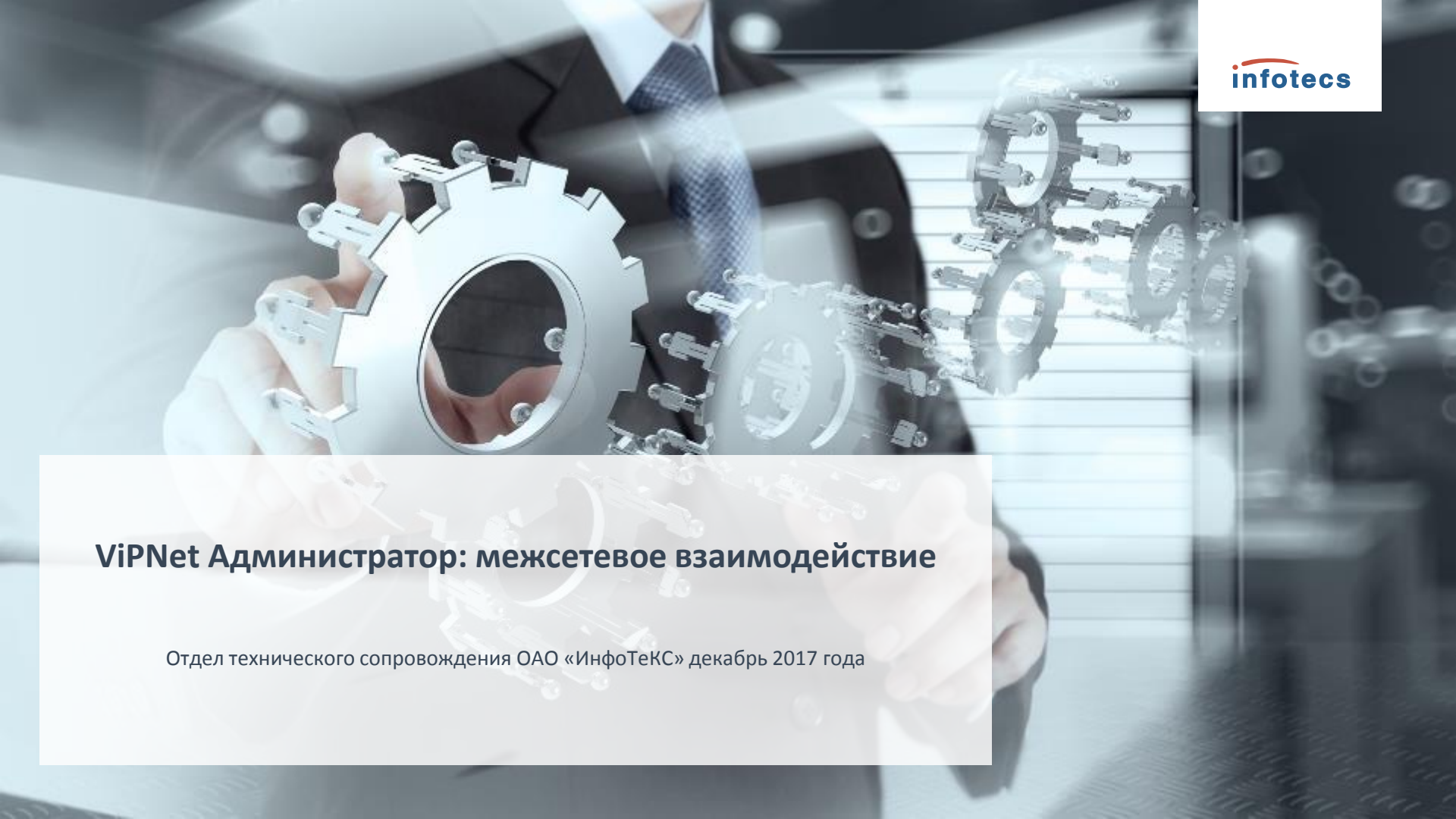


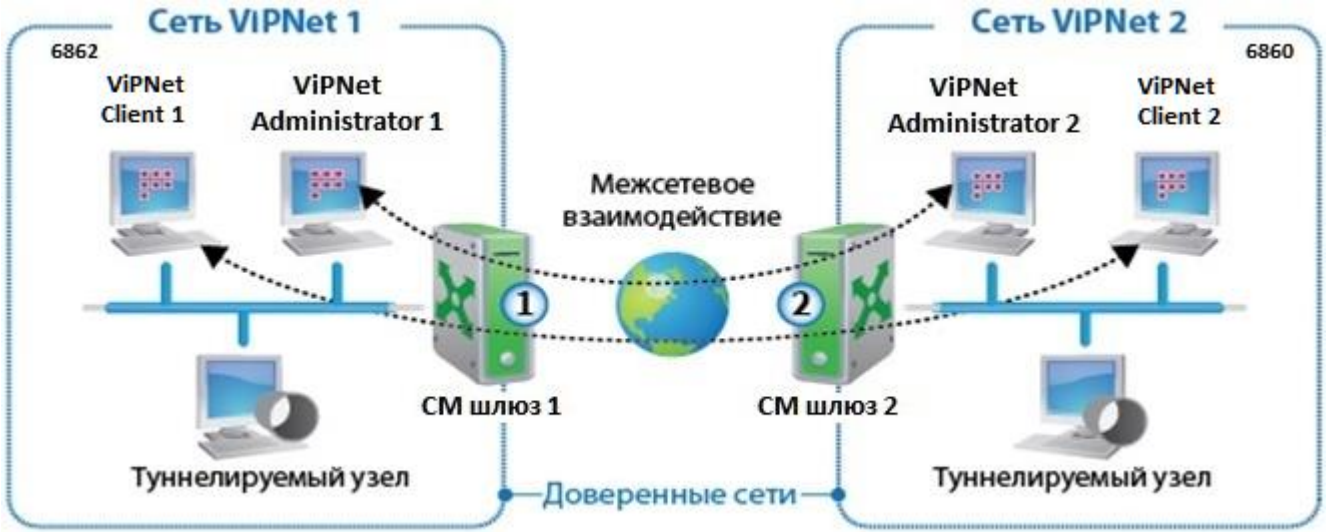
ViPNet Администратор: межсетевое взаимодействие

Отдел технического сопровождения ОАО «ИнфоТеКС» декабрь 2017 года

Последовательность материалов:

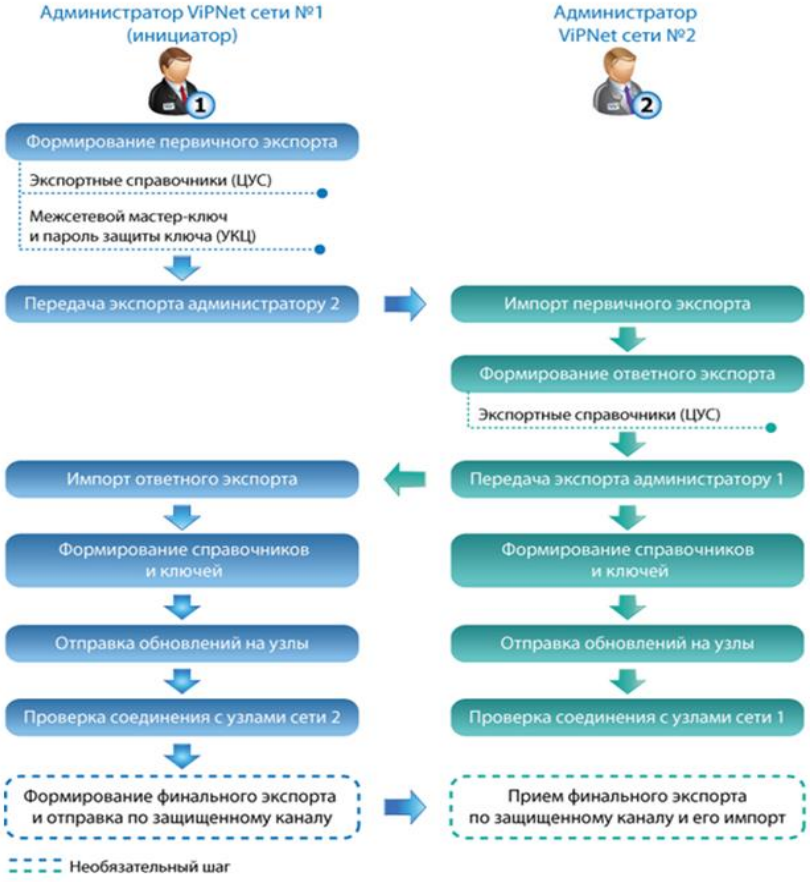
- общая информация, регламент и последовательность установления взаимодействия;
- состав минимального набора объектов и начало установления взаимодействия;
- создание справочников начального экспорта и ключей в версиях 3.2 и в 4.6;
- формирование ответного в версии 4.6 и его прием в 3.2;
- обсудим элементы эксплуатации межсетевого взаимодействия;
- причины блокировки IP трафика с регистрацией 2-го события;
- причины нарушения обмена служебными данными между ЦУС-ами;
- проблемы приема межсетевой информации;
- нарушение приема конвертов MFTP из доверенной сети (Bad/Invalid/Trash);

В завершении обсудим ваши вопросы.



