Межсетевое взаимодействие

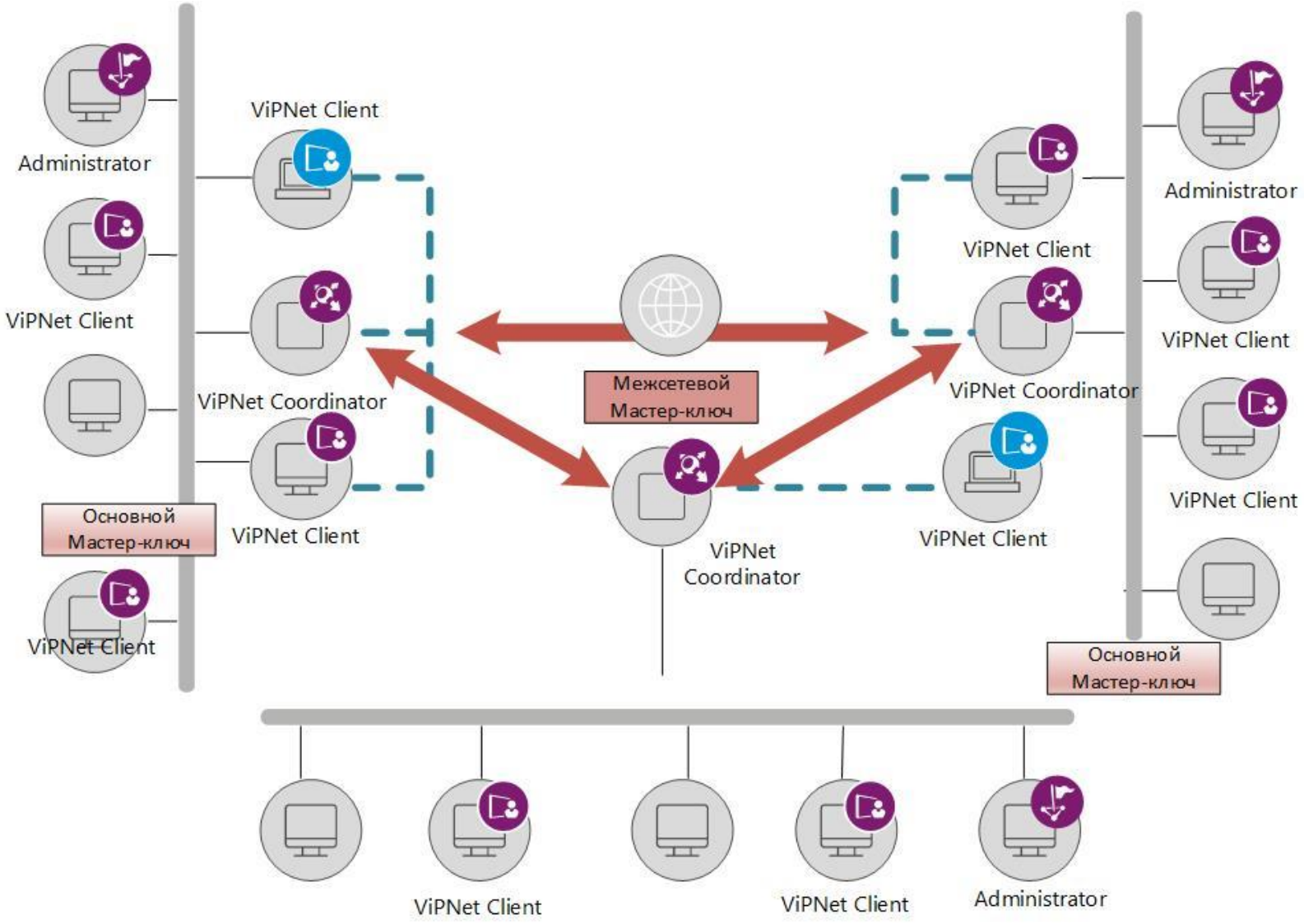
НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»
education@infotecs.ru

