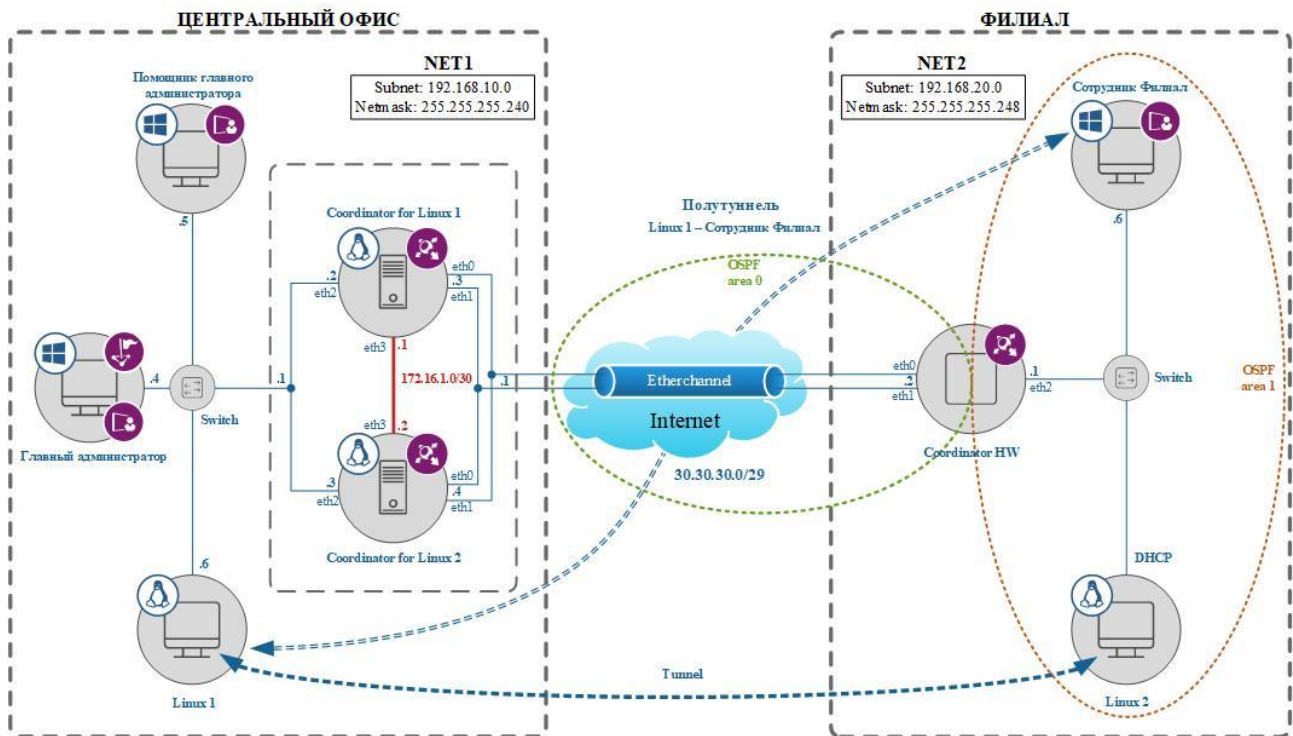


Топология сети

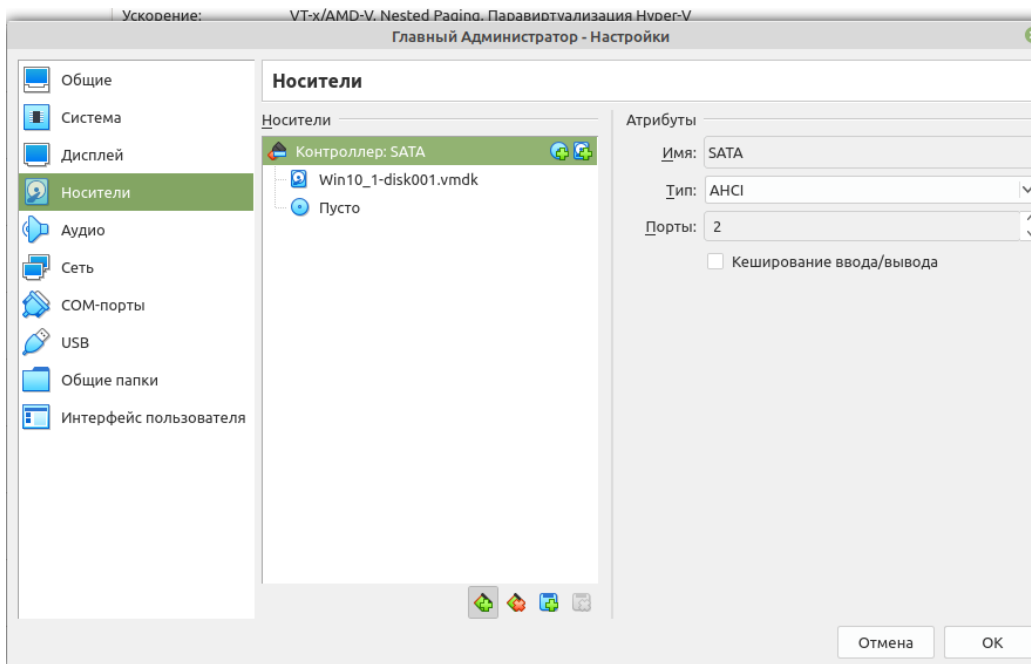


Связи с пользователями

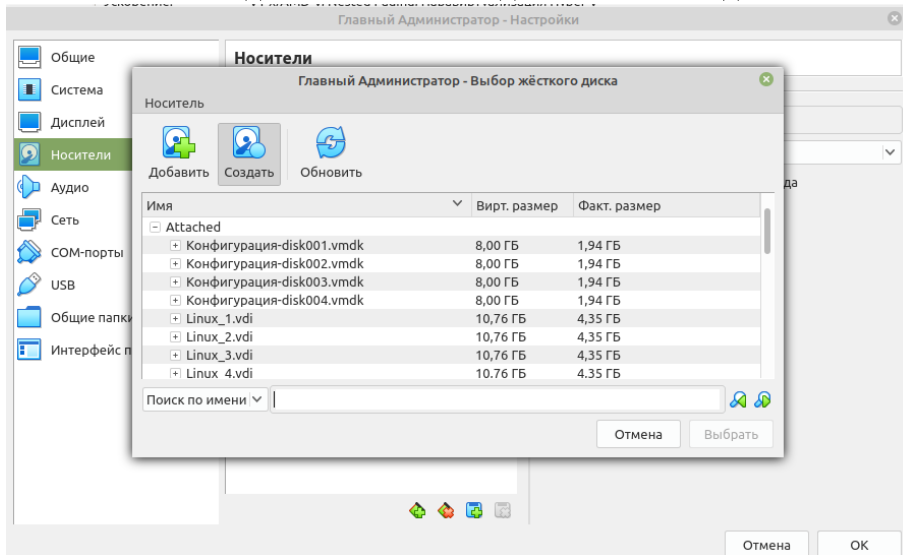
<i>Связи пользователей</i>	Главный администратор	Помощник главного админа	Сотрудник Филиал	Coordinator for Linux	Coordinator HW
Главный администратор		•	•	•	•
Помощник главного админа	•			•	
Сотрудник Филиал	•				
Coordinator for Linux	•	•			•
Coordinator HW	•			•	

!!!!Так же надо выдать связь Сотрудник Филиал с Coordinator for Linux для полутуннеля

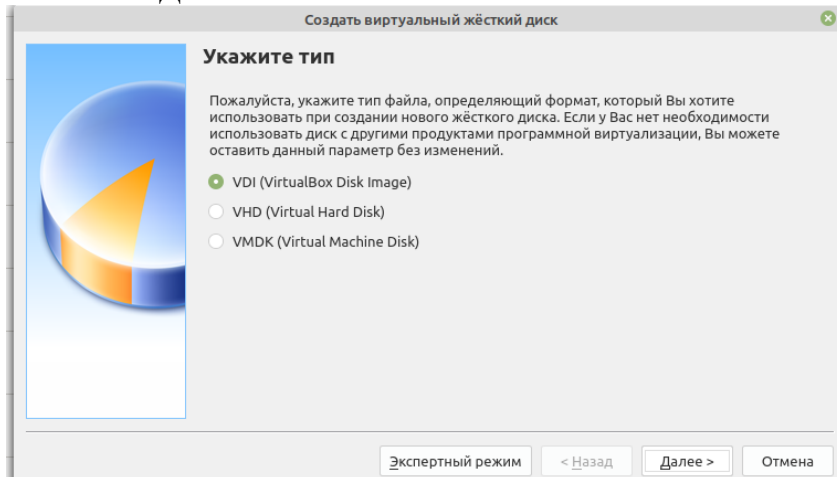
Заходим в VirtualBox, выбираем Главный администратор, заходим в Настройки → Носители и добавляем контроллер USB



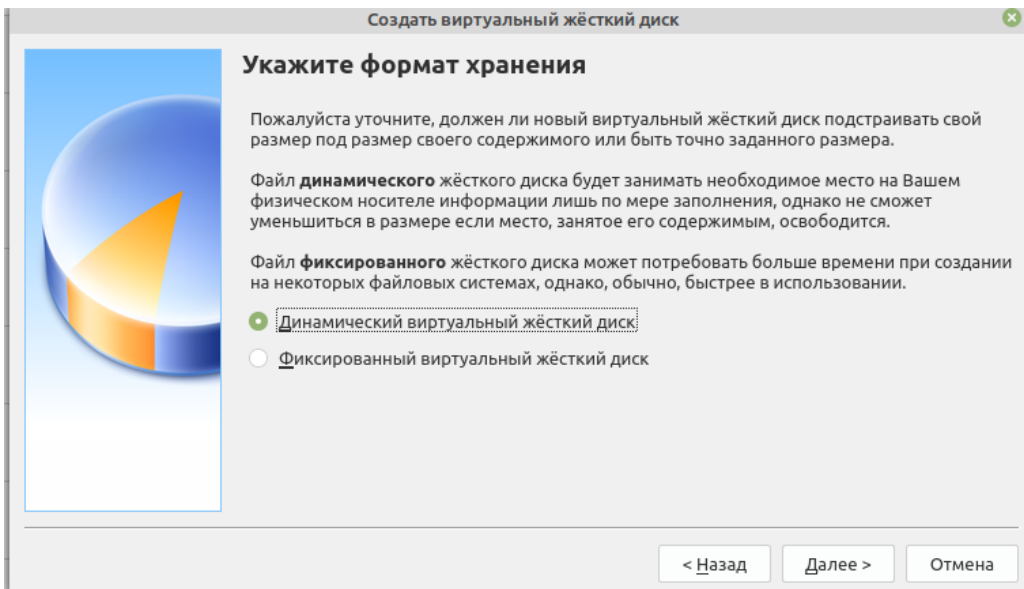
После нажимаем добавить жесткий диск и ждем создать



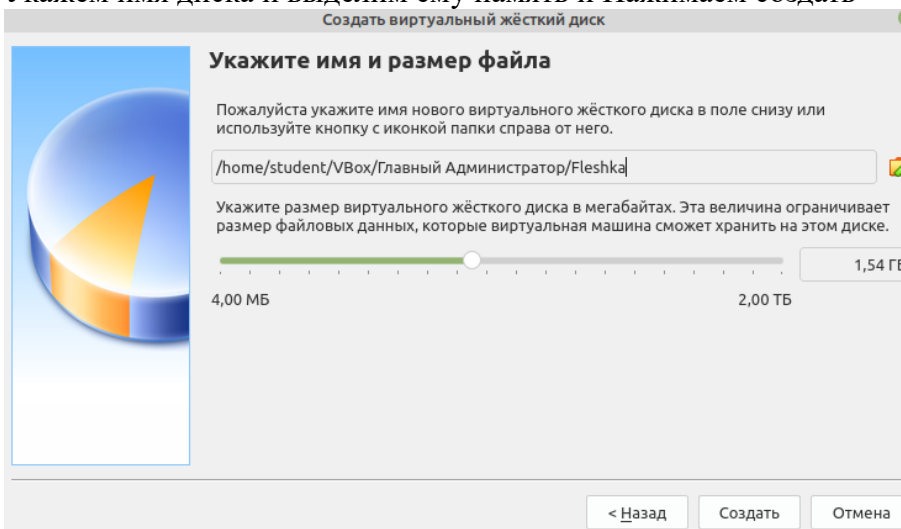
Нажимаем Далее



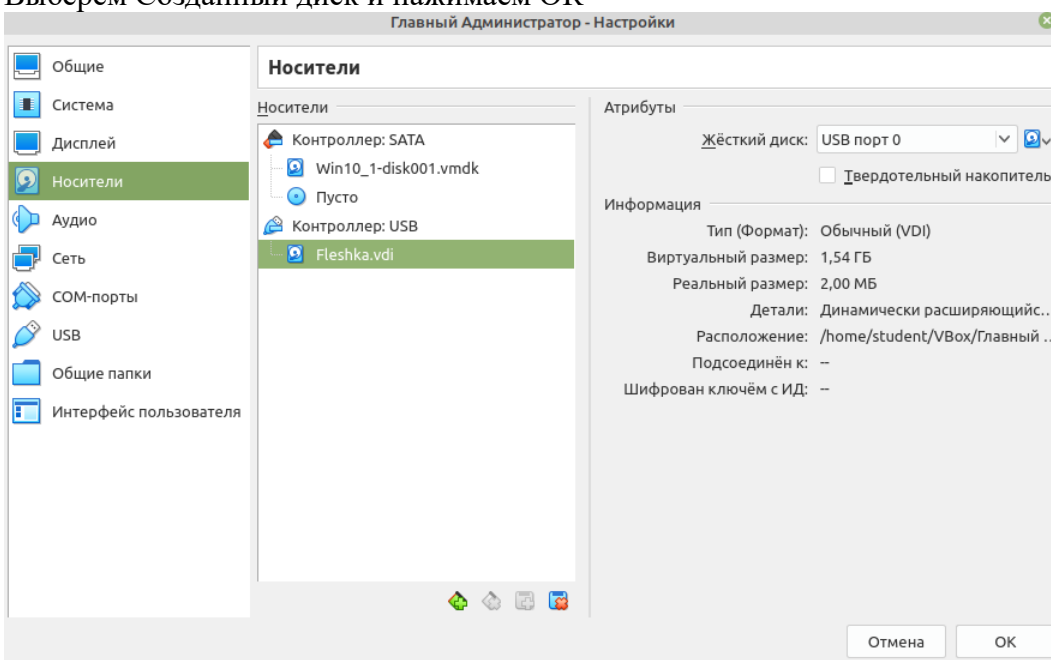
Нажимаем Далее



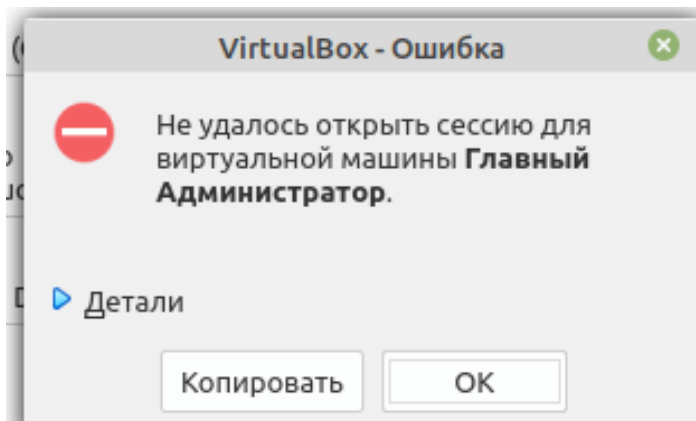
Укажем имя диска и выделим ему память и Нажимаем создать



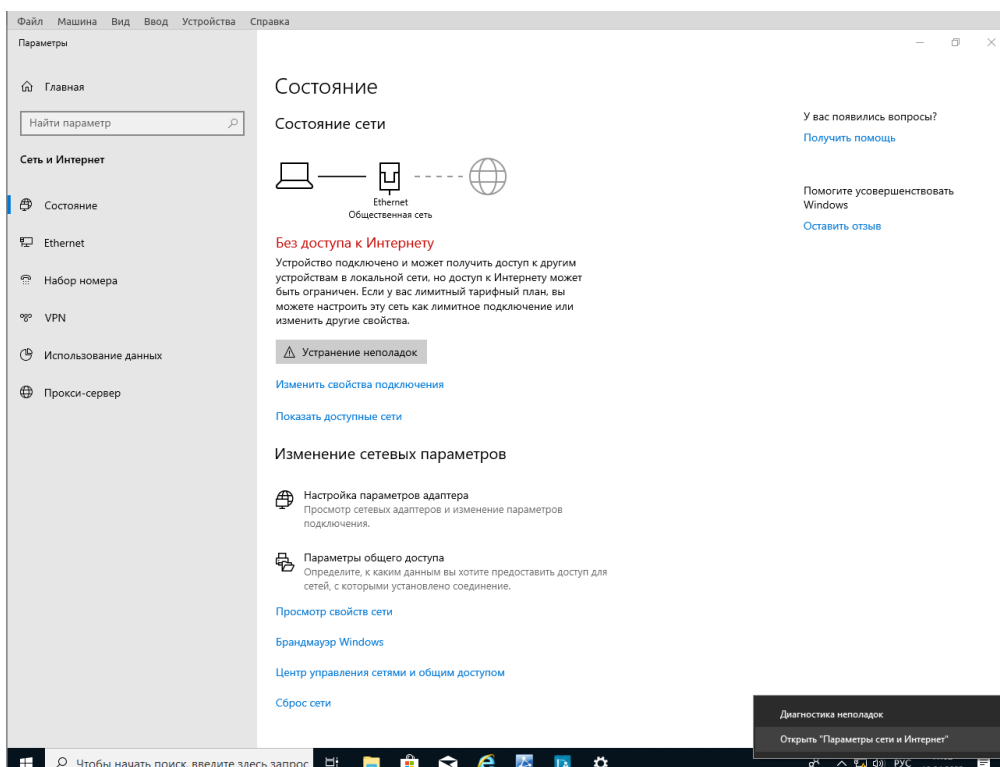
Выберем Созданный диск и нажимаем ОК



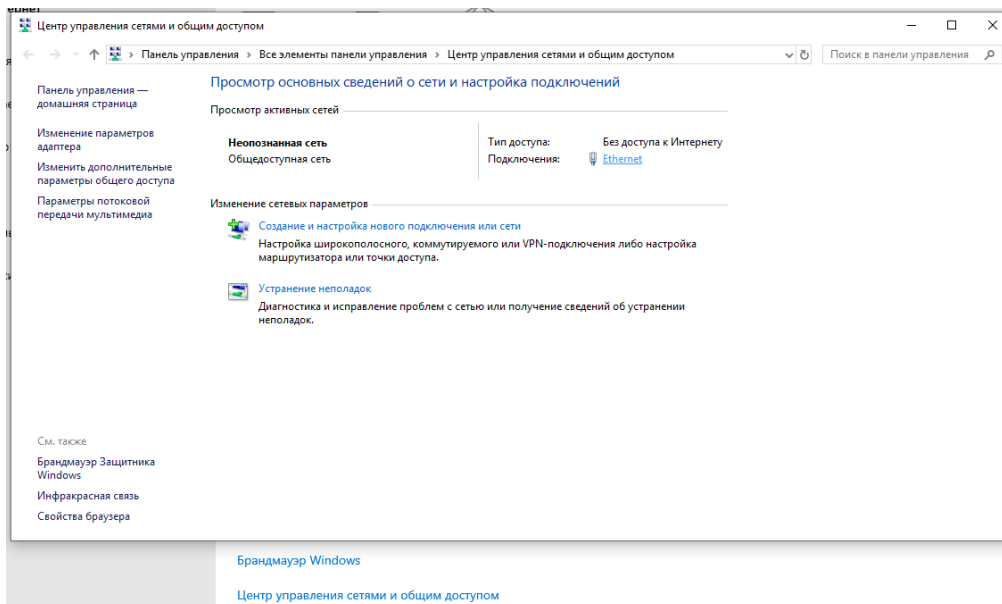
Запускаем машину. Появится окно с ошибкой, нажимаем ОК и запускаем еще раз



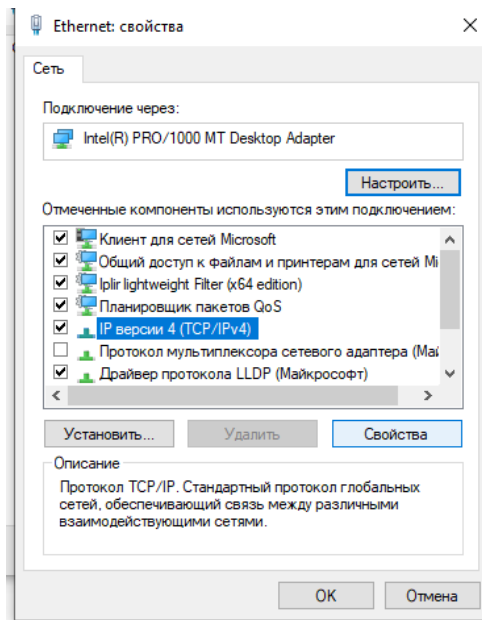
Выдача IP- адреса на машину Главного администратора. Открываем параметры сети и интернет



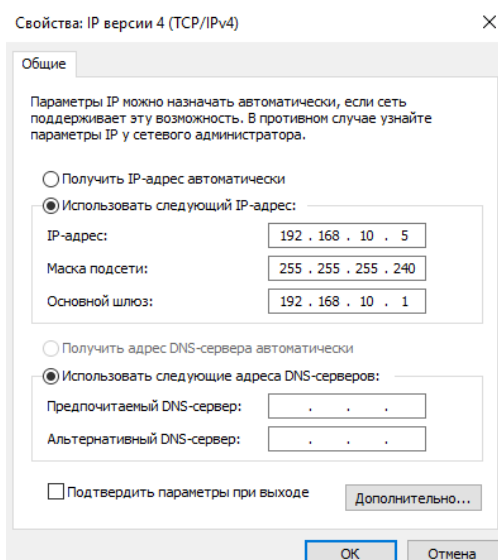
Нажимаем Центр управление сетями общим доступом и нажать на Ethernet, свойства



Найти IPv4 и нажать свойства

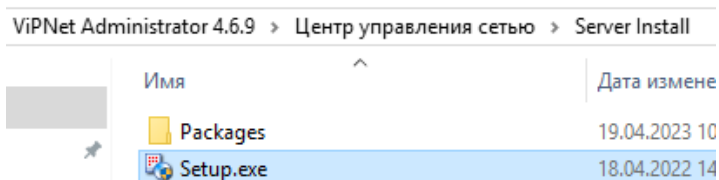


Выдать IP-адрес как показано на схеме

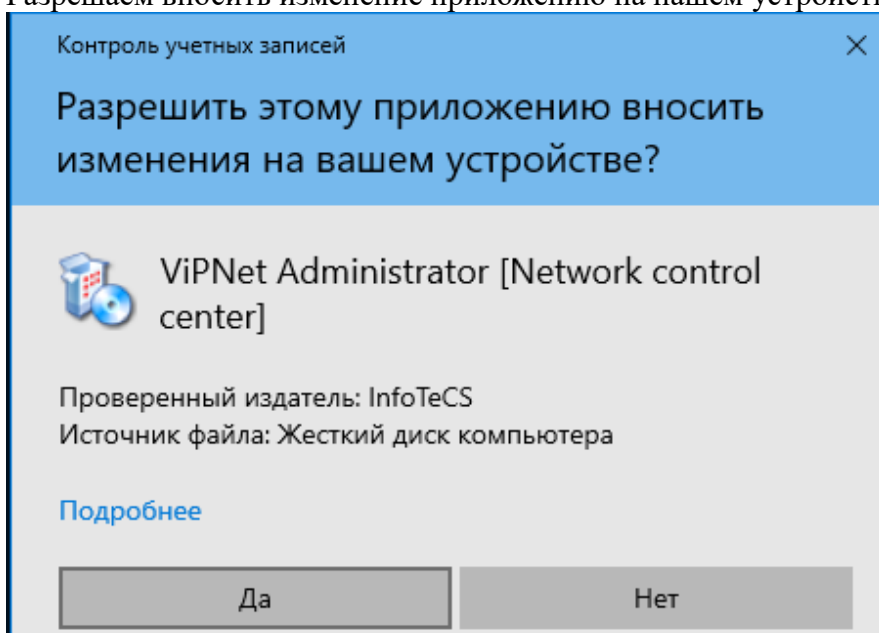


Загрузка ViPNet Administrator

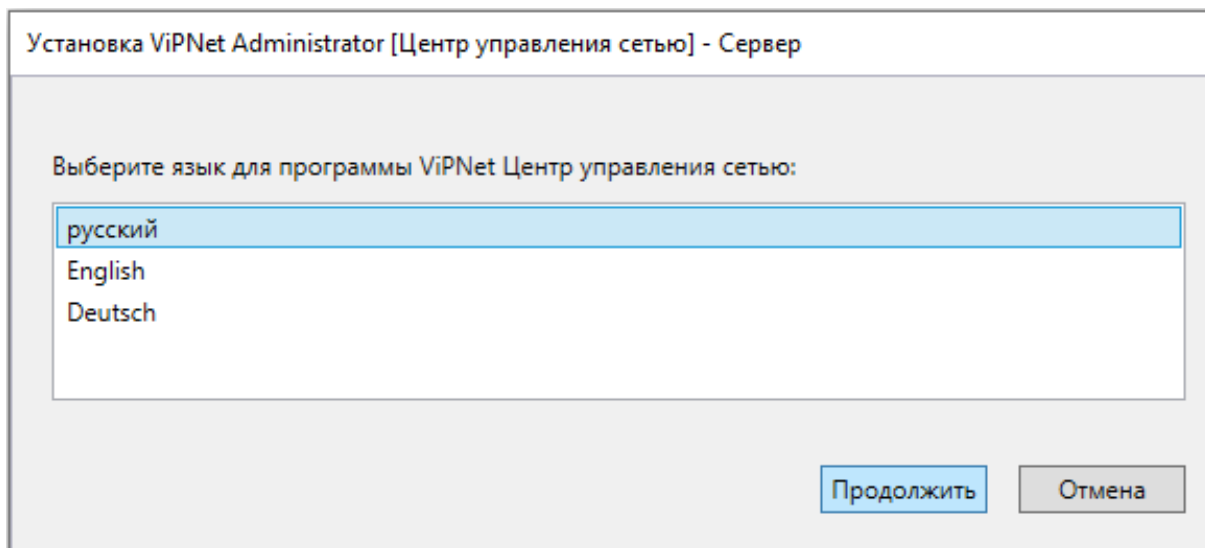
Запускаем Setup.exe в папке ViPNet Administrator 4.6.9\Центр управление сетью\Server Install



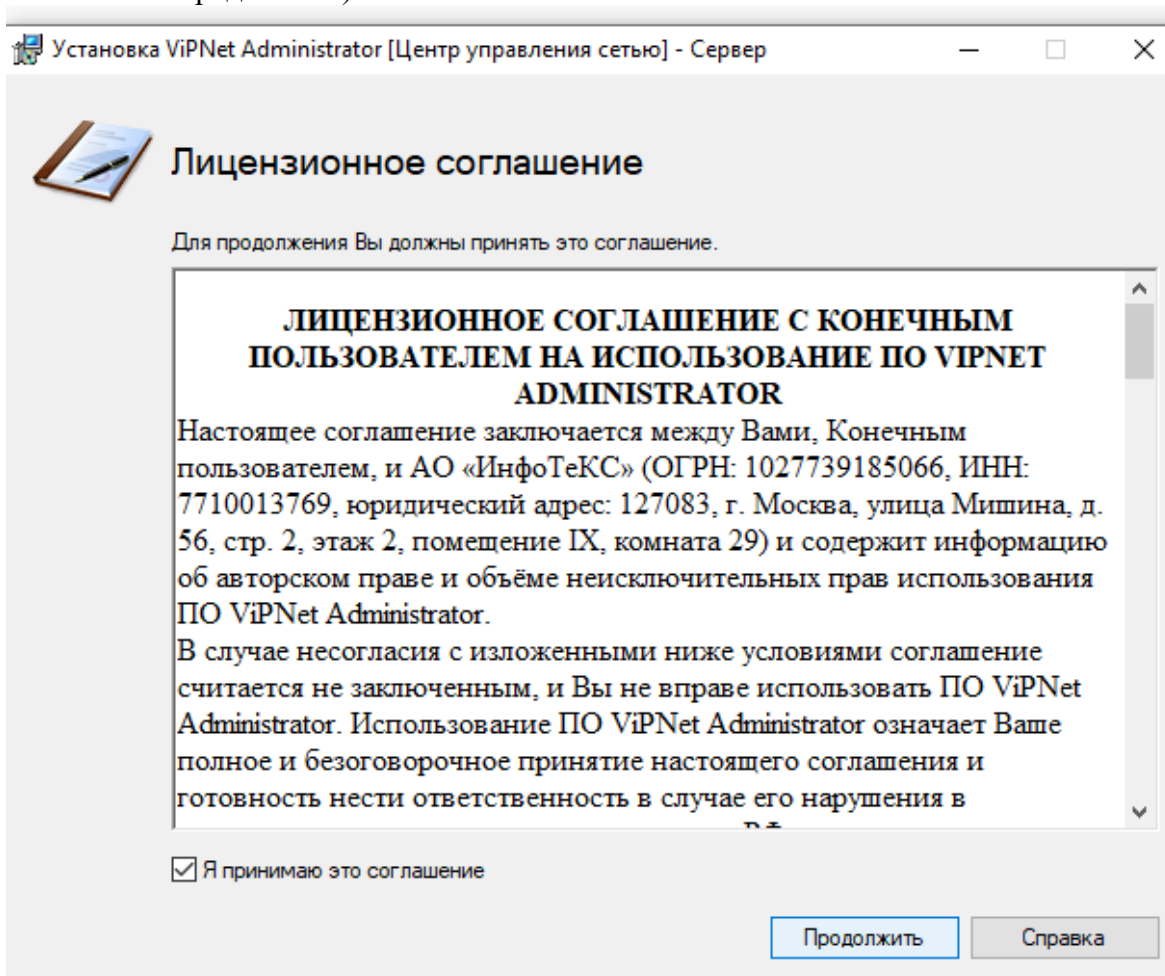
Разрешаем вносить изменение приложению на нашем устройстве



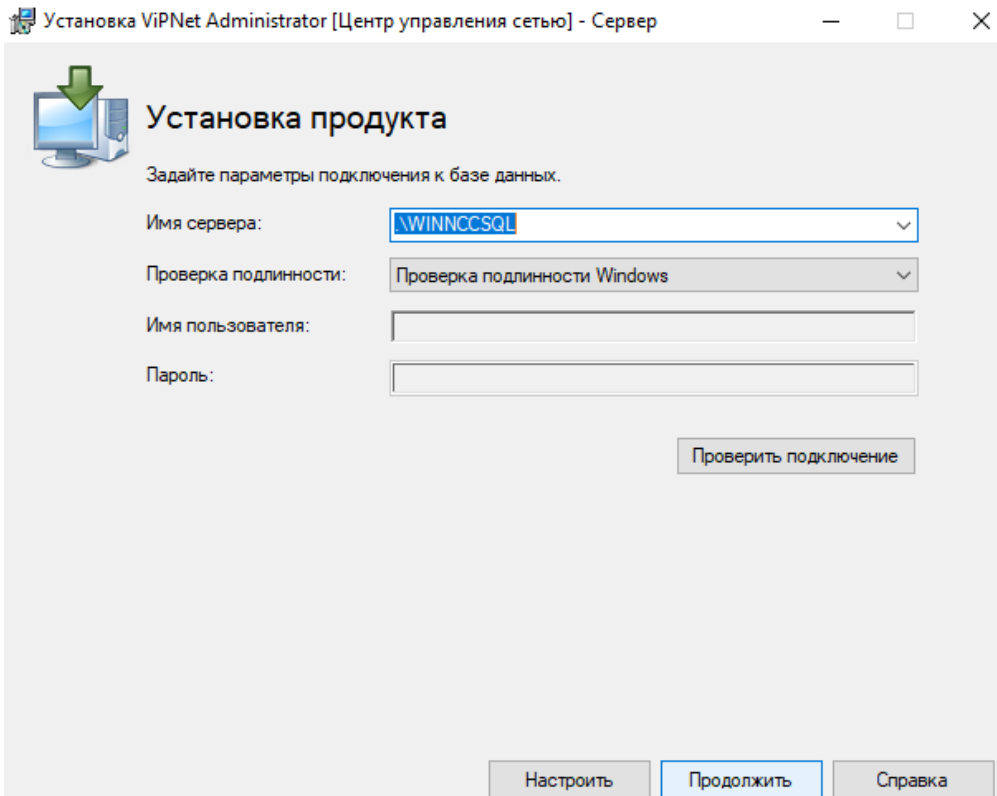
Выбираем язык для программы



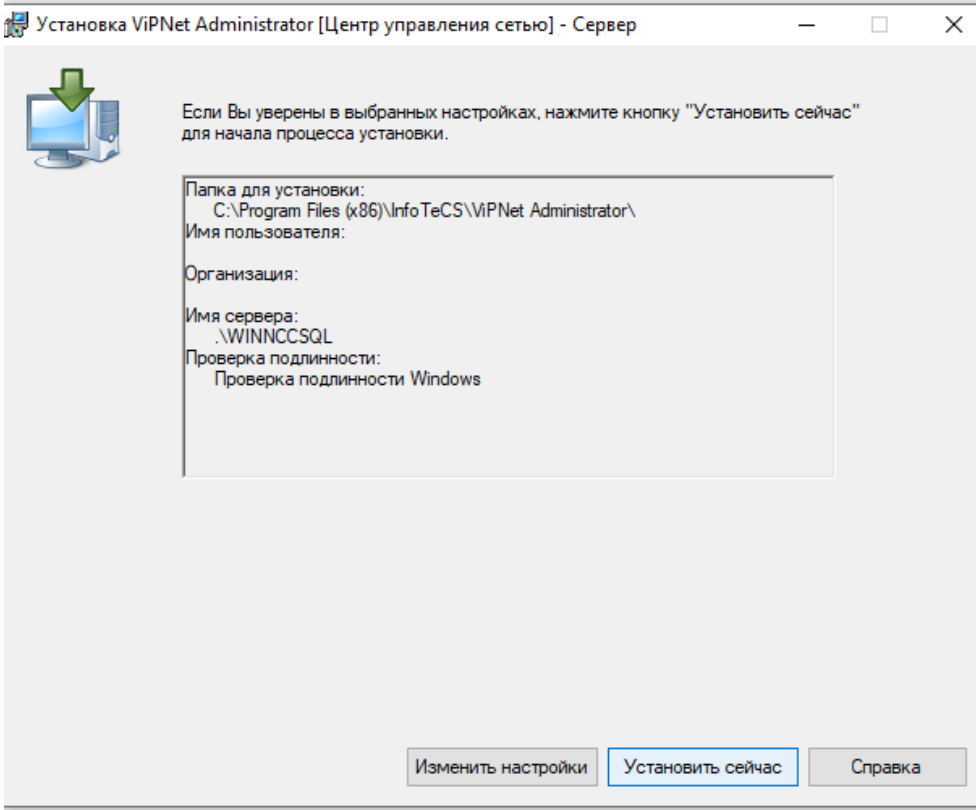
Читаем и принимаем лицензионное соглашение (Ставим галочку я принимаю это соглашение и нажимаем продолжить)



