Обновление мастер-ключей сети ViPNet

Обновление мастер-ключей сети ViPNet

Основные темы:

- Подготовка к смене мастер-ключей
- Смена мастер-ключей
- Обновление ключей на узлах после смены мастер-ключей
- Возможные неполадки и способы их устранения
- Ответы на вопросы

Выбор технологического окна для проведения обновления мастер-ключей

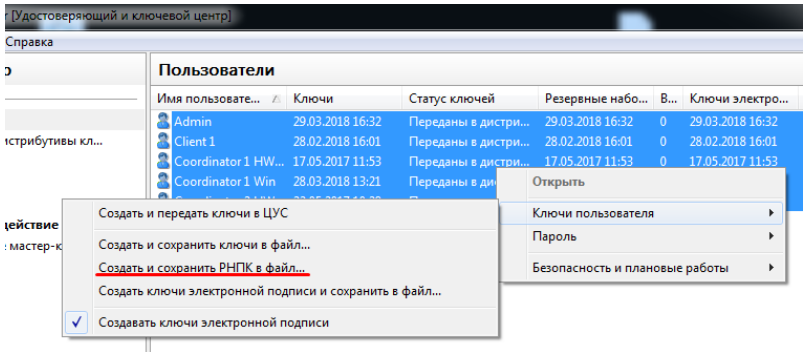
- Промежуток времени выбирается исходя из масштабов ViPNet сети. (Рекомендуется 5-10 дней)
- В выбранный период не рекомендуется обрабатывать межсетевую информацию, изменять структуру сети, менять способ аутентификации пользователям сетевых узлов, рассылать обновления CRL

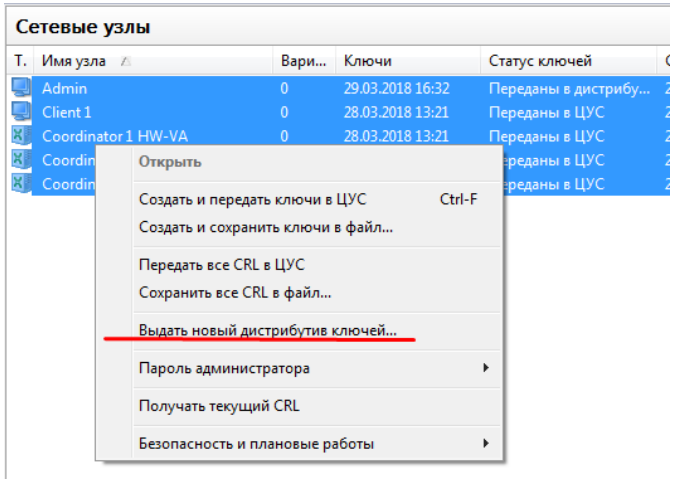
Оповещение пользователей и администраторов ViPNet сети

При оповещении рекомендуется сразу запросить у пользователей следующую информацию:

- Изменялся ли назначенный ранее пользовательский пароль
- Используется ли ЭЦП ViPNet во внешних приложениях
- Используется ли внешнее устройство аутентификации ViPNet
- Информацию о часовых поясах пользователей (при наличии территориально-удаленных регионов). Если в ОС установлено некорректное время, следует скорректировать его заранее.

