

Важно! Пункты методички, будут отличаться от задания, поэтому перед выполнением задания стоит ознакомиться.

Все пароли, сети и имена сетевых узлов, пользователей и координаторов, так же имена ВМ будут отличаться от методички, корректные сведения будут в задании.

IP адреса защищенных сетей

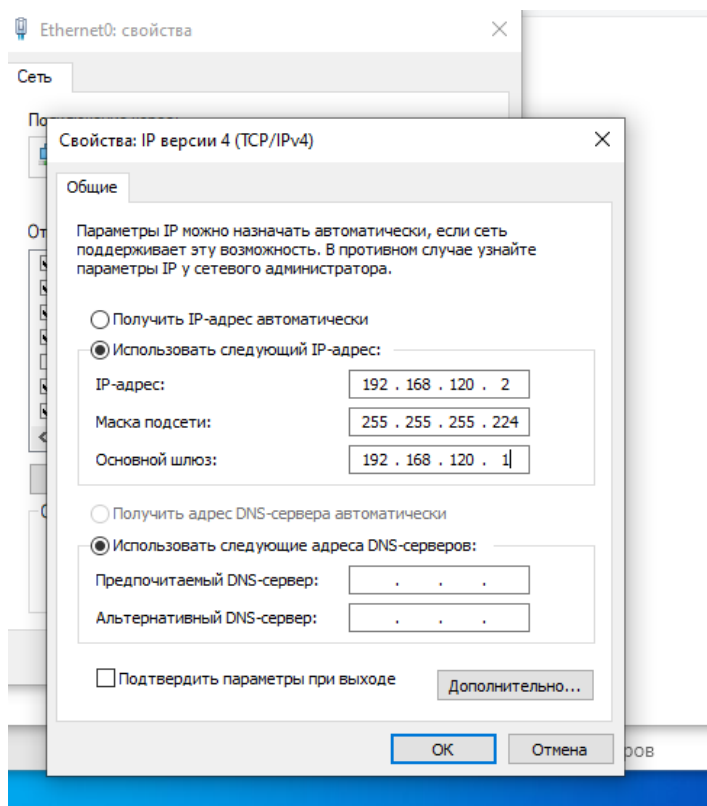
- Центральный офис «Сеть 1 ЦО»: 192.168.120.0/27
- Офис филиал «Сеть 1 Филиал»: 10.10.20.0/25
- Офис сеть 2 «Сеть 2 Офис»: 172.22.10.0/26
- «Интернет» для всех координаторов: 198.18.20.0/20

Адреса выбираются самостоятельно из указанного диапазона.

На незащищенных узлах отключить firewall

1. Установить базу данных MSSQL на ВМ Net1-DB (незащищенный узел).

1.1 При включении ВМ, на которую будет установлена БД, следует зайти в настройки сети и установить следующие параметра. Также установить часовой пояс и изменить время, как на хостовой машине.

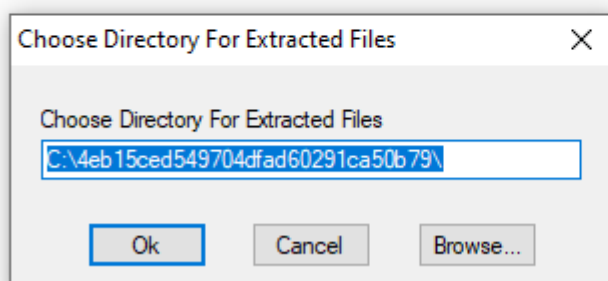


Обратить внимание! Шлюзом указывается IP координатора внутри сети.

1.2 Следующим шагом будет **отключение брандмауэра**. Сочетанием клавиш win + r вызываем окно, в котором приписывается firewall.cpl и далее отключаем все профиля.

1.3 Для того, чтобы установить БД, нужно перейти в папку «Packages» и найти «SqlExpress», запустить exe'шник для 64 битной системы.

Имя	Дата изменения	Тип	Размер
SQLEXPR_x64_ENU	19.09.2022 12:02	Папка с файлами	
SQLEXPR_x64_ENU	11.02.2020 8:01	Приложение	311 283 КБ
SQLEXPR_x86_ENU	11.02.2020 8:00	Приложение	271 493 КБ



1.4 На первом этапе нужно выбрать установщик новой базы данных.



[New SQL Server stand-alone installation or add features to an existing installation](#)

Launch a wizard to install SQL Server 2014 in a non-clustered environment or to add features to an existing SQL Server 2014 instance.

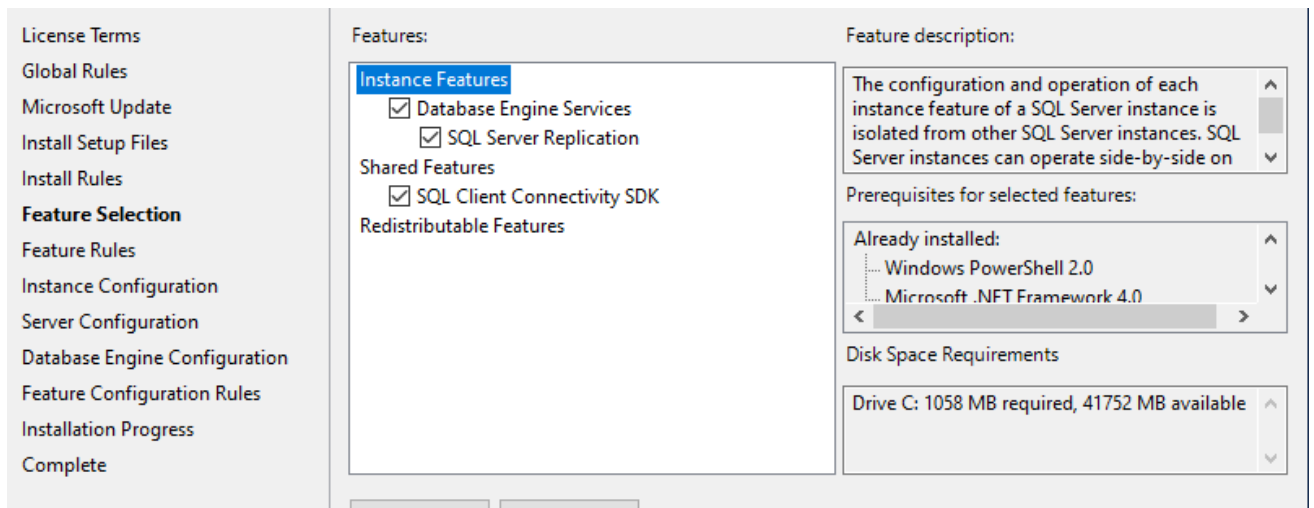
1.5 Устанавливаем галочку в лицензионном соглашении и переходим далее.



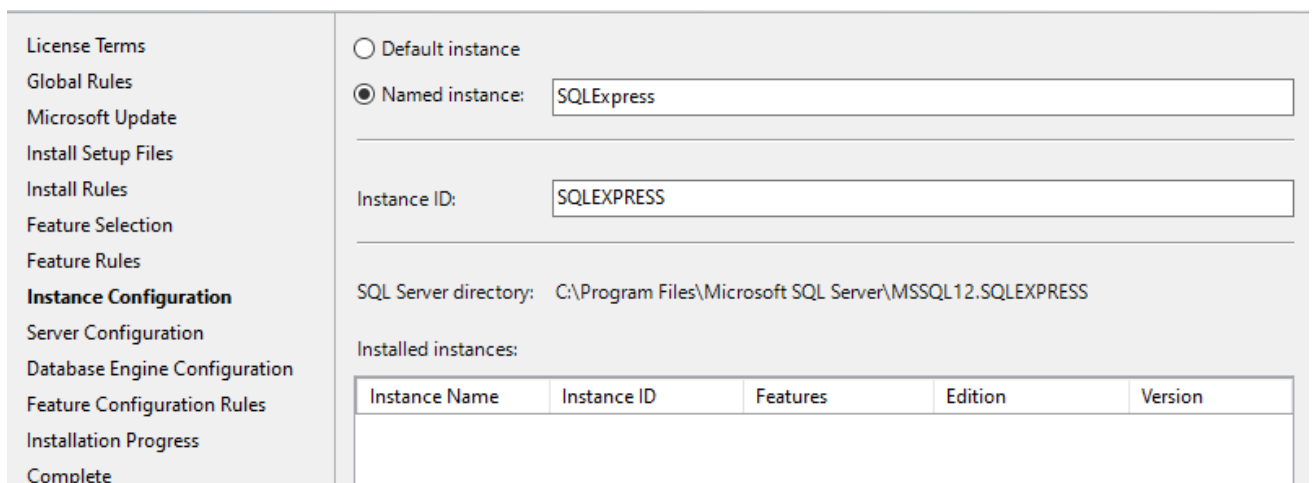
1.6 В окне «Microsoft Update» оставить все по умолчанию (т.е. не ставить галочку для проверки обновлений).

1.7 В окне «Product Updates» просто перейти далее.

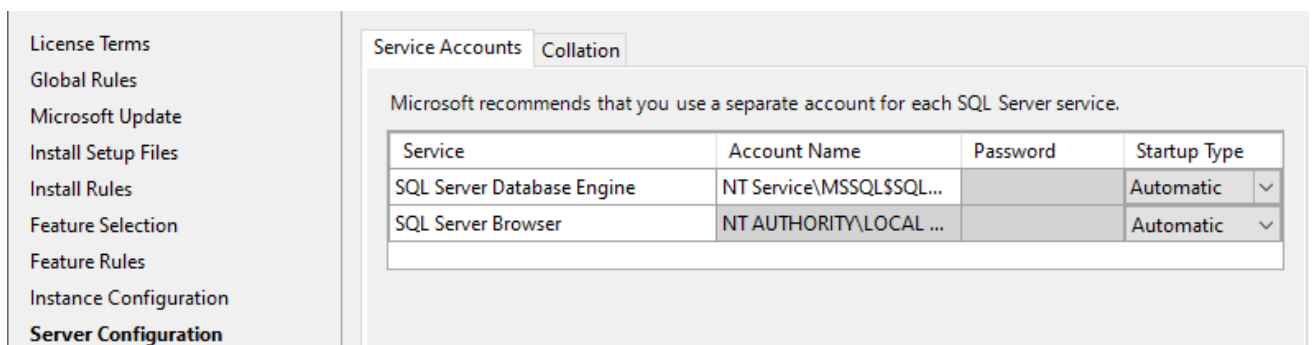
1.8 В окне «feature Selection» оставить все по умолчанию.



1.9 В окне «Instance Configuration» можно задать любое название БД на латинице. Рекомендуется! В строке «Named instance» и «Instance ID» записывать одинаковое название БД.



1.10 В окне «Server Configuration» установить все сервисы на автоматический запуск



1.11 В окне «Database Engine Configuration» в вкладке «Sever Configuration» установить «Mixed Mod» и установить пароль администратора БД (sa). Перейти в вкладку «FILESTREAM» и установить галочки везде.

Feature selection

- Feature Rules
- Instance Configuration
- Server Configuration
- Database Engine Configuration**
- Feature Configuration Rules
- Installation Progress
- Complete

☒ **Mixed Mode** (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account. _____

Enter password:

Confirm password:

Specify SQL Server administrators _____

DESKTOP-2QKRGAB\Net1-DB (Net1-DB)	SQL Server administrators have unrestricted access
-----------------------------------	--

Server Configuration | Data Directories | User Instances | **FILESTREAM**

☒ Enable FILESTREAM for Transact-SQL access

☒ Enable FILESTREAM for file I/O access

Windows share name:

☒ Allow remote clients access to FILESTREAM data

1.12 После начнется установка БД.

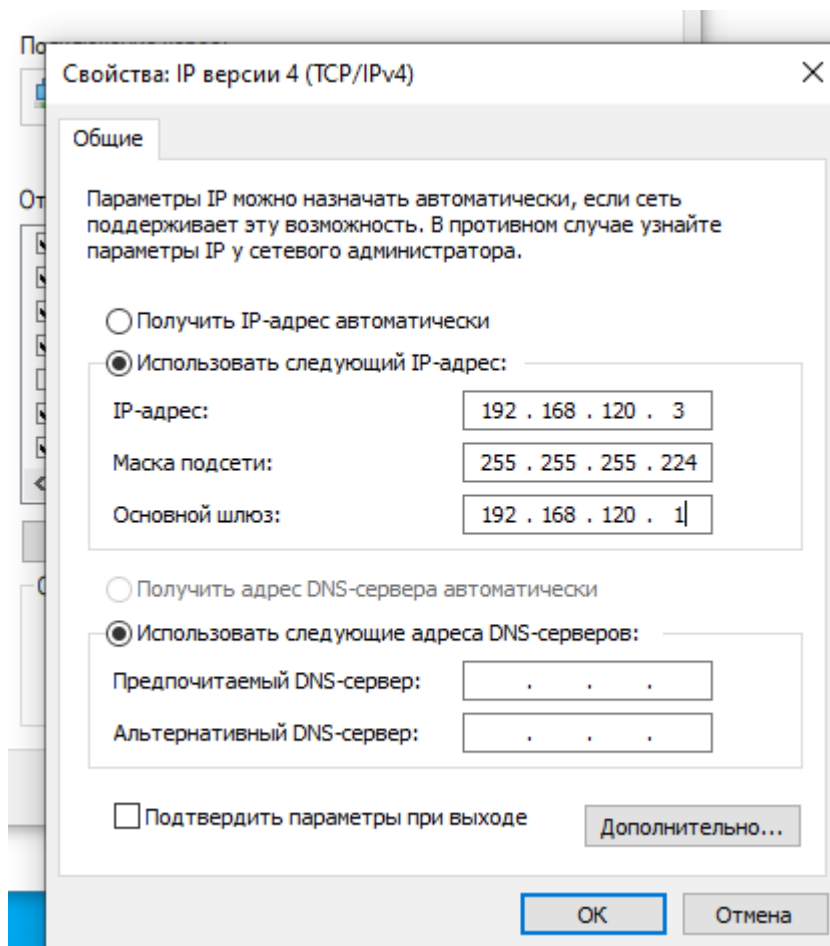
1.13 В строке поиска прописывает «manager» и запускаем. Следует просмотреть все протоколы БД, на каждом должен быть установлен статус «Enabled», если же статус иной, поменять на «Enabled».

1.14 Перезагружаем виртуальную машину.

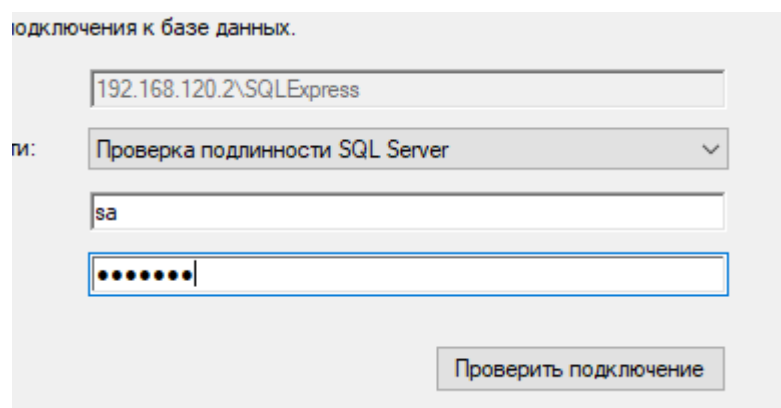
2. Установить и настроить рабочее место администратора Certification Authority (на базе виртуальной машины Net1-Admin (ЦО)): Центр управления сетью (серверное приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ); использовать ранее установленную БД.

Установить клиент ЦУС на ВМ Net1-DB (незащищенный узел).

2.1 При настройке рабочего места администратора, нужно начать с настройки времени и часового пояса, также параметров сети.



2.2 Следующим шагом будет установка серверной части ЦУС. В параметрах подключения к БД, указывает IP адрес незащищенного узла \ название БД. Проверку подлинности изменить с Windows на SQL Server. В строке имя пользователя указать системного администратора БД (sa) и его пароль (п. 1.14). Проверить подключение. Если проверка подключения прошла успешно, продолжить установку.

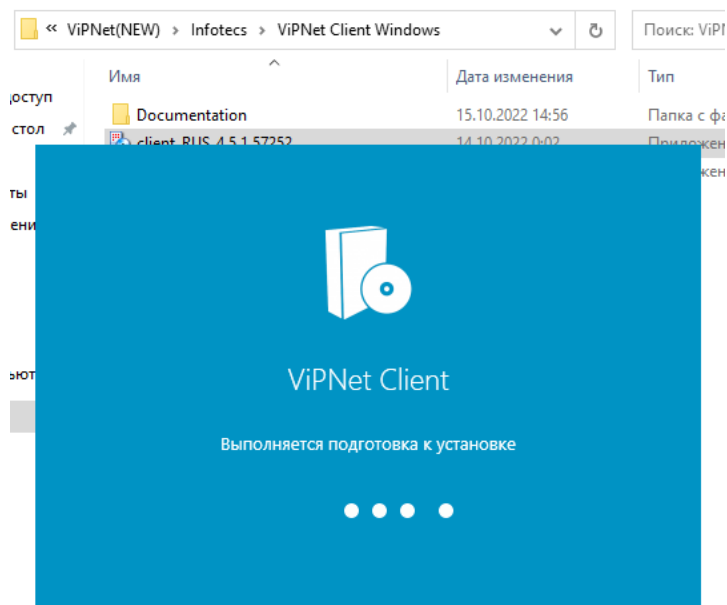


2.3 Установить ЦУС клиент на Net1-Admin и Net1-DB (незащищенный узел)

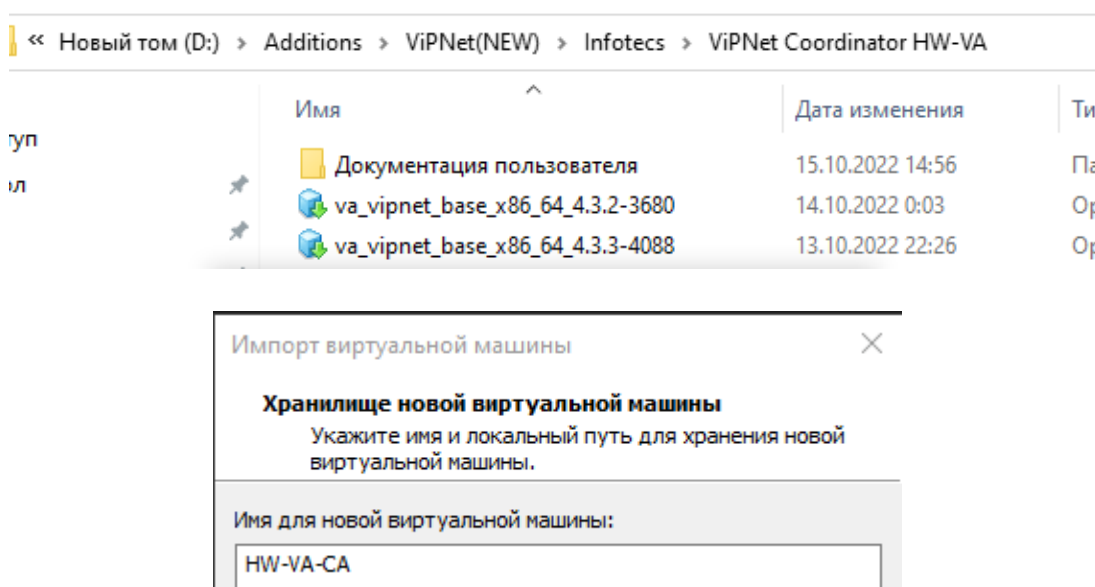
2.4 Установить УКЦ.

3 Установка ПО VPN Coordinator и ПО VPN Client для Certification Authority
 На компьютере на Net1-AdminCA (ЦО) установить ПО Client (Пользовательская или серверная ОС), рабочее место администратора;
 На компьютере на Net1-CoordCA (ЦО) установить ПО Coordinator (Пользовательская или серверная ОС).

3.1 На Net1-AdminCA запустить установщик Client. Выполнить установку и не устанавливая ключи в завершении установки.



3.2 Запустить OVA образ самой новой версии координатора. На скриншоте снизу представлен путь. Запускать образ на хостовой машине



Внимание! Перед запуском ВМ с координатором, обратить внимание, чтобы сетевые адаптеры соответствовали другим ВМ.

Задание 4. Установка центра регистрации, сервиса публикации и сервиса информирования Certification Authority на соответствующие виртуальные машины.

На компьютере на Net1-OperatorCA (ЦО) установить ПО Client (Пользовательская или серверная ОС).

На компьютере на Net1-OperatorCA (ЦО) установить ПО Publication Service.

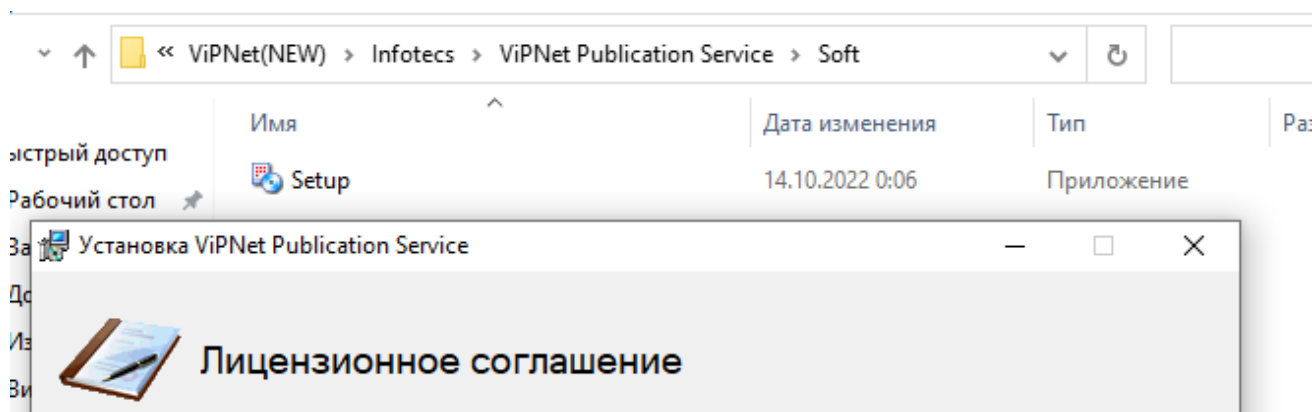
На компьютере на Net1-OperatorCA (ЦО) установить ПО Registration Point.

На компьютере на Net1-AdminCA (ЦО) установить ПО CA Informing.

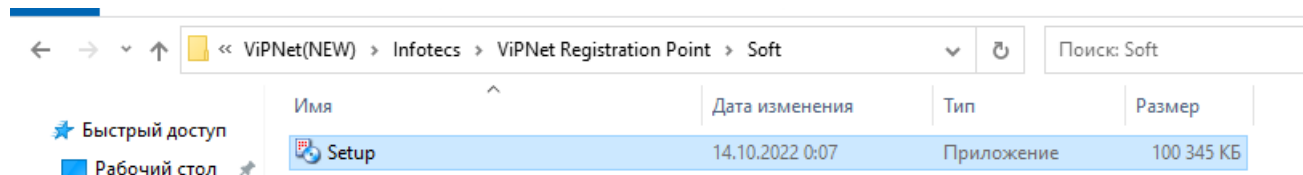
4.1 Начать настройку машины OperatorCA аналогично предыдущим (т.е. настройки сети, времени и часового пояса).

4.2 На машине OperatorCA запустить установку Клиента (п. 3.1).

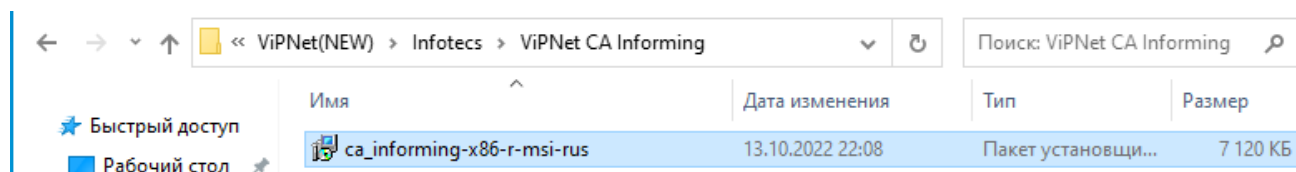
4.3 На машине OperatorCA запустить установку Сервиса публикаций.



4.4 На машине OperatorCA запустить установку Сервиса регистрации



4.5 На машине AdminCA запустить установку CA Informing



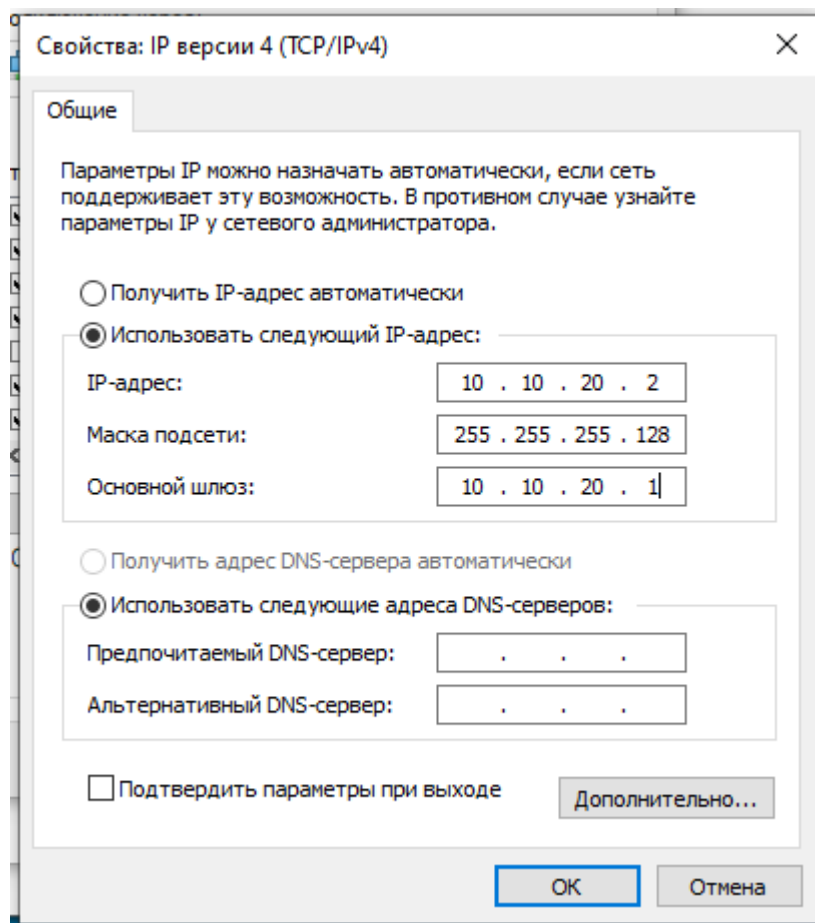
Задание 5 Установка ПО Coordinator и ПО Client для организации сети филиала
На компьютере на Net2-Coord (Филиал) установить ПО Coordinator (Пользовательская или серверная ОС).

На ВМ на Net2-Client (филиал) установить ПО Client, рабочее место пользователя.

Для организации сети филиала используется другая сеть. Адреса находятся на первой странице.

5.1 Запустить OVA образ (см. п. 3.2).

5.2 Настроить на Net2-Client параметры сети, время и часовой пояс.



5.3 Запустить установку клиента (см. п. 3.1).

Задание 6. Развертывание удостоверяющего центра в составе защищенной сети.

Необходимо использовать рабочее место администратора (созданное ранее) для создания структуры защищенной сети, развернуть с помощью технологии виртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями.

Схема сети, которую требуется создать, приведена далее.

IP адреса сетей перечислены в начале задания (по названию сетей).

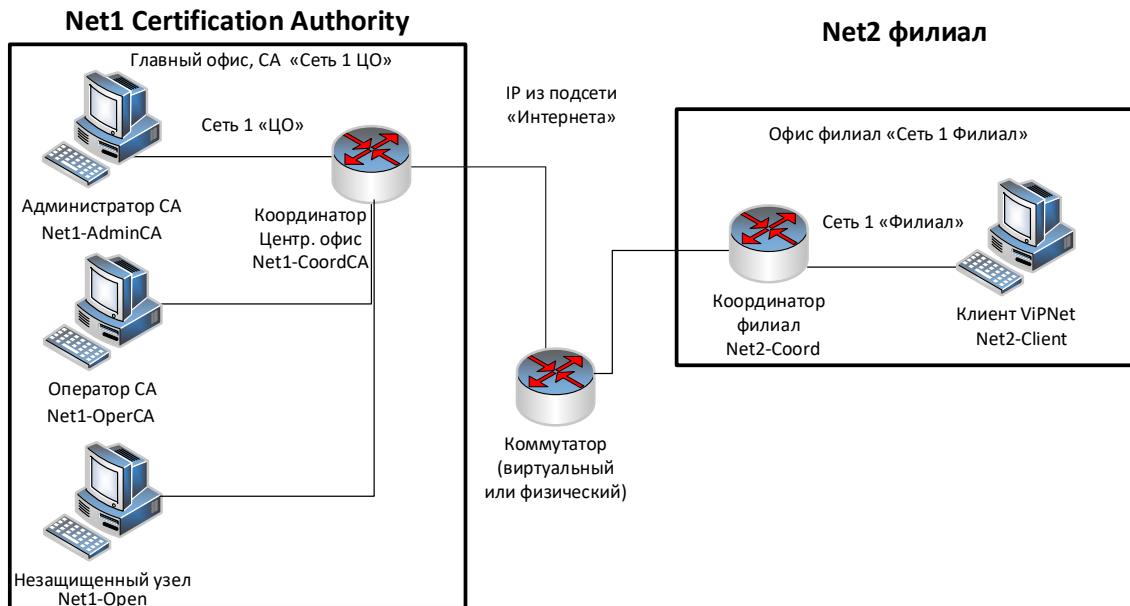


Схема защищенной сети

В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети (см. таблицу).

Таблица 1 Узлы защищенной сети если УКЦ и ЦУС на одной машине

Вирт. машина	Название сетевого узла	ПО	ОС сетевого узла	Имя пользователя сетевого узла, уровень полномочий
Net1-AdminCA (ЦО)	Главный администратор (VM)	Administrator (ЦУС клиент и сервер + УКЦ), Client, CA Informing	Пользовательская или серверная ОС	AdminCA
Net1-CoordCA (ЦО)	Координатор Центр Офис (VM)	Coordinator	HW-VA	CoordinatorCA
Net1-OperatorCA (ЦО)	Оператор УЦ (VM)	Client, Publication Service, Registration Point	Пользовательская или серверная ОС	OperatorCA
Net2-Coord (Филиал)	Координатор Филиал (VM)	Coordinator	Пользовательская или серверная ОС	CoordinatorSub
Net2-Client (филиал)	Пользователь_2 Филиал (VM)	Client	Пользовательская или серверная ОС	UserCli

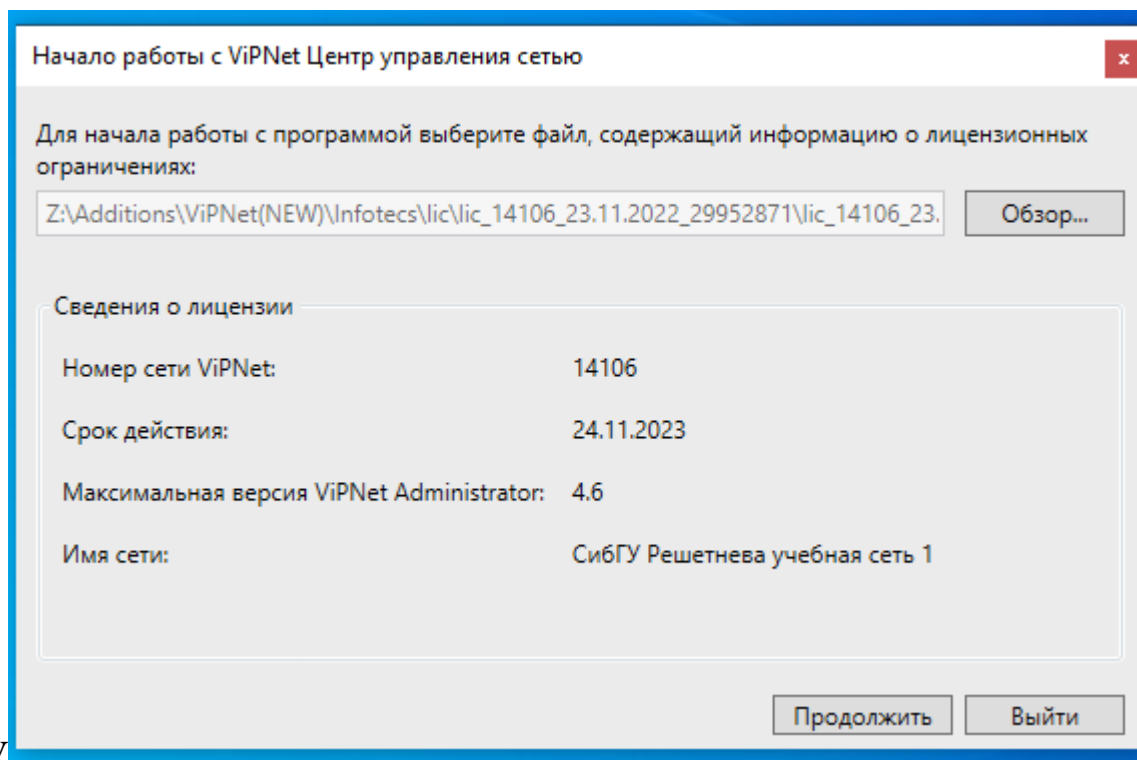
Связи между узлами необходимо настроить самостоятельно.