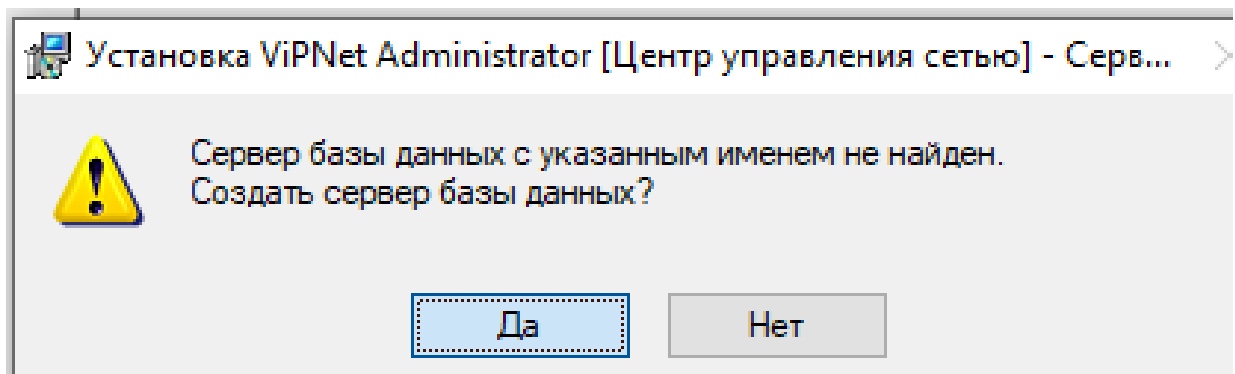
Подключаемся к Базе Данных



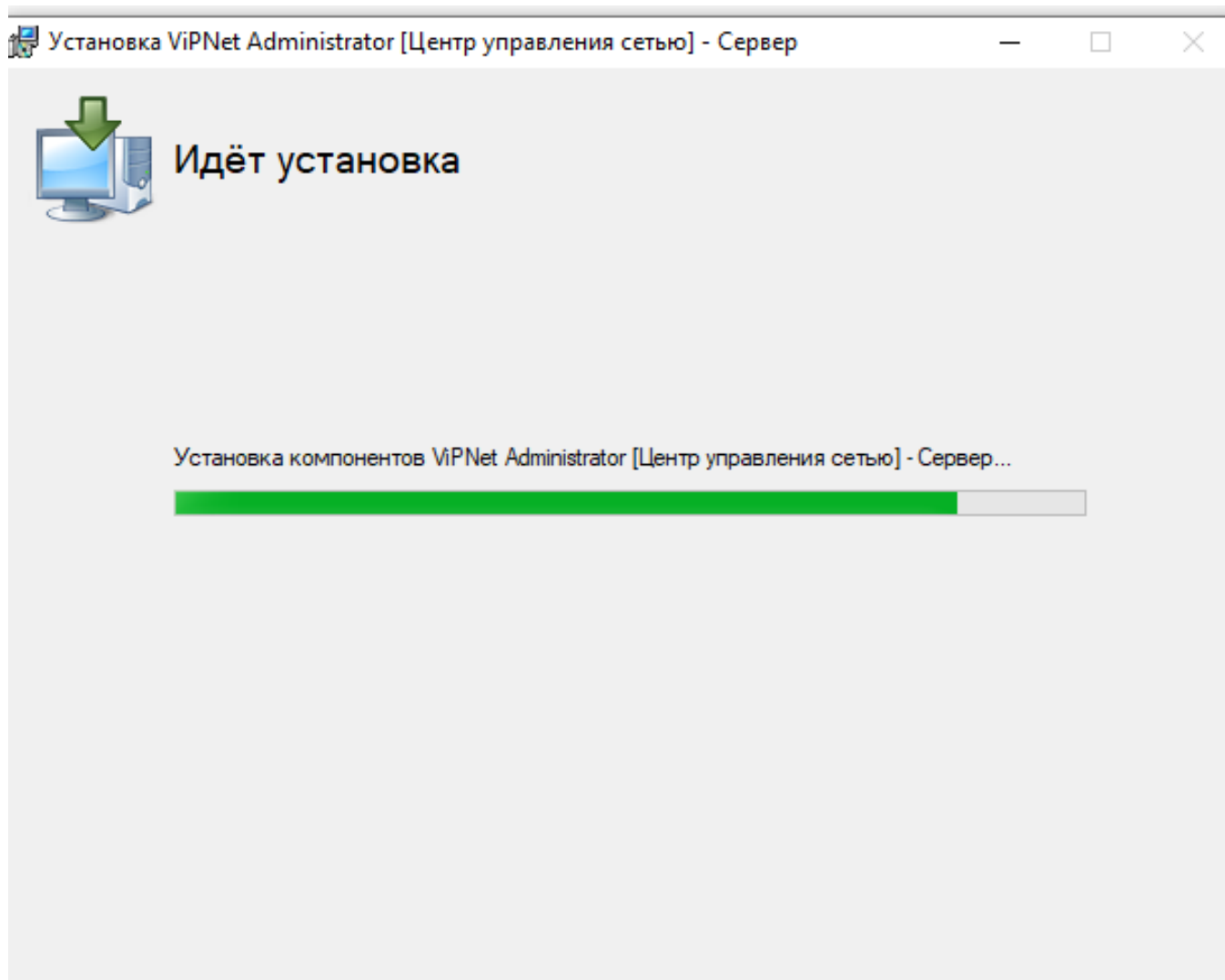
Нажимаем Установить сейчас



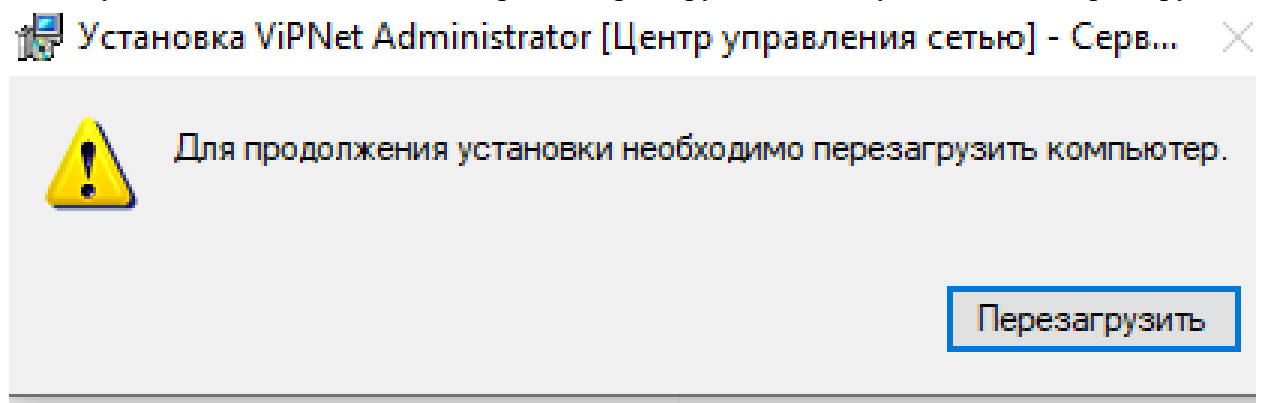
Центр управление сетью не находит Базу с указанным именем и просит создать. Нажимаем Да



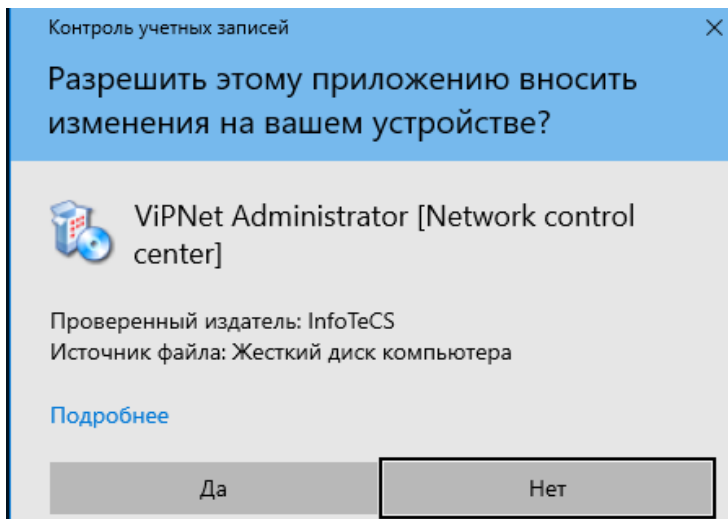
После чего начнется создание Баз Данных



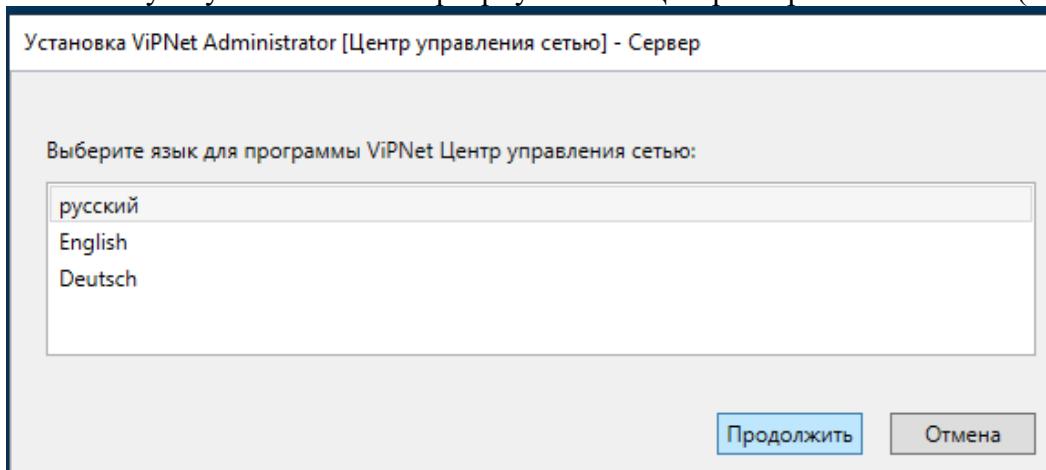
После установки базы данных, он просит перезагрузить машину. Нажимаем перезагрузить



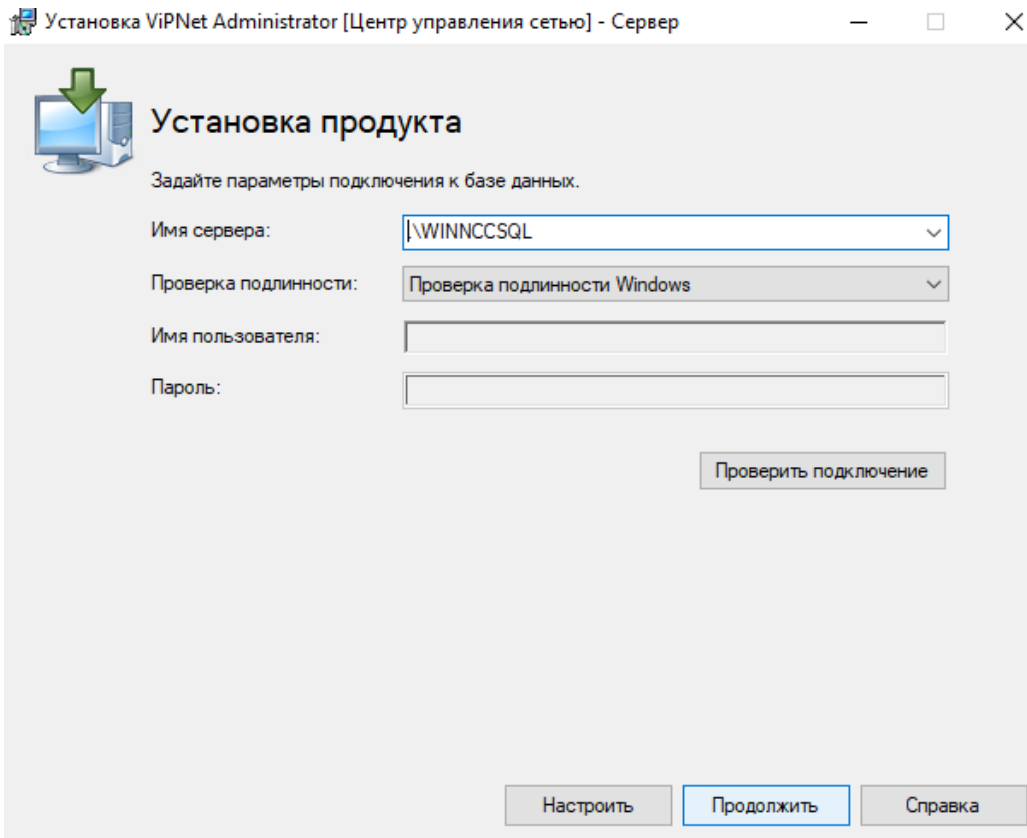
После перезагрузки вновь просит разрешение. Нажимаем Да



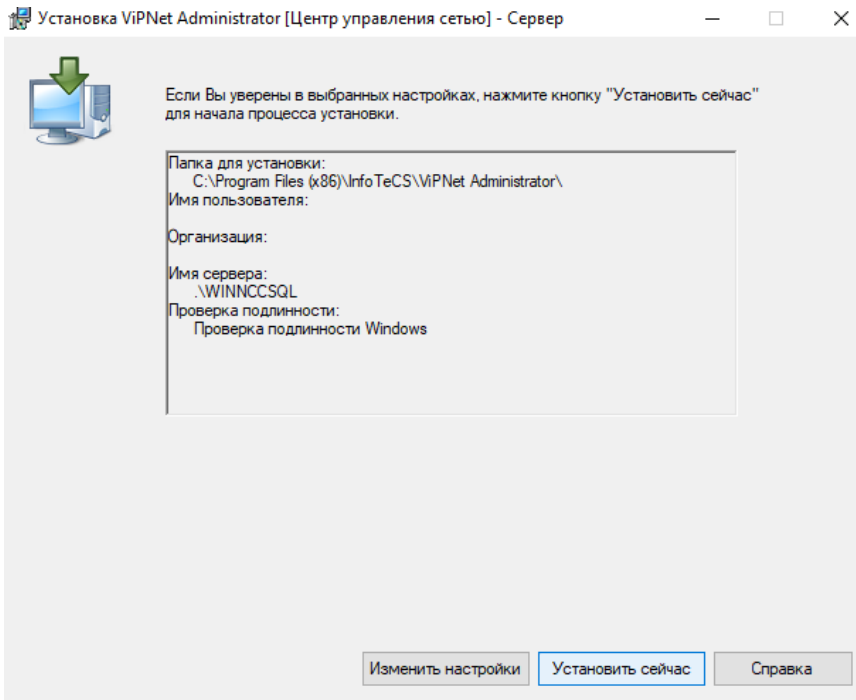
После он попросит выбрать язык для установки (До перезагрузки он создавал базу данных, а сейчас он уже устанавливает серверную часть Центра Управления Сетью (ЦУС))



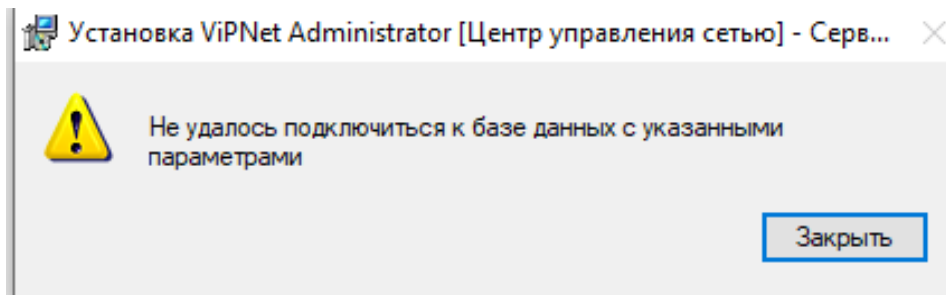
Подключаемся к Базе Данных



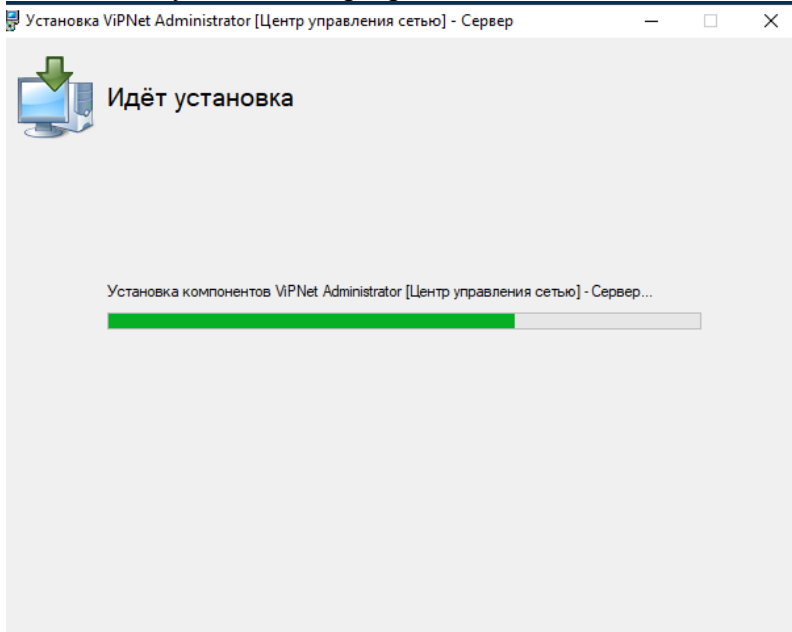
Нажимаем Установить сейчас



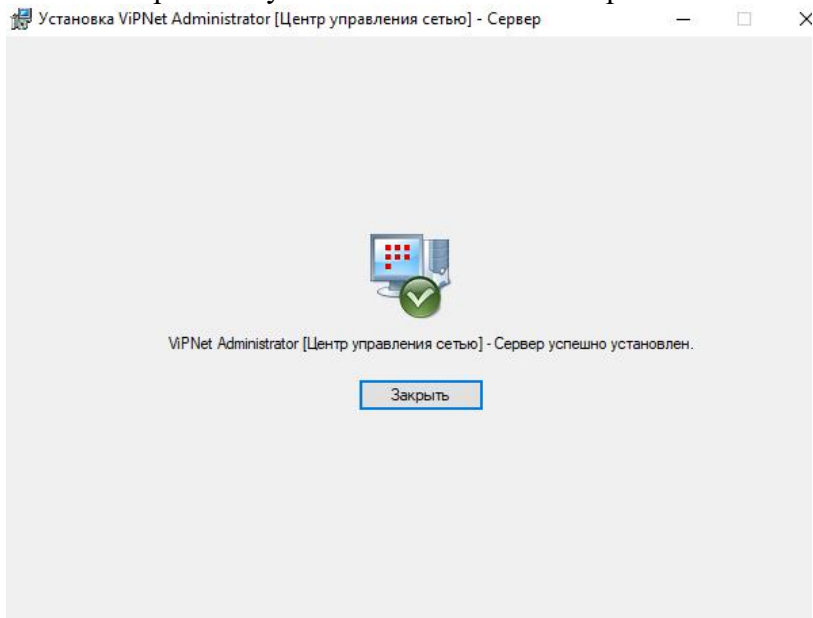
!!!При появлении данного окна, Нажимаем Закрывать. Ждём пока запуститься База Данных и снова жмём Установить сейчас



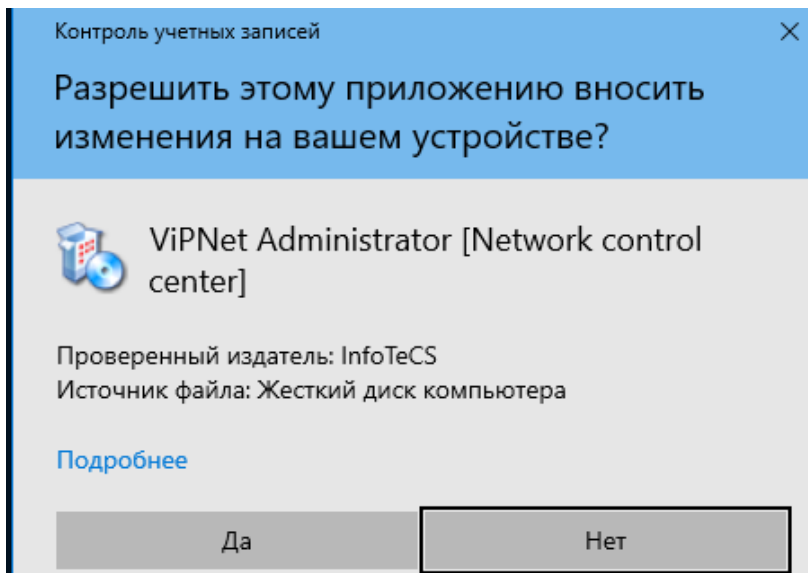
Начинается установка серверной части ЦУС



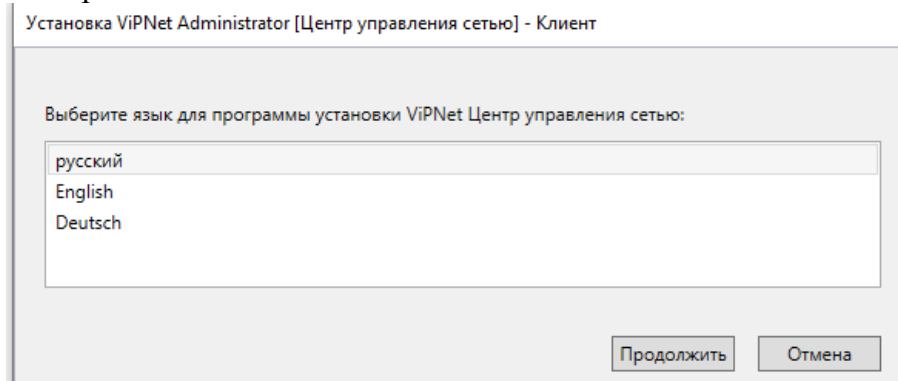
После завершения установки нажимаем Закреть



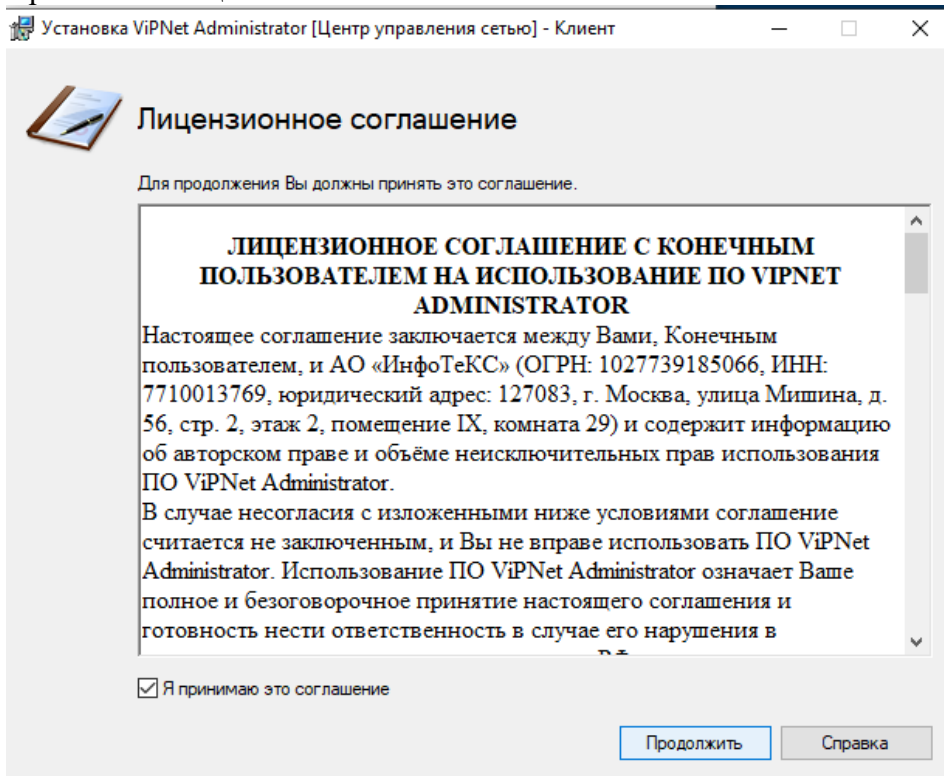
Возвращаемся в папку VIPNet Administrator 4.6.9\Центр управление сетью\
Но теперь устанавливаем Клиентскую часть (Client Install)
Нажимаем Setup.exe
Разрешаем вносить изменение



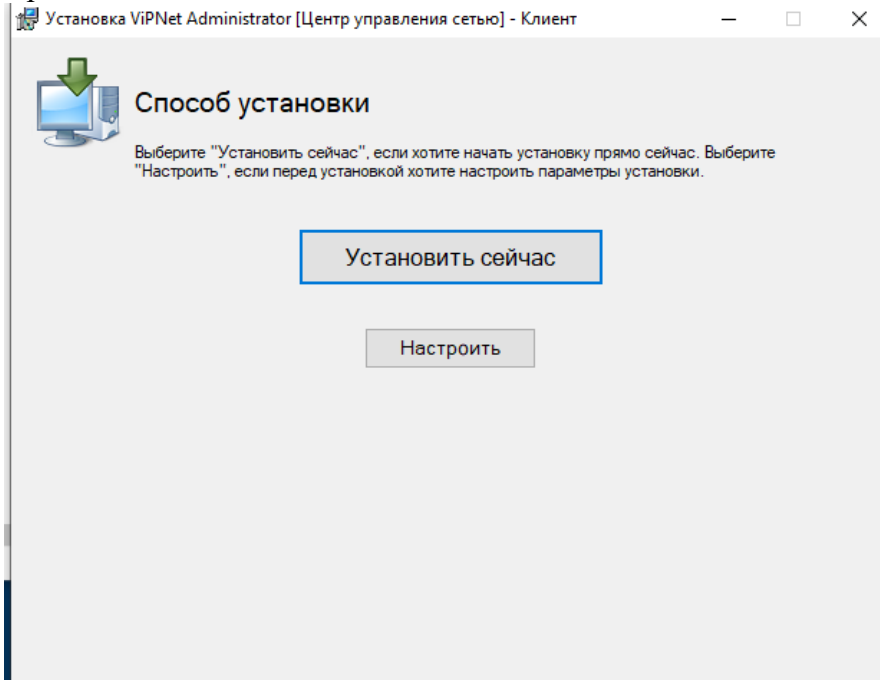
Выбираем язык



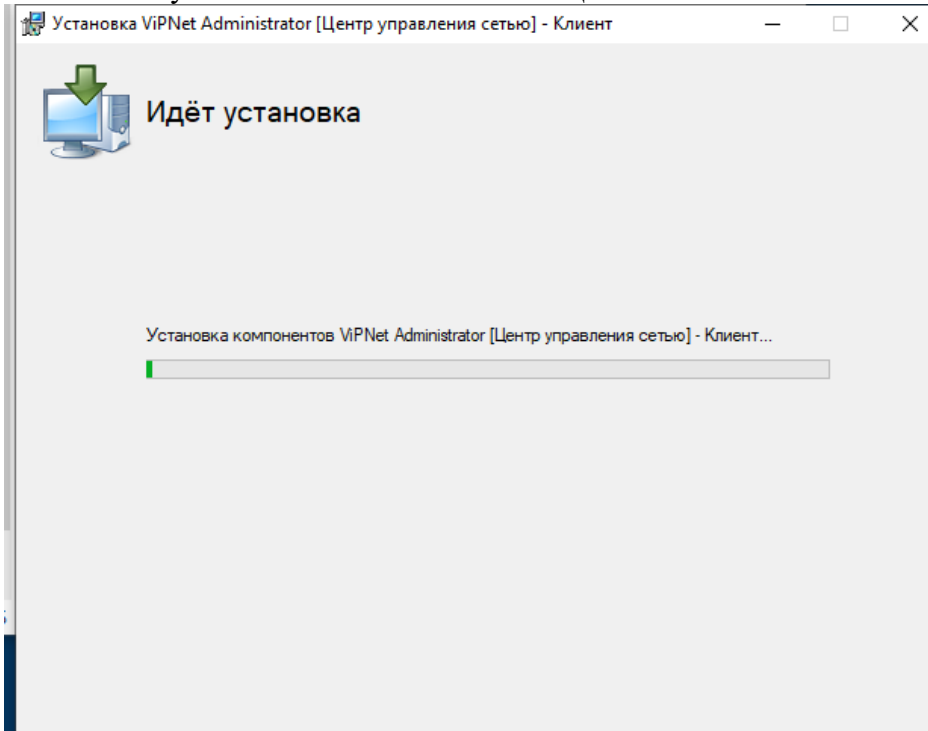
Принимаем лицензионное соглашение



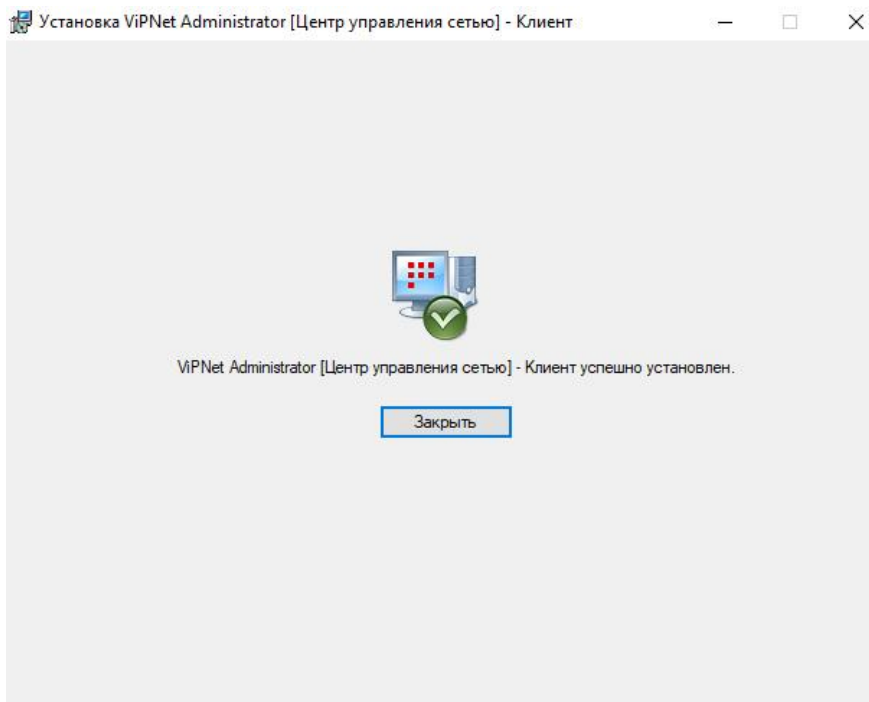
Просто нажимаем Установить сейчас



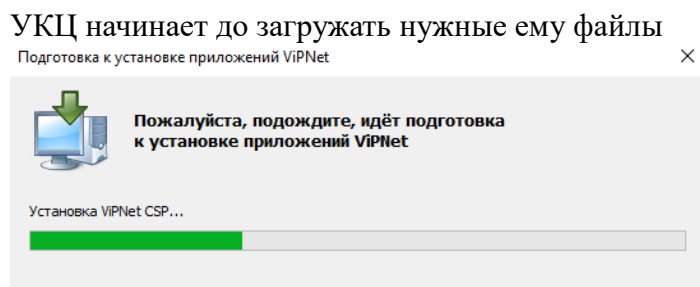
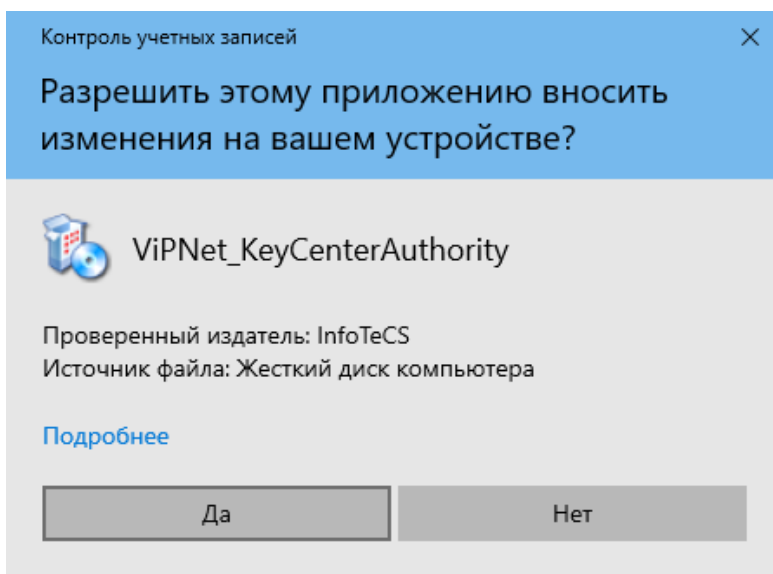
Начинается установка клиентской части ЦУС



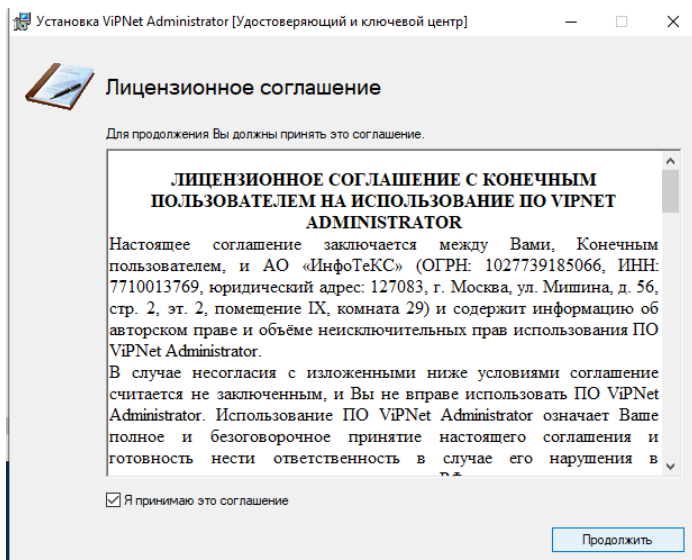
По завершению установки клиентской части нажимаем Закреть



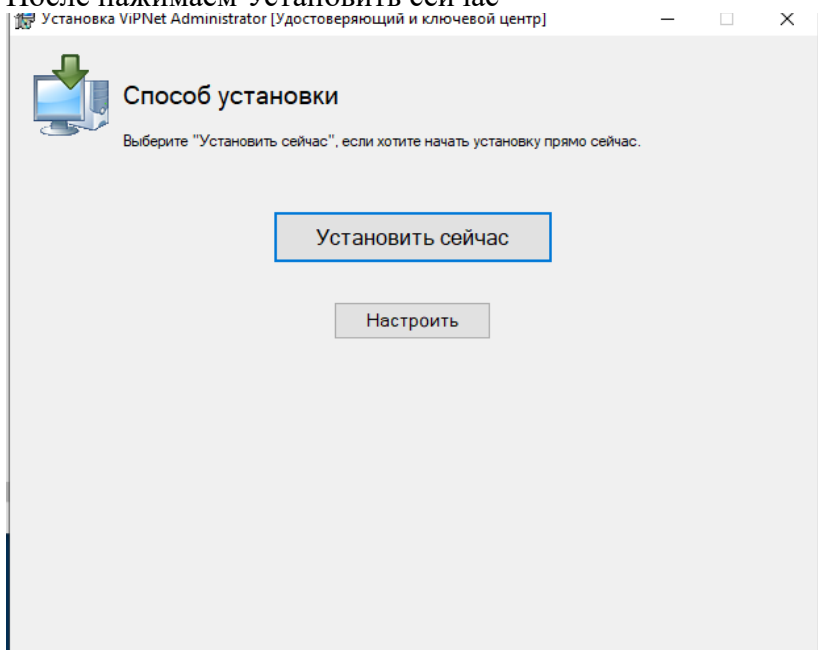
Возвращаемся в папку ViPNet Administrator 4.6.9 заходим в Удостоверяющий и Ключевой Центр (УКЦ). Тут только Setup.exe Запускаем его и разрешаем вносить изменения