ОАО «ИнфоТеКС», Москва
(495) 737-61-92
www.infotecs.ru

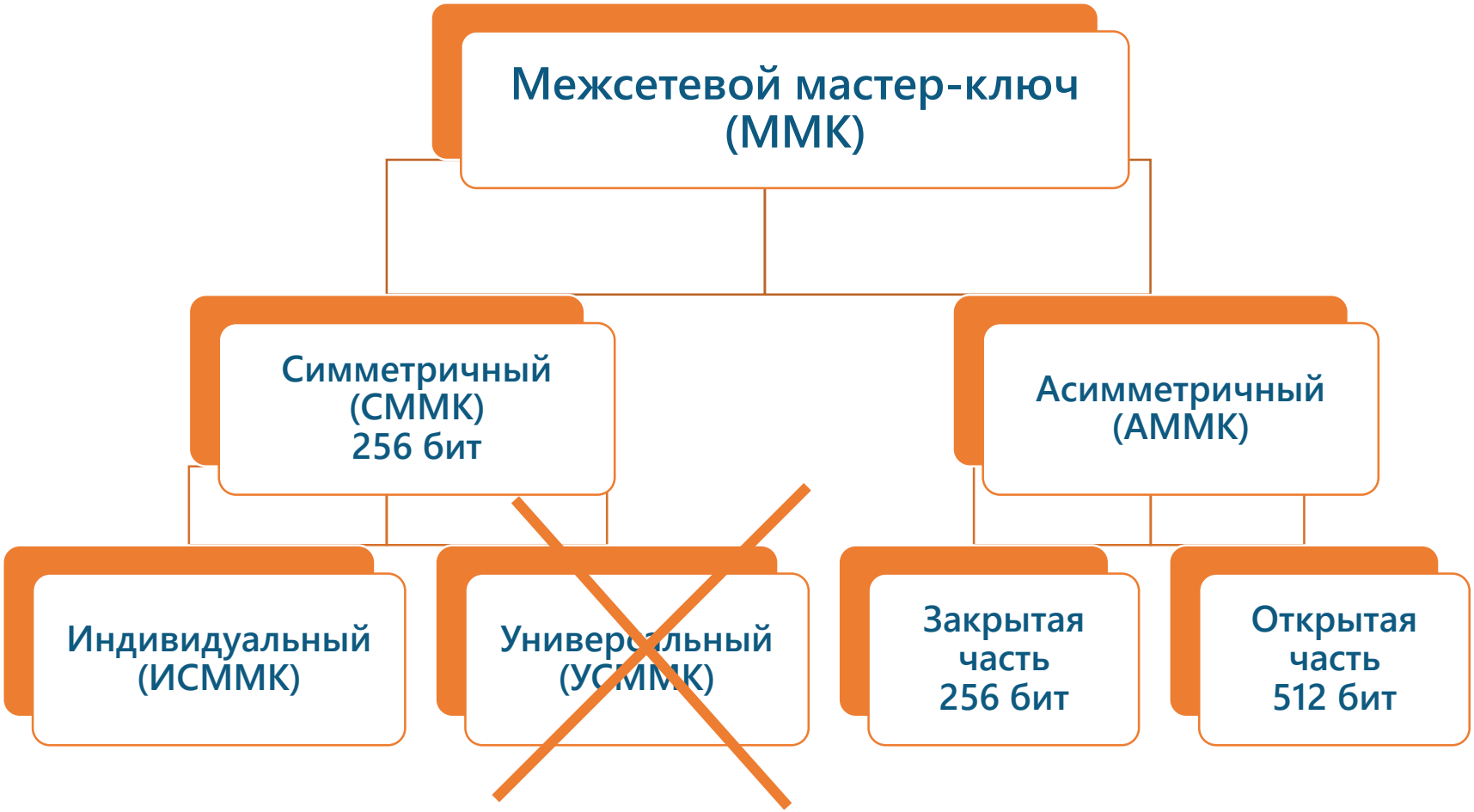
Межсетевое взаимодействие

- процесс взаимосвязи различных (с разными номерами) защищенных сетей ViPNet, с целью обеспечения защиты передаваемых данных с использованием технологий шифрования, туннелирования, ЭП.

Типы мастер-ключей



Типы мастер-ключей при межсетевом взаимодействии



Порядок организации межсетевого взаимодействия

Организация межсетевого взаимодействия на основе ИСММК

Этап 1

Происходит определение, кто будет инициатором. Затем инициатор формирует справочную информацию (в которой содержаться только сведения о предлагаемых сетевых узлах и их пользователях) и ИСММК (защищенный на пароле). На данном этапе должны быть учтены следующие особенности:

-сетевые узлы **Главного администратора** сети и **Шлюзового координатора** обязательны при установлении взаимодействия и автоматически добавляются в справочную информацию;

-пользователи сетевых узлов **Главного администратора** сети и **Шлюзового координатора** могут не добавляться в межсетевую информацию;

-добавление пользователей других сетевых узлов (рядовых узлов) является обязательным условием.

Организация межсетевого взаимодействия на основе ИСММК

Этап 2

На втором этапе администратор доверенной сети принимает входящую межсетевую информацию (справочники и ИСММК), обрабатывает и формирует ответный файл (.**lzh**) в ЦУС, содержащий связи пользователей и узлов сети.

Обязательным на данном этапе является принятие предложенных сетевых узлов.

Этап 3

Инициатор межсетевого взаимодействия также должен принять предложенные сетевые узлы, их пользователей и установленные связи.

После успешного обмена и обработки межсетевой информации в обеих сетях, администраторы могут формировать справочно-ключевую информацию для своих узлов добавленных в межсетевое взаимодействие и рассылать ее.

