Задание № 3.2. Первоначальная настройка межсетевого взаимодействия

Формулировка задания

В настоящем задании необходимо:

3.2.1. Развернуть защищенную сеть Федеральной службы.

3.2.2. Настроить межсетевое взаимодействие с использованием индивидуального симметричного межсетевого мастер-ключа.

Предварительные настройки

Для подготовки к заданию № 3.2 выполните следующие действия:

- Проверьте, что на виртуальной машине VM_1 установлено программное обеспечение *ViPNet Administrator, ViPNet Policy Manager и ViPNet Client*.
- Проверьте, что на виртуальной машине VM_2 установлено программное обеспечение ViPNet Coordinator с установленными ключами пользователя *Координатор Центр офис*.
- На виртуальных машинах VM_3 и VM_4 удалите программное обеспечение ViPNet (если было установлено).

3.2.1. Развертывание защищенной сети Федеральной службы

Формулировка задания

Развернуть защищенную сеть Федеральной службы на базе виртуальных машин VM_3 и VM_4 (*используя при этом второй комплект регистрационных файлов, которые были выданы на первом занятии*). Создать структуру сети в соответствии с предложенными таблицами 5,6,7. Сформировать справочники и ключи и на основе созданных дистрибутивов ключей развернуть на виртуальных машинах *Координатор Федеральной службы* и *Администратор ViPNet Федеральной службы*

Пояснение к заданию

На виртуальной машине VM_4 необходимо установить программное обеспечение *ViPNet Administrator* и *ViPNet Client*, а на виртуальной машине VM_3 – *ViPNet Coordinator*.

Защищенная сеть Федеральной службы состоит из 3 узлов – 1 координатор и 2 клиента (Таблица 1).

Таблица 1 – Состав защищенной сети Федеральной службы

№	Тип СУ	Название СУ	Расположение СУ	Комментарии

1	Координатор	*Координатор Федеральной службы*	Федеральная служба	Для развертывания ViPNet Coordinator
2	Клиент	*Администратор ViPNet Федеральной службы*		Для развертывания ViPNet Administrator
3		*Специалист по отчетности*		Рабочее место специалиста по приему отчетности

Матрица связей узлов защищенной сети Федеральной службы представлена в таблице 6.

Таблица 2 – Матрица связей узлов в сети Федеральной службы

Матрица связей сетевых узлов	*Координатор Федеральной службы*	*Администратор ViPNet Федеральной службы*	*Специалист по отчетности*
Координатор Федеральной службы		+	+
Администратор ViPNet Федеральной службы	+		+
Специалист по отчетности	+	+	

На каждом узле защищенной сети присутствует по одному пользователю (Таблица 3).

Таблица 3 – Определение пользователей

№	Название СУ	Имя пользователя на СУ
1	*Координатор Федеральной службы*	*Координатор Федеральной службы*
2	*Администратор ViPNet Федеральной службы*	*Админ ФедСлужбы Новиков*
3	*Специалист по отчетности*	*Спец отчетности Морозов*

Связи между пользователями не установлены.

Не забудьте отключить у пользователей создание электронной подписи.

Порядок выполнения задания

Развертывание программного обеспечения *ViPNet Центр управления сетью, ViPNet Удостоверяющий и ключевой центр, ViPNet Client и ViPNet Coordinator* осуществляется в том же порядке, что и в предыдущих практических занятиях.

При настройке программ *ViPNet* задайте пароли:

- *11111111* – для входа в программы ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр (пароль администратора сети ViPNet);
- *11111111* – для пользователей защищенной сети.

Имя администратора ViPNet Федеральной службы – *Константин*.

3.2.2. Настройка межсетевого взаимодействия с использованием индивидуального симметричного межсетевого мастер-ключа

Формулировка задания

Настроить взаимодействие защищенной сети *Компании* и защищенной сети *Федеральной службы* таким образом, чтобы узлы *Координатор Центр офис* и *Координатор Федеральной службы* могли взаимодействовать друг с другом по шифрованному каналу.

Проверка взаимодействия осуществляется в окне программы *ViPNet Coordinator Монитор> Защищенная сеть> в контекстном меню узла выбрать Проверить соединение*. На узле *Координатор Федеральной службы* должен быть доступен узел *Координатор Центр офис* и наоборот.

