

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра защиты информации и систем связи

УТВЕРЖДАЮ

Проректор по учебной работе

_____ О.Г. Локтионова

« ____ » _____ 2014 г.

НАСТРОЙКА МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

Методические указания по выполнению лабораторной работы по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Программно-аппаратная защита информации», «Методы и средства защиты информации в системах электронного документооборота» для студентов специальностей 090104.65, 090303.65, 090900.62, 090900.68.

Курск 2014

УДК 004

Составители: И.В. Калуцкий, С.В. Пономарев

Рецензент

Кандидат технических наук, доцент кафедры
защиты информации и систем связи *А.Г. Сневаков*

Настройка межсетевого взаимодействия: Методические указания по выполнению лабораторной работы по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Программно-аппаратная защита информации», «Методы и средства защиты информации в системах электронного документооборота» / Юго-Зап. гос. ун-т; сост.: И.В. Калуцкий, С.В. Пономарев. Курск, 2014. 20 с.: ил. 15., Библиогр.: с. 20

Содержит сведения по вопросам настройки взаимодействия между сетями ViPNet. Так же содержит подробное описание и порядок создания файлов экспорта, ключевой информации и правила создания межсетевых ключей.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Комплексная защита объектов информатизации», «Информационная безопасность», «Информационная безопасность автоматизированных систем».

Предназначены для студентов специальностей 090104.65, 090303.65, 090900.62, 090900.68 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.

Усл. печ. л. 1,16. Уч. –изд. л. 1,05. Тираж 30 экз. Заказ . Бесплатно.

Юго-Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. Введение	4
2. Цель работы	5
3. Порядок выполнения работы.....	5
4. Содержание отчета.....	5
5. Теоретическая часть.....	6
5.1. Общие сведения о сетевом взаимодействии.....	6
5.2. Межсетевые мастер-ключи.....	7
5.3. Логика выбора меж сетевого мастер-ключа.....	8
6. Выполнение работы	9
6.1. Подготовка и отправка файла экспорта	9
6.2. Создание меж сетевого мастер-ключа	11
6.3. Импорт файла экспорта.....	13
6.4. Создание и рассылка ключевых наборов.....	16
6.5. Прекращение сетевого взаимодействия.....	17
7. Варианты заданий	18
8. Контрольные вопросы.....	19
9. Библиографический список.....	20

ВВЕДЕНИЕ

В деятельности любой организации при увеличении штата компьютеров и территориальном расширении возникает необходимость взаимодействия между уже созданными сетями и новыми – межсетевое взаимодействие, что может нести определённые трудности в настройке.

Межсетевые взаимодействия (*internetworks*) являются коммуникационными структурами, работа которых заключается в объединении локальных и глобальных сетей. Их основная задача состоит в эффективном перемещении информации куда угодно быстро согласно запросу и в полной целостности. Поэтому наличие навыков, позволяющих объединять сети, необходимы.

Так же, как и в обычных сетях, настройка меж сетевого взаимодействия между виртуальными сетями является первостепенной, так как позволяет абонентам двух сетей обмениваться информацией между собой. Однако настройка взаимодействия в виртуальных сетях – процесс трудоемкий. Ведь каналы VPN шифруется для повышения безопасности с помощью меж сетевого ключа и для объединения двух сетей нужно создать новый ключ, чтобы сети смогли взаимодействовать друг с другом. Так же, необходимо удостовериться в подлинности сертификата администратора другой сети, иначе пользователи этих не смогут взаимодействовать между собой.

В данной лабораторной работе будут приведены примеры и способы настройки меж сетевого взаимодействия между сетями ViPNet.

ЦЕЛЬ РАБОТЫ

Цель лабораторной работы – научиться налаживать сетевое взаимодействие между сетями.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание
2. Изучить теоретическую часть
3. Описать со скриншотами предметную область
4. Написать вывод

СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист
2. Задание в соответствии с вариантом
3. Описание предметной области со скриншотами
4. Вывод

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Общие сведения о сетевом взаимодействии

Между двумя различными сетями ViPNet может быть организовано межсетевое взаимодействие. В этих целях в программе ЦУС предусмотрены специальные меры по формированию экспортных данных для ЦУС других сетей и импорта данных от других ЦУС.

Обмен информацией между пользователями двух различных сетей производится через один из СМ каждой сети, называемых шлюзовыми.

При формировании экспорта в программе ЦУС каждой сети указывается, какие коллективы, на каких АП должны взаимодействовать с пользователями другой сети. Указывается, какой из СМ данной сети является шлюзовым для другой сети. Эти данные оформляются в виде экспорта для другой сети. Одновременно в данные экспорта автоматически включаются все пользователи, зарегистрированные в экспортированных коллективах на выбранных АП.