Особенности связей с объектами доверенных сетей

В межсетевом взаимодействии обязательно участвует пара объектов — **пользователь и сетевой узел этого пользователя**. Участие в межсетевом взаимодействии сетевого узла и пользователя **по отдельности невозможно**.

Исключение составляют узлы, которые являются **Центром управления сетью и шлюзовым координатором вашей сети**. По умолчанию пользователи этих узлов не участвуют в межсетевом взаимодействии, вы можете добавить их вручную.

При межсетевом взаимодействии вы можете изменить **только связи между пользователями**. Связи между сетевыми узлами изменяются автоматически.

При изменении связей с объектами доверенной сети необходимо согласовать изменения с администратором этой доверенной сети. Для этого предназначены статусы связей между объектами доверенных сетей.

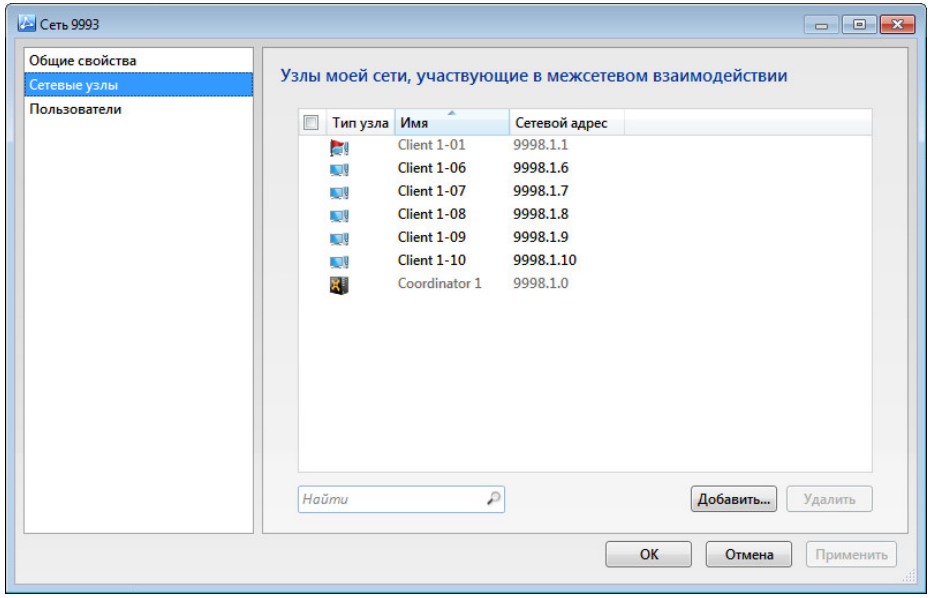
Модификация межсетевого взаимодействия (часть 1)

Изменение списка объектов, участвующих в межсетевом взаимодействии

Для каждой доверенной сети вы можете задать список сетевых узлов и пользователей вашей сети, которые могут участвовать в межсетевом взаимодействии с определенной доверенной сетью.

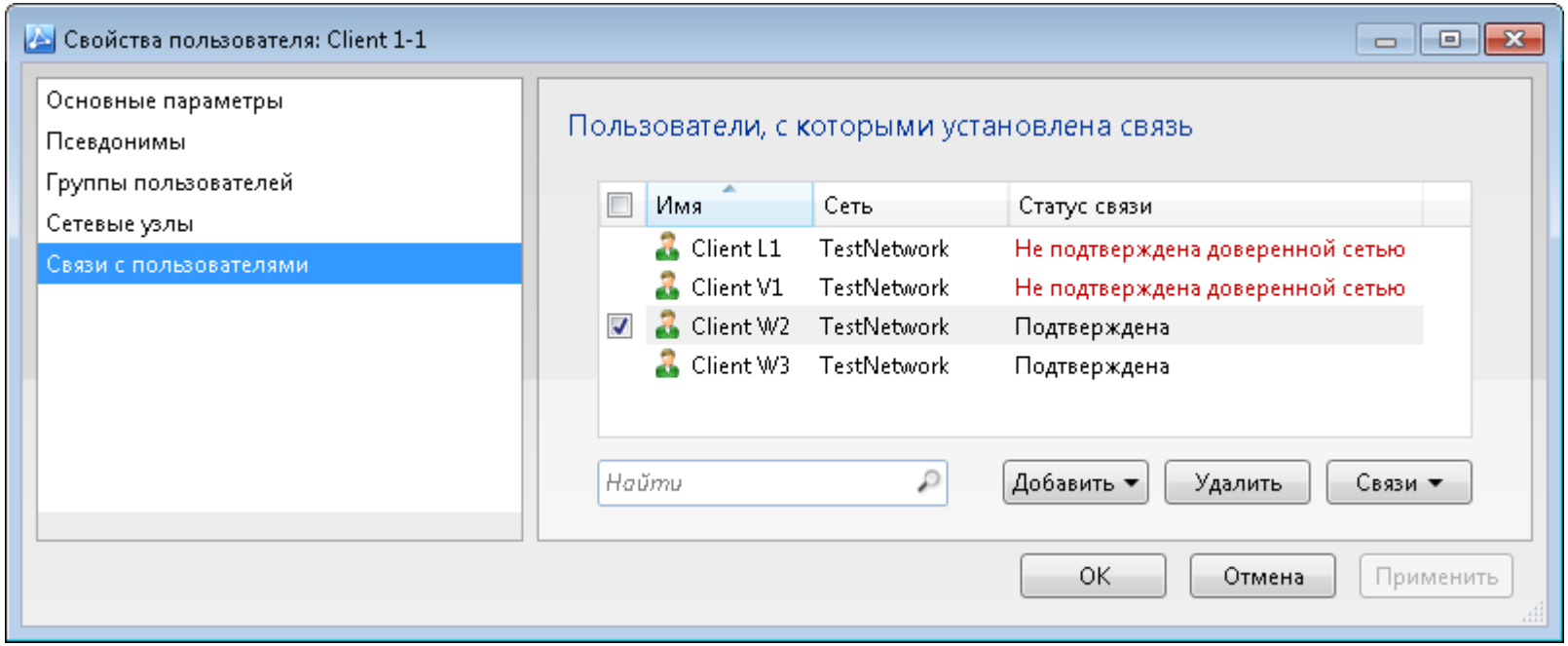
Изменение списка объектов, участвующих в межсетевом взаимодействии с определенной доверенной сетью, осуществляется в **ЦУС** в представлении **Доверенные сети.**