Таблица 2. Схема связей пользователей

Схема связей пользователей	Coordinator Office	Admin	OperatorCA	Coordinator Subsidiary	UserCli
CoordinatorOffice	×	*	*	*	
Admin	*	×	*		*
OperatorCA	*	*	×	*	
CoordinatorSub	*		*	×	*
UserCli		*		*	×

6.1 Запустить ЦУС. При первом запуске пароль и логин Administrator. Задайте новый пароль.

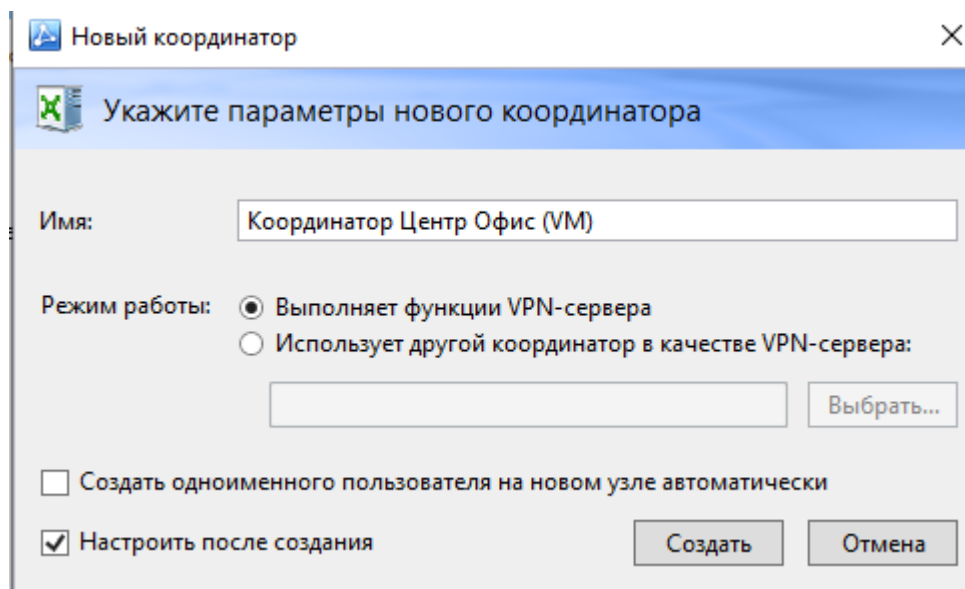
6.2 Выбрать лицензию.




.У

6.3 Выбрать настройку структуры сети самостоятельно.

6.4 Во вкладке «Координаторы», создать координаторы в соответствии с таблицей 1.



6.5 Удаляем все роли и добавляем «Coordinator HW-VA».

Роли координатора			
<input type="checkbox"/>	Имя	Максимальна...	Срок действия
	Coordinator HW-VA	Не ограничено	Не ограничено

6.6 Добавить адреса координатора во внешних и внутренних сетях.

Настройка адресации координатора во внешних сетях

IP-адреса, зарегистрированные на координаторе

192.168.120.1
198.18.20.1

Добавить...
Изменить...
Использовать для MFTP
Удалить

Аналогично создать координатор для филиала.

Новый координатор

Укажите параметры нового координатора


Имя:

Режим работы: ☒ Выполняет функции VPN-сервера
☐ Использует другой координатор в качестве VPN-сервера:

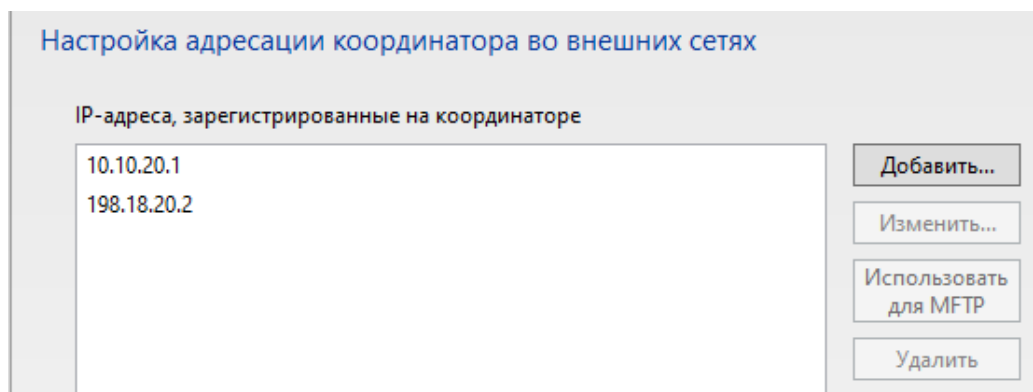
☐ Создать одноименного пользователя на новом узле автоматически

☒ Настроить после создания

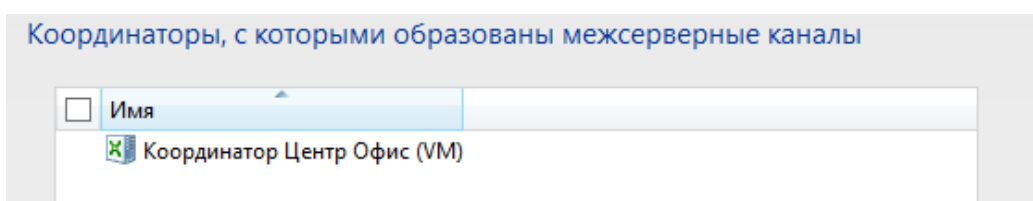
Добавить роль.

Роли координатора			
<input type="checkbox"/>	Имя	Максимальна...	Срок действия
	Coordinator HW-VA	Не ограничено	Не ограничено

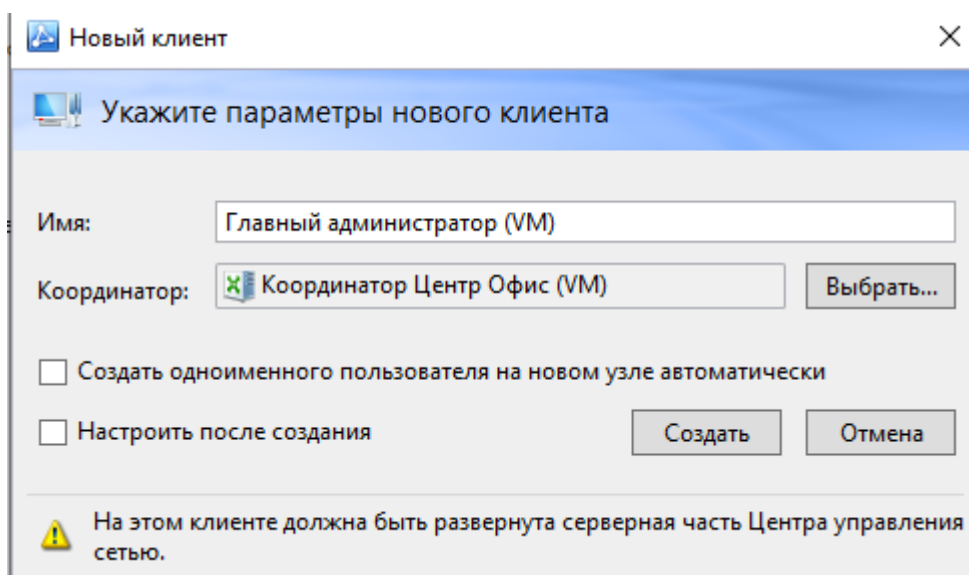
Добавить адреса.



Добавить межсерверный канал.



6.7 Создать сетевые узлы для сети в соответствии с таблицей 1.




Для сетевого узла Оператор УЦ добавить роль «Registration Point»

Новый клиент

Укажите параметры нового клиента

Имя:

Координатор: 

☐ Создать одноименного пользователя на новом узле автоматически

☐ Настроить после создания


Выбор объектов

<input type="checkbox"/>	Имя	Свободные лицензии	Максимальна...	Срок действия
<input type="checkbox"/>	DNS-Сервер	Не ограничено	Не ограничено	Не ограничено
<input type="checkbox"/>	Policy Manager	1	Не ограничено	Не ограничено
<input checked="" type="checkbox"/>	Registration Point 1	Не ограничено	Не ограничено	Не ограничено
<input type="checkbox"/>	StateWatcher	1	Не ограничено	Не ограничено
<input type="checkbox"/>	WINS-Сервер	Не ограничено	Не ограничено	Не ограничено

Новый клиент

Укажите параметры нового клиента

Имя:

Координатор: 

☐ Создать одноименного пользователя на новом узле автоматически

☐ Настроить после создания

Обратить внимание! Каждый сетевой узел закрепляется к координатору, за которым находится!

6.8 Создать пользователей в соответствии с таблицей 1.

Новый пользователь

Укажите параметры нового пользователя

Имя: AdminCA

Сетевой узел: Главный администратор (VM) Выбрать...

☐ Настроить после создания Создать Отмена

Новый пользователь

Укажите параметры нового пользователя

Имя: CoordinatorCA

Сетевой узел: Координатор Центр Офис (VM) Выбрать...

☐ Настроить после создания Создать Отмена

Новый пользователь

Укажите параметры нового пользователя

Имя: OperatorCA

Сетевой узел: Оператор УЦ (VM) Выбрать...

☐ Настроить после создания Создать Отмена

Новый пользователь

Укажите параметры нового пользователя

Имя: CoordinatorSub

Сетевой узел: Координатор Филиал (VM) Выбрать...

☐ Настроить после создания Создать Отмена

Новый пользователь

Укажите параметры нового пользователя

Имя: UserCli

Сетевой узел: Пользователь_2 Филиал (VM) Выбрать...

☐ Настроить после создания Создать Отмена

6.9 Создать связь с пользователями в соответствии с таблицей 2.
Связь отвечает за взаимодействие между клиентами сети.

Свойства пользователя: CoordinatorCA

Пользователи, с которыми установлена связь

Имя	Сеть	Статус связи
AdminCA	СибГУ Решетне...	Связь с пользователем своей сети
CoordinatorSub	СибГУ Решетне...	Связь с пользователем своей сети
OperatorCA	СибГУ Решетне...	Связь с пользователем своей сети

Свойства пользователя: AdminCA

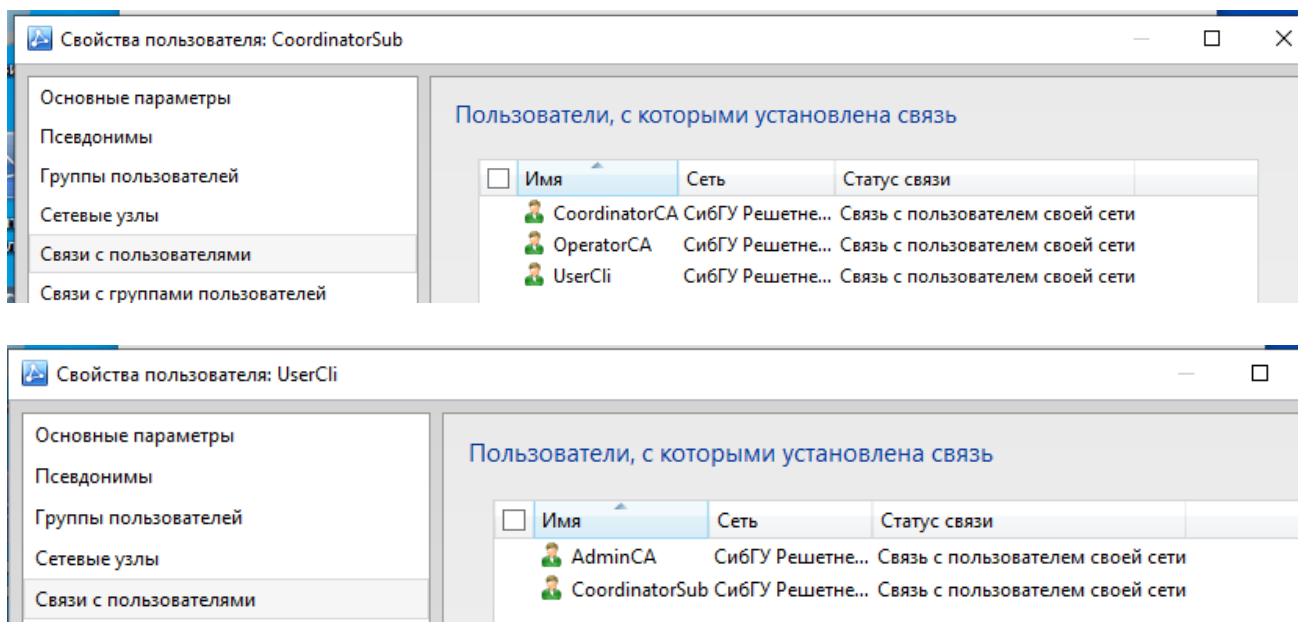
Пользователи, с которыми установлена связь

Имя	Сеть	Статус связи
CoordinatorCA	СибГУ Решетне...	Связь с пользователем своей сети
OperatorCA	СибГУ Решетне...	Связь с пользователем своей сети
UserCli	СибГУ Решетне...	Связь с пользователем своей сети

Свойства пользователя: OperatorCA

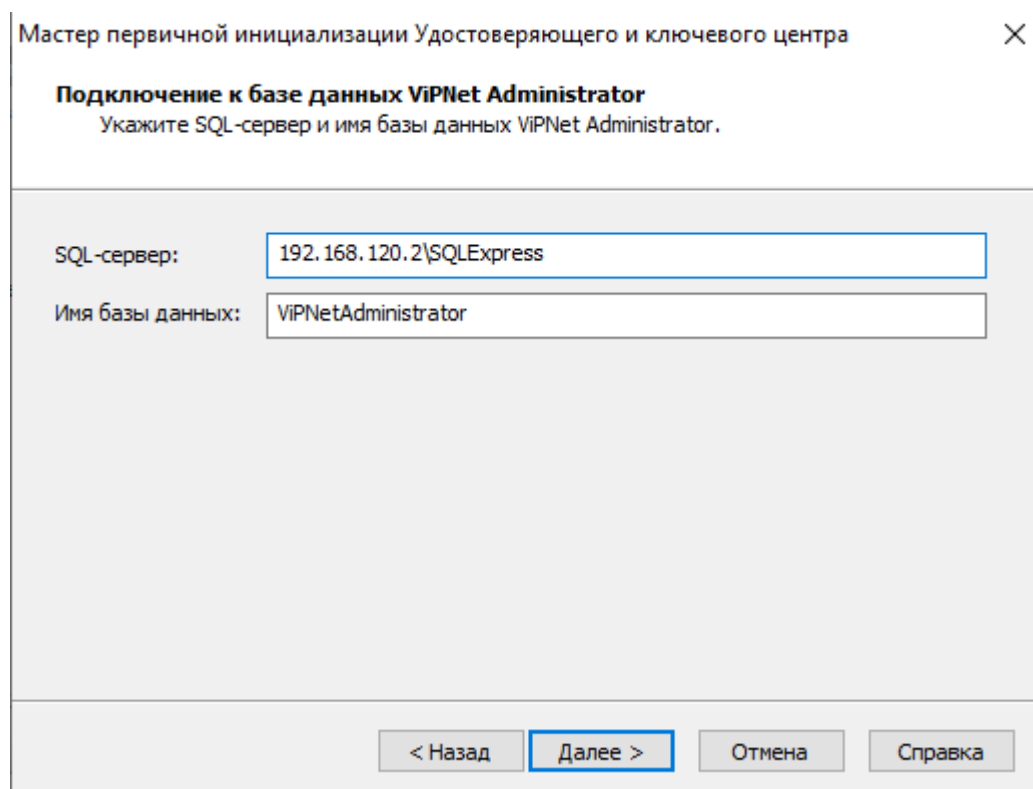
Пользователи, с которыми установлена связь

Имя	Сеть	Статус связи
AdminCA	СибГУ Решетне...	Связь с пользователем своей сети
CoordinatorCA	СибГУ Решетне...	Связь с пользователем своей сети
CoordinatorSub	СибГУ Решетне...	Связь с пользователем своей сети



Далее создаем справочники и переходим к настройке УКЦ.

6.10 Первый запуск УКЦ. Настраиваем новую БД. В окне подключения к БД в строке SQL-сервер прописываем IP\имя базы данных, имя БД оставить по умолчанию.



Настройку подлинности пользователя оставить по умолчанию. При удачном подключении будет переход к следующему этапу.

Ввести имя администратора AdminCA.

Мастер первичной инициализации Удостоверяющего и ключевого центра

Создание администратора сети ViPNet

Введите имя администратора сети ViPNet.

AdminCA

В соответствии с пунктом 7.2 заполнить сведения о владельце сертификата.

Мастер первичной инициализации Удостоверяющего и ключевого центра

Сведения о владельце сертификата

Заполните сведения о владельце запрашиваемого сертификата.

Имя:	AdminCA
Фамилия:	
Приобретенное имя:	
ИНН:	
СНИЛС:	
Электронная почта:	AdminCA@DemoVip.lab

< Назад Далее > Отмена Справка

Мастер первичной инициализации Удостоверяющего и ключевого центра

Сведения о владельце сертификата
Заполните сведения о владельце запрашиваемого сертификата.

Город: Москва

Область: Московская

Страна: RU ...

Адрес, улица:

< Назад Далее > Отмена Справка

Мастер первичной инициализации Удостоверяющего и ключевого центра

Сведения о владельце сертификата
Заполните сведения о владельце запрашиваемого сертификата.

Организация: WorldSkills

ОГРН:

Подразделение: IT-отдел

Должность: Администратор

< Назад Далее > Отмена Справка

Мастер первичной инициализации Удостоверяющего и ключевого центра

Дополнительные сведения о владельце сертификата
Укажите дополнительные сведения о владельце сертификата.

Атрибуты	Значения
Неструктурированное имя	
Инициалы	
Компонента доменного имени	
Неструктурированный адрес	
Телефон	
Департамент	
ОГРНИП	
Описание	
Почтовый индекс	112344
Почтовый ящик	

Изменить

< Назад Далее > Отмена Справка

Важно! Нужно будет настроить УКЦ в аккредитованном режиме, можно настроить после первичной инициализации или после.

В параметрах настройки пароля, указать «Собственный пароль».

Мастер первичной инициализации Удостоверяющего и ключевого центра

Настройка паролей
Укажите тип паролей, который будет использоваться для создания новых паролей, а также способ выдачи паролей пользователям.

Тип создаваемого пароля:

☒ Собственный пароль

☐ Случайный пароль на основе парольной фразы

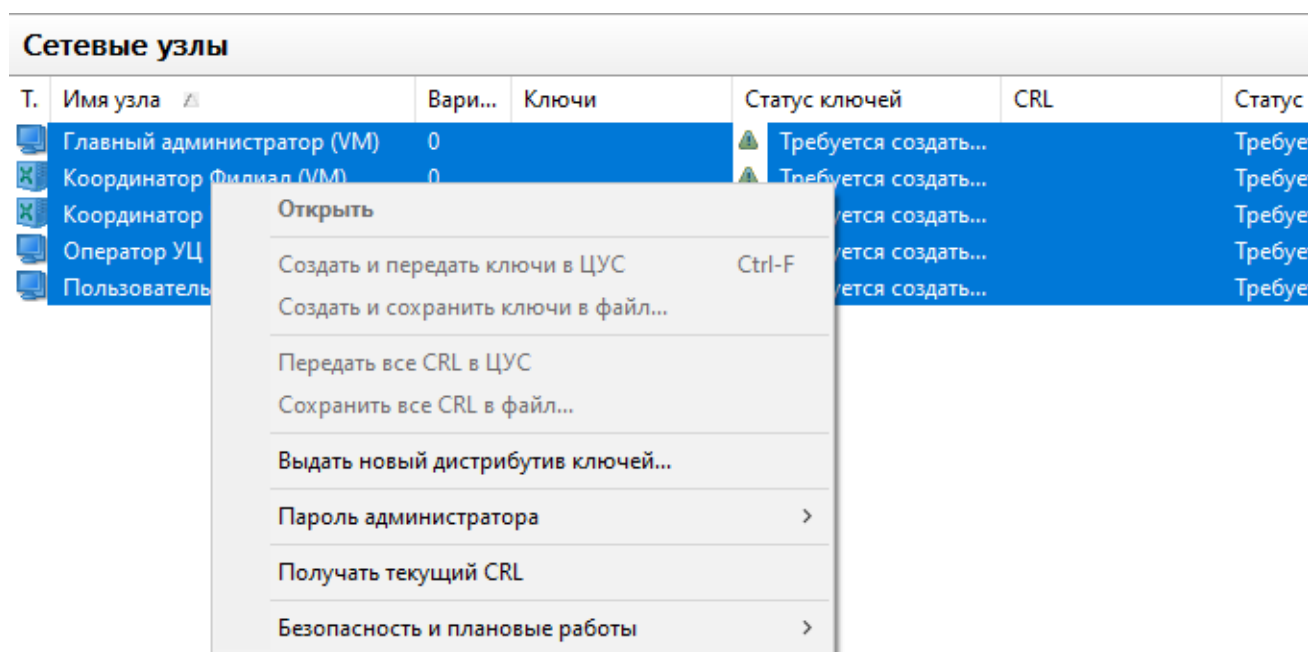
Способ выдачи пароля пользователя:

☒ Сохранять пароль в файл XPS в папку:

C:\ProgramData\InfoTeCS\VIPNet Administrator\KC\Export\Authentication Users ...

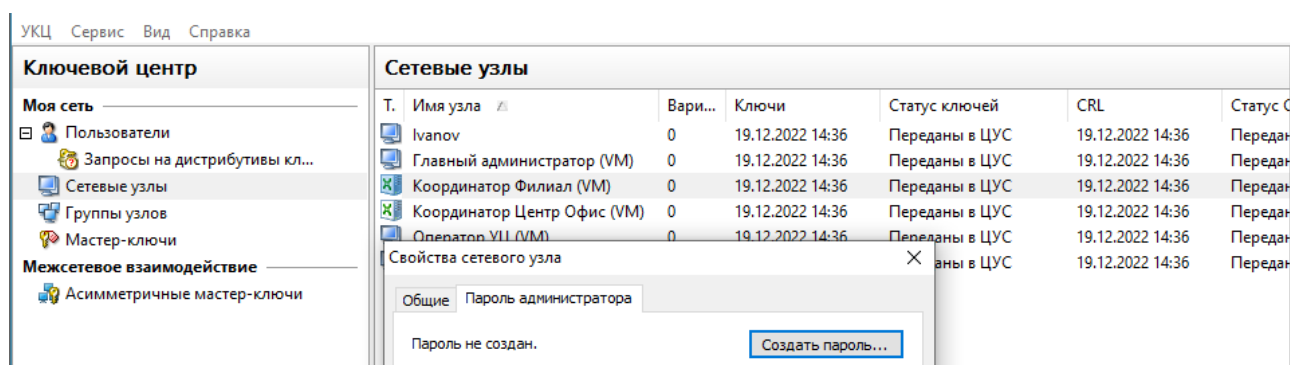
Все последующие пункты оставлять по умолчанию и завершить установку.

6.11 После настройки УКЦ следует выпустить dst-ключи для сетевых узлов. Перейти в вкладку «Сетевые узлы» и создать новый дистрибутив ключей.



Помнить! Все пароли пользователей и администраторов сети прописаны в условии задания!

Важно! Установить пароль администратора для каждого координатора



После оставляем все последующие параметры по умолчанию и создаем пароли пользователей

Помнить! Все пароли пользователей и администраторов сети прописаны в условии задания!

6.12 Разнести dst-файлы по сетевым узлам (скачать созданные dst-файлы на флеш-накопитель или в общую папку и установить их в программе ViPNet Client).

6.13. Открыть методичку HW-VA и произвести настройку координатора. Также можно сразу развернуть и настроить второй координатор сети и настроить взаимодействие между узлами сетей (см. схему защищённой сети).

Задание 7 Создание структуры защищенной сети.

ЦУС. Необходимо создать в ЦУС структуру защищенной сети в соответствии с заданной схемой (выгрузить отчет в HTML). Создать пользователей узлов, настроить полномочия пользователей и их связи в соответствии со схемой.

УКЦ. Провести инициализацию УКЦ, сохранить контейнер ключей администратора в общей папке (создать подпапку Задание 1.6), поменять тип паролей для пользователей («собственный»). Задать пароли пользователей и сохранить в текстовый файл. Сформировать дистрибутивы ключей для всех сетевых узлов (сохранить на жесткий диск). Создать группы узлов для центрального офиса (удостоверяющего центра) и филиала, настроить пароль администратора группы сетевых узлов для каждой из групп (проверить, что пароль работает).

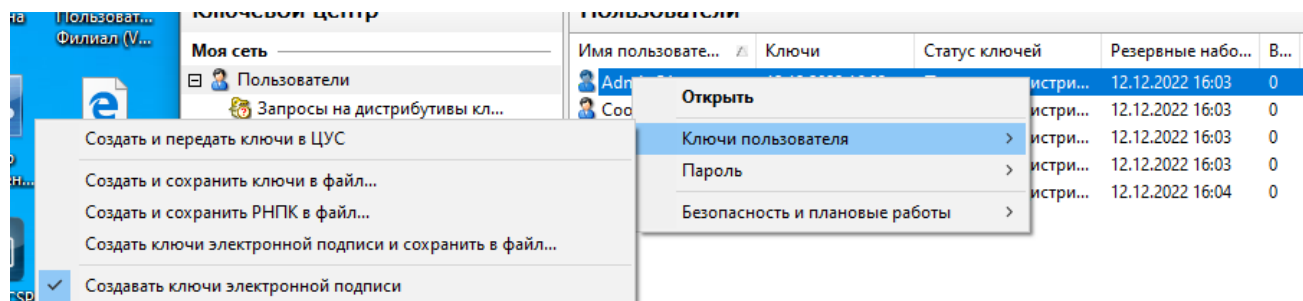
На всех узлах сети корректно настроить или проверить корректность настройки сетевых интерфейсов в соответствии со схемой, проверить доступность соседних узлов.

Разнести DST файлы по АРМ, провести первичную инициализацию узлов защищенной сети (координаторов и клиентов), проверить доступность узлов защищенной сети и сделать скриншоты работоспособности узлов.

7.1 ЦУС. Поскольку пользователи узлов и полномочия пользователей, и их связи были настроены, нужно создать в ЦУС структуру защищенной сети.

Запускаем ЦУС и сверху в пункте «Моя сеть» выбрать «Сохранить отчет о структуре сети в файл». Стоит обратить внимание на тип, в котором просят выгрузить файл. Сохраняем на рабочий стол.

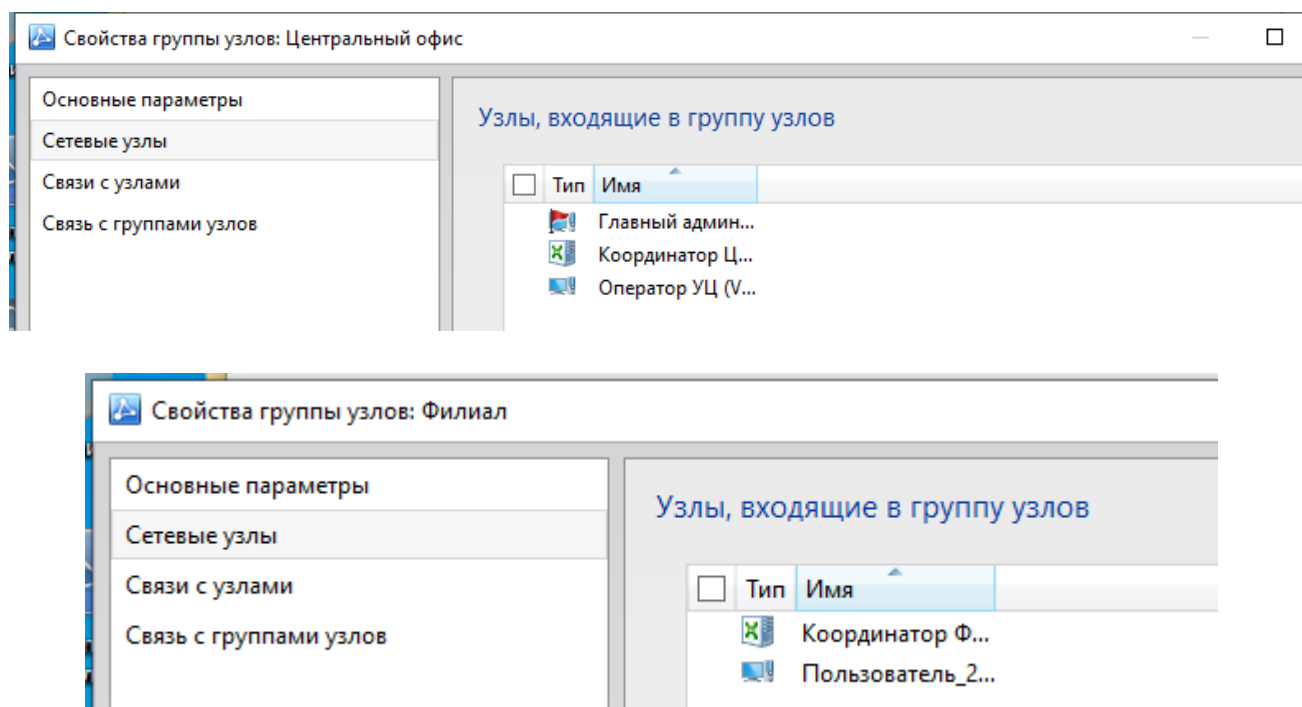
7.2 УКЦ. Инициализация была выполнена. Для того, чтобы сохранить контейнер ключей администратора в общей папке, нужно перейти в «Пользователи» выбрать администратора, ПКМ – «Ключи пользователя» - «Создать ключи электронной подписи и ...».



Пароль типа «Собственный» был установлен во время первичной инициализации УКЦ. Однако, для настройки типа пароля, нужно перейти в «Настройки» и вкладка «Пароли». После того как все пароли были заданы, нужно просто создать текстовый документ и записать в нем имя пользователя + пароль (пример, AdminCA - *****).

Дистрибутивы ключей для сетевых узлов уже были сформированы и сохранены на жесткий диск (для удобства можно скопировать на рабочий стол)

Для того чтобы создать группу узлов, нужно перейти в ЦУС – «Группа узлов» - «Создать новую группу узлов» (пользователи, прикрепленные за координатором СА, то есть центрального офиса, попадают в группу центральный офис, пользователи филиала, в группу филиала).



Для настройки пароля администратора для групп сетевых узлов, нужно перейти в УКЦ – «группы узлов» и создать пароль администратора отдельно для каждой группы. Чтобы проверить пароль администратора на сетевом узле, нужно перейти в «Клиент» - «Файл» - «Войти в режим администратор». Для проверки на координаторе, ввести enable и после пароль администратора.

7.3 Для проверки сети и доступности узлов, достаточно открыть «Клиент» выбрать сетевой узел и отправить сообщение, затем в обратную сторону.

Внимание! После какого-либо изменения структуры сети, первым делом нужно создать справочники в ЦУС, в УКЦ создать ключи и направить в ЦУС, после этого отправить справочники и ключи по сетевым узлам!

Однако, если происходит компрометация пользователя или смена мастер-ключа, то отправлять все обновления на узлы НЕЛЬЗЯ!

Задание 8 Настройка работы удостоверяющего центра в аккредитованном режиме

Необходимо перевести УКЦ в режим аккредитованного удостоверяющего центра, настроить параметры издания квалифицированных сертификатов, указав:

- сведения о средствах УЦ

- средство электронной подписи издателя: CSP
- средства удостоверяющего центра: ПК УЦ 4
- сертификат на средство электронной подписи издателя: Сертификат DemoVip.lab.crt
- сертификат на средство удостоверяющего центра: Сертификат DemoVip.lab.p7b
- класс защищенности, которому соответствуют программные средства УЦ,
- место хранения контейнеров ключа ЭП и ключа защиты УКЦ (файл на диске).

После перевода УКЦ в аккредитованный режим необходимо выпустить:

- Корневой квалифицированный сертификат. Назначить текущим.
- Квалифицированную электронную подпись для пользователя Admin. Выдать с новым дистрибутивом ключей.
- Квалифицированную электронную подпись для пользователя Client. Сохранить электронные ключи в файл.