Копирование РНПК и дистрибутивов ключей из УКЦ

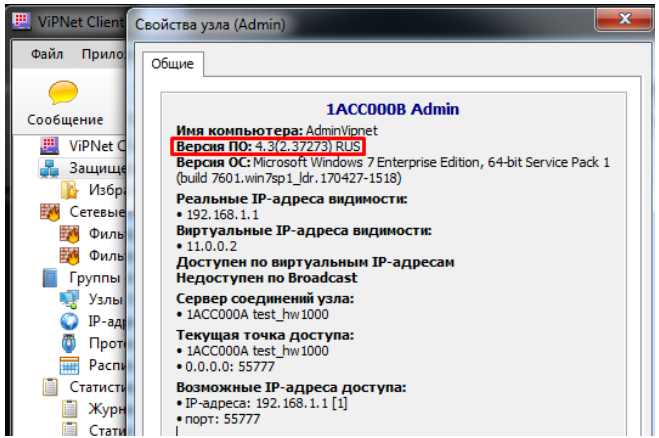


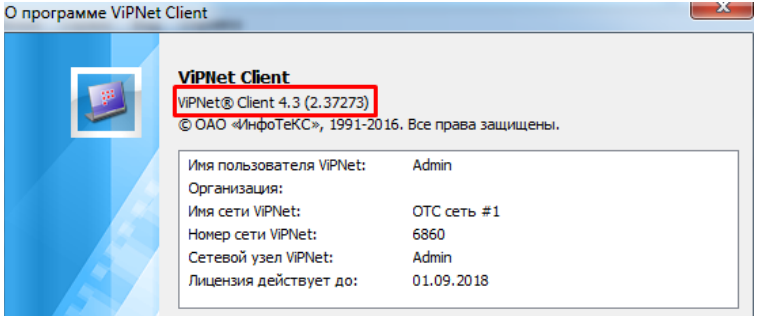


- При сохранении дистрибутивов ключей в целевом каталоге допустимо сохранить пароль для каждого пользователя. Передачу следует осуществлять доверенным способом, исключающим утечку данных
- После завершения процедуры смены мастер-ключей неактуальные дистрибутивы, РНПК и файлы паролей пользователей следует надежно удалить.

Подготовка узлов с ПО ViPNet Client

Обновление ПО до минимально-необходимой версии.

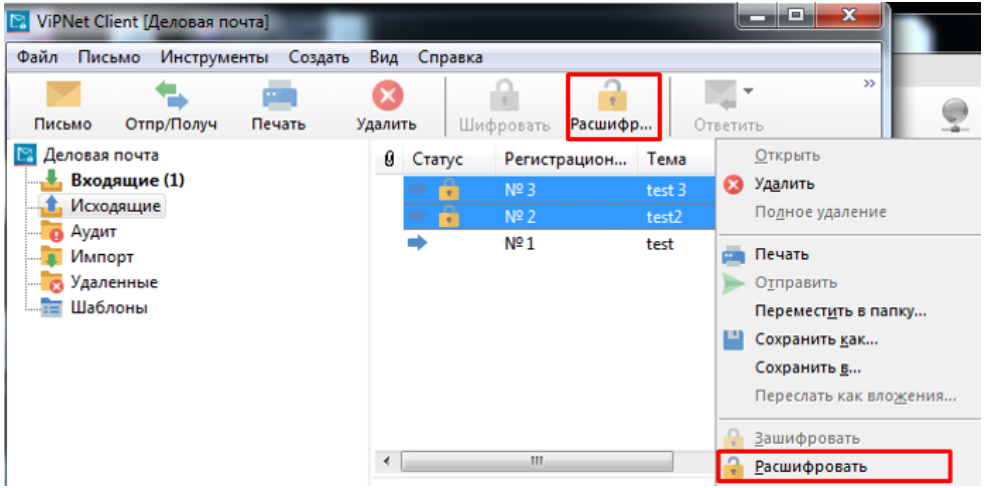




- Проверку можно выполнить с узла администратора средствами ПО ViPNet Client
- Пользователь самостоятельно может проверить версию установленного ПО в разделе «Справка» -> «О программе»
- ПО промежуточных версий рекомендуется обновить до актуальной или сертифицированной 4.3

Расшифровка писем в ПО ViPNet «Деловая почта»

- Зашифрованные письма помечены индикатором замка. Расшифрованные не имеют данной индикации. Подробная информация по расшифровке описана в документе «ViPNet Деловая почта. Руководство пользователя»
- Расшифровка писем требуется не только для текущего хранилища, но и для всех архивных каталогов
- При большом количестве писем расшифровка может занимать продолжительное время



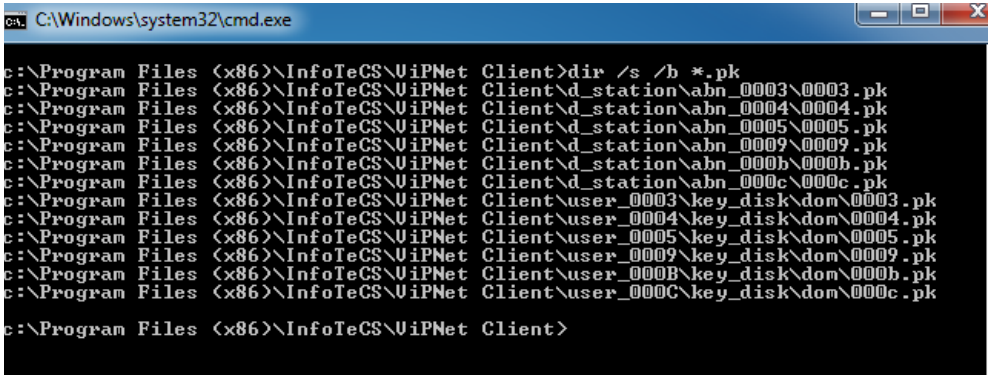
Проверка наличия РНПК (ОС Windows)

