту область, необходимо настроить наиболее общие параметры DHCP-сервера.
Вместе с адресом клиенты получают также и другие параметры DHCP: IP-адреса маршрутизаторов (шлюзов по умолчанию) и DNS-серверов и параметры WINS для этой области.
Параметры, которые вы выберете здесь, будут применены к этой области и переопределят параметры, настроенные в папке "Параметры сервера" для этого сервера.
Вы хотите настроить параметры DHCP для этой области сейчас?
Да, настроить эти параметры сейчас
Нет, настроить эти параметры позже
< Назад
Далее >
Отмена

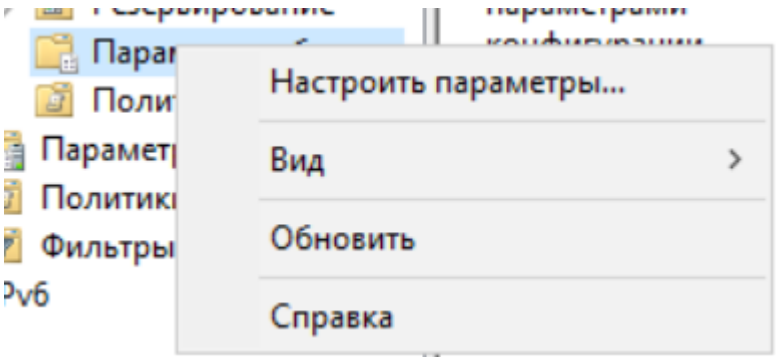

Мастер создания области
Завершение мастера создания области
Вы успешно завершили работу с мастером создания области.
Перед тем, как клиенты смогут получать адреса, следует:
1. Добавить любые специальные параметры области (не обязательно).
2. Активировать область.
Для обеспечения высокой доступности этой области настройте отработку отказа для недавно добавленной области. Для этого щелкните правой кнопкой мыши область и выберите команду для настройки отработки отказа.
Чтобы завершить работу мастера, нажмите кнопку "Готово".
< Назад
Готово
Отмена

После чего необходимо ПКМ нажать на созданую облять и нажать «Активировать», пул загорится зелененьким

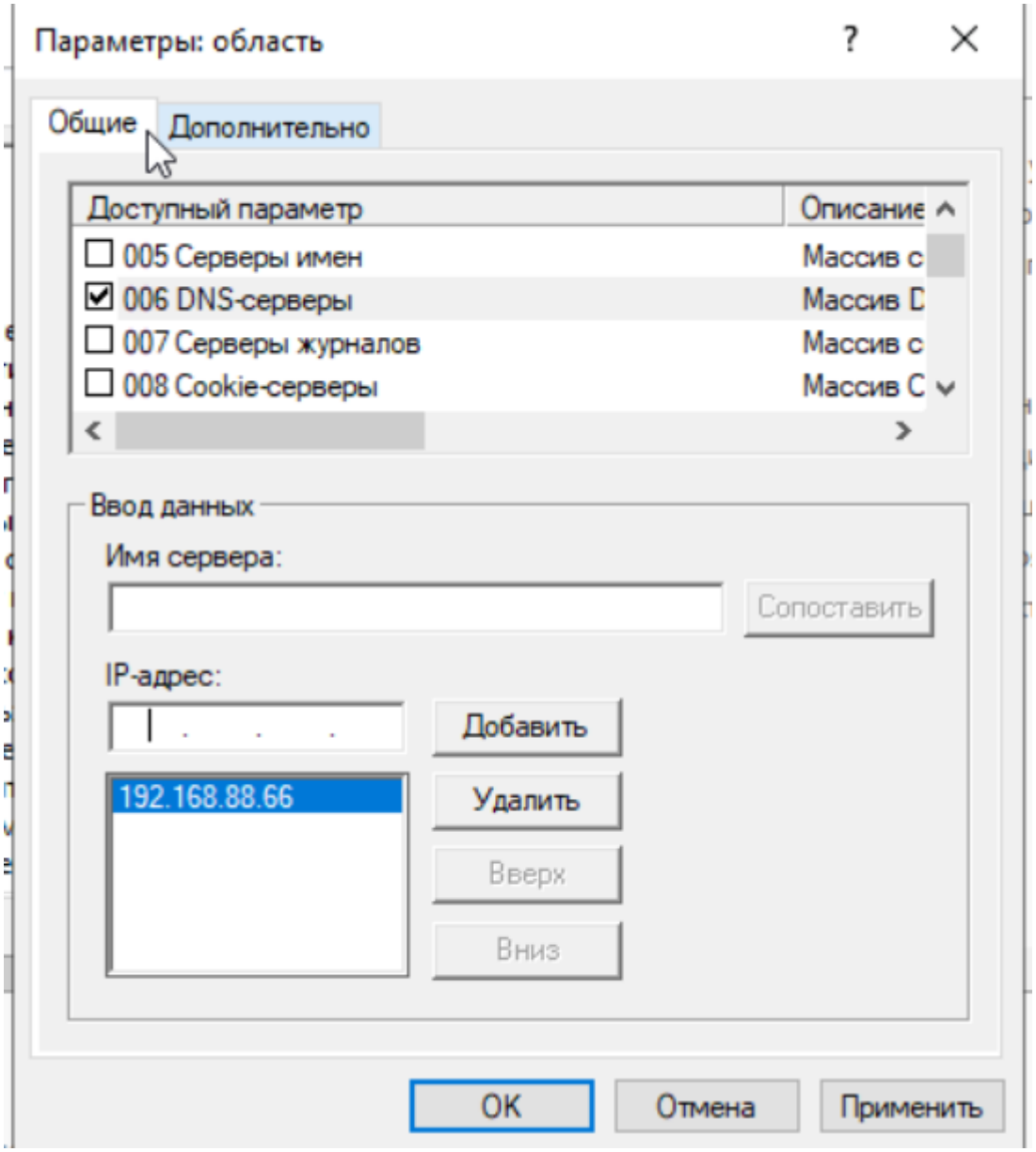


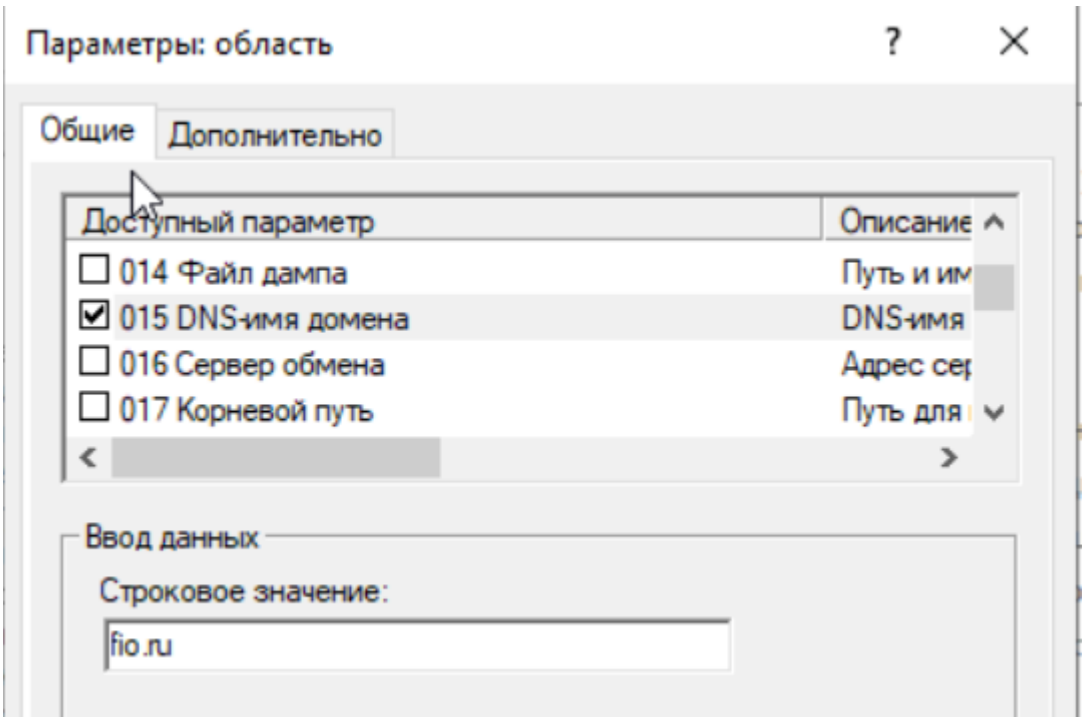
Далее необходимо нажать пкм на «параметры области» и выбрать «Настроить параметры»

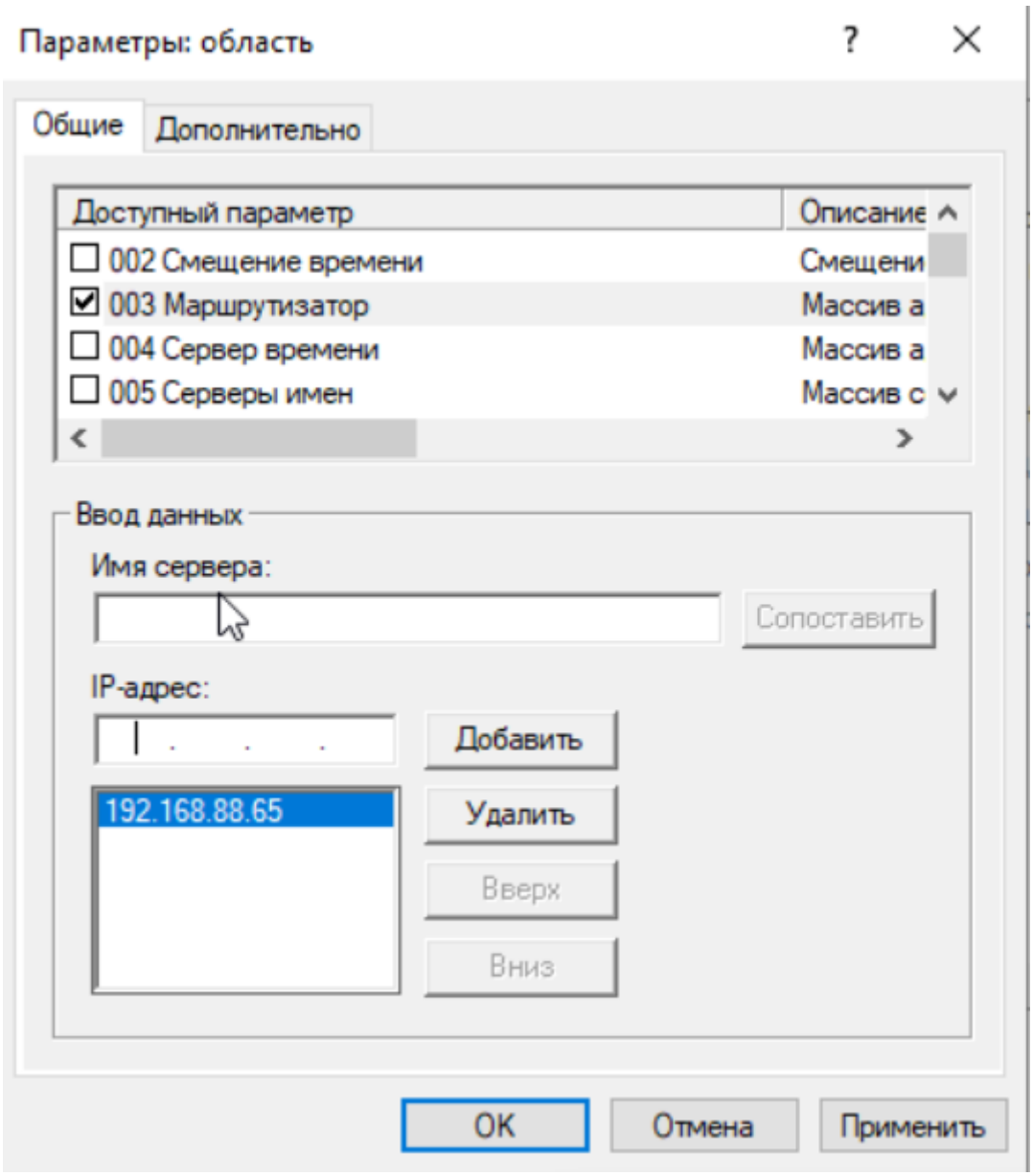


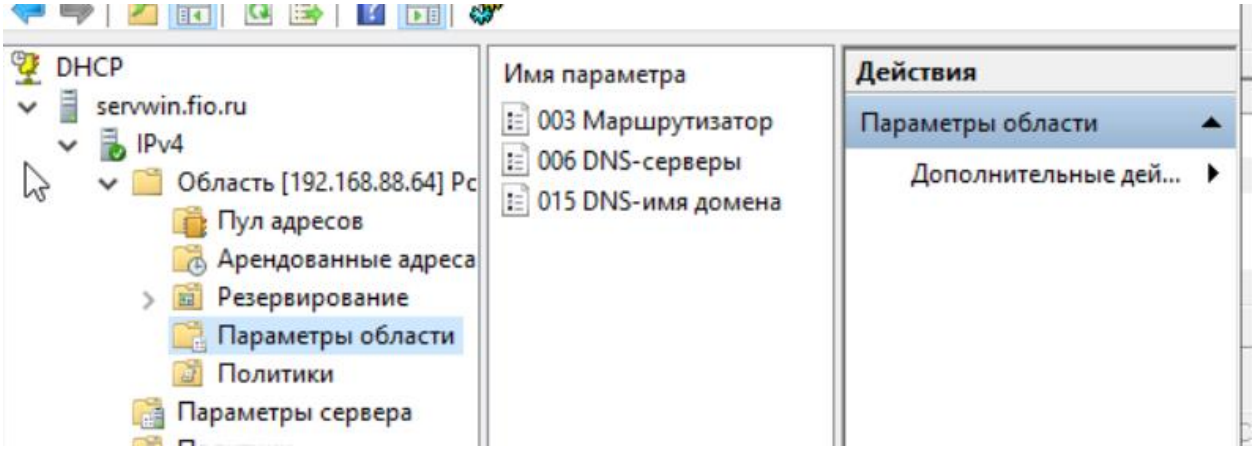


Далее необходимо указать DNS сервер, шлюз и днс имя домена

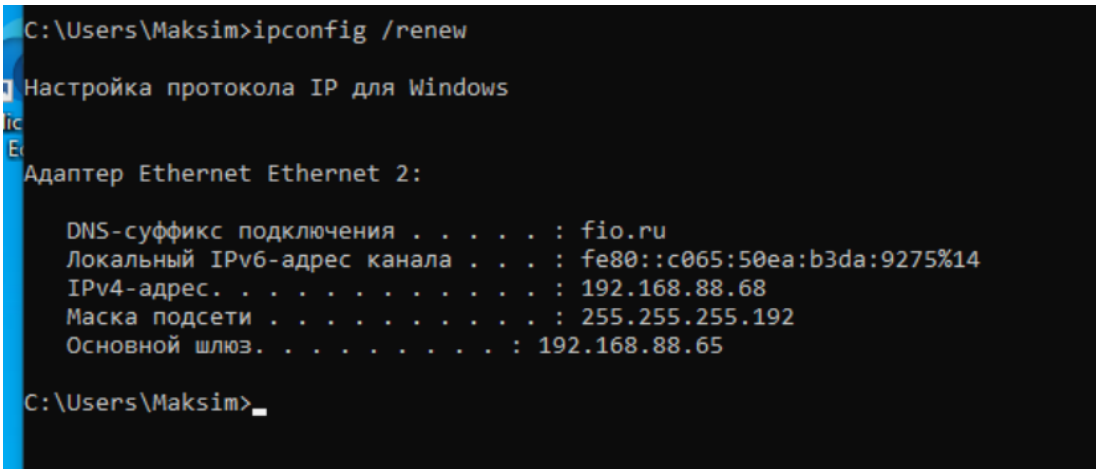



Параметры: область
Общие
Дополнительно
Доступный параметр
Описание
014 Файл дампа
Путь и им
015 DNS-имя домена
DNS-имя
016 Сервер обмена
Адрес сер
017 Корневой путь
Путь для
Ввод данных
Строковое значение:
fio.ru