Фрагмент материала из документации, входящей в комплекты ПО ViPNet Administrator и содержащей практические сценарии использования сетей ViPNet включая организацию межсетевого взаимодействия. Более детальные материалы содержат методические руководства Учебного центра ИнфоТеКС и авторизованных региональных Учебных центров. По конкретным приложениям надо использовать документы, такие как «ViPNet Центр управления сетью. Руководство администратора» и «ViPNet Удостоверяющий и ключевой центр 4. Руководство администратора». http://edu.infotecs.ru http://docs.infotecs.ru www.youtube.com/user/InfotecsDoc

Фрагмент документа «ViPNet Administrator: Практические сценарии использования»

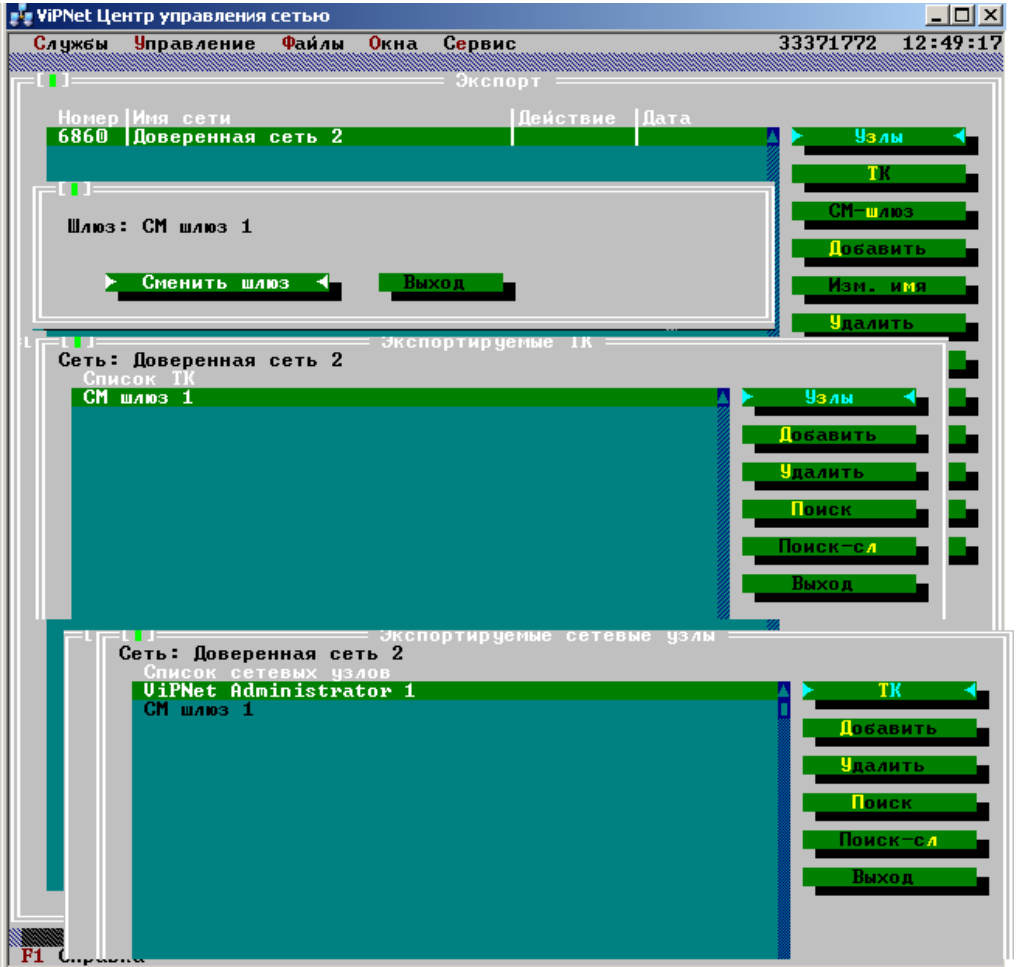


Рисунок·4:·Схема·настройки·межсетевого·взаимодействия¶

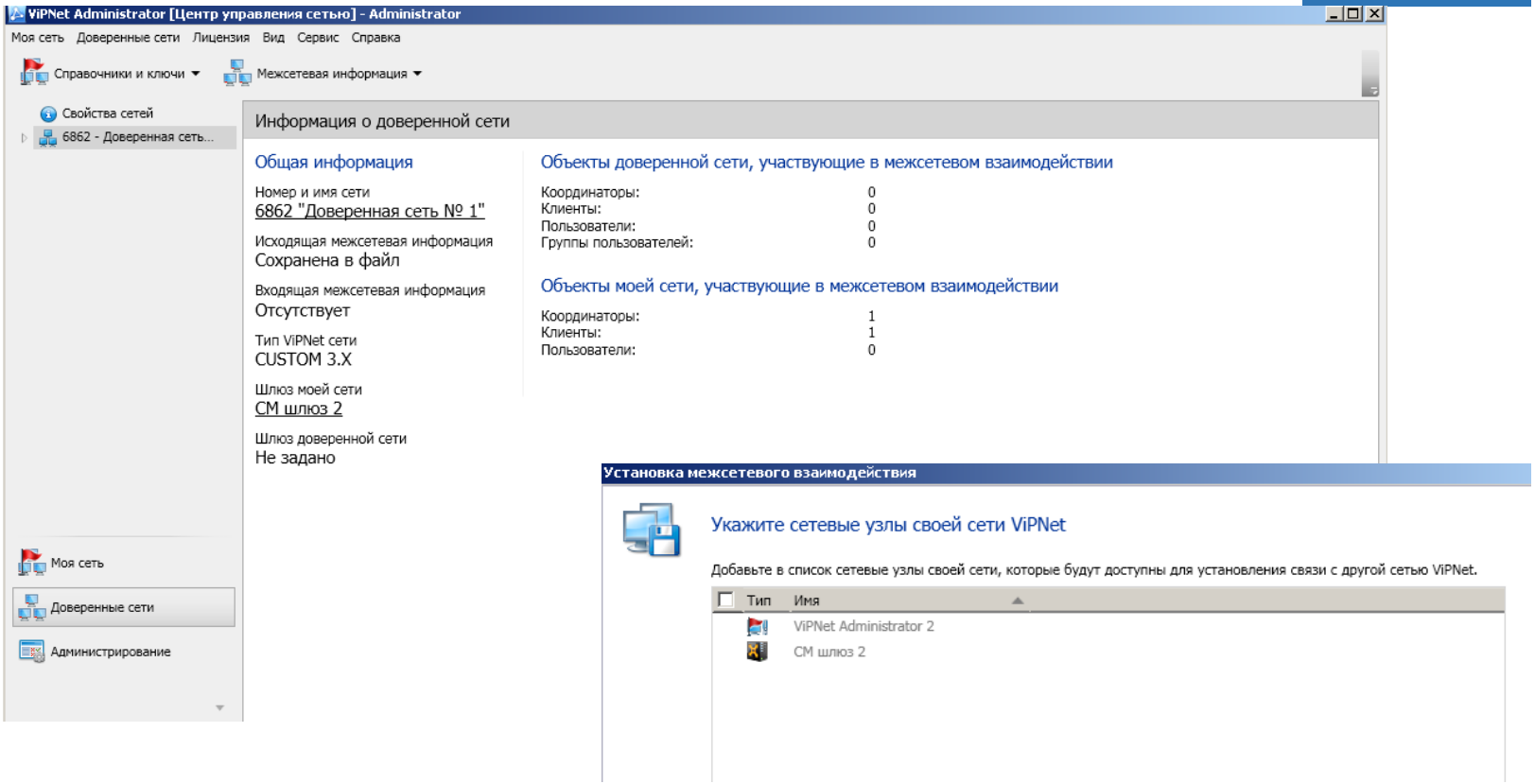
Согласуйте Регламент взаимодействия:

1. Цели взаимодействия и используемые средства.
2. Типы и таблицу объектов связей с их наименованием.
3. Контактные данные ответственных исполнителей, администраторов обоих сетей для оперативной связи.
4. Даты и время проведения технических, регламентных работ, во время которых связь взаимодействия может временно прекращаться.
5. Допустимое время реакции на восстановление при возникновении аварий оборудования.
6. Значимость применения электронной цифровой подписи пользователей.
7. Класс СКЗИ допустимый участникам взаимодействия.
8. Даты обновления межсетевых ключей обмена.
9. Порядок действий при компрометациях объектов взаимодействия или смены вариантов ключей объектов.