Данные экспорта другой сети импортируются в базу данных ЦУС. В результате в списке коллективов данного ЦУС появляются коллективы из другой сети, зарегистрированные на АП внешней сети. В списке СМ появляется СМ другой сети. Установив логический канал связи между импортированным СМ и своим СМ, переданным в качестве шлюзового в другую сеть, и установив связи между импортированными коллективами и коллективами своей сети, переданными в другую сеть, в каждом из ЦУС формируются абонентские справочники и маршрутные таблицы для своих АП и СМ, в которых видны пользователи другой сети. Если сторона, установившая связи своих коллективов с коллективами другой сети опять отправит экспорт в другую сеть, то эти связи также автоматически импортируются ЦУС другой сети.

После первоначального обмена данными экспорта и импорта дальнейшее обновление этих данных в обоих ЦУС производится автоматически по защищенным каналам связи при помощи транспортного модуля ViPNet MFTP.

Межсетевые мастер-ключи

Для обеспечения независимого криптографического межсетевого взаимодействия между криптографическими администрациями организуется обмен специальными межсетевыми мастер-ключами. Между каждой парой сетей могут быть как свои мастер-ключи, так и использоваться общие межсетевые мастер-ключи для связи со всеми сетями. Внутренний обмен осуществляется на основе своих мастер-ключей, независимых от межсетевых.

Межсетевые мастер-ключи могут быть трех видов:

- **Индивидуальный симметричный межсетевой мастер-ключ** – ключ используется для создания классических ключей между объектами двух сетей (своей и конкретной чужой). **Следует отметить**, что данный ключ для каждой пары сетей должен быть один и тот же, следовательно, создаваться он должен только в одной сети, а в другую он должен быть каким-то образом передан, естественно, с исключением возможности доступа к нему посторонних лиц.
- **Универсальный симметричный межсетевой мастер-ключ** – ключ используется для создания классических ключей между объектами разных сетей, если нет индивидуального. **Следует отметить**, что данный ключ во всех сетях должен быть один и тот же, следовательно, создаваться он должен только в одной сети, а в другие он должен быть каким-то образом передан, естественно, с исключением возможности доступа к нему посторонних лиц.
- **Асимметричный межсетевой мастер-ключ** – такой ключ используется при организации связи между двумя сетями как альтернативный классическому межсетевому мастер-ключу. Для каждой сети он свой. Секретный асимметричный межсетевой мастер-ключ хранится в УКЦ своей сети, а соответствующий открытый асимметричный межсетевой мастер-ключ делается общедоступным и может быть использован в УКЦ любой доверенной сети для организации связи между двумя сетями. **Следует отметить**, чтобы асимметричный ключ использовался при создании ключевой информации, необходимо наличие секретного асимметричного ключа своей сети и открытого асимметричного ключа доверенной сети. На их основе формируется общий ключ, имеющий ту же

структуру, и используемый точно так же, как и симметричный межсетевой мастер-ключ.

Для связи двух сетей (или при плановой смене межсетевого мастер-ключа) необходимо создать какой-либо один мастер-ключ и осуществить операции экспорта и/или импорта мастер-ключа для обмена межсетевыми мастер-ключами по симметричной или асимметричной схеме, а также ввести этот ключ в действие.

Логика выбора межсетевого мастер-ключа

Если в Вашем УКЦ создано (или импортировано) и введено в действие несколько межсетевых мастер-ключей разного вида, то выбор мастер-ключа при формировании ключа между объектом данной сети (например, сеть с номером 1111 {0457 hex}) и объектом другой сети (например, сеть с номером 2222 {08AE hex}) происходит по логике, описанной ниже. Объектами могут являться коллективы или СУ.

Сначала программа ищет действующий индивидуальный мастер-ключ для данной сети. Если ключ найден, то он и будет использоваться при формировании ключей связи сетевых объектов.

При отсутствии индивидуального мастер-ключа программа ищет действующий секретный асимметричный межсетевой мастер-ключ сети 1111 и открытый асимметричный межсетевой мастер-ключ сети 2222. Если они есть, то на их основе создается симметричный ключ, который и используется при формировании ключей связи сетевых объектов.

Если асимметричного межсетевого мастер-ключа тоже нет, то программа ищет действующий универсальный ключ, который и используется при формировании ключей связи сетевых объектов.

Если и универсального ключа нет, то выдается сообщение об ошибке.

ПРАКТИЧЕСКАЯ ЧАСТЬ

Подготовка и отправка файла экспорта

После настройки сети VIPNet необходимо сделать так, чтобы они могли обмениваться информацией между собой, т.е. объединить их. Для этого, нам необходимо создать файлы в ЦУС1 с описанием нашей сети, ее структурой и т.д. и передать это всё в ЦУС2 с помощью защищенного носителя информации.