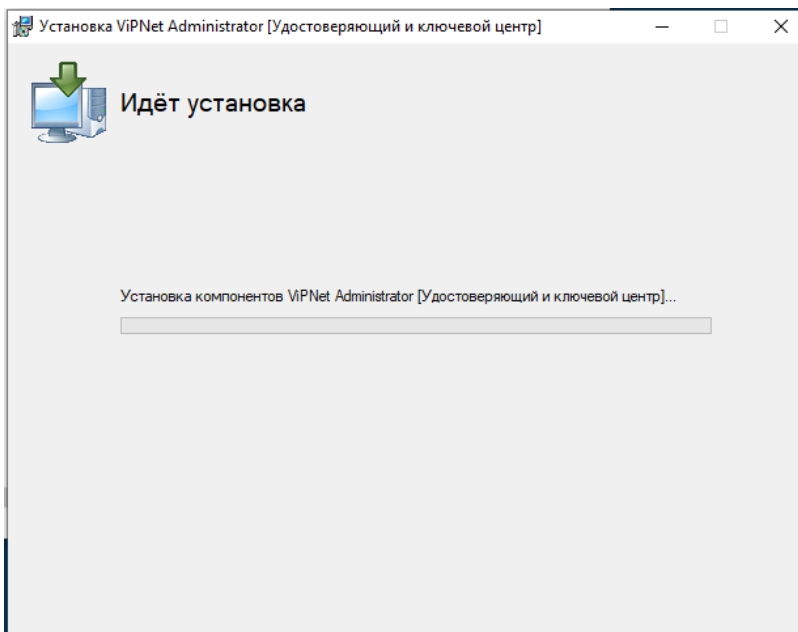
Принимаем лицензионное соглашение



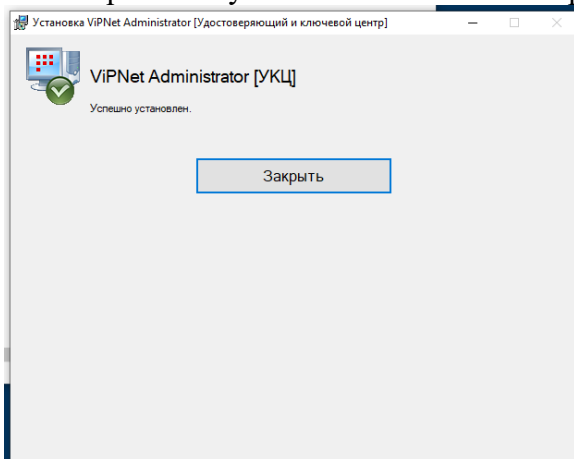
После нажимаем Установить сейчас



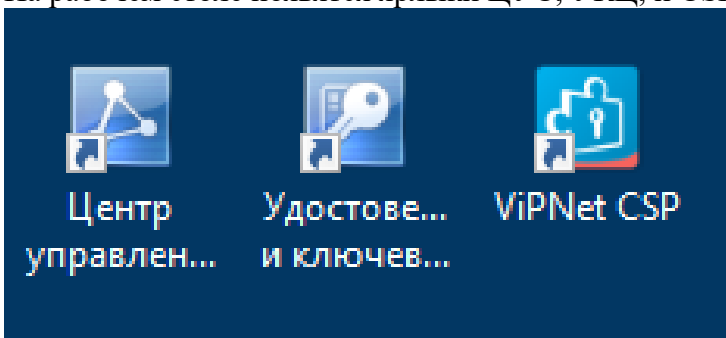
Он начинает установку УКЦ



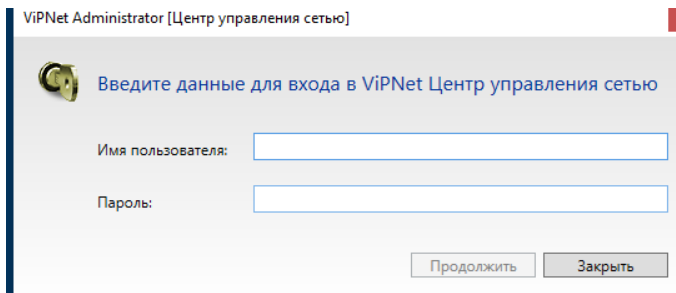
По завершению установки нажимаем **Закреть**



На рабочем столе появятся ярлыки ЦУС, УКЦ, и CSP

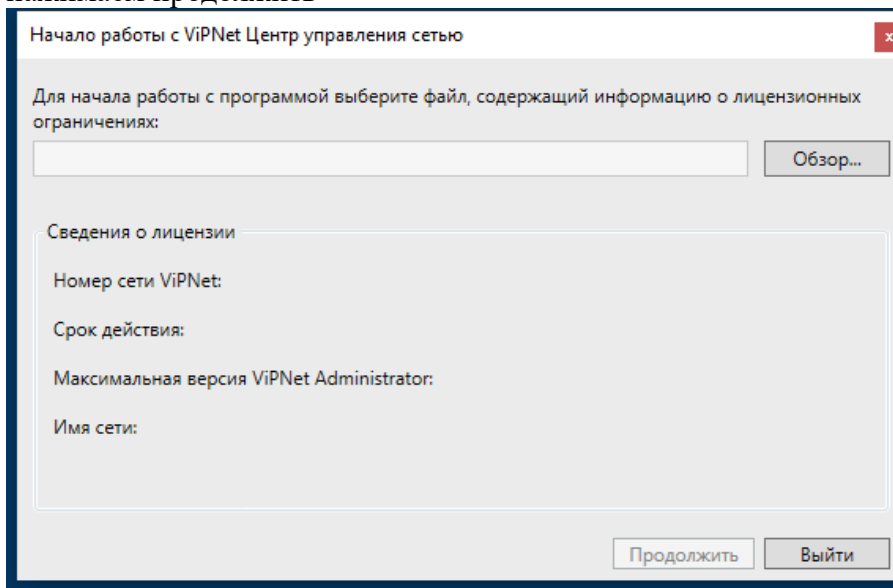


Запускаем ЦУС. В появившемся окне вводим данные. В первый раз по умолчанию стоит Administrator|Administrator

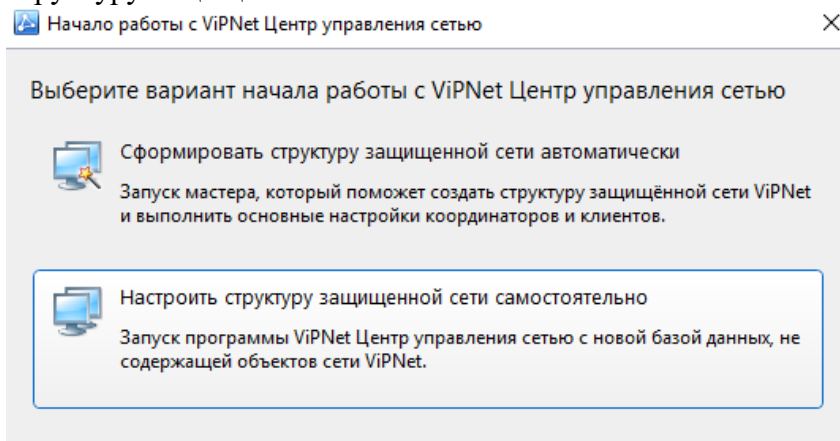


После ввода данных он попросит поменять пароль. Новый пароль будет восемь единиц (11111111)

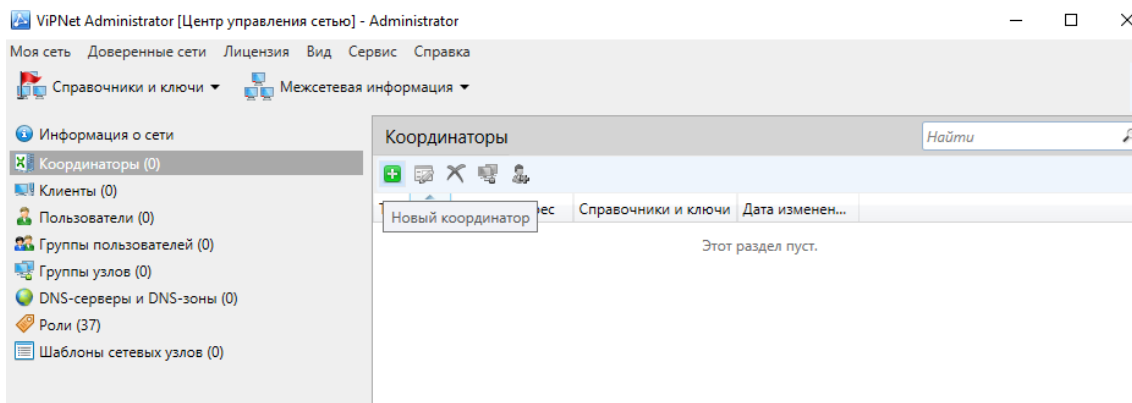
Затем ему нужны лицензия для запуска ЦУС. Нажимаем обзор и прикрепляем лицензию и нажимаем продолжить



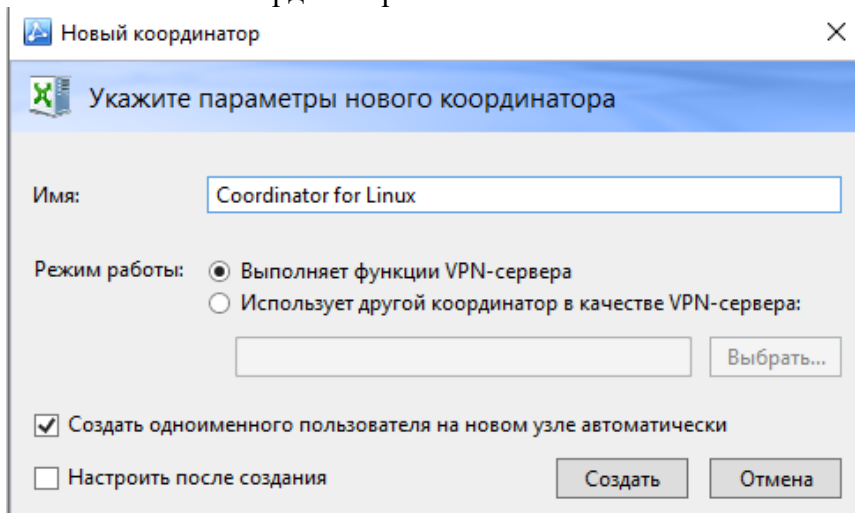
При первом запуске появится окно с началом работы в ViPNet. Нажимаем пункт Настроить структуру защищенной сети самостоятельно



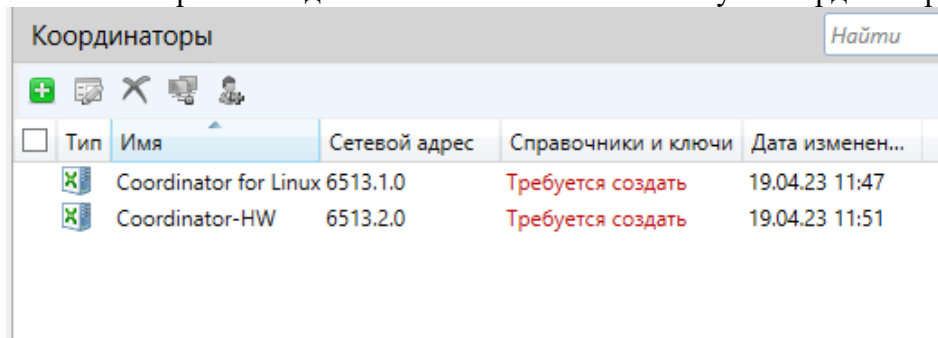
В данном окне нажимаем на пункт Координаторы и затем нажимаем на Плюс



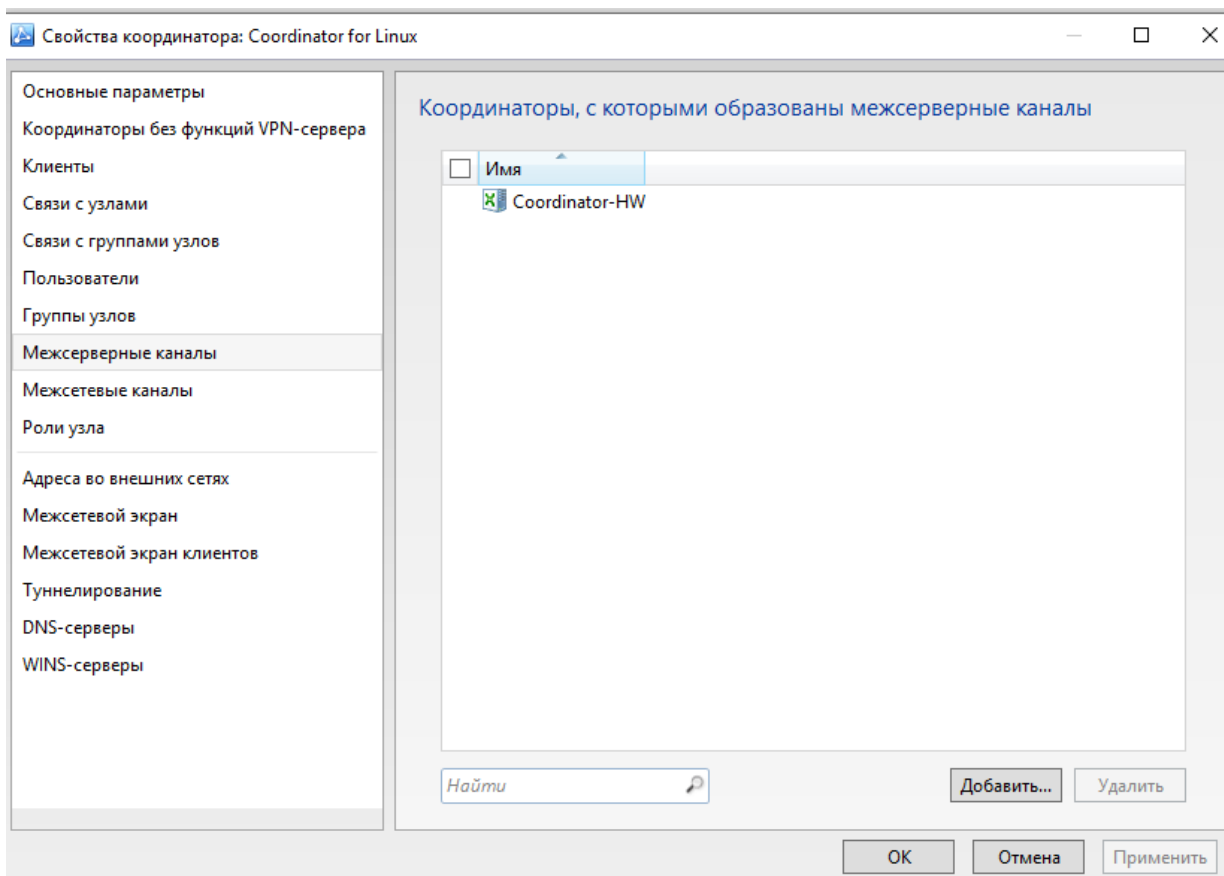
Указываем имя Координатора Coordinator for Linux и нажимаем создать



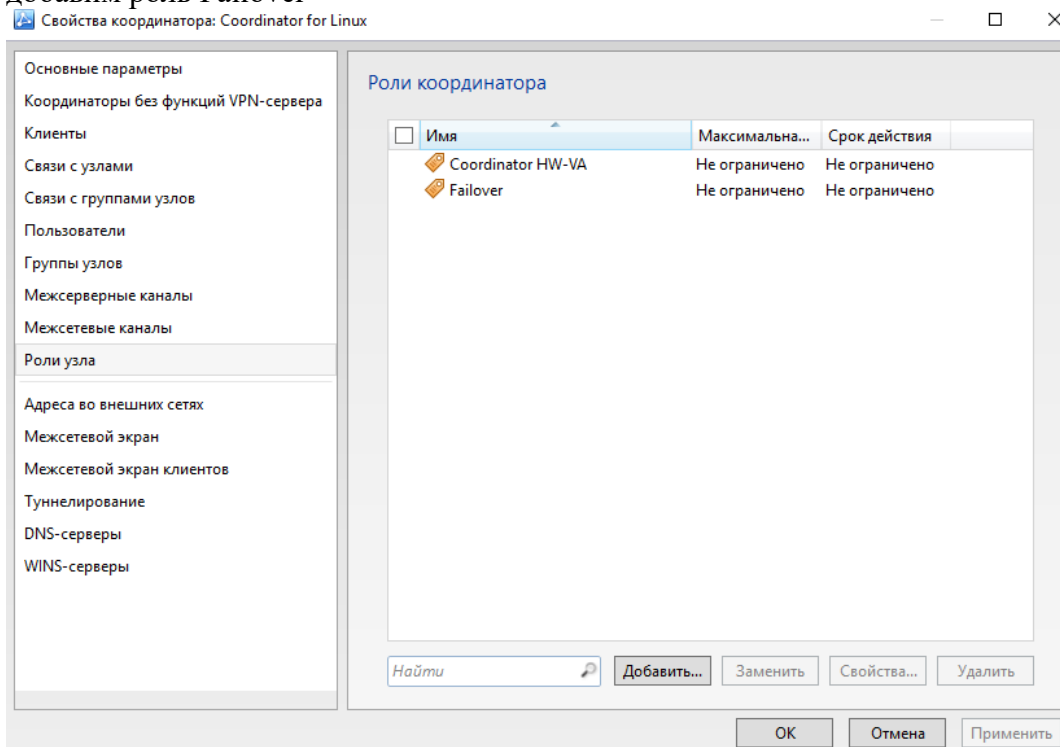
Таким же образом создаем Coordinator-HW. По итогу 2 Координатора



Нажимаем 2 раза на Coordinator for Linux и переходим во вкладку межсерверные каналы и добавляем туда Coordinator-HW

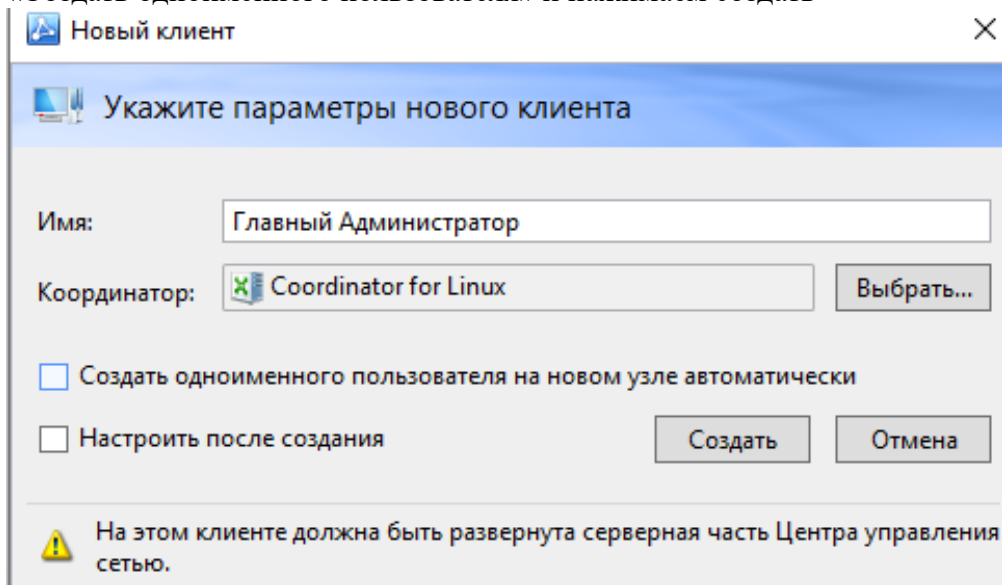


Далее переходим в роли узла и удаляем имеющиеся роли. После нажимаем добавить и выбираем роль Coordinator HW-VA. Нажимаем Добавить. Затем еще раз нажмем добавить и добавим роль Failover

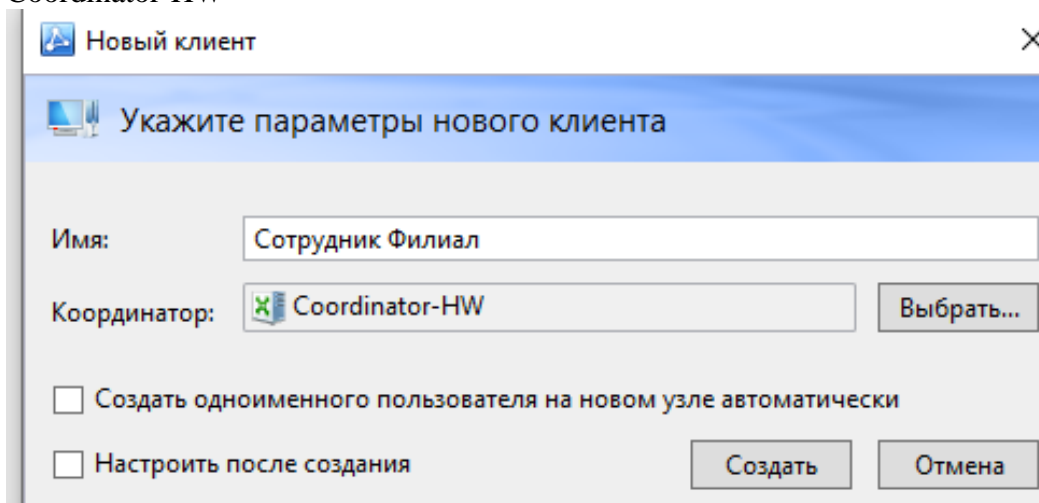


На Coordinator-HW даем такие же роли

После выдачи роли на координаторы, нажимаем на пункт клиенты и создаем Главного Администратора и выбираем координатор Coordinator for Linux. Надо убрать галочку «Создать одноименного пользователя» и нажимаем создать



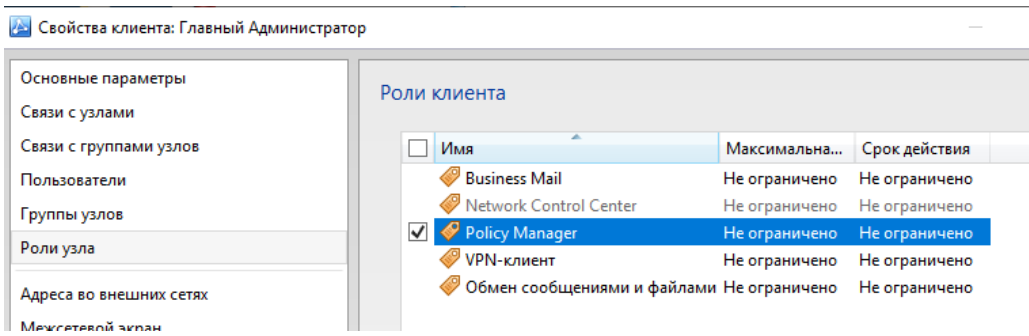
Таким же образом создаем Помощника главного админа с таким же координатором После Помощника главного админа создаем Сотрудника Филиал, но ему ставим координатор Coordinator-HW



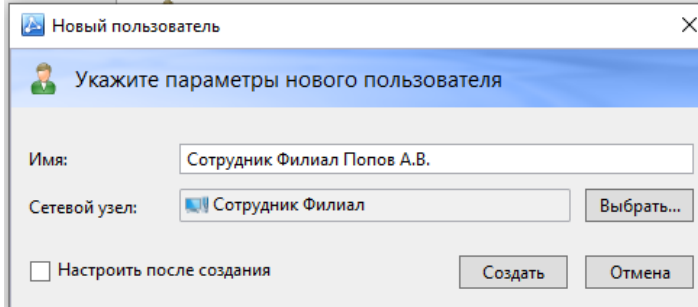
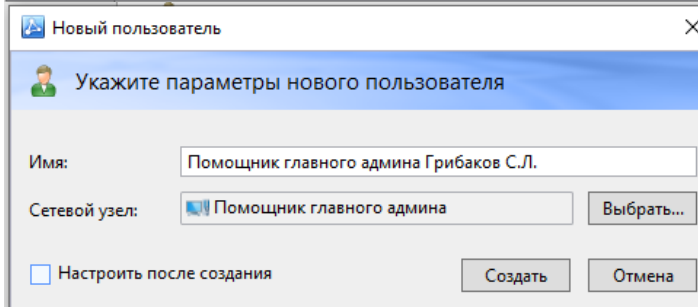
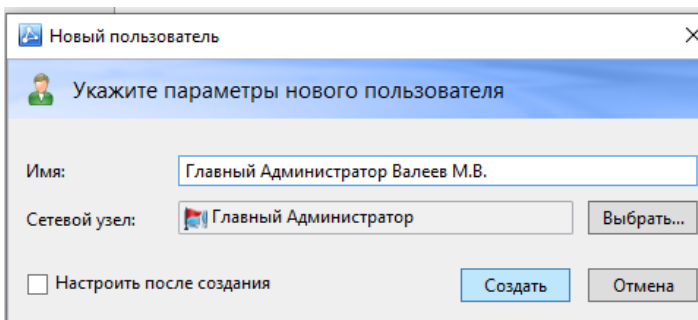
Должно получиться так

Имя	Сетевой адрес	Координатор	Дата изменен...	Справочники и кл...
<input type="checkbox"/> Главный Администратор	6513.1.1	Coordinator for Linux	19.04.23 12:03	Требуется создать
<input type="checkbox"/> Помощник главного админа	6513.1.2	Coordinator for Linux	19.04.23 12:04	Требуется создать
<input type="checkbox"/> Сотрудник Филиал	6513.2.1	Coordinator-HW	19.04.23 12:06	Требуется создать

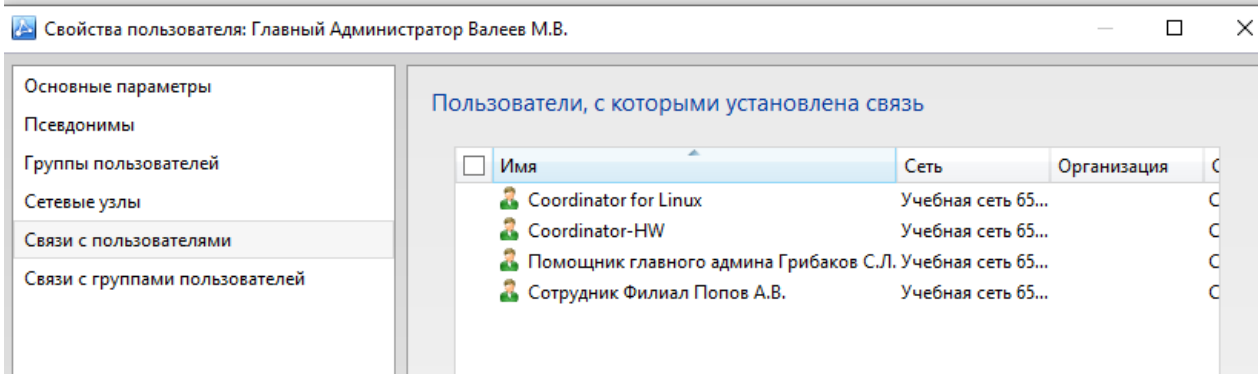
Нажимаем 2 раза на Главного Администратора и выдаем ему роль Police Manager



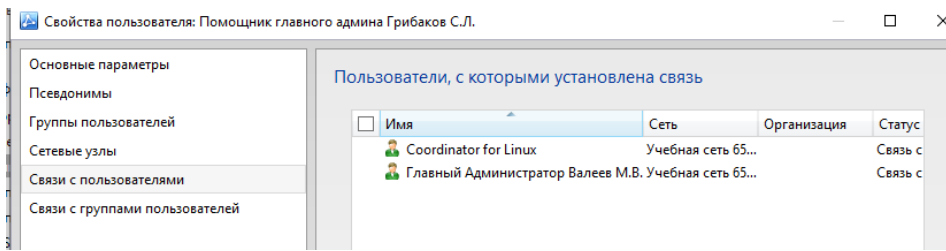
После создания клиентов нажимаем на пункт пользователи и создаем пользователей Главный Администратор Валеев М.В.; Помощник главного админа Грибаков С.Л.; Сотрудник Филиал Попов А.В.



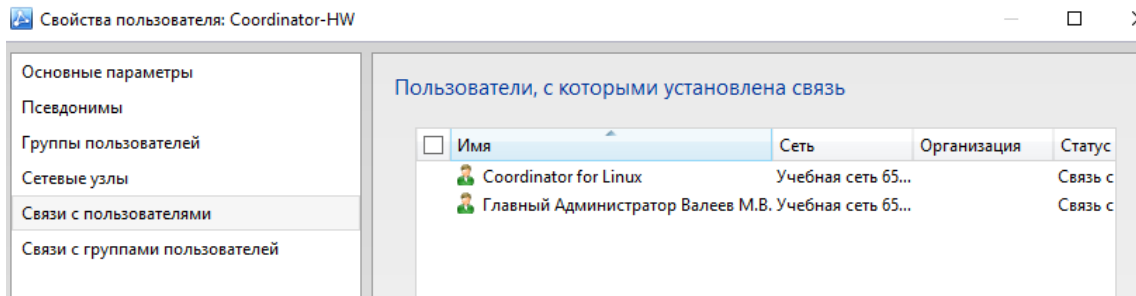
Заходим в Главного Администратора Валеев М.В. и переходим в Связи с пользователями и добавляем связи со всеми узлами



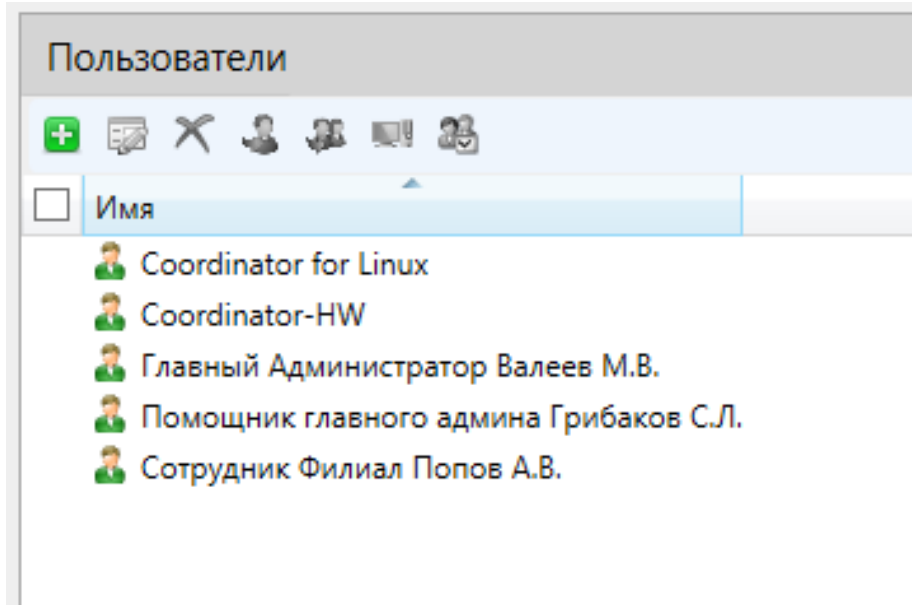
Помощнику главного админа Грибакова С.Л. добавляем связь с Coordinator for Linux



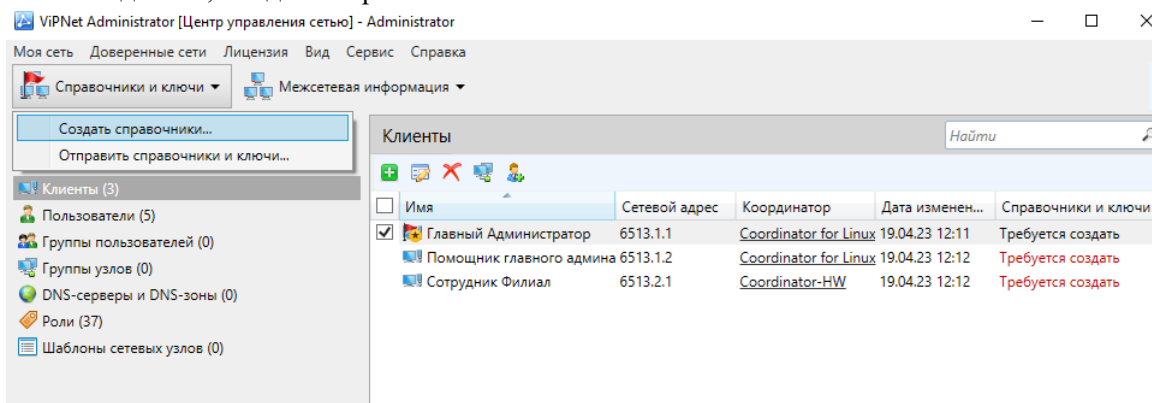
Coordinator for Linux добавляем связь с Coordinator-HW



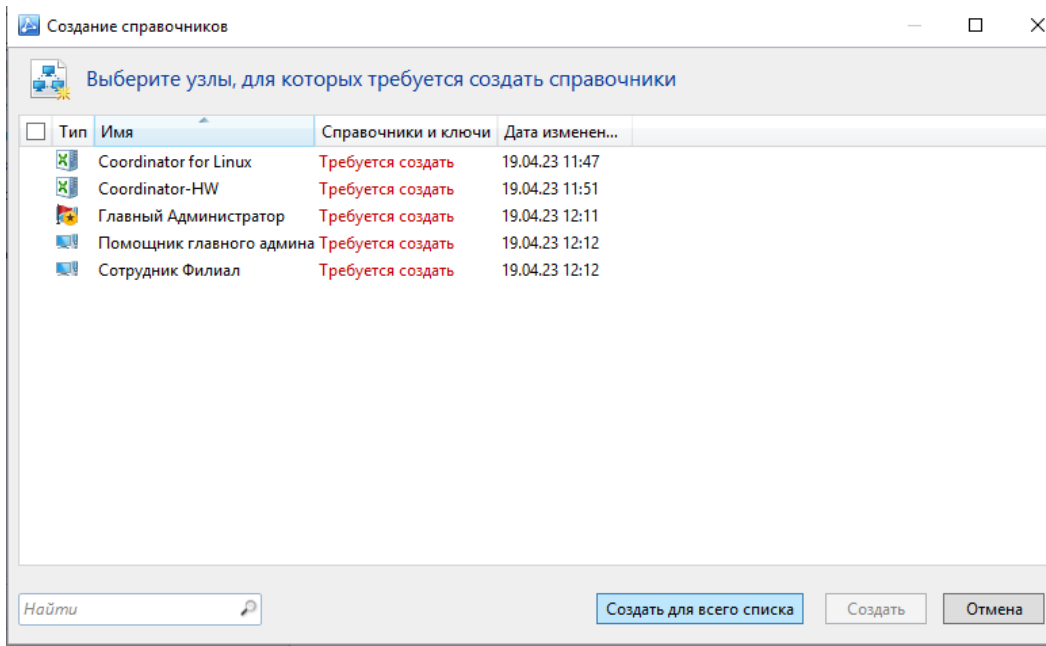
Весь список пользователей выглядит так



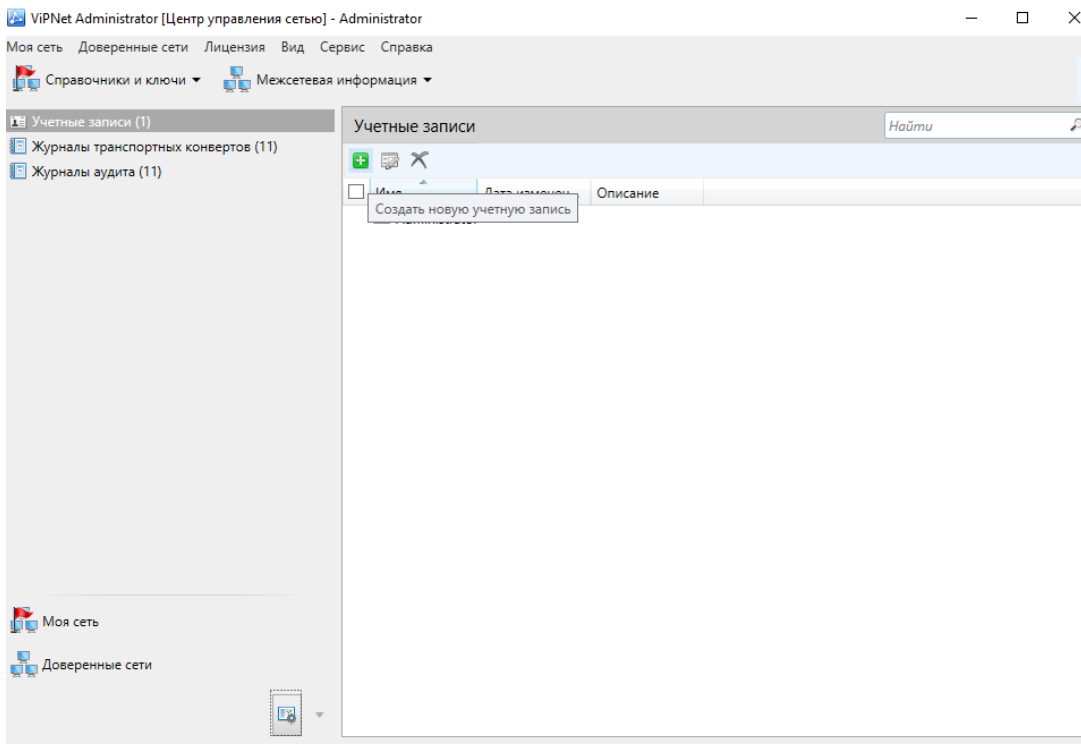
Как все сделали, Создаем справочники



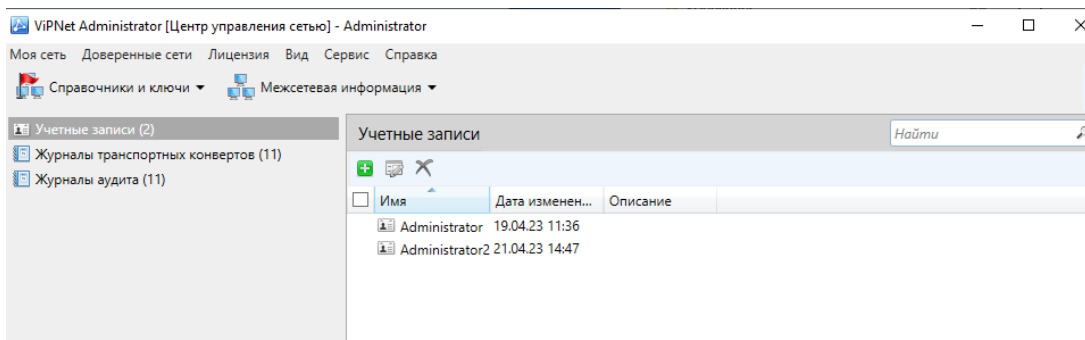
Нажимаем создать для всего списка



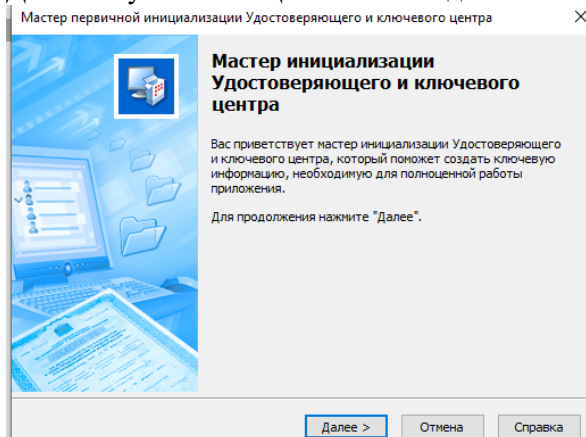
Нажимаем на кнопку Администрирование и создаем учетную запись для Помощника главного админа