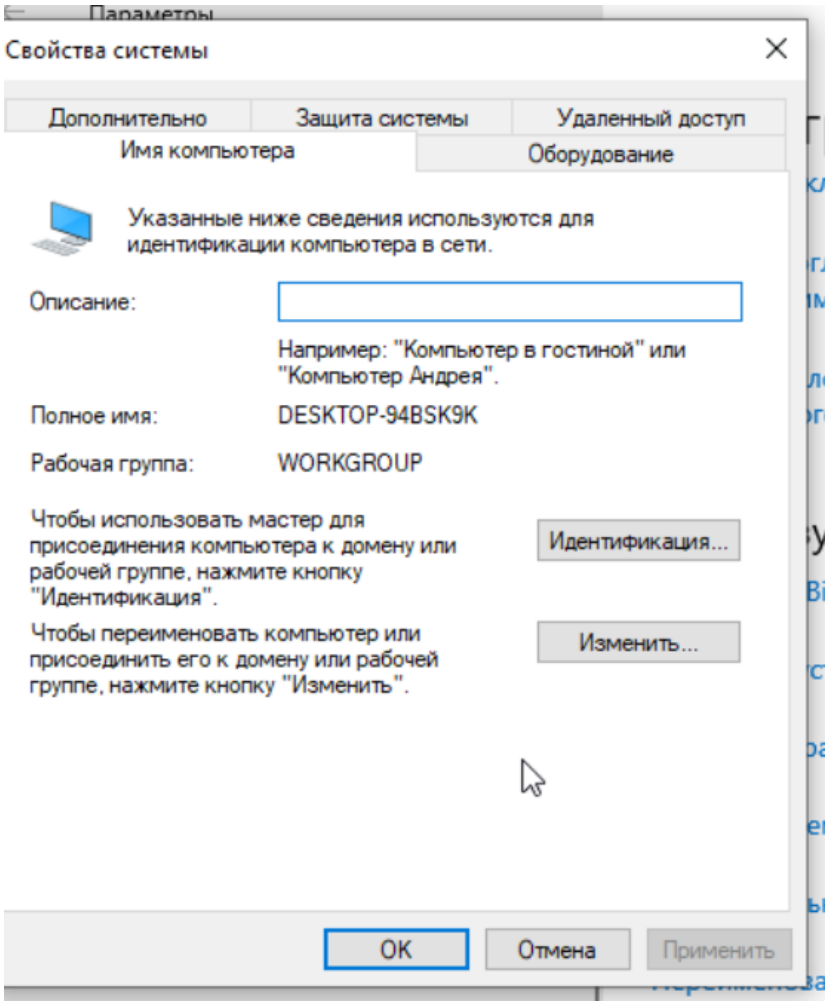

Параметры: область
Общие
Дополнительно
Доступный параметр
Описание
002 Смещение времени
Смещени
003 Маршрутизатор
Массив а
004 Сервер времени
Массив а
005 Серверы имен
Массив с
Ввод данных
Имя сервера:
Сопоставить
IP-адрес:
Добавить
192.168.88.65
Удалить
Вверх
Вниз
OK
Отмена
Применить

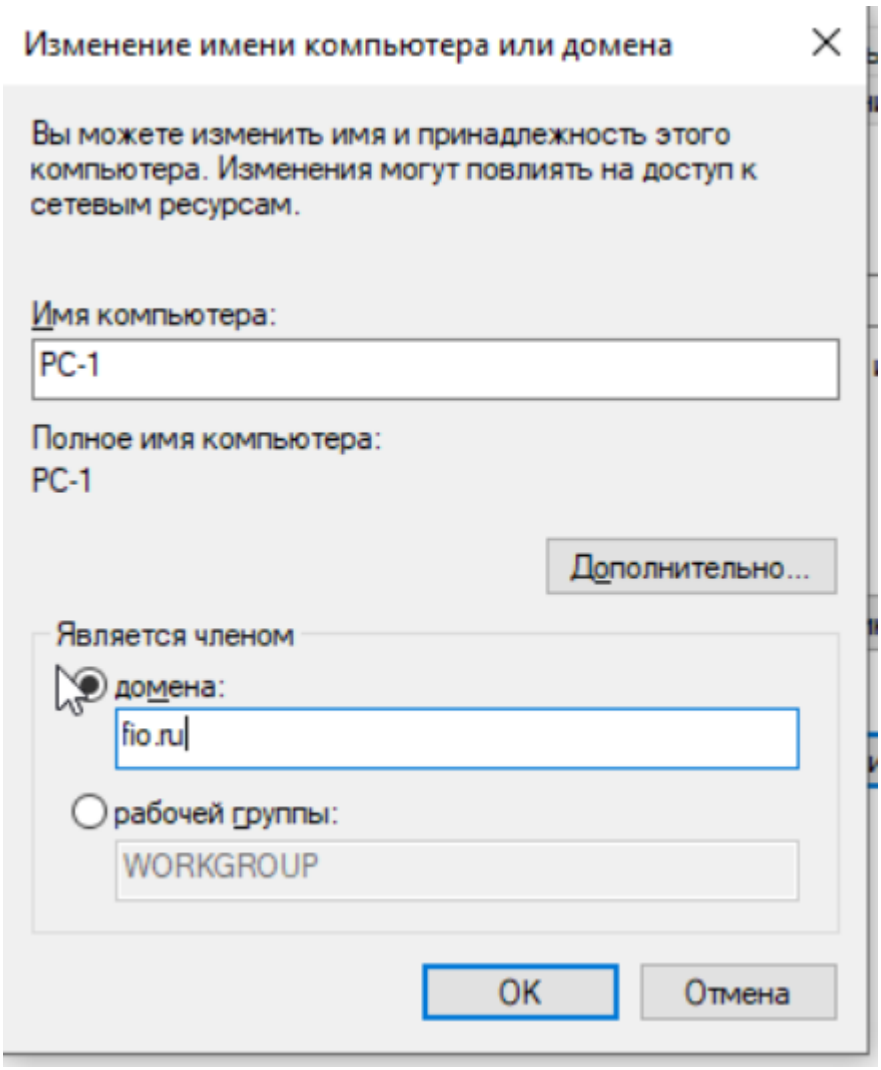

DHCP
servwin.fio.ru
IPv4
Область [192.168.88.64] Pc
Пул адресов
Арендованные адреса
Резервирование
Параметры области
Политики
Параметры сервера
Имя параметра
003 Маршрутизатор
006 DNS-серверы
015 DNS-имя домена
Действия
Параметры области
Дополнительные дей...

Далее необходимо перейти на компьтеры которые в 1 сети с сервером и написать ipconfig /renew для получения адреса. Если настроено все верно и dhcp и адаптеры тогда клиент получит ip и спокойно зайдет в домен

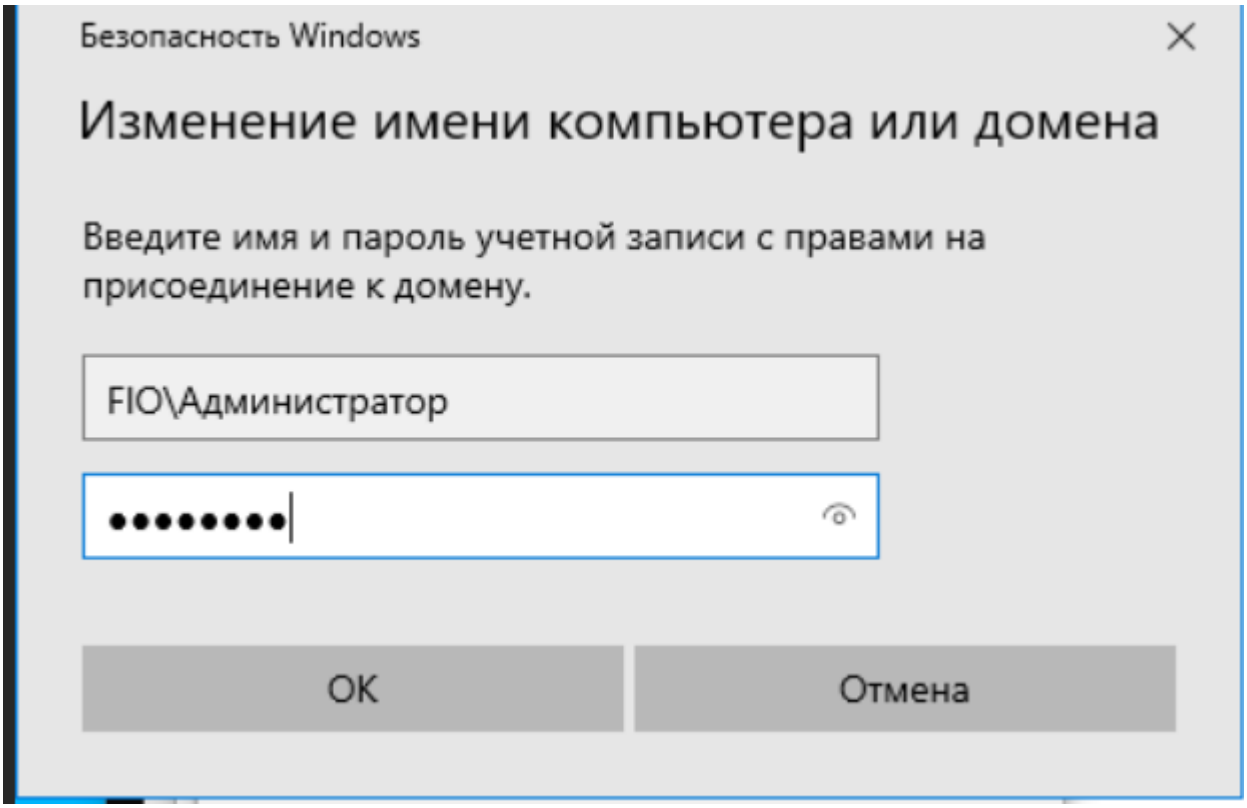


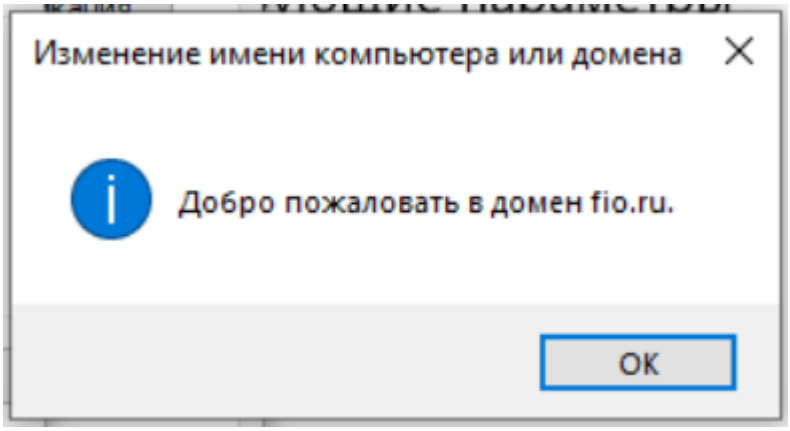
Тут надо нажать изменить и указать имя пк и его домен



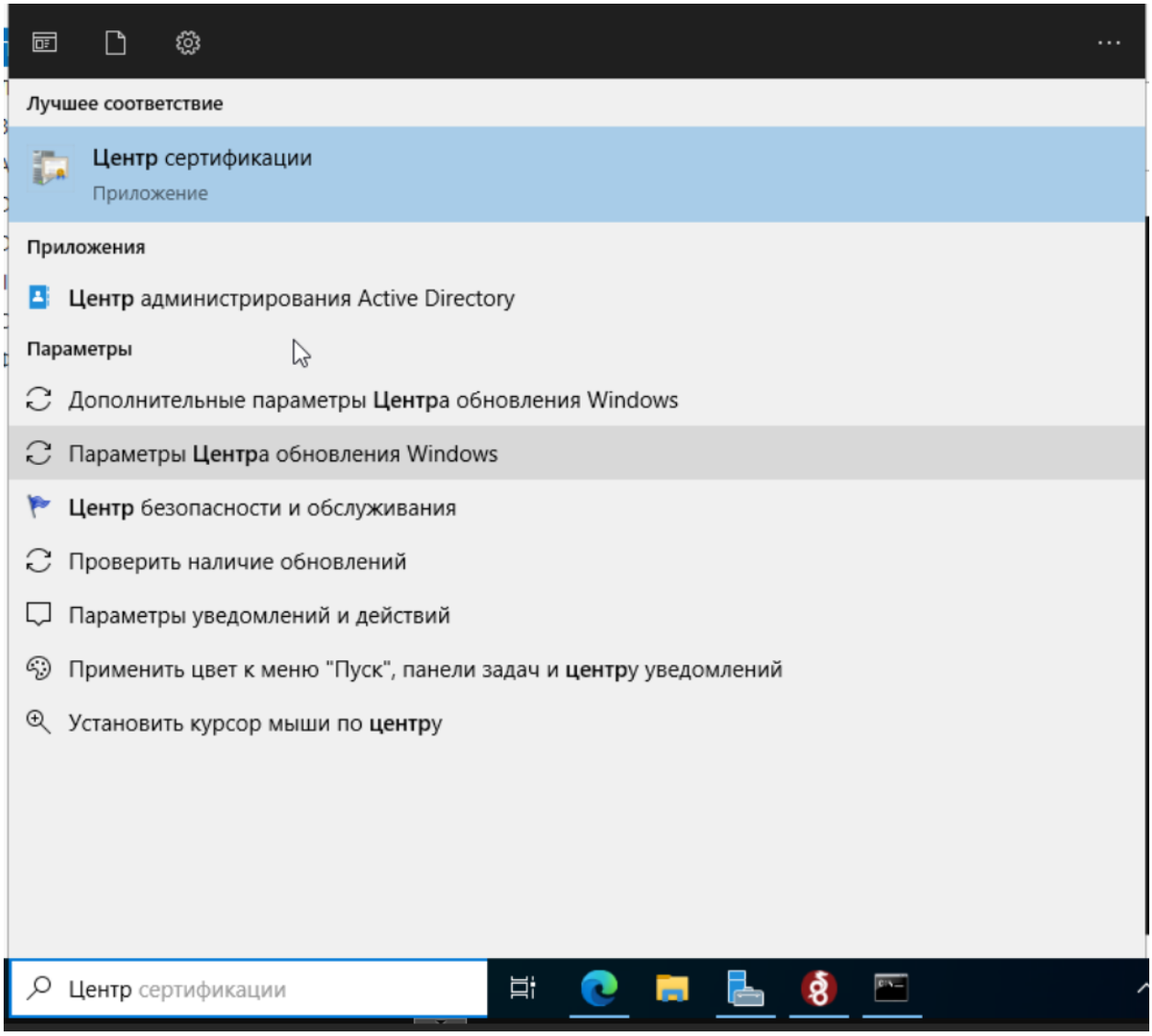

Изменение имени компьютера или домена
Вы можете изменить имя и принадлежность этого компьютера. Изменения могут повлиять на доступ к сетевым ресурсам.
Имя компьютера:
PC-1
Полное имя компьютера:
PC-1
Дополнительно...
Является членом
домена:
fio.ru
рабочей группы:
WORKGROUP
OK
Отмена

Далее надо указать логин и пароль администратора домена и если все указано верно тогда клиент войдет домен.ДАННЫЕ ДЕЙСТВИЯ НАДО СДЕЛАТЬ НА Net1-Open и Net1-OperCA

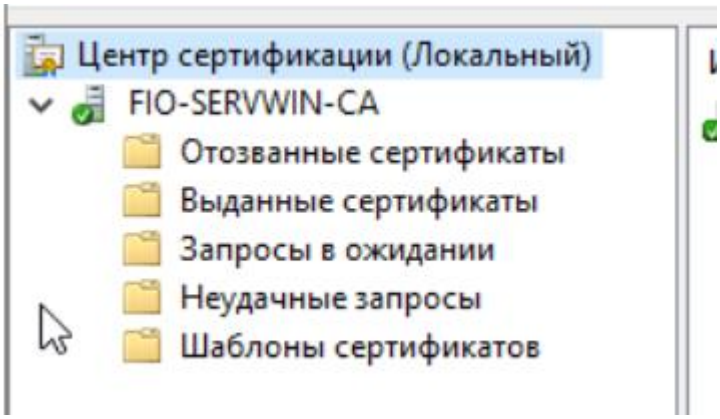


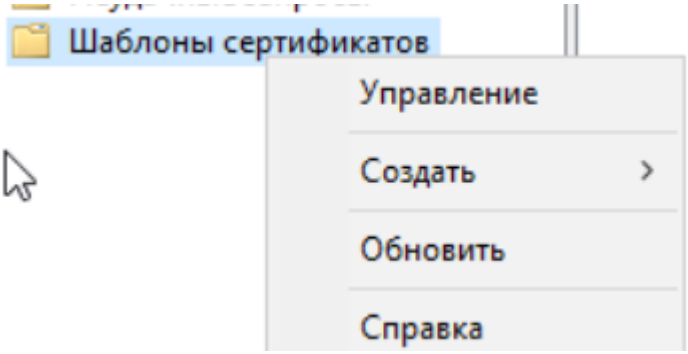


Открываем «Центр сертификации» на сервере.