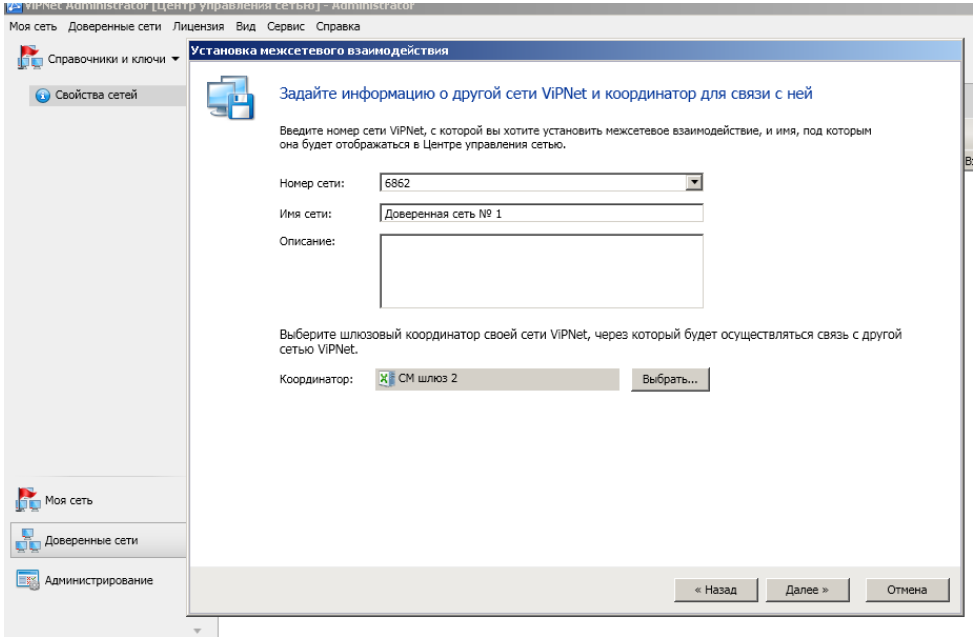
Состав минимального набора объектов экспорта в доверенную сеть (ЦУС версии 3.2):

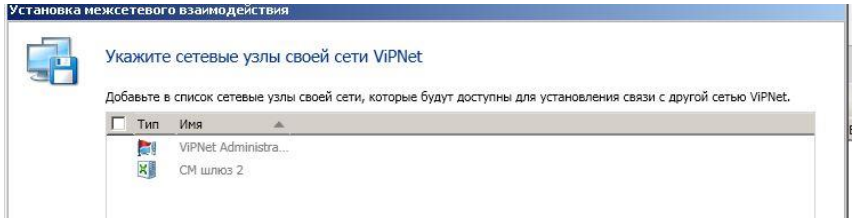


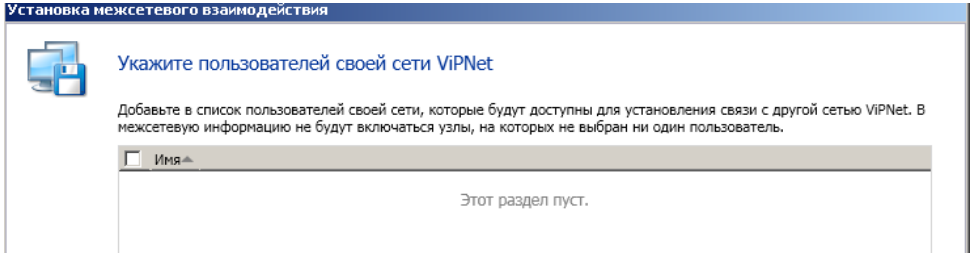
Состав минимального начального экспорта в доверенную сеть в ЦУС 4.6 :



Формирование минимального набора объектов экспорта в доверенную сеть (ЦУС версии 4.6):

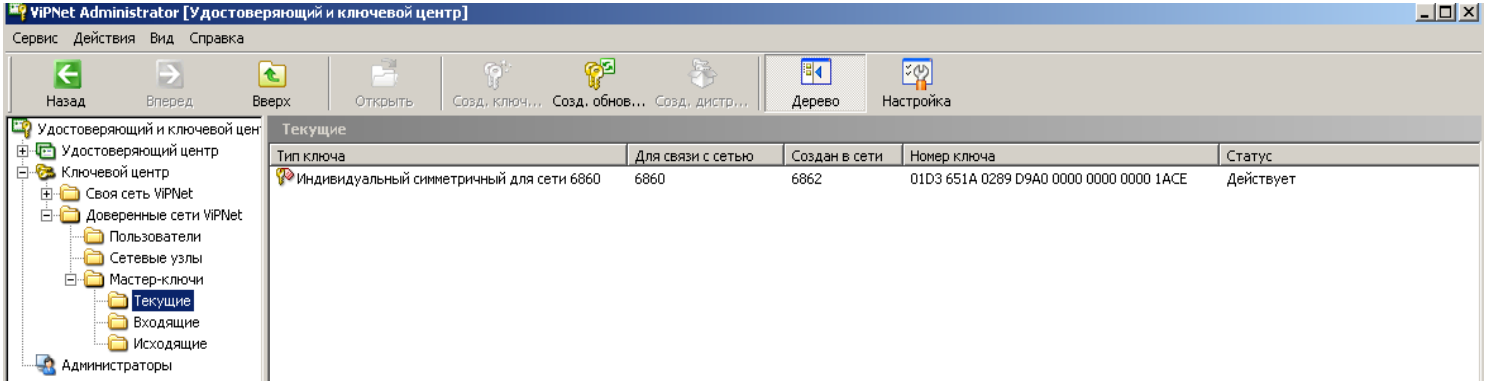




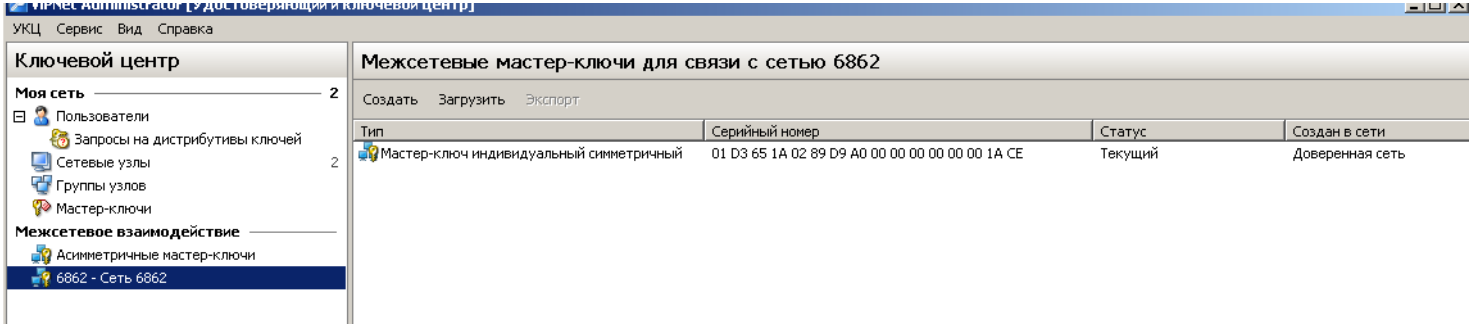


Создание межсетевых мастер ключей обмена

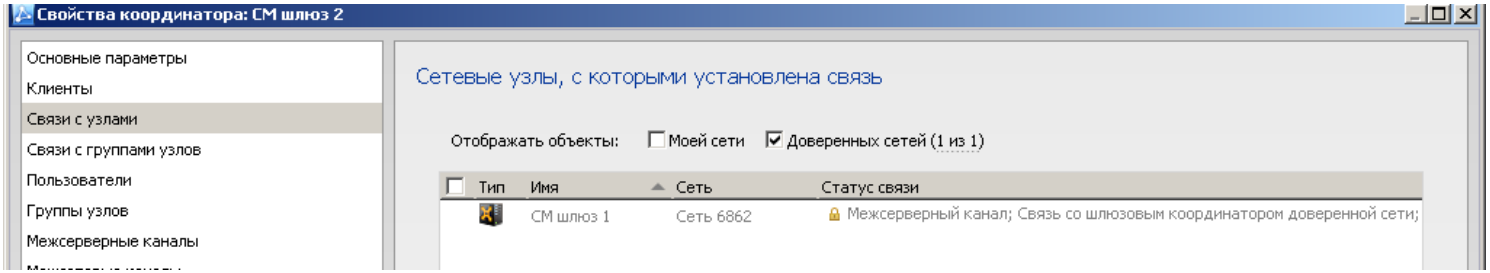
Создаем индивидуальный межсетевой ключ в УКЦ 3.2, экспортируем его и вводим его в действие :

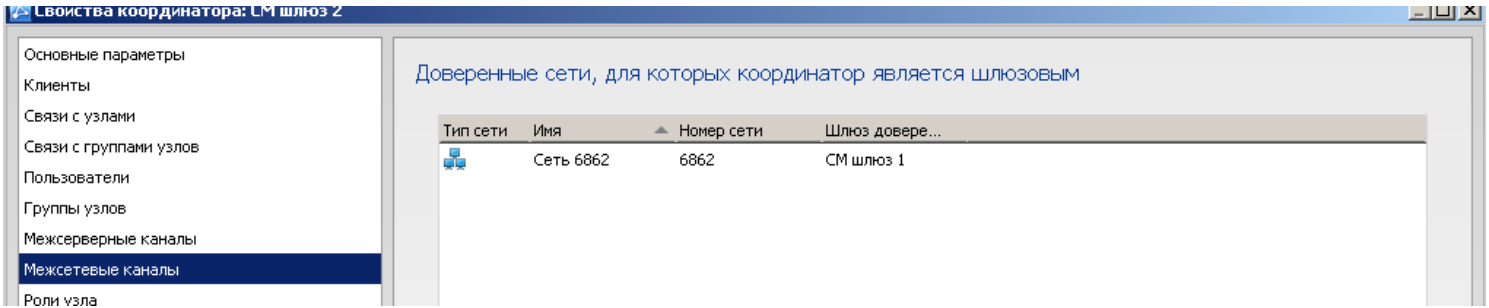


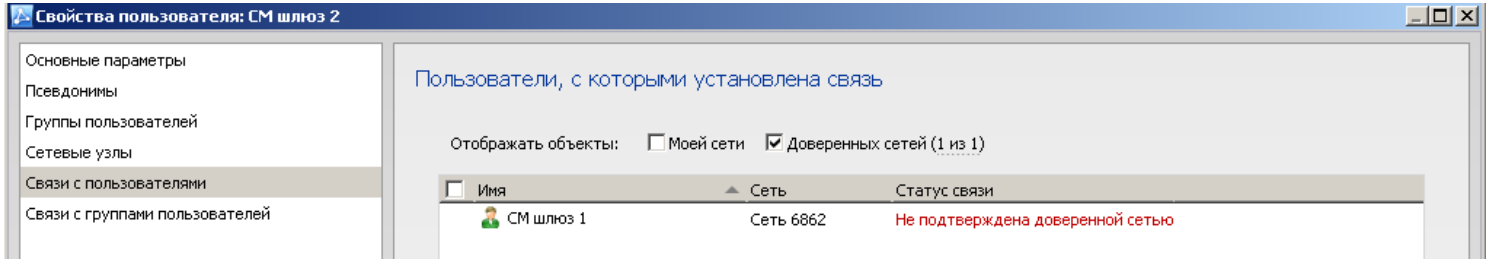
После приема справочников в ЦУС загружаем этот ключ в УКЦ 4.6 и задаем ему статус «Текущий» :