Открываем ЦУС1 и находим вкладку: Службы-Экспорт... и нажимаем Enter и оказываемся в меню экспорта:

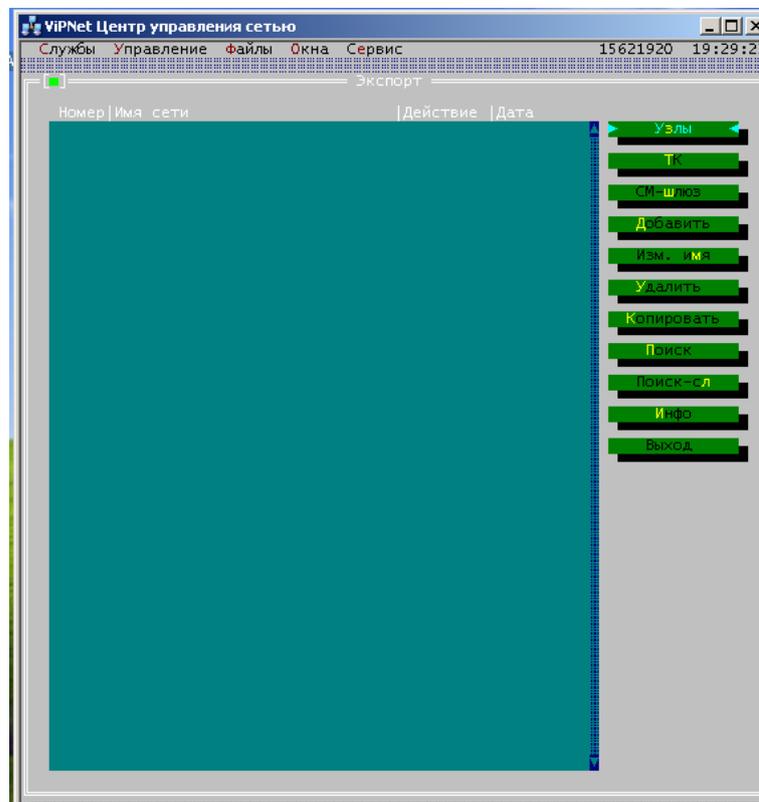


Рис.1 – Меню экспорта сети

Нажимаем на вкладку добавить и появляется окно с предложением назначить номер сети и ее имя.

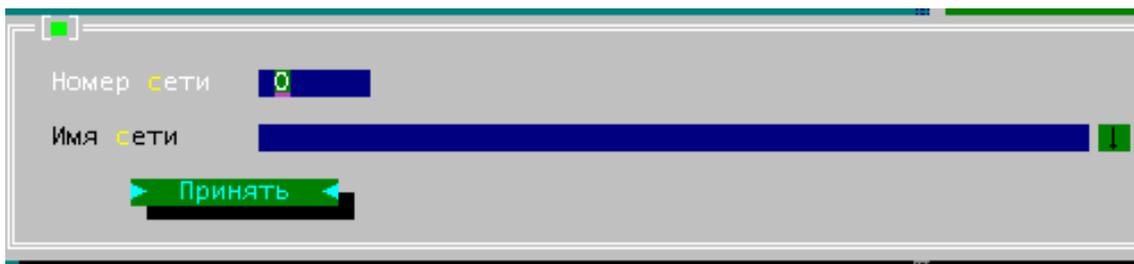


Рис.2 – Создание сети для экспорта

ВНИМАНИЕ!!!Номер сети необходимо указывать, согласно номеру ключа, установленного для ЦУС(т.е номер папки с файлом лицензии. Обязательно нужно указать номер сети ,для которой будут экспортироваться настройки.

После добавления сети, нам необходимо указать все ТК и узлы, которые имеются в данной сети. Можно это сделать или через вкладку Узлы или через вкладку ТК. Однако необходимо добавить ВСЕ узлы и коллективы, которые необходимо связать с другой сетью. В противном случае - другая сеть их не увидит и как следствие взаимодействие будет нарушено.

Настройка через вкладку Узлы:

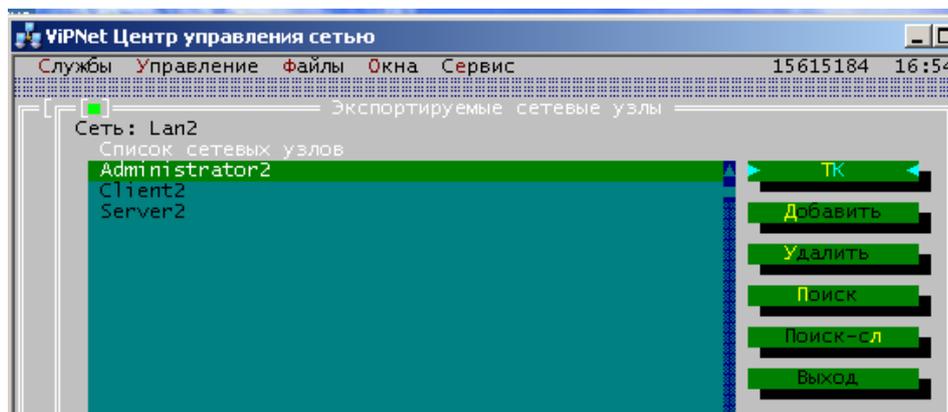


Рис.3 – Добавление сетевых узлов для экспорта

Добавить необходимо все АП с помощью вкладки добавить. После их добавление, необходимо указать ТК, для этого щелкаем по вкладке ТК и выбираем имеющийся ТК.