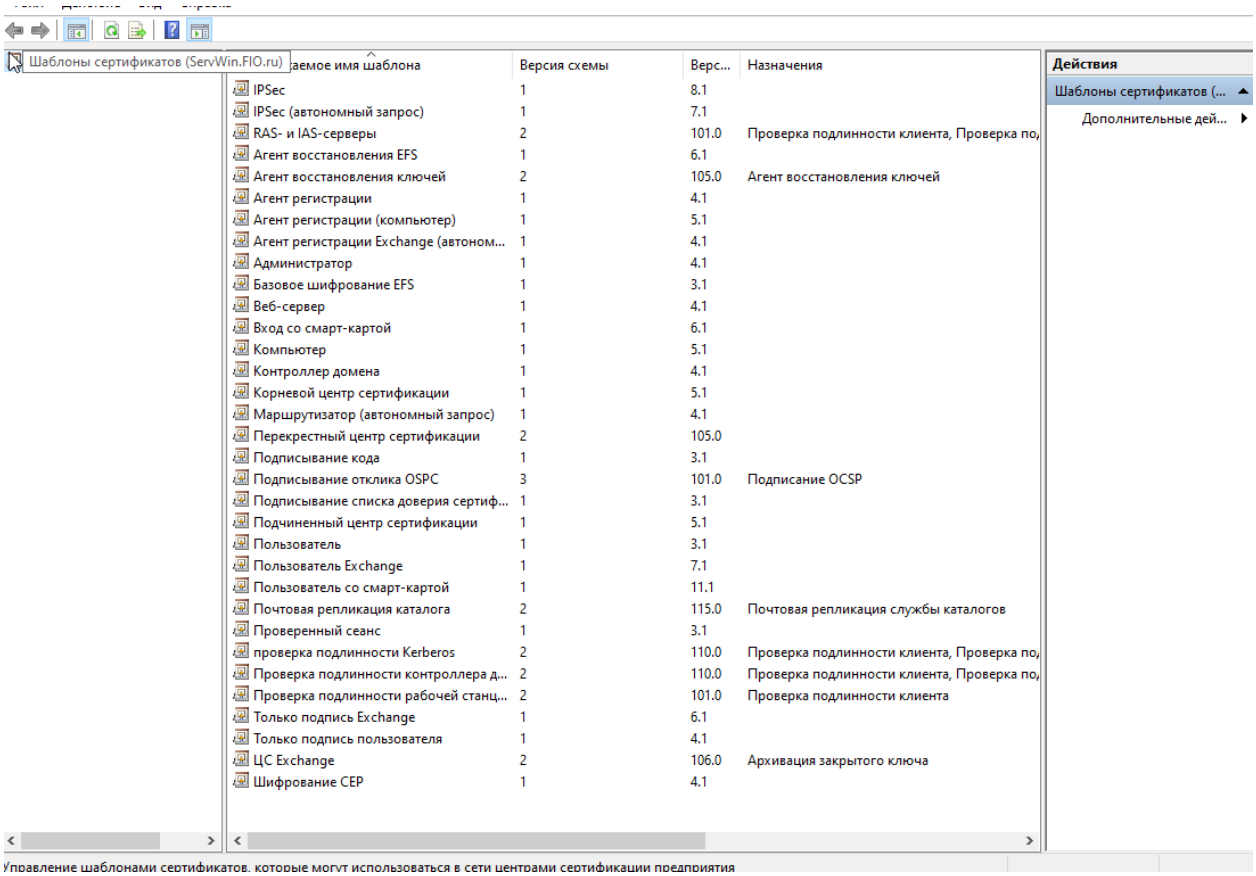


ПКМ на «шаблоны сертификатов» - «управление».

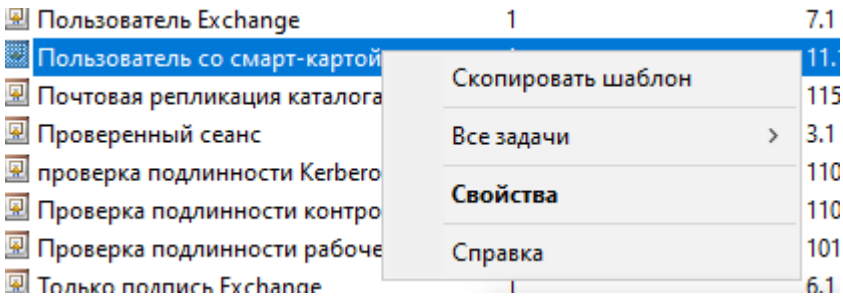




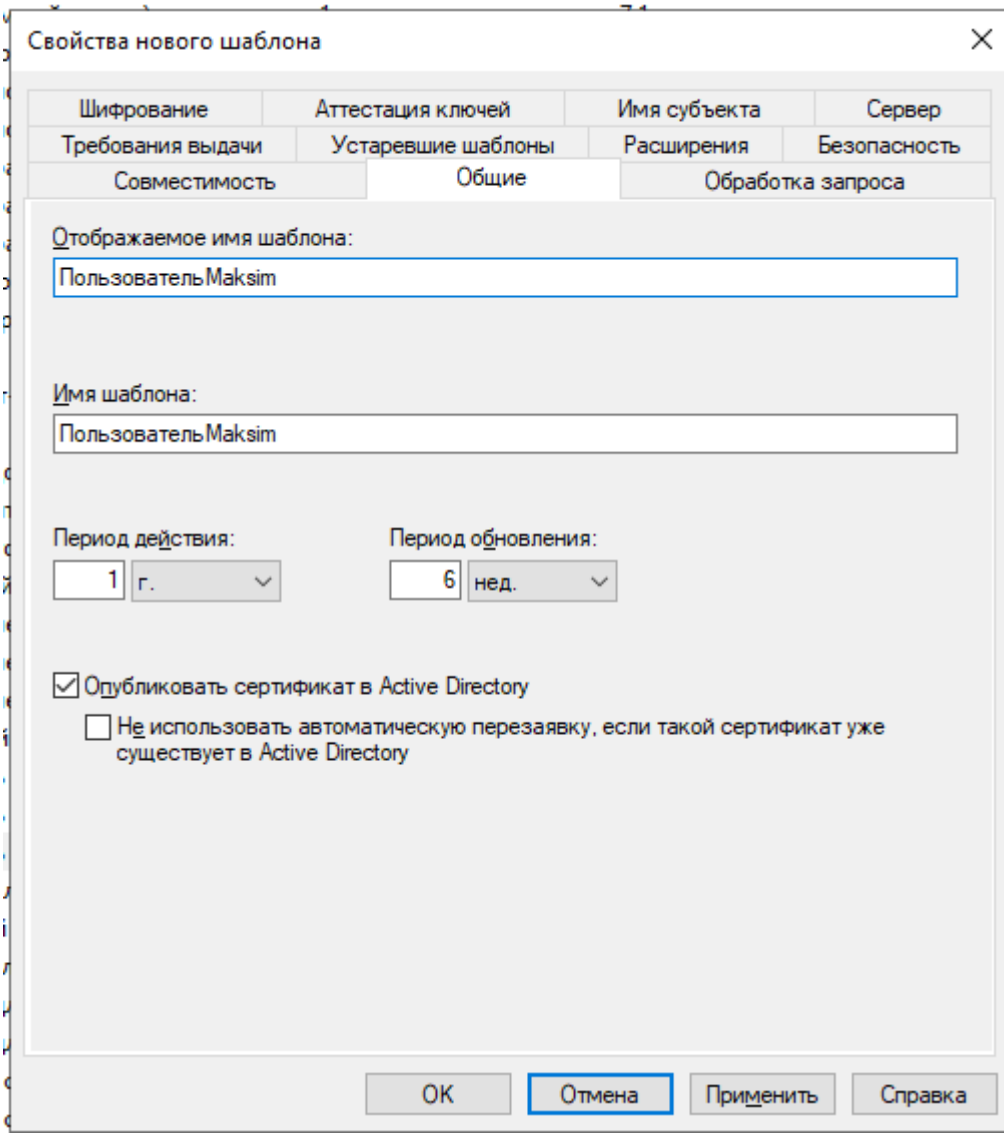
Копируем шаблон «Пользователь со смарт-картой»



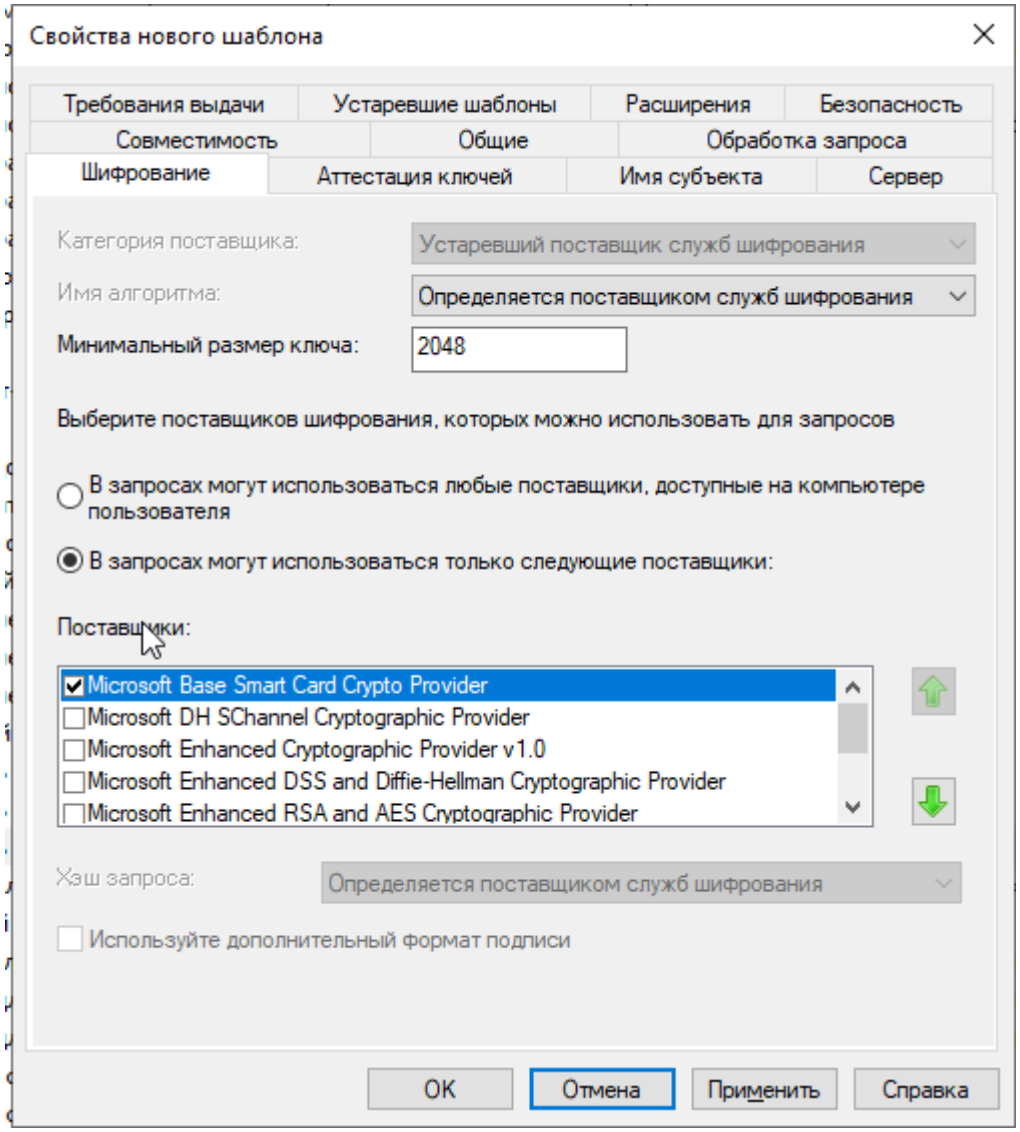
Имя шаблона	Версия схемы	Верс...	Назначения
IPSec	1	8.1	
IPSec (автономный запрос)	1	7.1	
RAS- и IAS-серверы	2	101.0	Проверка подлинности клиента, Проверка по,
Агент восстановления EFS	1	6.1	
Агент восстановления ключей	2	105.0	Агент восстановления ключей
Агент регистрации	1	4.1	
Агент регистрации (компьютер)	1	5.1	
Агент регистрации Exchange (автоном...	1	4.1	
Администратор	1	4.1	
Базовое шифрование EFS	1	3.1	
Веб-сервер	1	4.1	
Вход со смарт-картой	1	6.1	
Компьютер	1	5.1	
Контроллер домена	1	4.1	
Корневой центр сертификации	1	5.1	
Маршрутизатор (автономный запрос)	1	4.1	
Перекрестный центр сертификации	2	105.0	
Подписывание кода	1	3.1	
Подписывание отклика OSPC	3	101.0	Подписание OCSP
Подписывание списка доверия сертиф...	1	3.1	
Подчиненный центр сертификации	1	5.1	
Пользователь	1	3.1	
Пользователь Exchange	1	7.1	
Пользователь со смарт-картой	1	11.1	
Почтовая репликация каталога	2	115.0	Почтовая репликация службы каталогов
Проверенный сеанс	1	3.1	
проверка подлинности Kerberos	2	110.0	Проверка подлинности клиента, Проверка по,
Проверка подлинности контроллера д...	2	110.0	Проверка подлинности клиента, Проверка по,
Проверка подлинности рабочей станц...	2	101.0	Проверка подлинности клиента
Только подпись Exchange	1	6.1	
Только подпись пользователя	1	4.1	
ЦС Exchange	2	106.0	Архивация закрытого ключа
Шифрование CEP	1	4.1	