При формировании сертификатов необходимо заполнить следующие поля:

- Имя: <Имя пользователя или узла>
- Электронная почта: <Имя пользователя>@DemoVip.lab
- Город: Москва
- Область: Московская
- Организация: WorldSkills
- Подразделение: ИТ-отдел
- Почтовый индекс: 112344

7.1 Для того, чтобы настроить УКЦ в аккредитованном режиме, необходимо в УКЦ перейти в «Настройки» - «Программные средства» и поставить галочку «Функционировать в режиме ...».

«Средства удостоверяющего центра» и «Средство электронной подписи владельцев сертификатов» в соответствии с параметрами издания квалифицированных сертификатов.

Средства удостоверяющего центра

Программные средства Сертификаты соответствия Класс защищенности

Укажите наименование криптографического средства, которое используется для создания электронной подписи издателя, а также наименование программного средства, используемого для реализации функций удостоверяющего центра.

Средство электронной подписи издателя:

CSP

Средство удостоверяющего центра:

ПК УЦ 4

OK Отмена Справка

Средства удостоверяющего центра

Программные средства Сертификаты соответствия Класс защищенности

Укажите номера сертификатов соответствия средства электронной подписи издателя и средства удостоверяющего центра требованиям контролирующих органов. Сертификаты предоставляются вашим поставщиком программного обеспечения.

Сертификат на средство электронной подписи издателя:

Сертификат DemoVip.lab.crt

Сертификат на средство удостоверяющего центра:

Сертификат DemoVip.lab.p7b

OK Отмена Справка


Средства удостоверяющего центра

Программные средства Сертификаты соответствия Класс защищенности

Укажите класс защищенности, которому соответствует используемое программное обеспечение:

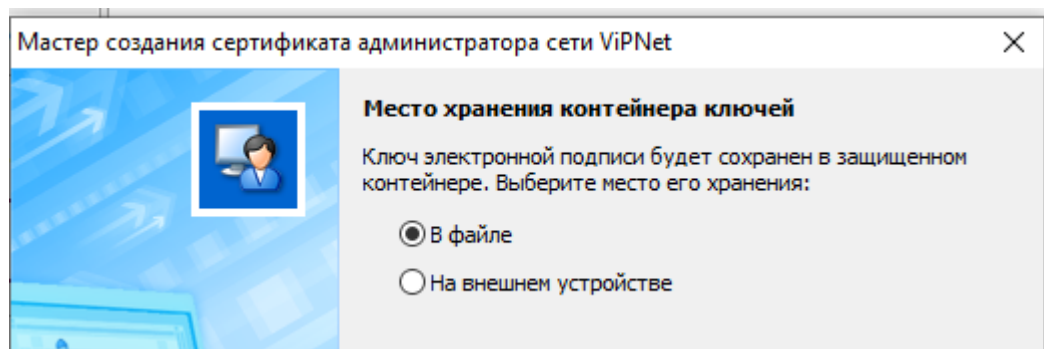
☒ КС2 и ниже

☐ КС3 и ниже

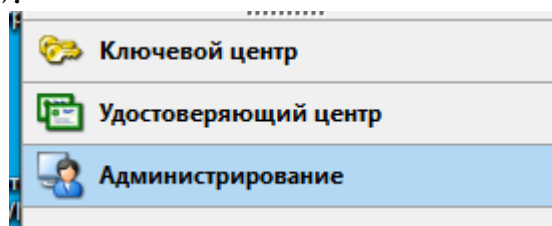
 Согласно выбранному выше классу в издаваемые квалифицированные сертификаты будут добавляться нужные политики классов защищенности.

OK Отмена Справка

Место хранения контейнеров ключа ЭП и ключа защиты УКЦ задаются во время создания сертификата.



7.2 После перевода УКЦ в аккредитованный режим необходимо выпустить корневой квалифицированный сертификат. Для этого нужно в УКЦ перейти в «Администрирование».



Выбрать корневые сертификаты и «Создать», все сведения о владельце сертификата указаны выше.

Мастер создания сертификата администратора сети ViPNet

Сведения о владельце сертификата
Заполните сведения о владельце запрашиваемого сертификата.

Город: Москва

Область: Московская

Страна: RU

Адрес, улица:

Мастер создания сертификата администратора сети ViPNet

Сведения о владельце сертификата
Заполните сведения о владельце запрашиваемого сертификата.

Организация: WorldSkills

ОГРН:

Подразделение: IT-отдел

Должность: Администратор

Мастер создания сертификата администратора сети ViPNet

Дополнительные сведения о владельце сертификата
Укажите дополнительные сведения о владельце сертификата.

Атрибуты	Значения
Телефон	
Департамент	
ОГРНИП	
Описание	
Почтовый индекс	112344
Почтовый ящик	

Мастер создания сертификата администратора сети ViPNet

Место хранения контейнера ключей
Ключ электронной подписи будет сохранен в защищенном контейнере. Выберите место его хранения:

☒ В файле

☐ На внешнем устройстве

Остальные пункты оставить по умолчанию.

После выпуска корневого сертификата, он автоматически принимает статус текущего сертификата.

Для того, чтобы квалифицированную электронную подпись для пользователя «Admin» выдать с новым дистрибутивом ключей, следует в УКЦ перейти в «Пользователи» выбрать пользователя администратора, после создать и передать ключи в ЦУС.

Внимание! Всегда заполнении сведений о владельце сертификата, заполнять в соответствии с требованиями, приписанными в задании.

Для того, чтобы квалифицированную электронную подпись для пользователя «Client» сохранить в файл, нужно в УКЦ перейти в «Пользователи» выбрать клиента и «Создать ключи ЭП и сохранить в файл». Сохранить на рабочий стол.

Задание 8. Создать квалифицированные ключи ЭП и ключи проверки ЭП для пользователей сети.

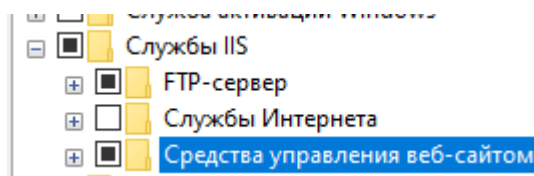
Настроить схему обмена файлами между УКЦ посредством Сервиса Публикации (Publication Service).

Настроить переход в автоматический режим (при бездействии администратора): передачу на публикацию и обновление CRL с периодичностью 1 день.

Реализовать автоматическую публикацию сертификатов издателей на FTP-сервере.

8.1 Ключи ЭП и проверки ЭП уже были созданы для пользователей сети.

8.2 Для того чтобы настроить схему обмена файлами между УКЦ посредством сервиса публикации, нужно перейти на машину OperatorCA, перейти в панель управления и выбрать пункт «Включение и отключение компонентов Windows». Найти пункт службы IIS и установить следующие параметры.

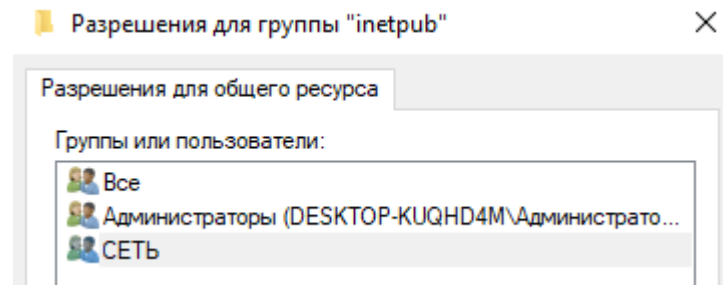


Дождаться конца установки.

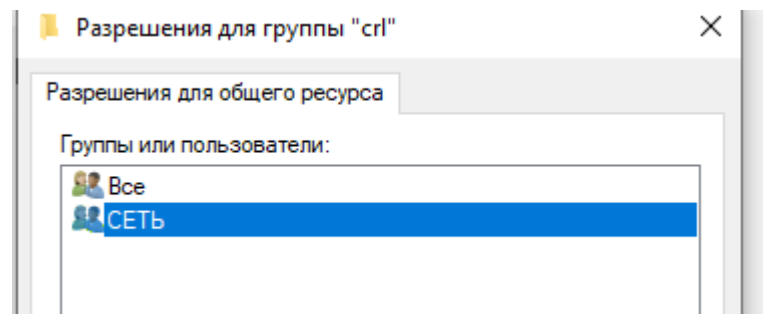
Как установка завершится, на диске С появится папка inetpub, нужно открыть свойства папки, перейти в «доступ» и настроить «общий доступ».

Имя	Уровень разрешений
F7	Чтение и запись ▼
Все	Чтение и запись ▼
СЕТЬ	Чтение и запись ▼
СИСТЕМА	Владелец

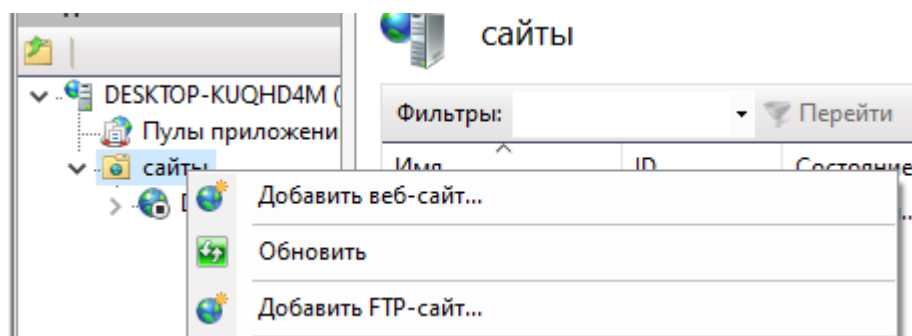
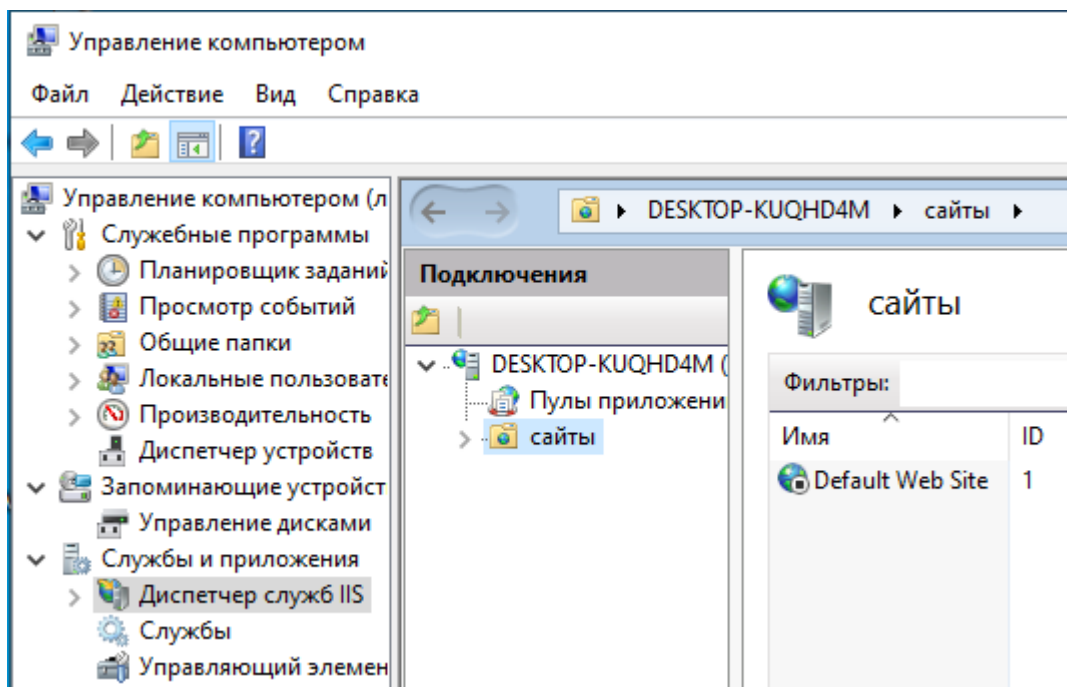
Далее перейти в настройки расширенного доступа, «Разрешения» и настроить. Все должны иметь полный доступ.



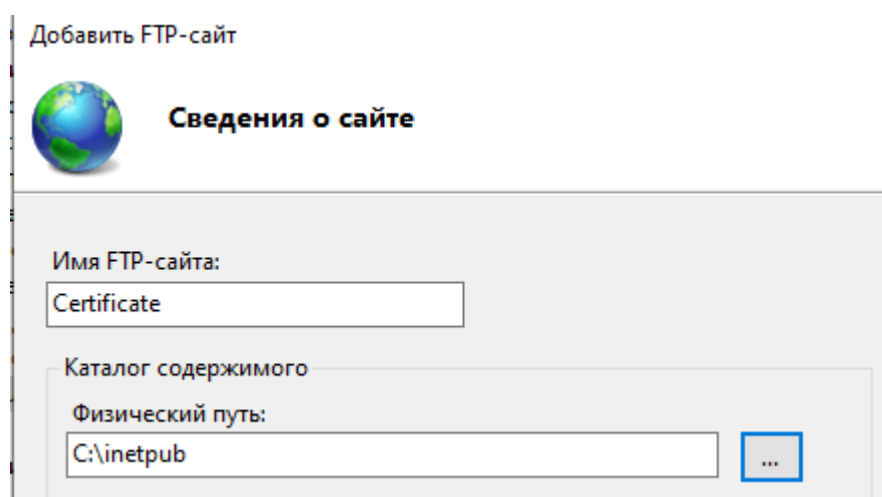
Зайти в папку inetpub и создать папку CRL и также настроить расширенные настройки общего доступа, как и для корневой папки ftproot.



После настройки доступа, нужно поднять FTP сервер. Для этого ПКМ по «Пуск» и выбрать «Управление компьютером».



Добавляем FTP-сайт. Имя сайта, например, Certificate. Для каталога выбираем физический путь до папки inetpub.



**Параметры привязки и SSL****Привязка**

IP-адрес:

Все свободные

Порт:

21

☐ Разрешить имена виртуальных узлов:

Виртуальное имя и узел (пример: ftp.contoso.com):

☒ Запускать сайт FTP автоматически**SSL**☒ Без SSL☐ Разрешить SSL☐ Требовать SSL

SSL-сертификат:

Не выбрано

Выбрать...

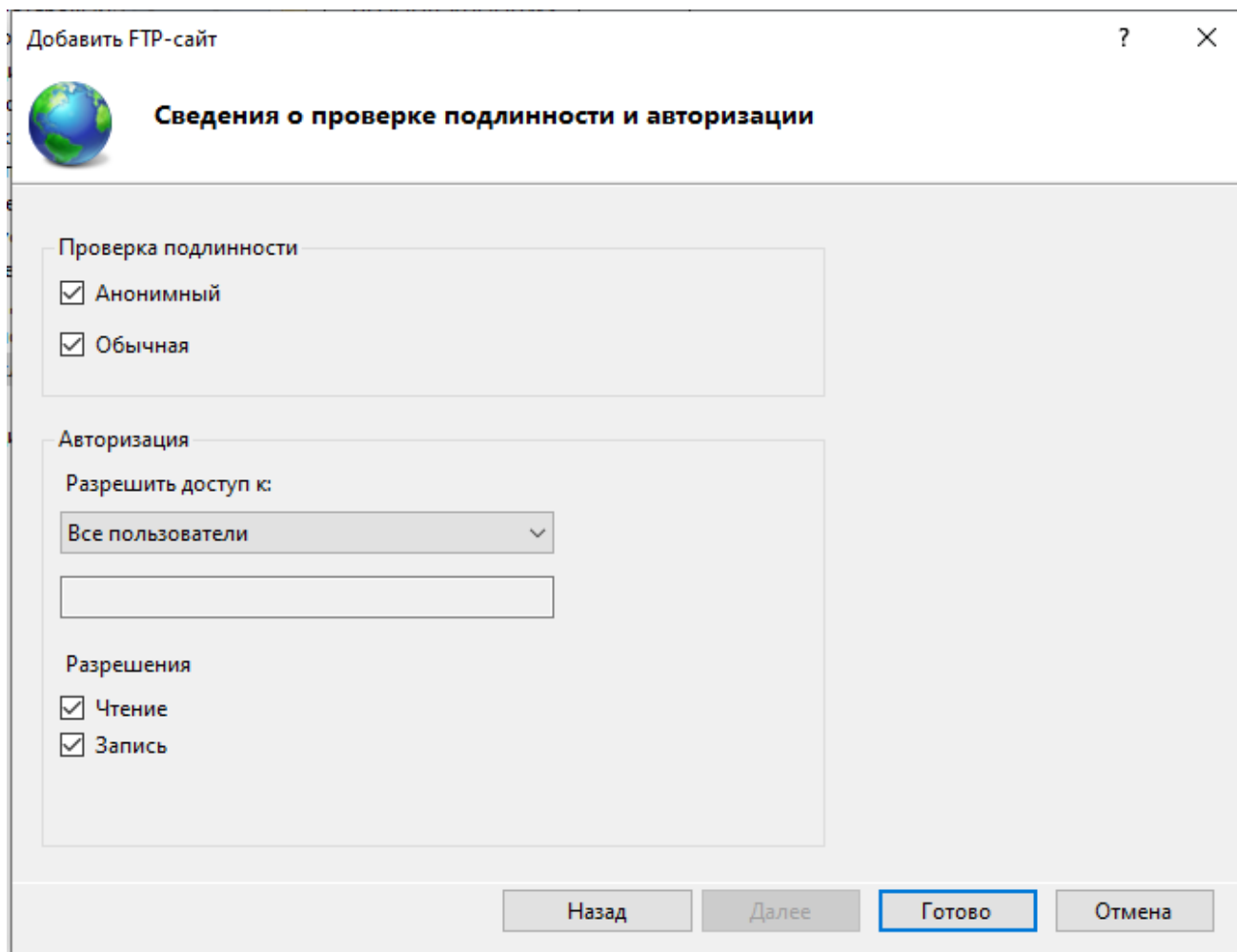
Просмотреть.

Назад

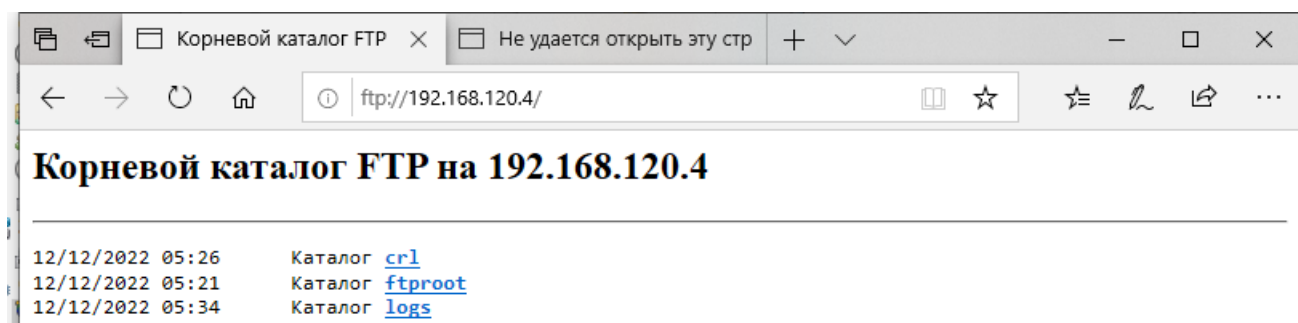
Далее

Готово

Отмена



Для проверки работы сервера, открывает браузер и в строке URL прописываем следующее: ftp://адрес компьютера, на котором развернут сервер.



Сервер доступен.

Следующий шаг, настроить публикацию сертификатов на сервер.

На машине где развернут сервер, создать пользователя с именем FTP и паролем FTP, он понадобится для работы «Сервиса публикации» (необязательно аналогично методичке, можно абсолютно любой). Далее создать папку (пример) на рабочем столе «Pub», в ней 2 папки «in» и «out». Настроить к ней общий доступ (см. п. 8.2).

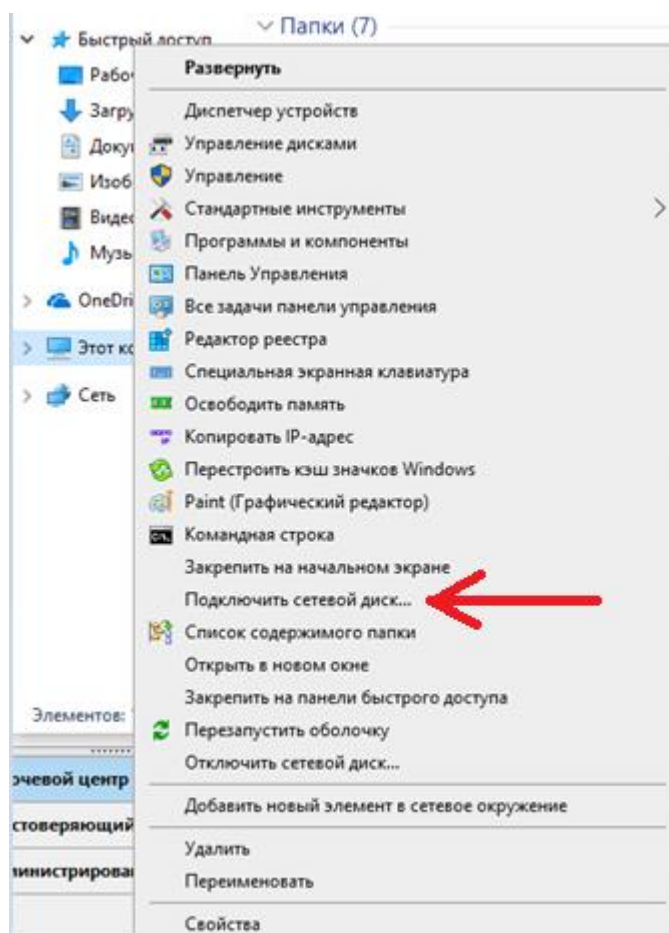
Проверить доступность общей папки. В случае ошибок с подключением, на машине OperatorCA следует перейти в параметры общего доступа и отключить парольную защиту.

Общий доступ с парольной защитой

Если включена парольная защита общего доступа, только пользователи с учетной записью и паролем на этом компьютере могут получить доступ к общим файлам, принтерам, подключенным к этому компьютеру, и общим папкам. Чтобы открыть доступ другим пользователям, нужно отключить парольную защиту общего доступа.

- ☐ Включить общий доступ с парольной защитой
- ☒ Отключить общий доступ с парольной защитой

Для удобства, на компьютере администратора сети, открыть этот компьютер и добавить новый сетевой диск.



Какую сетевую папку вы хотите подключить?

Укажите букву диска для подключения и папку, к которой вы хотите подключиться:

Диск: ▼

Папка:

Пример: \\сервер\общий_ресурс

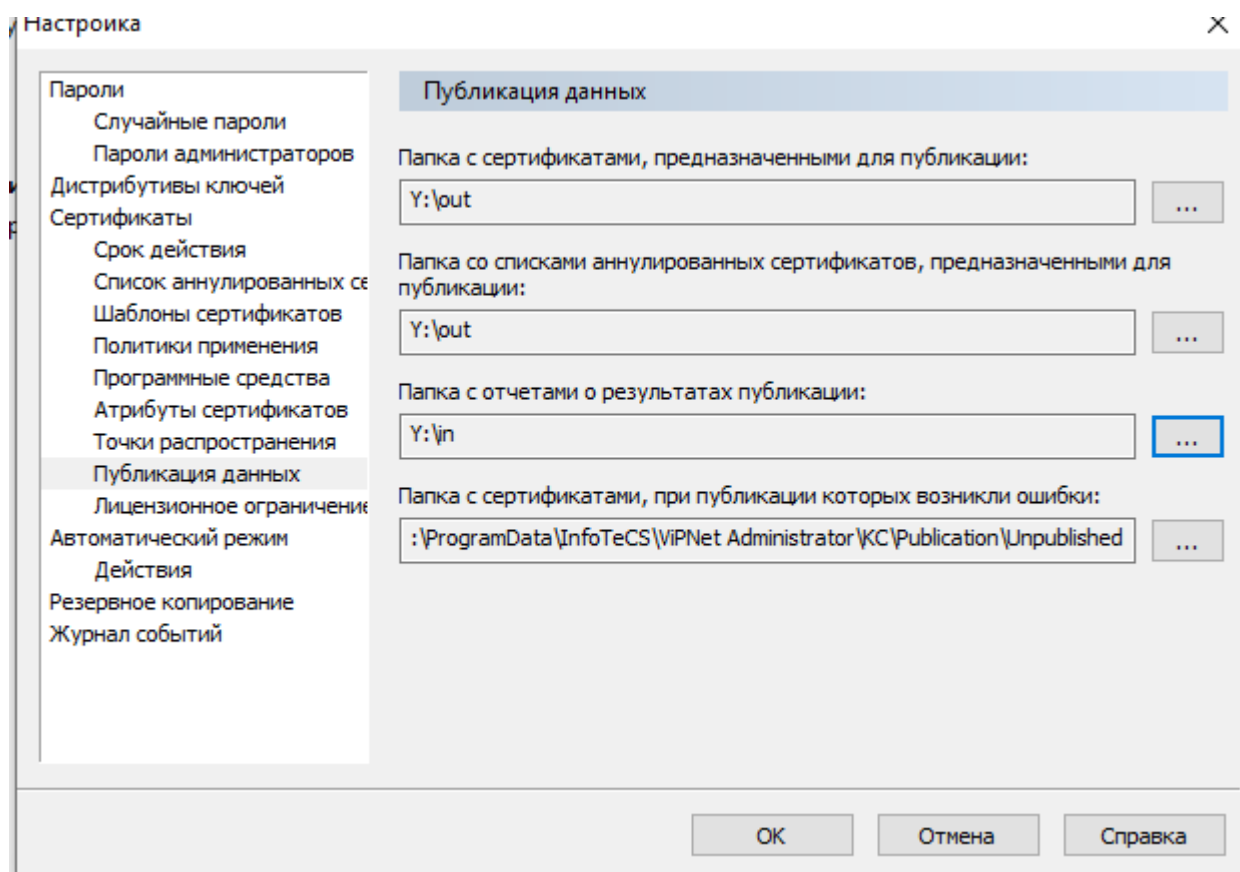
☒ Восстанавливать подключение при входе в систему

☐ Использовать другие учетные данные

Сетевые расположения (2)

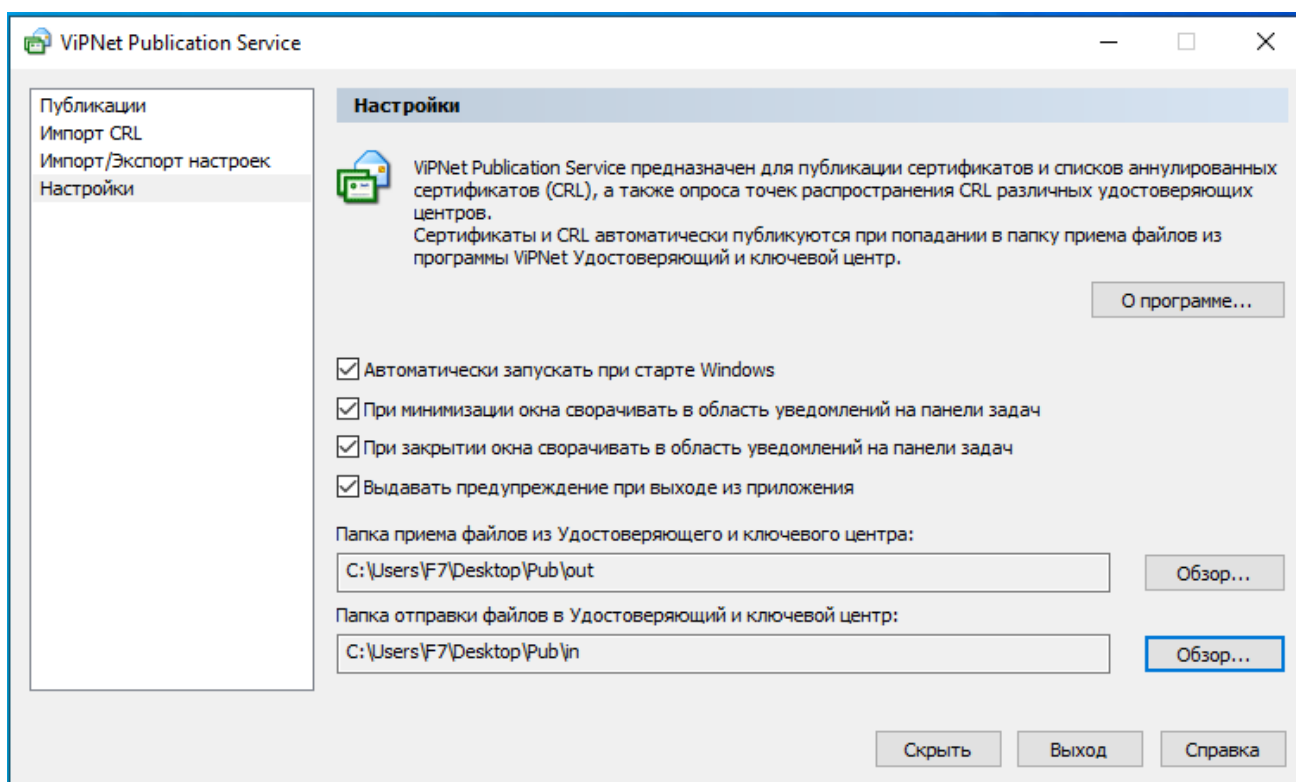
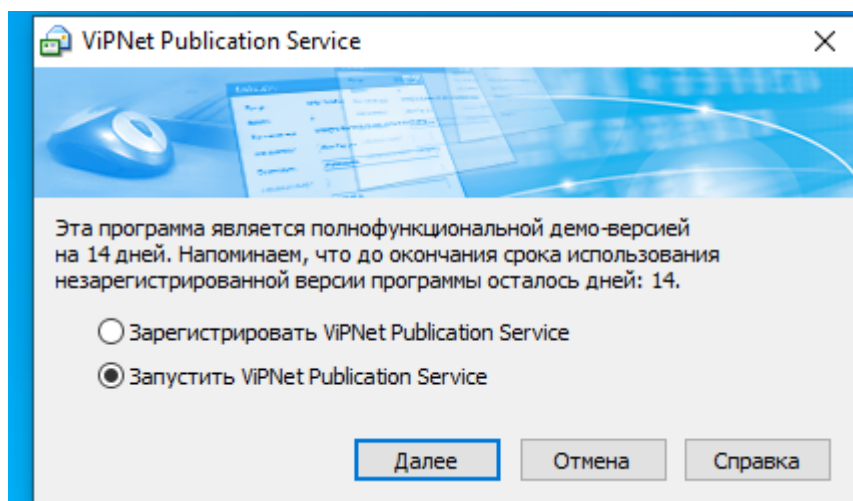


Далее перейти на рабочее место администратора сети и зайти в настройки УКЦ – «Публикация данных» и настроить в соответствии с рисунком ниже.

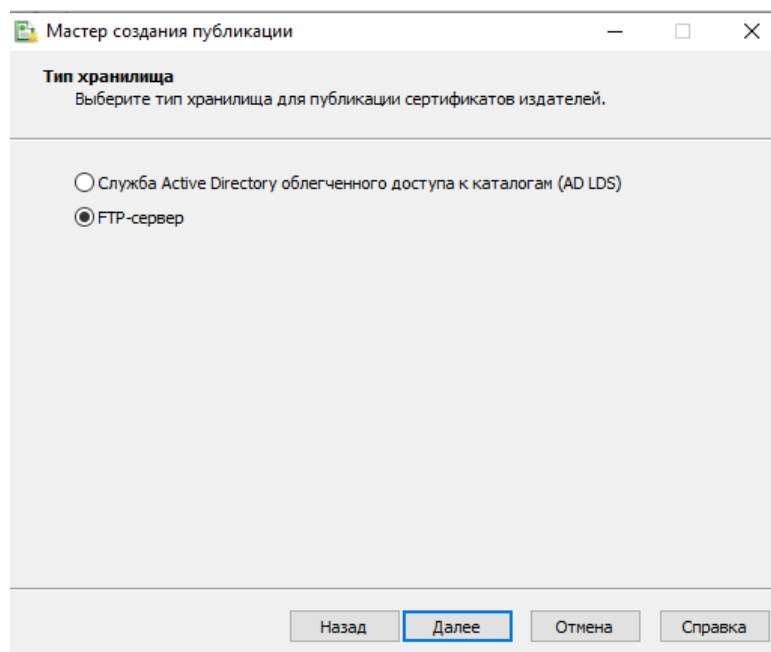
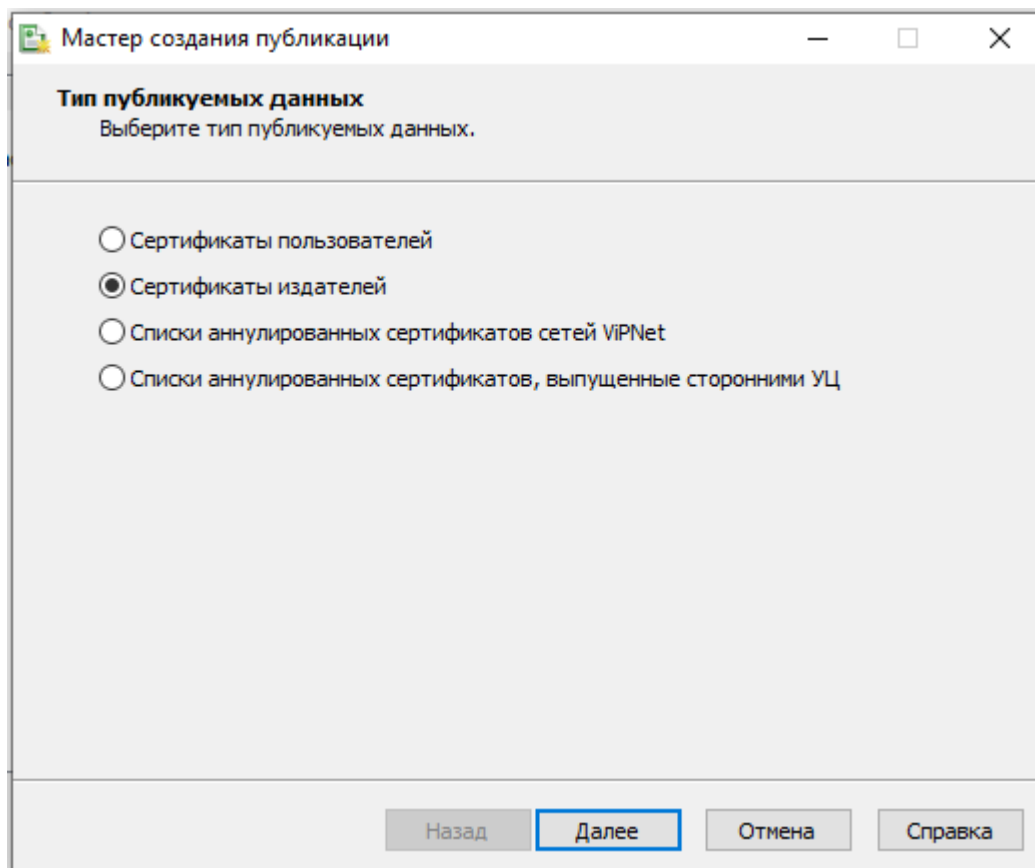


Сохраняем настройки и переходит на машину OperatorCA.