Пояснение к заданию

Если требуется организовать канал для защищенного обмена информацией между двумя разными сетями ViPNet, то между этими сетями следует установить межсетевое взаимодействие. Сети ViPNet, с которыми в вашей сети установлено межсетевое взаимодействие, называются доверенными сетями.

Для каждой доверенной сети в Удостоверяющем и ключевом центре создается межсетевой мастер-ключ, на основе которого формируются ключи для защищенного обмена информацией с данной доверенной сетью.

Также для каждой доверенной сети назначается шлюзовой координатор. Шлюзовой координатор своей сети связан с аналогичным координатором доверенной сети, и через эти координаторы направляются все транспортные конверты, передаваемые между двумя сетями.

Чтобы обеспечить возможность защищенного соединения между сетевыми узлами вашей и доверенной сетей, обмена письмами в программе ViPNet Деловая почта, файлами и так далее, следует создать связи между объектами вашей сети ViPNet и объектами доверенной сети.

Организация межсетевого взаимодействия между сетями ViPNet состоит из следующих этапов:

1. Администратор первой сети ViPNet, инициирующий межсетевое взаимодействие, создает в Центре управления сетью файл межсетевой информации, а в Удостоверяющем и ключевом центре – межсетевой мастер-ключ. Затем по доверенным каналам связи он передает файл межсетевой информации и межсетевой мастер-ключ администратору второй сети ViPNet.
2. Администратор второй сети ViPNet принимает межсетевую информацию, затем создает файл с ответной межсетевой информацией и передает его администратору первой сети.
3. Администратор второй сети импортирует переданный ему межсетевой мастер-ключ.
4. Администратор первой сети завершает организацию межсетевого взаимодействия приемом ответной межсетевой информации.
5. Администратор каждой сети создает новые справочники и ключи и отправляет их на узлы своей сети.

После этого узлы доверенных сетей, участвующие в межсетевом взаимодействии, смогут обмениваться информацией друг с другом.

	**Внимание!** Необходимо учитывать, что при организации межсетевого взаимодействия в реальной сети, пользователя Главный администратор не рекомендуется включать в межсетевую информацию и связывать его с другими пользователями доверенной сети из соображений безопасности. Также следует обратить внимание, что в Фильтрах защищенной сети по умолчанию разрешено подключение по RDP (на клиентах и координаторах), поэтому при организации межсетевого взаимодействия, необходимо будет запретить подключение по RDP из доверенной сети, а также проверить Настройки удаленного доступа в ОС.

Порядок выполнения задания

Инициация межсетевого взаимодействия

Чтобы инициировать межсетевое взаимодействие с сетью ViPNet *Федеральной службы*, выполните следующие действия на рабочем месте *Главный администратор* сети *Компании*:

1. В окне программы *ViPNet Центр управления сетью* в меню *Доверенные сети* выберите пункт *Установить взаимодействие*. Будет запущен мастер *Установка межсетевого взаимодействия*.

2. На первой странице мастера выберите вариант *Я инициатор межсетевого взаимодействия* и нажмите кнопку *Далее*.
3. На странице *Задайте информацию о другой сети ViPNet и координатор для связи с ней* **(необходимо правильно указать номер доверенной сети, с которой вы устанавливаете межсетевое взаимодействие, в противном случае могут возникнуть проблемы)**, имя сети – *Федеральная служба*, которое будет отображаться в программе *ViPNet Центр управления сетью*, и выберите шлюзовой координатор своей сети – *Координатор Центр офис*. Затем нажмите кнопку *Далее (Рисунок 130)*.