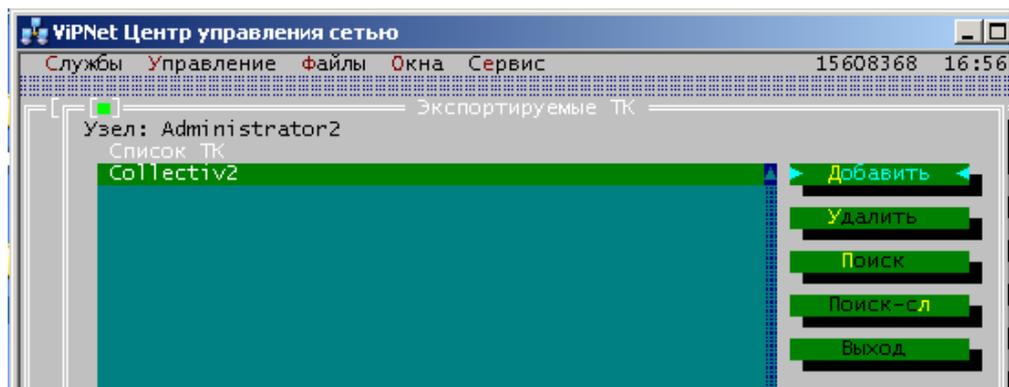


Рис.4 – Добавление коллективов для экспорта.

Настройка через вкладку ТК осуществляется в обратном порядке: сначала выбирается ТК, а потом добавляются узлы.

После настройки данной сети необходимо указать СМ-шлюз, через который данная сеть будет осуществлять обмен с другой сетью. Для этого щелкаем по вкладке СМ-шлюз и выбираем его из списка.

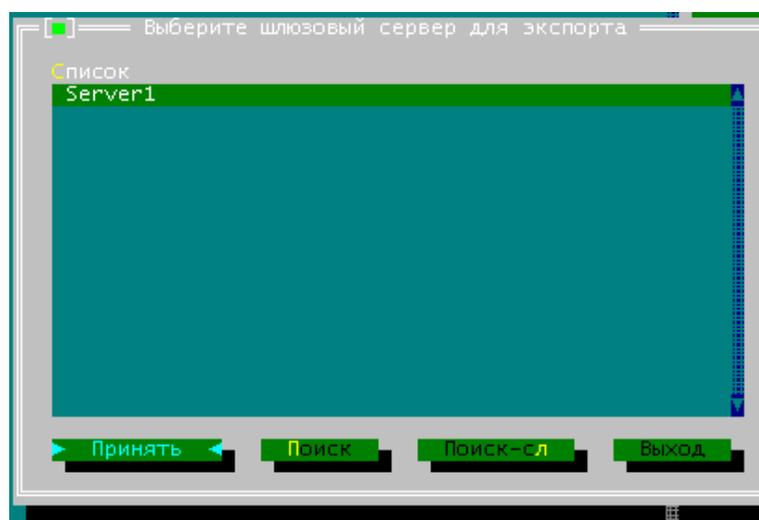


Рис.5 – Выбор СМ-шлюза

Далее, необходимо скопировать данные на съемный защищенный носитель информации и передать в ЦУС2. Для этого, необходимо нажать на вкладку Копировать и подтвердить копирование в директорию по умолчанию (C:\Program Files\InfoTeCS\ViPNetAdministrator\NCC\NEW\EXPORT). Обязательным условием успешного формирования файла для экспорта явля-

ется наличие в сети машины с ПО VIPNet Coordinator. Так же необходимо заново сформировать все справочники для сети. После этого, в данной папке создается папка с именем сети, которую необходимо скопировать на защищенный съемный носитель и перенести в ЦУС2.



Рис.6 – Файл с экспортом для другой сети

Создание межсетевого мастер-ключа

Теперь необходимо сгенерировать межсетевой мастер-ключ, необходимый для взаимодействия сетей. Для этого в УКЦ выбираем папку Ключевой центр / Доверенные сети ViPNet / Мастер-ключи / Текущие.