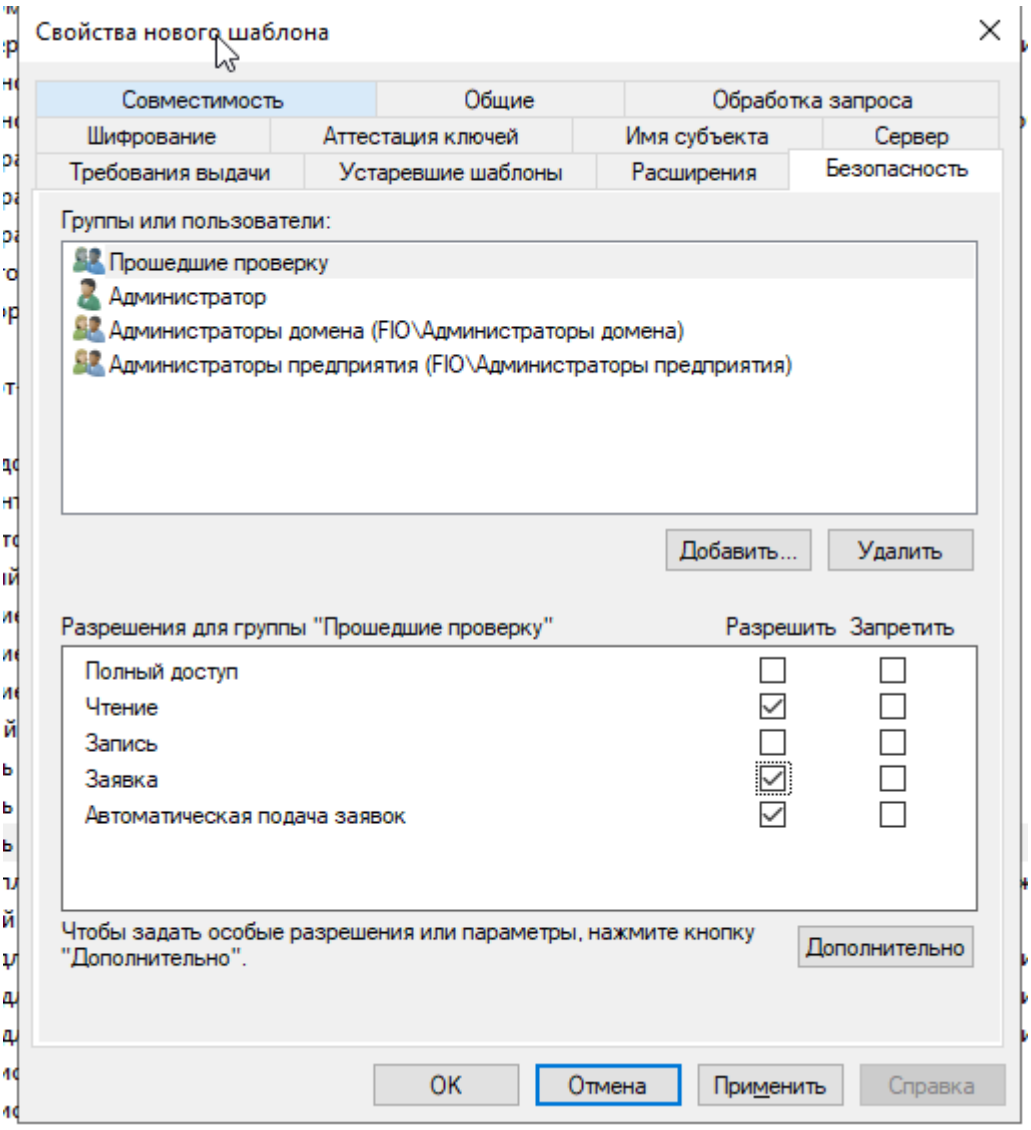
Открывается окно со свойствами нового шаблона. В «Общие» задаем имя шаблона и периоды. Нажимаем «применить».



В «Шифрование» указываем поставщика для запросов – «Microsoft Base Smart Card Crypto Provider». Нажимаем «применить».

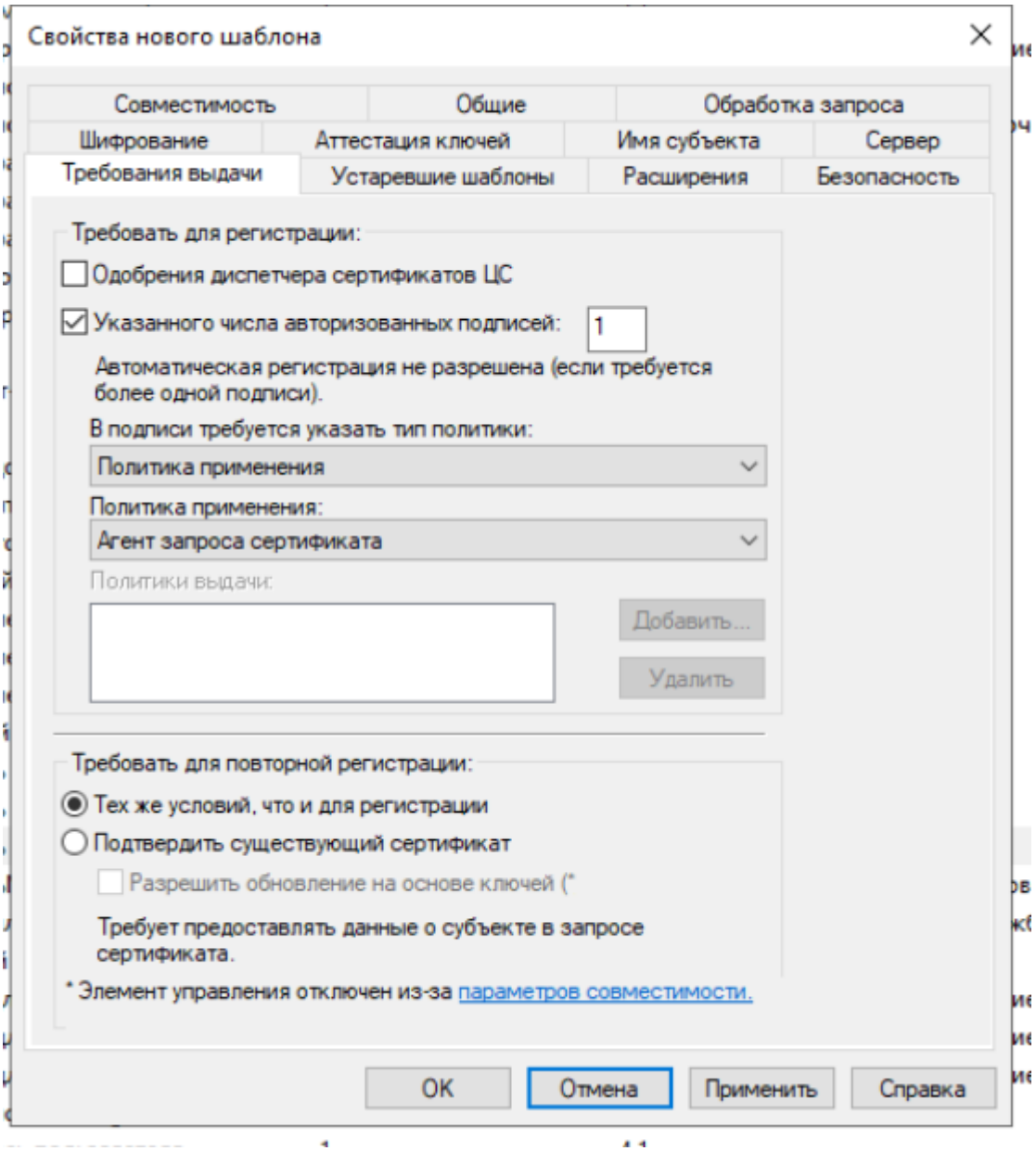


В «Безопасность» выдаем разрешения для группы «Прошедшие проверку» на «Заявку» и «Автоматическую подачу заявок». Нажимаем «применить».

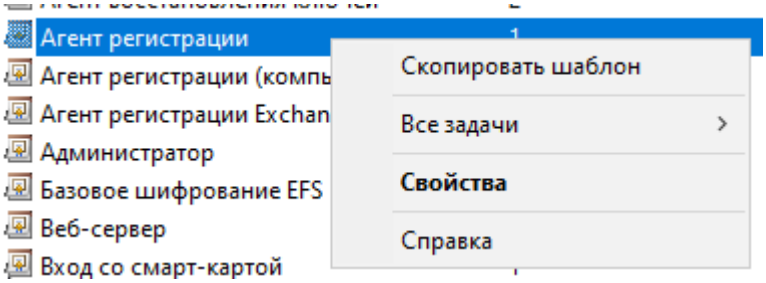


В «Требования выдачи» указываем тип политики «Политика применения» и в политике применения «Агент запроса сертификата».

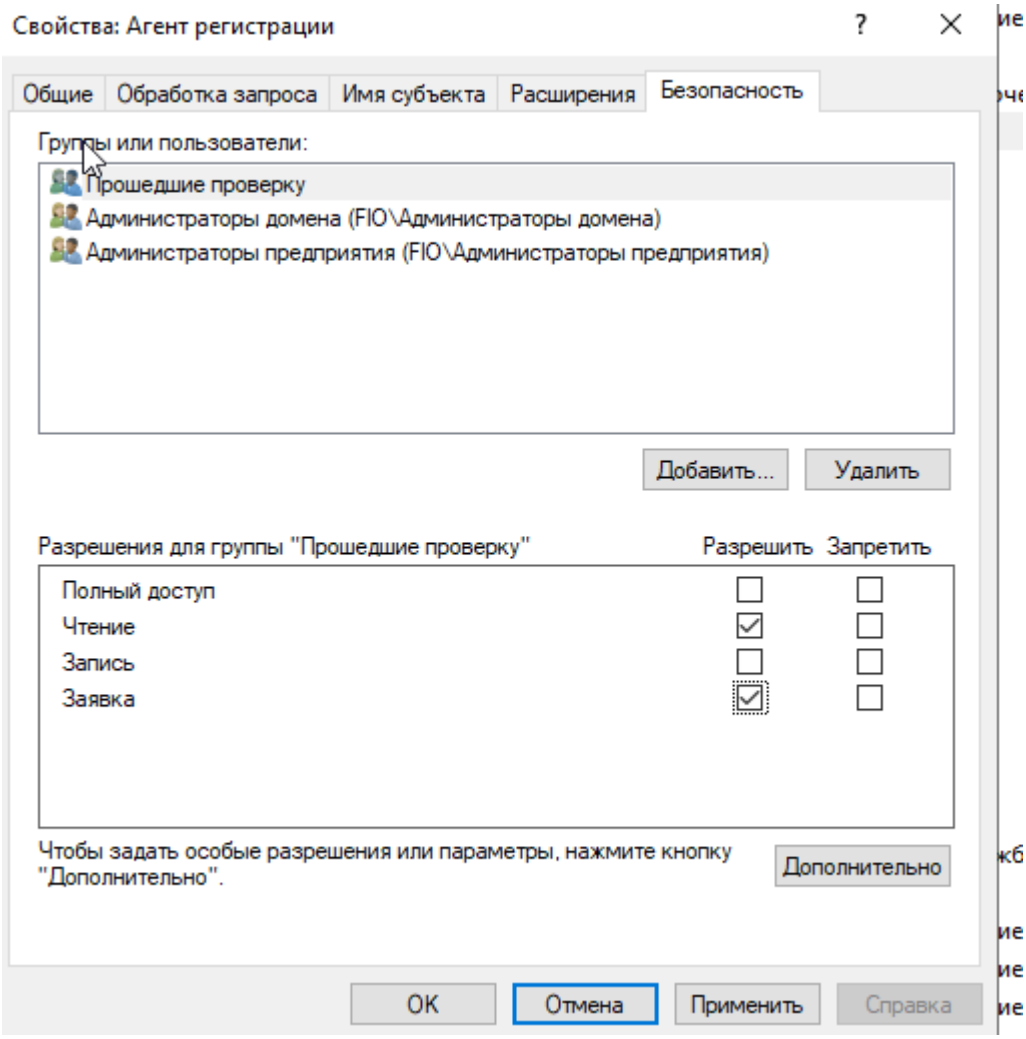
Нажимаем «применить». Остальные свойства были оставлены по умолчанию.



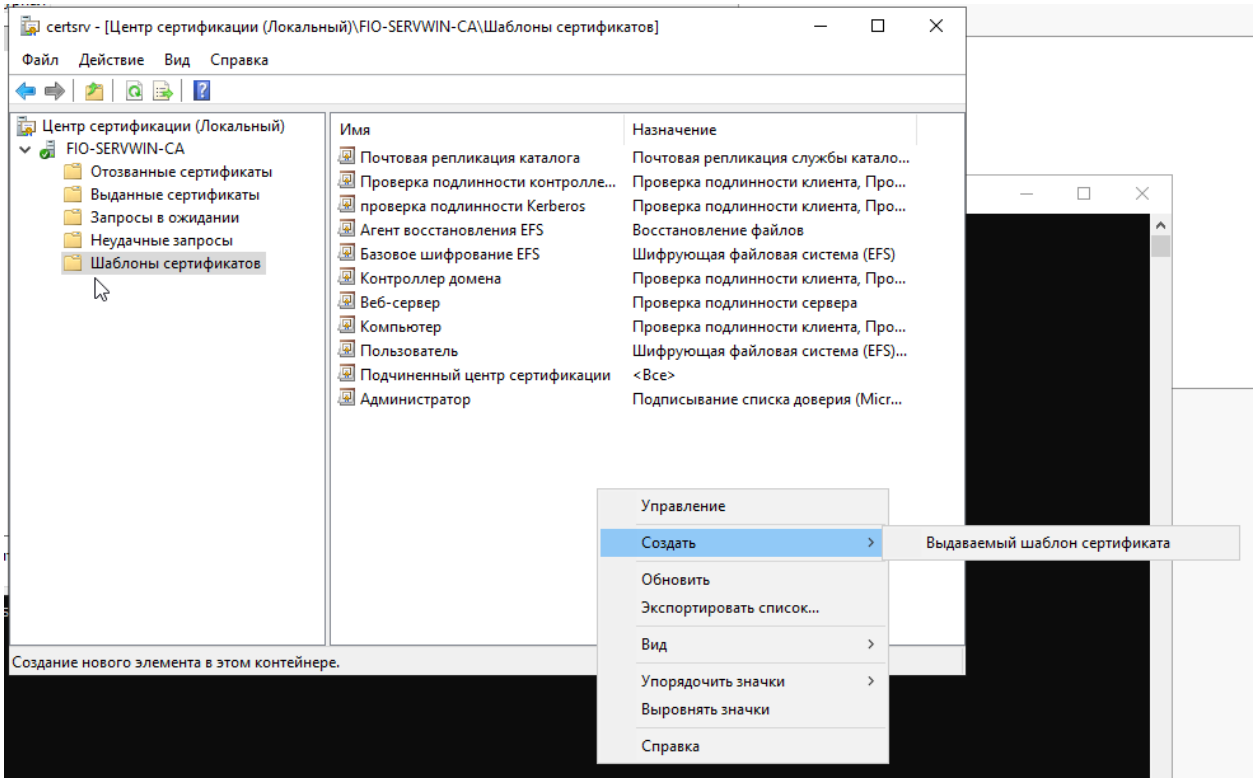
После этого в консоли находим шаблон «Агент регистрации» и жмем ПКМ – «Свойства».