Примечание.
Невозможно исключить из межсетевого взаимодействия сетевые узлы, которые имеют связи с узлами доверенной сети в статусе ***Предложена доверенной сетью.***



Изменение связей с объектами доверенной сети

Управление связями между объектами своей сети и объектами доверенной сети осуществляется с помощью изменения связей между пользователями этих сетей. Если со стороны доверенной сети в межсетевом взаимодействии участвуют группы пользователей, вы также можете создать связи между этими группами и пользователями вашей сети.



Модификация межсетевого взаимодействия (часть 3)

Изменение статуса связей с объектами доверенных сетей

Предложена доверенной сетью — связь между объектами создана администратором доверенной сети и пока не подтверждена и не запрещена в вашей сети.

Не подтверждена доверенной сетью — связь между объектами создана в вашей сети и пока не подтверждена и не запрещена администратором доверенной сети.

Подтверждена — связь между объектами подтверждена в вашей сети и в доверенной сети.

Запрещена доверенной сетью — администратор доверенной сети запретил создавать связь между объектами.

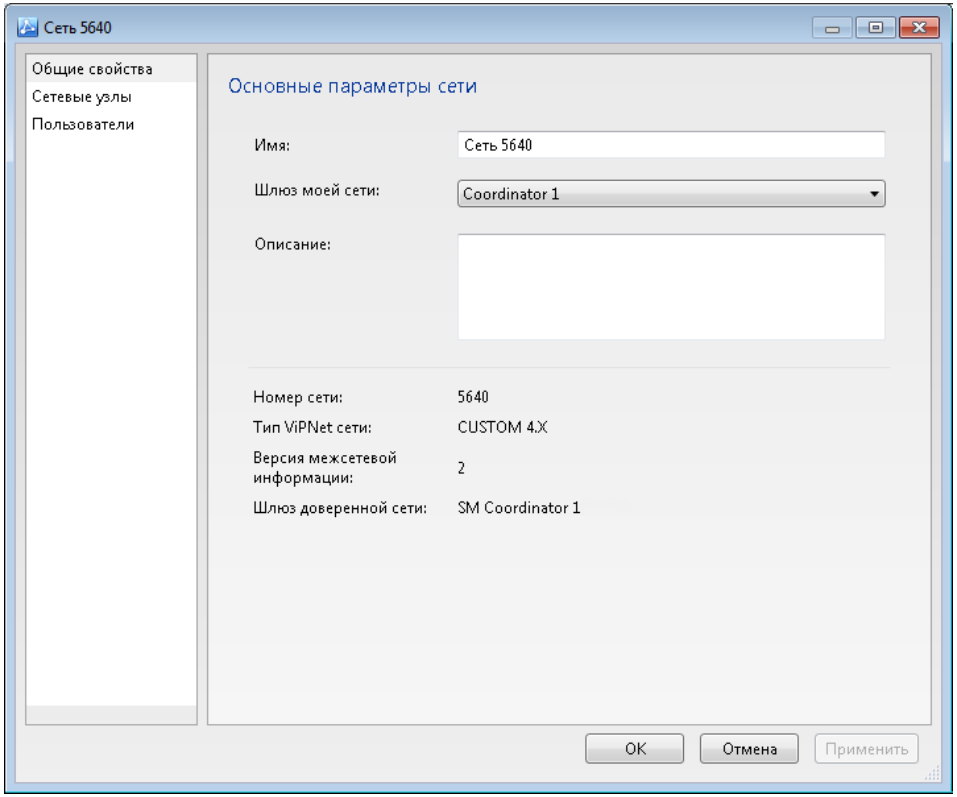
Запрещена своей сетью — связь запрещена в вашей сети, администратор доверенной сети не сможет создать связь между объектами.