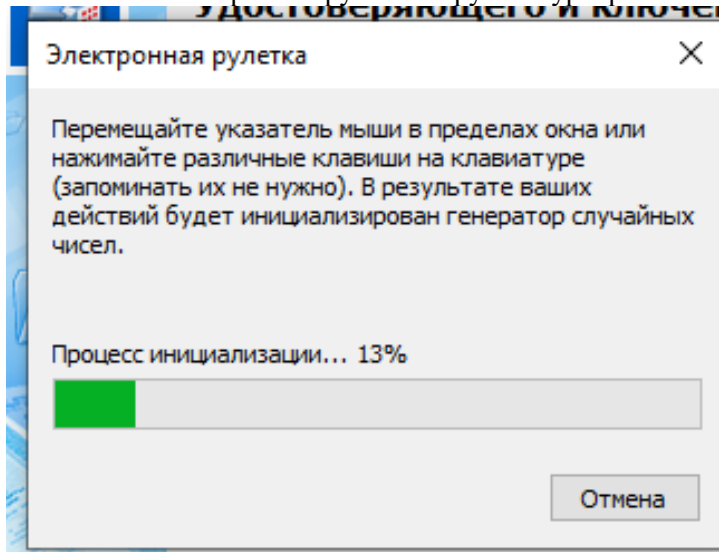
В появившемся окне вводим имя пользователя и вводим пароль. После создания учетной записи будет вот так



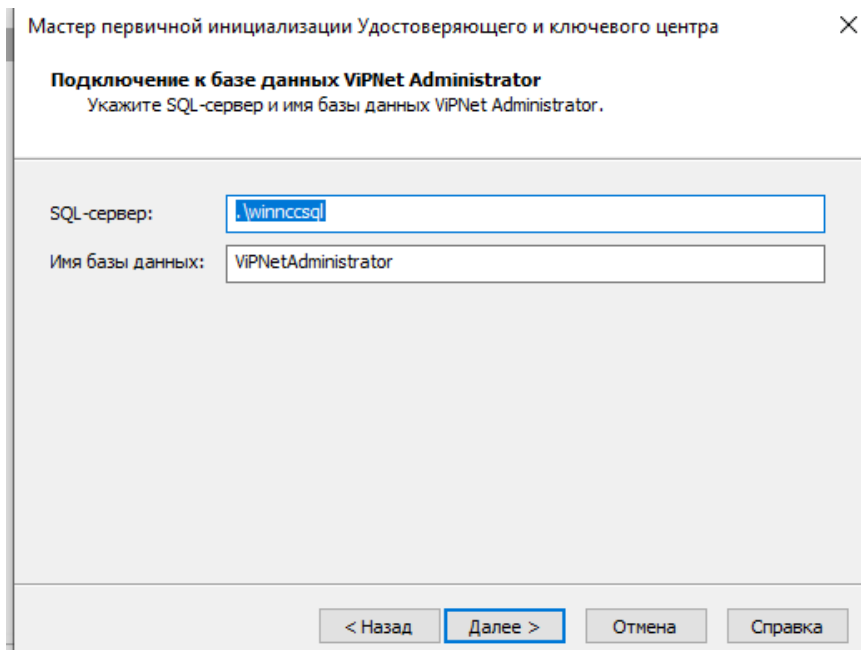
Далее запускаем УКЦ и нажимаем далее



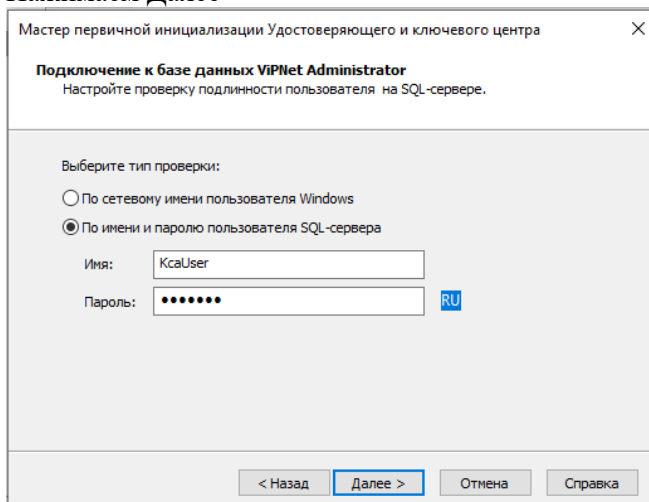
Появляется Электронная рулетка. Крутим курсором мыши в этом окошке



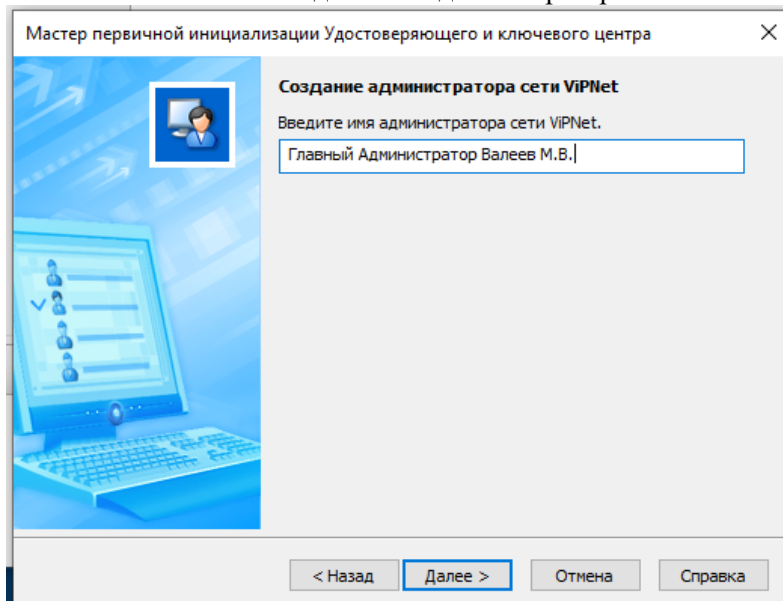
После того как закончится рулетка, ничего не меняя нажимаем далее



Нажимаем Далее



В появившемся окне вводим имя администратора сети VIPNet



Далее заполняем сведения (по желанию)

Мастер первичной инициализации Удостоверяющего и ключевого центра

Сведения о владельце сертификата
Заполните сведения о юридическом лице.

Наименование:

ОГРН:

ИНН ЮЛ:

Уполномоченный представитель юридического лица:

Фамилия:

Приобретенное имя:

СНИЛС:

Электронная почта:

< Назад **Далее >** Отмена Справка

Нажимаем Далее

Мастер первичной инициализации Удостоверяющего и ключевого центра

Сведения о владельце сертификата
Заполните сведения о юридическом лице.

Организация:

Уполномоченный представитель юридического лица:

Подразделение:

Должность:

< Назад **Далее >** Отмена Справка

Нажимаем Далее

Мастер первичной инициализации Удостоверяющего и ключевого центра

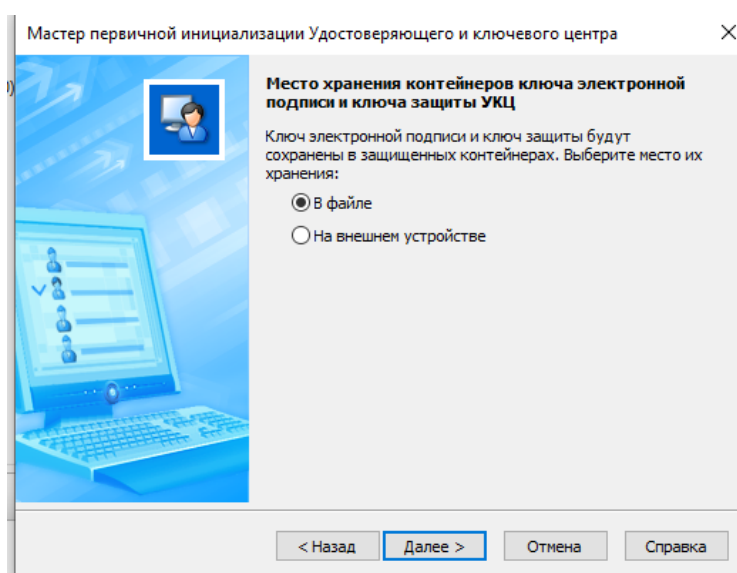
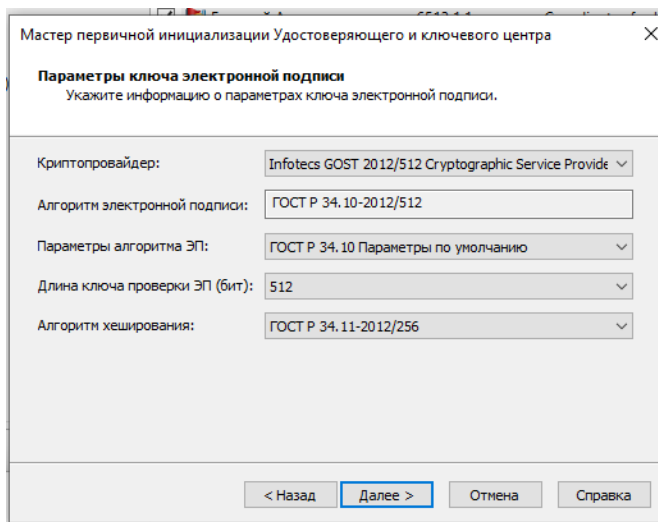
Дополнительные сведения о владельце сертификата
Заполните сведения о юридическом лице.

Атрибуты	Значения
Инициалы	
Серийный номер	
Псевдоним	
Неструктурированное имя	
Компонента доменного имени	
Неструктурированный адрес	
Телефон	
Департамент	
Описание	
Почтовый индекс	

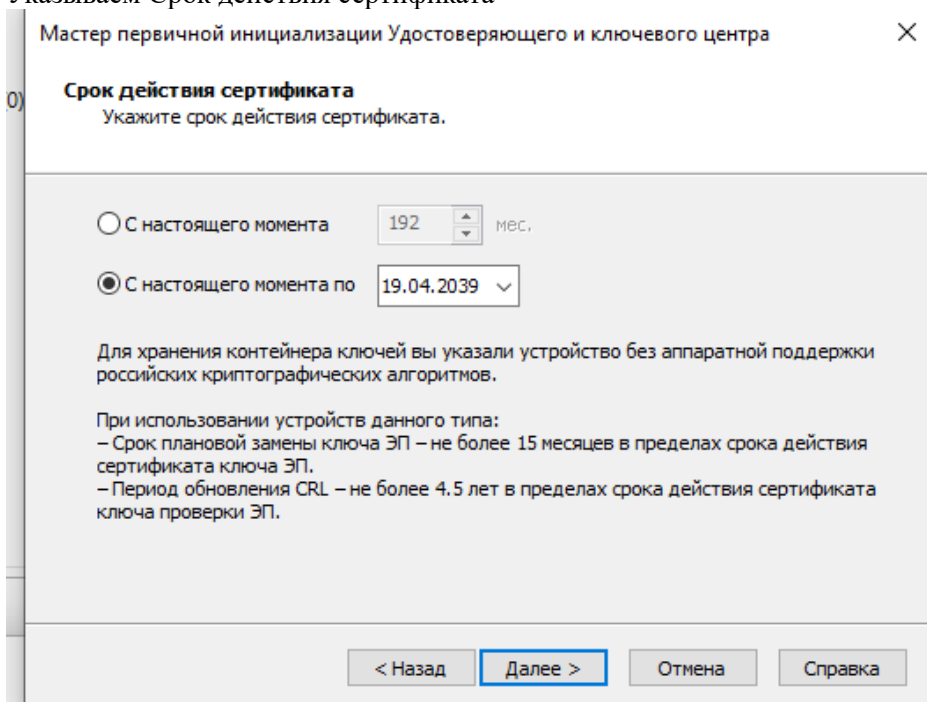
Изменить

< Назад **Далее >** Отмена Справка

Указываем параметры ключа электронной подписи и ставим сохранение в файле



Указываем Срок действия сертификата



Нажимаем Далее

Мастер первичной инициализации Удостоверяющего и ключевого центра

Сведения о точках распространения

Укажите данные о точках распространения, которые Удостоверяющий центр будет помещать в издаваемые сертификаты пользователей.

Сервер	Сетевой путь

Впоследствии данную информацию можно изменить в окне настроек.

Мастер первичной инициализации Удостоверяющего и ключевого центра

Программные средства

Укажите информацию о средствах удостоверяющего центра и средстве электронной подписи владельцев сертификатов.

Функционировать в режиме аккредитованного удостоверяющего центра

Средства удостоверяющего центра:

Средство электронной подписи владельцев сертификатов:

Данная информация будет добавляться в издаваемые квалифицированные сертификаты.

Впоследствии данную информацию можно изменить в окне настроек.

Выставляем время бездействия на 30 минут

Мастер первичной инициализации Удостоверяющего и ключевого центра

Автоматический режим работы

Настройте параметры автоматического режима.

Переходить в автоматический режим работы, если администратор не совершает никаких действий в программе

Время бездействия администратора: минут

Впоследствии данные настройки можно изменить в окне настроек.

Нажимаем на Создать ключи узлов, настроить, создавать ключи при получении запроса из ЦУС и нажимаем Далее

Параметры действия в автоматическом режиме

Создавать ключи узлов:

Каждые час.

Каждый день в

При получении запроса из Центра управления сетью

После создания ключи узлов будут переданы на узлы через Центр управления сетью.

Мастер первичной инициализации Удостоверяющего и ключевого центра

Автоматический режим работы

Настройте параметры операций, которые должны выполняться в автоматическом режиме.

Ключи узлов

Создавать ключи узлов
Выполняется

Запросы

Удовлетворять запросы на сертификаты из центров регистрации
Не выполняется

Удовлетворять запросы на сертификаты от пользователей
Не выполняется

Удовлетворять запросы на аннулирование сертификатов
Не выполняется

Удовлетворять запросы на дистрибутивы ключей

Выставляем собственный пароль и ставим пароль. В данном случае будет 8мь единиц (11111111)

Мастер первичной инициализации Удостоверяющего и ключевого центра

Пароль администратора сети VIPNet
Пароль будет использован администратором сети VIPNet для входа в Удостоверяющий и ключевой центр.

Введите пароль:
●●●●●● RU

Введите пароль еще раз для подтверждения:
●●●●●●

< Назад **Далее >** Отмена Справка

Нажимаем Далее

Мастер первичной инициализации Удостоверяющего и ключевого центра

Все готово к первичной инициализации Удостоверяющего и ключевого центра

Субъект
Обычное имя: Главный Администратор Валеев М.В.
Организация: Учебная сеть 6513
Подразделение: Удостоверяющий и ключевой центр
Должность: Администратор

Срок действия
С 19.04.2023 12:38 по 19.04.2039 23:59

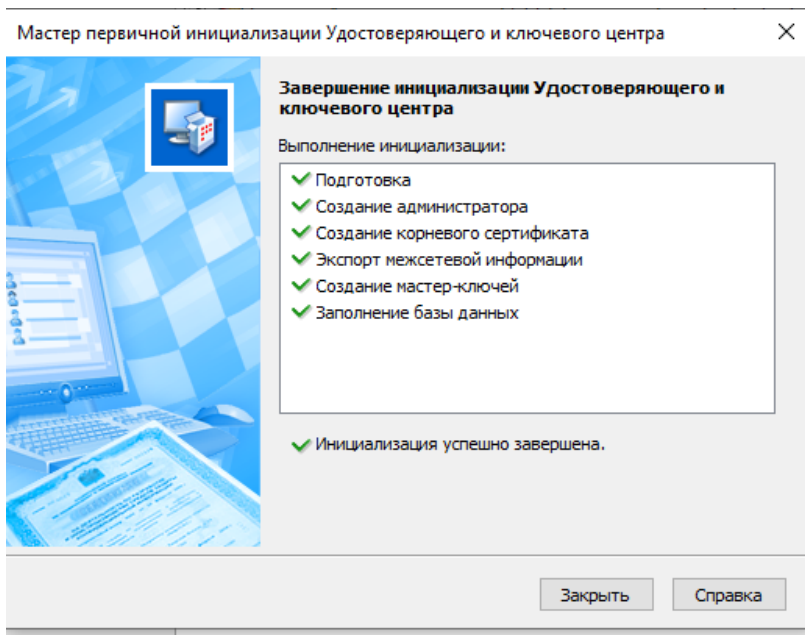
Ключ проверки электронной подписи
ГОСТ Р 34.10-2012 256

Контейнер ключей
Папка: C:\Users\Student\AppData\Roaming\InfoTeCS\VIPNet Administrator
Пароль: *****

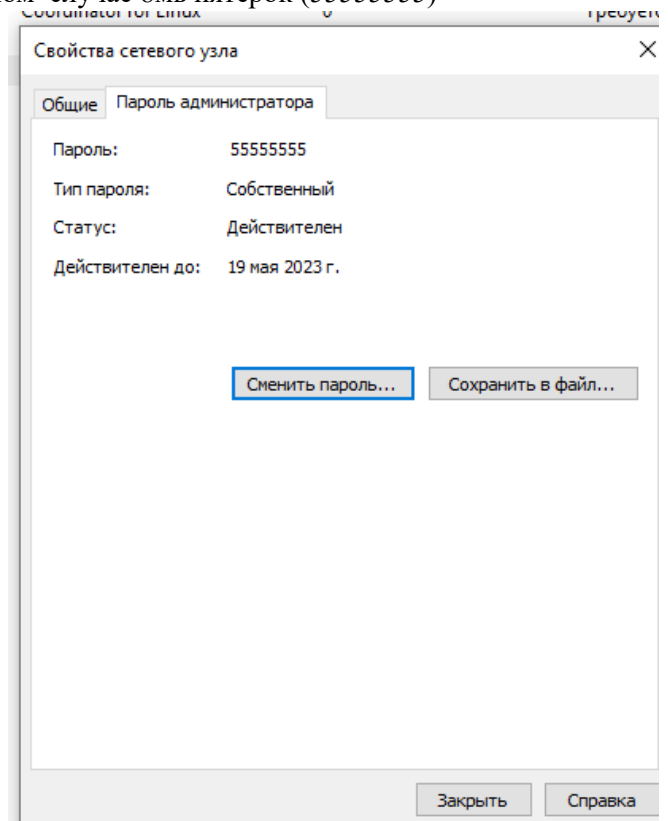
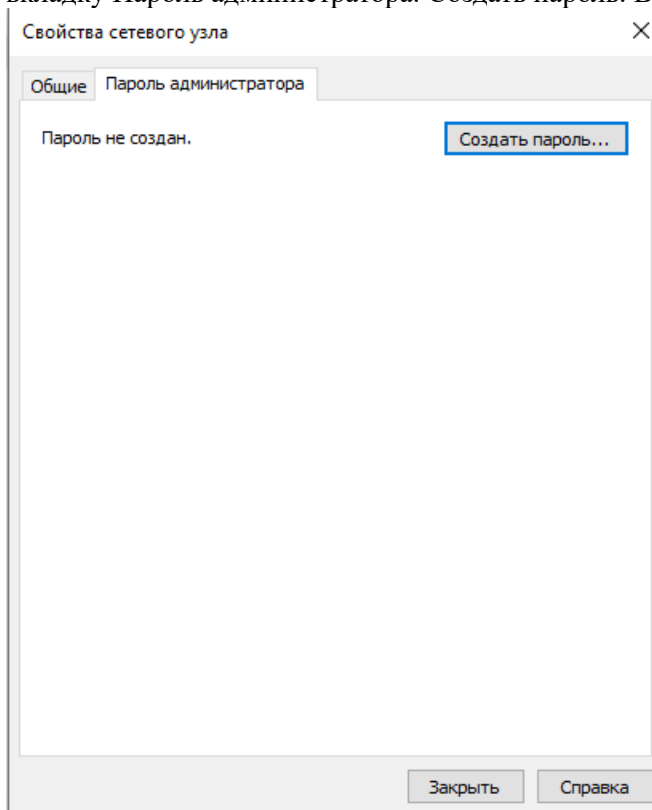
Печать

< Назад **Далее >** Отмена Справка

После завершения нажимаем закрыть

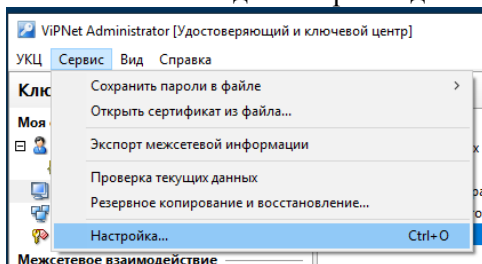


В появившемся окне нажать на пункт Сетевые узлы. Нажать 2 раза на Главного Администратора во вкладку Пароль администратора. Создать пароль. В данном случае 8мь пятёрок (55555555)

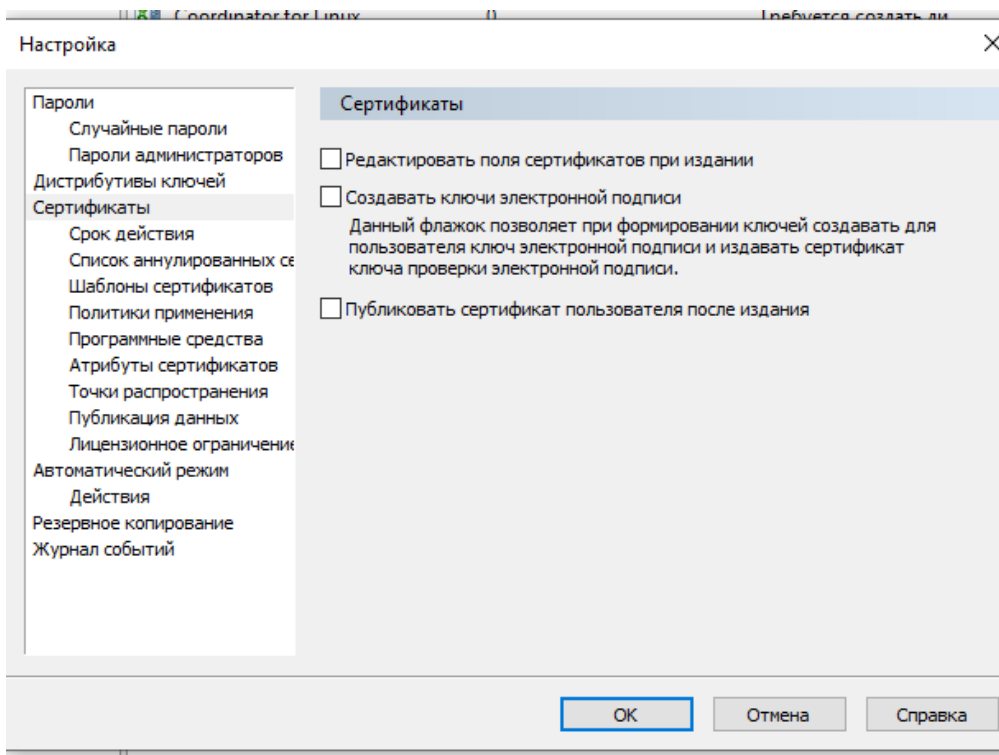


Сделать так с каждым сетевым узлом

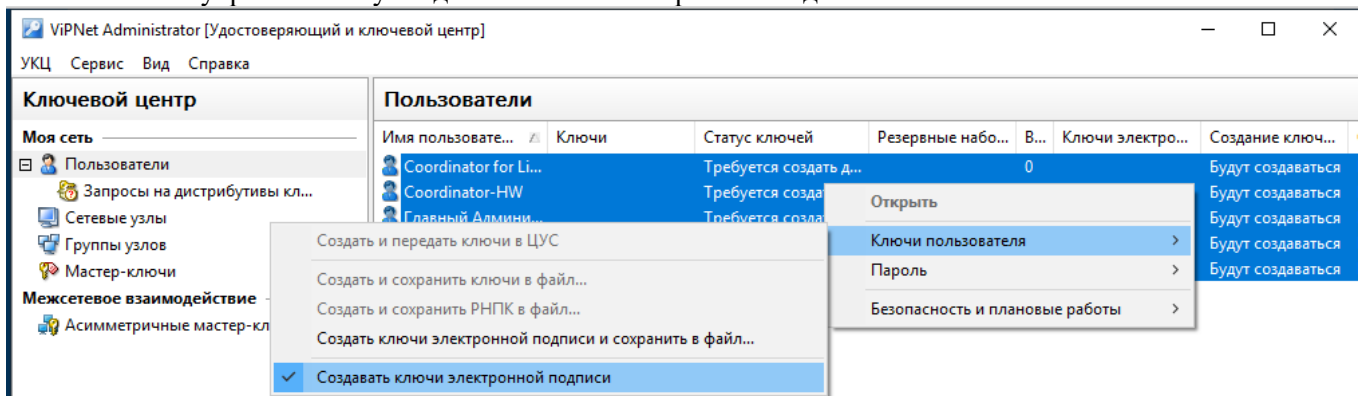
После того как выдали Пароль администратора нажимаем вкладку сверху Сервис→ Настройка



В пункте Сертификаты убрать галочки Редактировать поля и Создавать ключи электронной подписи

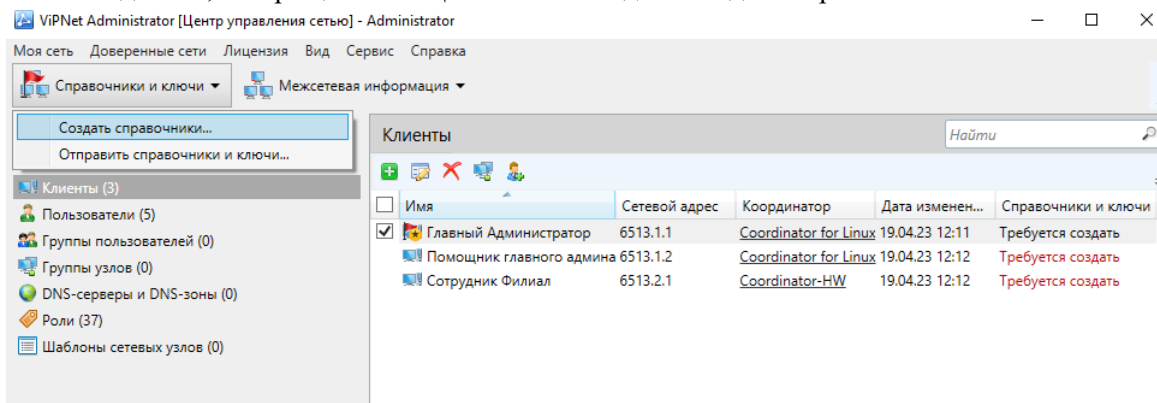


После нажимаем ОК и переходим в пункт пользователи, выделить всех, нажать ПКМ → Ключи пользователя и убрать галочку создавать ключи электронной подписи

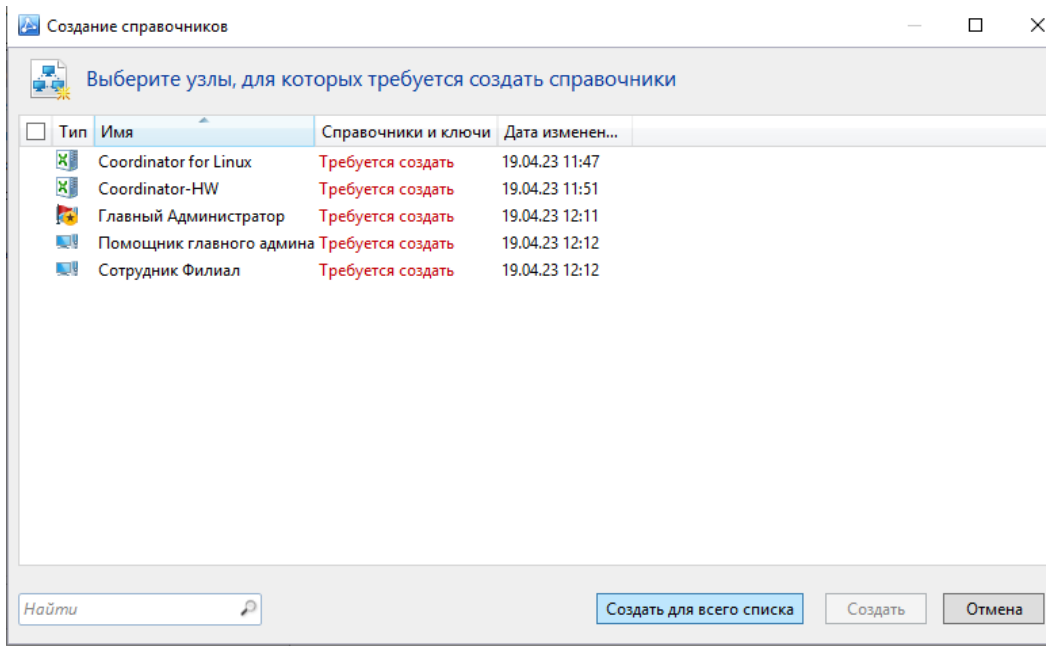


После чего выделим ТОЛЬКО Помощника главного админа и ему поставим галочку Создавать ключи электронной подписи

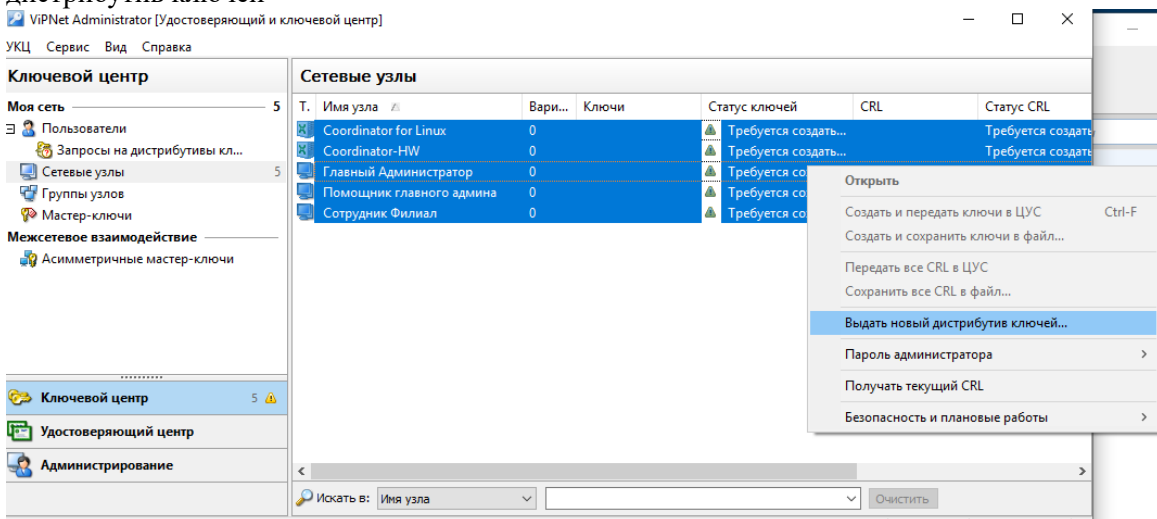
Как все сделали, возвращаемся в ЦУС что бы создать Создать справочники



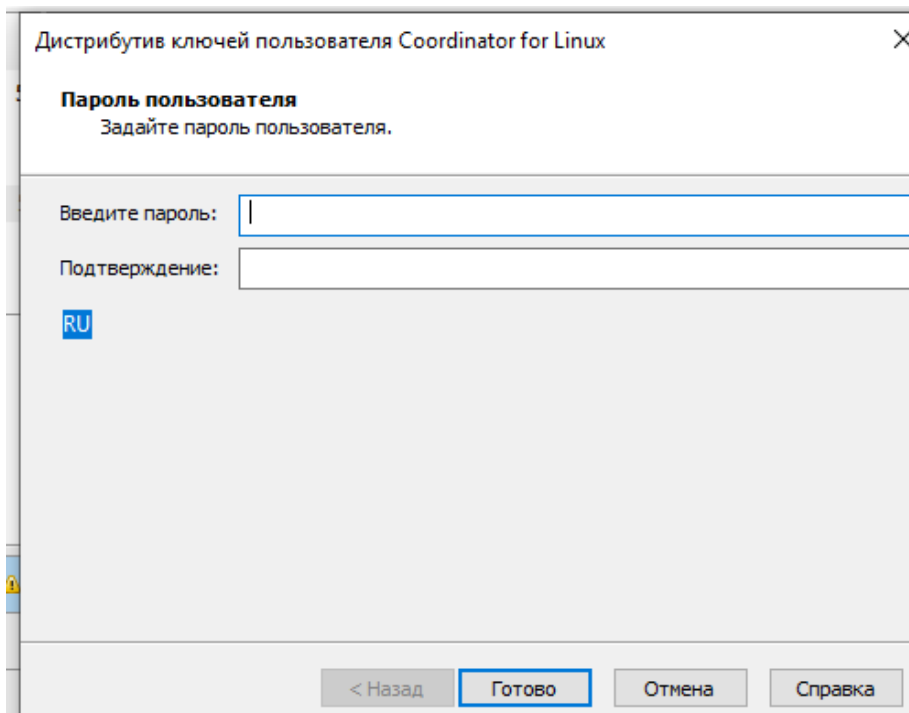
Нажимаем создать для всего списка



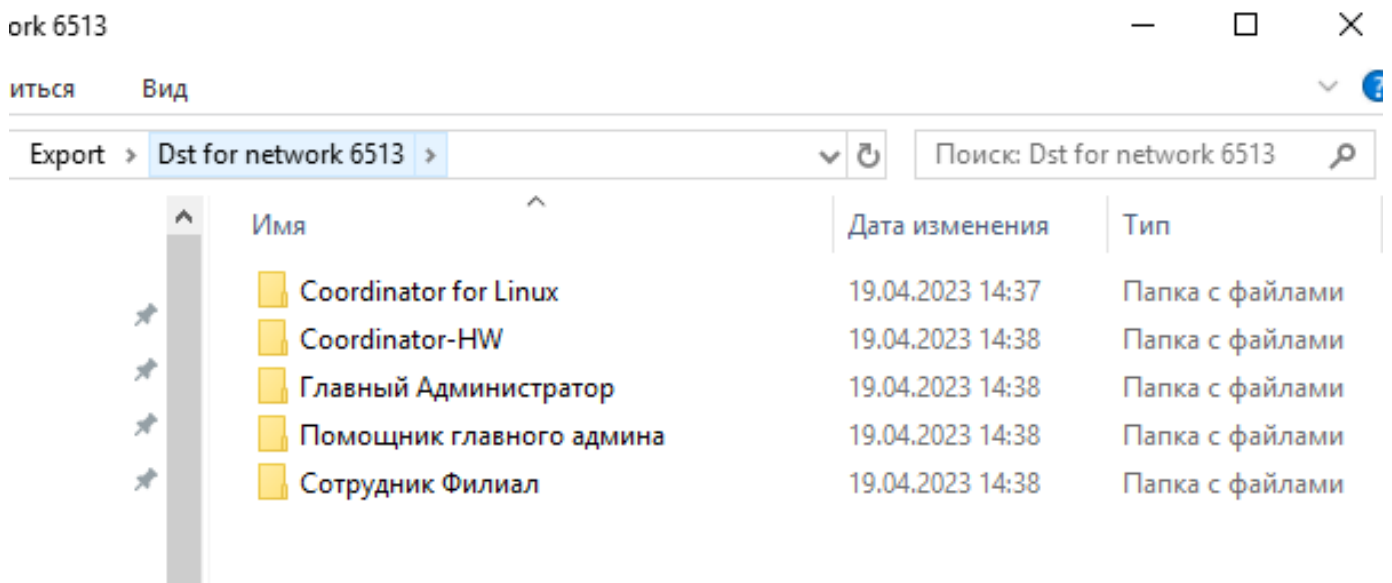
После этого возвращаемся в УКЦ, в пункте Сетевые узлы выделяем всех и выдаем новый дистрибутив ключей