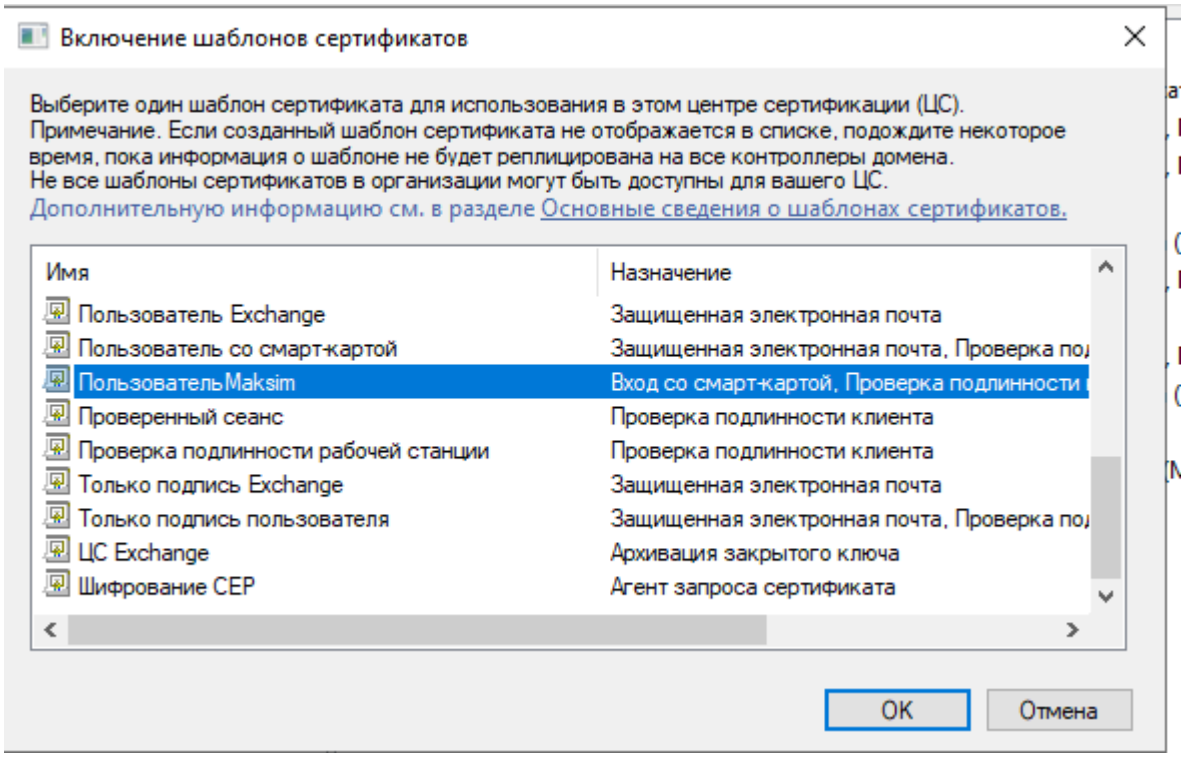
Во вкладке «Безопасность» выдаем право на «Заявку» и «Чтение» для группы «Прошедшие проверку». Нажимаем «применить».



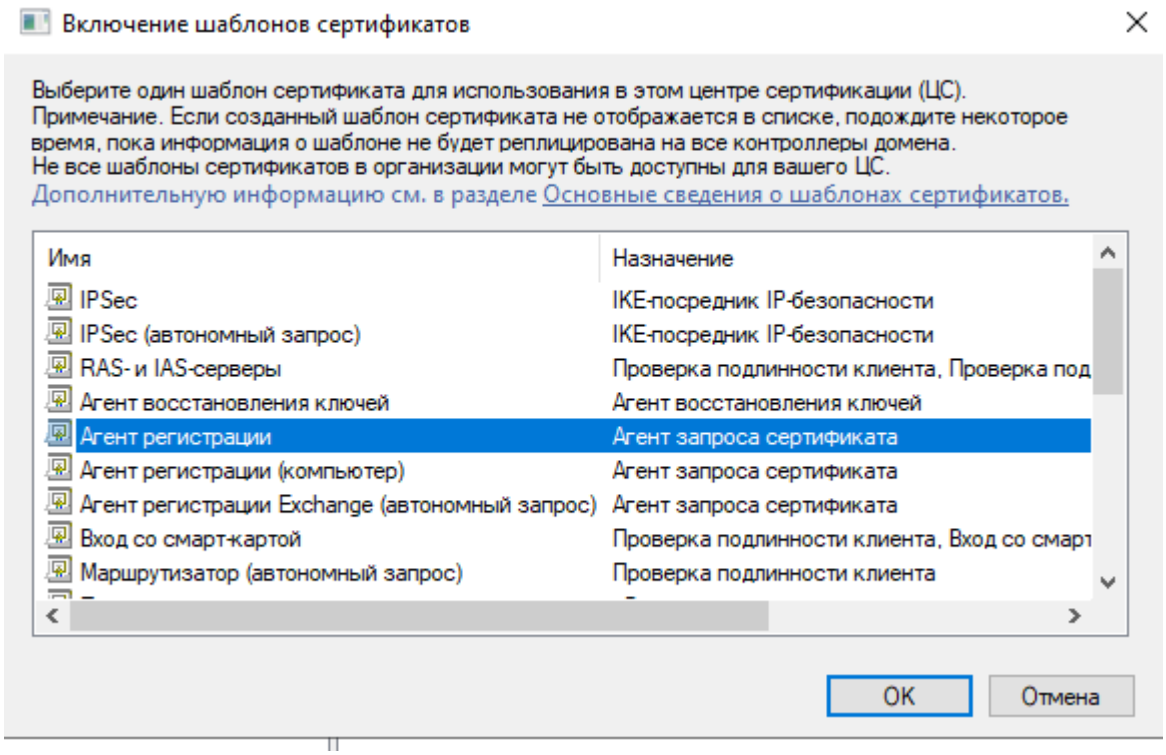
Возвращаемся в Центр сертификации и жмем ПКМ – «Создать» - «Выдаваемый шаблон сертификата».



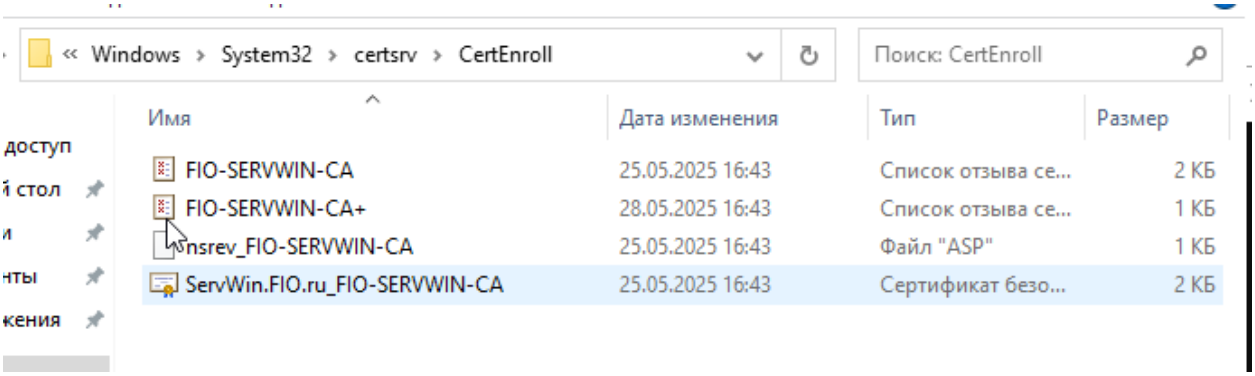
Выбираем ранее созданный шаблон для пользователя.



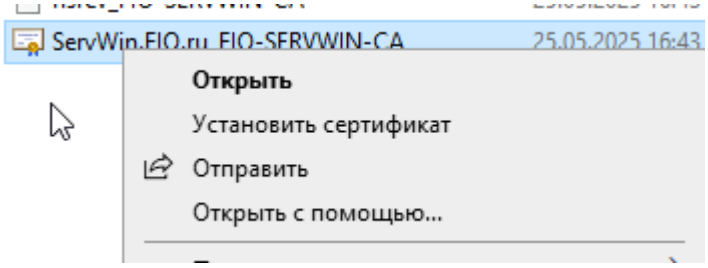
Создаем еще один выдаваемый шаблон сертификата – «Агент регистрации».



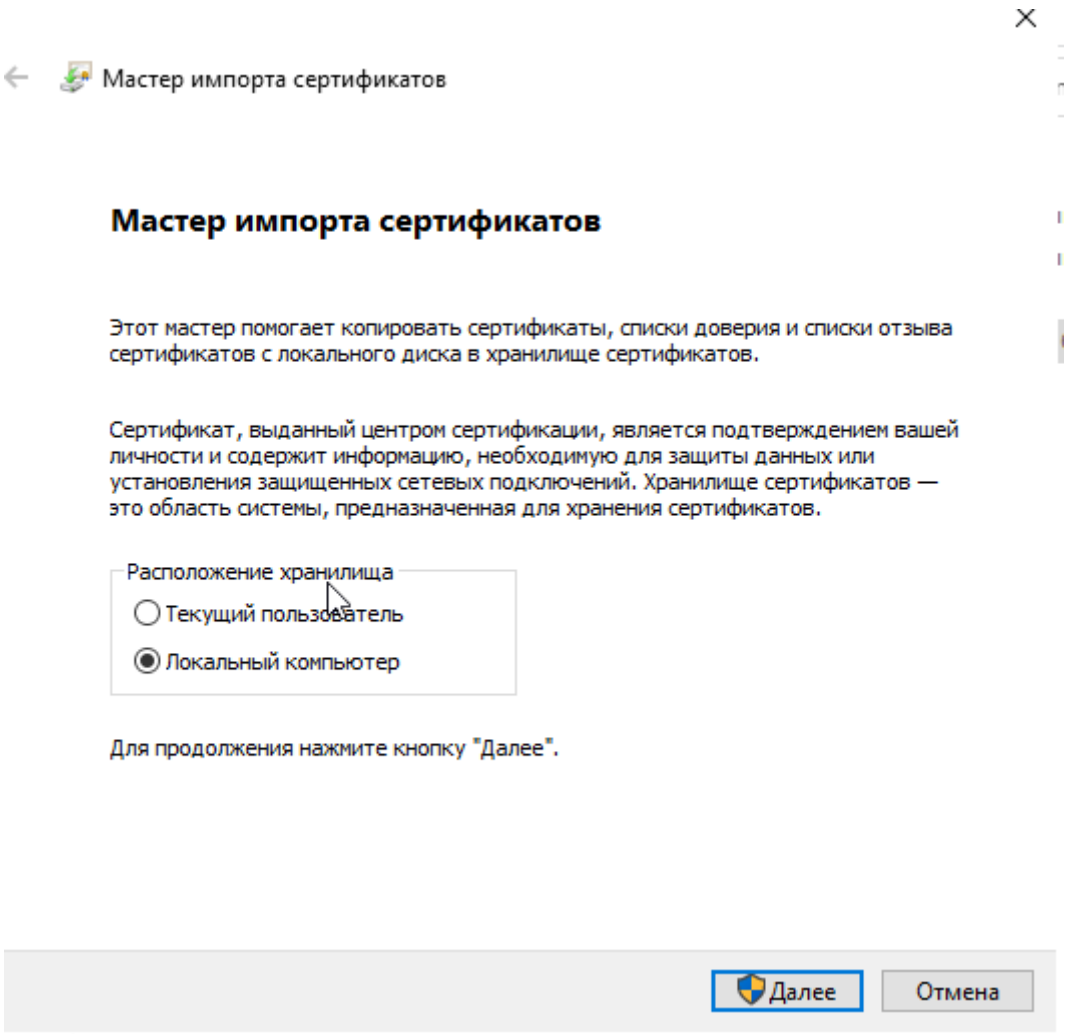
Заходим в проводник на сервере и идем по пути C:\Windows\System32\CertSrv\CertEnroll и находим там файл сертификата сервера.



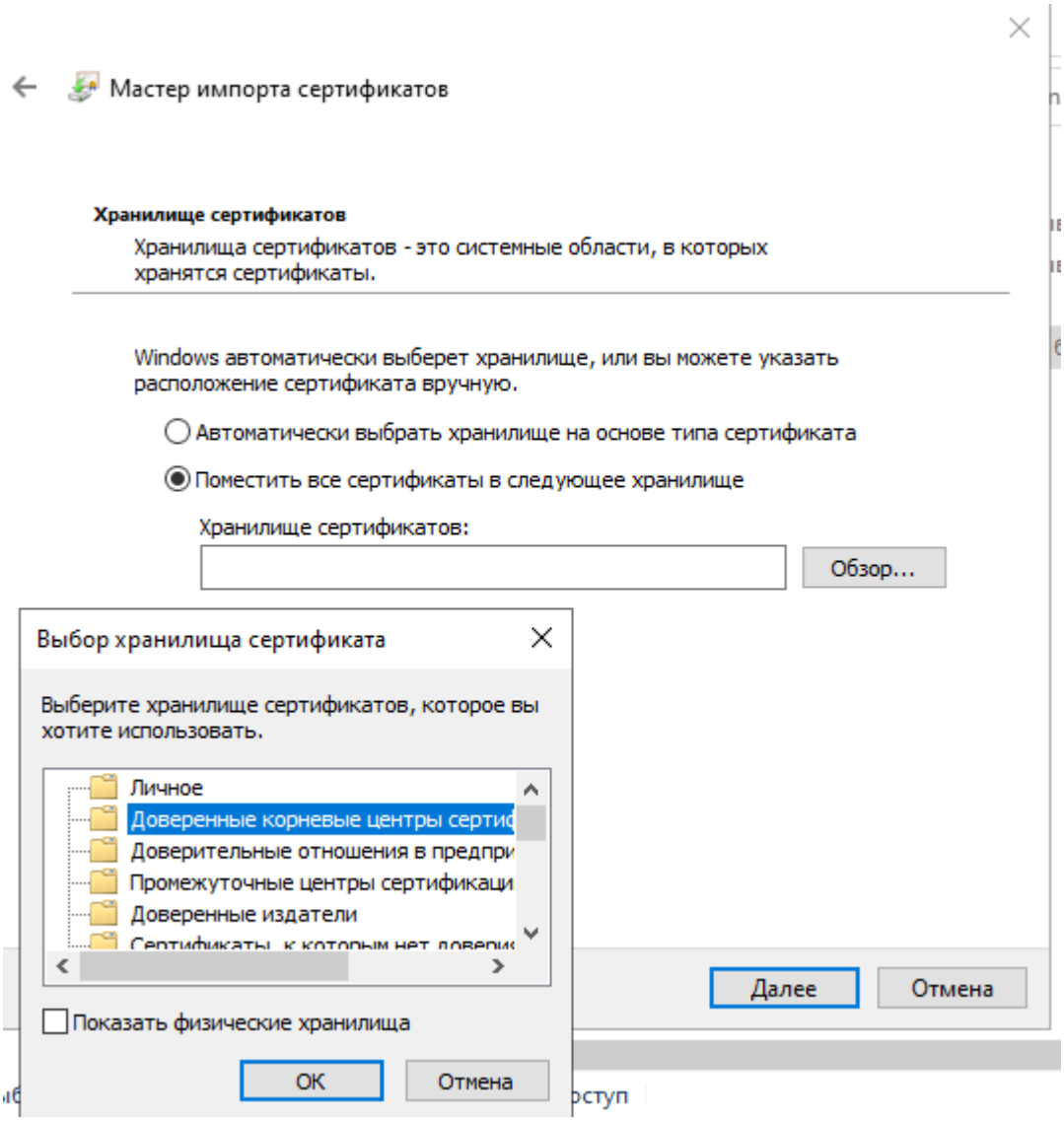
ПКМ по файлу сертификата – «Установить сертификат».



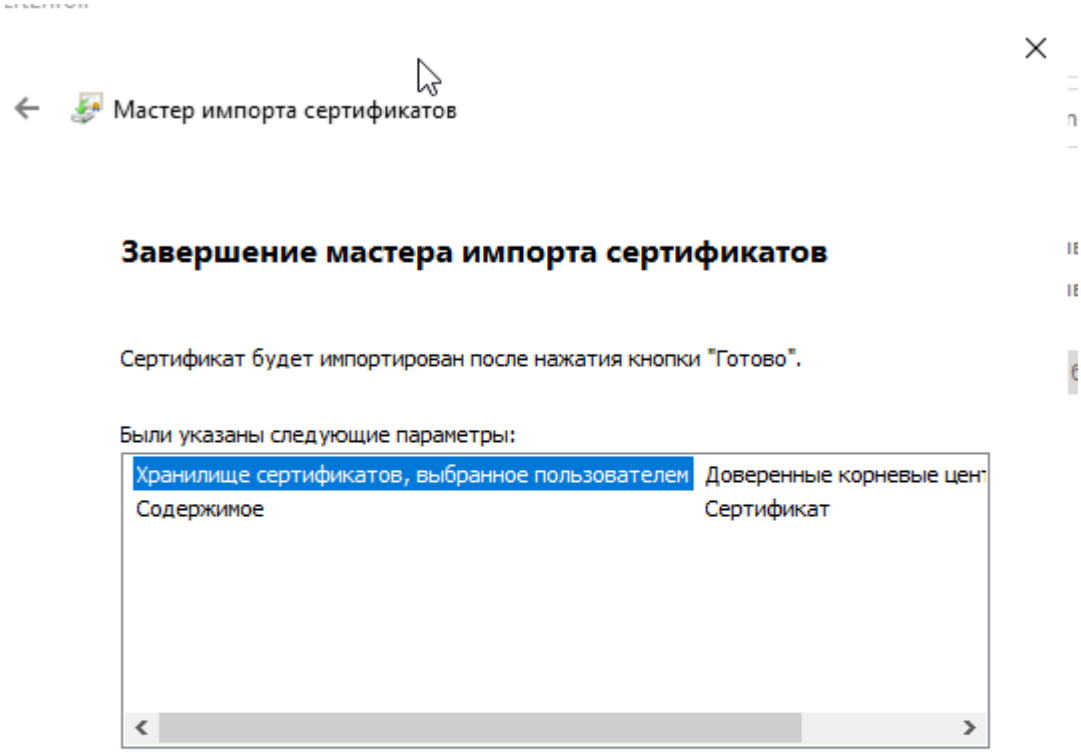
Откроется мастер импорта сертификатов. Выбираем «Локальный компьютер».