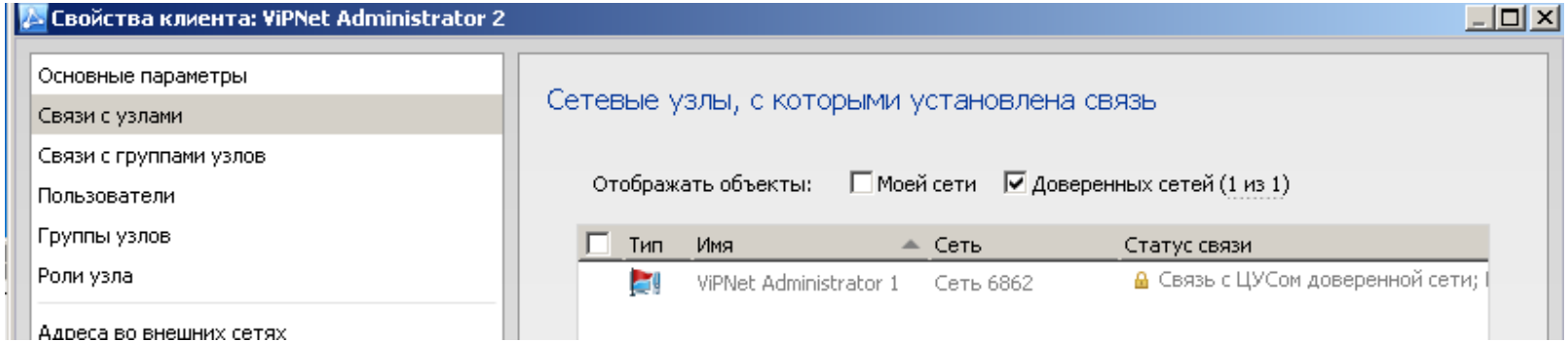
Перед формированием справочников ответного экспорта проверяем минимум связей в ЦУС 4.6 :

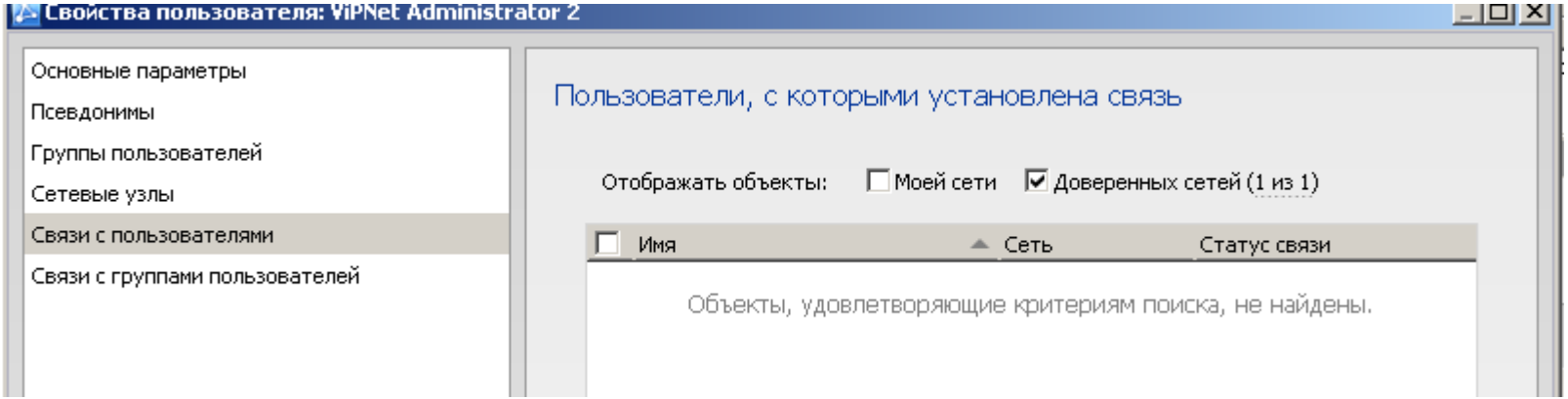




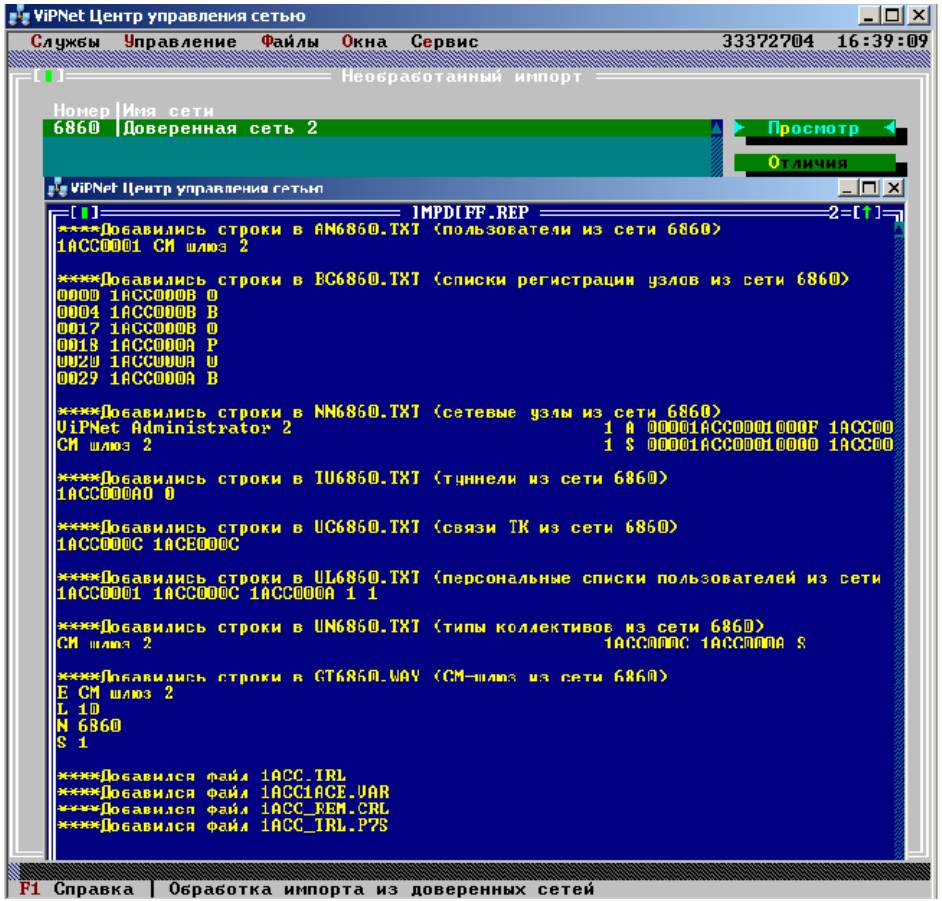


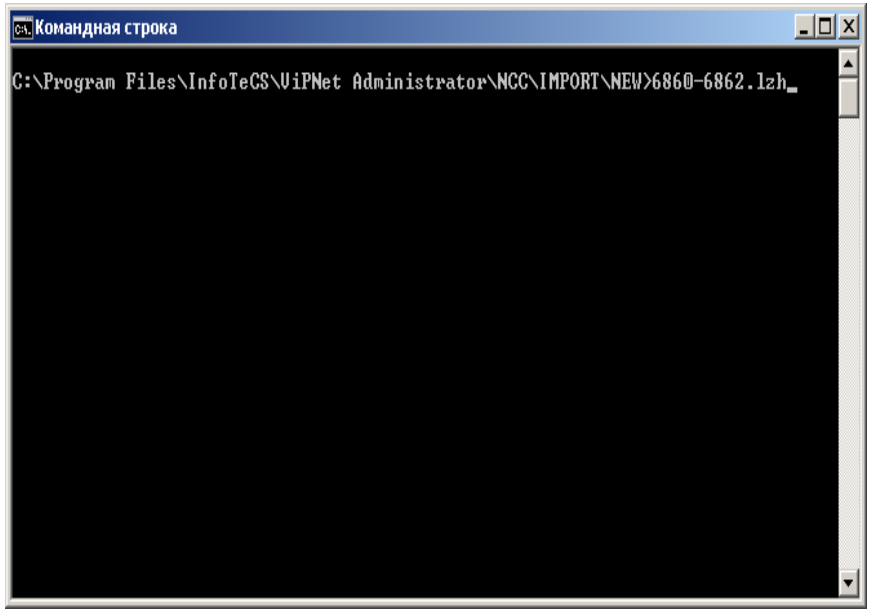
Связи узлов «ViPNet Administrator» не изменяем :