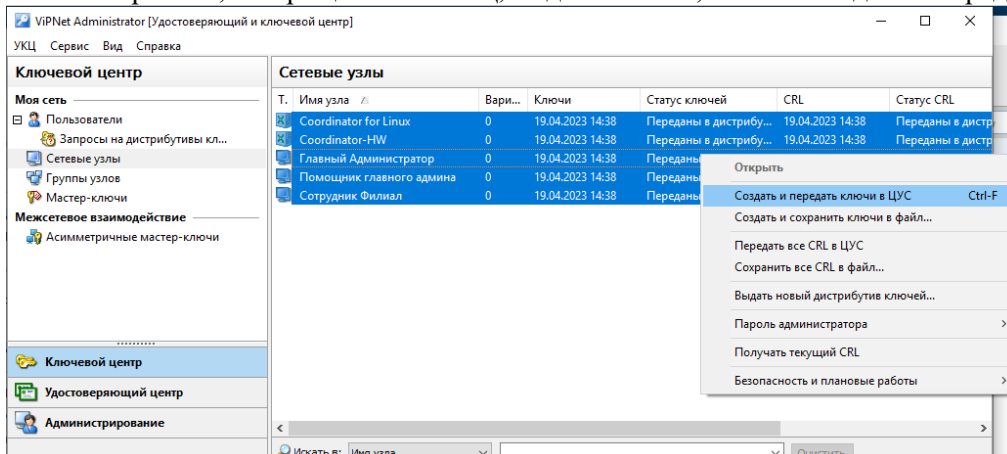
Выдаем пароль пользователя на сетевые узлы



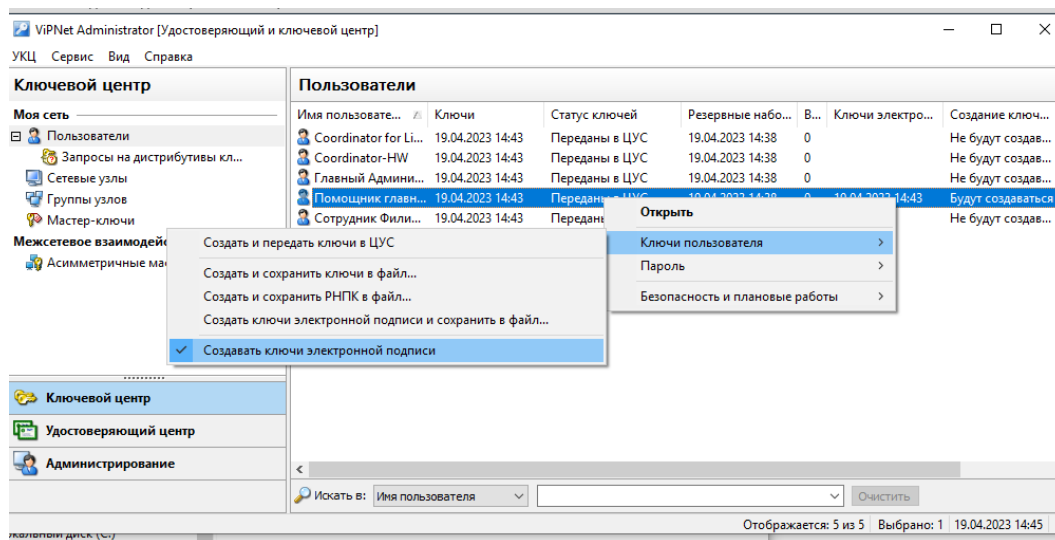
Как выдали пароль, копируем папку Dst for network 6513 в общую папку [trator \[Удостоверяющий и ключевой центр\]](#)



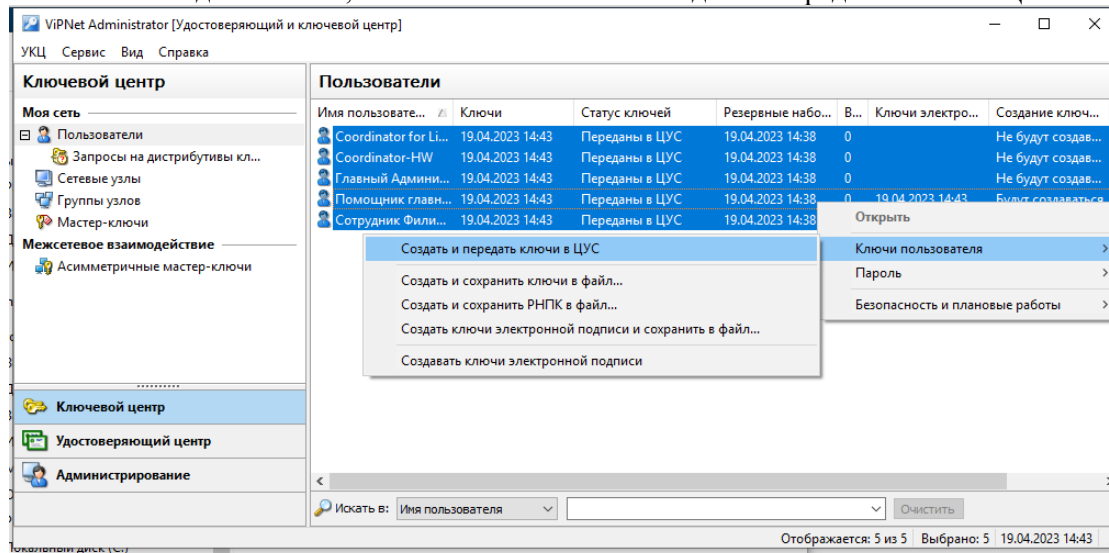
Как скопировали, возвращаемся в УКЦ, выделяем всех, ПКМ и Создать и передать ключи в ЦУС



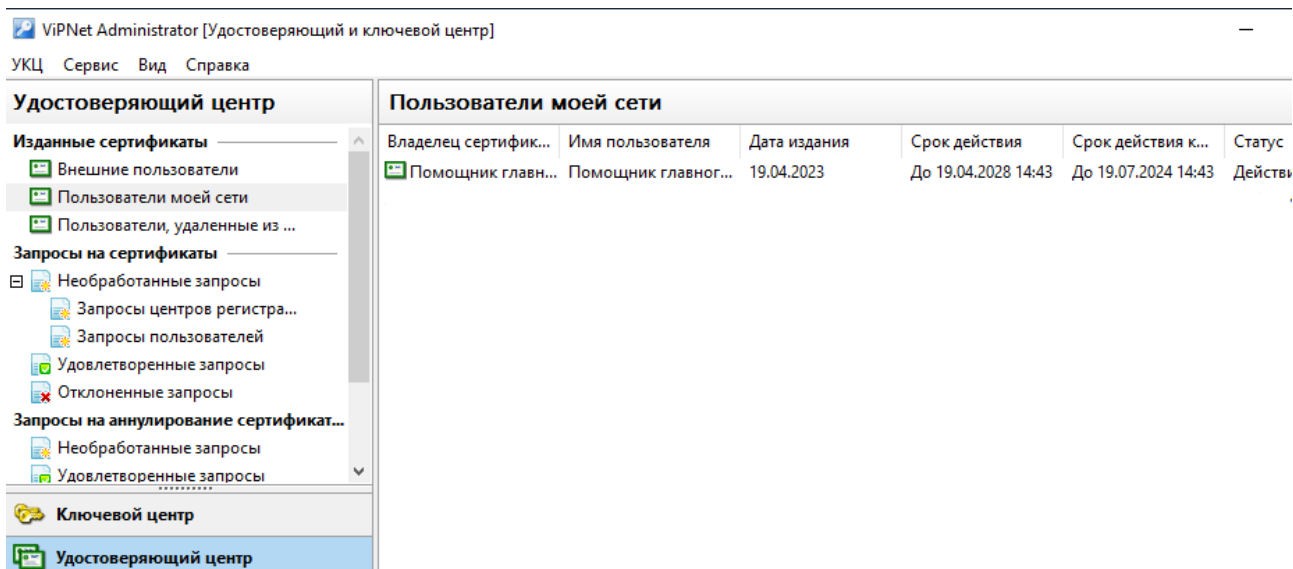
Переходим в пункт пользователи, выбираем помощника главного админа и убираем галочку Создать ключи электронной подписи



После чего выделяем всех, Ключи пользователя и Создать и передать ключи в ЦУС

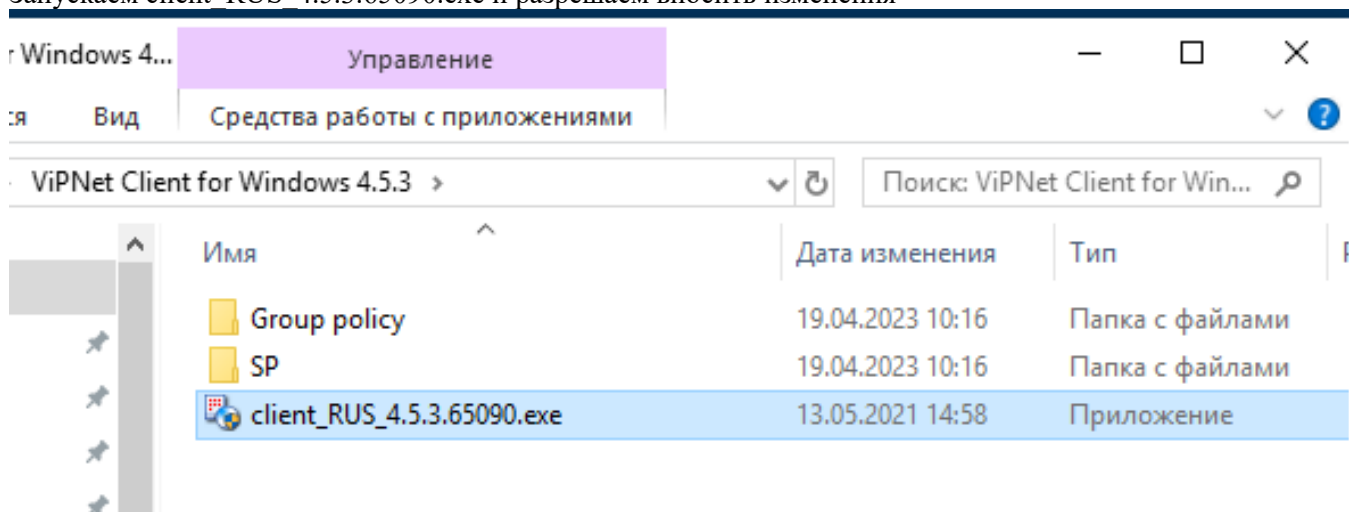


Переходим в вкладку Удостоверяющий центр → Пользователи моей сети и видим, что выдан только один сертификат, только для Помощника главного админа

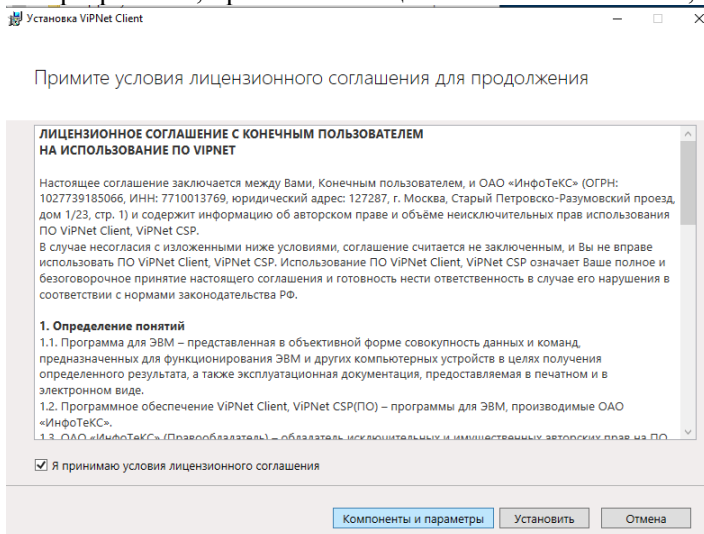


Устанавливаем ViPNet Client на машину Главного Администратора

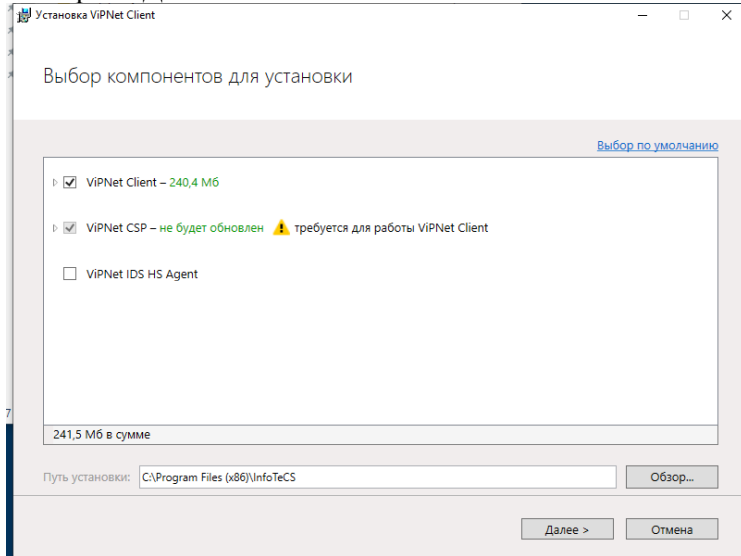
Запускаем client_RUS_4.5.3.65090.exe и разрешаем вносить изменения



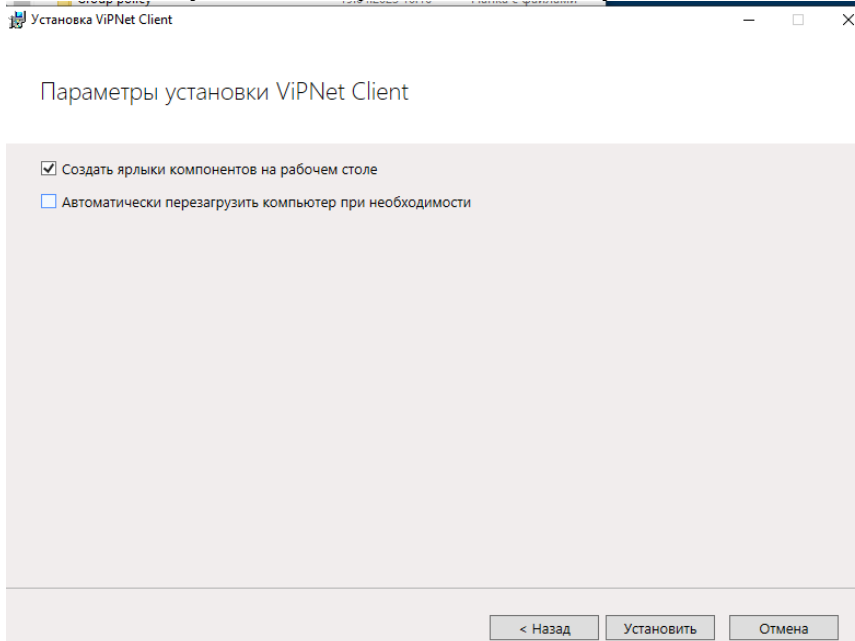
Как разрешили, принимаем лицензионное соглашение, нажимаем Компоненты и параметры



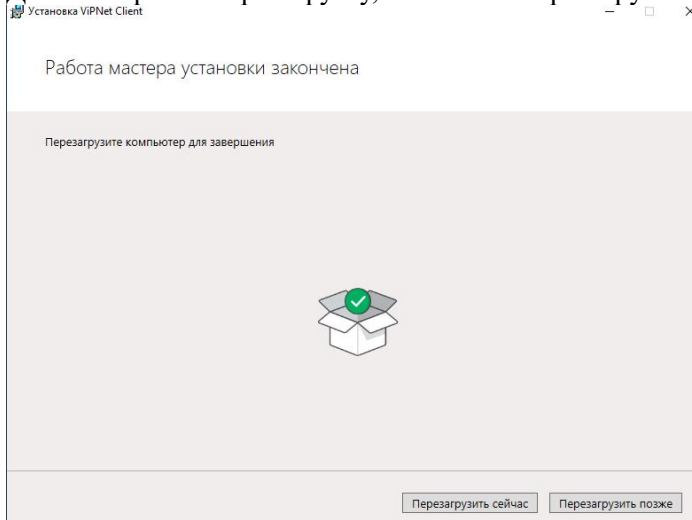
Выбираем Далее



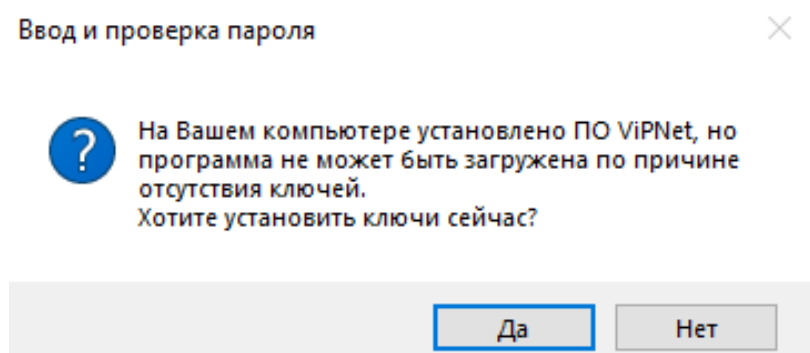
Ставим галочку Создавать ярлыки и нажимаем установить



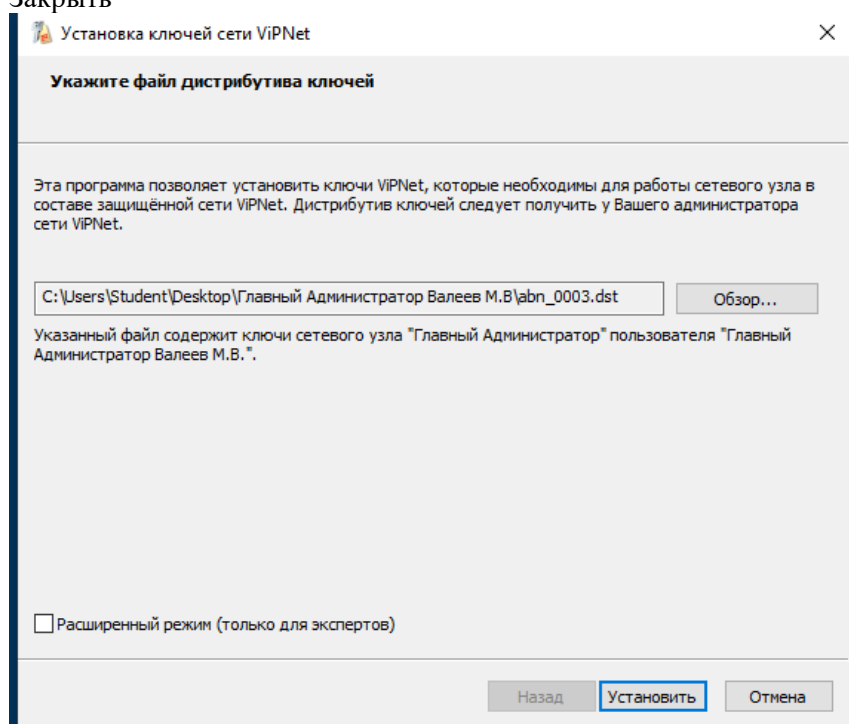
Далее попросит перезагрузку, нажимаем перезагрузить



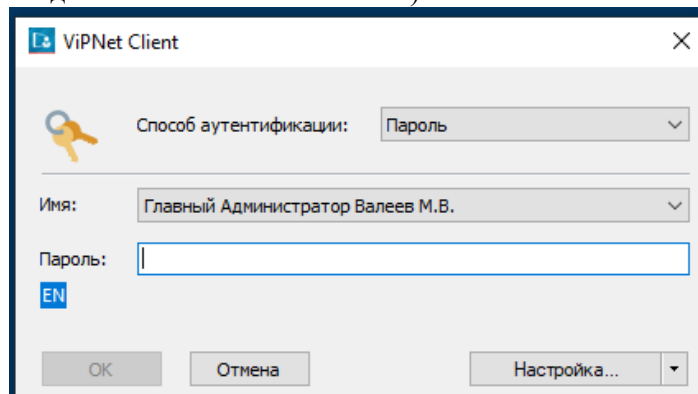
После перезагрузки появится окно, нажимаем Да



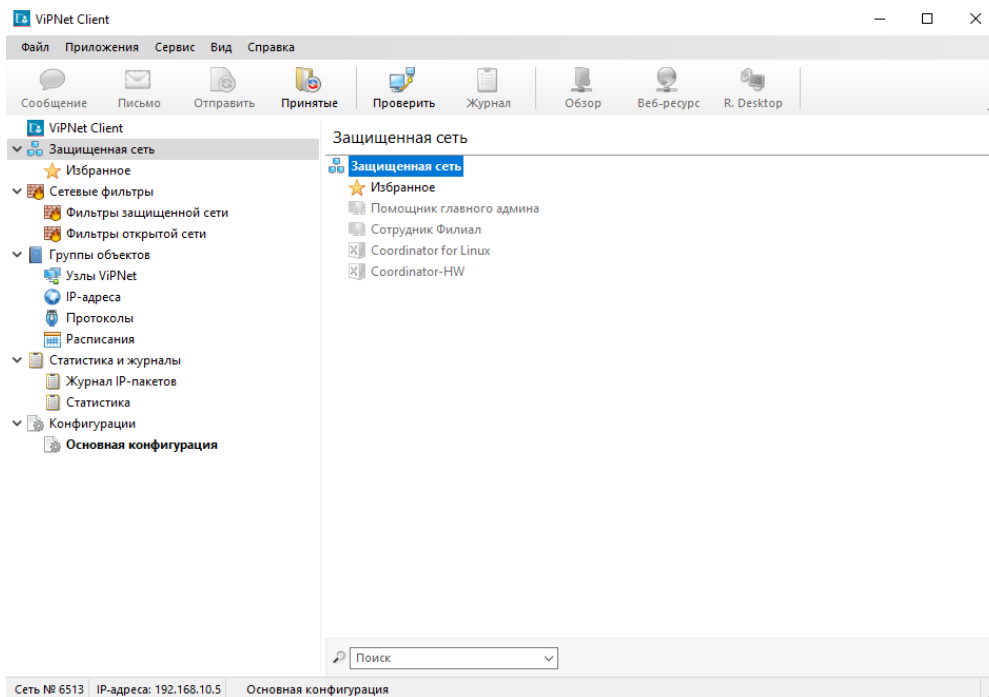
Прикрепляем дистрибутив ключей для Главного Администратора и нажимаем установить и кнопку Закреть



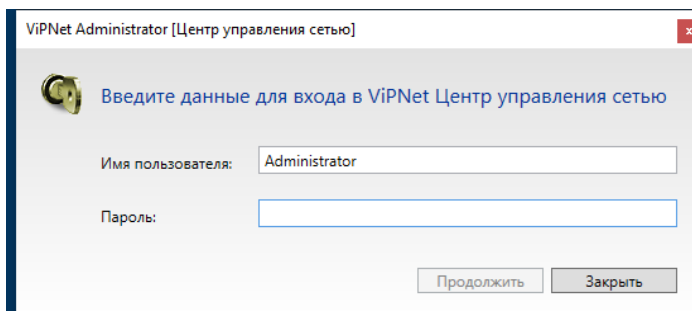
Вводим пароль который мы выдавали (Данный пароль выдавали в УКЦ при создании дистрибутива. На данный момент это 11111111)



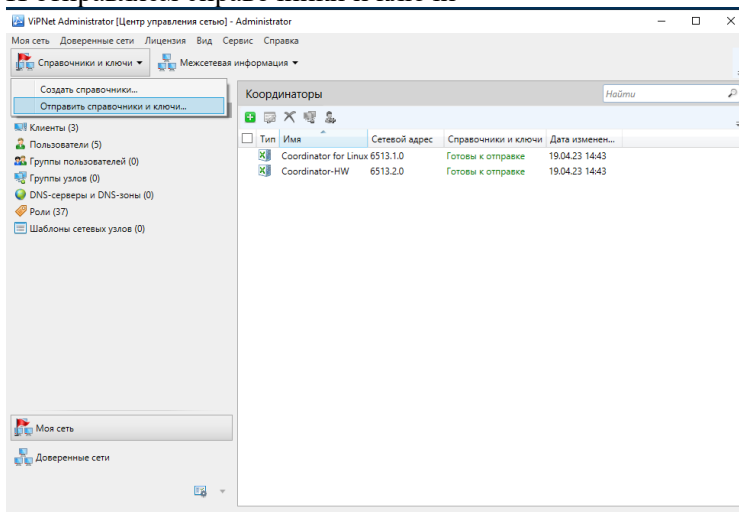
После ввода пароля запускаем ярлык ViPNet Client. Появится данное окно



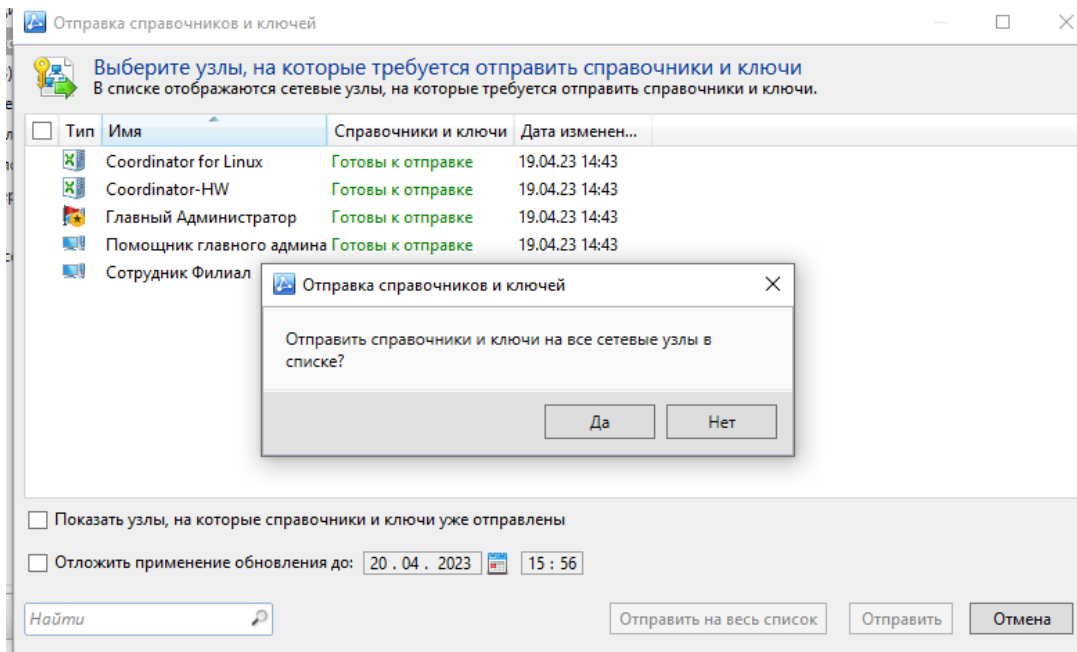
Запускаем ЦУС и вводим пароль и нажимаем продолжить



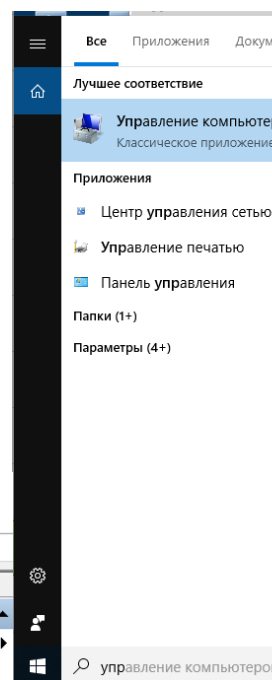
И отправляем справочники и ключи



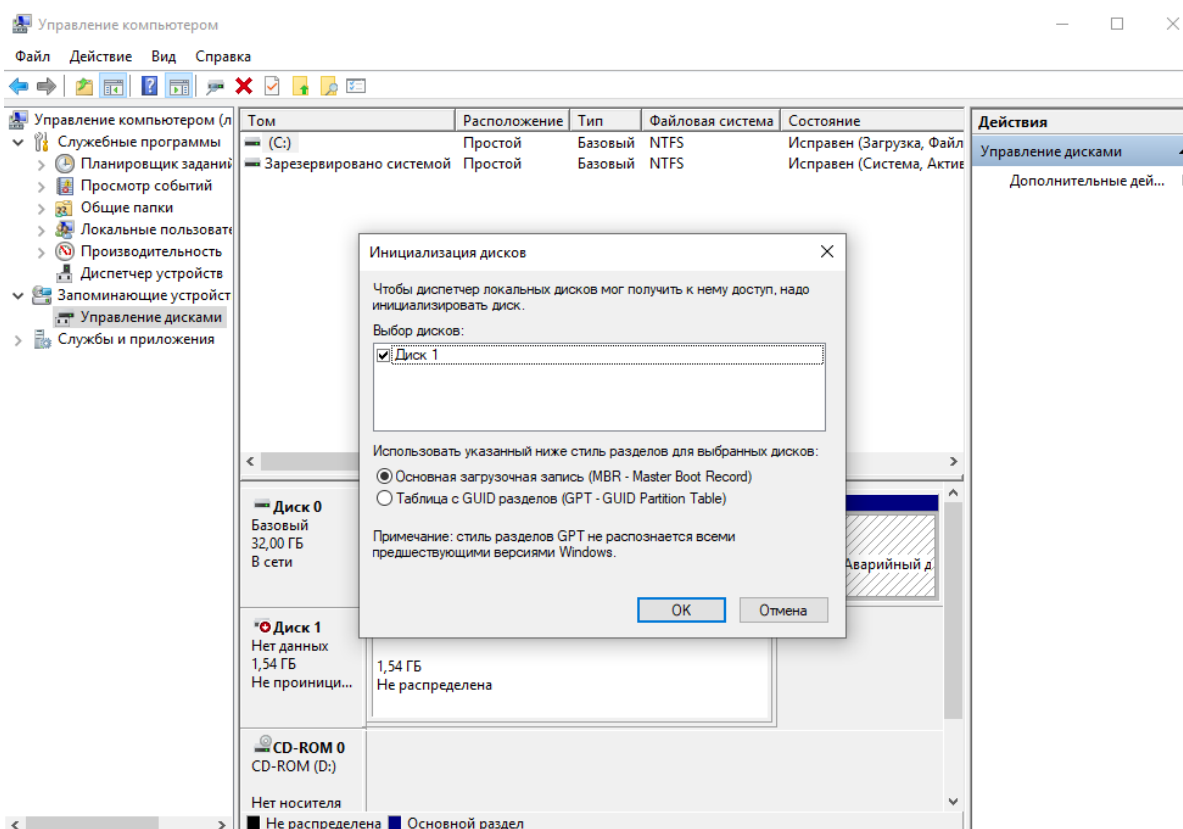
Нажимаем отправить на весь список и нажимаем Да



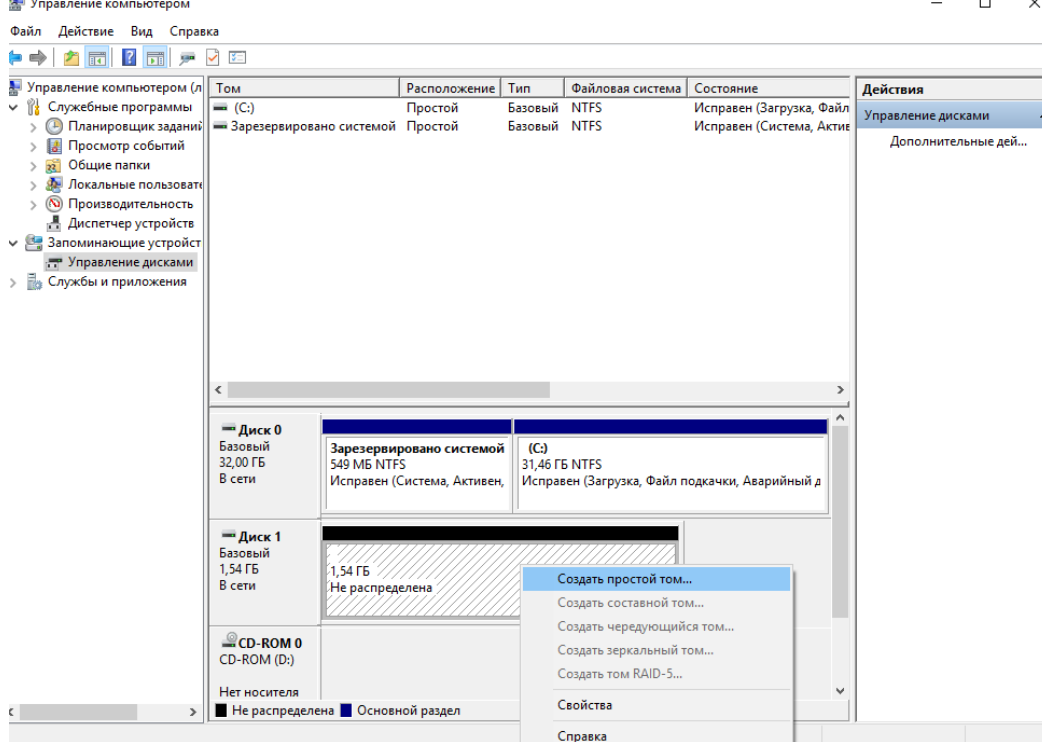
Создадим флешку с дистрибутивом для Coordinator for Linux. Нажимаем Win и пишем управление компьютером



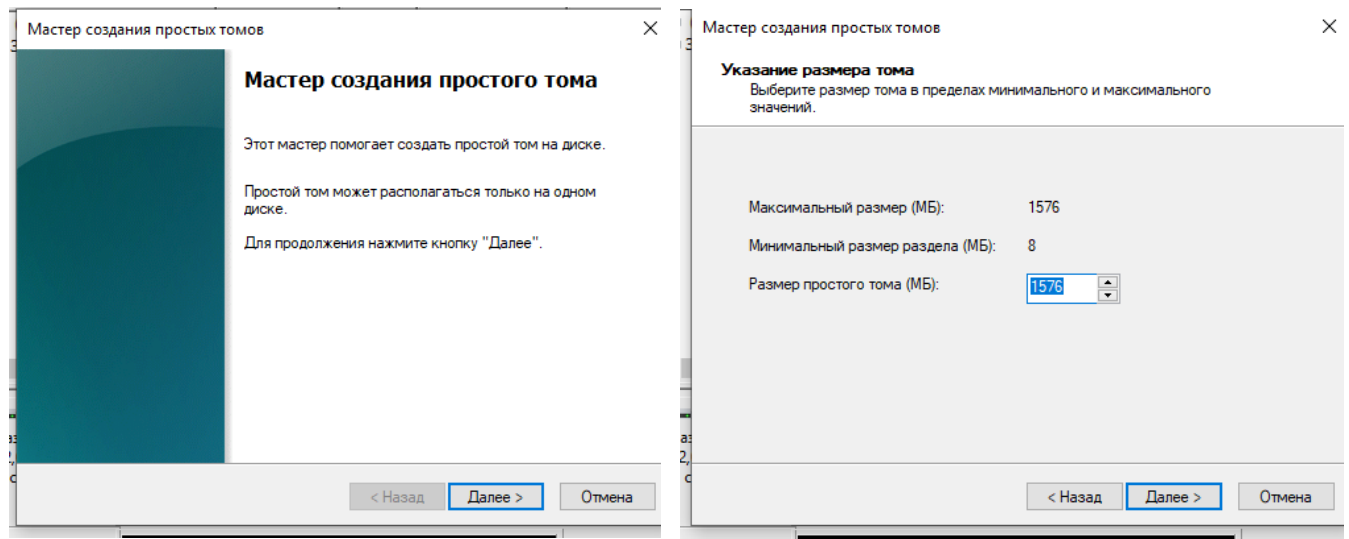
Нажимаем на пункт Управление дисками и в появившемся окне нажимаем ОК



Нажимаем ПКМ по не распределенной зоне и нажимаем создать простой том



Нажимаем Далее



Выбираем любую букву и нажимаем Далее

Назначение буквы диска или пути

Чтобы упростить доступ, вы можете назначить разделу букву диска или путь к диску.