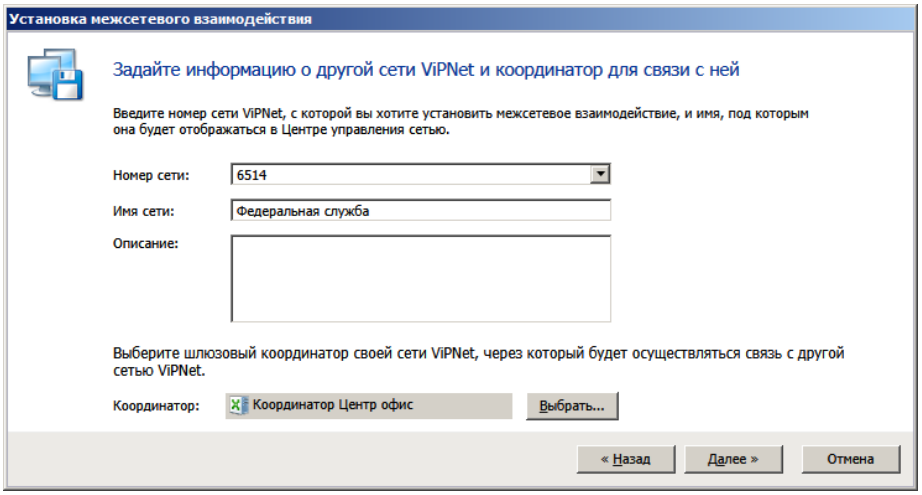

Рисунок 1 – Фрагмент окна *Установка межсетевого взаимодействия*

4. На странице *Укажите сетевые узлы своей сети ViPNet для связывания* выберите узлы сети, которые будут участвовать во взаимодействии с узлами сети *Федеральной службы – Главный администратор* и *Координатор Центр*.
5. Центр управления сетью и шлюзовой координатор своей сети должны обязательно присутствовать в списке узлов для взаимодействия, их невозможно удалить. Выбрав узлы, нажмите кнопку *Далее*.
6. На странице *Укажите пользователей своей сети ViPNet* для связывания выберите пользователя *Координатор Центр офис*.
7. Если для межсетевого взаимодействия выбран сетевой узел, но не выбран ни один пользователь этого узла, сведения об этом узле не будут включены в межсетевую информацию. Исключениями являются *Центр управления сетью и шлюзовой координатор*. Выбрав пользователей, нажмите кнопку *Далее*.
8. На открывшейся странице *Подготовка к сохранению межсетевой информации завершена* при необходимости укажите комментарий для администратора сети Федеральной службы и нажмите кнопку *Далее*.

9. На странице *Укажите файл для сохранения межсетевой информации* нажмите кнопку *Обзор* и укажите каталог для сохранения файла межсетевой информации – *Рабочий стол*. Затем нажмите кнопку *Далее*.
10. На странице *Сохранение межсетевой информации* после завершения записи файла нажмите кнопку *Далее*, на следующей странице нажмите кнопку *Готово*.

Чтобы создать индивидуальный симметричный межсетевой мастер-ключ, выполните следующие действия:

1. В окне программы *ViPNet Удостоверяющий и ключевой центр* на панели навигации выберите представление *Ключевой центр*.
2. Перейдите в раздел с номером доверенной сети, для связи с которой будет использоваться межсетевой мастер-ключ, и на панели инструментов нажмите кнопку *Создать*.
3. Появится окно с сообщением о необходимости согласования мастер-ключа с администратором доверенной сети. Нажмите в данном окне кнопку *Да*. В результате межсетевой мастер-ключ будет создан и отобразится в соответствующем разделе *(Рисунок 131)*.