Модификация межсетевого взаимодействия (часть 3)

Изменение шлюзового координатора своей сети

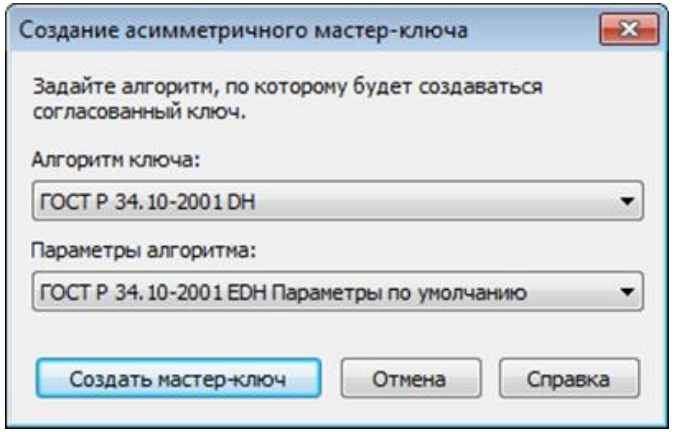
В процессе работы сети может потребоваться изменить координатор своей сети, который используется в качестве шлюзового для связи с определенной доверенной сетью.

Необходимо учитывать при выполнении данной процедуры, что сперва необходимо создать и отправить межсетевую информацию в доверенную сеть и только после этого формировать и отправлять справочную и ключевую информацию на старый и новый шлюзовые координаторы, своей сети.



Особенности установления межсетевого взаимодействия на АММК (часть 1)

При установке межсетевого взаимодействия с использованием **асимметричного межсетевого мастер-ключа** администраторам сетей на подготовительном этапе необходимо согласовать параметры асимметричного ключа.

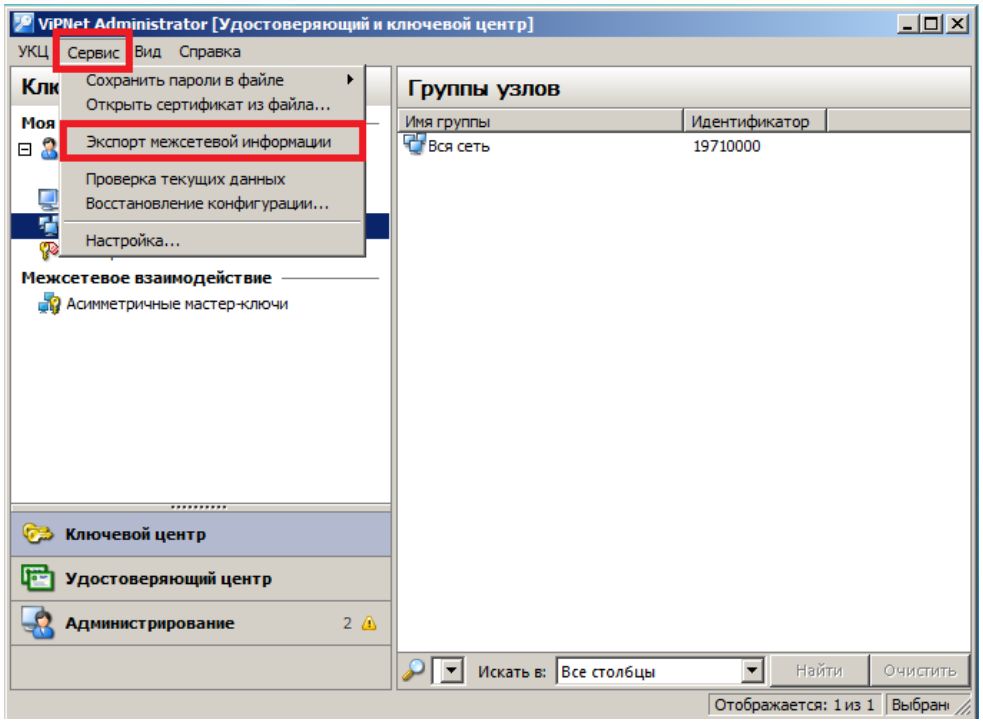


При передаче мастер-ключа асимметричного типа необходимо в состав межсетевой информации включить **сертификат администратора**, которым был подписан данный мастер-ключ.

Также из УКЦ должны быть экспортированы:

- списки аннулированных сертификатов (CRL) пользователей своей сети ViPNet;
- изданные кросс-сертификаты.