Назначить букву диска (A-Z): F

Подключить том как пустую NTFS-папку: Обзор...

Не назначать буквы диска или пути диска

< Назад Далее > Отмена

Ставим файловую систему FAT32 и Называем свой том в поле Метка тома. После нажимаем Далее и ГОТОВО

Форматирование раздела

Для сохранения данных на этом разделе его необходимо сначала отформатировать.

Укажите, хотите ли вы форматировать этот том и какие параметры форматирования при этом нужно использовать.

Не форматировать данный том

Форматировать этот том следующим образом:

Файловая система: FAT32

Размер кластера: По умолчанию

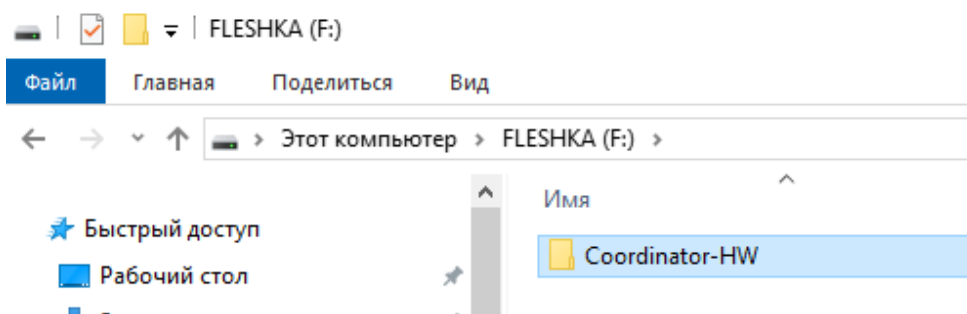
Метка тома: Fleshka

Быстрое форматирование

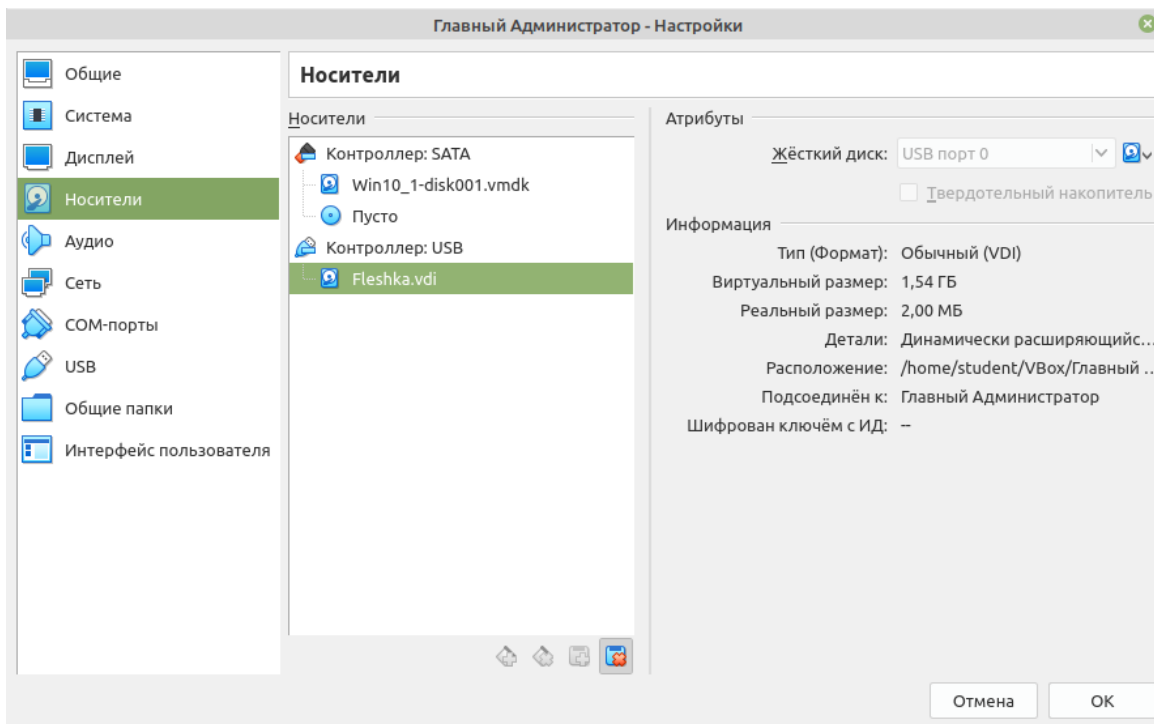
Применять сжатие файлов и папок

< Назад Далее > Отмена

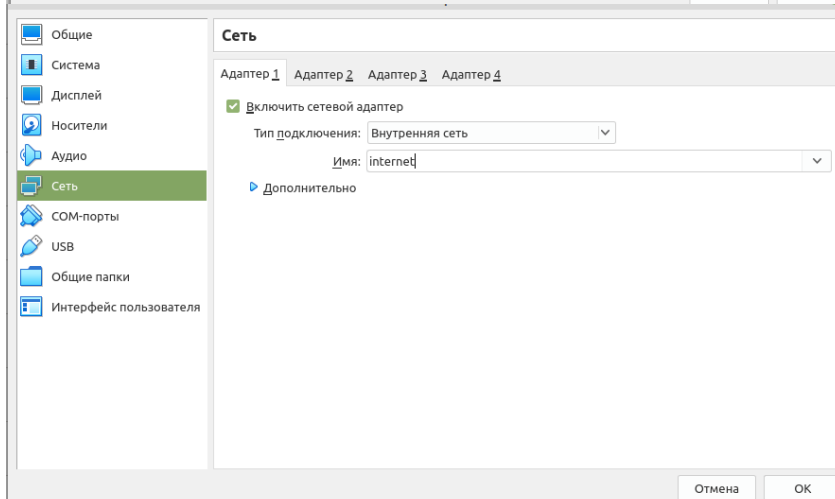
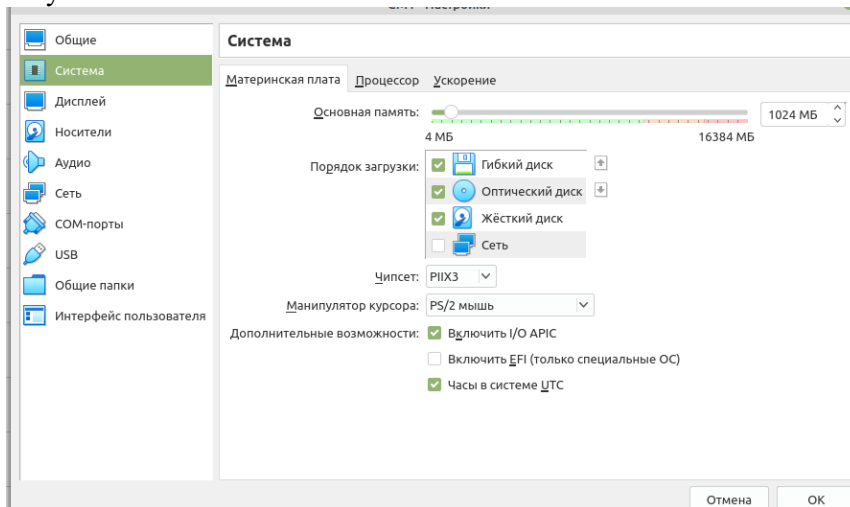
Закидываем на этот диск дистрибутив для Coordinator-HW



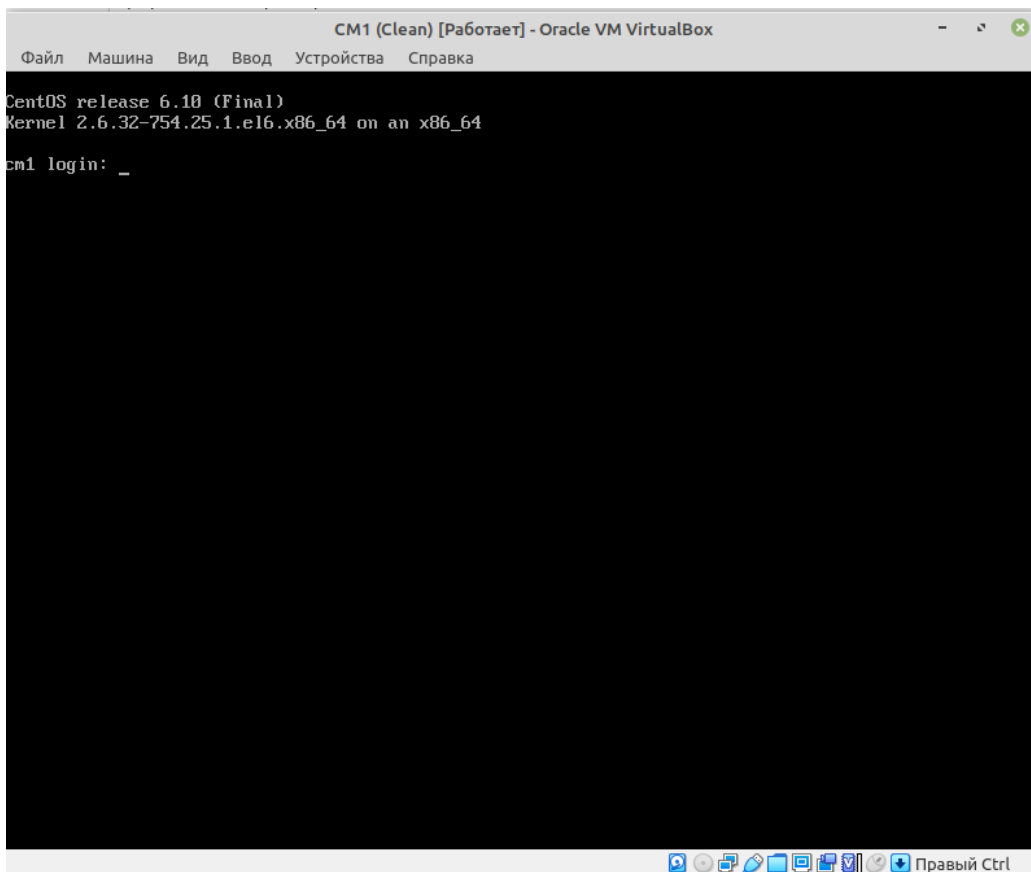
Заходим в VirtualBox, настройки машины Главного Администратора, Носители и выключаем созданный нами диск и нажимаем ОК



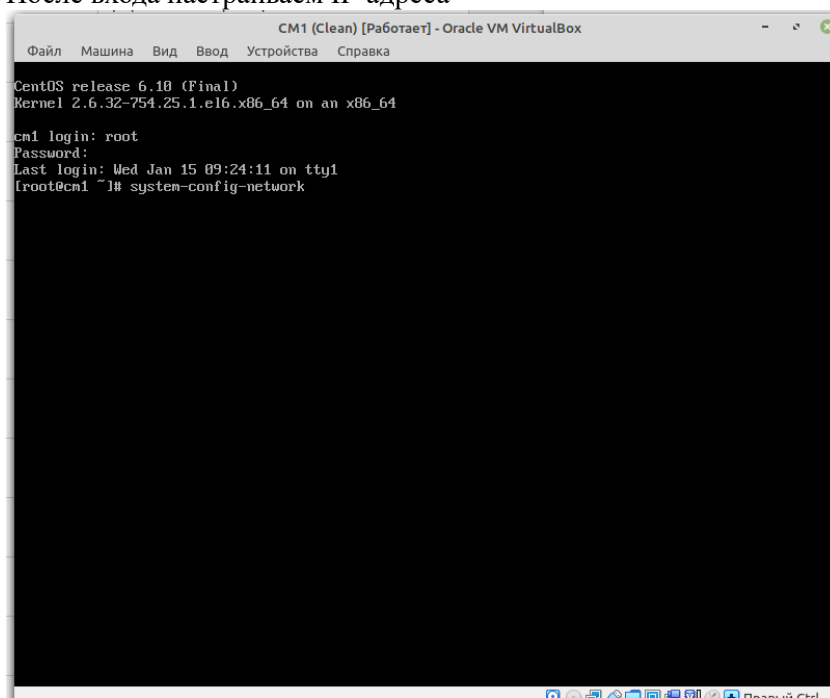
В VirtualBox выбираем машину Coordinator for Linux в Настройке, Система. Проверяем что бы выставлены были часы в системе UTC, затем заходим в Сеть и настраиваем адаптеры 1 и 2 адаптер это внутренняя сеть- Internet, 3 адаптер NET1 и 4 адаптер в sun. Нажимаем ОК и запускаем



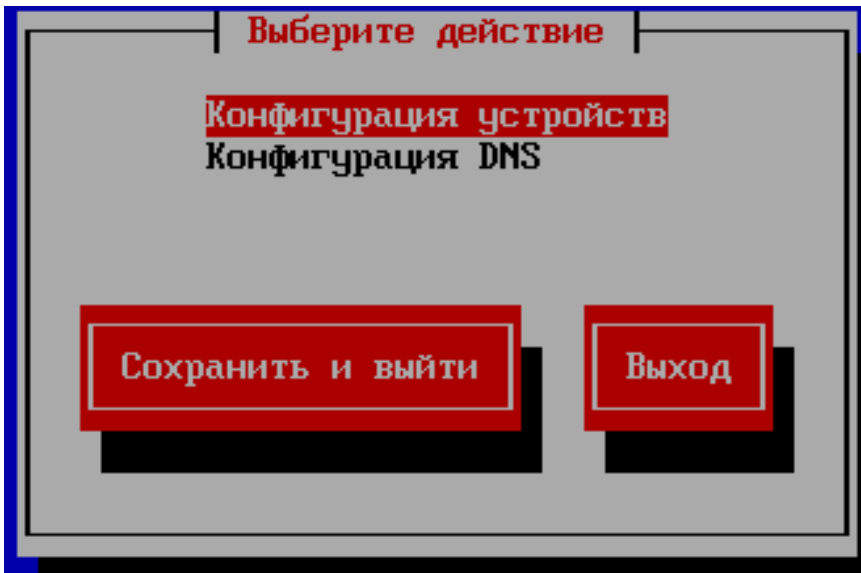
Для авторизации вводим root пароль бть единиц (111111)



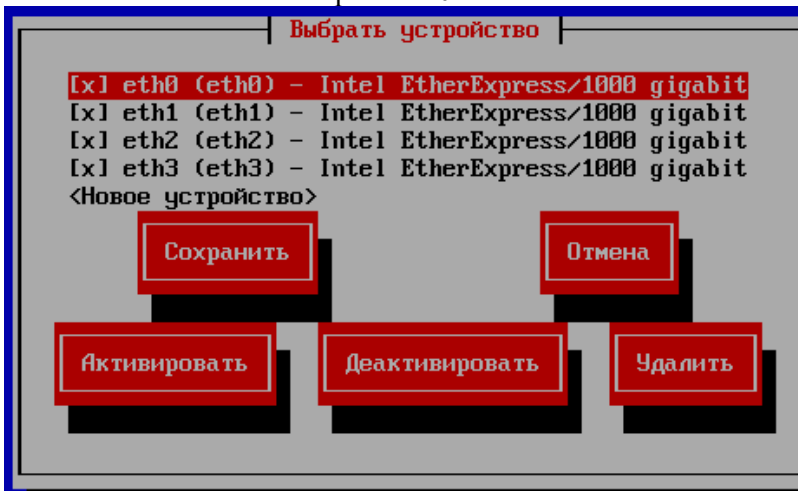
После входа настраиваем IP-адреса



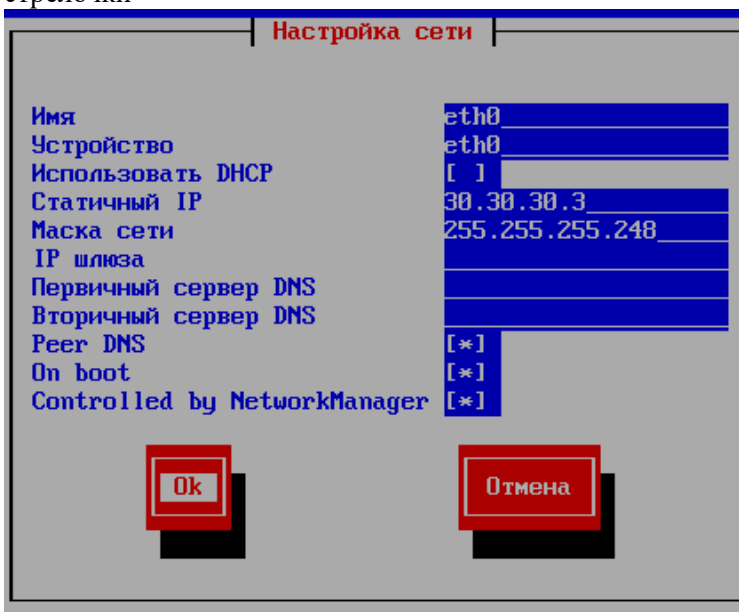
Нажимаем Enter

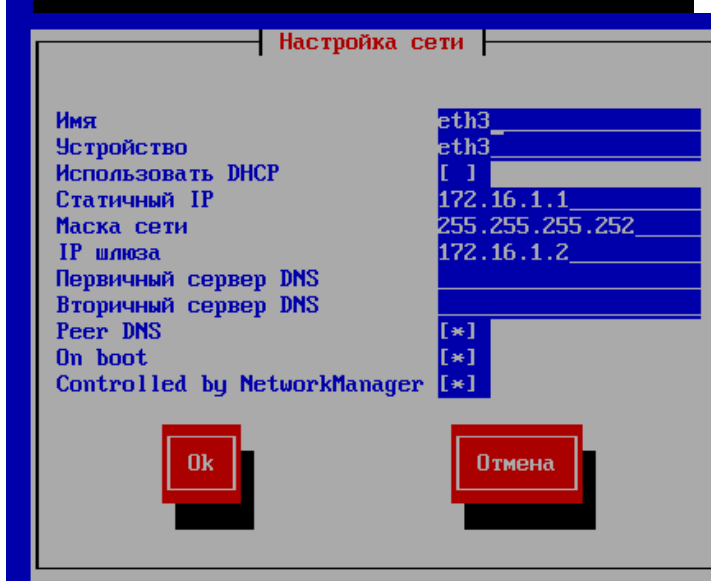
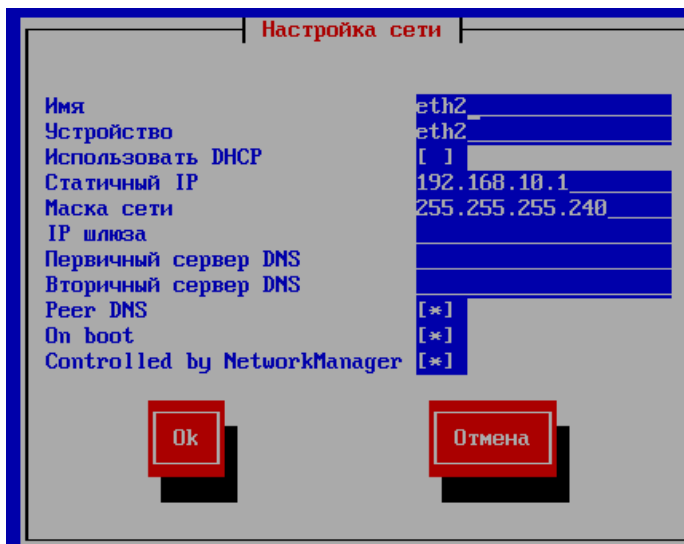


В появившемся окне выбираем eth0 и нажимаем Enter

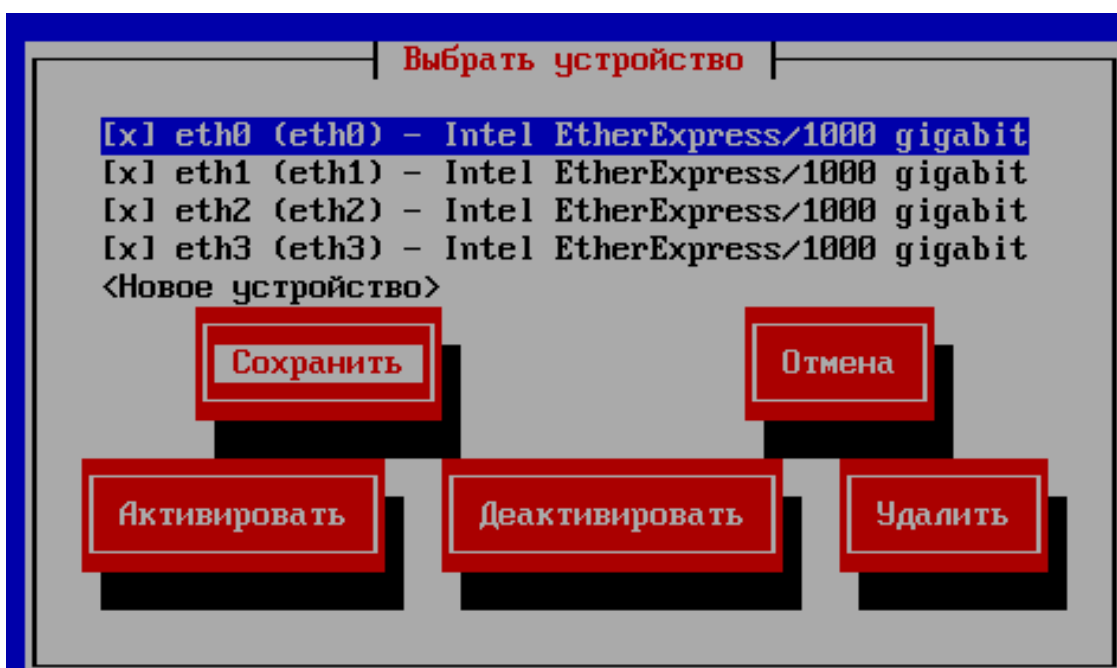


Задаем IP-адреса как на схеме. Для того что бы перейти на следующий элемент надо использовать стрелочки





После того как задали IP- адреса, что бы переключиться на кнопку Сохранить нажмите Tab



Затем нажимаем Сохранить и выйти



После того как вышли, прописываем `service network restart`



После того как он перезагрузился начнем создавать агрегированный канал. Создадим `bond0`

```
[root@cm1 ~]# vi /etc/sysconfig/network-scripts/ifcfg-bond0_
```

Пропишем прописываем туда конфигурацию (для редактирования нажать кнопку insert, для выхода нажимаем ESC пишем `:wq` и Enter)


```
DEVICE=bond0
IPADDR=30.30.30.3
NETMASK=255.255.255.248
GATEWAY=30.30.30.1
TYPE=Bond
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=static
```

Отредактируем eth0 и eth1

```
[root@cm1 ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Дописываем изменяем значение на no и дописываем 2 строчки. Сохраняем и выходим. Делаем тоже самое с eth1

```
NM_CONTROLLED=no
```

```
MASTER=bond0
SLAVE=yes
```

Создаем файл bonding.conf

```
[root@cm1 ~]# vi /etc/modprobe.d/bonding.conf
```

```
alias bond0 bonding
option bond0 mode=0 miimon=100
```

Перезапустим сеть, затем проверим что все работает

```
[root@cm1 ~]# ifconfig bond0
bond0 Link encap:Ethernet HWaddr 08:00:27:5A:B9:5F
       inet addr:30.30.30.3 Bcast:30.30.30.7 Mask:255.255.255.248
       inet6 addr: fe80::a00:27ff:fe5a:b95f/64 Scope:Link
       UP BROADCAST RUNNING MASTER MULTICAST MTU:1500 Metric:1
       RX packets:13 errors:0 dropped:0 overruns:0 frame:0
       TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:798 (798.0 b) TX bytes:978 (978.0 b)
```

```

[root@cm1 ~]# cat /proc/net/bonding/bond0
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: load balancing (round-robin)
MII Status: up
MII Polling Interval (ms): 0
Up Delay (ms): 0
Down Delay (ms): 0

Slave Interface: eth0
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 08:00:27:5a:b9:5f
Slave queue ID: 0

Slave Interface: eth1
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 08:00:27:9c:a1:d4
Slave queue ID: 0

```

Устанавливаем Coordinator for Linux

Прописываем mc и делаем так, что бы с левой стороны была директория tmp, а с правой стороны общая папка, в которой лежит установщик (директория media)

/tmp				/media/sf_Share/5. Exchange			
'и	Имя	Размер	Время правки	'и	Имя	Размер	Время правки
/..		-ВВЕРХ-	Апр 19 16:20	/..		-ВВЕРХ-	Май 4 2021
/.ICE-unix		4096	Апр 19 16:20	/Admin		4096	Апр 19 10:14
/mc-root		4096	Апр 19 17:09	/Dst for network	6513	4096	Апр 19 14:41
vboxguest-Module.symvers		25752	Янв 14 2020	/VIPNet Client	indows 4.5.3	4096	Апр 18 2022
yum.log		0	Янв 14 2020	/VIPNet Coordi	Linux 4.2.5	4096	Апр 25 2022
				*ua_vipnet_bas	.5.2-343.ova	446650K	Май 27 2022

Копируем установщик в директорию tmp (кнопка F5)

Копировать

Копировать каталог "distribute" с исходным шаблоном:

* [x] Метасимволы shell

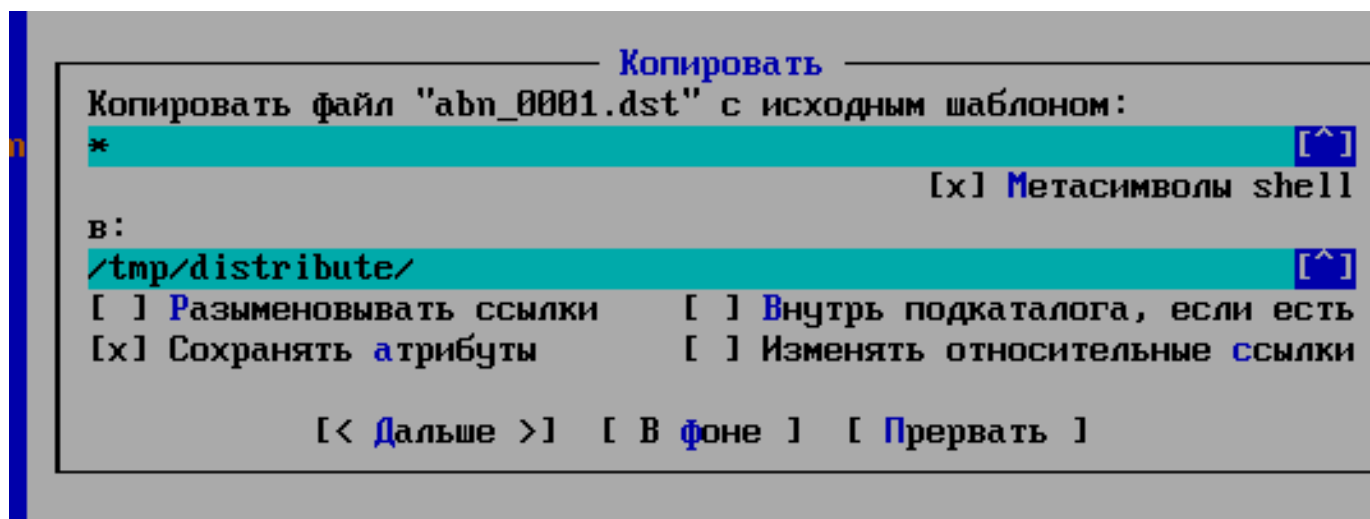
в: /tmp/

[] Разыменовывать ссылки [] Внутри подкаталога, если есть

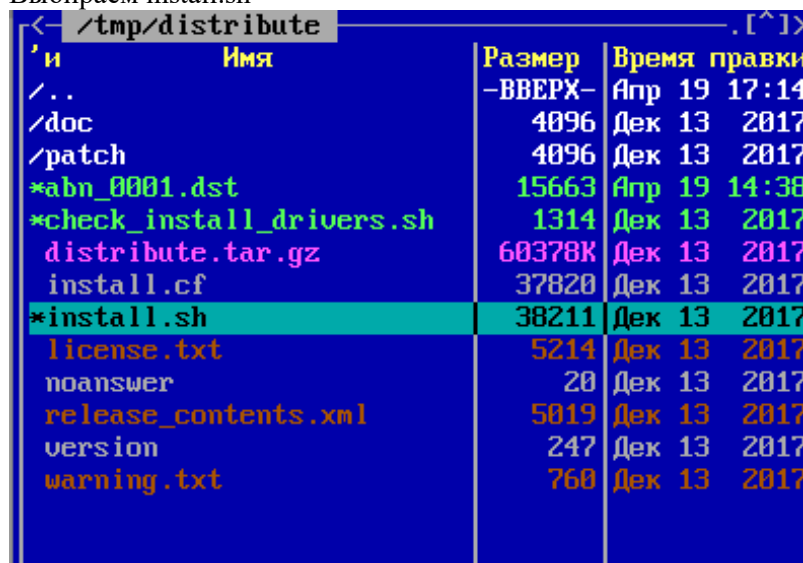
[x] Сохранять атрибуты [] Изменять относительные ссылки

[< Дальше >] [В фоне] [Прервать]

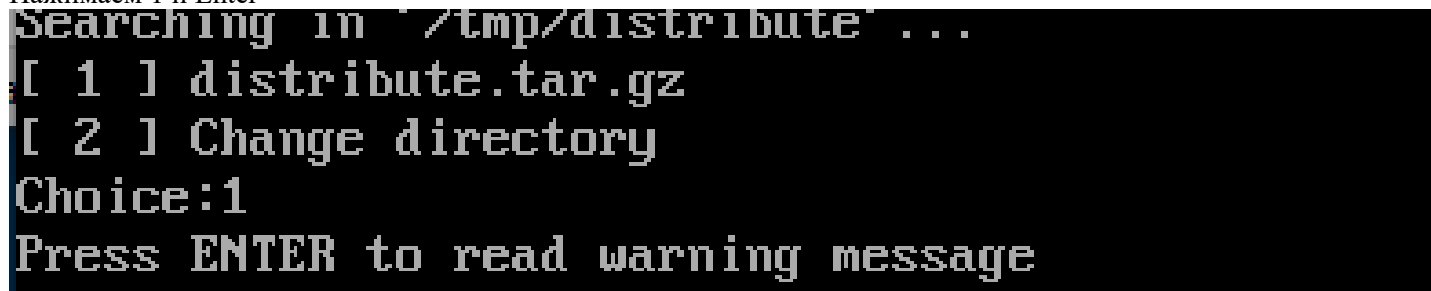
Слева заходим в директорию /distribute . Справа в общей папке Dst for network 6513 и в /distribute копируем ключ для Coordinator for Linux



Выбираем install.sh



Нажимаем 1 и Enter



Снова нажимаем Enter. Это установщик, он спрашивает продолжать ли установку, пишем y и Enter

```
This wizard will guide you through the installation of VipNet Software.
Before starting the installation process make sure that you have a key set
(*.DST file) and corresponding password. If you do not have a key set and
password stored on your hard drive or remote media, please abort the
installation.
```

```
If you have downloaded VipNet software for demo purposes, you can apply to our
helpdesk at support@infotecs.biz to receive key sets and passwords.
Alternatively you can generate them by yourself with the VipNet Manager or
VipNet Administrator. If you already use VipNet in your company, you should ask
your administrator to issue you the required key set and password to
accomplish the installation.
```

```
Do you want to continue installation? (y/n)y_
```

После нажимаем Enter, нажимаем Space для того что бы пролистать лицензионное соглашение, затем соглашаемся с соглашением написав у и нажав Enter

```
G. GENERAL:
```

```
This License is the entire agreement between us, superseding any other agreement or disc
l or written, and may not be changed except by a signed agreement. This License shall be
and construed in accordance with the laws. If any provision of this License is declar
t of competent jurisdiction to be invalid, illegal, or unenforceable, such a provision s
red from the License and the other provisions shall remain in full force and effect.
Do you agree to this License (y/n)y
```

После продолжаем установку

```
red from the License and the other provisions shall remain in full force and effect.
Do you agree to this License (y/n)y
STEP 3: Searching for current VipNet configuration
No current VipNet configuration found
STEP 4: Preparing for installation
This script will install
VipNet Virtual Private Network (x86_64/Linux) Product version: 4.2.5 build 13595
Do you want to continue installation? (y/n)y_
```

Выбираем ключ для Coordinator for Linux

```
STEP 8: Select VipNet configuration file (*.DST)
Searching in '/tmp/distribute'...
[ 1 ] abn_0001.dst
[ 2 ] Change directory
[ 3 ] Skip selection
Choice:1
```

Оставляем директорию по умолчанию (нажимаем Enter)

```
Choice:1
STEP 9: Select directory to install VipNet configuration
Please enter directory path to install selected VipNet configuration (default '/etc/vipnet'):
```

Вводим пароль от дистрибутива

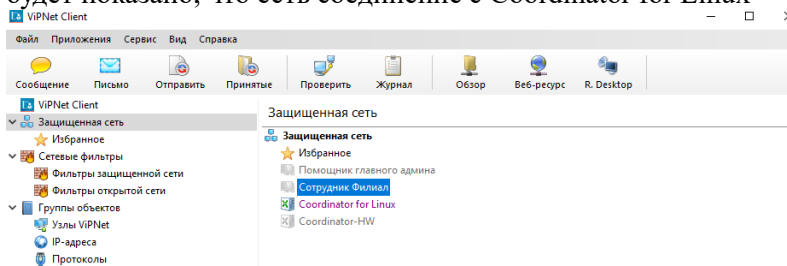
```
ViPNet Virtual Private Network (x86_64 Linux) Product version: 4.2.3 build 13333
Do you want to continue installation? (y/n)y
STEP 5: Installing drivers
Install drviplr.ko
Install itcswd.ko
Install itcscprt.ko
Install itcskrniface.ko
STEP 6: Installing applications
Adding user www-data to system
Installing man pages
STEP 7: Saving startup configuration
STEP 8: Select ViPNet configuration file (*.DST)
Searching in '/tmp/distribute'...
[ 1 ] abn_0001.dst
[ 2 ] Change directory
[ 3 ] Skip selection
Choice: 1
STEP 9: Select directory to install ViPNet configuration
Please enter directory path to install selected ViPNet configuration (default '/etc/vipnet'):
STEP 10: Abonent authentication
Enter your ViPNet password:
```

Подтвердить автозапуск ViPNet