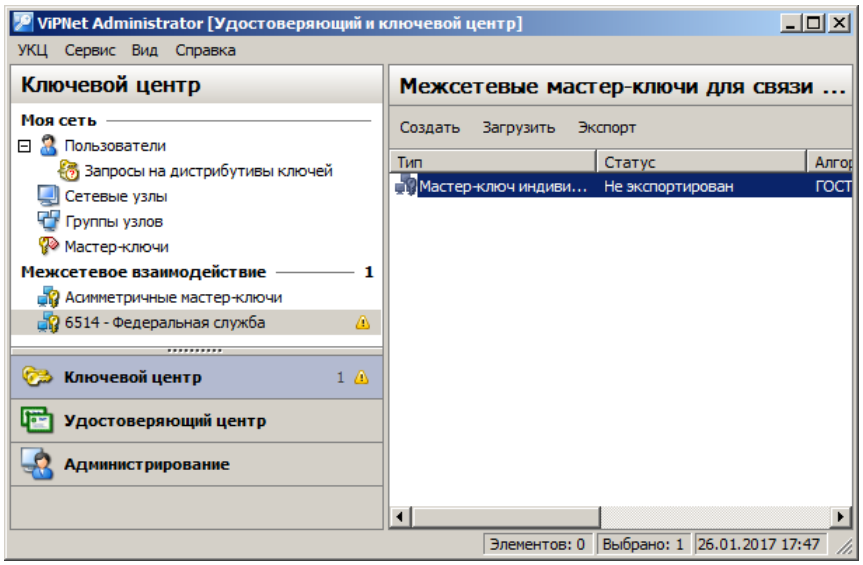

Рисунок 2 – Создание ИСММК

4. Щелкните по созданному межсетевому мастер-ключу правой кнопкой мыши и в контекстном меню выберите пункт *Экспорт*.
5. Появится окно ввода пароля. Укажите в нем пароль – *11111111* и нажмите кнопку *ОК*. На указанном пароле будет зашифрован экспортируемый ключ.
6. В появившемся окне укажите каталог, в который будет сохранен межсетевой мастер-ключ, – *Рабочий стол*, затем нажмите кнопку *ОК*.

7. Передайте доверенным способом файл межсетевой информации с расширением*.*lzh*, межсетевой мастер-ключ *«net ****.key»* и пароль, на котором зашифрован межсетевой мастер-ключ – *11111111*, администратору сети *Федеральной службы*.

Прием первичной межсетевой информации

Чтобы принять межсетевую информацию перейдите на рабочее место администратора сети *Федеральной службы* и выполните следующие действия:

1. В окне программы *ViPNet Центр управления сетью* в меню *Доверенные сети* выберите пункт *Установить взаимодействие*. Будет запущен мастер *Установка межсетевого взаимодействия*.
2. На первой странице мастера выберите вариант *Я принимаю файл с межсетевой информацией* и нажмите кнопку *Далее*.
3. На странице *Загрузка межсетевой информации из файла* укажите файл с межсетевой информацией, полученный от *Главного администратора* сети ViPNet *Компании*, который инициировал межсетевое взаимодействие. После указания файла в окне мастера появится предупреждение, что взаимодействие с сетью не установлено *(Рисунок 132)*.

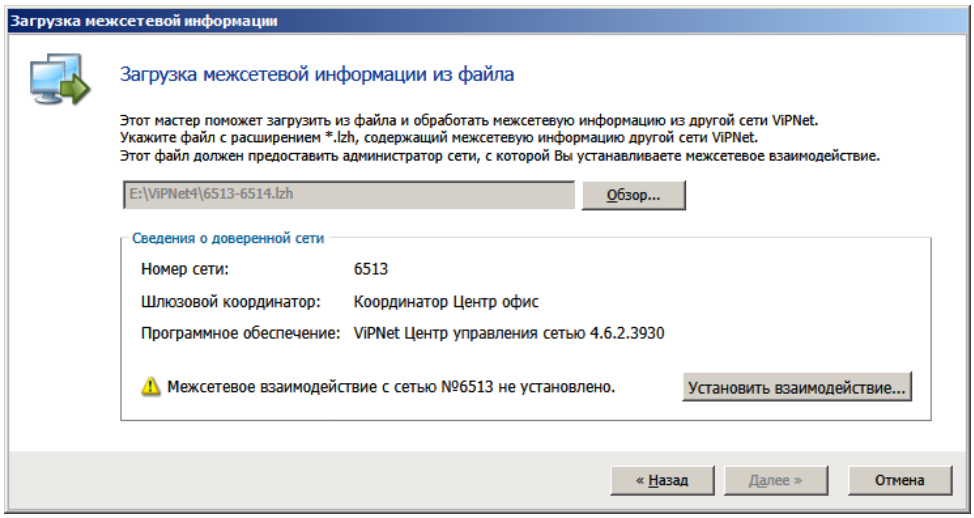

Рисунок 3 – Прием первичной межсетевой информации

1. Чтобы продолжить загрузку межсетевой информации, нажмите кнопку *Установить взаимодействие*.
2. На странице *Задайте информацию о другой сети ViPNet и координатор для связи с ней* выберите шлюзовой координатор – *Координатор Федеральной службы*, затем нажмите кнопку *Далее*.
3. На странице *Изменения в межсетевой информации* ознакомьтесь со списком узлов и пользователей, которые были выбраны для межсетевого взаимодействия *Главным администратором сети ViPNet Компании*, который инициировал межсетевое взаимодействие. Затем нажмите кнопку *Далее*.