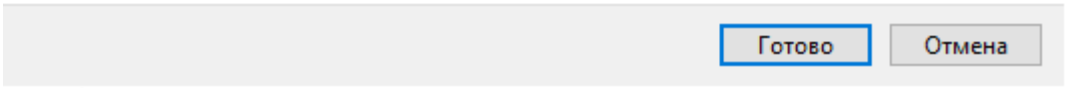


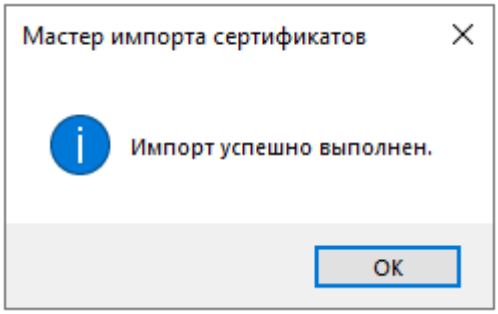
Выбираем «Поместить все сертификаты в следующее хранилище» - «Обзор» - «Доверенные корневые центры сертификации».



Жмем на следующем этапе «Готово» и видим сообщение об успешном импорте.







ВАЖНО ЗАРАНЕЕ СОЗДАЙТЕ ПОЛЬЗОВАТЕЛЯ ДОМЕНА И ВНЕГО ВХОДИТЕ НА КЛИЕНТЕ.

Чтобы создать пользователя переходите в Средства «Пользователи и компьютеры АД» затем папка users и создавайте юзера.

Далее любыми способами перекидываете сертификат на клиента вот 1 из примеров

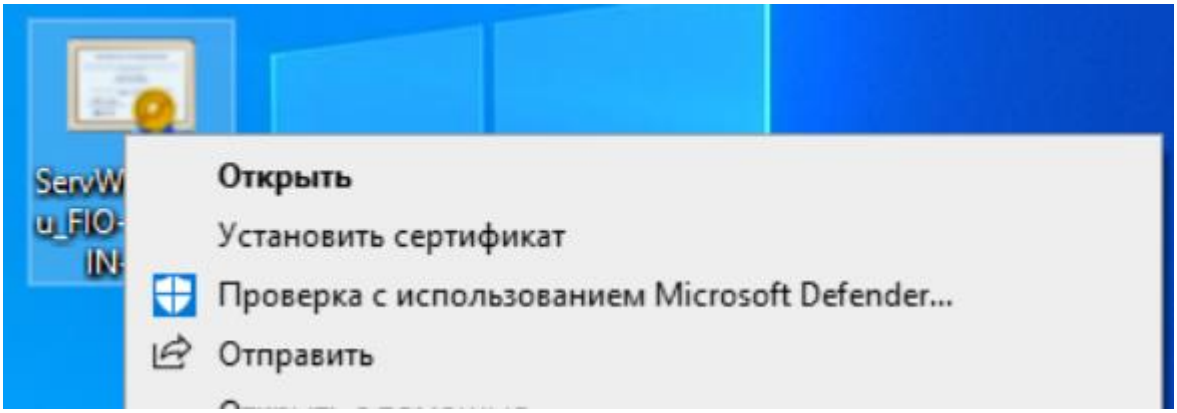
1. На двух машинах — сервере (AdminCA) и клиенте (неважно, будь то OperCA или Open) — в верхней панели VirtualBox в разделе «Устройства» была выбрана опция «Подключить образ диска Дополнительной гостевой ОС». После этого необходимо открыть проводник, перейти в раздел «Мой компьютер», найти подключённый диск VirtualBox и запустить VBoxWindowsAdditions.exe.

2. На серверной машине (AdminCA) в верхней панели VirtualBox в разделе «Устройства» была включена функция Drag and Drop. После этого папка с сертификатом была перетащена с виртуальной машины на рабочий стол физической машины с помощью мыши.

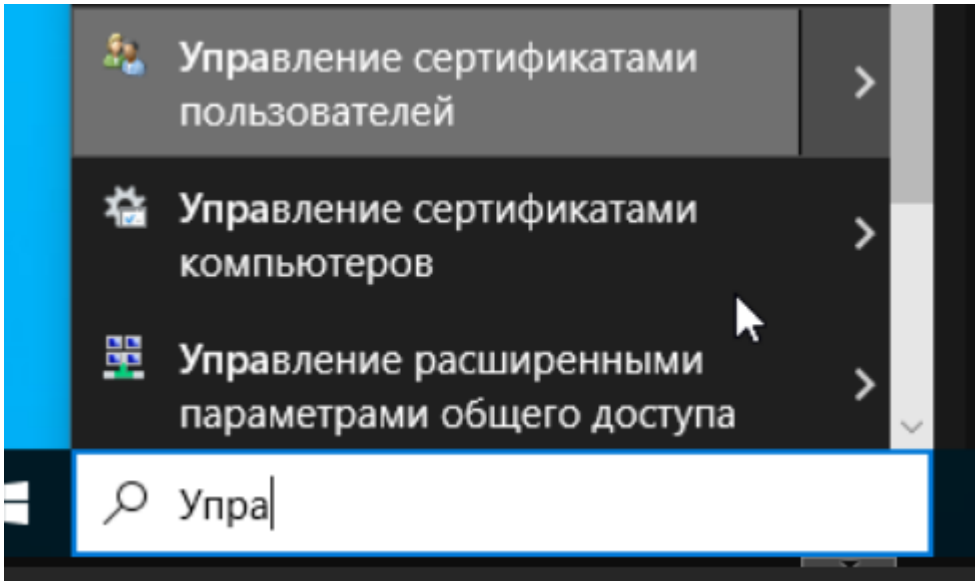
3. На клиентской машине (неважно, будь то OperCA или Open) в верхней панели VirtualBox в разделе «Устройства» была подключена общая папка, при этом был установлен флажок «Автоподключение» с указанием пути к папке на физической машине (на рабочем столе). Данная папка обеспечивает взаимодействие между виртуальной и физической машинами.

4. Затем, открыв проводник на клиентской машине и перейдя в раздел «Мой компьютер», можно обнаружить дополнительный диск, на котором находится сертификат

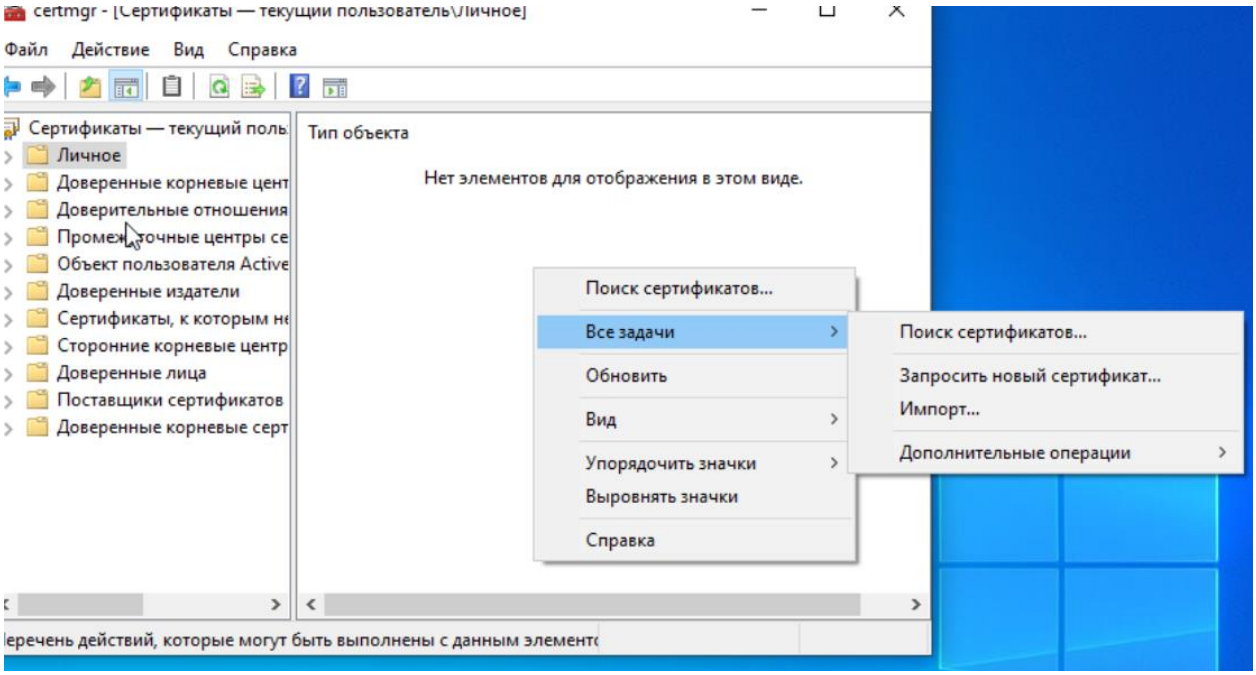
Устанавливаем сертификат, также, как и на сервере В ходе установки сертификата на локальный компьютер потребуют учетные данные администратора, используем «Администратор» и пароль от администратора домена.



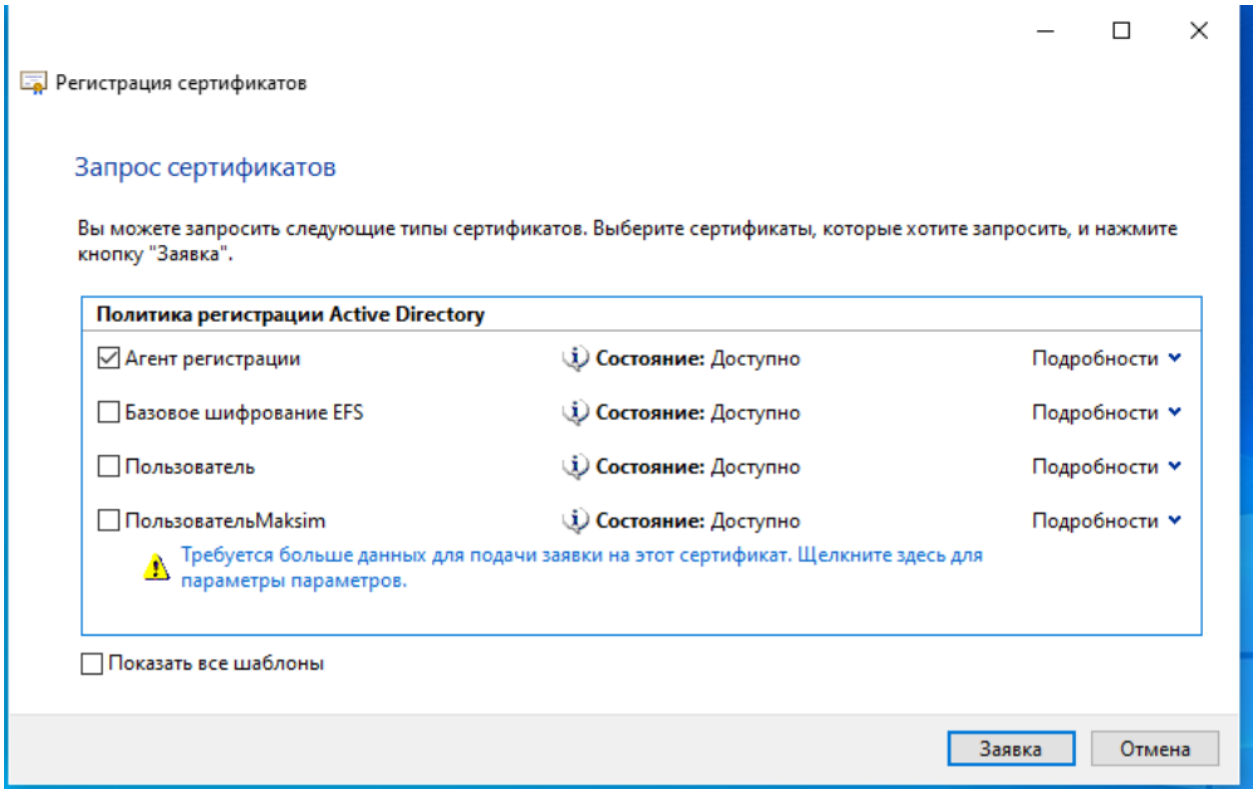
Открываем на клиенте «Управление сертификатами пользователей».



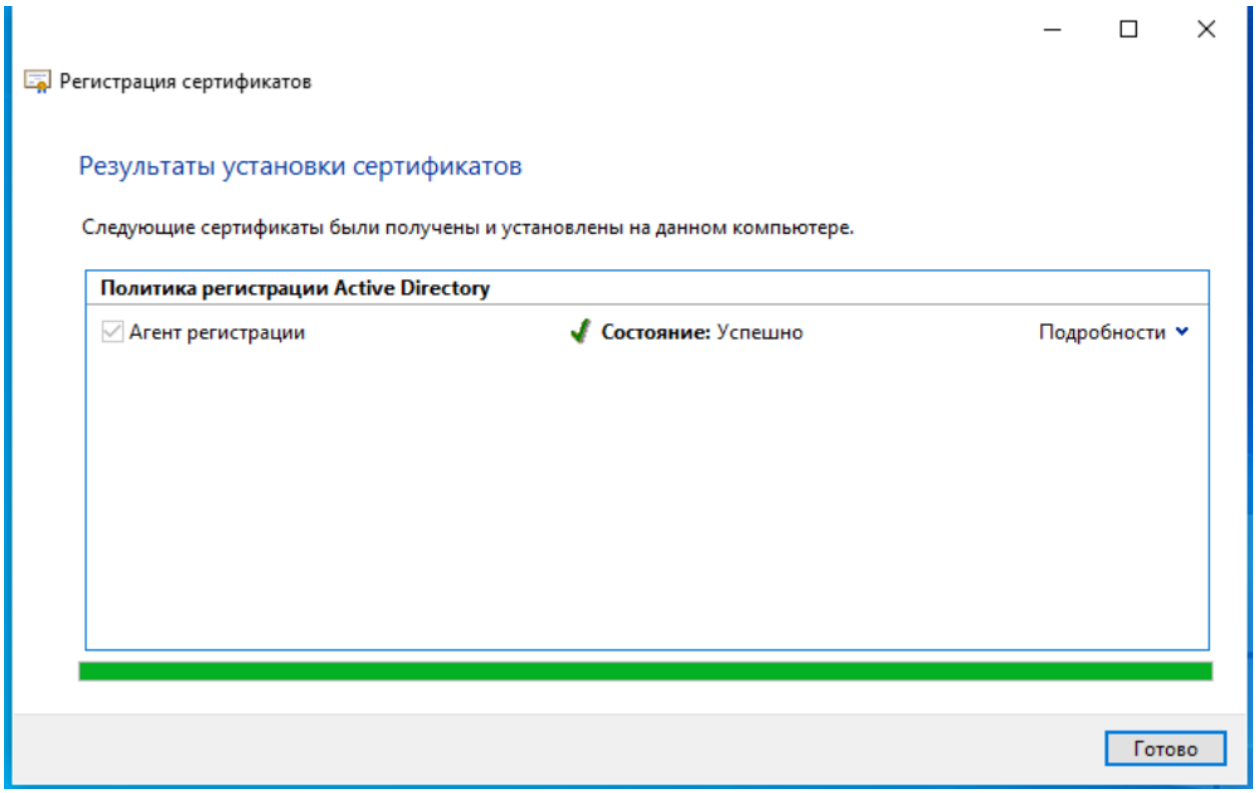
Нажимаем на папку «Личное», затем ПКМ по пустой области, «Все задачи» - «Запросить новый сертификат».