Запускаем «Сервис публикации».

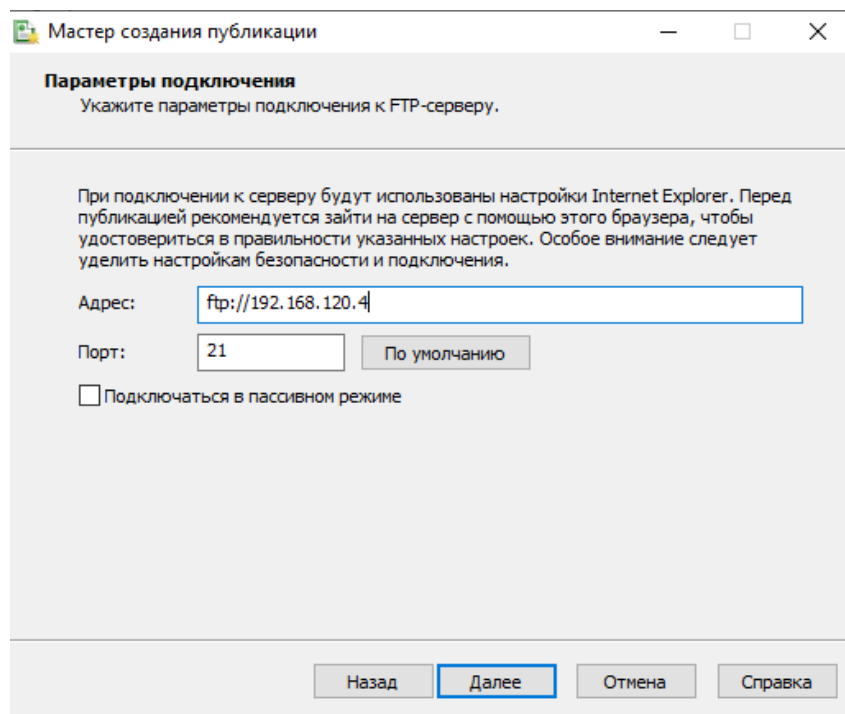


Далее добавим автоматическую публикацию сертификатов на FTP сервер (тип публикуемых данных зависит от задания, в этом случае, сертификаты издателей).

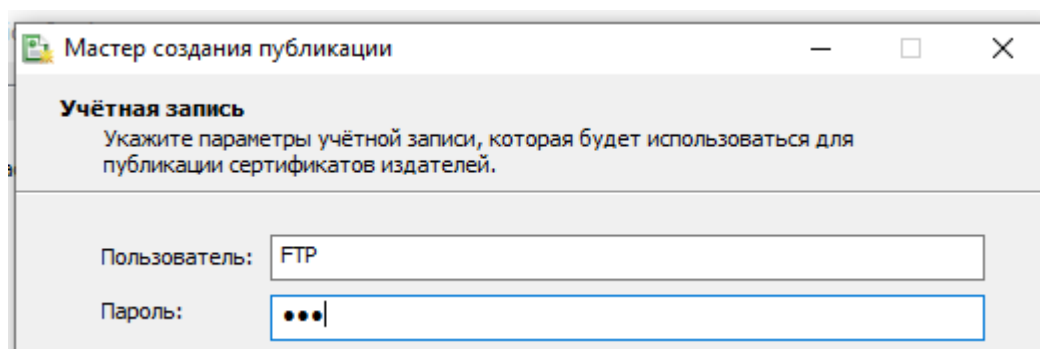


В параметрах подключения к FTP серверу, следует убрать галочку с подключения в пассивном режиме, т.к. в таком случае подключение не будет происходить.

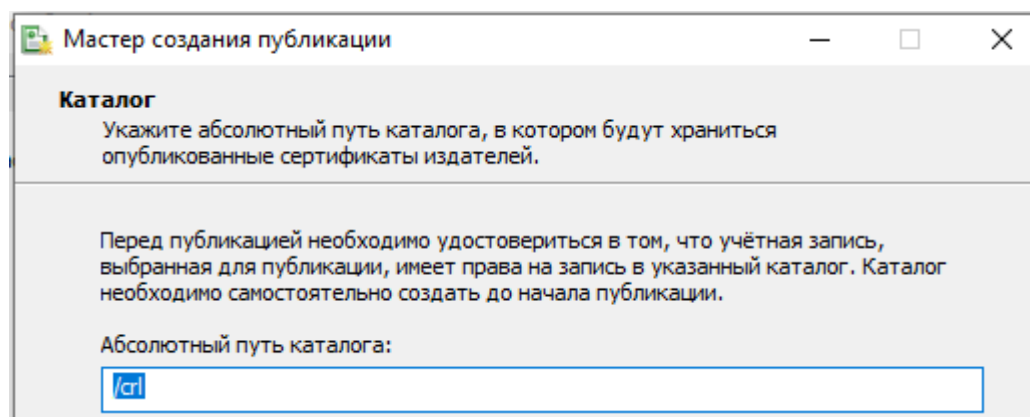
Адрес сервера указать как: 192.168.120.4 (пример). **Без FTP://*!!!**



В параметрах учетной записи указываем пользователя, которого создали для FTP (см. п. 8.2, после проверки работы сервера).

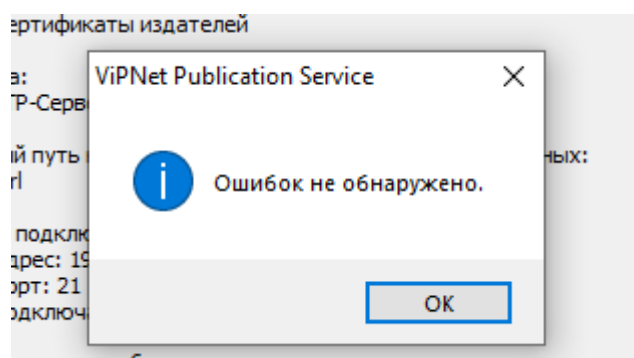


В параметрах каталога указать папку /crl. Так как корневую папку inetpub мы указываем как сервер, и папке в ней будут задаваться без /inetpub перед нужной папкой.



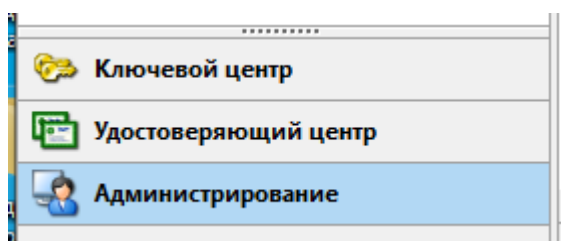
Название публикаций можно оставить по умолчанию.

Проверяем указанные параметры. При корректных настройках, получим следующее сообщение.

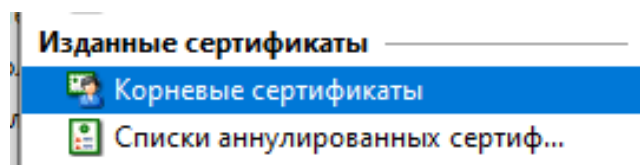


Завершаем настройку сервиса публикации. Теперь нужно проверить работоспособность.

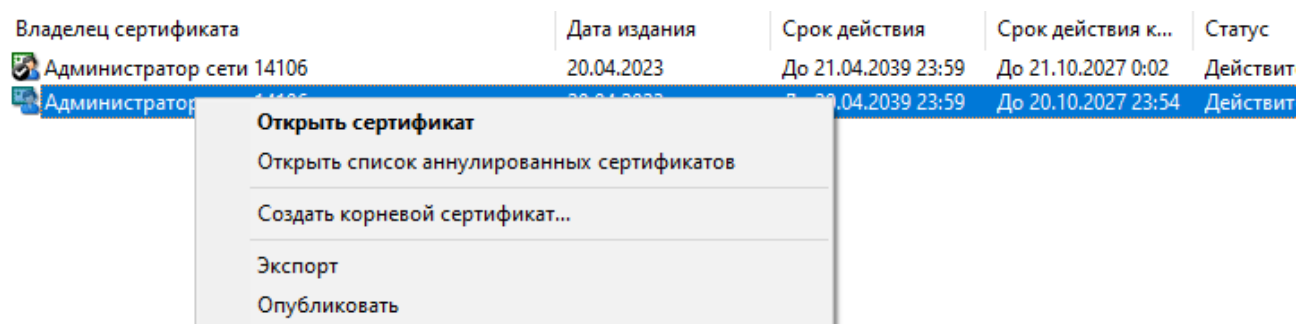
Для этого переходим на машину администратора и в меню «Администрирование».



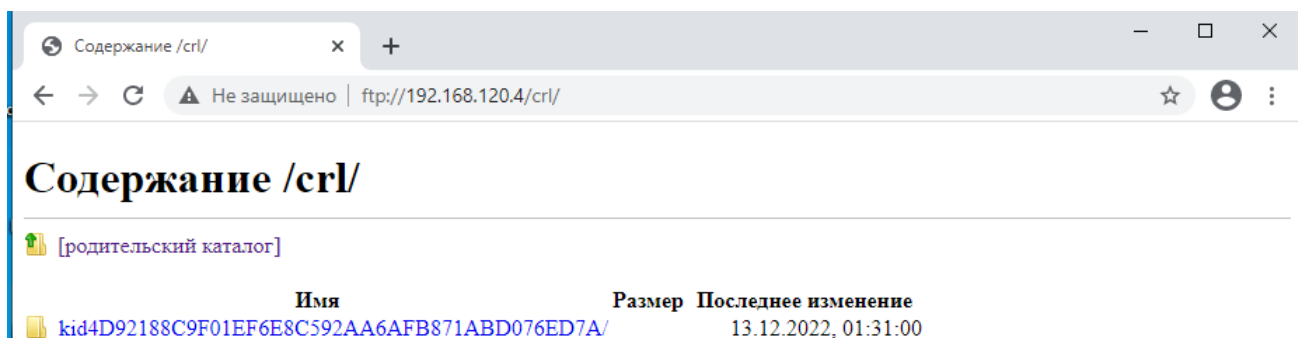
Переходим в список корневых сертификатов.



Выбираем старый корневой сертификат администратора и опубликуем его.



Проверим доступность и опубликовался ли сертификат на сервере. Для этого следует запустить Internet Explorer или Google Chrome.



Сертификат опубликовался и доступ с администратора на сервер оператора есть. На эту работу с сервисом публикации завершена.

Задание 9. Посредством Центра Регистрации (Registration Point):

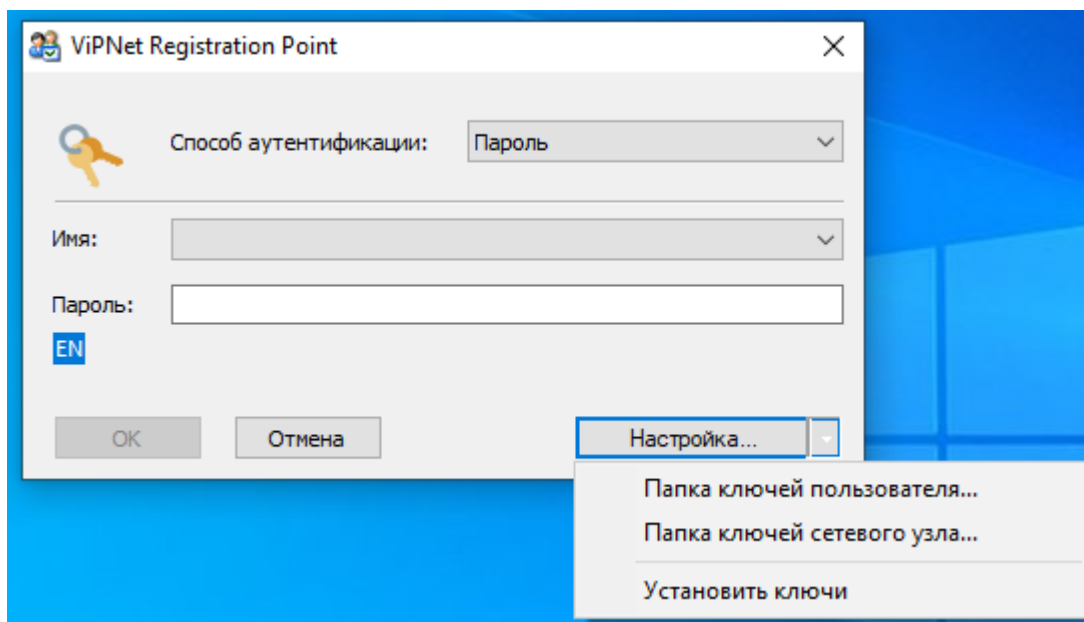
1. зарегистрировать пользователя: UserCli;
2. отправить запрос в УКЦ на выпуск сертификата, удовлетворить запрос. Результат выпуска сертификата зафиксировать скриншотом;
3. отправить запрос в УКЦ на аннулирование ранее выпущенного сертификата, удовлетворить запрос. Результат зафиксировать скриншотом.

Посредством Сервиса Информирования (CA Informing):

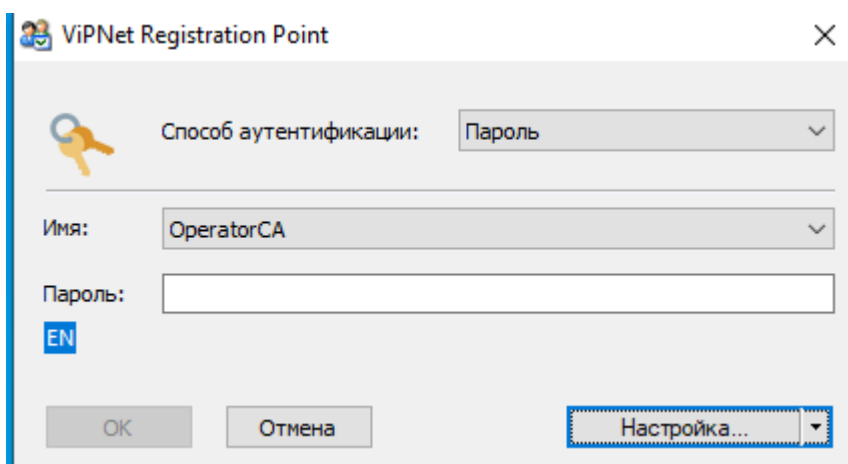
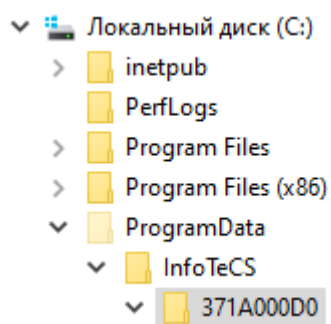
4. настроить способ выдачи уведомлений (файлы *.eml локально для последующей отправки должны сохраняться в папке на рабочем столе);
5. сформировать отчет о выданных за текущие сутки сертификатах, предварительно в настройках указав место хранения отчетов (на рабочем столе).

9.1 Для выполнения задания, запускаем «Центр регистрации» и видно, что отсутствует пользователь для аутентификации.


Для работы центра регистрации у пользователя должны быть настроены роль (см. п. 6.7).



Выбираем пункт «Папка ключей сетевого узла» и выбираем папку с идентификатором OperatorCA.



Авторизуемся на пользователе, как и на клиенте.

Выбираем «зарегистрировать пользователя» 

Регистрация пользователя

Регистрация пользователя

Этот мастер поможет зарегистрировать нового пользователя. Зарегистрированного пользователя можно будет ввести в состав сети VIPNet и получить для него сертификат электронной подписи.

☒ Зарегистрировать пользователя самостоятельно
☐ Использовать внешние источники данных

Выберите шаблон, который будет использоваться при регистрации пользователя:

Стандартный шаблон имени пользователя ▾

☐ Использовать по умолчанию

< Назад **Далее >** Отмена Справка

Указываем имя пользователя как в задании и заполняем сведения о сертификате в соответствии с заданием (см. п. 7.2).

Регистрация пользователя

Сведения о пользователе
Заполните сведения о пользователе.

* Имя: UserCli

Должность:

Подразделение: IT-отдел

Организация: WorldSkills

ИНН:

ОГРН:

СНИЛС:

< Назад **Далее >** Отмена Справка

Регистрация пользователя

Сведения о пользователе
Заполните сведения о пользователе.

Город:

Область:

Страна: ...

Электронная почта:

Адрес, улица:

< Назад **Далее >** Отмена Справка

Регистрация пользователя

Система готова к регистрации пользователя
Убедитесь в правильности введенных сведений

Были указаны следующие сведения:

UserCli
Подразделение: IT-отдел
Организация: WorldSkills
Город: Москва
Область: Московская
Страна: RU
Электронная почта: UserCli@DemiVip.lab

Для завершения регистрации нажмите "Далее".

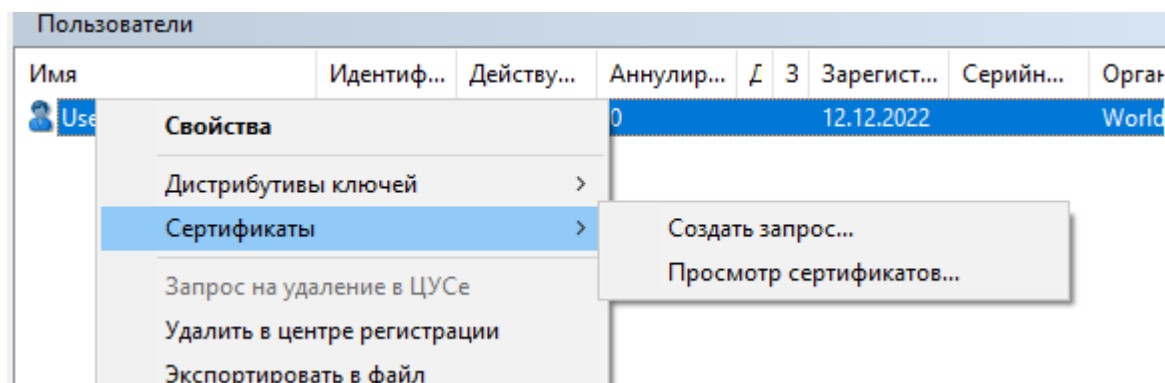
< Назад **Далее >** Отмена Справка

Не создаем запрос на дистрибутив ключей.

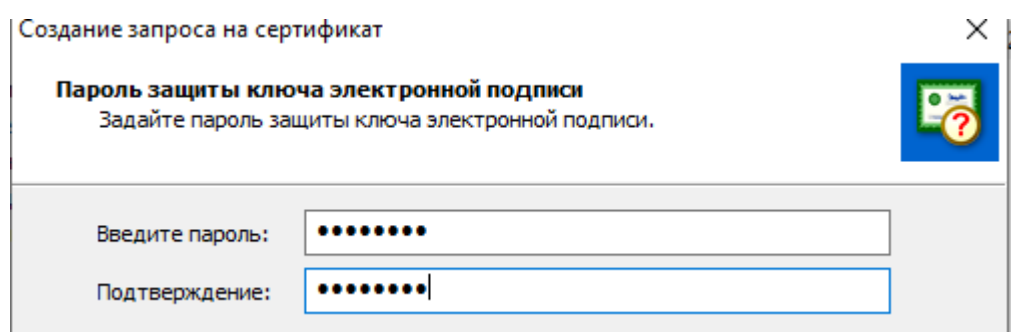
<div> <div> </div> <div> <div>Центр регистрации</div> <div>Пользователи</div> <div>Сертификаты</div> <div>Запросы</div> </div> </div>									
Пользователи									
Имя	Идентиф...	Действу...	Аннулир...	Д	З	Зарегист...	Серийн...	Орган...	
UserCli		0	0			12.12.2022		World	

Пользователь зарегистрирован.

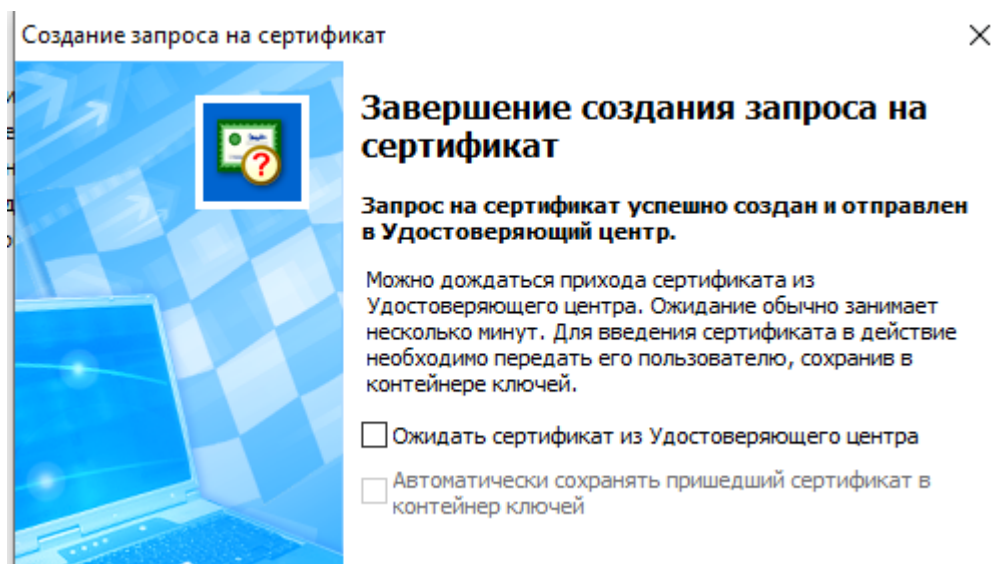
9.2 Чтобы отправить запрос на выпуск сертификата в УЦ, следует выбрать пользователя и создать запрос.



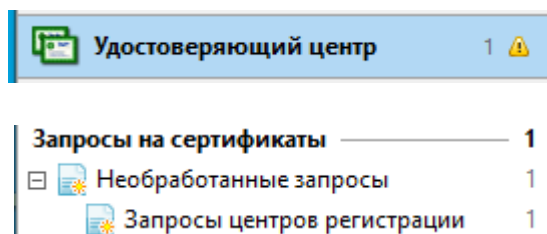
Все параметры оставляем по умолчанию и задаем пароль.



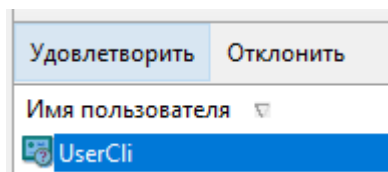
Убираем все галочки.



После отправления запросы на сертификат, в УКЦ на месте администратора появится уведомление.



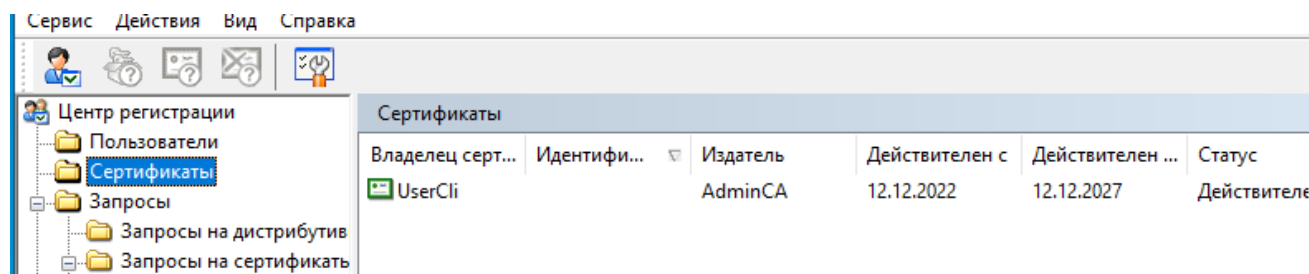
Выбираем сертификат пользователя и удовлетворяем.



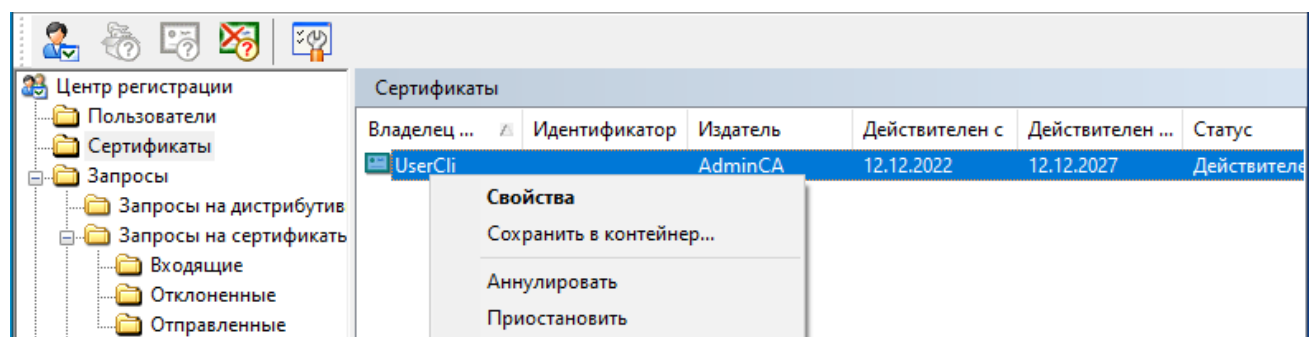
Все параметры оставляем по умолчанию.

После удовлетворения запроса, информация о сертификате появится в «Сертификаты».

В ситуации, когда от УЦ не пришел ответ, следует выбрать «Сервис» - «Отправить/получить запросы» и кнопку «Опросить».

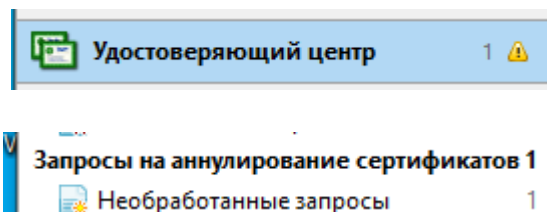


9.3 Для создание запроса на аннулирование сертификата, переходит в «сертификаты» и аннулируем сертификат пользователя.

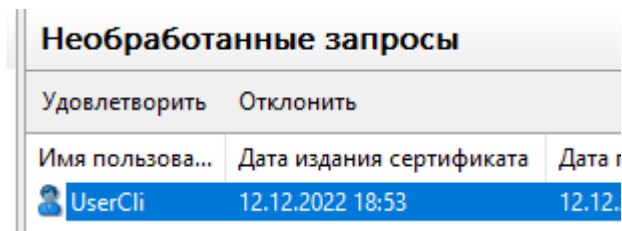


Причину оставляем по умолчанию и соглашаемся. После этого был отправлен запрос в УКЦ на аннулирование сертификата, переходим на рабочее место администратора.

Также появится уведомление.



Удовлетворяем запрос на аннулирование.



Переходим в сервис публикации и видим, что сертификат аннулирован.



9.4 настроить способ выдачи уведомлений (файлы *.eml локально для последующей отправки должны сохраняться в папке на рабочем столе).

Запускаем СА Informing на рабочем месте администратора сети. При первом запуске, встречает окно настройки программы, заполнить поля в соответствии с рисунком ниже

Настройки

Общие
Уведомления
OID

Выдача уведомлений

Способ выдачи уведомлений:

☐ Отправлять по электронной почте

Параметры отправки

☒ Сохранять в папку:

C:\Users\F7\Desktop\Уведомления CA

Обзор...

Свойства сообщений с уведомлениями:

Отображаемый адрес:

AdminCA@demo.lab

Отображаемое имя:

AdminCA

Адреса электронной почты для отправки уведомлений:

adminCA@demo.lab

База данных удостоверяющего центра

Тип базы данных:

SQL Server (YKЦ 4.x)

Строка подключения к базе данных:

atalog=ViPNetAdministrator;User Id=KcaUser;Password=Number1

Кросс-сертификаты

☐ Использовать кросс-сертификаты

Путь к файлу с кросс-сертификатами:

Обзор...

Отчеты

Путь сохранения отчетов:

C:\Users\F7\Desktop\отчеты

Обзор...

Проверить настройки

?

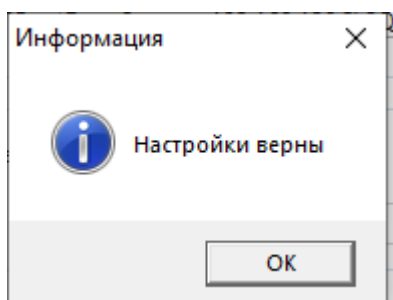
OK

Отмена

Т.к. используется 4 версия ПО ViPNet устанавливаем тип данных для 4 версии. Строка для подключения к бд имеет следующий вид:
Data Source = 1.2.3.2\SQLExpress; Initial Catalog = ViPNetAdministrator(по умолчанию при установке БД); User Id = KcaUser (по умолчанию при установке БД); Password=Number1 KcaUser (по умолчанию при установке БД)
Data Source = 1.2.3.2\SQLExpress; Initial Catalog = ViPNetAdministrator; User Id = KcaUser; Password=Number1 KcaUser
Заполним поле в соответствии с структурой сети, которая рассматривается в примере.

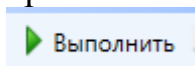
Data Source=192.168.120.2\SQLExpress; Initial Catalog=ViPNetAdministrator;UserId=KcaUser;Password=Number1

После заполнения всех полей, следует проверить настройки. При удачной проверке, появится уведомление

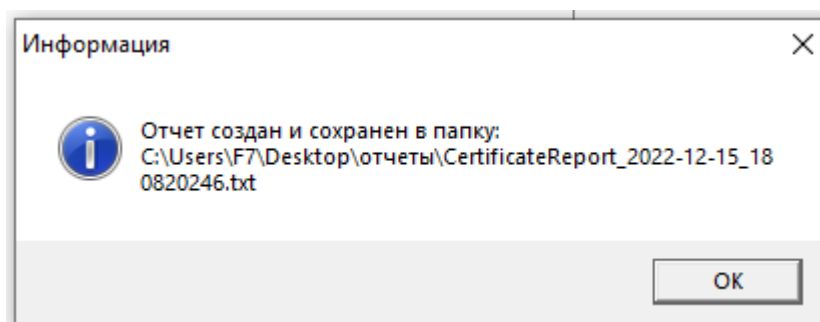


9.5 Сформировать отчет о выданных за текущие сутки сертификатах, предварительно в настройках указав место хранения отчетов (на рабочем столе).