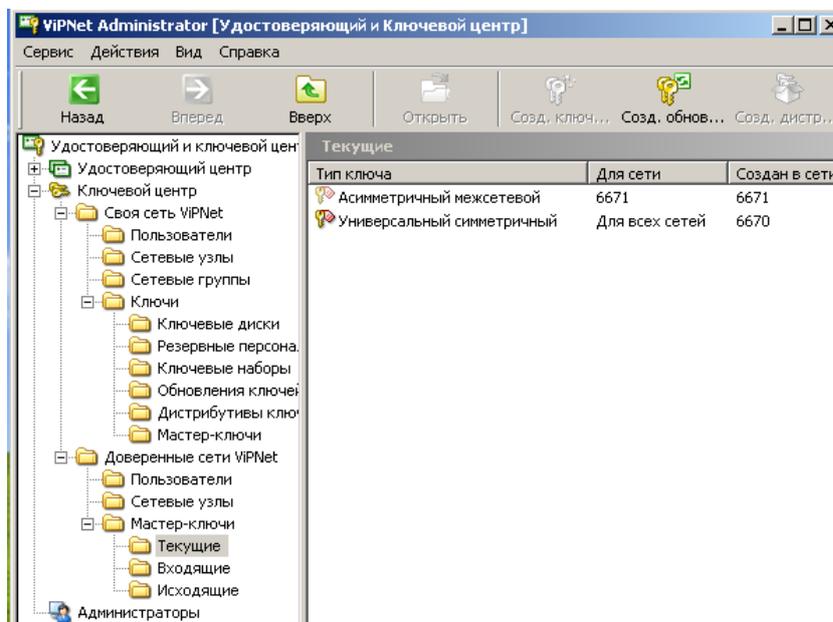


Рис.7 – Меню межсетевых мастер-ключей

Далее нужно создать общий межсетевой ключ. Для этого нужно щелкнуть правой кнопкой мыши и выбрать пункт создать и выбрать универсальный.

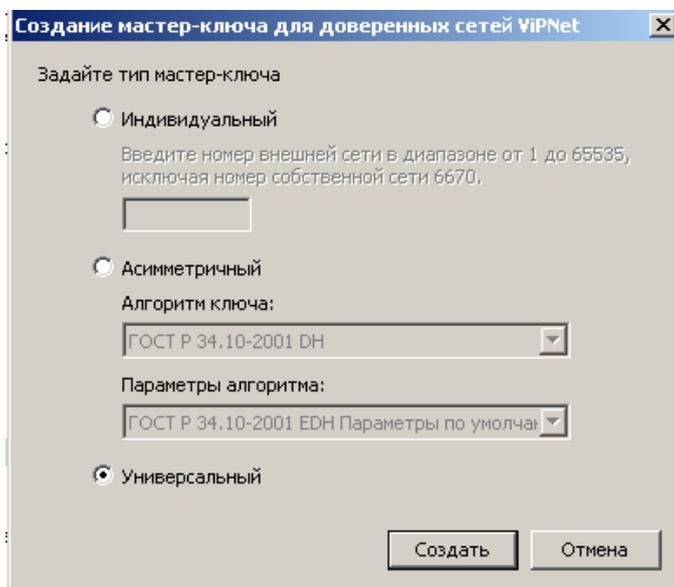


Рис. 8 – Создание межсетевого мастер-ключа

После этого необходимо установить пароль, затем щелкнуть правой кнопкой мыши и выбрать пункт Экспорт.

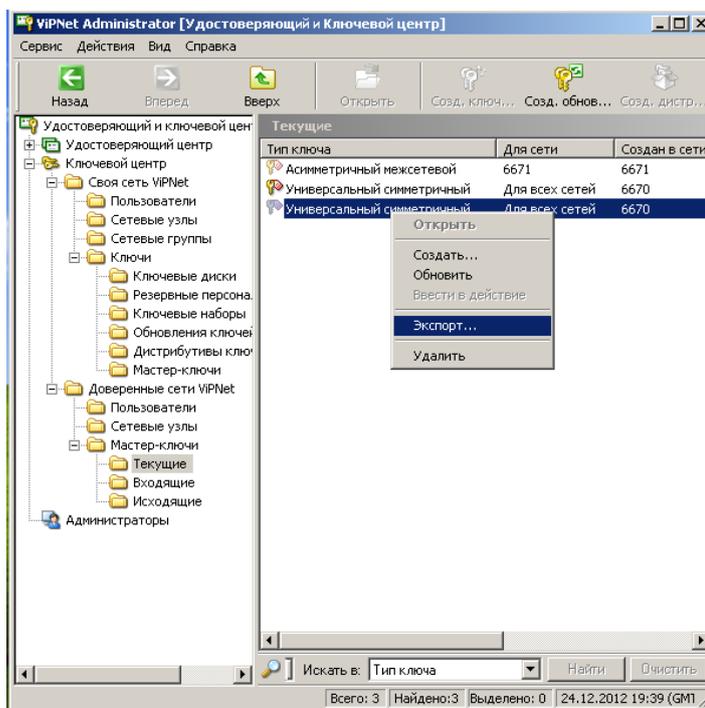


Рис. 9 – Экспорт межсетевого ключа

Ключ сохранится в папке КС\EXPORT.Его нужно скопировать вместе с информацией для экспорта и передать в другую сеть.