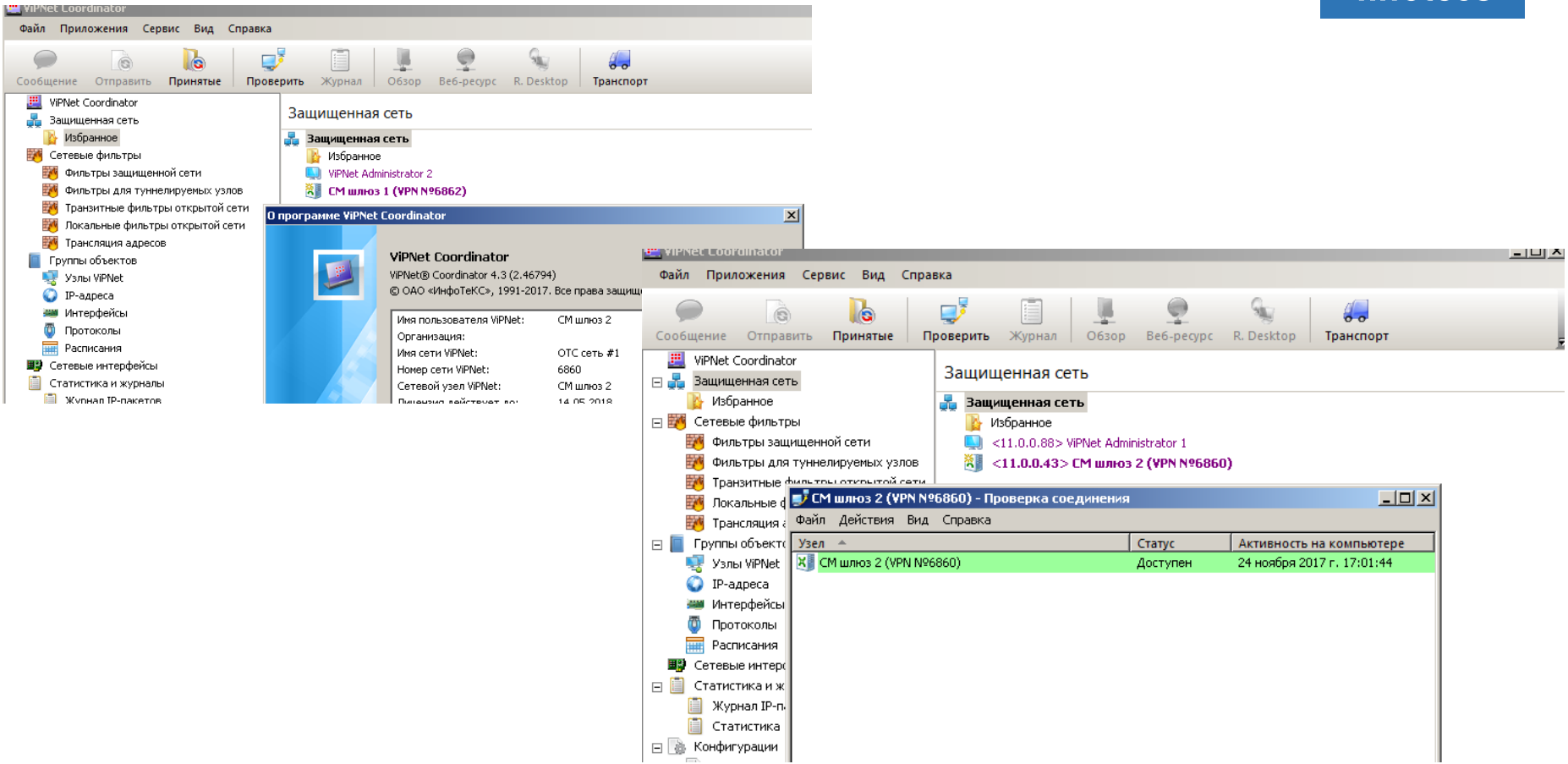


Прием ответного экспорта в ЦУС 3.2 инициатора взаимодействия :



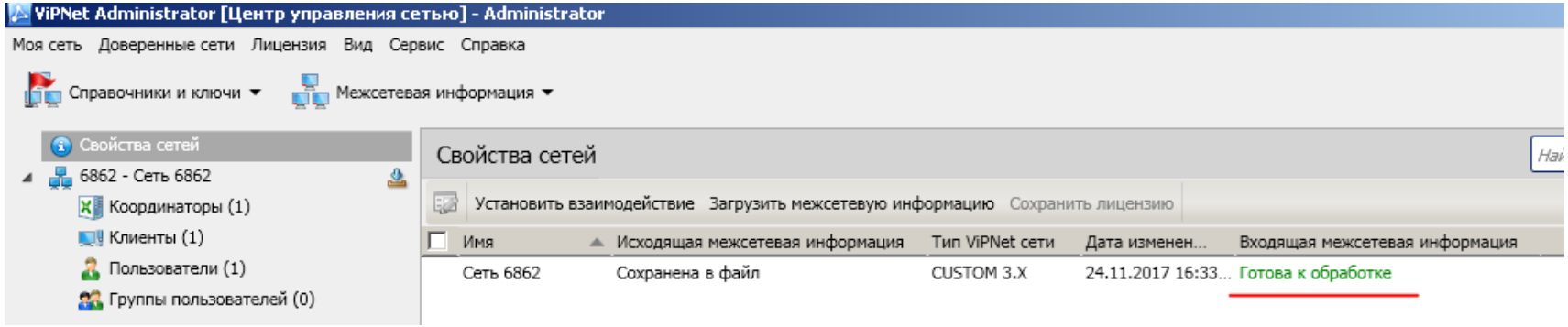


Получено защищенное соединение между шлюзовыми координаторами ::

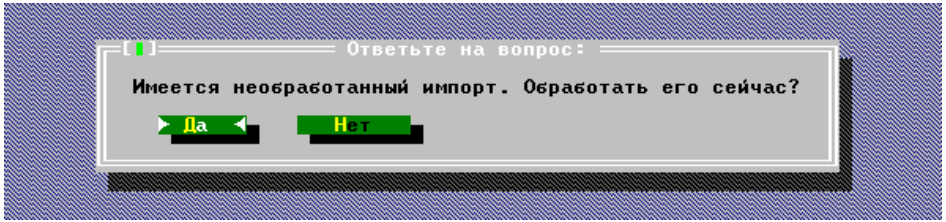


Индикация обмена межсетевой информацией между ЦУС обоих сетей :

Из ЦУС 3.2 отправлен заключительный экспорт и в ЦУС 4.6 он получен :



Из ЦУС 4.6 отправлен заключительный экспорт и в ЦУС 3.2 он получен :



Узел абонента перестал соединяться с узлом доверенной сети:
- в ViPNet Мониторе пользователя узла проверяем корректность задания типа межсетевого экрана;
- используем журналы IP пакетов для определения событий передачи защищенного трафика;
- при нарушении передачи писем Деловой почты и обмена файлами используем журналы MFTP на всех передаточных звеньях своей сети, проверяем актуальность справочников межсетевого взаимодействия;
- координируем поиск источника проблемы с Администратором доверенной сети по журналам IP пакетов.

Требуется изменение шлюзового координатора с действующего на другой:
- по соответствующему разделу документации Центра управления сетью составляем план действий и их сроки выполнения;
- убеждаемся в правильности синхронизации времени и часового пояса на узлах своей сети;
- в доверенную сеть отправляем данные для предварительного установления защищенной связи с новым шлюзовым координатором;
- убеждаемся что защищенная связь установлена;
- извещаем Администратора доверенной сети и отправляем исходящую межсетевую информацию (Экспорт) содержащую новый шлюз;
- на узлы своей сети отправляем обновления справочников содержащие новый межсетевой канал.

В своей сети проводится компрометация узла или его абонента имеющего связи с доверенной сетью:
- если это шлюзовой координатор, то до применения на нем новых вариантов ключей отправляем в доверенную сеть справочники с новыми вариантами и извещаем Администратора доверенной сети для оперативности смены ключевых параметров;
- если это узел или его абонент участвующие в передаче писем Деловой почты с применением автопроцессинга, то обязательно извещаем Администратора доверенной сети одновременно с отправкой новых данных (Экспорта) в его сеть так как может возникнуть необходимость в перенастройке элементов получателей/отправителей правил автопроцессинга.

Прекращение взаимодействия:
- извещаем Администратора доверенной сети и подтверждаем это протоколом к Регламенту взаимодействия;
- в ЦУС версий 3.2 удаляем экспорт в эту сеть, формируем справочники и в УКЦ удаляем все мастер-ключи, на свои узлы рассылаем обновления;
- в ЦУС версий 4.6 выполняем «Прекратить взаимодействие» с учетом флага удаления всех данных, формируем обновления и применяем их на своих узлах.

Передача в доверенную сеть сертификатов издателей:

- если в вашей сети применяются сертификаты издателя полученные от вышестоящего УЦ и точки распространения сертификата издателя и его списка аннулированных сертификатов публикуются на общедоступных ресурсах то об этом должен быть извещен Администратор доверенной сети;
- межсетевой экспорт не содержит всего необходимого для полной проверки действительности цепочек издателей, для успешного импорта корневого сертификата доверенной сети необходимо сначала импортировать всех его издателей и их списки отзыва;
- если у вас собственный корневой сертификат, то все необходимое будет помещаться в набор исходящей межсетевой информации.