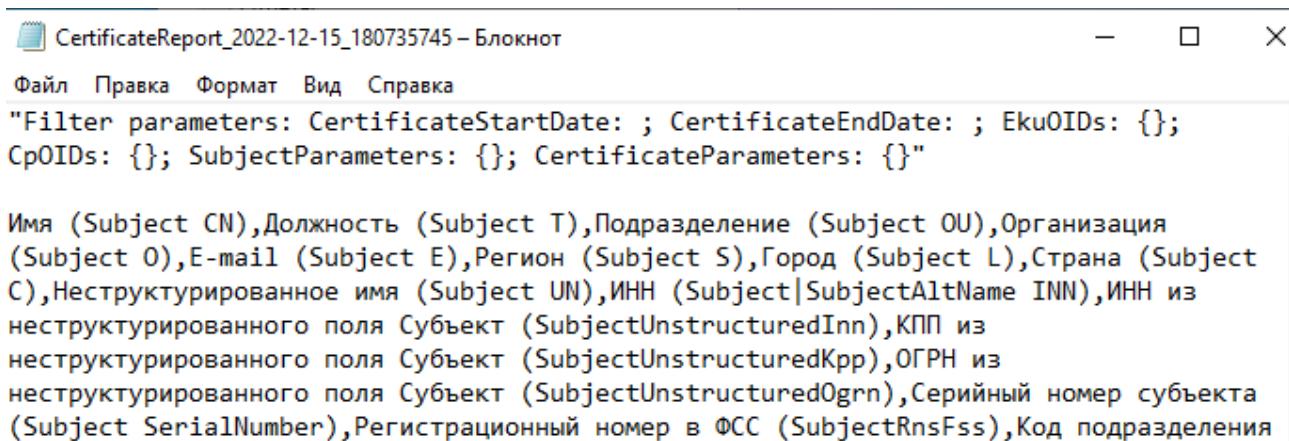
Для того, чтобы сформировать отчет, нужно зайти в вкладку «Отчеты» в меню CA Informing и добавить отчет. Так как нам нужна информация о сертификатах, которые выдались за последние сутки то никаких настроек, кроме имени отчета делать не нужно. Сохраняем отчет и выполняем



После завершения, появится уведомление о завершении, в котором говорится о успешном создании отчета и пути к нему.



Открыв отчет, будет видна информация о выданных сертификатах



```
File Edit Format View Help
"Filter parameters: CertificateStartDate: ; CertificateEndDate: ; EkuOIDs: {};
CpOIDs: {}; SubjectParameters: {}; CertificateParameters: {}"

Имя (Subject CN), Должность (Subject T), Подразделение (Subject OU), Организация
(Subject O), E-mail (Subject E), Регион (Subject S), Город (Subject L), Страна (Subject
C), Неструктурированное имя (Subject UN), ИНН (Subject|SubjectAltName INN), ИНН из
неструктурированного поля Субъект (SubjectUnstructuredInn), КПП из
неструктурированного поля Субъект (SubjectUnstructuredKpp), ОГРН из
неструктурированного поля Субъект (SubjectUnstructuredOgrn), Серийный номер субъекта
(Subject SerialNumber), Регистрационный номер в ФСС (SubjectRnsFss), Код подразделения
```

Задание 10 Модификация структуры защищенной сети

Перед началом выполнения сделать HTML выгрузку структуры сети и сделать скриншот ЦУС окна с пользователями.

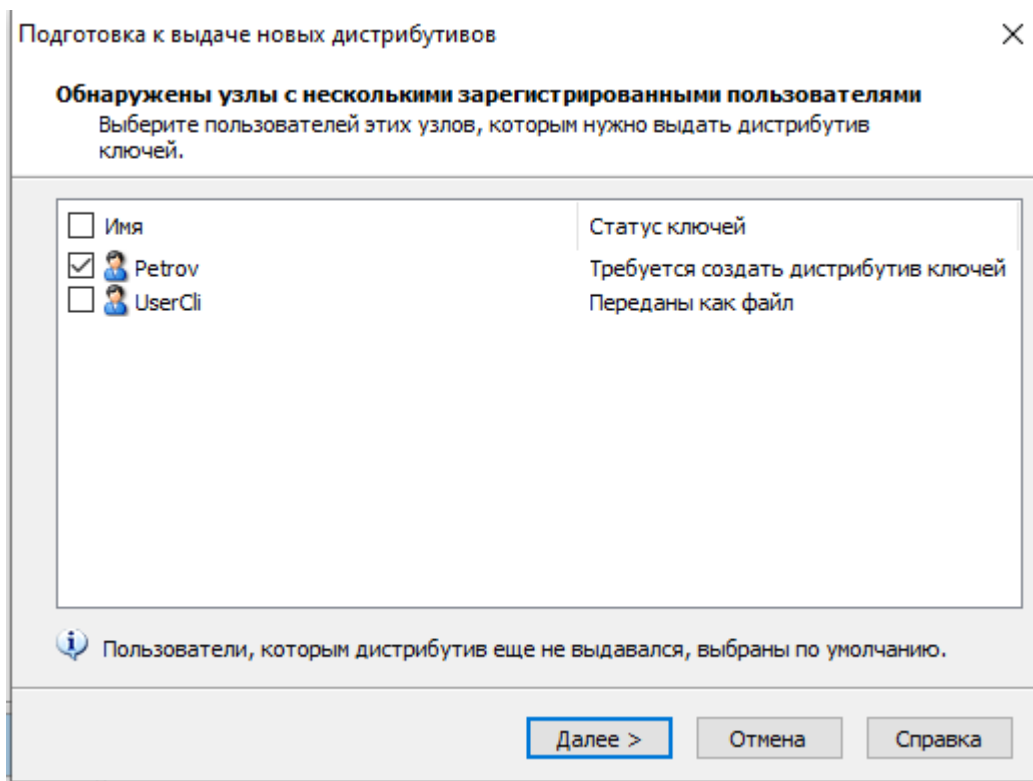
Модификация структуры сети:

1. добавить новый сетевой узел Ivanov и пользователя Ivanov за координатором ЦентрОфис (без фактического развертывания его на виртуальной машине). Добавить связь пользователя нового узла с пользователем UserCli. На указанных узлах проверить появление нового узла;
2. Добавить пользователя Petrov на узле Пользователь_2 Филиал (Net2-Client филиала 2), связать его со всеми пользователями группы узлов центральный офис. Для указанных пользователей проверить появление новой связи;
3. отправить письмо по Деловой почте пользователю Petrov с узла admin.
4. отправить текстовое сообщение пользователю Admin от пользователя Petrov
5. Необходимо зафиксировать процесс настройки скриншотами ключевых моментов и заполненных форм:
 - скриншоты деловой почты на отправителе и получателе (при отправке письма);
 - скриншоты текстового сообщения на отправителе и получателе;
 - скриншоты журнала IP-пакетов на координаторах, подтверждающие прохождение письма через координаторы.Кроме того, необходимо сохранить файл HTML с обновленной структурой защищенной сети, выгруженный из ЦУС.

Как выгрузить структуру сети, было рассмотрено в пункте 7.1

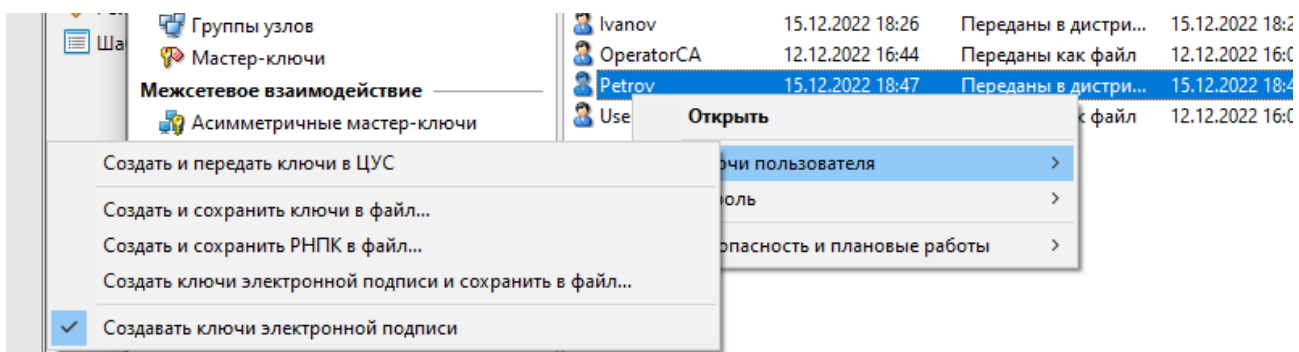
9.1 – 9.2 Как создать сетевой узел за координатором и пользователя, было рассмотрено в пунктах 6.7,6.8 и 6.9.

Так как на сетевом узле регистрируется новый пользователь, чтобы была возможность авторизации, нужно выдать дистрибутив ключей для пользователя Petrov. Для этого переходим в УКЦ, в сетевых узлах выбрать Пользователь_2 Филиал и «Выдать новый дистрибутив ключей»



Оставляем галочку на пользователе Petrov и продолжаем выдачу dst (см. п. 6.11)

После завершения выдачи новых dst выбрать сетевой узел Пользователь_2 Филиал и передать ключи и справочники в ЦУС. Также в УКЦ перейти в «Пользователи» выбрать пользователя «Petrov» и создать и передать ключи в ЦУС



Чтобы проверить появление новых узлов в сети, нужно создать справочники в ЦУС, создать и передать ключи в УКЦ, отправить на узлы и дождаться состояния «Приняты»

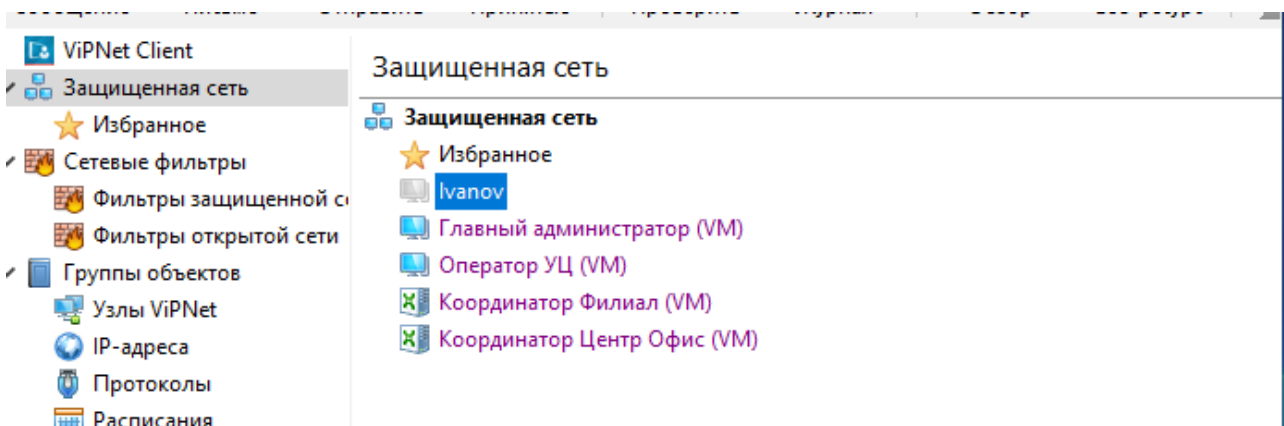
Состояние справочников и ключей на момент отправки

Клиенты					
Найти					
<input type="checkbox"/>	Имя	Сетевой адрес	Координатор	Дата изменен...	Справочники и ключи
<input checked="" type="checkbox"/>	Ivanov	14106.1.3	Координатор Центр Офис (VM)	15.12.22 18:27	Отправлены
<input type="checkbox"/>	Главный администратор (VM)	14106.1.1	Координатор Центр Офис (VM)	15.12.22 18:26	Доставлены
<input type="checkbox"/>	Оператор УЦ (VM)	14106.1.2	Координатор Центр Офис (VM)	15.12.22 18:26	Отправлены
<input type="checkbox"/>	Пользователь_2 Филиал (VM)	14106.2.1	Координатор Филиал (VM)	15.12.22 18:26	Отправлены

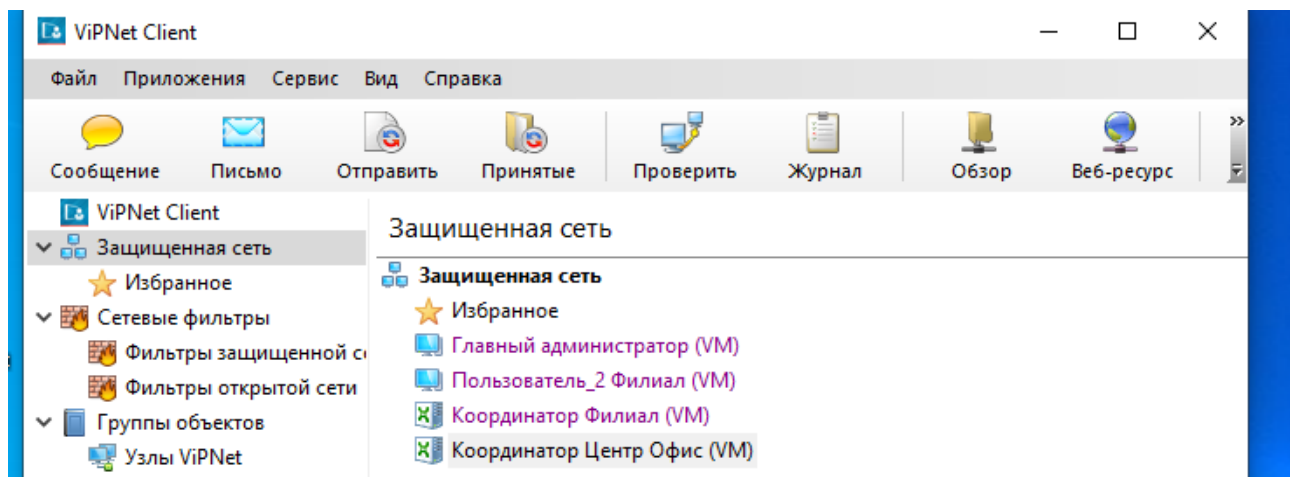
Статус справочников и ключей спустя некоторое время

Клиенты					
Найти					
<input type="checkbox"/>	Имя	Сетевой адрес	Координатор	Дата изменен...	Справочники и ключи
<input type="checkbox"/>	Ivanov	14106.1.3	Координатор Центр Офис (VM)	15.12.22 18:27	Отправлены
<input type="checkbox"/>	Главный администратор (VM)	14106.1.1	Координатор Центр Офис (VM)	15.12.22 18:29	Приняты
<input type="checkbox"/>	Оператор УЦ (VM)	14106.1.2	Координатор Центр Офис (VM)	15.12.22 18:34	Доставлены
<input type="checkbox"/>	Пользователь_2 Филиал (VM)	14106.2.1	Координатор Филиал (VM)	15.12.22 18:34	Приняты

Теперь следует перейти на UserCli и убедиться в наличии связи с узлом Ivanov



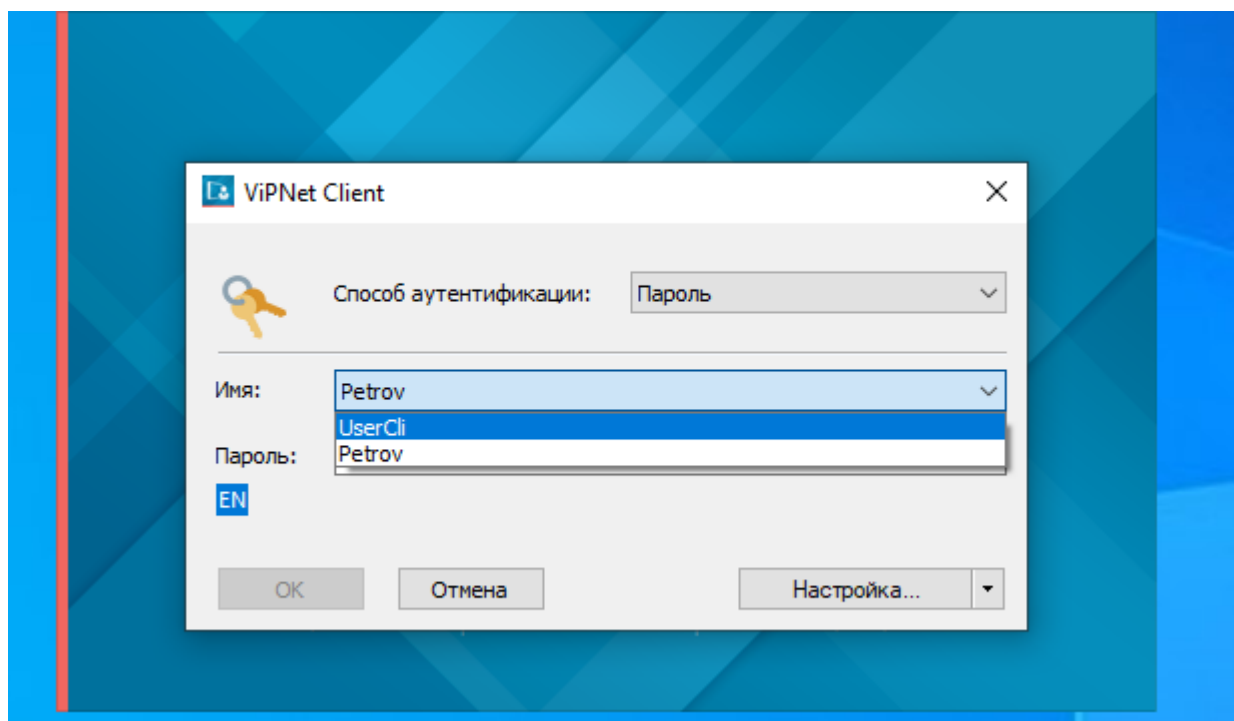
Также на любом сетевом узле (кроме администратора, так как там изначально была связь) центрального офиса посмотреть связь с пользователем_2 филиал



Все связи обновились

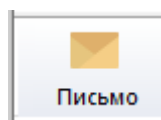
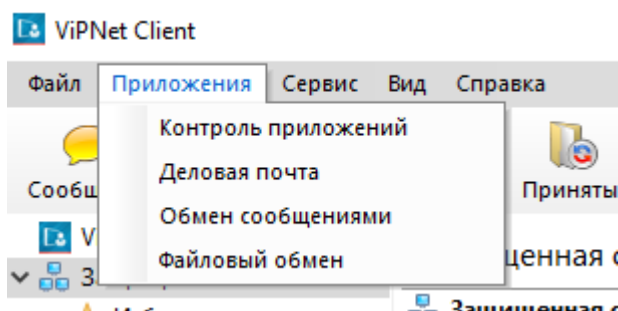
Перенести dst файлы пользователя Petrov на сетевой узел Пользователя_2 и установить

После установки dst файлов, запустить клиента и авторизоваться под пользователем Petrov

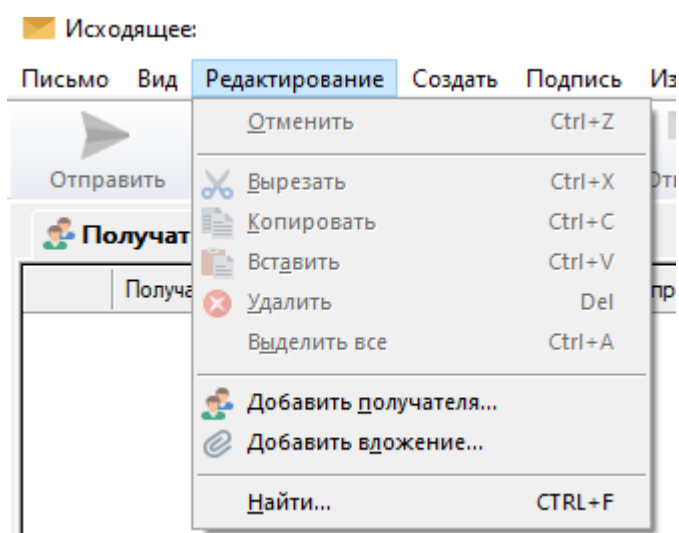


Если после авторизации на клиенте появится уведомление о

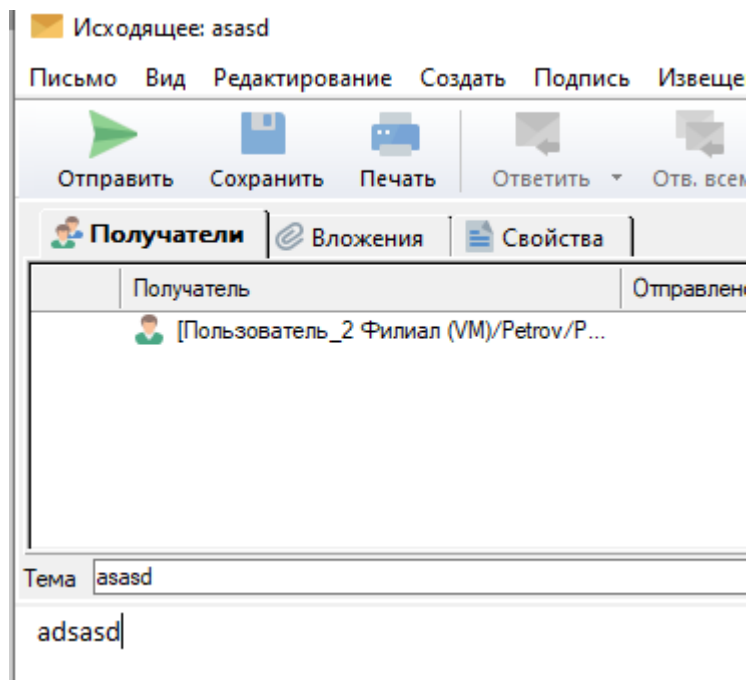
9.3 Чтобы отправить письмо по деловой почте пользователю Petrov с узла admin, нужно перейти на машину с администратором сети
В окне vipnet клиента выбрать «Приложения» - «Деловая почта»



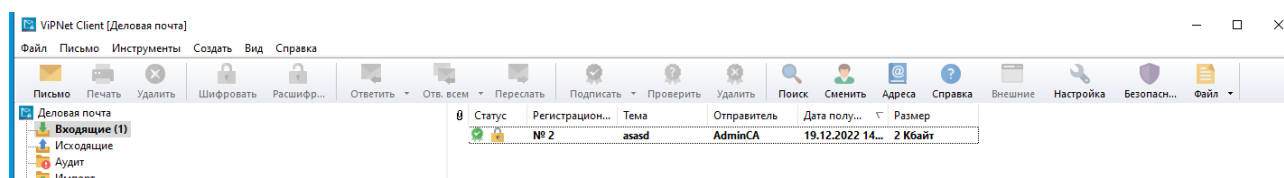
Далее выбрать пункт «Письмо» . Далее «Редактирование» и «Выбрать получателя»



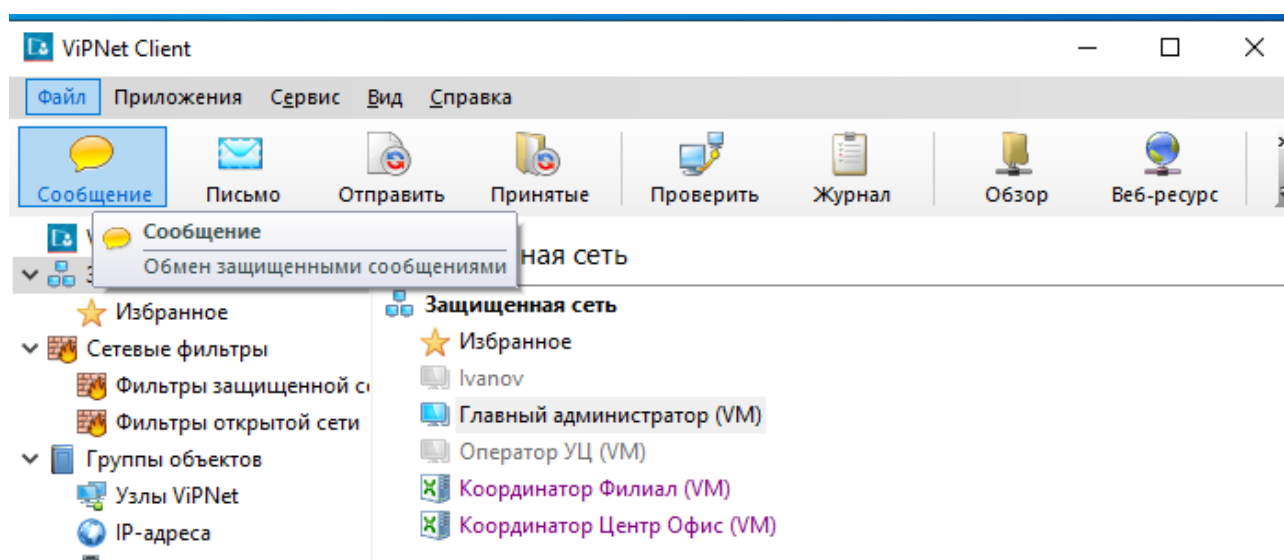
Выбираем пользователя Petrov, заполняем поля случайным содержимым и отправляем письмо



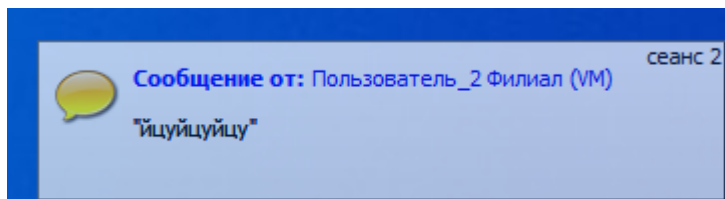
После отправки сообщения, на рабочем месте пользователя Petrov проверить деловую почту на наличие письма



9.4 Чтобы отправить текстовое сообщение пользователю Admin с пользователя Petrov, нужно на рабочем месте пользователя Petrov, в окне ViPNet клиент выбрать сетевой узел администратора и выбрать «Сообщение»



На рабочем месте администратора всплывет уведомление



Задание 10. Компрометация узла защищенной сети

Перед началом выполнения зафиксировать скриншотами имеющуюся структуру сети и окно УКЦ с вариантами персонального ключа компрометируемого пользователя, т. к. в случае неудачной компрометации структура сети может нарушиться.

Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС:

1. скомпрометировать ключи пользователя UserCli на узле Пользователь_2 Филиал,
2. произвести смену ключей пользователя и сетевых узлов,
3. отправить обновления и произвести процедуру смены ключа пользователя на узле Пользователь_2 Филиал (фиксировать все шаги),
4. проверить работу защищенной сети после обновления отправив сообщение от пользователя UserCli администратору.

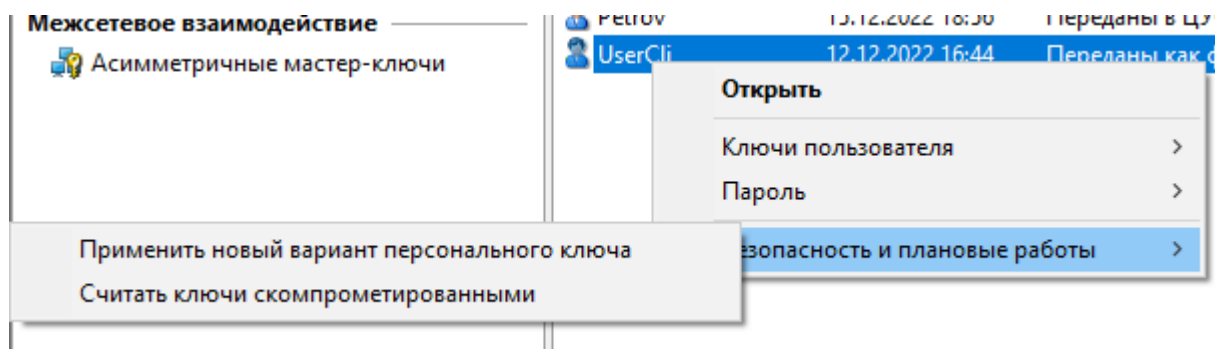
Восстановление взаимодействия с помощью ручной установки DST засчитано не будет.

Необходимо зафиксировать процесс настройки скриншотами или иным указанным способом:

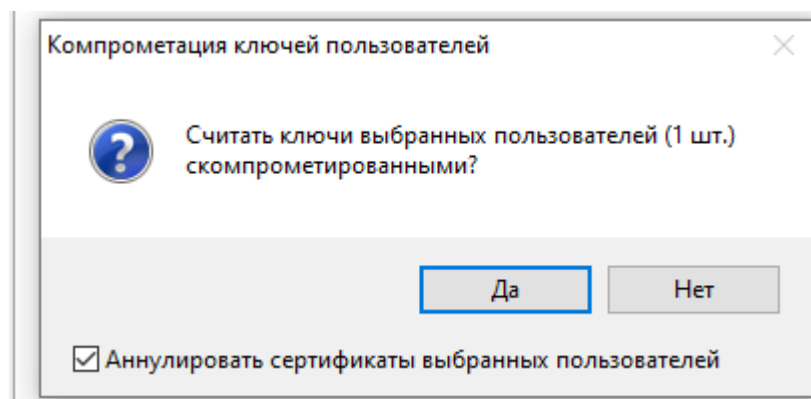
- компрометация пользователя.
- смена ключей пользователя и сетевых узлов.
- процедура смены ключа на клиенте с использованием резервного набора ключей.
- скриншот экрана «защищенная сеть» в Monitor на узле Пользователь_2 Филиал + результат проверки доступности узлов.

Кроме того, нужно сохранить архив директории, в которой расположен резервный набор ключей на рабочем столе компьютера (после смены ключей).