Импорт данных

Теперь приступаем к объединению двух сетей. Для этого, нам необходимо скопировать содержимое папки (ИМЕНННО СОДЕРЖИМОЕ ПАПКИ,А НЕ САМУ ПАПКУ С СОДЕРЖИМЫМ!) в папку C:\Program Files\InfoTeCS\ViPNet Administrator\NCC\IMPORT\NEW.

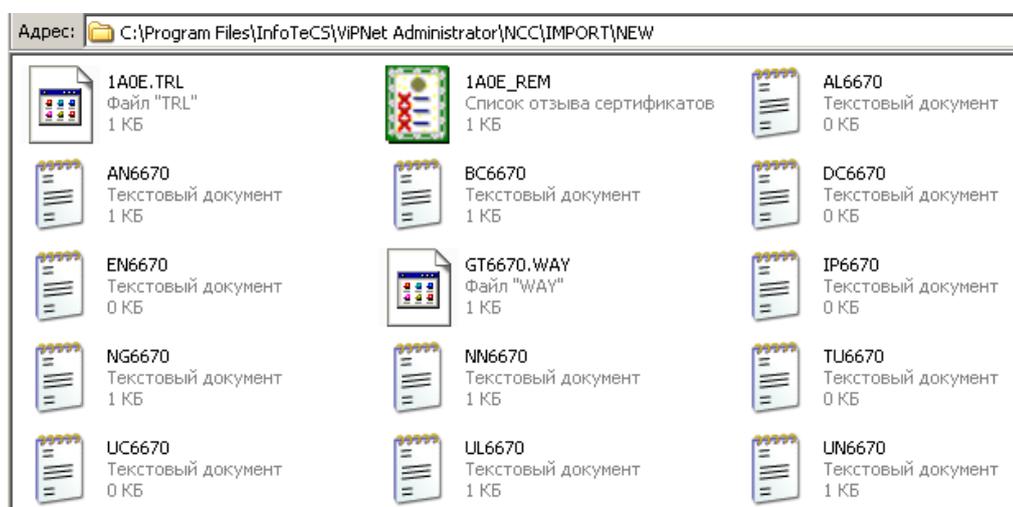


Рис.10 – Содержание файла экспорта

После этого, запускаем ЦУС2 и ждем, когда появится сообщение об необработанном импорте.

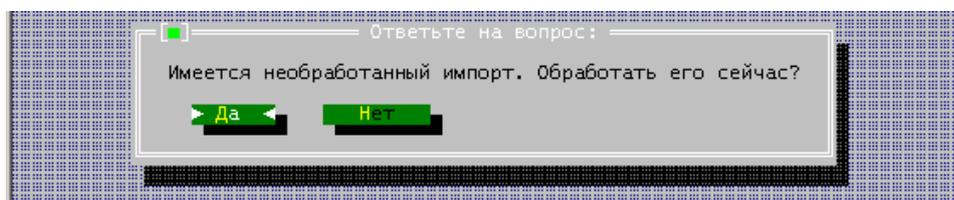


Рис.11 – Перенос экспорта в другую сеть

После появления данного сообщение выбираем да и оказываемся в меню необработанного импорта ,где нам необходимо выбрать вкладку Обработать всё и ждать окончания обработки.

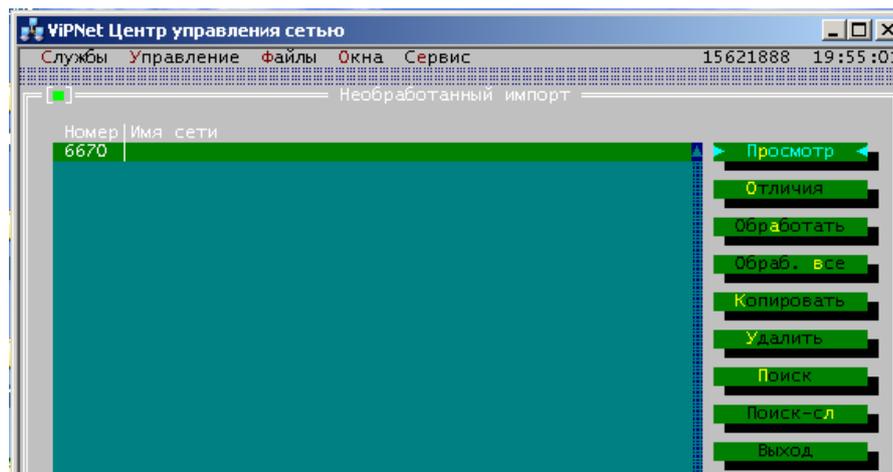


Рис.12 – Меню импорта другой сети

После этого появится сообщение о необходимости перенастроить сеть. Так же, нам необходимо связать типы коллективов. Начнем с настройки сети. Выбираем пункт Службы/Адресная администрация-Структура сети VIPNet. Далее выбираем вкладку Межсетевые каналы, где нам необходимо указать СМ-шлюз для нашей сети, для чего достаточно нажать клавишу Enter и выбрать предложенный сервер.