В зависимости от конкретной реализации функционала в вашей версии УКЦ для обоих вариантов всегда можно воспользоваться просмотром данных которые размещаются в вашем исходящем экспорте: - в УКЦ выполните проверку текущих данных; - в ЦУС создайте и сохраните экспорт в LZH-файл; - распакуйте архиватором во временную папку; - откройте файл формата AbCd_trl.p7s (где «AbCd» - шестнадцатеричный номер вашей сети, например для сети № 6860 это будет файл 1ACC_trl.p7s) и получите информацию по своим исходящим корневым сертификатам и соответствующим им спискам отзыва (CRL).

Обновление межсетевого мастер-ключа (ММК) в версии 3.2 :

- делается в соответствии с документацией по «обновить» при позиционировании на текущем ММК с полученным статусом «Не экспортирован»;
- после передачи в доверенную сеть, в согласованное время с Администратором доверенной сети, старый назначается <Не использовать> или <Удалить>, новый <Ввести в действие>;
- с использованием меню ЦУС <Файлы для создания ключей в УКЦ / Ключей узлов связанных с другими сетями> и указанием номера доверенной сети производится копирование и затем в УКЦ создаются ключи сетевых узлов;
- созданные, после смены ММК, ключи сетевых узлов применяются на абонентских пунктах своей сети.

Обновление межсетевого мастер-ключа (ММК) в версии 4.6 :

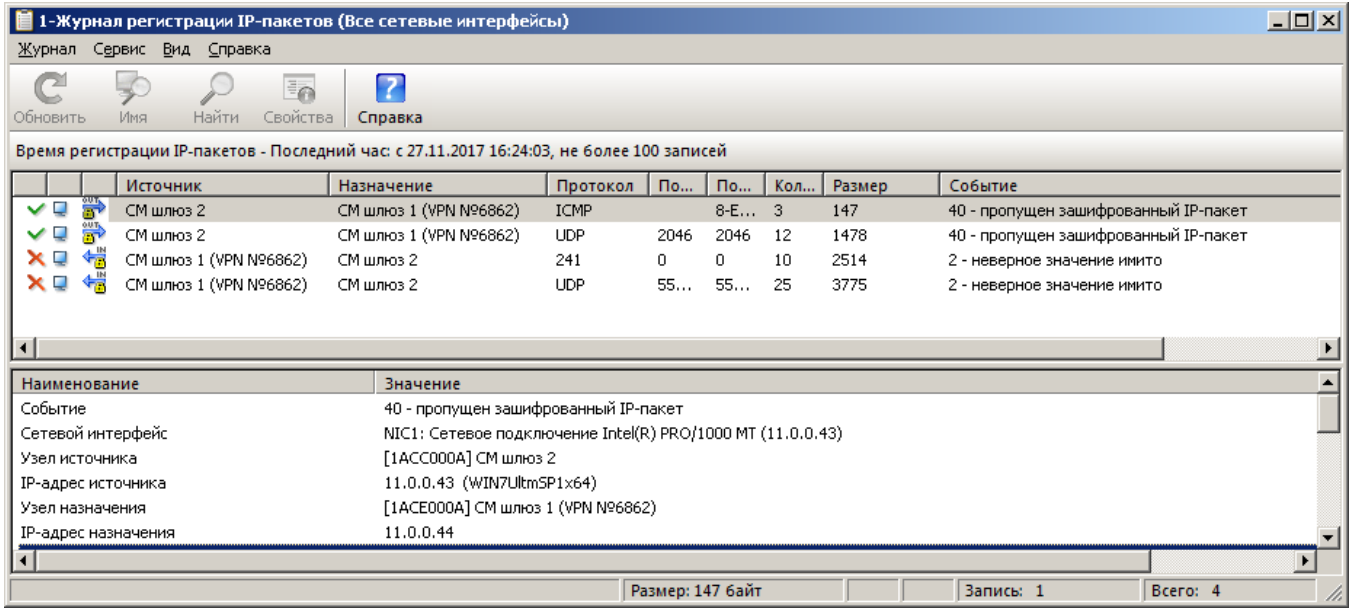
- реализовано проще, в разделе выбранной сети по <Создать> с получением статуса «Не экспортирован»;
- далее экспорт с заданием пароля, передача в доверенную сеть и перед созданием новых ключей узлов назначить текущим (ввести в действие).

Примечание: извлечь только ММК из архива можно восстановлением в виртуальной среде временного содержимого УКЦ с экспортом из него ММК затем уверенно удалить восстановленную архивную копию для предотвращения ее несанкционированного использования, например утилитой «Clean.exe».

Восстановление взаимодействия (ошибочные действия операторов в приложениях ЦУС и УКЦ или аварий):

- если существует актуальный архив в версии 4.6, созданный средствами УКЦ, то восстановившись из него вы получите ранее установленные связи и межсетевые ключи, например если текущие набор данных обнаруживает случайно утраченный ММК;
- в версии 3.2 надо располагать двумя архивами – актуальным архивом ЦУС и сопоставимым архивом УКЦ, эти два архива позволят восстановить утраченные данные межсетевого взаимодействия.

Решение возникающих проблем «событие № 2 неверное значение имито»: / 2 - Message authentication code is incorrect /



Причины возникновения блокировки трафика с этим событием:

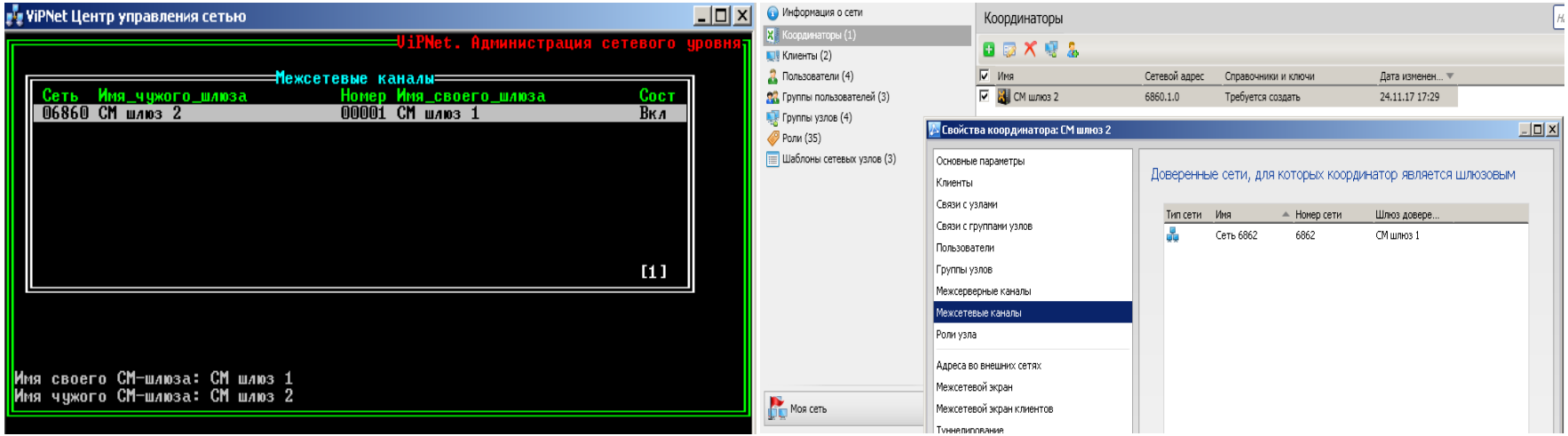
1. В УКЦ сетей разные мастер-ключи, решение - сверить серийные номера и задать статус «Текущий/Действующий» в зависимости от версии «4.6/3.2», если расхождение было определено и устранено, то сформировать и отправить новые обновления ключей сетевых узлов.
2. В одной из сетей сменен вариант сетевого узла, например из-за его компрометации или обновлении персонального ключа абонента, решение – обменяться актуальными наборами экспортов после выполнения в УКЦ экспорта справочников, сформировать и отправить новые обновления ключей сетевых узлов.
3. На координаторах разные версии ПО различающиеся классификацией и на одном из них возможно использование режима шифрования CTR который в версии ПАК HW ниже 3.0 не поддерживается (может сопровождаться регистрацией 7 события), решение – проверить временным заданием режима CFB (iplir set/show cipher-mode); провести обновление версии с 3.0 на более позднюю.