Нажимаем «Далее», «Далее» и видим список доступных для запроса сертификатов. В первую очередь запрашиваем «Агента регистрации», нажимаем «Заявка».



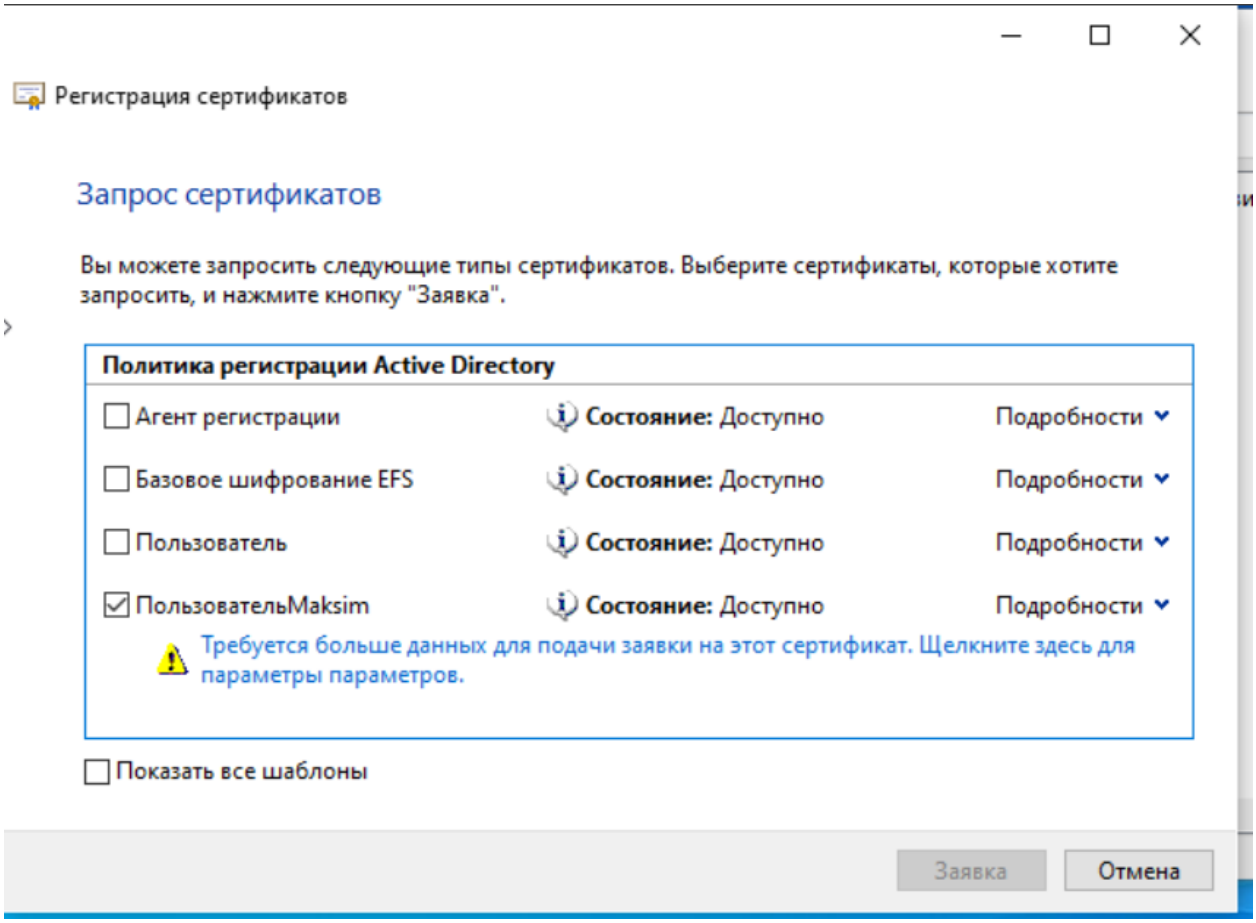
Результатом установки сертификатов должно быть следующее сообщение.



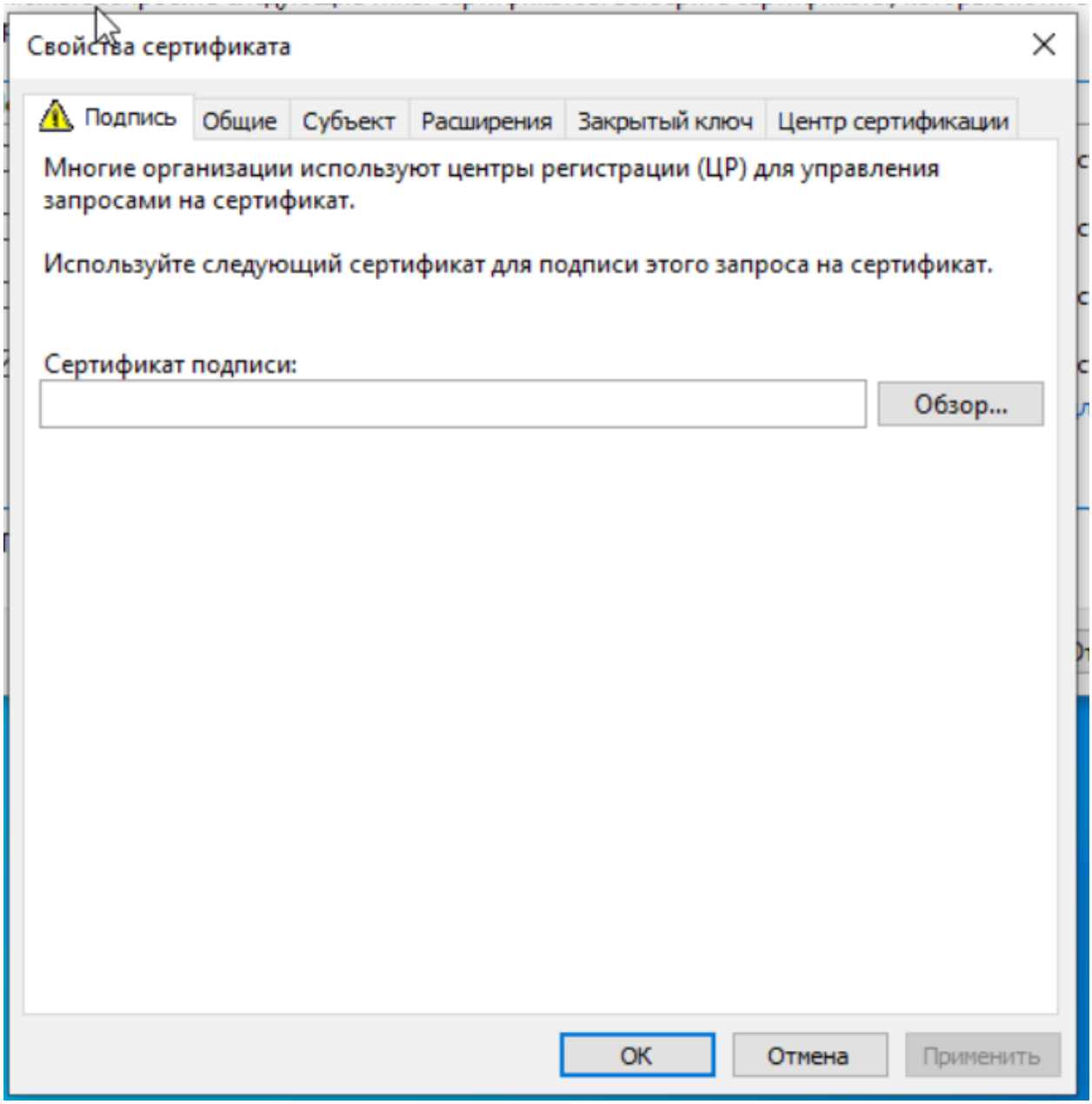
Появляется папка «Сертификаты», а в ней новый сертификат.

Повторяем процедуру с запросом.

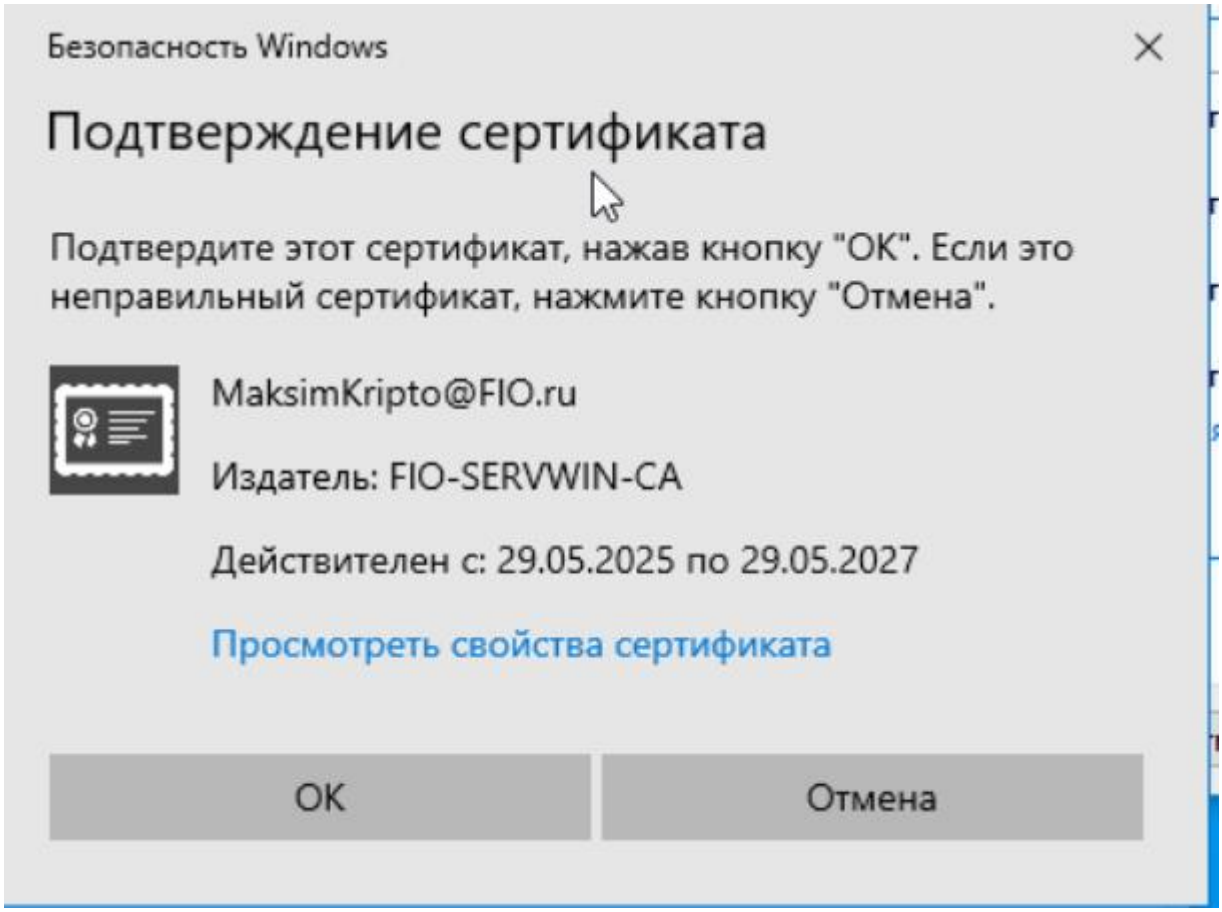
Нажимаем на синее сообщение под нашим созданным шаблоном «Пользователь Имя»



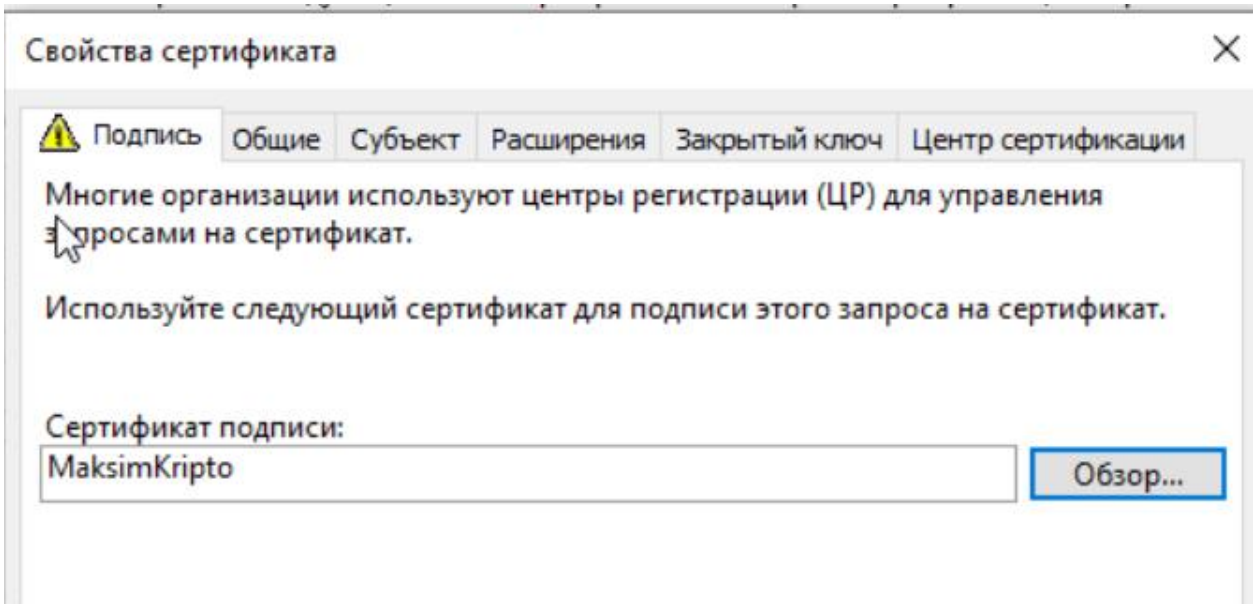
Нажимаем на «Обзор» рядом с «Сертификатом подписи».