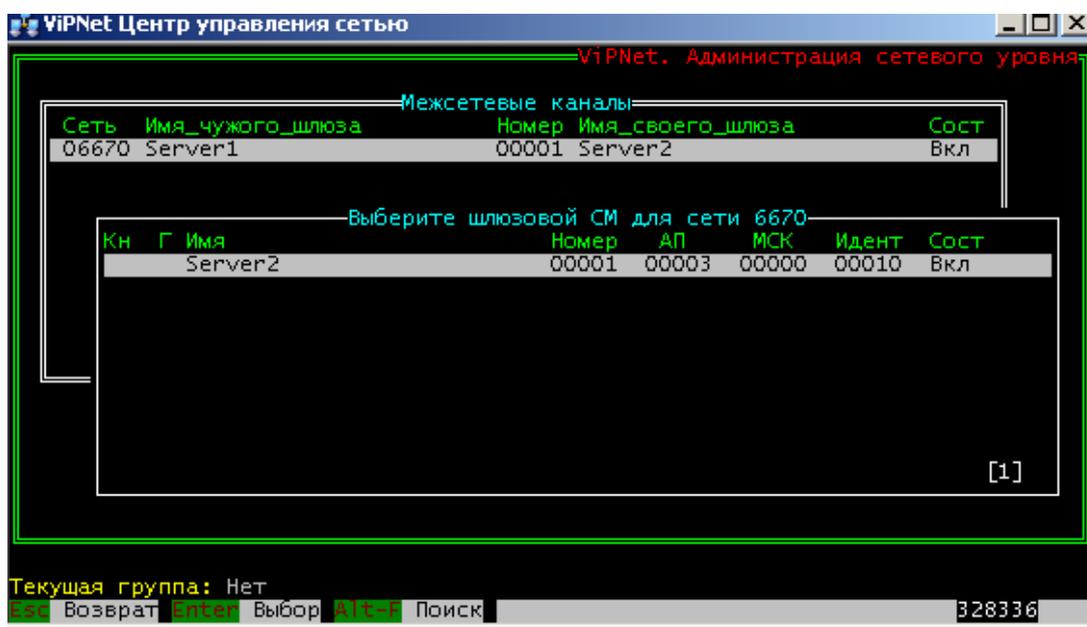


Рис.13 – Выбор СМ-шлюза для своей сети

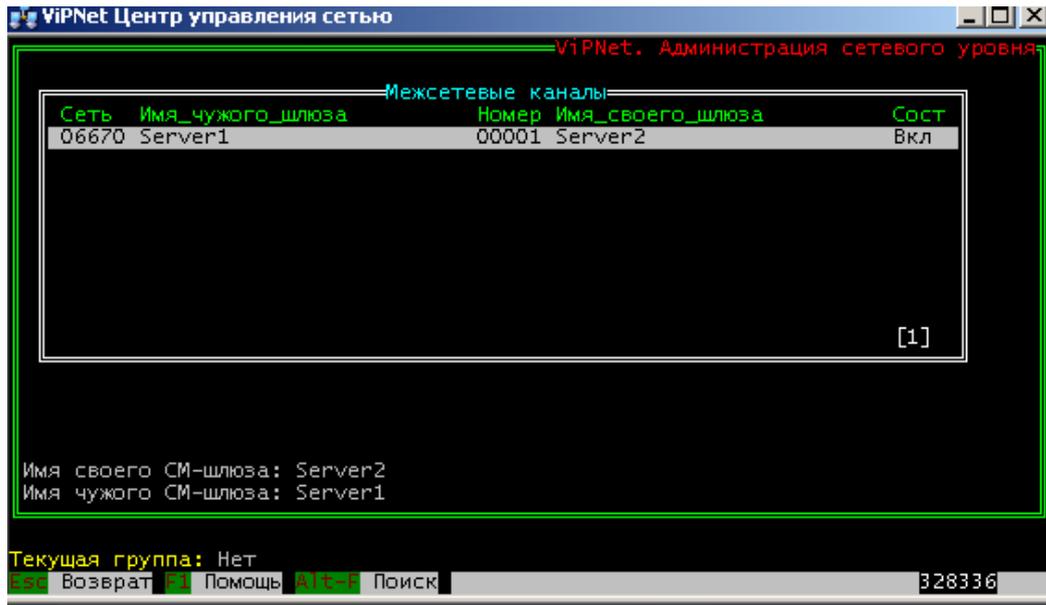


Рис.14 – Меню межсетевых каналов

После этого, необходимо вернуться в меню и выбрать пункт Выдать таблицы маршрутизации. Настройка окончена, теперь переходим к регистрации типов коллективов. Выбираем пункт Службы/Прикладная администрация-регистрация типов коллективов. Там мы увидим, что теперь у нас появилось 2 коллектива, и нам необходимо их связать между собой. Для этого нажимаем на вкладку Связи/Добавить и выбираем предложенный коллектив из таблицы.