Решение возникающих проблем «нет обмена экспортами по ViPNet сети»:

Исходящая межсетевая информация формируется в ЦУС и передается модулю MFTP для трансляции на узел ЦУС доверенной сети. Описание работы MFTP, как компонента входящего в состав продуктов ViPNet требующих передачи данных, очень подробно излагается в документации на эти продукты:

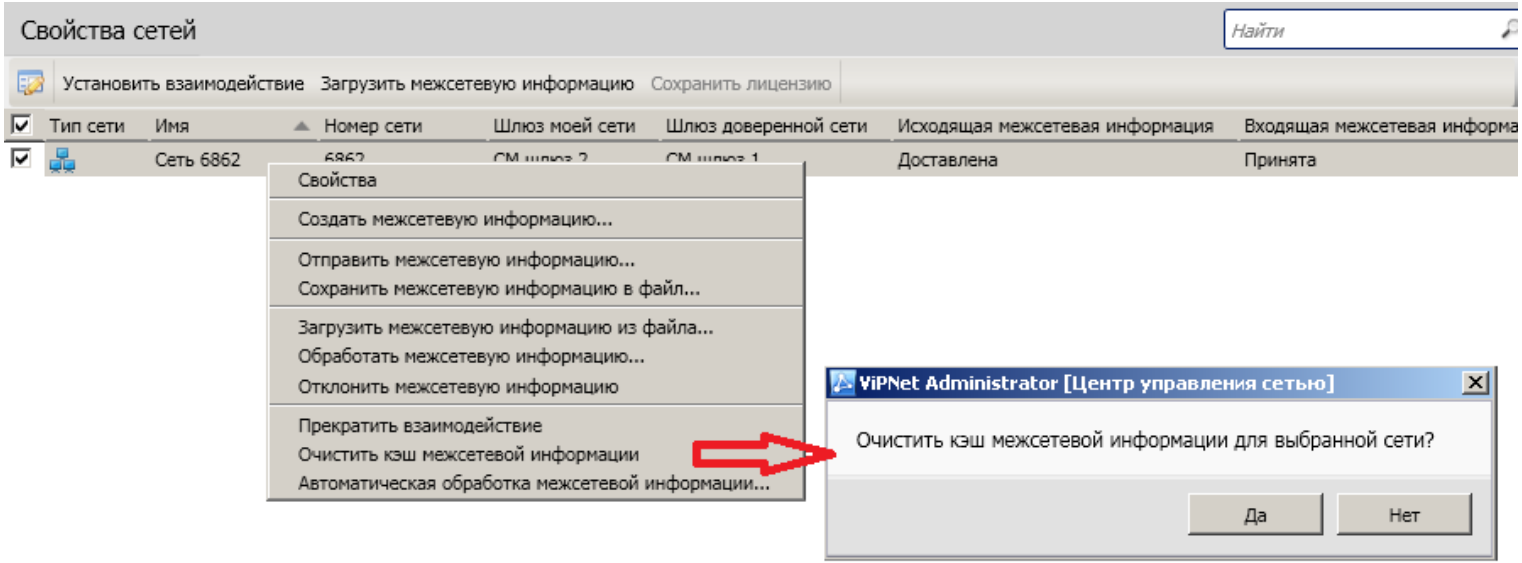
Рисунок 1. Передача конверта через свой координатор

Типовая ошибка при настройке межсетевого взаимодействия заключается в отсутствии образования и включения межсетевых каналов! Каналы должны быть включены и информация об этом в справочниках узлов должна быть сформирована, отправлена и применена на всех узлах передачи данных в доверенную сеть, конечный узел это шлюзовой координатор:



Возникают как следствие того, что перед миграцией данных из версии 3 в 4 администратором сети не произведено устранение аномалий связанных с данными принятыми из доверенных сетей и межсетевые связи регулярно не обновлялись. Устраняется выполнением действий изложенных в разделе документации «Возможные неполадки и способы их устранения» как <… удалите данные о межсетевой информации, загруженной для этой доверенной сети ранее … щелкните доверенную сеть правой кнопкой мыши и в контекстном меню выберите пункт "Очистить кэш межсетевой информации«, снова обработайте поступившую межсетевую информацию>.

Другие проблемы межсетевых связей устраняются удалением информации проблемных узлов/пользователей в обоих сетях из их экспортов с последующим обменом межсетевыми данными не содержащими уже этих проблемных узлов и новым возобновлением связей через их добавление в экспорты с подтверждением связей и рассылкой обновлений ключей узлов этим абонентам.



Из документа «ViPNet Administrator: Руководство по обновлению с версии 3.2.x до версии 4.x»
раздел «Особенности преобразования связей при конвертации»:

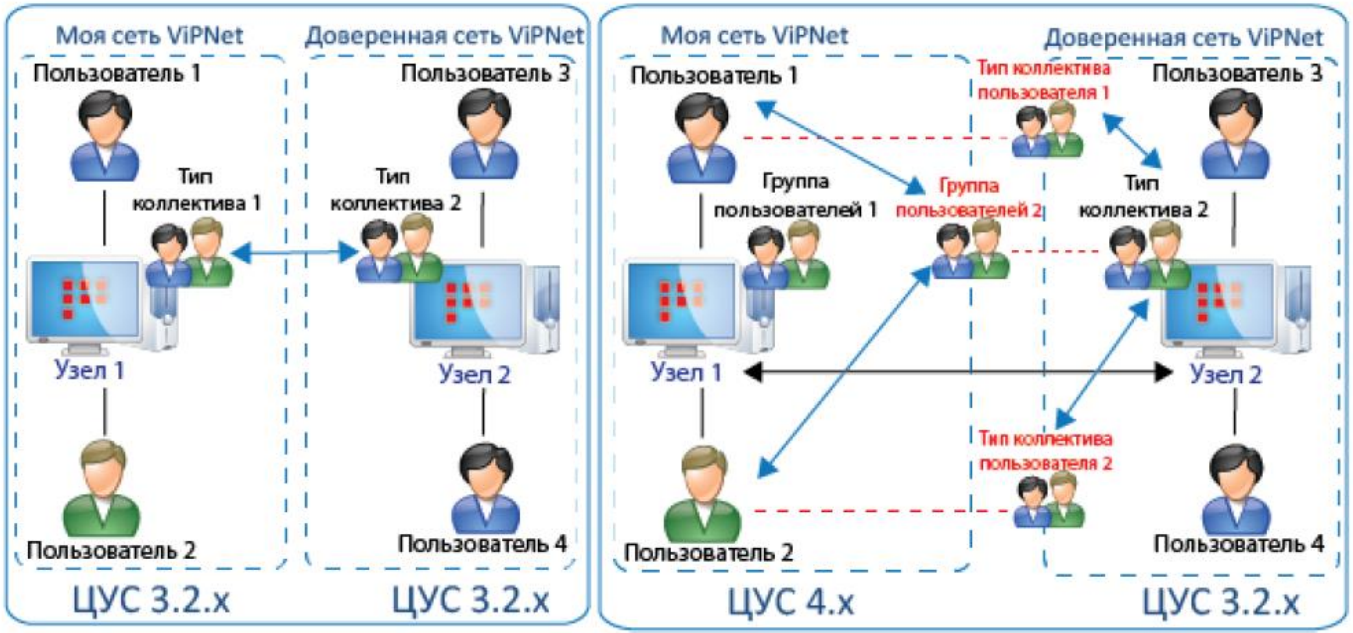
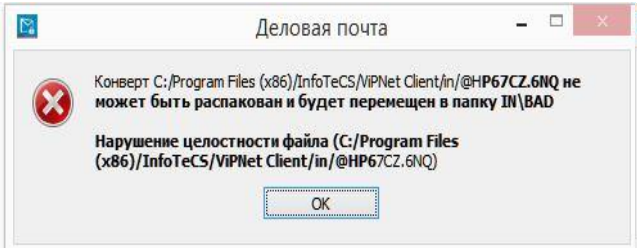
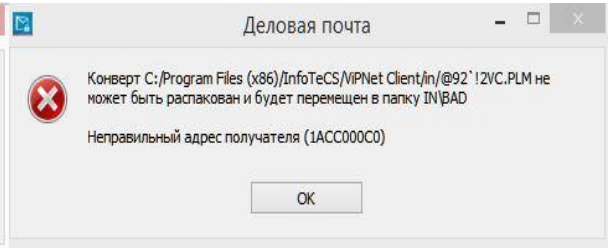
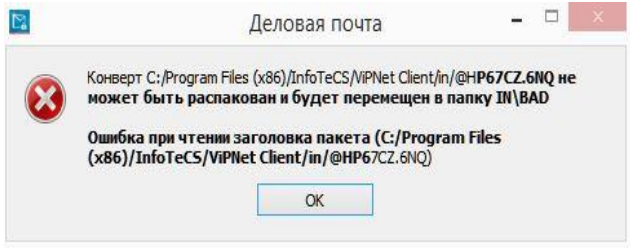


Рисунок 13. Преобразование связей между объектами своей и доверенной сетей

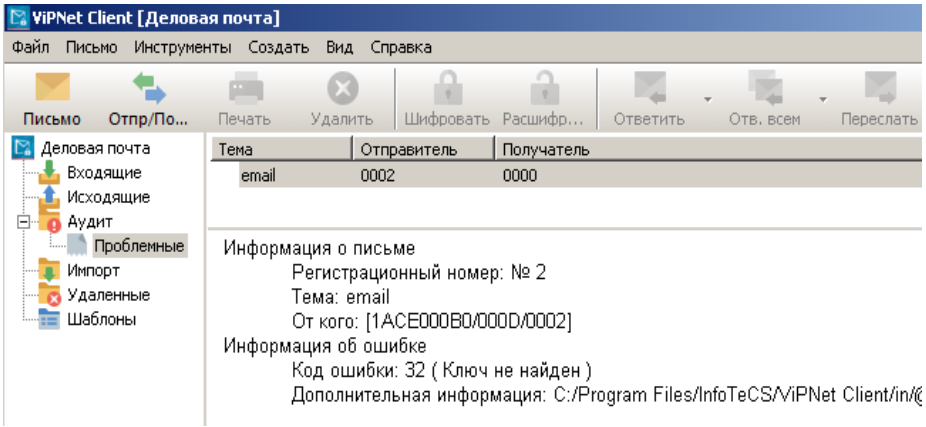
Нарушение приема данных получаемых по каналу MFTP из доверенной сети в основном происходит на узлах абонентов при работе Деловой почты, реже при файловом обмене и совсем редко при приеме управляющих конвертов на узле «ЦУС», проявляется как:

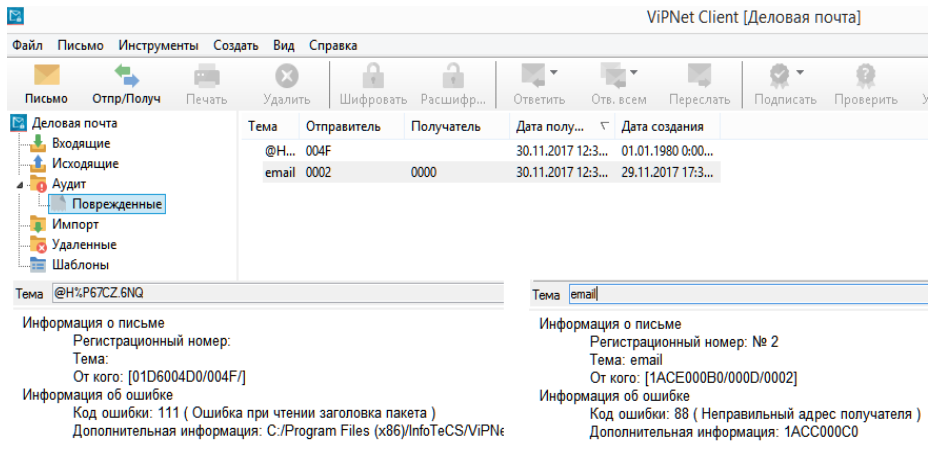






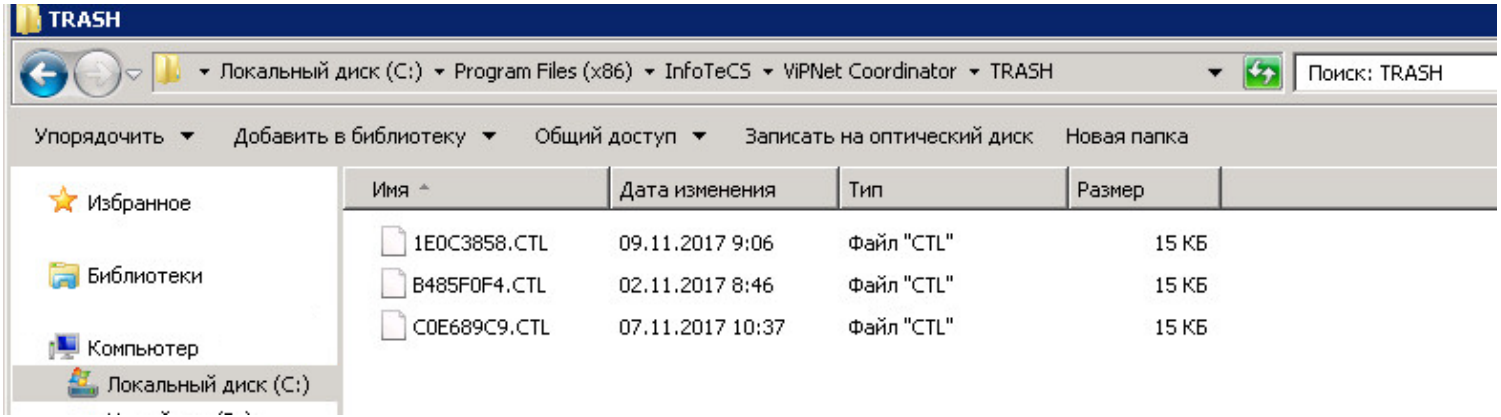
Без отображения сообщения пользователю регистрация этих событий есть здесь:



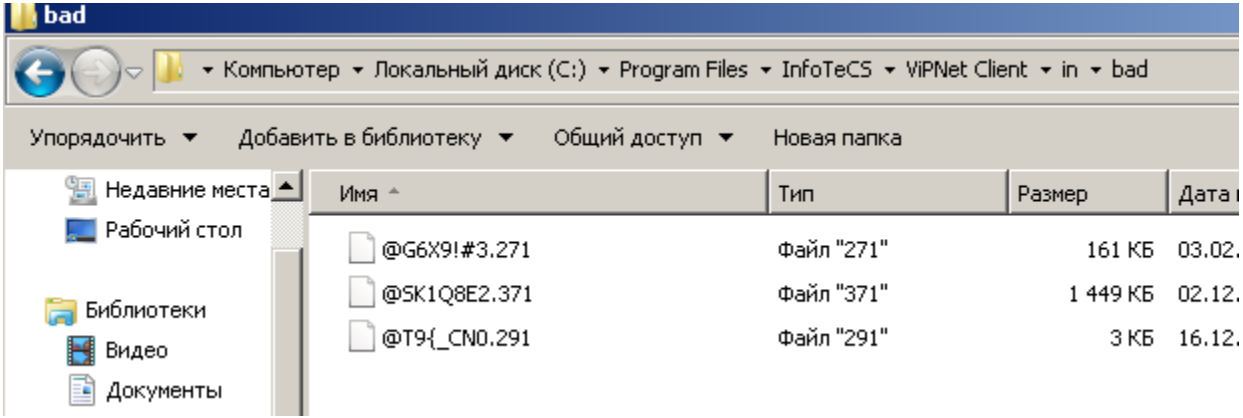


Конверты MFTP от узлов доверенной сети перемещаются сразу в <транспортный каталог>\TRASH
Общие причины:
- для поступившего конверта не определяется получатель на данном узле;
- конверт пришел от узла не являющегося ЦУС или PolicyManager для данного узла;
- конверт зашифрован с помощью одного из не поддерживаемых типов шифрования;
- конверт от PolicyManager содержит некорректную информацию прикладной задачи;
- ключ транспортного уровня на получателе имеет другой вариант, неизвестный отправителю;
- не выполнилась успешно проверка имитозащиты внутренних данных.

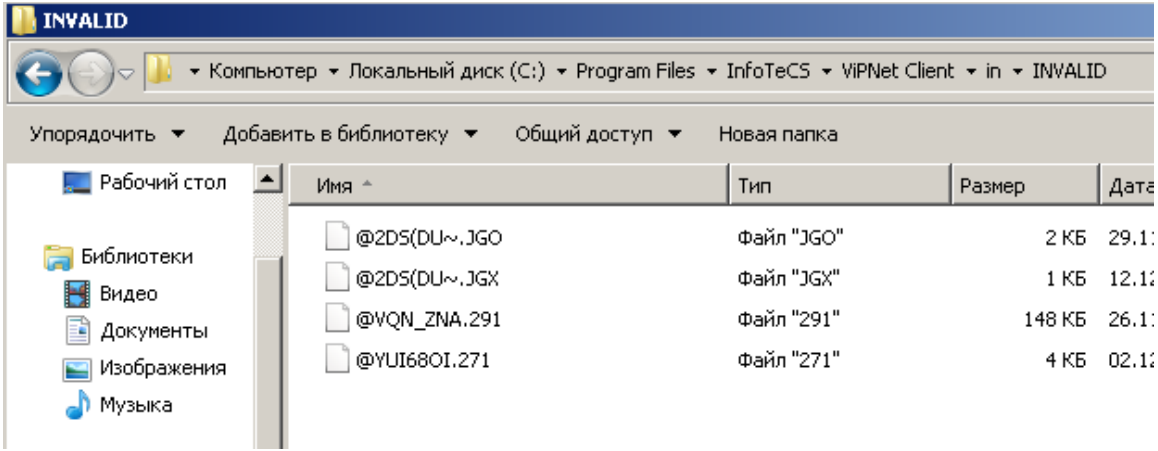
Примечание: каталог TRASH служит еще и для временного хранения устаревших исходящих конвертов и очищается в соответствии с настройками (90 дней).



Конверт MFTP получен и транслирован для дальнейшей обработки приложениями ViPNet в каталог ..\IN, но:
Деловая почта перемещает его в <транспортный каталог>\IN\BAD
Общие причины:
- неправильно определился отправитель внутренним функционалом почты, одного из идентификаторов отправителя нет в текущих справочниках;
- целостность конверта не может быть гарантирована из-за его нарушения при передаче на узлах посредниках (в редких случаях для полученного конверта нет соответствующего алгоритма расшифрования, например если он упакован на старой версии ПО ViPNet 2.8 или 3.0);
- определение непредусмотренных приложением ошибок таких как "access violation", "divide by zero" уровня операционной системы.



Конверт MFTP получен и транслирован для дальнейшей обработки приложениями ViPNet в каталог ..\IN, но:
Деловая почта перемещает его в <транспортный каталог>\IN\INVALID
Общие причины:
- алгоритм шифрования отправителя не соответствуют имеющимся у получателя;
- ключи шифрования отправителя не соответствуют ключам получателя;
- ключи расшифрования письма рассогласованны со справочниками связей узла.
Примечание:
1. Конверты перемещенные в INVALID могут быть повторно обработаны Деловой почтой если их переместить в корень каталога <транспортный каталог>\IN или перезапустить Деловую почту / сменить пользователя Деловой почты.
2. Конверты при обработке которых произошли ошибки ввода-вывода и доступа (недостаток ОЗУ, блокировка антивирусом и т.д.), считаются временно необработанными и остаются в каталоге ..\IN они будут повторно идентифицированы на возможность приема.




infotecs
Благодарим за внимание!
Готовы ответить на вопросы ...