10.1 Чтобы выполнить компрометацию ключи пользователя UserCli, следует на рабочем месте администратор сети в УКЦ перейти в «Пользователи», выбрать пользователя UserCli и считать ключи скомпрометированными

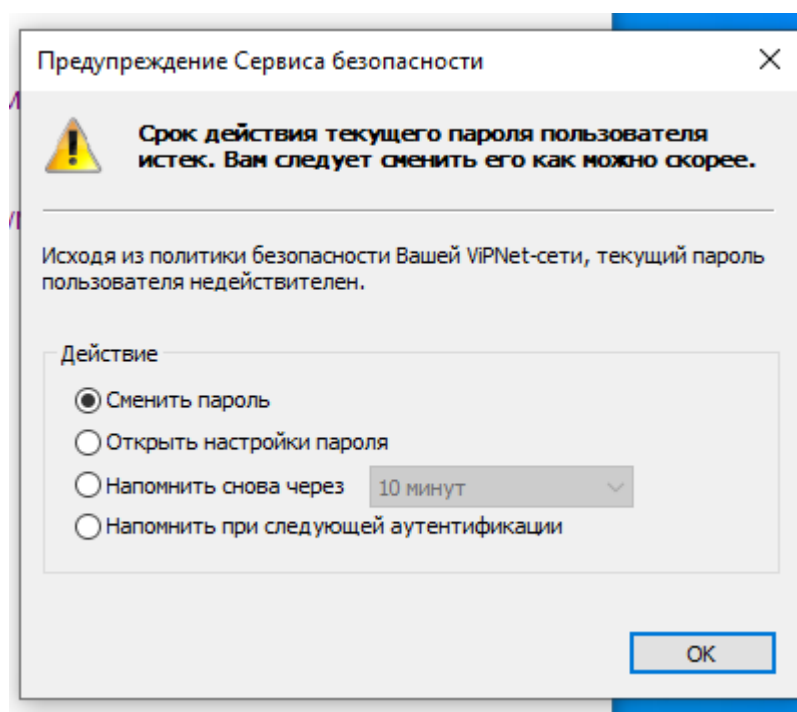


Аннулируем сертификаты

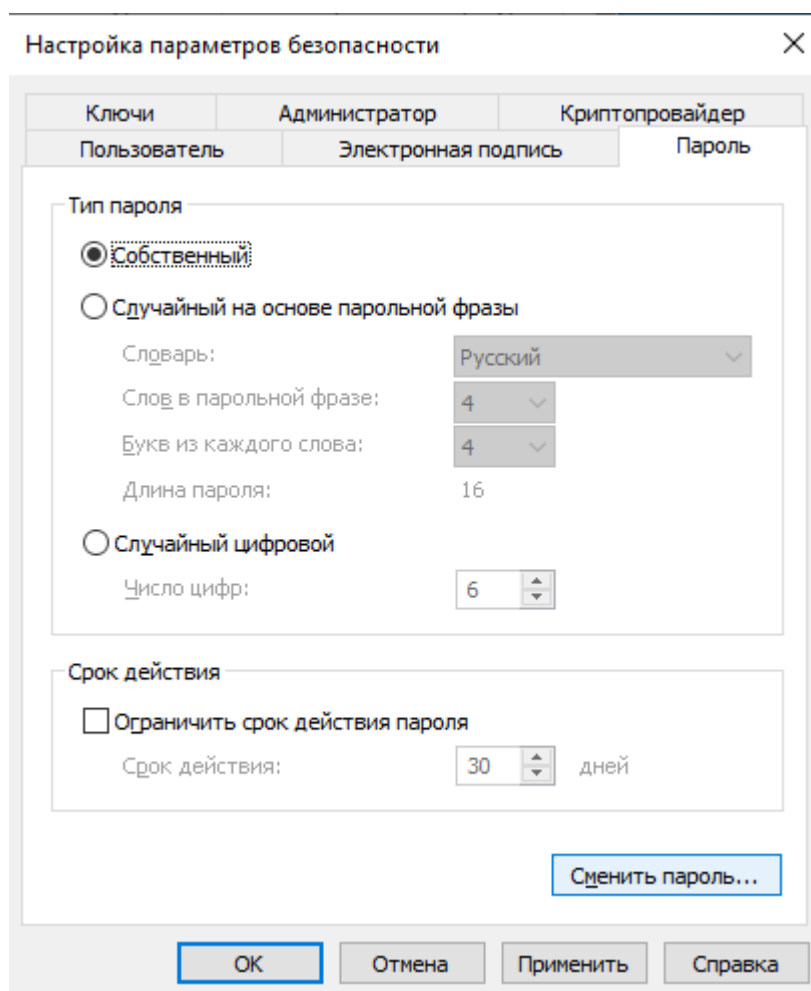


Важно! Создаем новые ключи пользователя и передаем в ЦУС, затем в сетевых узлах передаем в ЦУС. Сначала отправляем обновление на сетевой узел Пользователь_2 и дожидаемся уведомления от Системы безопасности

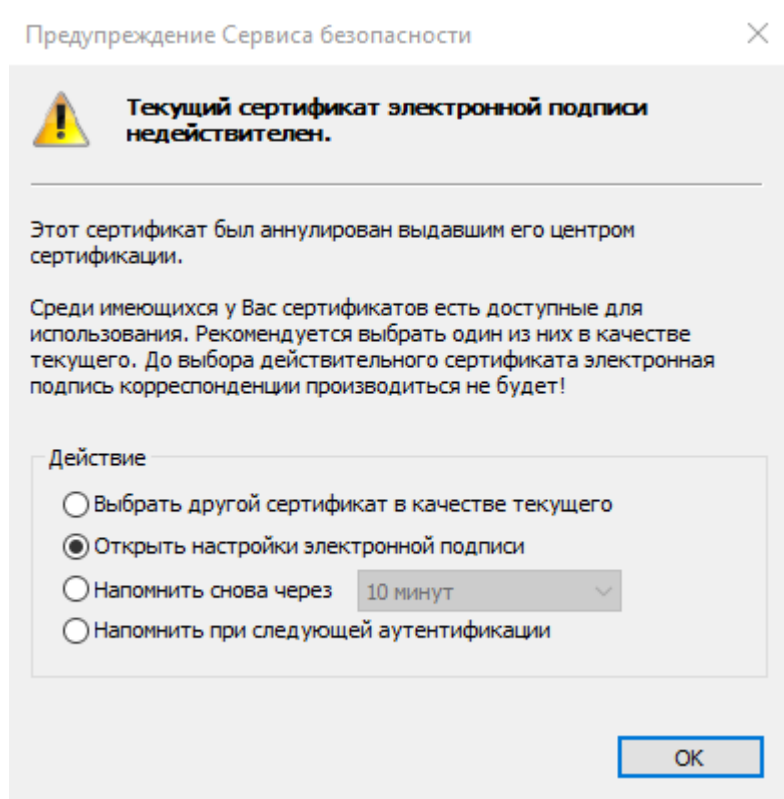
Имя	Сетевой адрес	Координатор	Дата изменен...	Справочни
Ivanov	14106.1.3	Координатор Центр Офис (VM)	19.12.22 14:36	Готовы к от
Главный администратор (VM)	14106.1.1	Координатор Центр Офис (VM)	19.12.22 14:36	Готовы к от
Оператор УЦ (VM)	14106.1.2	Координатор Центр Офис (VM)	19.12.22 14:36	Готовы к от
<input checked="" type="checkbox"/> Пользователь_2 Филиал (VM)	14106.2.1	Координатор Филиал (VM)	19.12.22 14:37	Отправлен



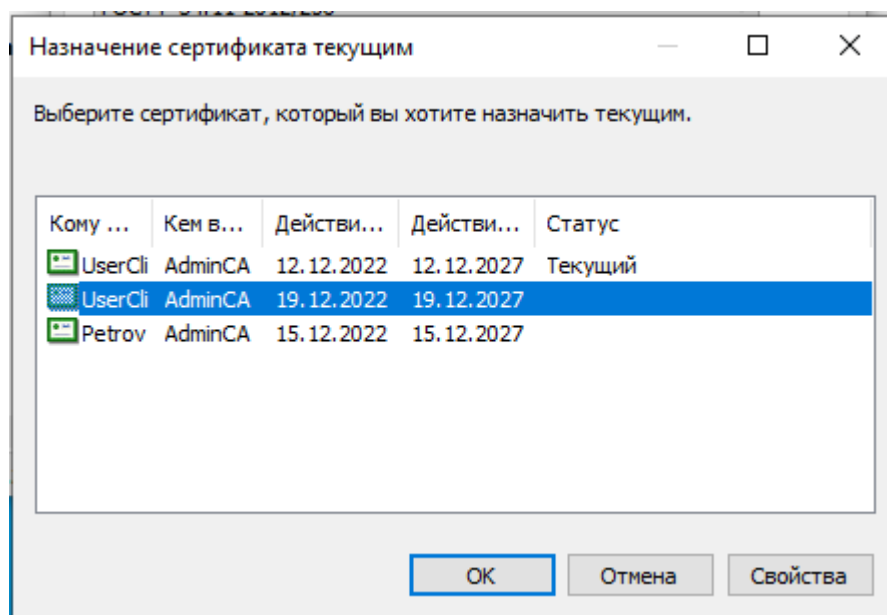
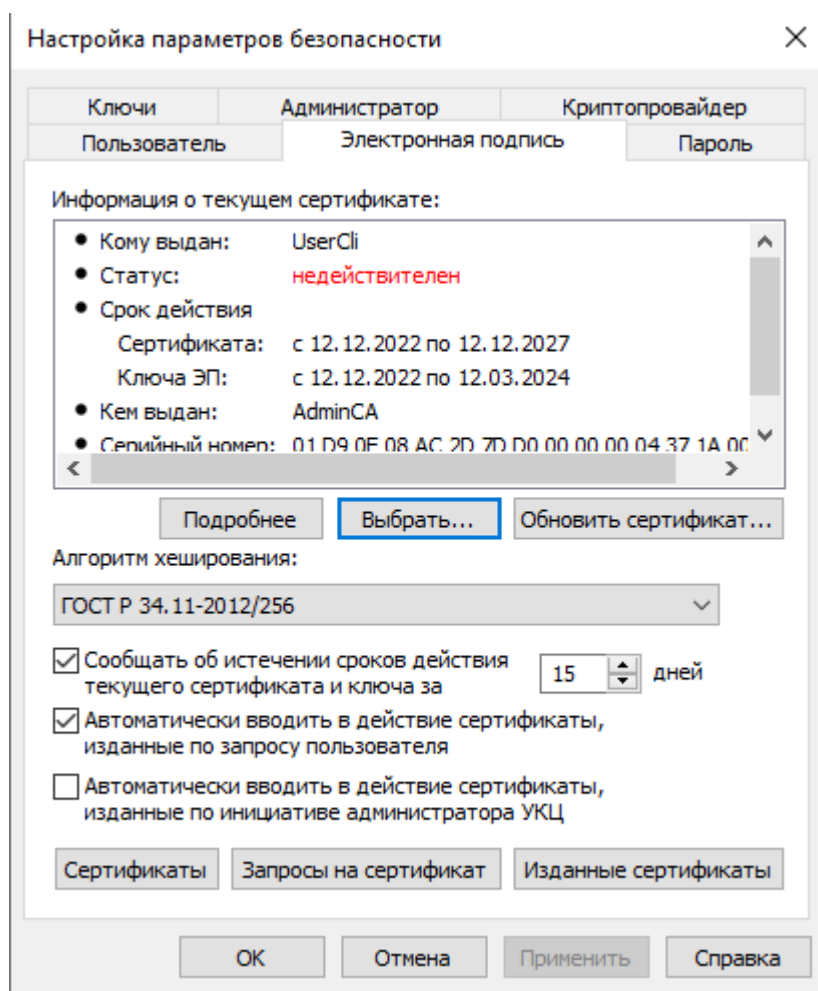
Открыть настройки пароля, тип пароля установить собственный и «Установить пароль»



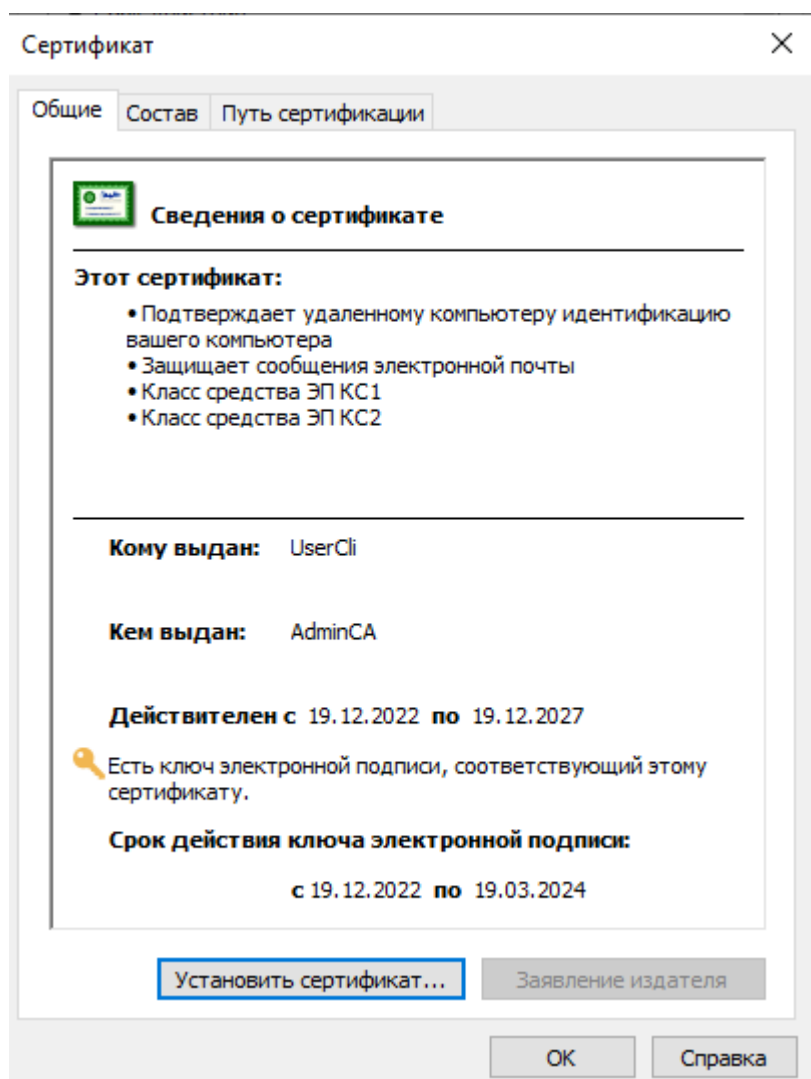
Устанавливаем пароль. Сохраняем изменения. После снова Сервис безопасности уведомит нас. Открываем настройки ЭП



В настройках электронной подписи, выбираем сертификат



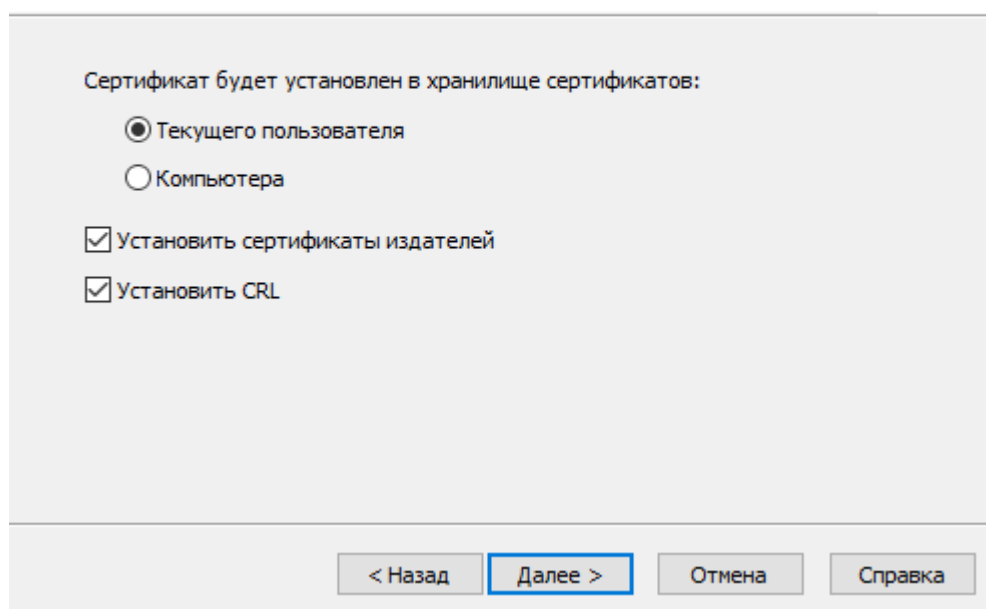
Текущий сертификат от 12.12.2022 был аннулирован во время компрометации пользователя, выбираем новый сертификат от 19.12.2022, который выпускали вместе с ключами и устанавливаем сертификат



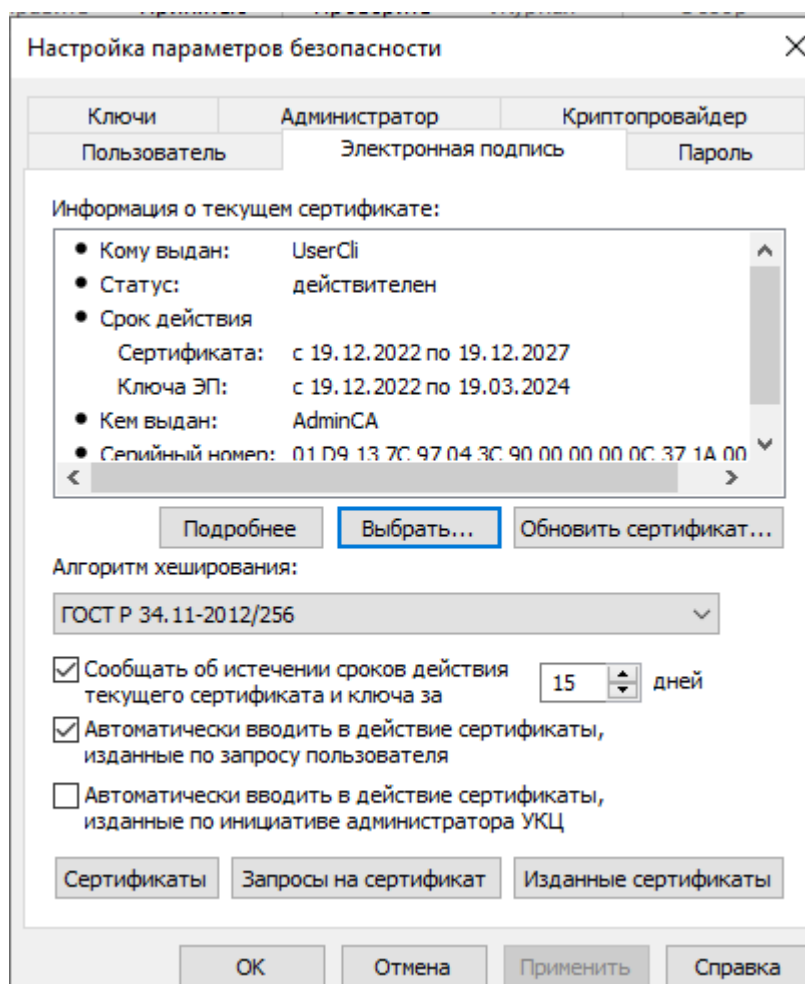
Мастер установки сертификатов

Выбор хранилища сертификатов

Хранилища сертификатов - это области системы, в которых производится хранение сертификатов.



После установки сертификата, статус о текущем сертификате изменился на действителен. Сохраняем.





Следующее, что нужно сделать, обновить справочники и ключи на сетевых узлах и после на координаторах

Проверить статусы справочников на всех узлах и координаторах

Клиенты					Найти
<input type="checkbox"/>	Имя	Сетевой адрес	Координатор	Дата изменен...	Справочники и
	Ivanov	14106.1.3	<u>Координатор Центр Офис (VM)</u>	19.12.22 14:58	Отправлены
	Главный администратор (VM)	14106.1.1	<u>Координатор Центр Офис (VM)</u>	19.12.22 15:00	Приняты
	Оператор УЦ (VM)	14106.1.2	<u>Координатор Центр Офис (VM)</u>	19.12.22 15:05	Приняты
	Пользователь_2 Филиал (VM)	14106.2.1	<u>Координатор Филиал (VM)</u>	19.12.22 15:05	Приняты

Координаторы

<input type="checkbox"/>	Тип	Имя	Сетевой адрес	Справочники и ключи	Дата изменен...
		Координатор Филиал (VM)	14106.2.0	Приняты	19.12.22 15:05
		Координатор Центр Офис (VM)	14106.1.0	Приняты	19.12.22 15:05

Для более точной проверки сети, можно перезагрузить всю сеть

После перезагрузки, на машине UserClientправить всем доступным сетевым узлам (клиентам) сообщения и дождаться ответа, также проверить доступность узлов сети (F5)

Задание 11. Межсетевое взаимодействие защищённых сетей (со связями «все со всеми»)

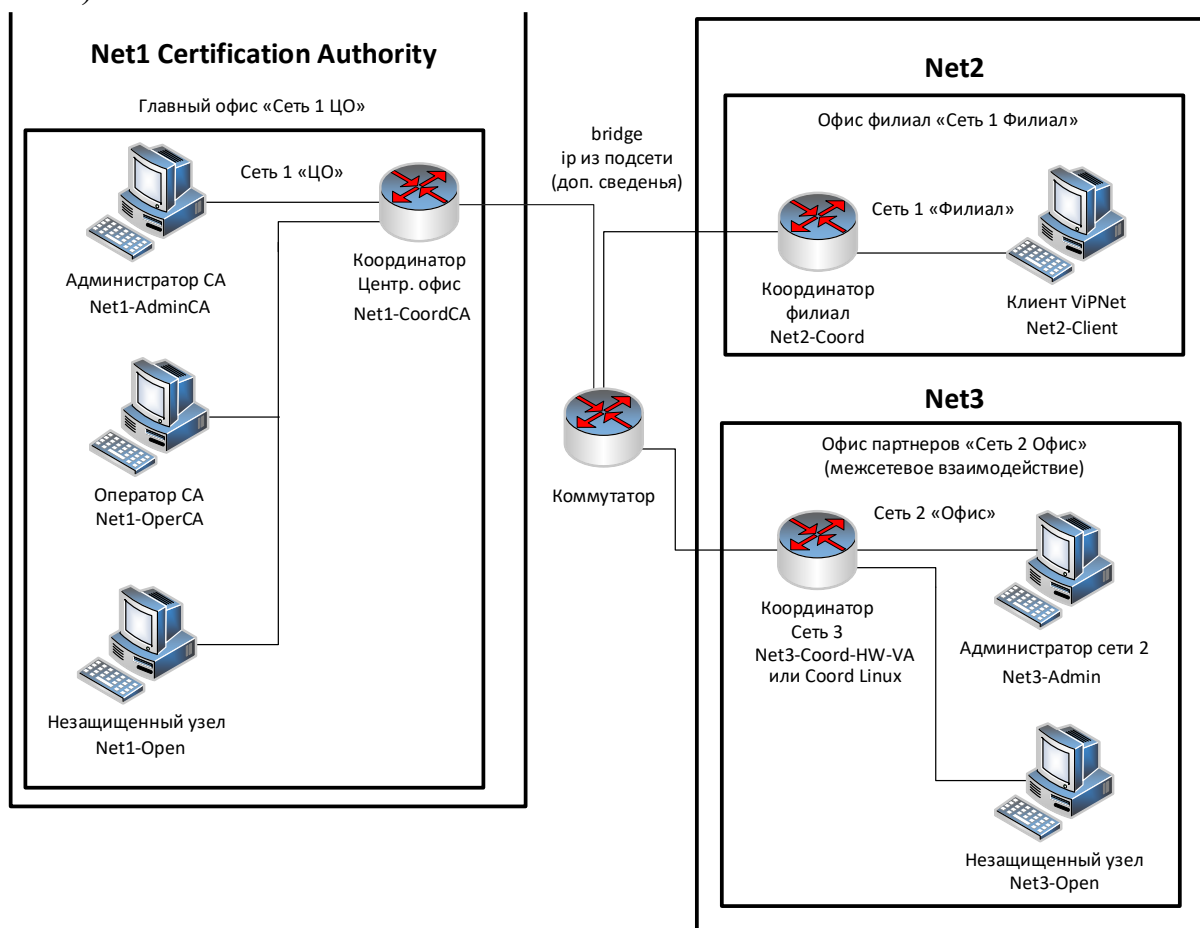


Рисунок 2 Схема межсетевого взаимодействия

Развернуть на Net3-Admin (Сеть 3 межсеть) на ПК рабочее место Администратора партнёрской сети, создать структуру второй сети: Рабочее место администратора (БД, ЦУС, УКЦ, Client)

- 1 координатор (Net3-Coord-HW-VA или координатор Linux),
- 1 узел Admin (Net3-Admin) и пользователь Admin,
- Установите координатор.

Все пароли пользователей в сети сделать ххХХ2233

Пароли администраторов сети сделать 3322ХХхх

Установить и настроить необходимое ПО

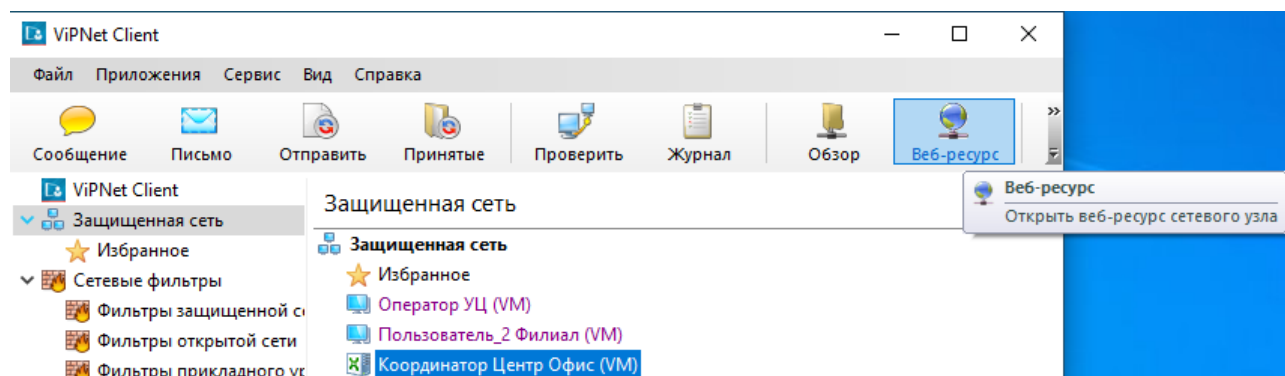
Настроить межсетевое взаимодействие между двумя защищёнными сетями, сделать скриншоты всех этапов установки межсетевого взаимодействия.

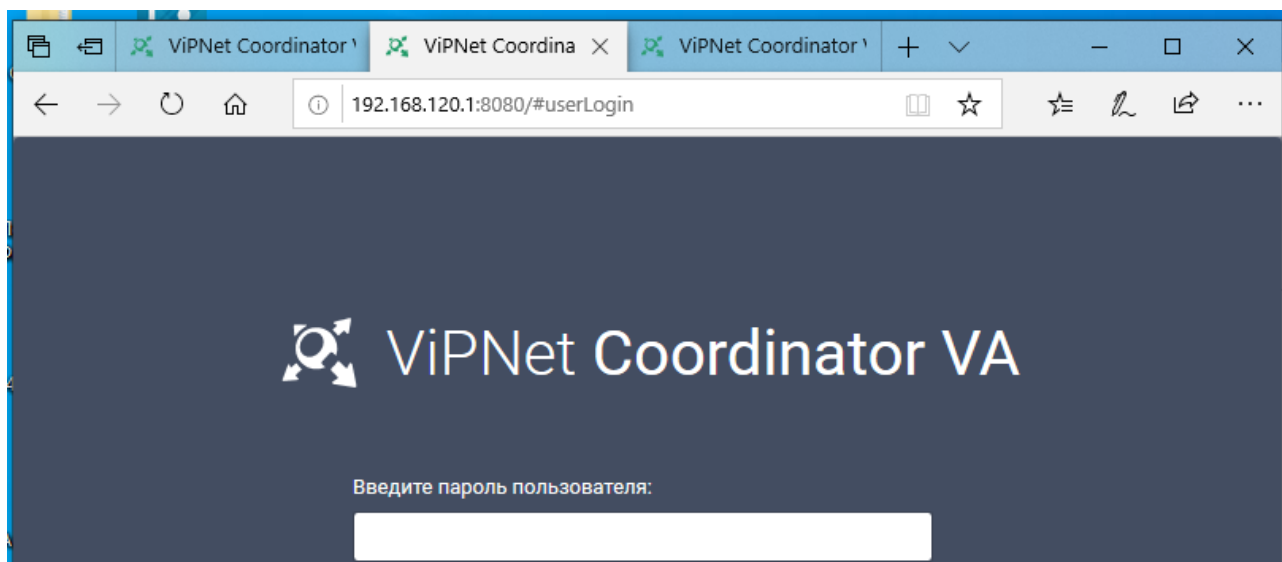
Проверить взаимодействие узлов, отправив сообщение деловой почты в программе Client Monitor с узла AdminCA (Net1-AdminCA) на Admin (Net3-Admin).

Настройка и развертывание сети выполнить в соответствии с пунктами 1-7. Но для установки лицензии выбрать 2-ю.

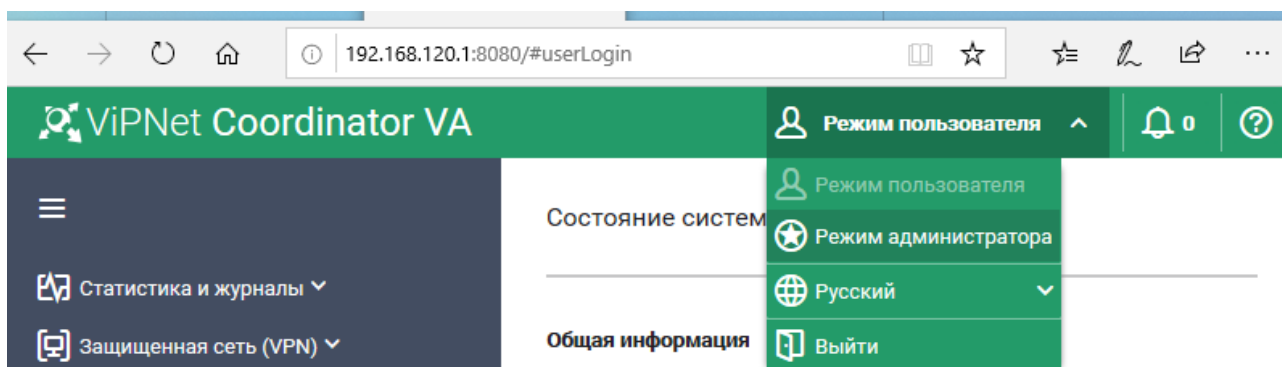
Для балансировки трафика и правильного распределения маршрутов для трафика, на всех 3 координаторах нужно выполнить настройку шлюзов.

На координаторе СА зайдем на веб интерфейс

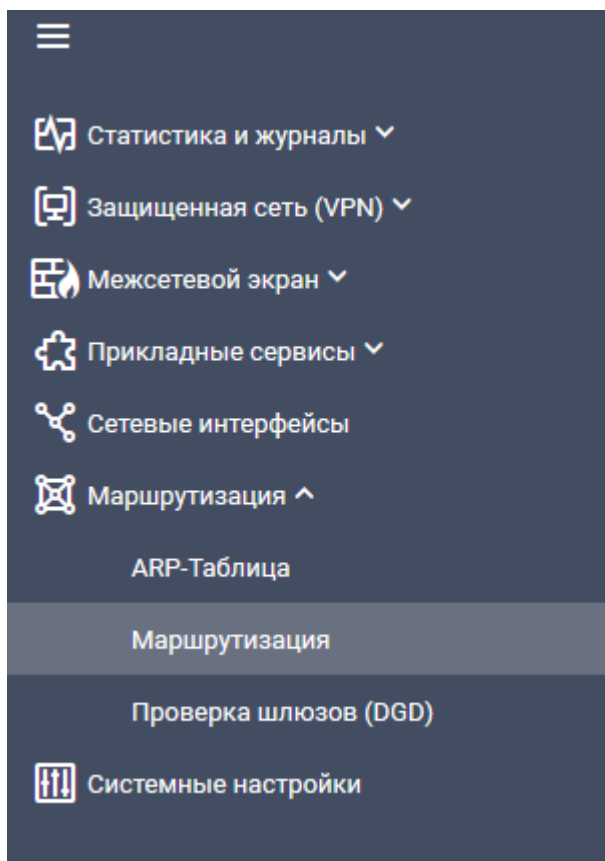




Подключимся к режиму администратора



Перейти в настройки маршрутизации и в статическую маршрутизацию




Маршрутизация



Сводная таблица

Статическая

Политики маршрутизации

 [Добавить маршрут](#)

Адрес назначения ...	Шлюз	Дис...	Вес
----------------------	------	--------	-----

Таблица маршрутизации по умолчанию

0.0.0.0/0	198.18.20.2	10	1
-----------	-------------	----	---

Таблица показывает, что для маршрута по умолчанию установлен шлюз координатора филиала, нужно добавить внешний ip-адрес координатора из 3 сети (198.18.20.3)

Добавление маршрута

Таблица маршрутизации:

По умолчанию

▼

Подсеть назначения:

По умолчанию

0 - 0.0.0.0

▼

Адрес шлюза:

198.18.20.3

Дистанция:

10

Вес:

2

Сохранить

Отмена

Аналогично повторяет для других Координаторов

Для координатора филиала

Добавление маршрута

Таблица маршрутизации:

По умолчанию

▼

Подсеть назначения:

По умолчанию

0 - 0.0.0.0

▼

Адрес шлюза:

198.18.20.3

Дистанция:

10

Вес:

2

Сохранить

Отмена

Для координатора 3 сети

Добавление маршрута

Таблица маршрутизации:

По умолчанию

Подсеть назначения:

По умолчанию

0 - 0.0.0.0

Адрес шлюза:

198.18.20.2

Дистанция:

10

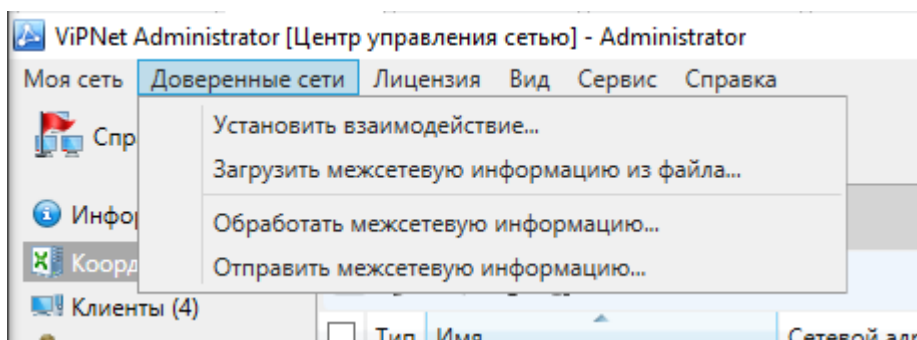
Вес:

2

Сохранить

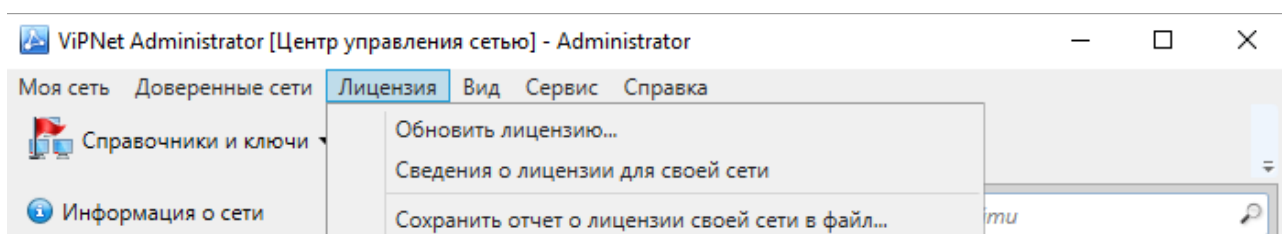
Отмена

Для настройки межсетевого взаимодействия в УКЦ главного администратора СА в «Доверенные сети» устанавливаем взаимодействие

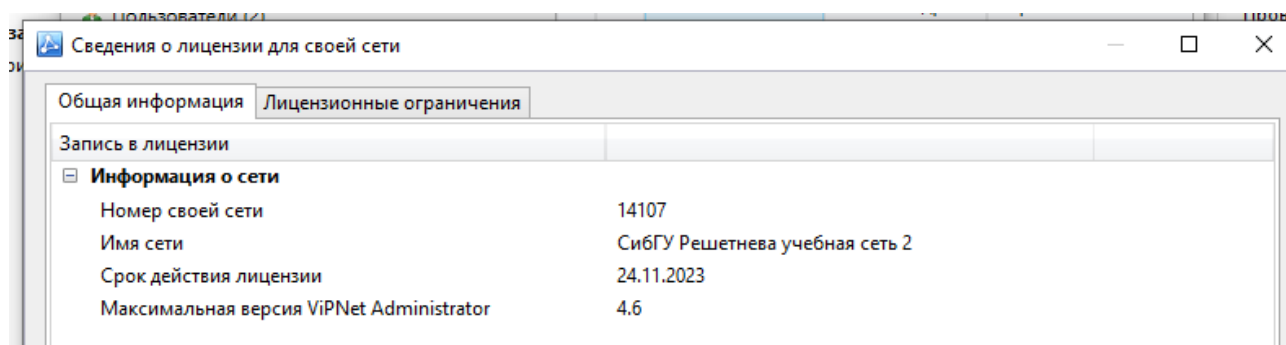


Выбираем пункт, что «Я инициатор ...». После потребуется указать номер сети, установить имя сети и выбрать координатор, через который будет осуществляется связь.