Особенности установления межсетевого взаимодействия на АММК (часть 2)



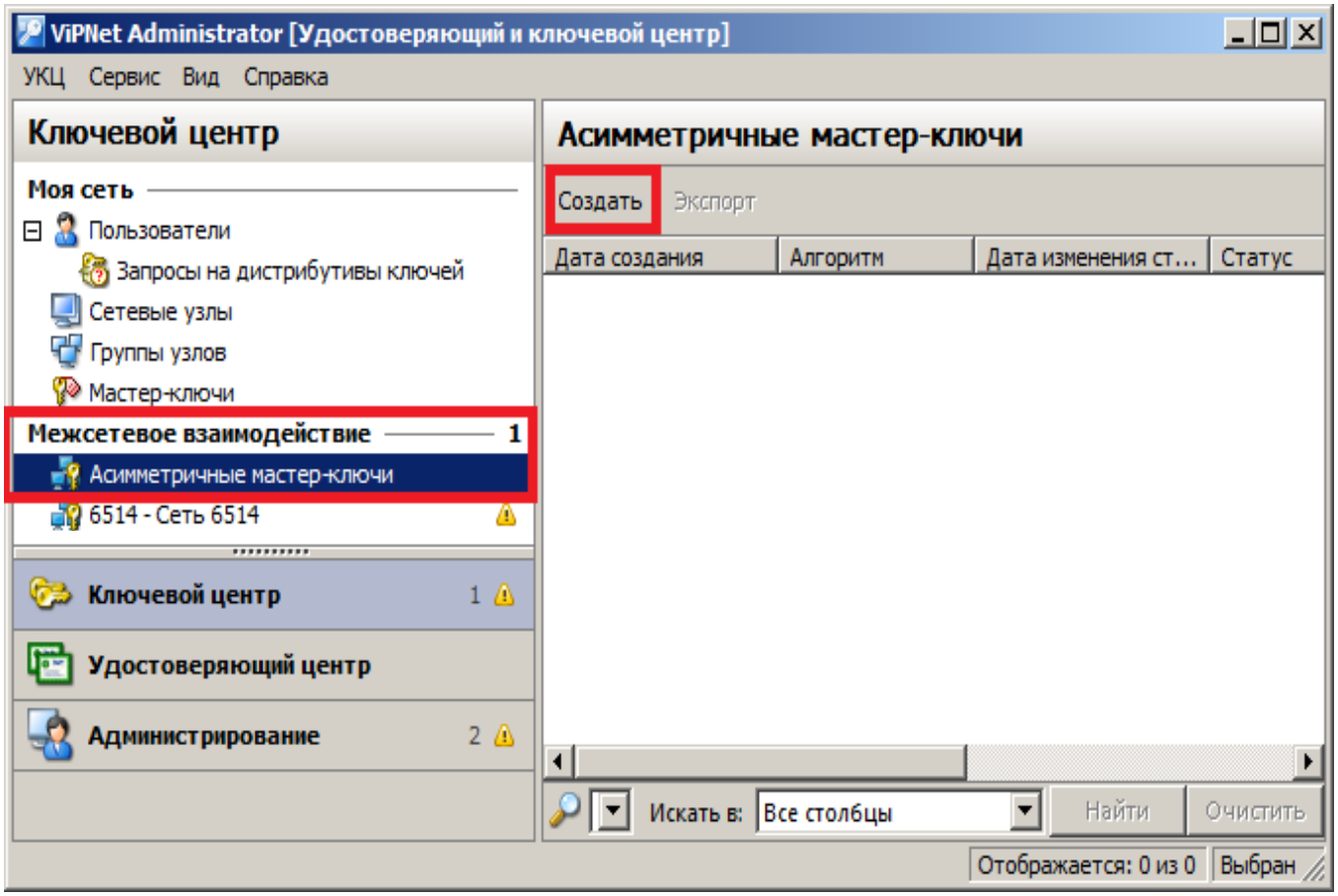
Эти данные должны быть включены в формируемый в ЦУСе файл с расширением **.lzh**.

Для переноса данных в ручном режиме необходимо в УКЦ зайти в меню **Сервис→Экспорт межсетевой информации.**

После этого можно формировать файл межсетевой информации в ЦУСе (действия в ЦУС аналогичны тем, что производились при установлении межсетевого взаимодействия на ИСММК).