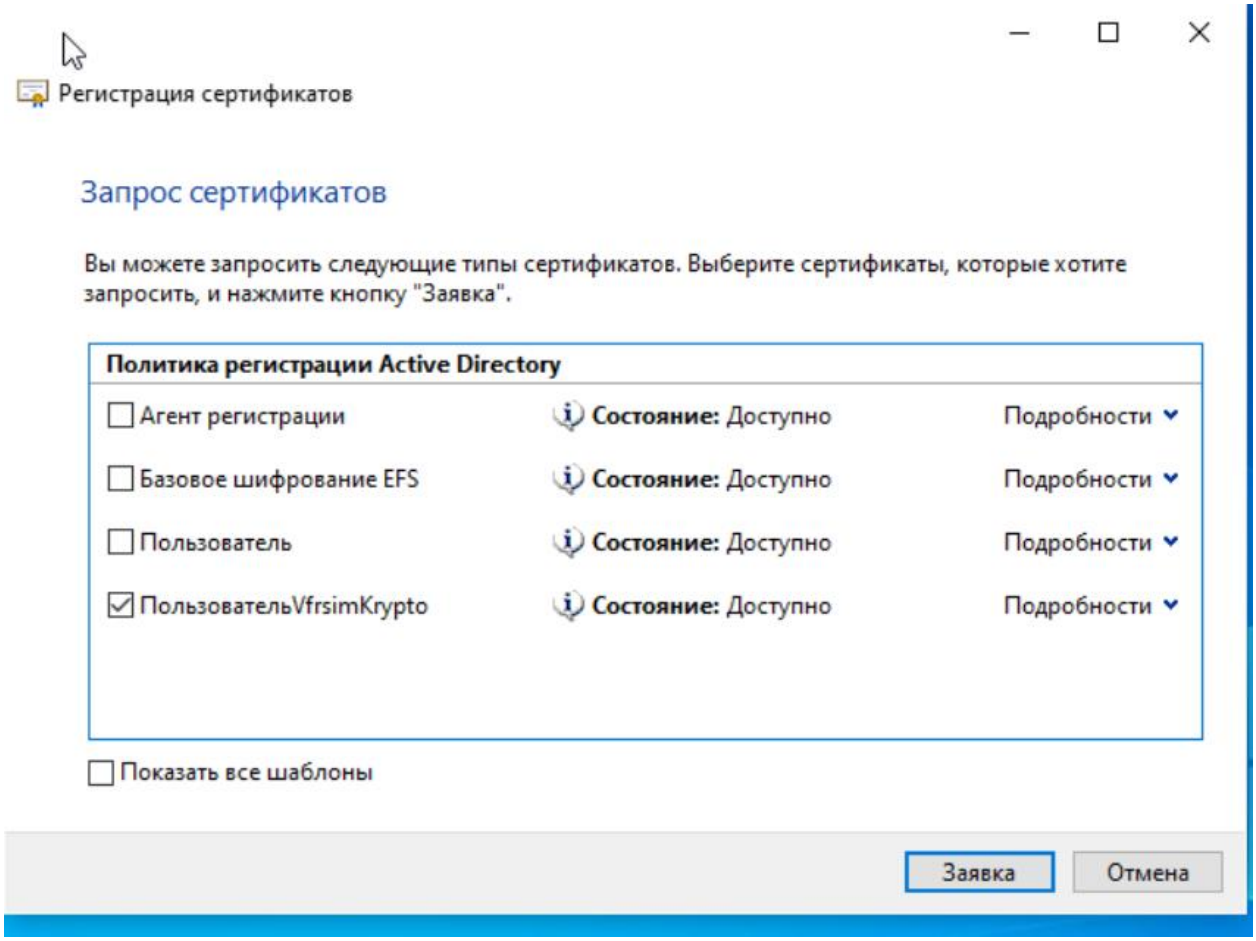
Появляется окно о подтверждении сертификата, жмем «ОК».



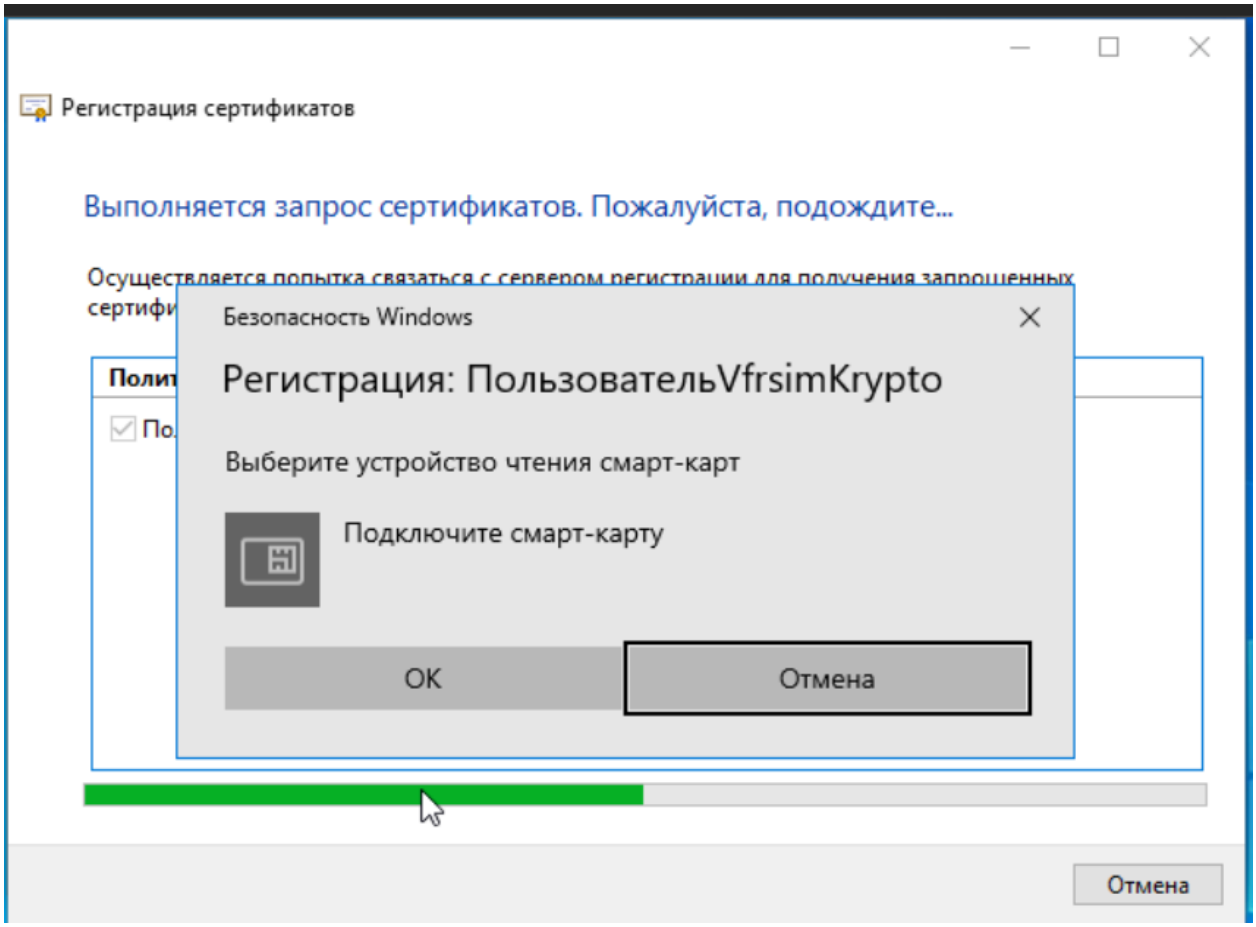
После этого жмем «Применить» и «ОК».



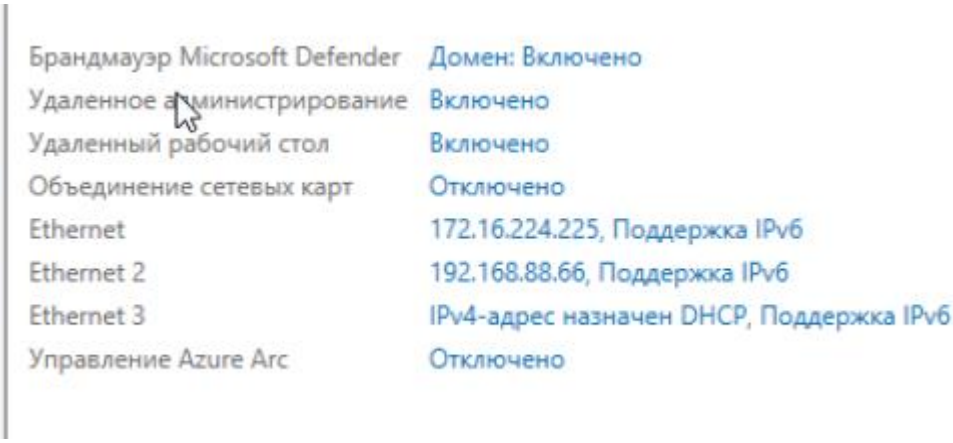
Теперь сообщения нет и можно делать заявку на сертификат созданного шаблона.



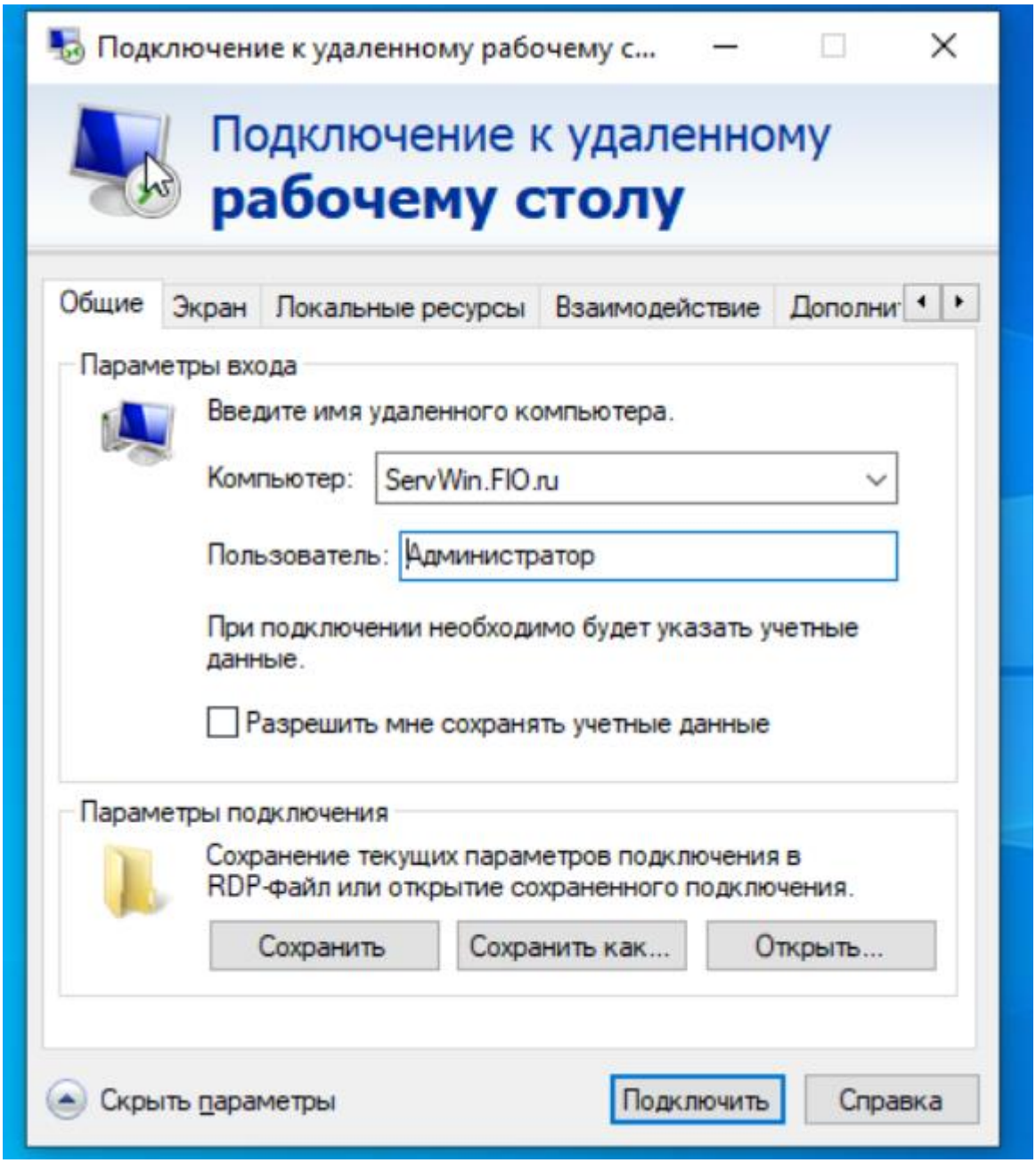
Появляется сообщение о подключении «Смарт-карты», жмем «Отмена» и радуемся жизни



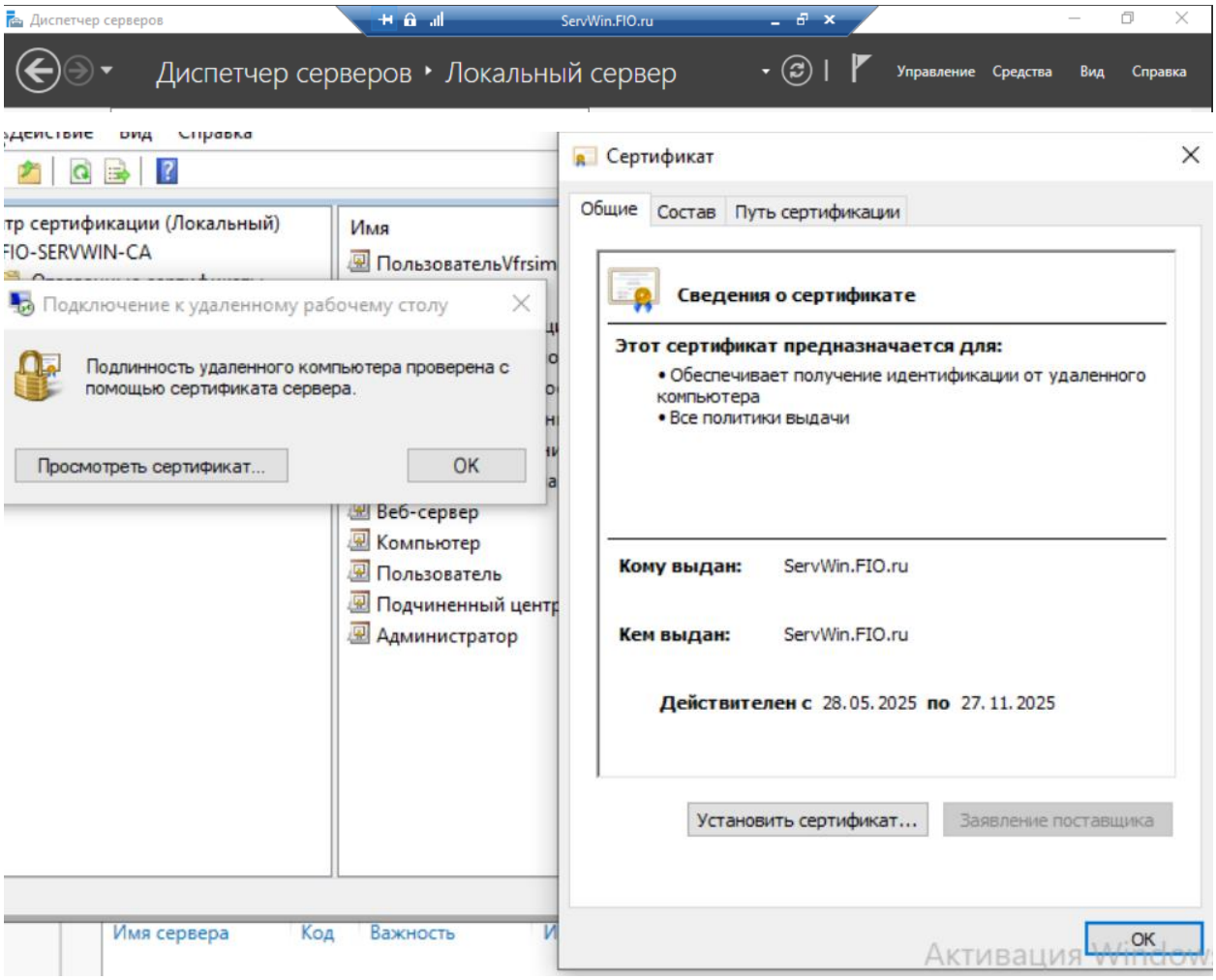
Возвращаемся на сервер, жмем «Локальный сервер» и включаем удаленный рабочий стол.



Открываем «Подключение к рабочему столу» на клиенте и в качестве компьютера пишем полное доменное имя сервера, а также пользователя«Администратор».



После установки соединения в верхней панели появится значок замочка, нажав на который можно убедиться в защищенности соединения. В случае если его нет, попробуйте установить сертификат.



```
PostUp = iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A
POSTROUTING -o eth0 -j MASQUERADE

PostDown = iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D
POSTROUTING -o eth0 -j MASQUERADE
```