4. Если файл межсетевой информации содержит ошибки, откроется страница *Проверка межсетевой информации* со списком обнаруженных конфликтных или неполных данных. При обнаружении конфликтных данных загрузка межсетевой информации будет невозможна. В этом случае обратитесь к администратору доверенной сети для устранения конфликтов.
5. Чтобы продолжить обработку межсетевой информации, нажмите кнопку *Далее*.
6. На странице *Загрузка межсетевой информации* после завершения обработки информации нажмите кнопку *Готово*.
7. В представлении *Доверенные сети* выберите *Сеть №**** (вместо звездочек будет номер сети, инициировавшей межсетевое взаимодействие)* и перейдите на вкладку *Пользователи*. В свойствах пользователя *Координатор Центр офис* на вкладке *Связи с пользователями* установите связь с *Координатор Федеральной службы (Рисунок 133)*.

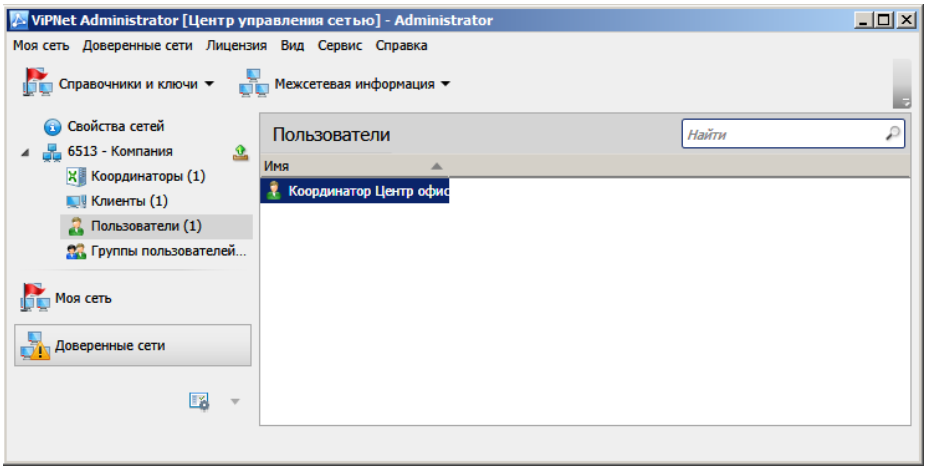

Рисунок 4 – Вкладка *Пользователи* доверенной сети

После приема первичной межсетевой информации в программе *ViPNet Удостоверяющий и ключевой центр* импортируйте переданный *Главным администратором Компании* межсетевой мастер-ключ. Для этого:

1. В окне программы на панели навигации выберите представление *Ключевой центр* и перейдите в раздел с номером доверенной сети, из которой поступил данный мастер-ключ.
2. На панели инструментов нажмите кнопку *Загрузить*.
3. При импорте индивидуального симметричного межсетевого мастер-ключа *«net ****.key»* появится окно ввода пароля. Введите пароль, на котором был зашифрован данный ключ – *11111111*. При правильном вводе пароля мастер-ключ будет импортирован.

Импортированный мастер-ключ будет сразу добавлен в список межсетевых мастер-ключей выбранного раздела.

После того, как ключ будет импортирован, в УКЦ необходимо зайти в раздел *Межсетевое взаимодействие* выбрать строку с ИСММК, щелкнуть по строке правой кнопкой мыши и выбрать пункт *Использовать*.

4. Подготовьте сертификаты администраторов и списки аннулированных сертификатов вашей сети для передачи в доверенную сеть (сеть Компании) в составе ответной межсетевой информации. Для этого в программе *ViPNet Удостоверяющий и ключевой центр* в меню *Сервис* выберите пункт *Экспорт межсетевой информации*.
5. В программе *ViPNet Центр управления сетью* в представлении *Доверенные сети* выберите раздел *Свойства сетей*.
6. На панели просмотра щелкните правой кнопкой мыши добавленную доверенную сеть и в контекстном меню выберите пункт *Создать межсетевую информацию (Рисунок 134)*.
7. В появившемся окне нажмите кнопку *Создать*.
8. После создания ответной межсетевой информации сохраните ее на жесткий диск. Для этого снова щелкните доверенную сеть правой кнопкой мыши и в контекстном меню выберите пункт *Сохранить межсетевую информацию в файл*, затем в окне *Сохранить как* укажите папку для сохранения файла межсетевой информации ****-****.lzh – *Рабочий стол*.