- Так как версионность ПО клиентов может сильно отличаться, файл РНПК следует располагать в двух каталогах:

  \Program Files*\InfoTeCS\ViPNet Client\d_station\abn_AAAA\

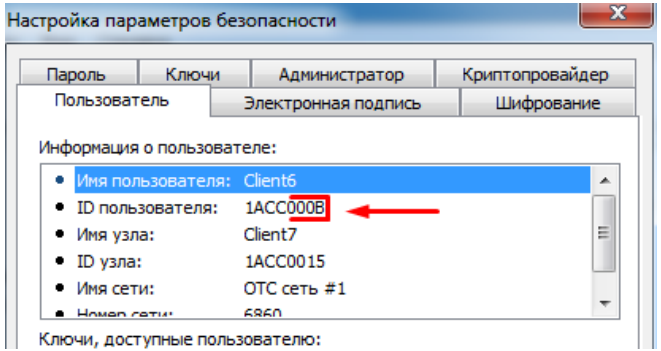
  \Program Files*\InfoTeCS\ViPNet Client\user_AAAA\key_disk\dom\

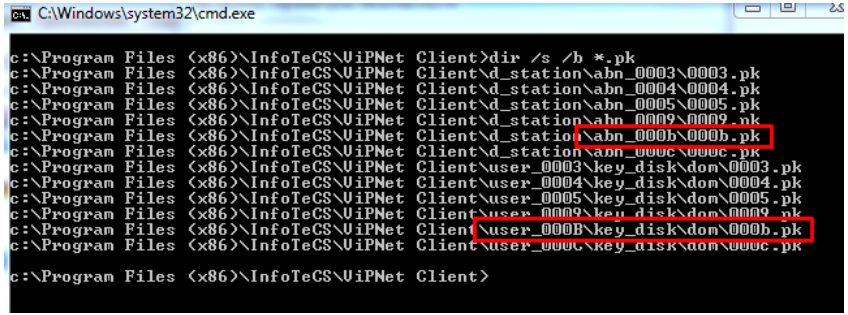
- Если на узле зарегистрировано несколько пользователей, РНПК каждого из них должен присутствовать в указанных каталогах.



Проверка соответствия РНПК пользователю

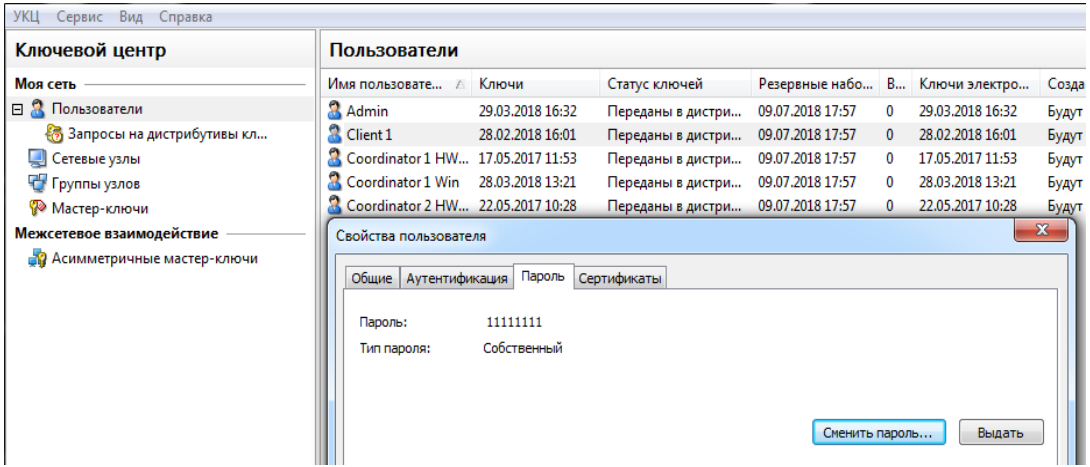
- Имя файла РНПК (*.pk) должно соответствовать номеру пользователя.
- Чтобы просмотреть номер пользователя в программе ViPNet Монитор, порекомендуйте пользователю или администратору сетевого узла в программе ViPNet Монитор в меню «Сервис» выбрать пункт «Настройка параметров безопасности» и в открывшемся окне на вкладке «Пользователь» в строке «ID пользователя» просмотреть значение идентификатора.
- Значение идентификатора вида NNNNAAAA состоит из восьми 16- разрядных чисел, где <NNNN> — номер сети ViPNet, <AAAA> — номер пользователя в сети ViPNet. Именно вторая часть идентификатора сверяется с именем файла РНПК