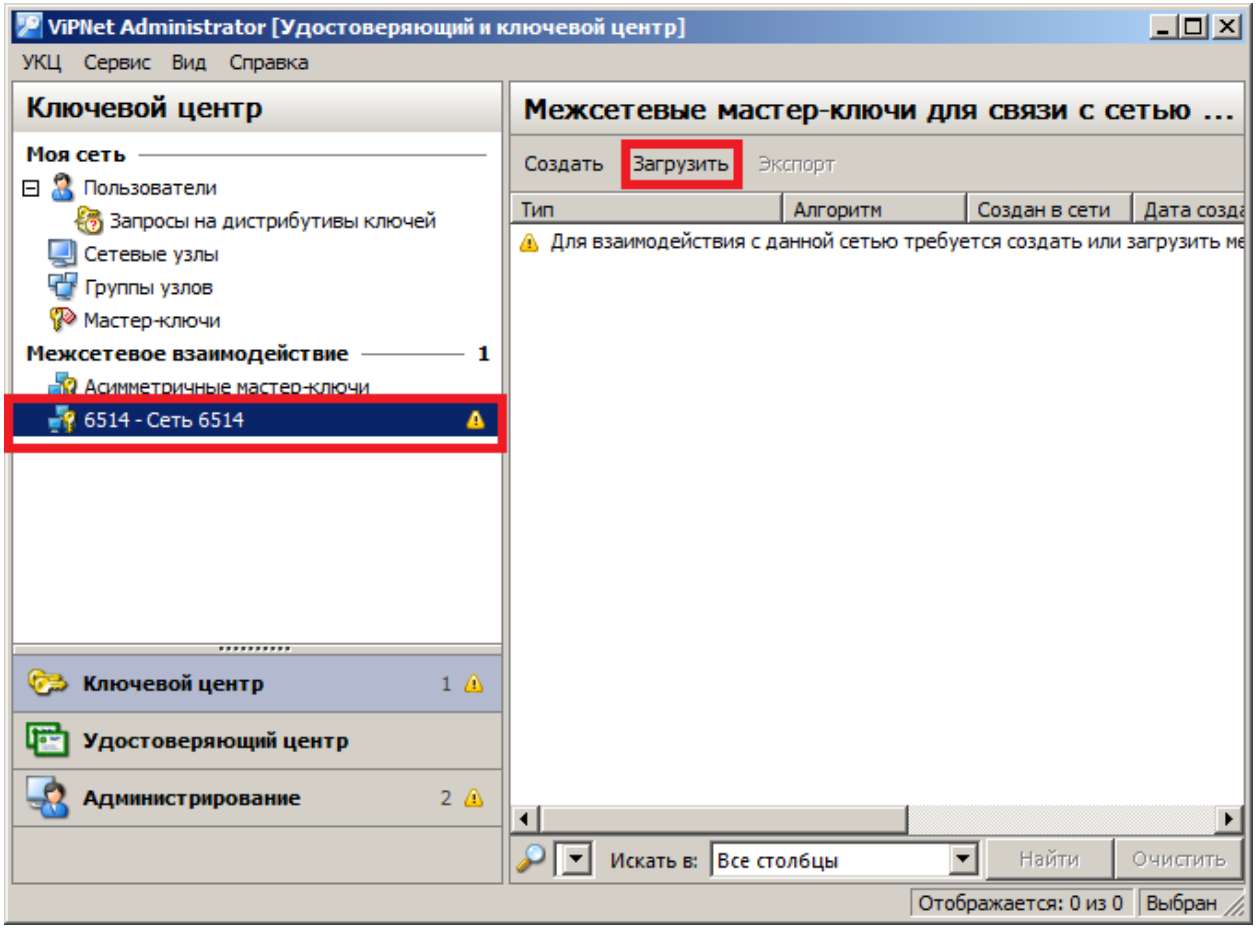
Особенности установления межсетевого взаимодействия на АММК (часть 3)

После того, как была сформирована и сохранена в файл (**.lzh**) справочная информация в ЦУС, необходимо в УКЦ в разделе **Асимметричные мастер-ключи** создать АММК, выгрузить его и сохранить в виде файла **номер сети.cer**.



Особенности установления межсетевого взаимодействия на АММК (часть 4)

Эти файлы **администратор доверенной сети** после получения должен обработать: справочную информацию в ЦУС, а сертификат администратора и АММК **в УКЦ в разделе конкретной доверенной сети**.



Ввод в действие и прекращение использования межсетевого мастер-ключа

Межсетевой мастер-ключ используется для формирования ключей обмена между узлами вашей и доверенной сети, в случае если он является **действующим**.

- Если межсетевой мастер-ключ **импортируется** из другой сети, он вводится в действие **автоматически**.
- Если вы **экспортировали** межсетевой мастер-ключ в другую сеть, введите его в действие в своем Удостоверяющем и ключевом центре **вручную**, чтобы начать использовать.

- Если для связи с определенной сетью в УКЦ имеется несколько симметричных или асимметричных межсетевых мастер-ключей, действующим может быть только один из них.

Действие межсетевого мастер-ключа можно прекратить, например, если был выявлен факт его компрометации.