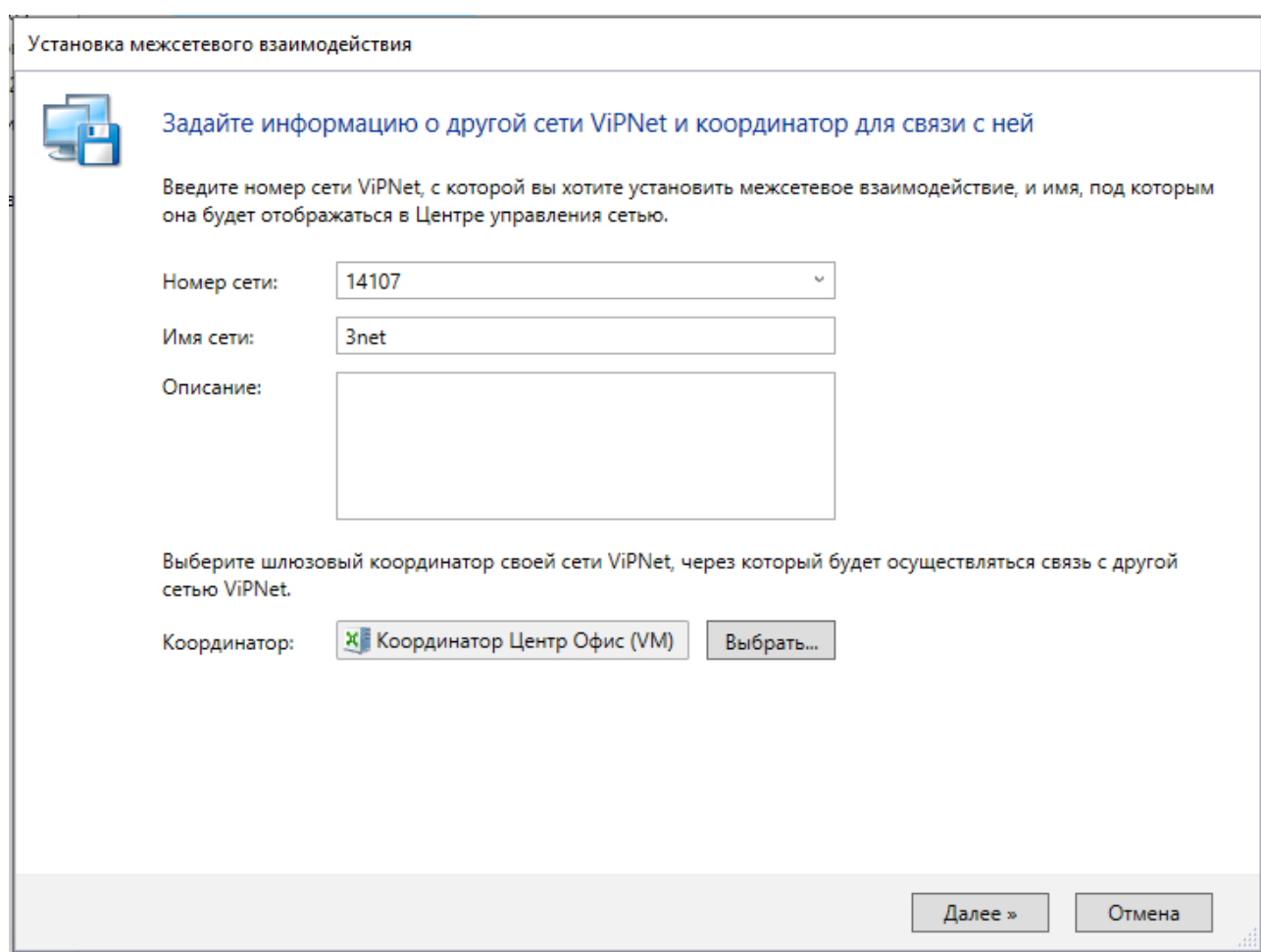
Чтобы узнать номер сети, переходим на рабочее место администратора 3-й сети и в УКЦ в меню «Лицензия» и смотрим сведения о лицензии своей сети



В открывшемся окне виден номер сети ViPNet



Заполненная информация о другой сети будет иметь следующий вид



Переходим далее. Выбираем 2 сетевых узла, которые нужны для установления связи

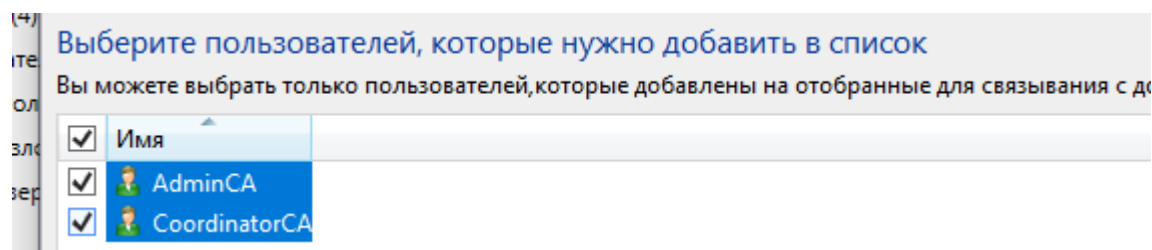


Укажите сетевые узлы своей сети ViPNet

Добавьте в список сетевые узлы своей сети, которые будут доступны для установ ViPNet.

<input checked="" type="checkbox"/>	Тип	Имя
<input checked="" type="checkbox"/>		Главный админ...
<input checked="" type="checkbox"/>		Координатор Ц...

Добавляем 2-х пользователей



Сообщение для администратора сети можно не заполнять

Создадим на рабочем столе папку с произвольным названием и сохраним туда файл межсетевой информации



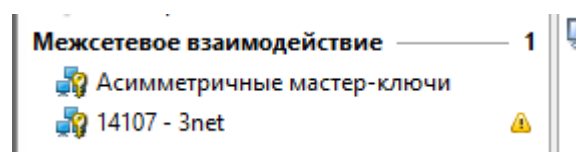
Укажите файл для сохранения межсетевой информации

Задайте папку и имя файла, в который будет сохранена межсетевая информация для другой сети ViPNet.

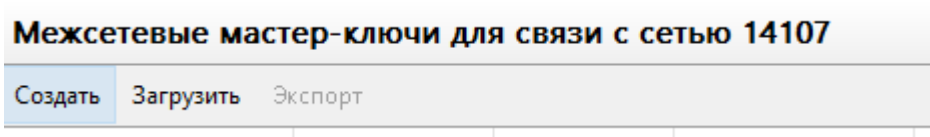
C:\Users\F7\Desktop\14107\14106-14107.lzh

Обзор...

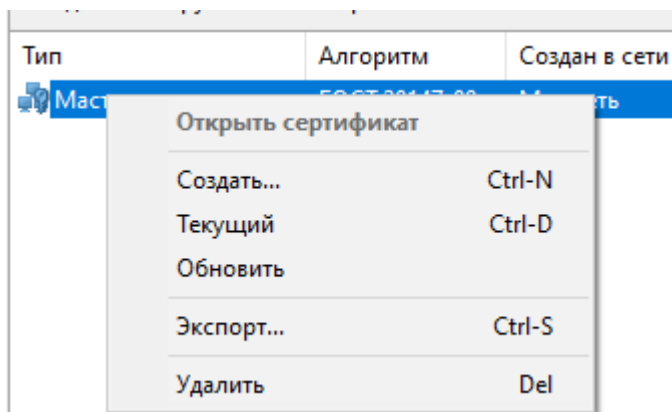
Следующим шагом переходим в УКЦ. Появляется пункт для создания мастер-ключа для доверенной сети



Создадим мастер-ключ

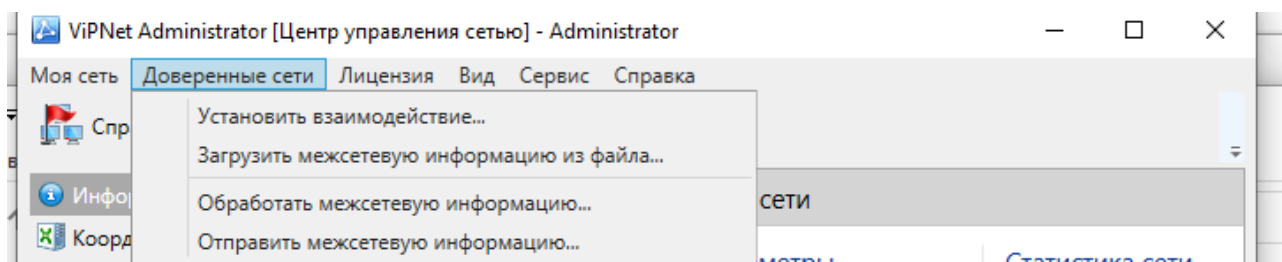


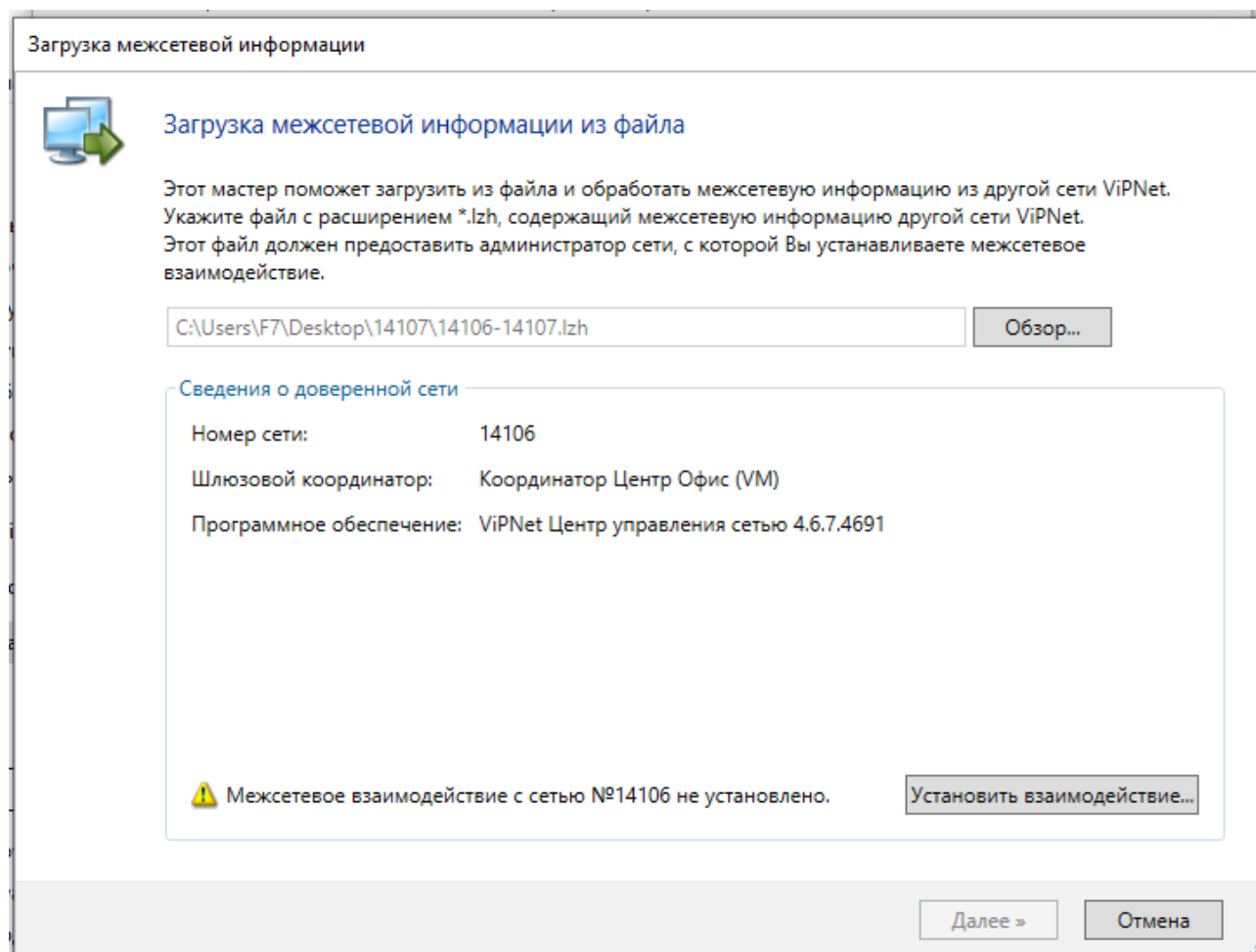
Далее экспортируем мастер-ключ в ту же папку что и файл межсетевой информации и установим этот мастер-ключ как текущий.



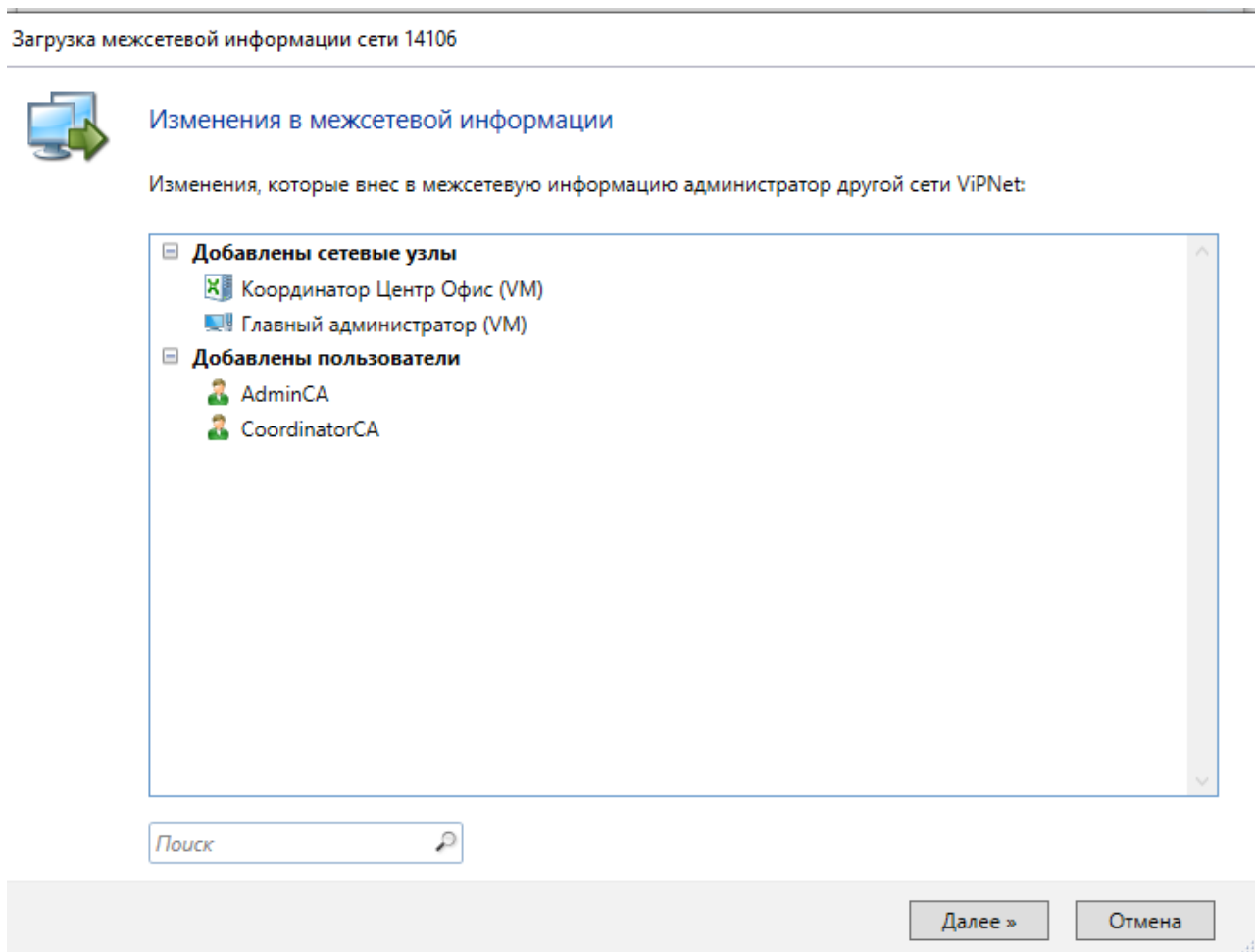
Теперь, после того как все файлы созданы и сохранены их нужно передать администратору доверенной сети

На месте администратора (Net3) в ЦУС выбираем «Доверенные сети» и загружаем межсетевую информацию из файла

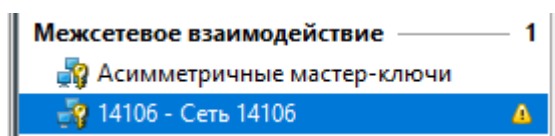




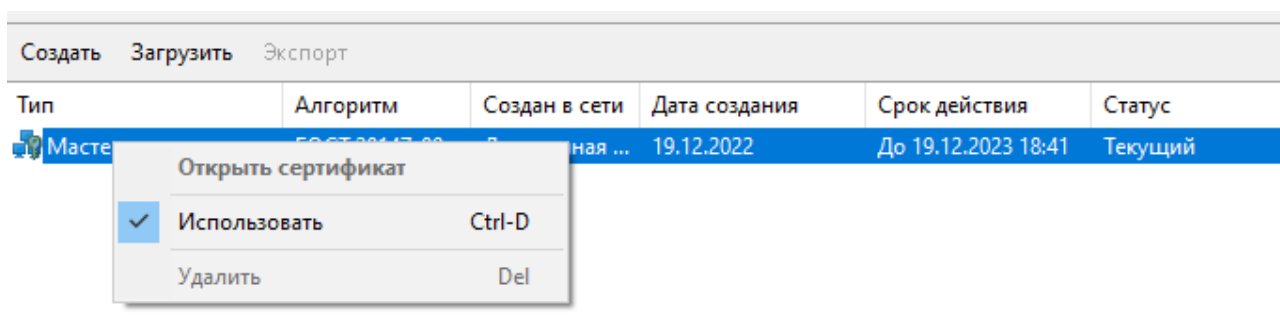
Устанавливаем взаимодействие. Выбираем координатора и продолжаем



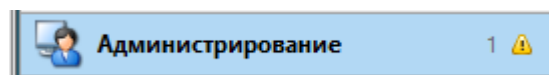
Оставляем как есть и переходим далее. Загрузка межсетевой информации завершена. Переходим в УКЦ. Появляется новая вкладка для мастер-ключа



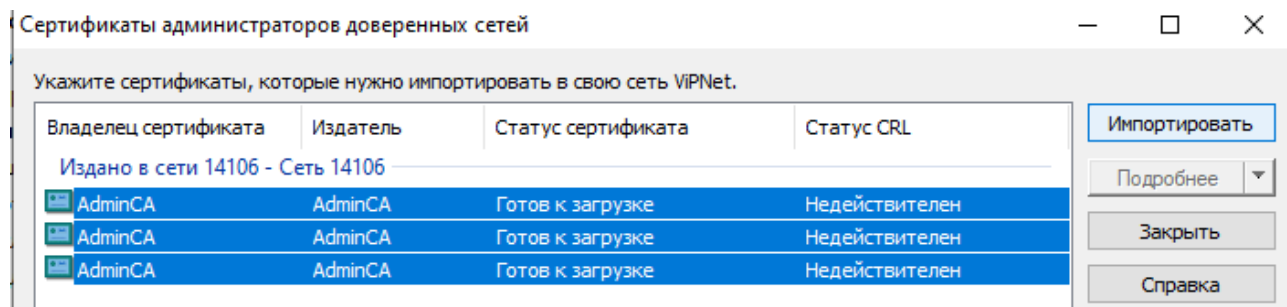
Загружаем мастер-ключ и используем



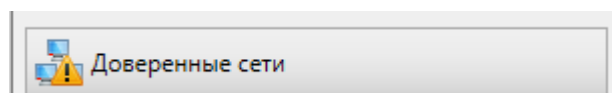
В меню «Администрирование»



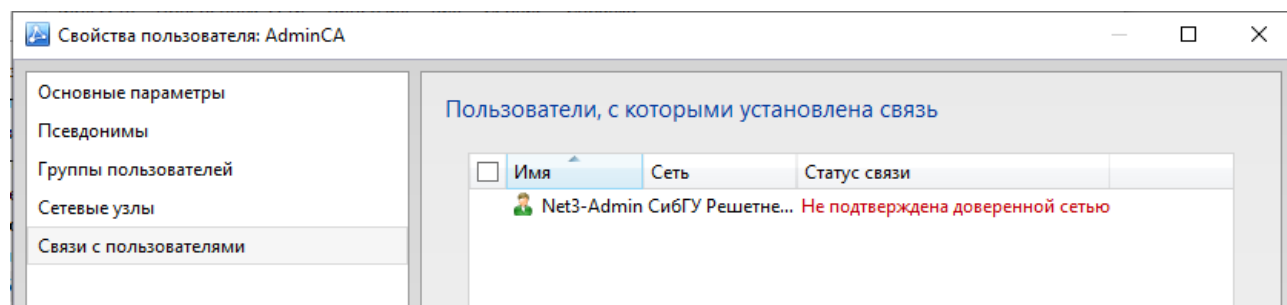
Обрабатываем сертификат из доверенной сети. Импортируем все сертификаты.



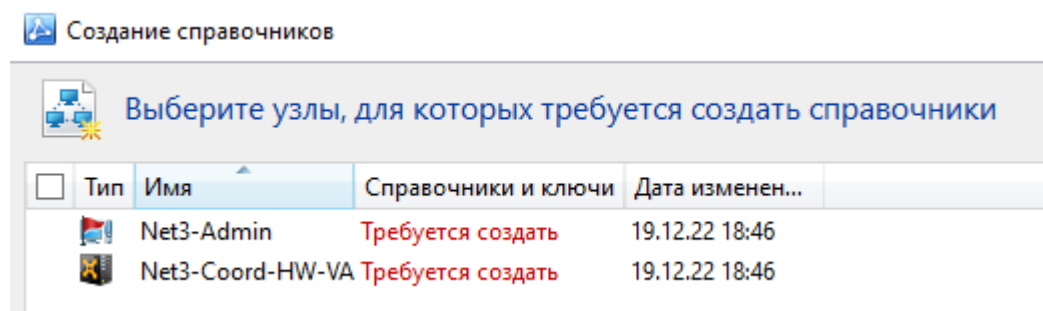
В ЦУС переходим в доверенные сети



Открываем вкладку с пользователями. С пользователем AdminCA устанавливаем связь с пользователем Net3-Admin



Создаем справочники в ЦУС для сетевых узлов. В УКЦ – Сетевые узлы создаем ключи и передаем их в ЦУС. После этого отправляем справочники и ключи на сетевые узлы



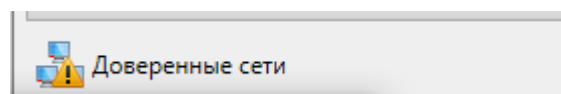
Сетевые узлы						
Т.	Имя узла	Вари...	Ключи	Статус ключей	CRL	Статус С
	Net3-Admin	0	19.12.2022 17:05	Требуется создать...	19.12.2022 17:05	Неактуа
	Net3-Coord...		19.12.2022 17:05	Требуется создать...	19.12.2022 17:05	Неактуа

Отправка справочников и ключей

Выберите узлы, на которые требуется отправить справочники и ключи. В списке отображаются сетевые узлы, на которые требуется отправить справочники и ключи.

<input type="checkbox"/>	Тип	Имя	Справочники и ключи	Дата изменен...
<input type="checkbox"/>		Net3-Admin	Готовы к отправке	19.12.22 18:51
<input type="checkbox"/>		Net3-Coord-HW-VA	Готовы к отправке	19.12.22 18:51

В ЦУС переходим в доверенные сети и создаем межсетевую информацию



Свойства сетей

14106 - Сеть 14106

- Координаторы (1)
- Клиенты (1)
- Пользователи (2)
- Группы пользователей (0)

Информация о доверенной сети

Общая информация

Номер и имя сети
14106 "Сеть 14106"

Исходящая межсетевая информация
Требуется создать

Входящая межсетевая информация
Принята

Объекты д

Координатор
Клиенты:
Пользователи:
Группы поль:

Объекты м

Координатор
Клиенты:
Пользователи:

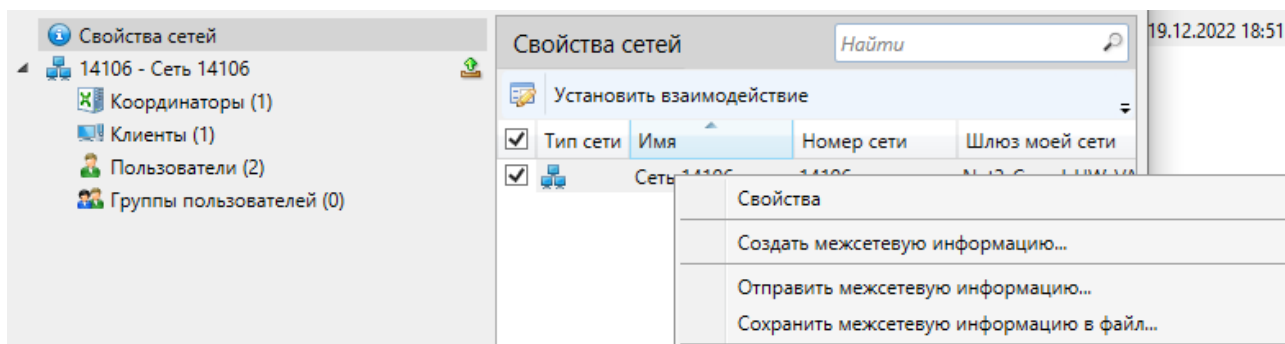
ViPNet Administrator [Центр управления сетью]

Будет создана межсетевая информация для выбранной сети.

☐ Отправить межсетевую информацию после создания

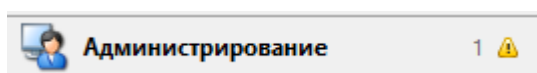
Создать Отмена

После этого выгружаем межсетевую информацию в файл и передаем ее администратору доверенной сети

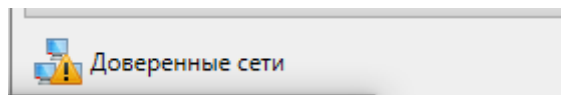


В ЦУС администратора СА загружаем межсетевую информацию из файла и подтверждаем все связи с пользователями и сетевыми узлами.

Обработаем контейнер с сертификатами от доверенной сети в «Администрирование»

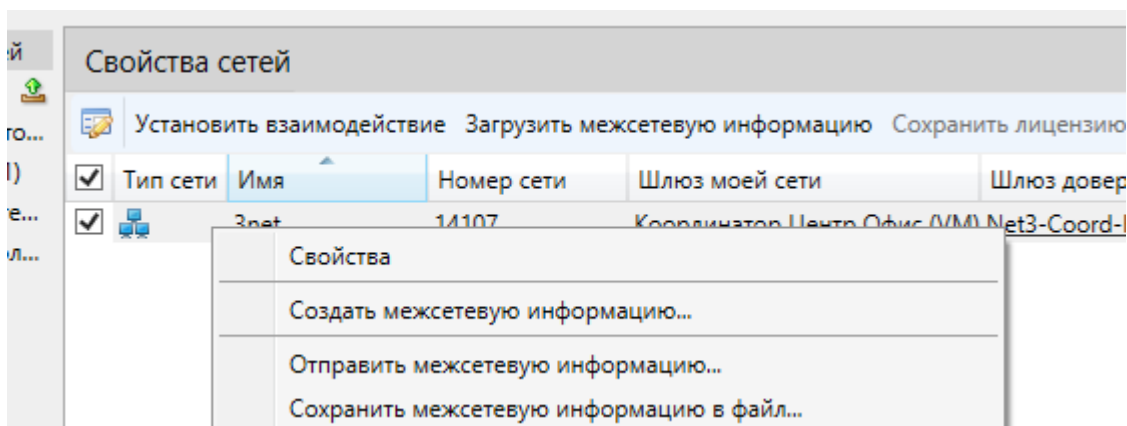


Создаем справочники в ЦУС для сетевых узлов. В УКЦ – Сетевые узлы создаем ключи и передаем их в ЦУС. После этого отправляем справочники и ключи на сетевые узлы



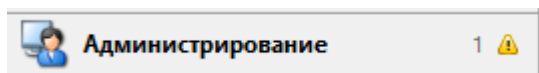
В ЦУС переходим в доверенные сети и создаем межсетевую информацию

После этого выгружаем межсетевую информацию в файл и передаем ее администратору доверенной сети



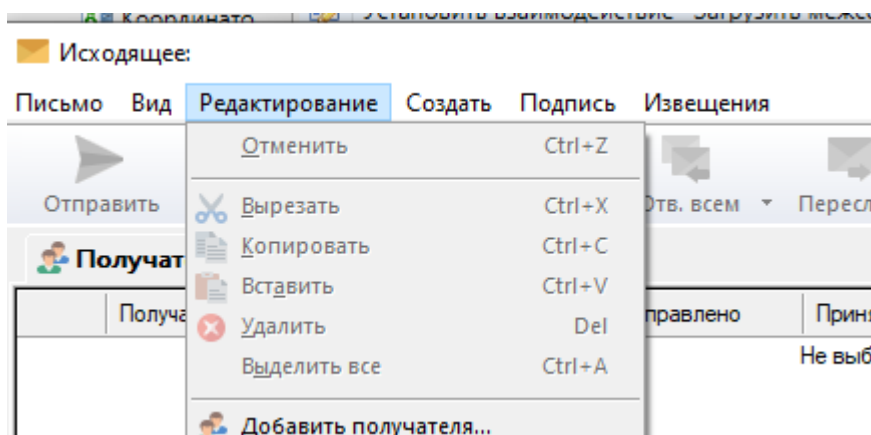
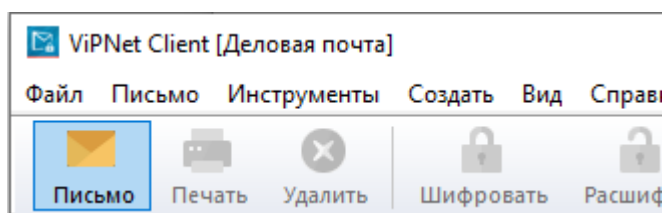
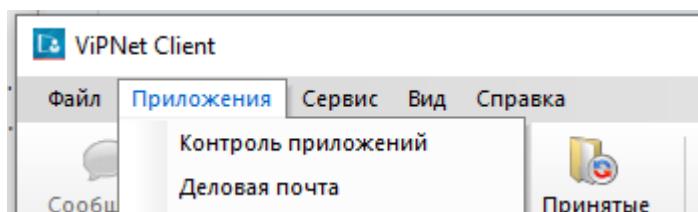
В ЦУС администратора СА загружаем межсетевую информацию из файла и подтверждаем все связи с пользователями и сетевыми узлами.



Обработаем контейнер с сертификатами от доверенной сети в «Администрирование»



Создаем справочники в ЦУС для сетевых узлов. В УКЦ – Сетевые узлы создаем ключи и передаем их в ЦУС. После этого отправляем справочники и ключи на сетевые узлы

На рабочем месте администратора СА открываем деловую почту и отправляем сообщение Net3-Admin, также отправить обычное сообщение через ViPNet клиент




Выбрать контакты		
Поиск		Основная адресная книга
Имя контакта	Имя узла	Описание
 AdminCA	Главный администратор (VM)	
 Net3-Admin	Net3-Admin (Сеть № 14107)	

Исходящее: asdas

Письмо Вид Редактирование Создать Подпись Извеще

Отправить Сохранить Печать Ответить Отв. всем

Получатели Вложения Свойства

Получатель	Отправлен
 [Net3-Admin (Сеть N 14107)/Net3-Admin/...	