```
STEP 9: Select directory to install ViPNet configuration
Please enter directory path to install selected ViPNet configuration (default '/etc/vipnet'):
STEP 10: Abonent authentication
Enter your ViPNet password:
Station name: Coordinator for Linux
User login: 19710001
User password successfully checked
/etc/hosts file is missing a necessary entry: 127.0.0.1 cm1.infotecs.edu
Please edit /etc/hosts file manually and provide this entry.
Do you want to start ViPNet services automatically now? (y/n)y
```

После установки нажимаем F10 и выходим обратно в консоль

Так как мы установили Coordinator for Linux на машине Главного Администратора в ViPNet Client будет показано, что есть соединение с Coordinator for Linux



Создаем кластер горячего резервирования

Останавливаем Демон Failover

```
[root@cm1 ~]# failover stop
Shutting down failover daemon
[root@cm1 ~]#
```

Заходим в vi и редактируем Failover.ini

```
[root@cm1 ~]# vi /etc/failover.ini
```

Добавляем еще один канал, выдаем активные и пассивные IP-адреса

```

[network]
checktime = 10
timeout = 2
activeretries = 3
channelretries = 3
synctime = 5
fastdown = yes

[channel]
device = eth0
activeip = 30.30.30.1
passiveip = 30.30.30.2
testip = 127.0.0.1
ident = iface-0
checkonlyidle = yes

[channel]
device = eth2
activeip = 192.168.10.2
passiveip = 192.168.10.3
testip = 127.0.0.1
ident = iface-1
checkonlyidle = yes

[sendconfig]
activeip = 172.16.1.2
sendtime = 60
device = eth3
keys = yes
config = yes
journals = yes
port = 10090

```

Устанавливаем кластер и запускаем в активном режиме

```

[root@cm1 ~]# failover install
Installing ViPNet failover system
[root@cm1 ~]# failover start active

```

Проверяем

```

[root@cm1 ~]# failover info
Running failover info
Versions: ViPNet 4.2.5 (13595), daemon 1.5 (1)
Workstation configured for ID 1971000A (Coordinator for Linux)
The workstation works in a cluster mode of protection against failures
Workstation time (utc: 1681982782) Thu Apr 20 12:26:22 2023

* local          * remote
failover mode    * active         * unknown
failover uptime  * 0d 0:00        * 0d 0:00
total cpu        * 100%           * 0%
total memory     * 1019920 kB     * 0 kB
free memory      * 808244 kB      * 0 kB
failover state   * works          * unknown
failover cpu     * 0%             * 0%
iplir state      * initializing   * unknown
mftp state       * initializing   * unknown
alg state        * initializing   * unknown
webgui state     * works          * unknown
webgui cpu       * 7%             * 0%
[root@cm1 ~]#

```

Создаем второй такой же Coordinator for Linux, но со своими IP-адресами (согласно схеме), но тот же дистрибутивом ключей что и первый, создаем агрегированный канал и ставим кластер

```
Файл  Машина  Вид  Ввод
[network]
checktime = 10
timeout = 2
activeretries = 3
channelretries = 3
synctime = 5
fastdown = yes

[channel1]
device = eth0
ident = iface-0
activeip = 30.30.30.1
passiveip = 30.30.30.3
testip = 127.0.0.1
checkonlyidle = yes

[channel1]
device = eth2
ident = iface-1
activeip = 192.168.10.1
passiveip = 192.168.10.3
testip = 127.0.0.1
checkonlyidle = yes

[sendconfig]
activeip = 172.16.1.2
sendtime = 60
device = eth3
config = yes
keys = yes
journals = yes
port = 10090
```

Как сделали на второй машине так же, на основной машине при вводе Failover info покажет так

```

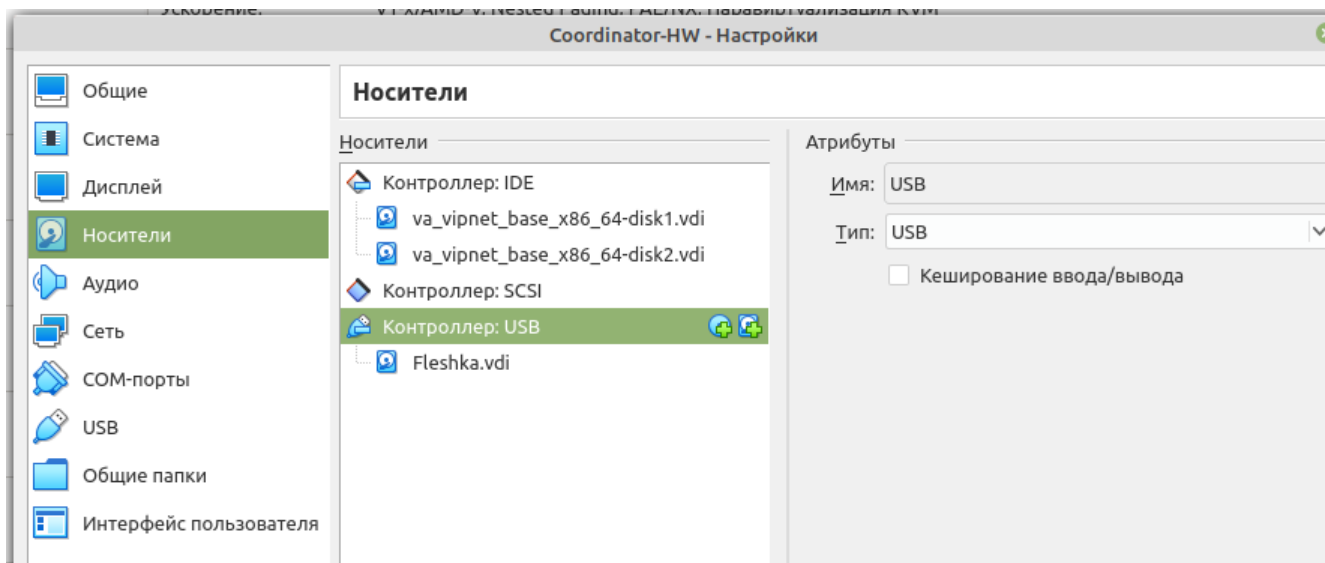
* local      * remote
failover mode * active    * passive
failover uptime * 0d 0:00  * 0d 0:00
total cpu      * 0%        * 1%
total memory   * 1019920 kB * 1019920 kB
free memory    * 790192 kB  * 843976 kB
failover state * works     * works
failover cpu   * 1%        * 0%
iplir state    * works     * works
iplir cpu      * 1%        * 0%
mftp state     * works     * works
mftp cpu       * 1%        * 2%
alg state      * works     * stopped
alg cpu        * 0%        * 0%
webgui state   * works     * stopped
webgui cpu     * 0%        * 0%
[root@cm1 ~]# _
```

Настройка Coordinator-HW

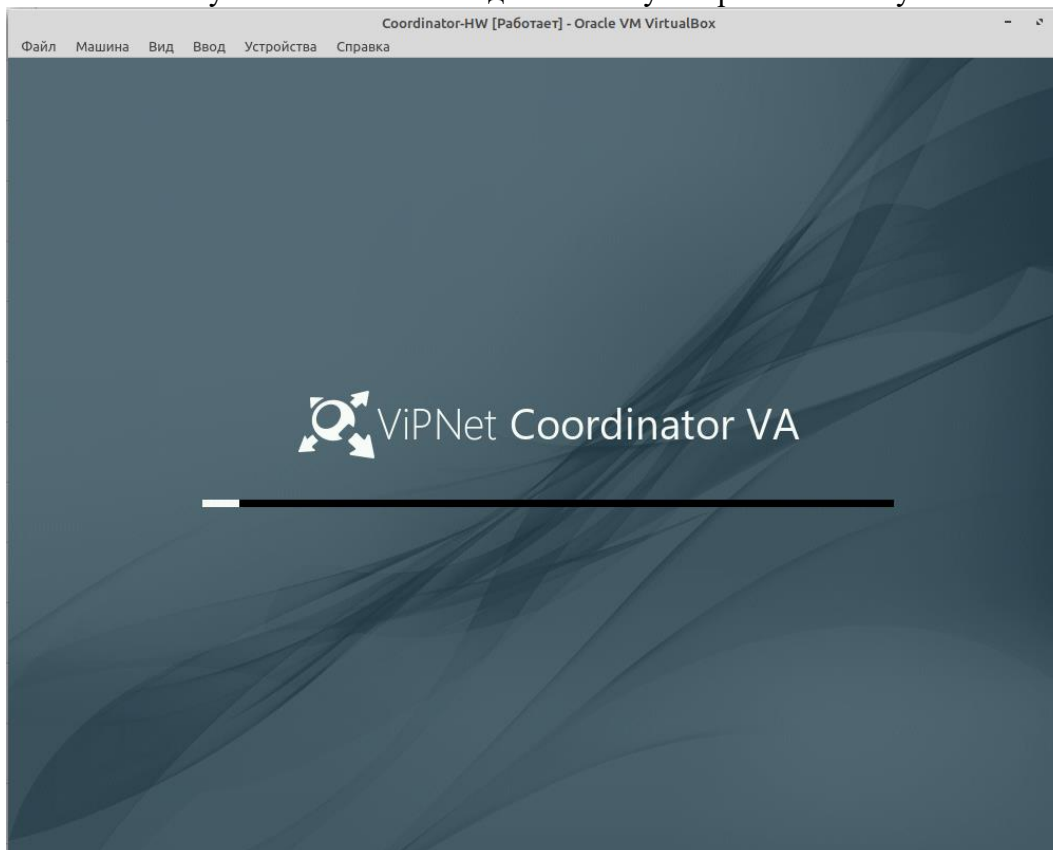
Заходим в настройка машины Coordinator-HW → Система и смотрим часы в системе UTC, затем переходим в Сеть и настраиваем адаптеры согласно схеме

!! Оставляем включенные все адаптеры. Последний адаптер замыкаем на N5 (при инициализации его выключим)

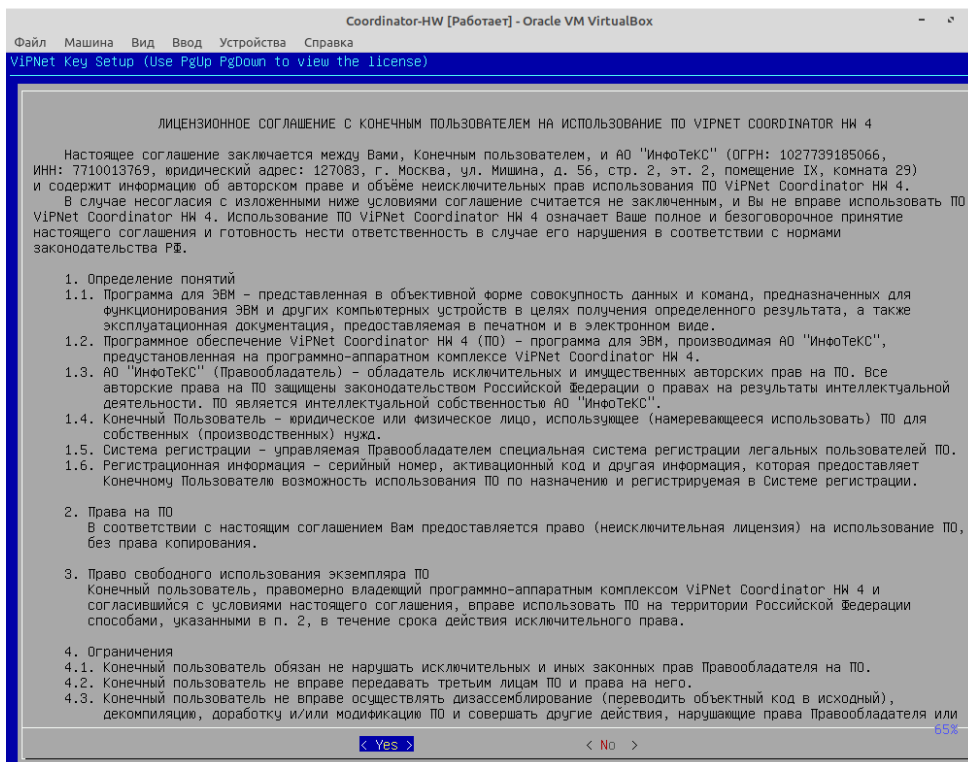
После того как настроили сеть заходим в Носители и подключаем флешку с дистрибутивом для Coordinator-HW



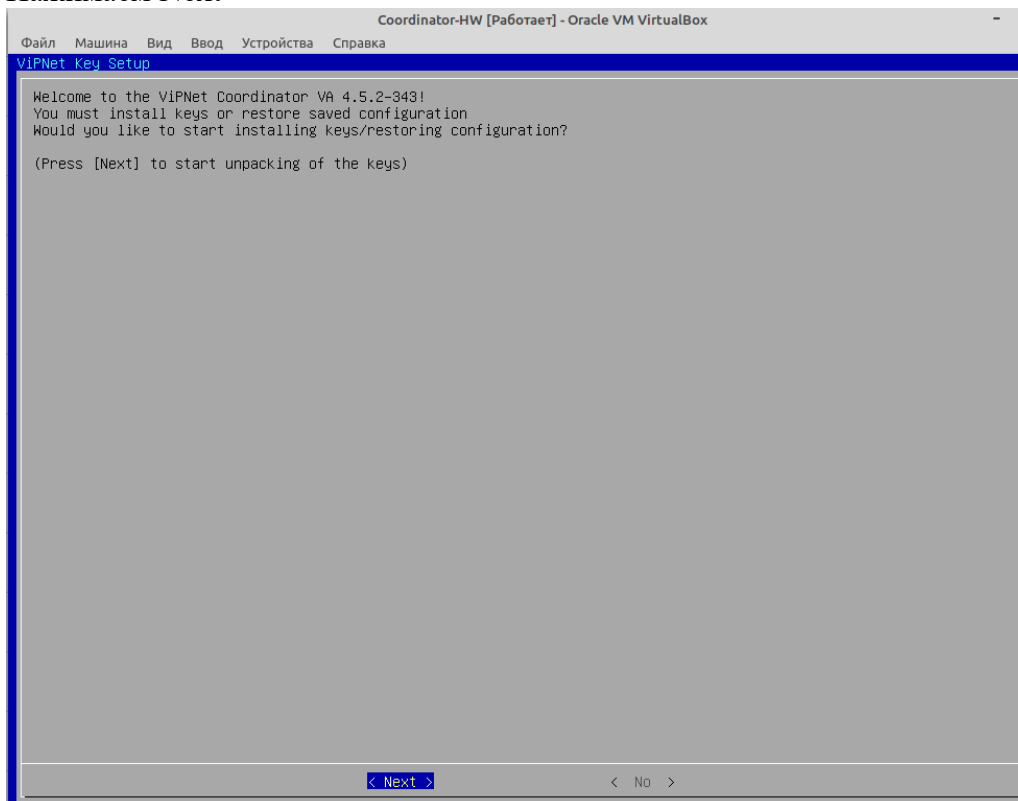
После чего запускаем. Он опять выдаст ошибку. Закрываем и запускаем снова



После запуска производим инициализацию. user|user
После чего выбираем установку в режиме full-screen interface. Далее принимаем лицензионное соглашение



Нажимаем Next



Далее выбираем регион Европа→Россия→ Москва, после проверяем и нажимаем Yes

```
The following information has been given:
```

```
Russia  
MSK+00 - Moscow area
```

```
Therefore TZ='Europe/Moscow' will be used.  
Local time is now: Thu Apr 20 15:00:08 MSK 2023.  
Universal Time is now: Thu Apr 20 12:00:08 UTC 2023.  
Is the above information OK?
```

Проверяем Дату и Время. Если не совпадают то выставляем самостоятельно. Если поставить неправильное время и дату, не будет ничего работать

```
Date and time were set to 2023-04-20 15:01:55
```

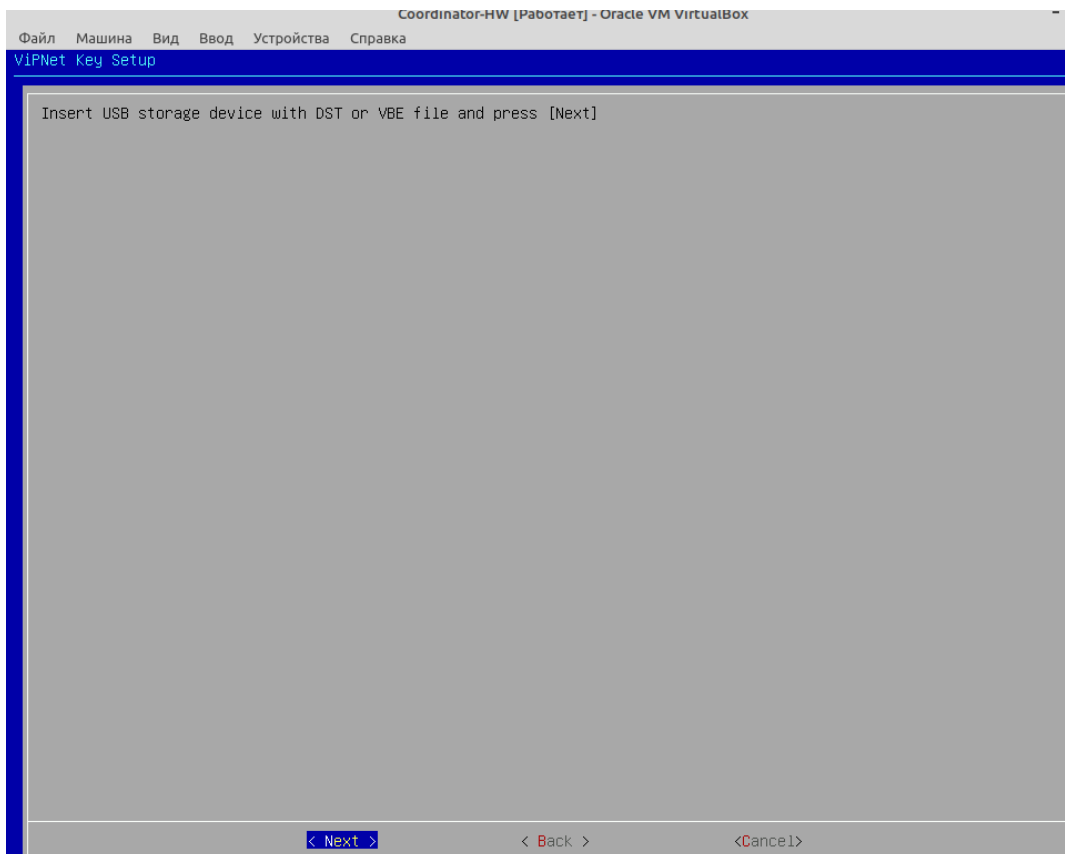
Оставляем загрузку ключей через USB

```
ViPNet Key Setup
```

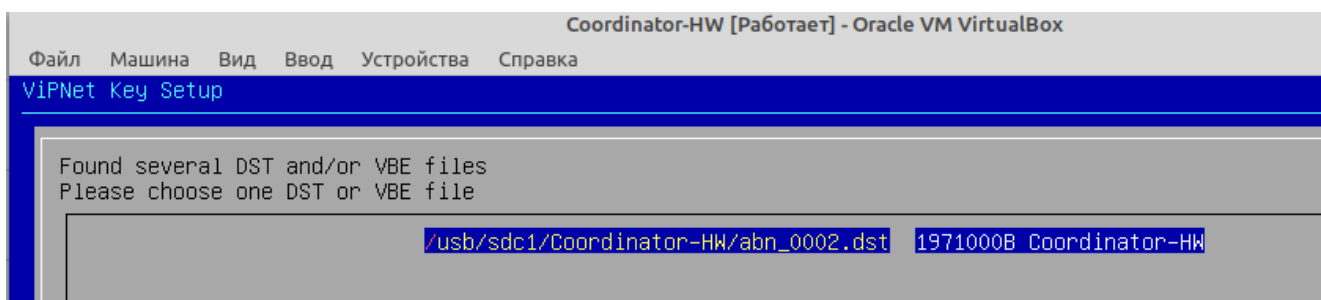
```
Would you like to start installing keys from TFTP, USB or CD storage device?
```

```
( ) tftp Upload keys by TFTP  
(* ) usb Load keys from USB storage device  
( ) cd Load keys from CD disk
```

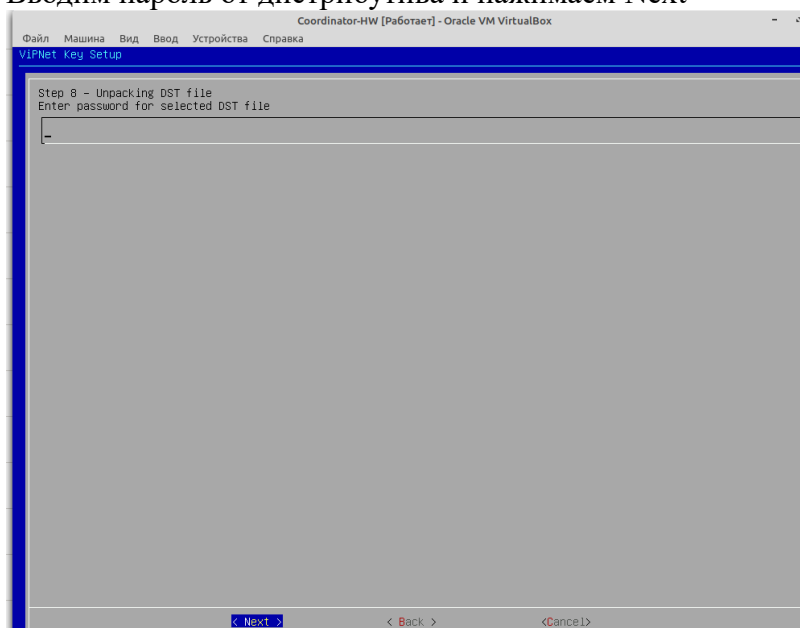
Нажимаем Next



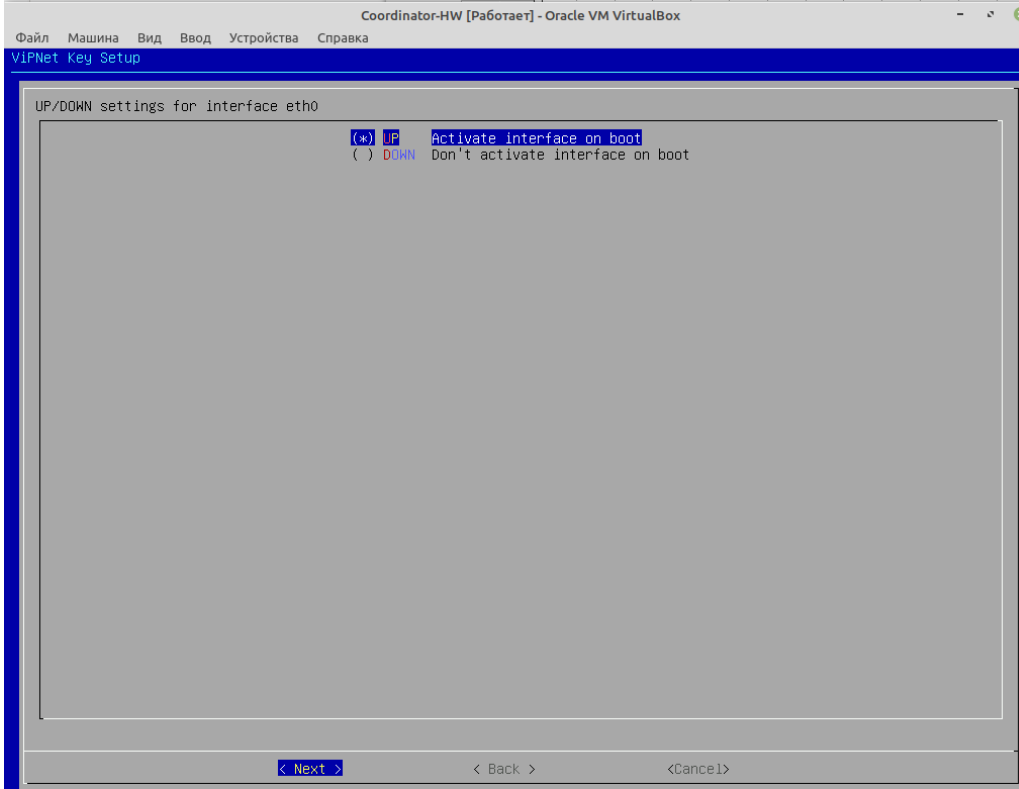
После чего выбираем наш дистрибутив ключей для Coordinator-HW



Вводим пароль от дистрибутива и нажимаем Next



После чего настраиваем адаптеры согласно схеме. Eth1 и 3 выбираем Down



Ставим статичный IP-адрес



Выдаем IP-адрес

Static IP-address settings for eth0

Interface Name	eth0
IP-address	30.30.30.2
Netmask	255.255.255.248

< Next > < Back > <Cancel>

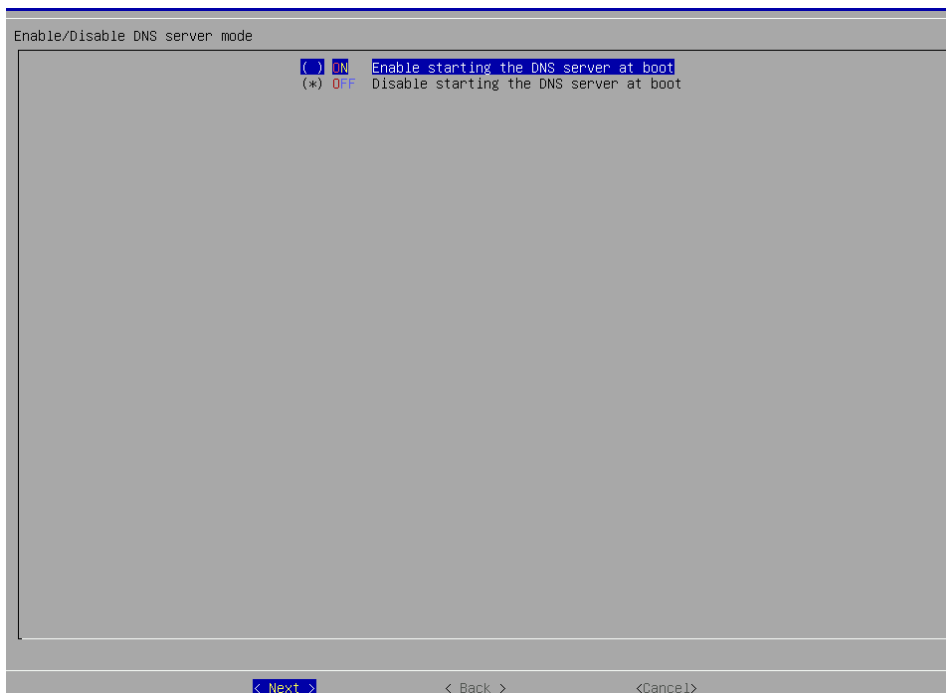
Шлюз пишем IP-адрес другого Coordinator`а

Enter IP-address of the default gateway

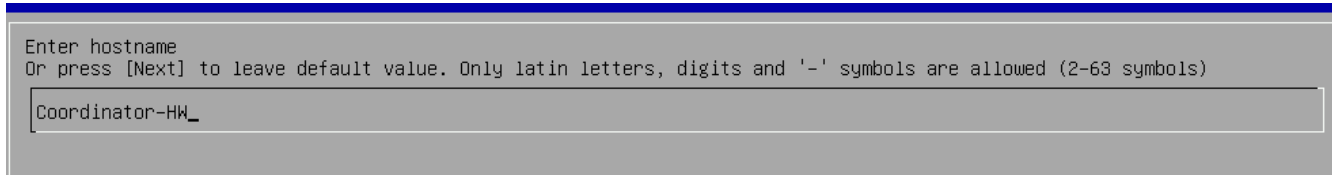
IP-address	30.30.30.1
------------	------------

< Next > < Back > <Cancel>

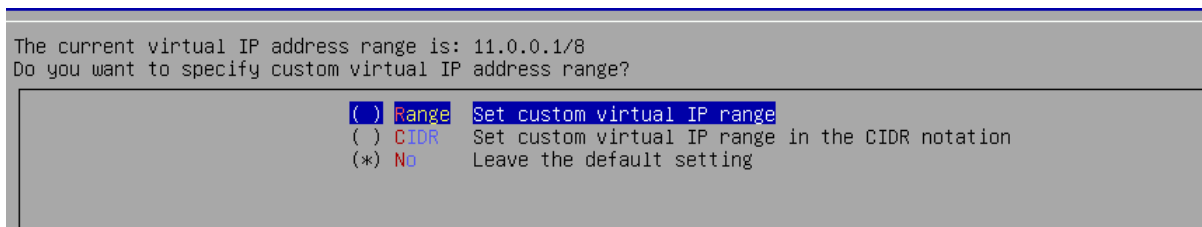
Dns и NTP выключаем



Выдаем hostname



Оставляем вариант No



Здесь выбираем No

Do you want to probe VPN-connection with some host in order to verify the configuration you've just made?

< Yes >

< Back >

< No >

Тут нажимаем ОК

IPNet Key Setup

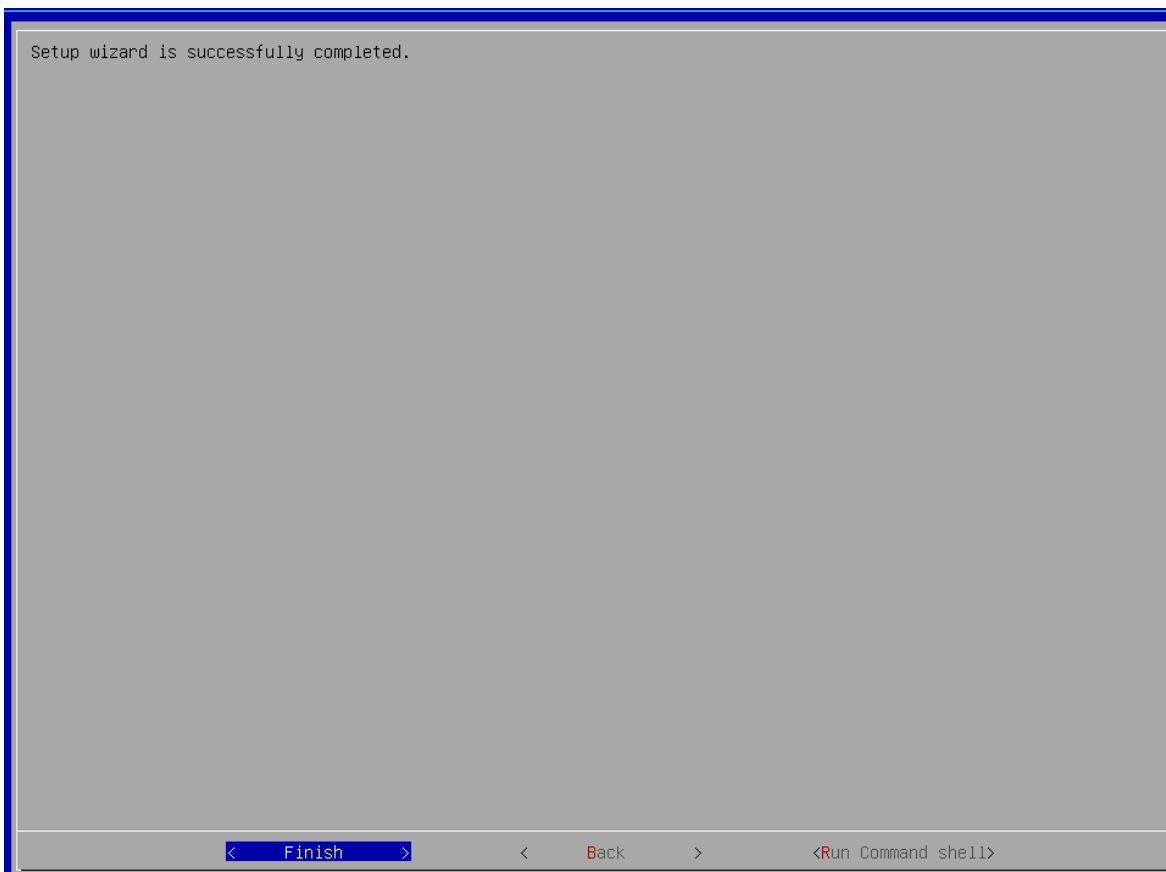
The Appliance management is available via web-interface from a browser.
You may access web-interface using the Appliance address on port 8080.

< OK >

Запускаем VPN сервис после завершения загрузки. Нажимаем Yes



Завершаем установку. Нажимаем Finish



Производим авторизацию и входим в режим администратора

```
Product: VIPNet Coordinator VA
Platform: VA VIRTUALBOX
License: HW-VA
Software version: 4.5.2-343
(C) JSC InfoTECS, 2022; website: www.infotecs.ru, email: soft@infotecs.ru; phone (Russia): 8 800 250-0-260, phone (Moscow): +7 4
95 737-61-92
Coordinator-HW login: user
Password:
Last login: Thu Apr 20 15:08:49 MSK 2023 on tty1
Loading command shell, please wait...
Starting the command line interface of Platform: VA VIRTUALBOX
Coordinator-HW> en
Type the administrator password:
Coordinator-HW# _
```

Настроим Dhcp server для eth2

```
Coordinator-HW#
Coordinator-HW# inet dhcp server add interface eth2
Coordinator-HW# inet dhcp server add range 192.168.20.2 192.168.20.5 interface eth2
Coordinator-HW# inet dhcp server add router 192.168.20.1 interface eth2
Coordinator-HW# inet d
Coordinator-HW#
Coordinator-HW# dhcp dgd dns
Coordinator-HW# inet dhcp server mode on
DHCP server is enabled and will be started on the next reboot
You need to start the DHCP server manually or reboot to start it
Coordinator-HW# inet dhcp server start
Starting DHCP server ...
Coordinator-HW#
```

Создаем туннель для Linux 1 и Linux 2

Останавливаем работу демона iplir и вносим изменения в iplir config

```
more are no changes in ip
Coordinator-HW# iplir stop
Shutting down IpLir
Coordinator-HW#
Coordinator-HW# iplir config
```

Меняем с auto на manual (tunnel_virt_assignment)

```
[misc]
config_version= 4.7.1-1
packettype= 4.1
timediff= 7200
timesync= off
warnoldautosave= on
client_pollinterval= 300
server_pollinterval= 900
ifcheck_timeout= 30
ipforwarding= on
iscaggregate= on
msg_compress_level= 3
ompnumthreads= 1
mssdecrease= 0
tcptunnel_establish= off
tunnel_virt_assignment= manual
cef_enabled= no
cef_port= 514
```

И прописываем туннель для Linux 1 и Linux 2

```
[id]
id= 0x1971000b
name= Coordinator-HW VPN-6513
ip= 192.168.20.1
ip= 30.30.30.2
tunnel= 192.168.20.2-192.168.20.2
```

```
[id]
id= 0x1971000a
name= Coordinator for Linux VPN-6513
ip= 30.30.30.3, 11.0.0.1
ip= 30.30.30.1, 11.1.0.1
ip= 172.16.1.1, 11.2.0.1
ip= 192.168.10.2, 11.3.0.1
accessip= 11.0.0.1
tunnel= 192.168.10.6-192.168.10.6 to 192.168.10.6-192.168.10.6
```

После всего запускаем `iplir`

Делаем так на всех Координаторах (на Coordinator-HW в будущем)

Делаем агрегированный канал

Поднимаем `eth1`

```
eth0 eth1 eth2 eth3
Coordinator-HW# inet ifconfig eth1 up
Attention: Upon changing the network interface settings, make similar changes to the services that use this interface
and then restart them.
Coordinator-HW#
```

Прописываем класс Slave для `eth0` и `eth 1`

```
Coordinator-НМ# inet ifconfig eth0 class
trunk access slave
Coordinator-НМ# inet ifconfig eth0 class slave
Attention: Upon changing the network interface settings, make similar changes to the services that use this interface
and then restart them.
All IP addresses and their aliases on eth0 interface will be removed. Continue? [Yes/No]: Yes
eth0 set to slave class.
Coordinator-НМ# inet ifconfig eth1 class slave
Attention: Upon changing the network interface settings, make similar changes to the services that use this interface
and then restart them.
eth1 set to slave class.
Coordinator-НМ#
```

Создаем агрегированный канал и выдаем на него IP-адрес