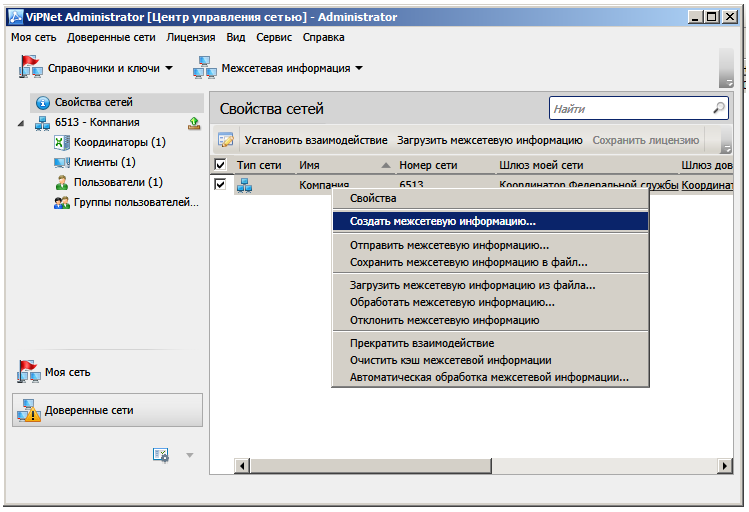

Рисунок 5 – Создание ответной межсетевой информации для доверенной сети

9. Создайте новые справочники и ключи для узлов сети *Федеральной службы*, участвующих в межсетевом взаимодействии – *Администратор ViPNet Федеральной службы и Координатор Федеральной службы*, и отправьте их на узлы.
10. Передайте созданный файл межсетевой информации ****-****.lzh администратору сети *Компании*.

Завершение организации межсетевого взаимодействия

Чтобы принять ответную межсетевую информацию и завершить организацию взаимодействия, выполните следующие действия на рабочем месте *Главный администратор* (сеть Компании):

1. Получите у администратора доверенной сети ViPNet *Федеральной службы* файл, содержащий ответную межсетевую информацию ****-****.*lzh*.
2. В окне программы ViPNet Центр управления сетью в меню *Доверенные сети* выберите пункт *Загрузить межсетевую информацию из файла*.
3. В окне *Загрузка межсетевой информации* укажите файл межсетевой информации, полученной от администратора другой сети ViPNet, и следуйте мастеру, нажимая кнопку *Далее*, а на заключительном шаге – *Готово*.
4. Примите ответную межсетевую информацию с помощью мастера *Обработка межсетевой информации (Рисунок 135)*.

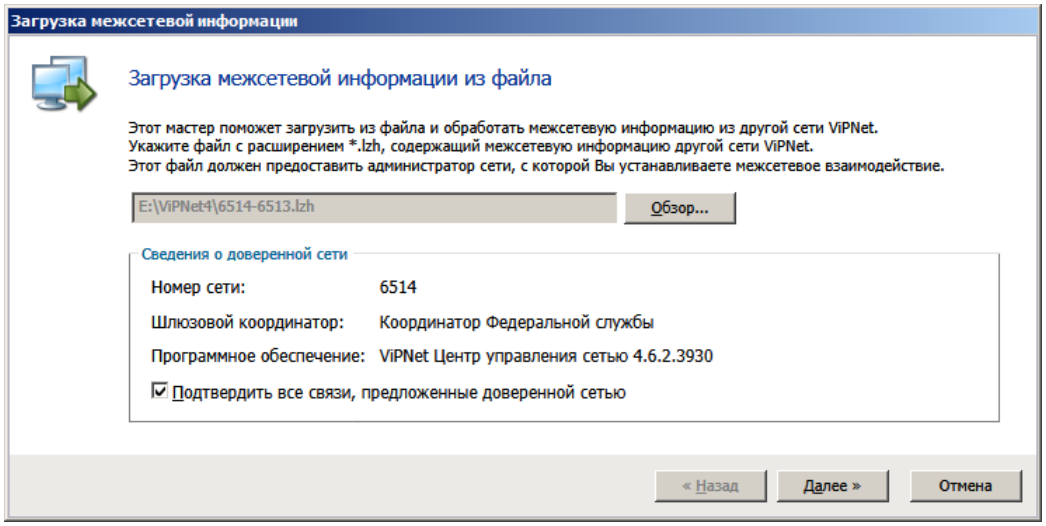

Рисунок 6 – Прием ответной межсетевой информации из сети Федеральной службы

5. В окне программы *ViPNet Удостоверяющий и ключевой центр* перейдите в представление *Администрирование* и на панели навигации выберите раздел *Необработанные данные* > *Контейнеры сертификатов администраторов сетей ViPNet*.
6. На панели просмотра выберите контейнер *Федеральная служба* и на панели инструментов нажмите кнопку *Обработать (Рисунок 136)*.