Тема asdas

asdasd

ViPNet Client

Файл Приложения Сервис Вид Справка

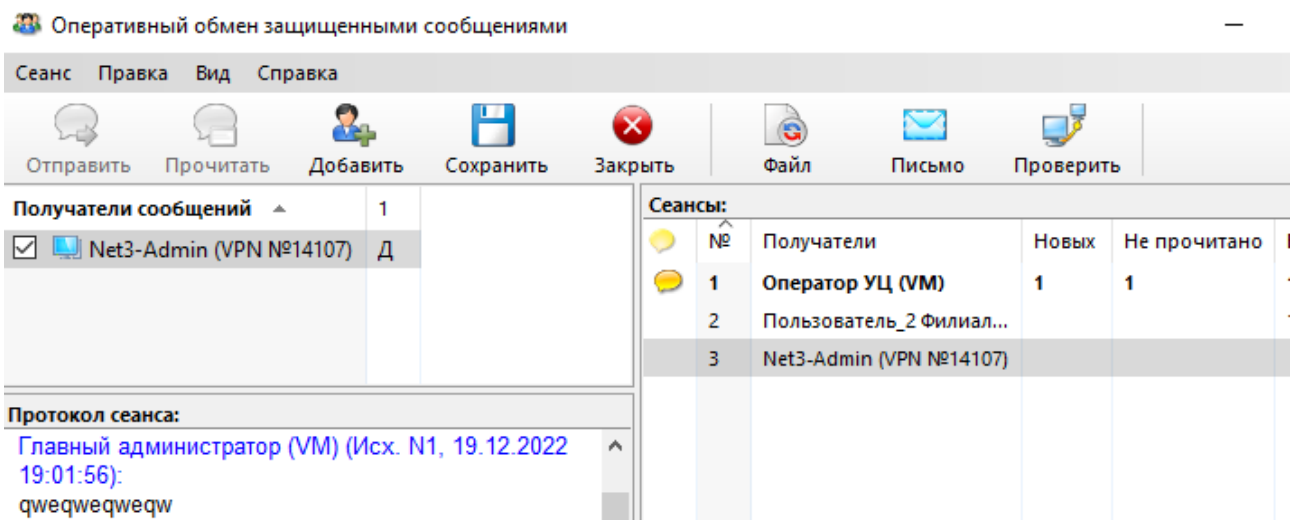
Сообщение Обмен защищенными сообщениями

Защищенная сеть

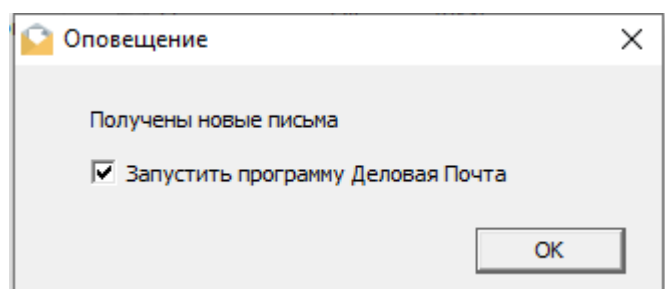
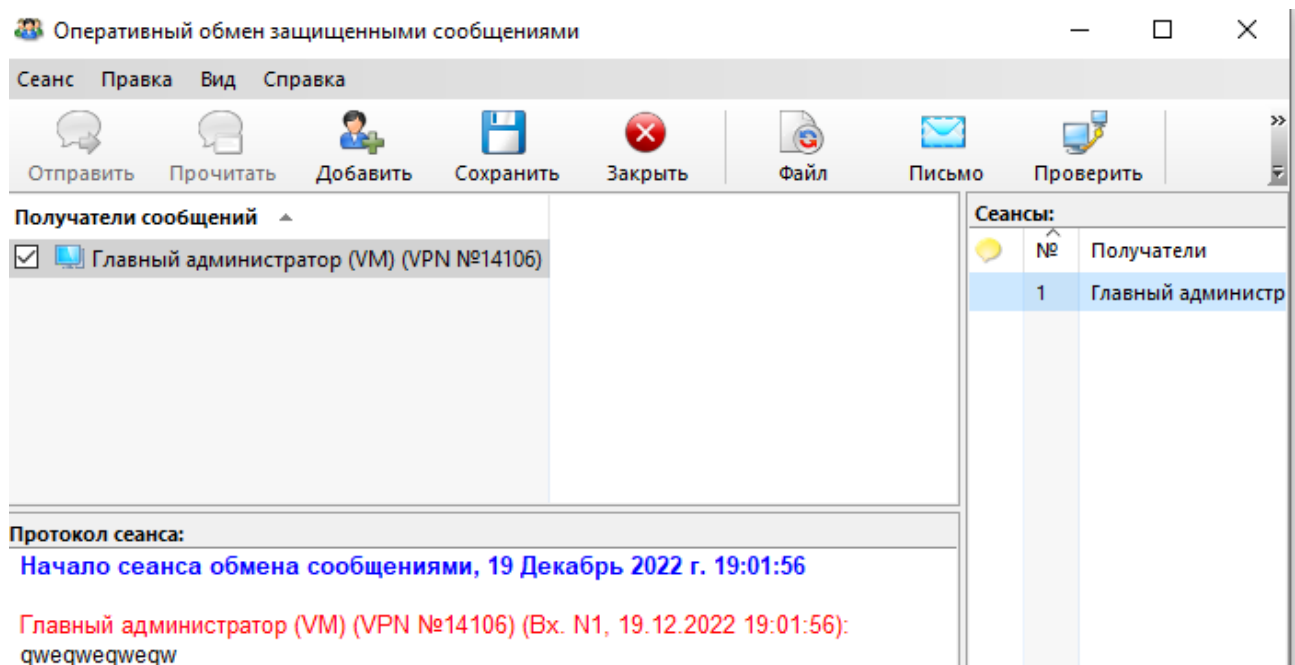
- Избранное
- Сетевые фильтры
- Фильтры защищенной сети

Защищенная сеть

- Избранное
- Net3-Admin (VPN №14107)



На администраторе 3-й сети подтвердить получение всех сообщений. И отправить сообщения в обратную сторону. Подтвердить их получение на администраторе СА.



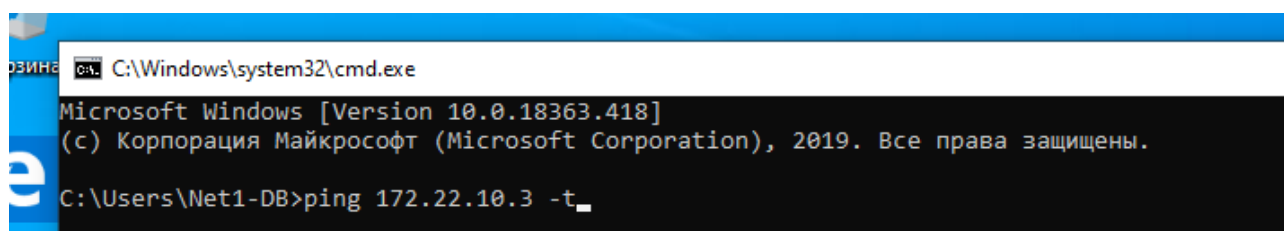
Задание 12. Туннелирование в рамках межсетевого взаимодействия

Подключить незащищенную машину в сети 3 (Net3-Open).

Для второй открытой машины использовать Net1-Open узел в сети 1

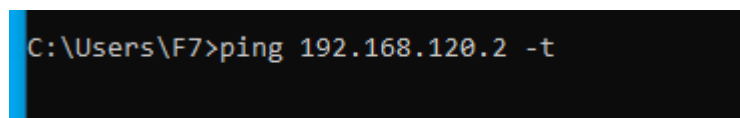
Настроить туннелирование таким образом, чтобы взаимодействие между открытыми узлами из разных сетей осуществлялось по зашифрованному каналу. Проверить доступность незащищённых машин друг другу с помощью ICMP (ping), а также любым другим протоколом, например smb (общая сетевая папка) или другим удобным (кроме ICMP); проанализировать журналы IP-пакетов на координаторах.

Для наглядного примера работы туннелирования, отправим с конечных узлов обеих сетей icmp пакеты. С незащищенного узла 1-ой сети



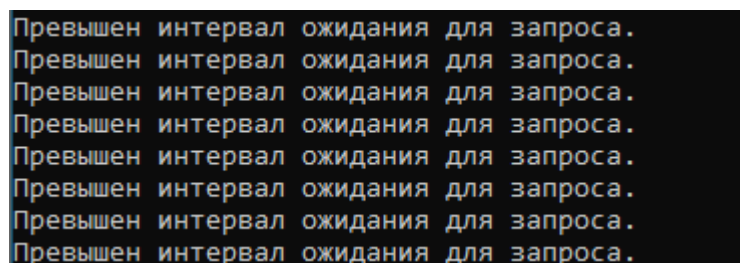
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.18363.418]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.
C:\Users\Net1-DB>ping 172.22.10.3 -t
```

С незащищенного узла 3-й сети



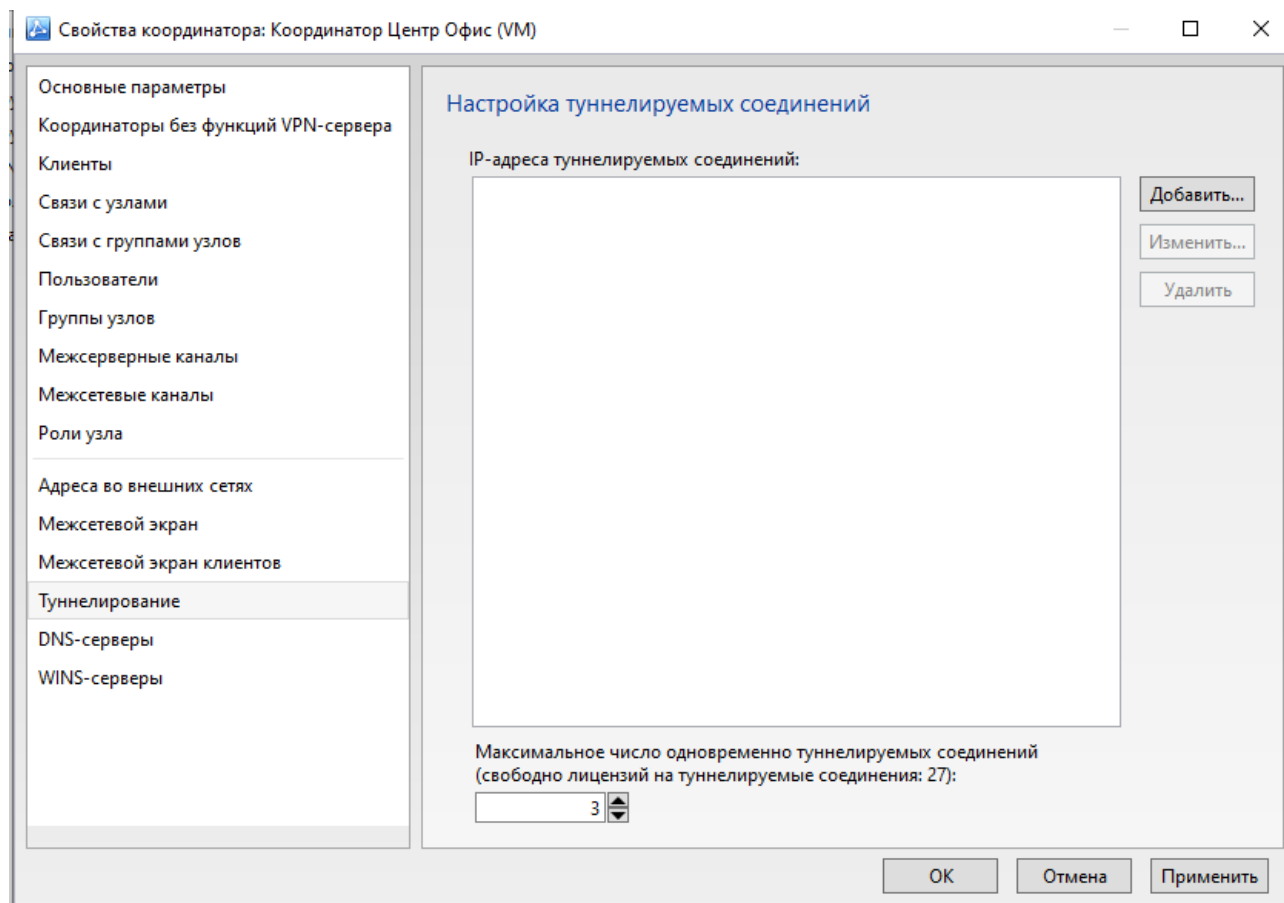
```
C:\Users\F7>ping 192.168.120.2 -t
```

На обеих машинах пинг не проходит с одинаковым сообщением

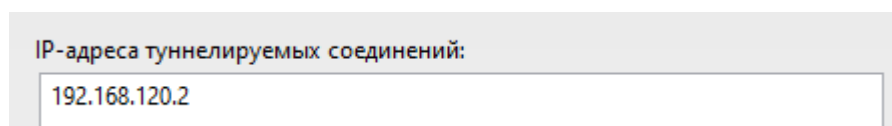


```
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
```

На рабочем месте администратора СА в УКЦ выбираем координатора, который будет туннелировать незащищенные узлы и в его свойствах «Туннелирование» указываем кол-во одновременных туннелируемых соединений, например, 3.

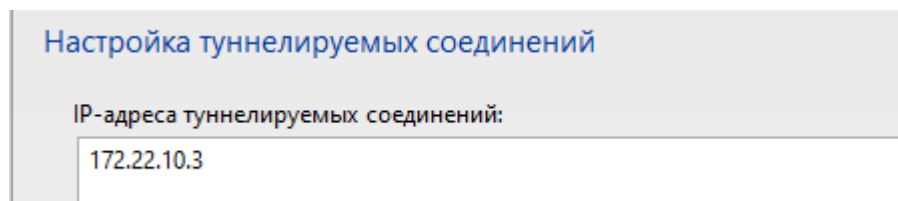


Добавим туннелируемый адрес



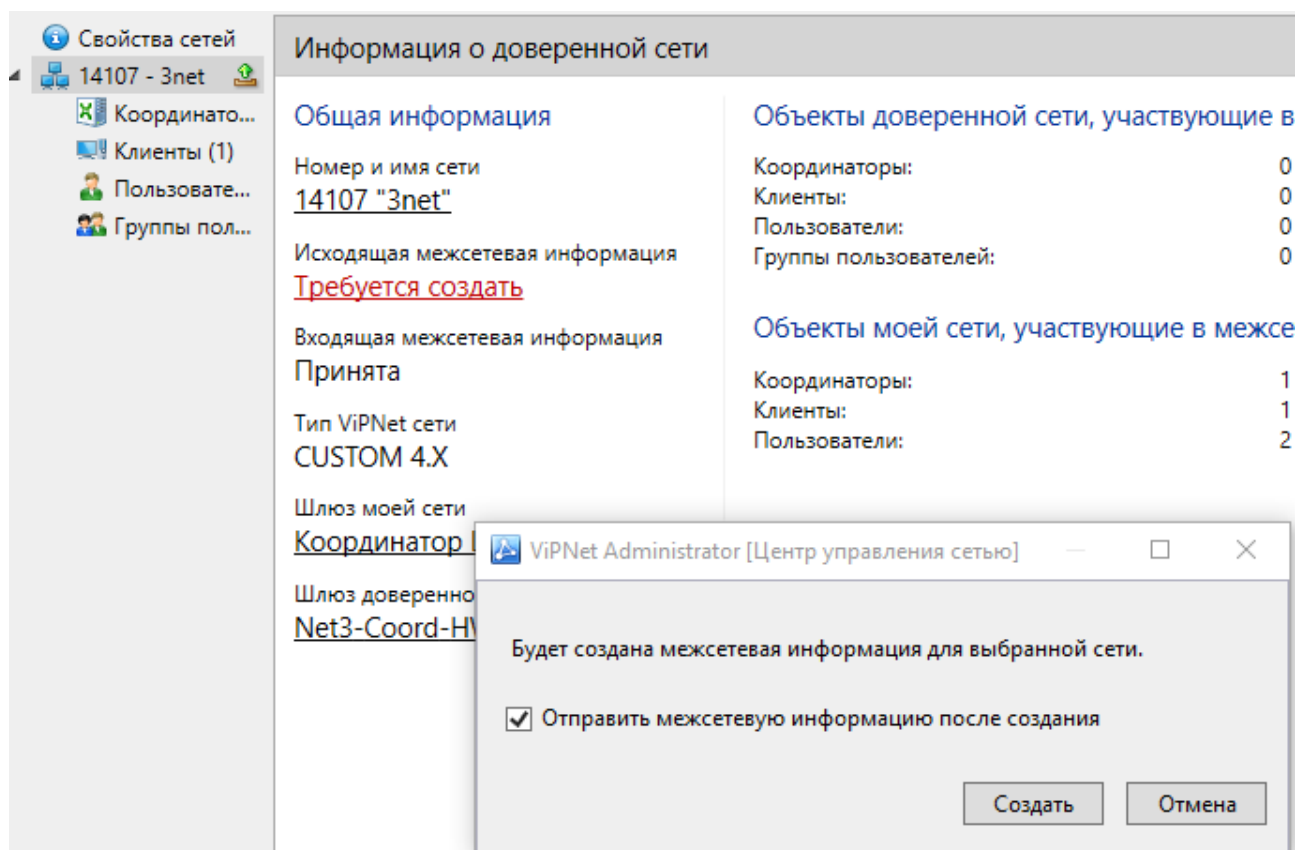
На рабочем месте администратора 3-й сети выполняем аналогичные действия.

Туннелируемый адрес

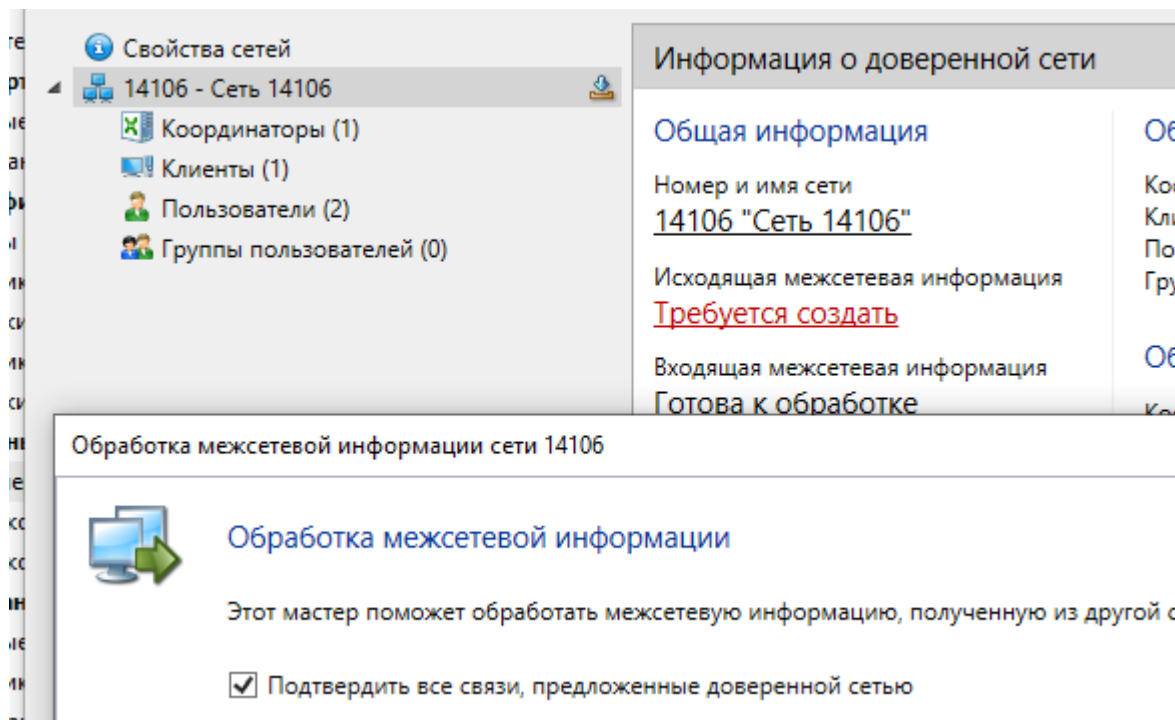


Создаем справочники и отправляем их в УКЦ, из УКЦ отправляем ключи в ЦУС и создаем справочники и ключи, после отправляем их на узлы. На рабочем месте администратора 3-й сети выполняем аналогичные действия.

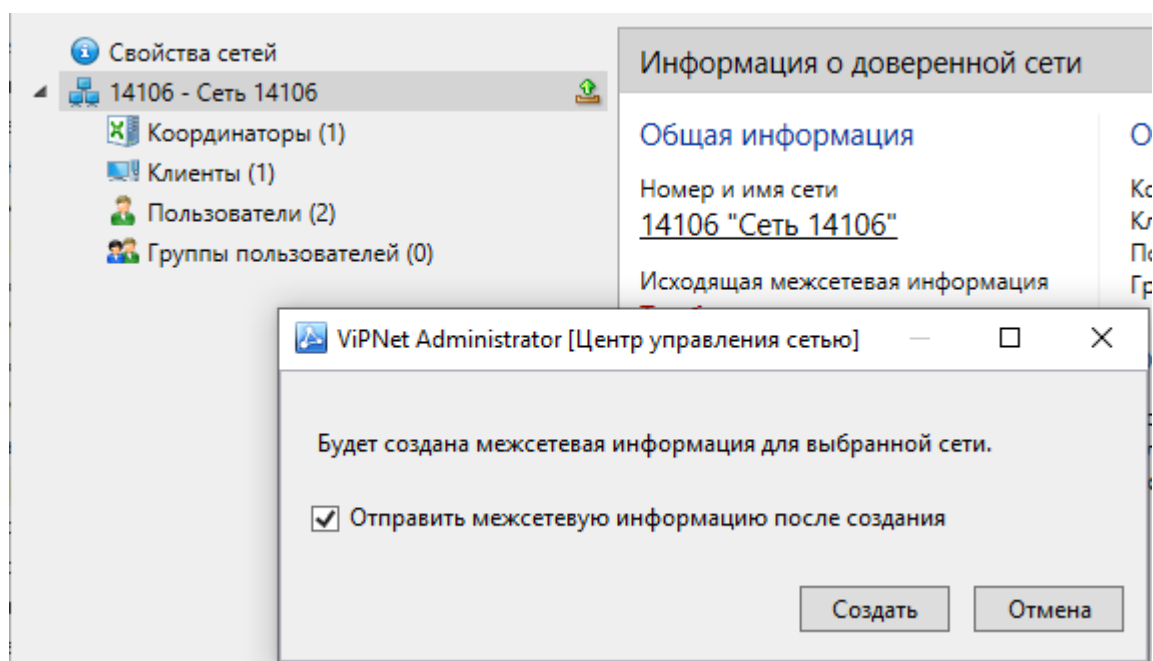
После отправки всех справочников, на рабочем месте администратора СА отправляем межсетевую информацию доверенной сети



На рабочем месте администратора перед тем как создать межсетевую информацию, обработаем входящую межсетевую информацию из 1-ой сети

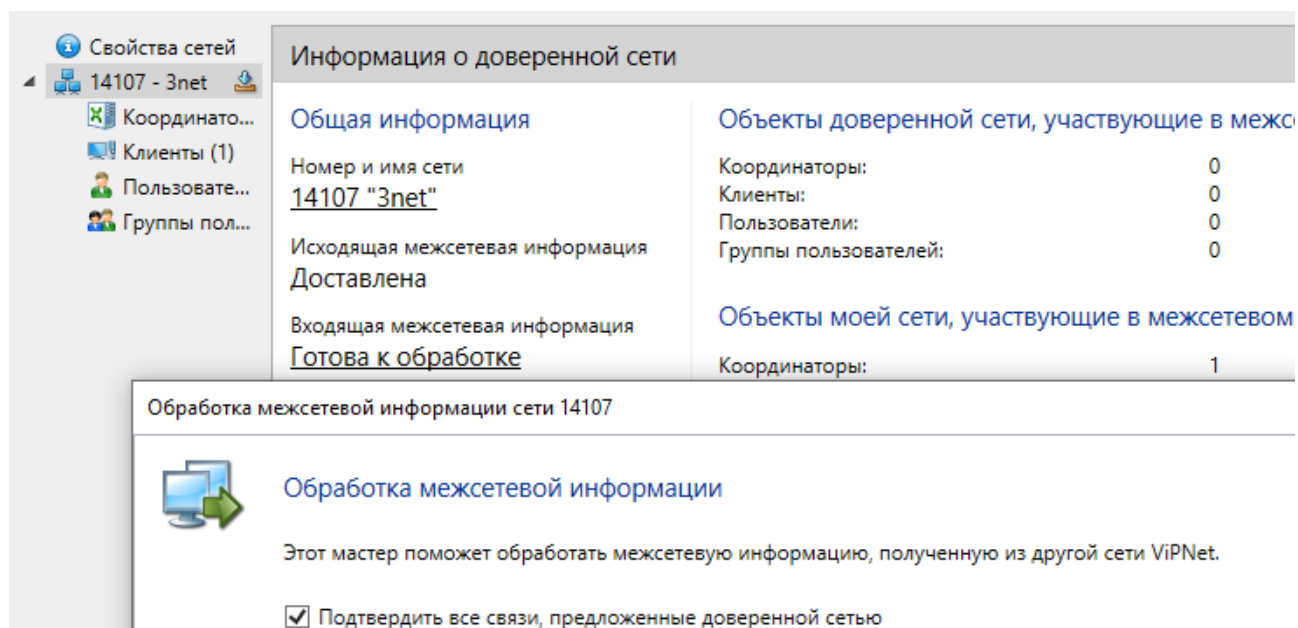


После этого создаем и отправляем межсетевую информацию в 1-ю сеть



После обработки межсетевой информации, всегда обновляем справочники и ключи на узлах (то есть создаем и отправляем на сетевые узлы)

На рабочем месте администратора СА обрабатываем входящую межсетевую информацию



Создаем и отправляем справочники и ключи на сетевые узлы

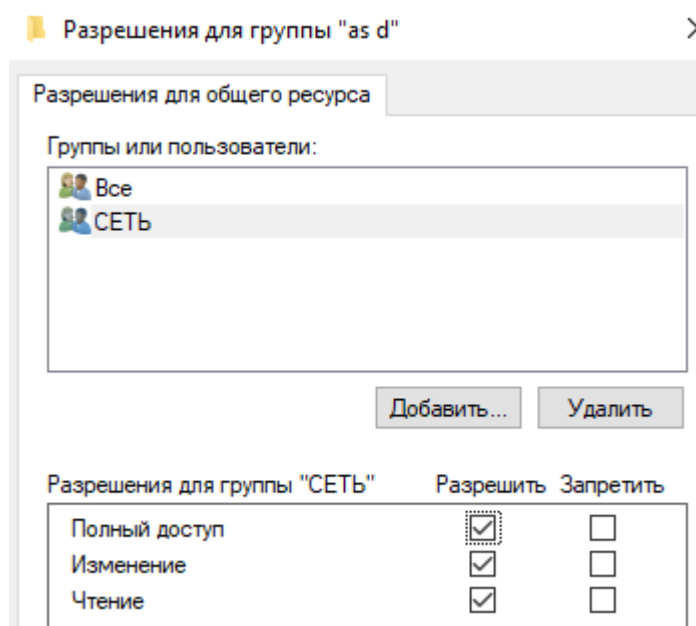
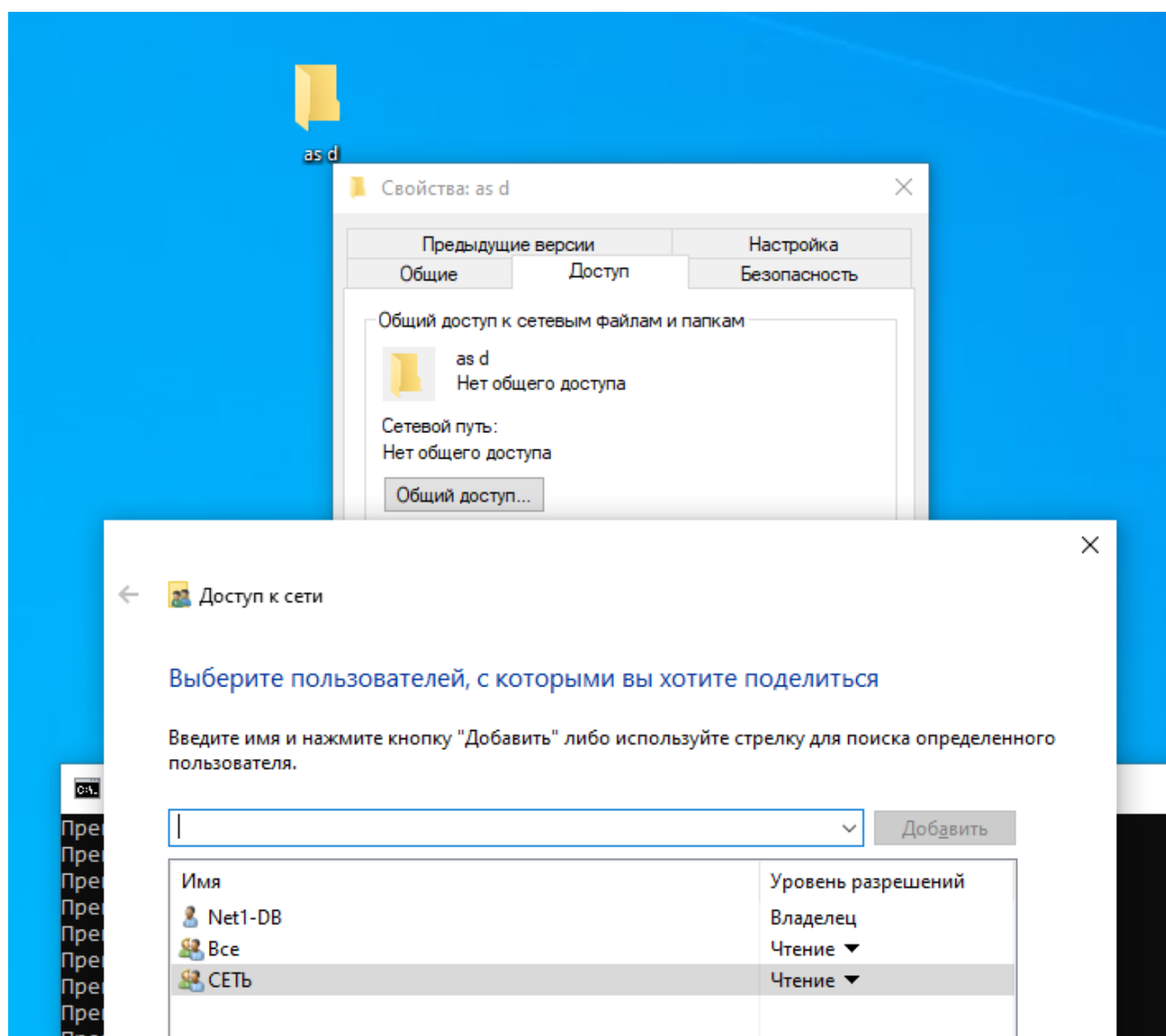
После обновления всех справочников и межсетевой информации у обеих машин проходит пинг

```
Ответ от 172.22.10.3: число байт=32 время<1мс TTL=126
Ответ от 172.22.10.3: число байт=32 время=4мс TTL=126
Ответ от 172.22.10.3: число байт=32 время<1мс TTL=126
Ответ от 172.22.10.3: число байт=32 время<1мс TTL=126
Ответ от 172.22.10.3: число байт=32 время<1мс TTL=126
Ответ от 172.22.10.3: число байт=32 время<1мс TTL=126
Ответ от 172.22.10.3: число байт=32 время<1мс TTL=126
Ответ от 172.22.10.3: число байт=32 время<1мс TTL=126
Ответ от 172.22.10.3: число байт=32 время<1мс TTL=126
Ответ от 172.22.10.3: число байт=32 время=1мс TTL=126
Ответ от 172.22.10.3: число байт=32 время<1мс TTL=126
Ответ от 172.22.10.3: число байт=32 время<1мс TTL=126
```

Проверить работает ли туннелирование можно на веб-ресурсе координаторов, например, на координаторе СА

The screenshot shows the 'ViPNet Coordinator VA' web interface. The top navigation bar is green with the title 'ViPNet Coordinator VA', a user profile icon labeled 'Режим пользователя', a notification bell with '0', and a help icon. The left sidebar is dark blue with a menu containing: 'Статистика и журналы', 'Защищенная сеть (VPN)' (expanded to show 'ViPNet узлы' and 'L2OverIP'), 'Туннелирование' (selected), 'Межсетевой экран', 'Прикладные сервисы', 'Сетевые интерфейсы', 'Маршрутизация', and 'Системные настройки'. The main content area is white and titled 'Туннелирование'. It displays 'Количество туннелируемых узлов' with a table: 'Указано в лицензии: 3', 'Активных сейчас: 1', and 'Пиковое значение: 1 (19 Дек 2022, 19:34)'. Below this is a section for 'IP-адреса для туннелирования' with an 'Обновить' button and a list of IP addresses, currently showing '192.168.120.2'.

Для проверки smb протокола на рабочем месте открытого узла 1-й сети создаем общую папку



На рабочем месте незащищенного узла 3-й сети в проводнике прописываем адрес незащищенного узла 1-й сети и убеждаемся, что подключение по протоколу smb работает