Особенности создания межсетевой информации в ПО ViPNet Administrator 3

Для организации межсетевого взаимодействия с доверенной сетью, в которой используется ПО ViPNet Administrator версии 3.x, после формирования данных для экспорта администратору этой сети необходимо выполнить следующие дополнительные действия, чтобы создать файл межсетевой информации, поддерживаемый ПО ViPNet Administrator версии 4.x:

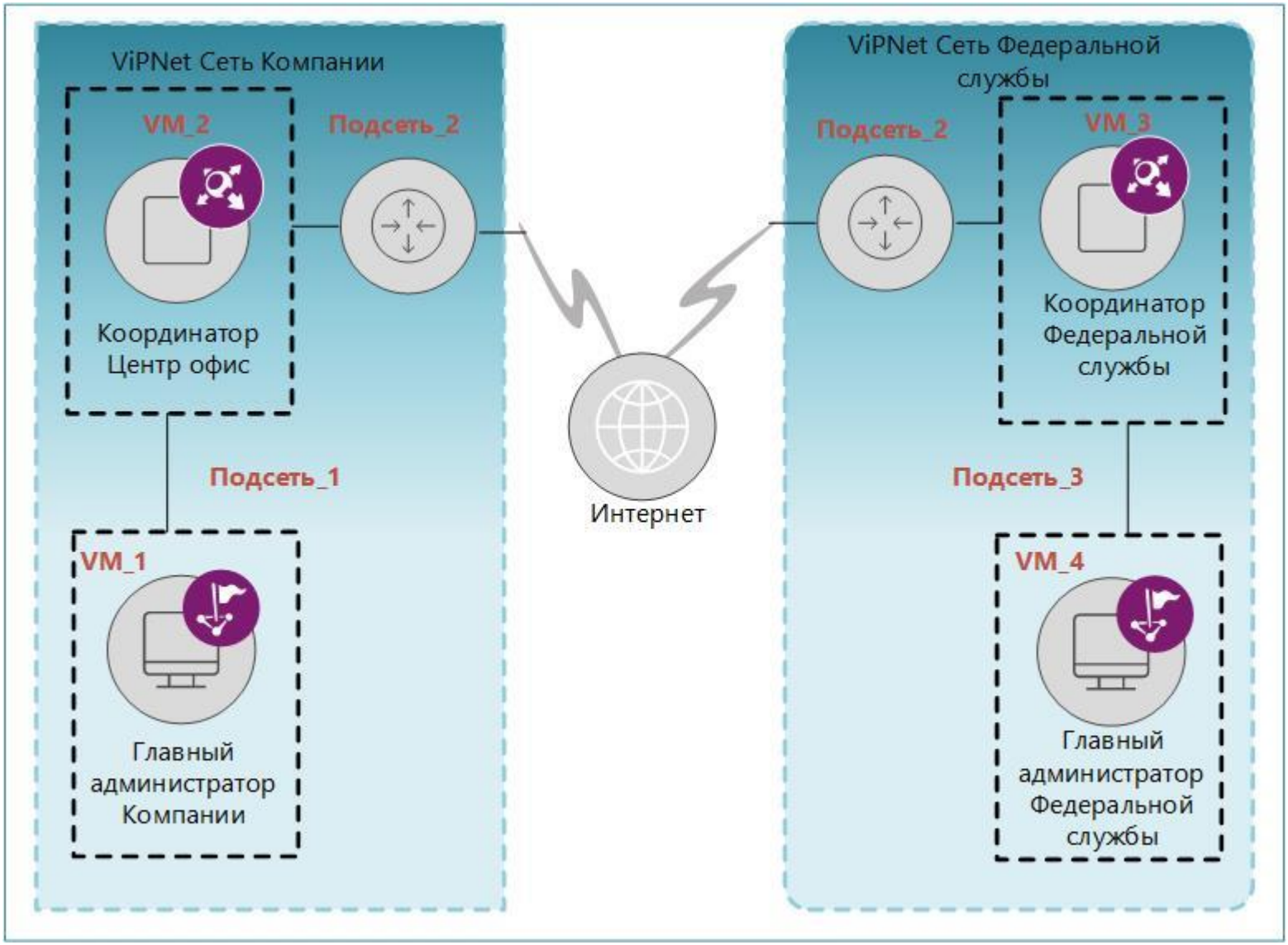
1 В окне **ViPNet Центр управления сетью** в меню **Службы** выбрать команду **Экспорт**.

2 В окне **Экспорт** выбрать нужную доверенную сеть и нажать кнопку **Архив**.

3 В окне **Задайте каталог назначения** указать папку, в которую будет скопирован архив (по умолчанию программа предлагает папку \NEW\EXPORT) и нажать кнопку **Принять**.

Файл формата **.lzh** будет помещен в папку с именем, совпадающим с номером доверенной сети, для которой предназначен экспорт. Далее администратор сети, в которой используется ПО ViPNet Administrator 3.x, может передать его вам.

Схема стенда для практического занятия



infotecs

Спасибо за внимание!

Вопросы?

НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»
education@infotecs.ru

ОАО «ИнфоТеКС», Москва
(495) 737-61-92
www.infotecs.ru