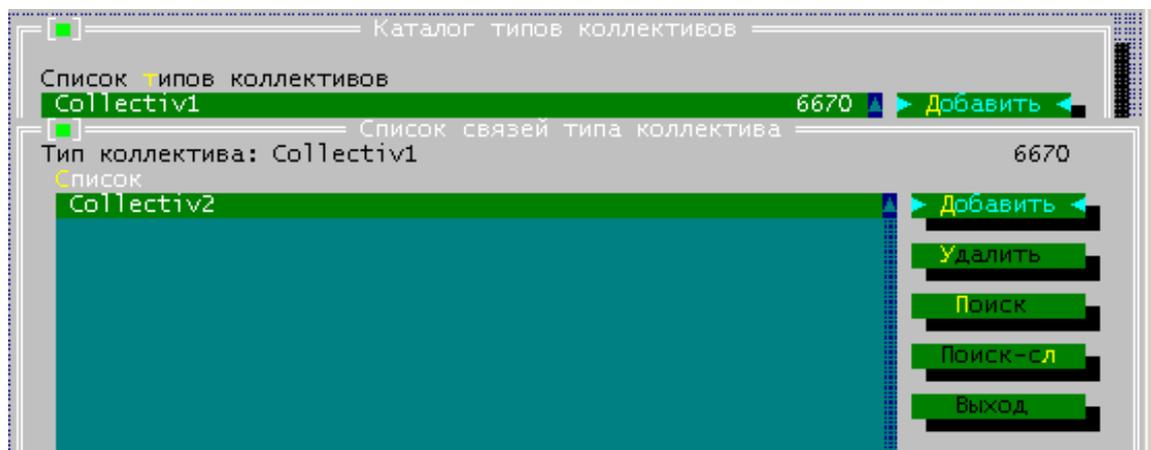


Рис.15 – Настройка связей между коллективами

После этого получаем два объединенных коллективов. Настройка окончена, но нам необходимо заново сформировать все справочники, в виду новой конфигурации сети, для этого выбираем вкладку Службы/Сформировать все справочники и ждём окончания.

Так же необходимо поместить межсетевой ключ в папку KC\IMPORT, затем выбрать межсетевые ключи-входящие щелкнуть правой кнопкой мыши и нажать импорт. Затем нужно применить данный ключ. Для этого так же щелкаем правой кнопкой мыши и выбираем пункт - ввести в действие.

Таким образом мы настроили ЦУС2 и теперь тоже самое нам необходимо сделать и для ЦУС1.

Создание ключевых наборов

После настройки ЦУСов необходимо зайти в УКЦ и принять сертификаты администраторов и обновить ключевую информацию. Для этого выбираем пункт меню Сервис / Автоматически создать / Ключевые наборы. Затем переходим Ключевой центр / Своя сеть ViPNet / Ключи / Ключевые наборы, щелкаем правой кнопкой мыши и выбираем пункт Перенести в ЦУС. Затем в ЦУСе выбираем Управление/отправка и отсылаем данные. После этого межсетевое взаимодействие настроено.

Прекращение сетевого взаимодействия

Для прекращения сетевого взаимодействия между сетями необходимо зайти в Службы/Экспорт.. и удалить файл экспорта. После этого межсетевое взаимодействие прекратиться. Затем необходимо зайти в Службы/Адресная администрация-структура сети ViPNet и сформировать новые таблицы маршрутизации.

ВАРИАНТЫ ЗАДАНИЙ

1. Сделать так, чтобы после объединения 2-ух сетей был виден только один пользователь другой сети.
2. Скомпрометировать сетевой узел и выполнить действия при компрометации сетевого узла.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Для чего предназначено межсетевое взаимодействие?
2. Межсетевые мастер ключи. Дать определения межсетевым мастер ключам.
3. Виды межсетевых мастер ключей.
4. Какими принципами следует руководствоваться при выборе меж сетевого мастер ключа?
5. Для чего необходимо прекращение взаимодействия между сетями?
6. Перечислите по порядку основные действия при настройке взаимодействия между сетями?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ViPNet Administrator [Центр Управления Сетью] – Руководство администратора. [Электронный ресурс]/ - <http://www.infotecs.ru>.
2. ViPNet Administrator [Удостоверяющий и Ключевой Центр] – Руководство Администратора. [Электронный ресурс]/ - <http://www.infotecs.ru>.