```
Coordinator-НМ# inet ifconfig bond0 address 30.30.30.2 netmask 255.255.255.248
```

Выключаем iplir и заходим в iplir config. Заменяем название eth0 на bond0. Затем запускаем iplir

```
[adapter]
name= bond0
allowtraffic= on
type= internal
```

Снова выключаем iplir и заходим в iplir config bond0

```
[db]
maxsize= 50 MBytes
timedif= 60
registerall= off
registerbroadcast= off
omittcpclientport= off
registerevents= on

[cef]
event= blocked
```

После всего выходим и запускаем ipcli и активируем bond0

```
Coordinator-HW# inet ifconfig bond0 up
Attention: Upon changing the network interface settings, make similar changes to the services that use this interface
and then restart them.
```

Проверяем

```
bond0: flags=5187<UP,BROADCAST,RUNNING,MASTER,MULTICAST> mtu 1500
inet 30.30.30.2 netmask 255.255.255.248 broadcast 30.30.30.7
ether 08:00:27:97:f4:74 txqueuelen 1000 (Ethernet)
RX packets 602 bytes 58622 (57.2 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 108 bytes 17905 (17.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

    Configured by DHCP: no
    Class: access

    Speed: 2000Mb/s
    Duplex: Full
    Auto-negotiation: off
    Link detected: yes

bond0 is a bond interface
mode: balance-rr
miimon: 100
primary: none
slave interfaces:
eth0 : up
eth1 : up
Coordinator-HW# inet ifconfig bond0 address 30.30.30.2 netmask 255.255.255.248
```

Создаем туннель для Linux 1 и Linux 2

Заходим в Coordinator на Linux и входим в режим администратора

```
[root@cm1 ~]# vipnet shell
Enter user password:
vpnshell> en
Enter administrator password:
vpnshell#
```

Проверим, существует ли по умолчанию правило фильтрации, разрешающий весь туннельный трафик

```
opnshell# firewall tunnel show
User:
+-----+-----+-----+-----+
|Num|Name|Option|Schedule|
+-----+-----+-----+-----+
|Act|Source|Destination|Protocol|
+-----+-----+-----+-----+
|1|To all tunnel nodes|User||
+-----+-----+-----+-----+
|pass|@any|@tunneledip|@any|
+-----+-----+-----+-----+
|2|From all tunnel nodes|User||
+-----+-----+-----+-----+
|pass|@tunneledip|@any|@any|
+-----+-----+-----+-----+
Default:
+-----+-----+-----+-----+
|Num|Name|Option|Schedule|
+-----+-----+-----+-----+
|Act|Source|Destination|Protocol|
+-----+-----+-----+-----+
|1|Block All Traffic|User||
+-----+-----+-----+-----+
|drop|@any|@any|@any|
+-----+-----+-----+-----+
opnshell#
```

Выходим, останавливаем демоны iplir, Failover и вносим изменения в параметр registerall=on на всех интерфейсах в iplir.conf-eth*

```
[root@cm1 ~]# iplir stop
Shutting down IpLir
[root@cm1 ~]# failover stop
Shutting down failover daemon
[root@cm1 ~]#
```

```
[root@cm1 user]# vi /etc/vipnet/user/iplir.conf-eth0_
```

```
[db]
maxsize= 50 MBytes
timedif= 60
registerall= on
registerbroadcast= off
omittcpclientport= off
registerevents= on
```

После настройки каждого интерфейса, сохраняем и запускаем iplir

```
[root@cm1 user]# iplir start
Loading Kernel Interface driver
Loading Iplir Watchdog driver
Loading IpLir Crypto driver
Loading IpLir driver
Loading IPCLS driver
Loading IpLir
[root@cm1 user]#
```

Снова отключаем и iplir и вводим команду

```
[root@cm1 user]# vi /etc/vipnet/user/iplir.conf
```

После чего добавляем такую строчку для id Coordinator for Linux (tunnel)

```
[id]
id= 0x1971000a
name= Coordinator for Linux
ip= 192.168.10.1
ip= 172.16.1.1
ip= 30.30.30.3
ip= 30.30.30.1
tunnel= 192.168.10.6-192.168.10.6
firewallip= 30.30.30.3
port= 55777
proxyid= 0x00000000
usefirewall= on
fixfirewall= off
tcptunnelport= 80
version= 3.0-670
```

Для id Coordinator-HW

```
[id]
id= 0x1971000b
name= Coordinator-HW
ip= 30.30.30.2, 11.0.0.1
ip= 192.168.20.1, 11.1.0.1
accessip= 30.30.30.2
tunnel= 192.168.20.2-192.168.20.2 to 192.168.20.2-192.168.20.2_
firewallip= 30.30.30.2
accessip= 30.30.30.2 auto 30.30.30.2 5 address
```

Сохраняем и запускаем iplir и Failover

После всего заходим в машину Главного Администратора в VipNet Client и видим что подключены к Coordinator-HW

Фильтрация незащищенного локального трафика На Coordinator-HW

```
Coordinator-HW# firewall local add src 192.168.20.2-192.168.20.5 dst 192.168.20.1 icmp pass
Coordinator-HW#
```

На Coordinator for Linux

```
root@cm1 ~]# vipnet shell
Enter user password:
upnshell> en
Enter administrator password:
upnshell# firewall local add src 192.168.10.6 dst 192.168.10.1 icmp pass
A rule was added:
Type:User ID:300007 local src 192.168.10.6 dst 192.168.10.1 service icmp:any pass Enabled
upnshell#
```

Фильтрация незащищенного транзитного трафика

На Coordinator for Linux

```
upnshell# firewall ip-object add name @myhost 192.168.10.6
A named object was added:
Type:User ID:1000056 ip-object name myhost including 192.168.10.6
upnshell# firewall ip-object add name @other 192.168.20.2
A named object was added:
Type:User ID:1000057 ip-object name other including 192.168.20.2
upnshell# firewall forward add src @myhost dst @any pass
A rule was added:
Type:User ID:300008 forward src @myhost dst @any service @any pass Enabled
upnshell# firewall forward add src @other dst @myhost pass
A rule was added:
Type:User ID:300009 forward src @other dst @myhost service @any pass Enabled
upnshell# _
```

На Coordinator-HW тоже самое

Прописываем фильтрацию туннельного трафика На машине Coordinator-HW

На машине Coordinator For Linux

```

[root@cn1 ~]# vipnet shell
Enter user password:
vpnshell> en
Enter administrator password:
vpnshell# firewall tunnel add src 192.168.10.6 dst 0x1971000b tcp dport 3389 pass
A rule was added:
Type:User ID:300004 tunnel src 192.168.10.6 dst 0x1971000b service tcp: to 3389 pass Enabled
vpnshell#

```

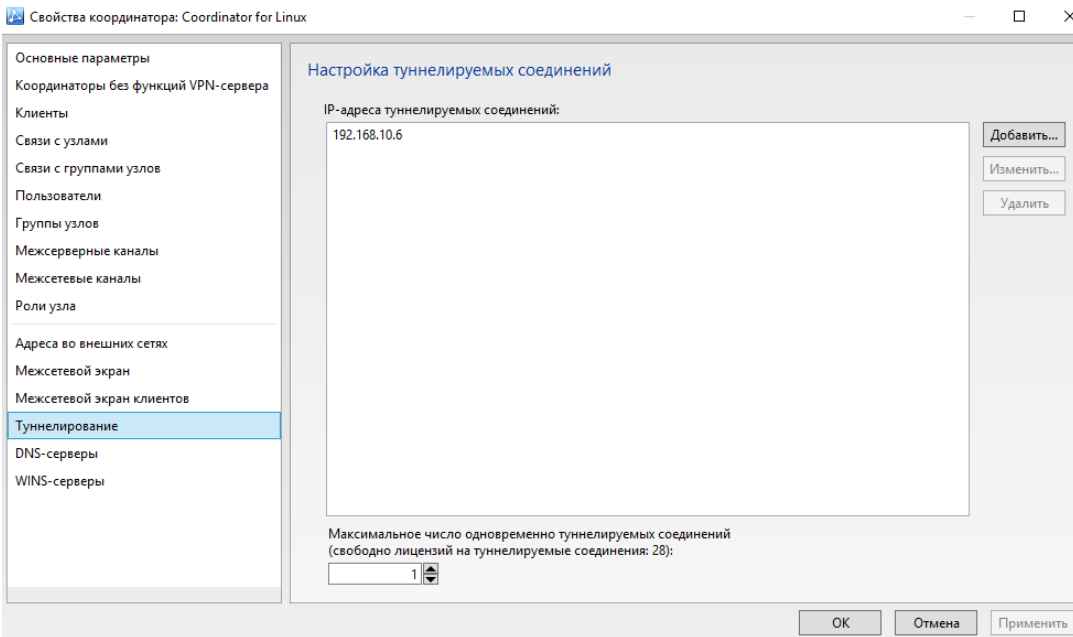
Включим и настроим OSPF на Coordinator-HW

```

Coordinator-HW#
Coordinator-HW# inet ospf mode on
Starting ospf ...
Coordinator-HW# inet ospf network add 30.30.30.0 netmask 255.255.255.248 area 0
The following OSPF network has been added:
Destination      Netmask          OSPF Area        Authentication
-----
30.30.30.0       255.255.255.248 0                 No
Coordinator-HW# inet ospf network add 192.168.20.0 netmask 255.255.255.248 area 1
The following OSPF network has been added:
Destination      Netmask          OSPF Area        Authentication
-----
192.168.20.0     255.255.255.248 1                 No
Coordinator-HW#
Coordinator-HW# inet ospf mode on
Starting ospf ...
Coordinator-HW# inet ospf network add 30.30.30.0 netmask 255.255.255.248 area 0
The following OSPF network has been added:
Destination      Netmask          OSPF Area        Authentication
-----
30.30.30.0       255.255.255.248 0                 No
Coordinator-HW# inet ospf network add 192.168.20.0 netmask 255.255.255.248 area 1
The following OSPF network has been added:
Destination      Netmask          OSPF Area        Authentication
-----
192.168.20.0     255.255.255.248 1                 No
Coordinator-HW# firewall local
show add delete move change
Coordinator-HW# firewall local add 0 rule "My_OSPF" src @any dst @local service @ospf pass
Error: Error while parsing command line. Column 19
'firewall local add 0 rule My_OSPF src @any dst @local service @ospf pass'
^ - here
Coordinator-HW# firewall local add 1 rule "My_OSPF" src @any dst @local service @ospf pass
Coordinator-HW# firewall local add 1 rule "My_OSPF" src @any dst @multicast service @ospf pass
Coordinator-HW# firewall local add 1 rule "My_OSPF" src @local dst @any service @ospf pass
Coordinator-HW#

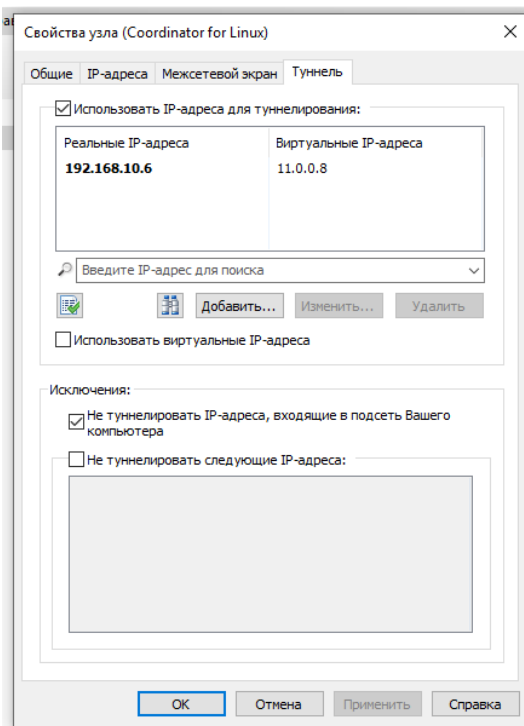
```

Заходим на машину Главного Администратора (ЦУС), пункт Координаторы и нажимаем на Coordinator for Linux, Туннелирование вписываем IP-адрес Linux 1 (если его нет) и выдаем лицензию



Так же делаем с Coordinator-HW
Создаем и отправляем справочники

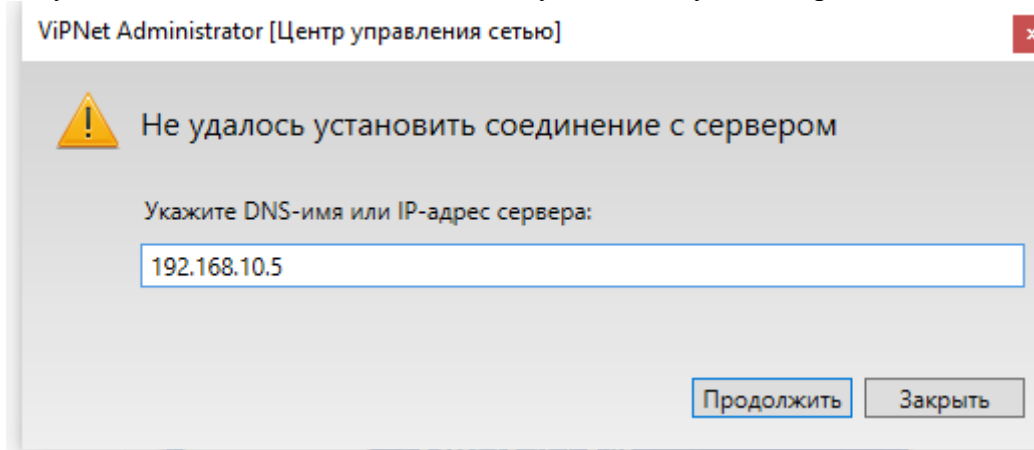
Затем заходим на машину Сотрудника Филиала, ViPNet Client, Нажимаем на Coordinator for Linux и у него появится вкладка Туннель и вводим (если нет Ip-адреса) адрес Linux 1



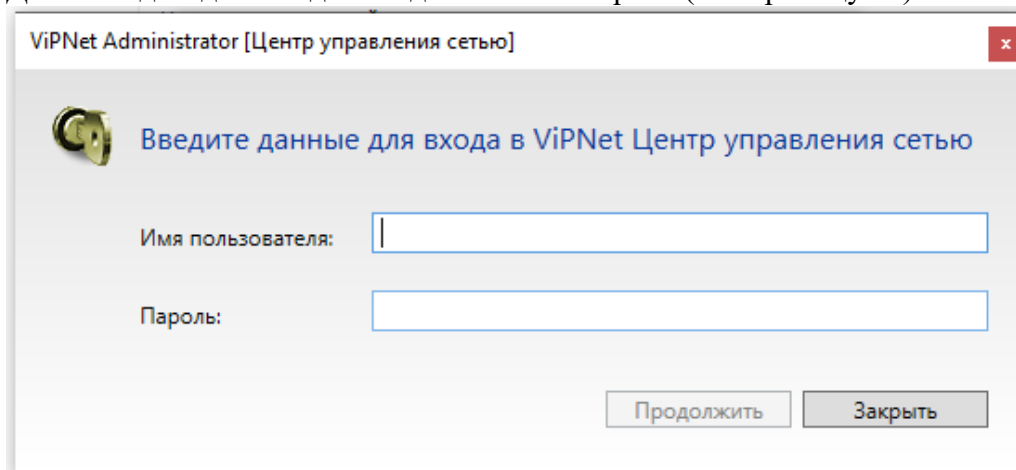
Настройка Помощника главного админа

Заходим в VirtualBox и в настройка машины Помощника главного администратора Сеть и настраиваем сеть. Запускаем. Выдаем IP-адрес. Устанавливаем на него ПО ViPNet Administrator Центр управление сетью (только клиент) и ViPNet Client. Выдать дистрибутив для Помощника главного админа

Запускаем ЦУС. Он выдает нам ошибку. Вводим туда IP-адрес Главного Администратора



Далее вводим данные для входа и меняем пароль (см страницу 23)

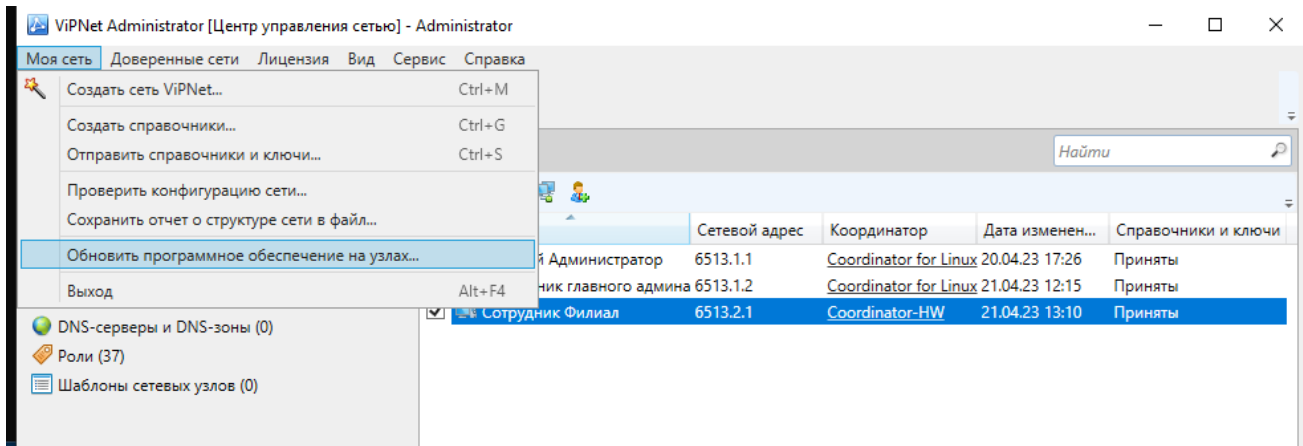


Настройка Сотрудника Филиала

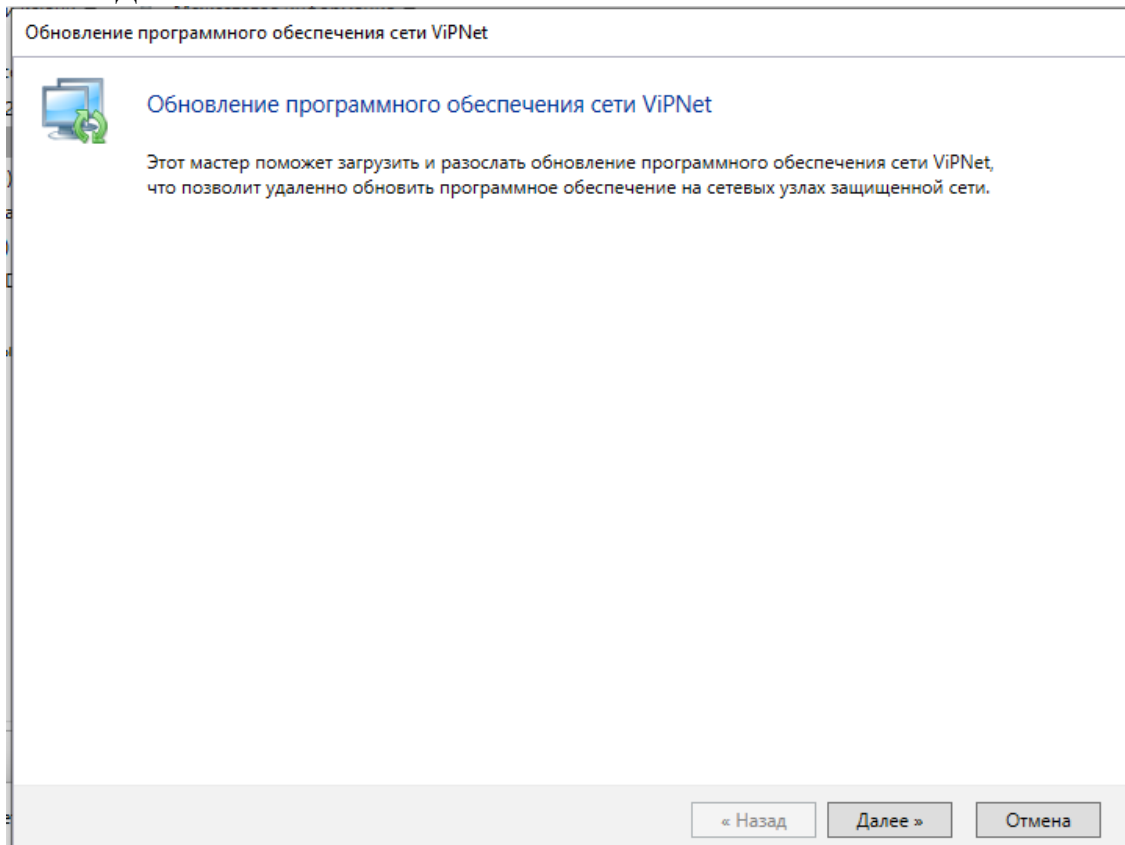
Заходим в VirtualBox и в настройка машины Сотрудник Филиал Сеть и настраиваем сеть. Запускаем. Выдаем IP-адрес. Устанавливаем на него ПО ViPNet Client версией 4.5.3.65090. Выдать дистрибутив для Сотрудника Филиала

Удаленное обновление ПО ViPNet Client на машине Сотрудник Филиал с версии Client`а 4.5.3.65090 на версию 4.5.3.65.117

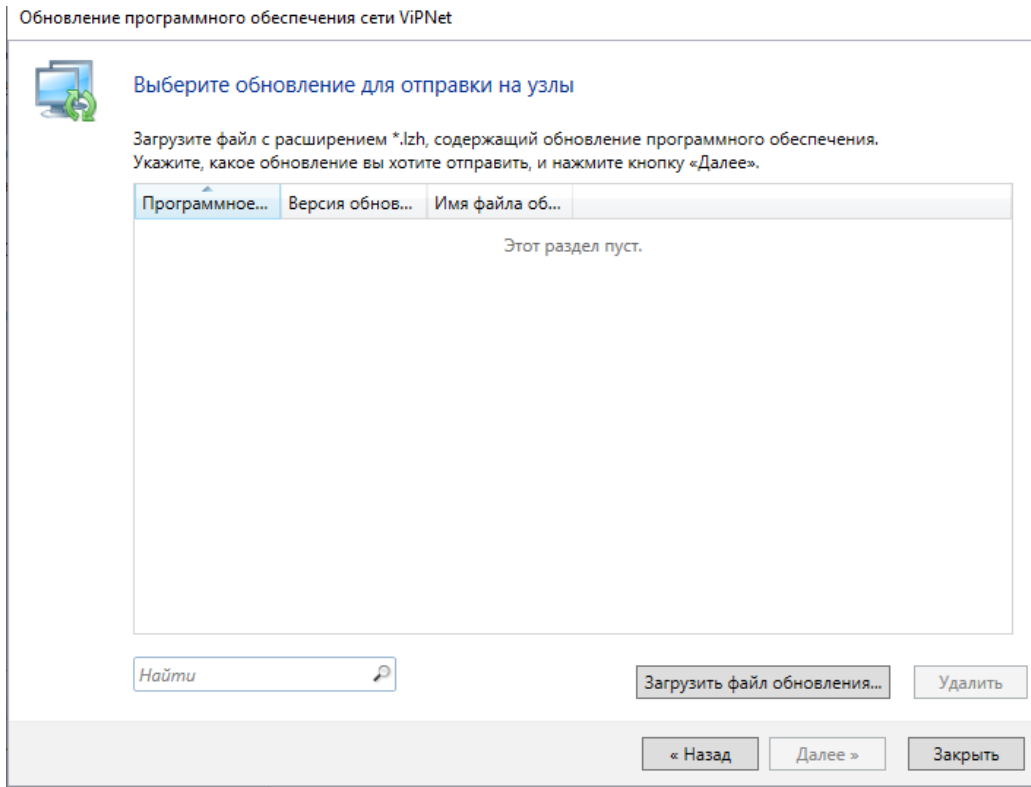
Заходим на машину Главного Администратора. Нажимаем моя сеть и обновить ПО на узлах



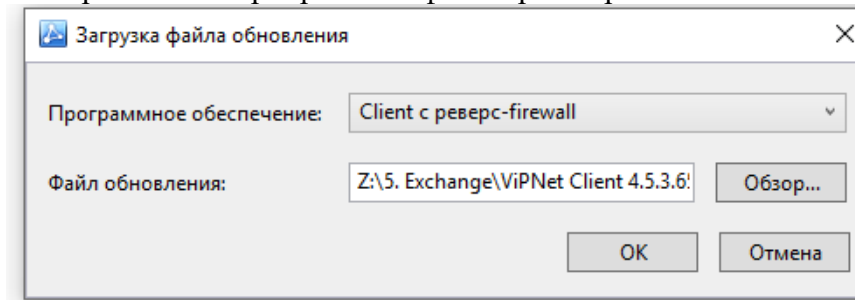
Нажать Далее



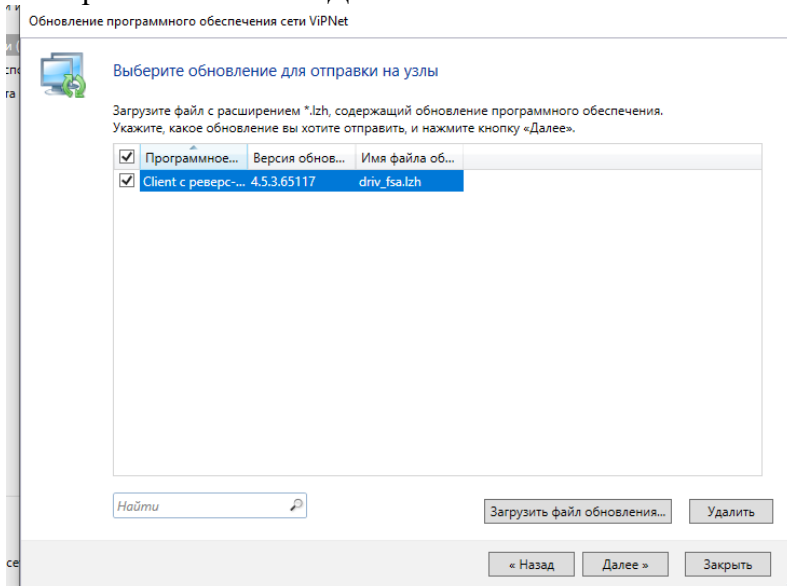
Загружаем файл обновления



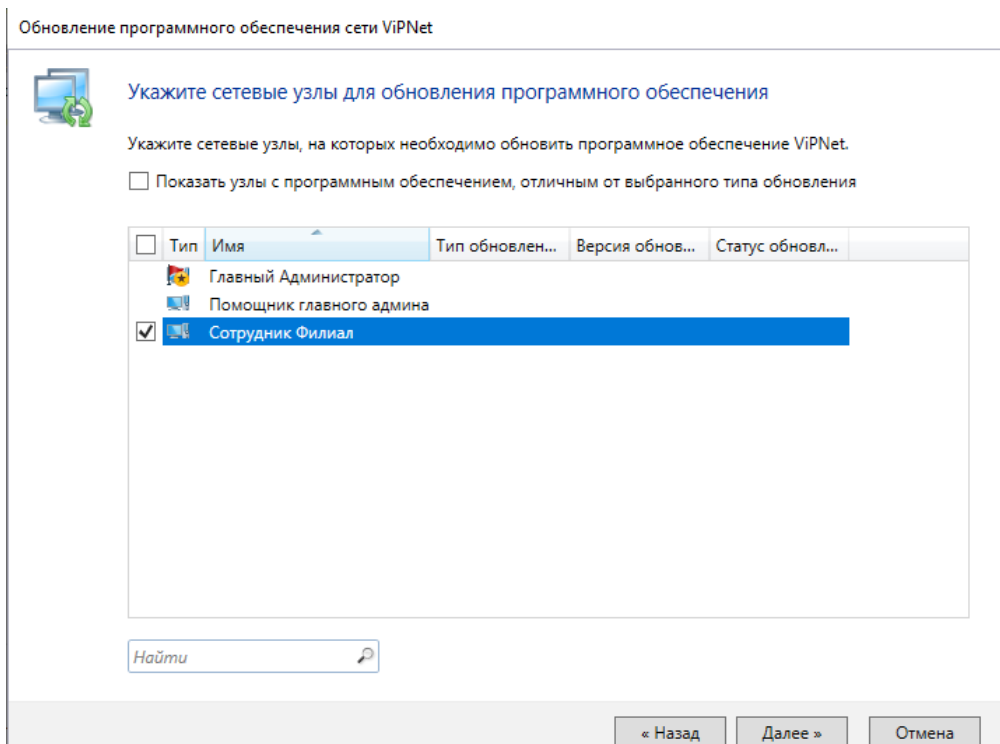
Выбираем ПО и прикрепляем файл с расширением .lzh VIPNet Client`а 4.5.365117



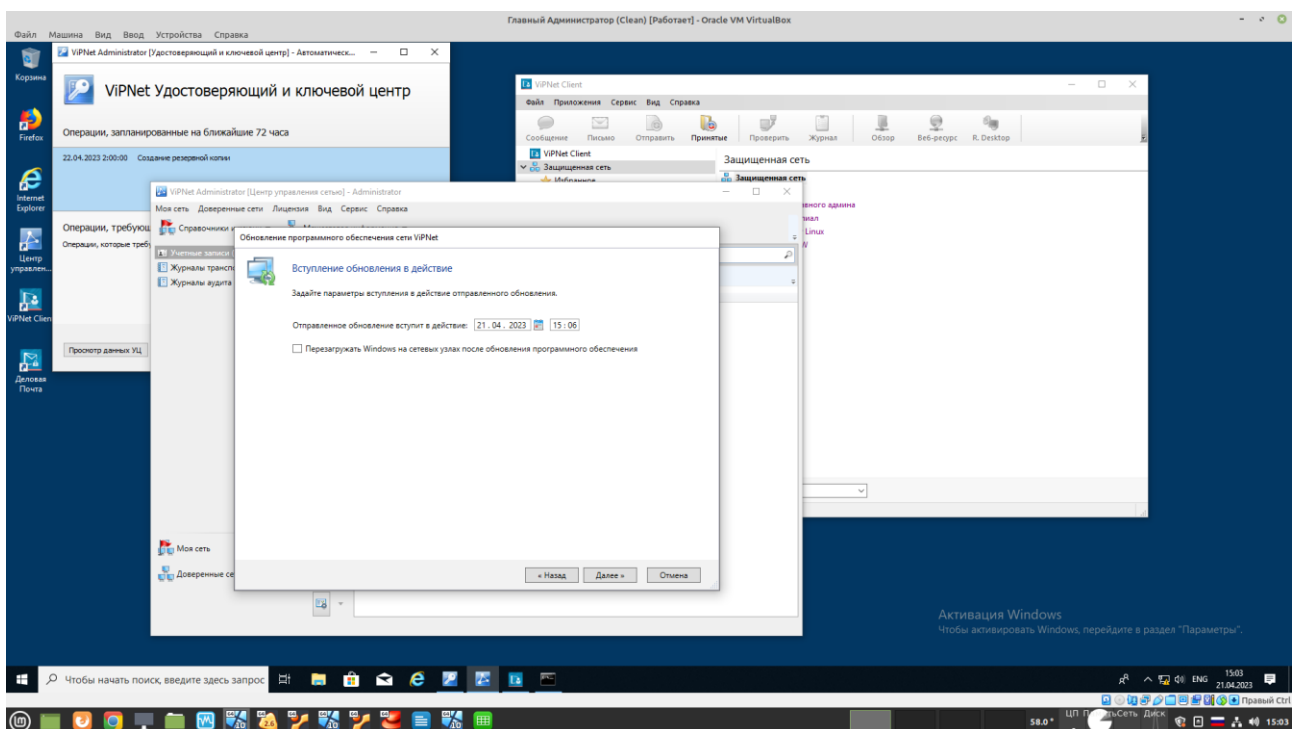
Выбираем и нажимаем Далее



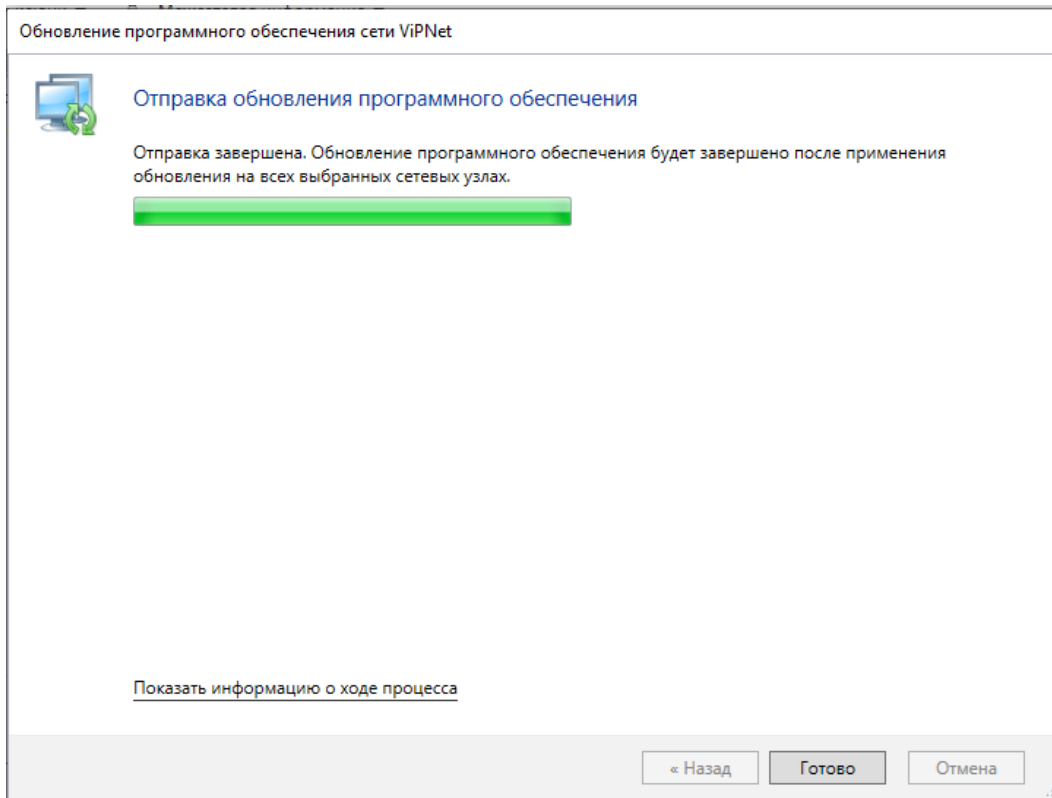
Выбираем узел на котором необходимо обновить ПО (в данном случае это Сотрудник Филиал). Нажимаем Далее



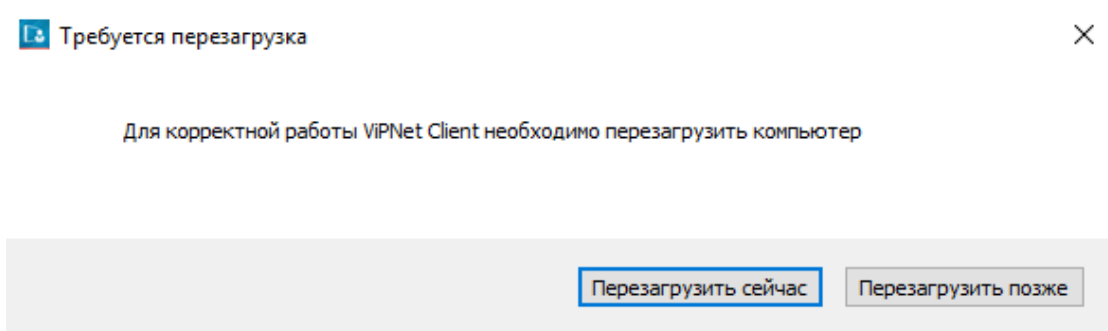
Вводим ближайшее время с запасом и нажимаем Далее



После того как он отправил, нажимаем Готово



На машине Сотрудник Филиал появится окно. Нажимаем перезагрузить сейчас



В Client нажимаем файл → Свойства моего узла и проверяем