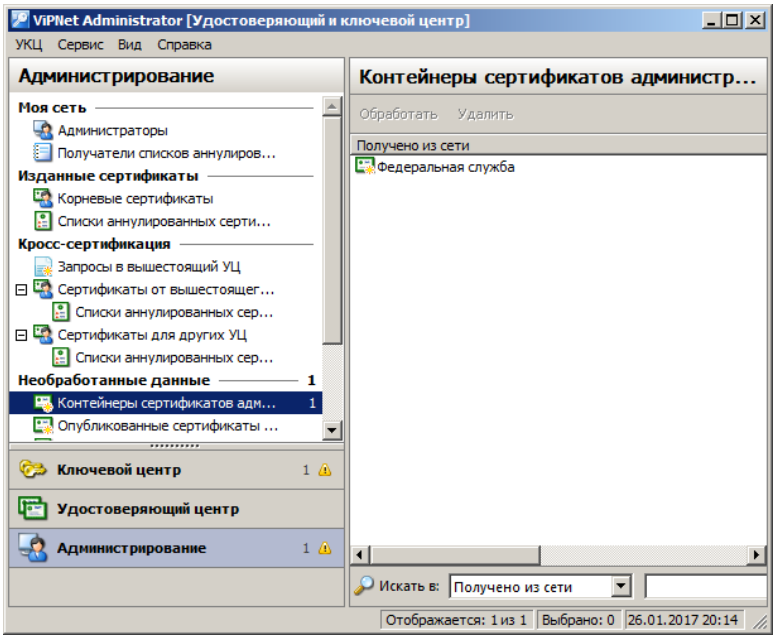

Рисунок 7 – Обработка контейнеров сертификатов и CRL Федеральной службы

7. В появившемся окне будет представлен список администраторов, сертификаты и CRL которых содержатся в выбранных контейнерах. Выберите администратора *Константин* и нажмите кнопку *Импортировать (Рисунок 137)*.

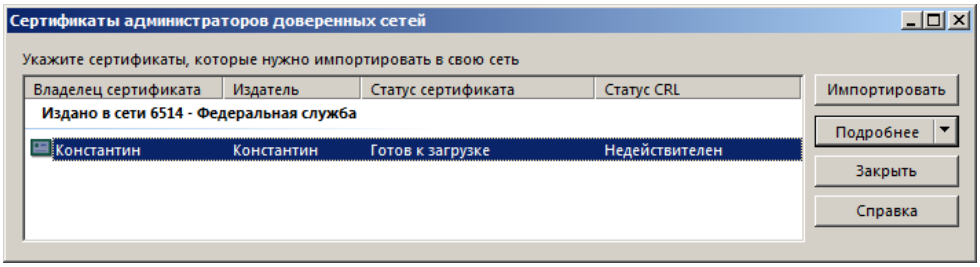

Рисунок 8 – Сертификаты администраторов доверенных сетей

8. В окне программы *ViPNet Удостоверяющий и ключевой центр* в представлении *Ключевой центр* выберите раздел *Межсетевое взаимодействие* > *Федеральная служба*.
9. Выберите межсетевой мастер-ключ и щелкните по нему правой кнопкой мыши. В контекстном меню выберите команду *Текущий* для ввода межсетевого мастер-ключа в действие.
10. Для узлов сети *Компании*, участвующих в межсетевом взаимодействии, *Главный администратор* и *Координатор Центр офис*, создайте и отправьте новые справочники и ключи.
11. Проверьте взаимодействие узлов *Координатор Федеральной службы* (сеть Федеральной службы) и *Координатор Центр офис* (сеть Компании).
12. На рабочем месте *Главного администратора* (сеть Компании), отправьте межсетевую информацию по защищенному каналу.

13. Убедитесь, что межсетевая информация поступила в ЦУС Федеральной службы и обработайте ее.

Проверка взаимодействия осуществляется в окне программы ViPNet Coordinator Монитор > *Защищенная сеть* > в контекстном меню узла выбрать *Проверить соединение*.