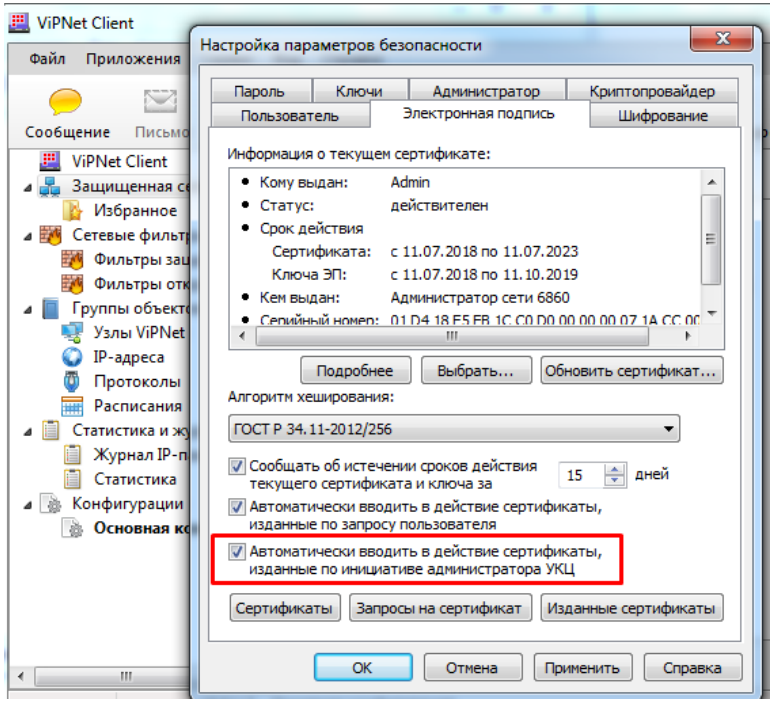
Проверка соответствия пароля пользователя в УКЦ

- Если пользователь не помнит свой пароль, выданный УКЦ (настроен автоматический вход), следует сообщить ему актуальную парольную информацию
- Если пользователь ранее самостоятельно менял пароль средствами ПО ViPNet Client, сообщите ему действующий пароль из УКЦ



Использование ЭЦП ViPNet во внешних приложениях

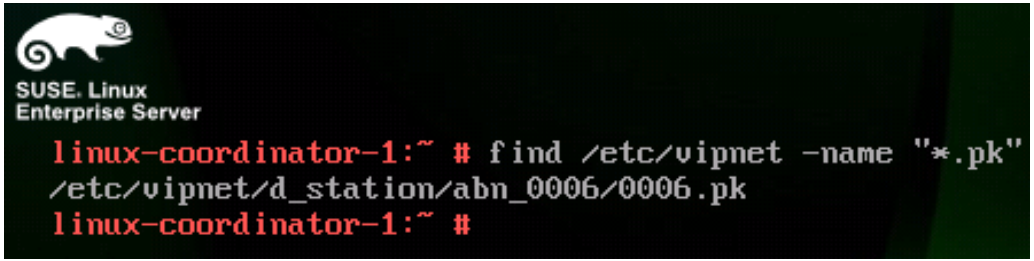
- При обновлении мастер-ключей сертификаты всех пользователей будут перевыпущены.
- Рекомендуется установить флаг «Автоматически вводить в действие сертификаты, изданные по инициативе администратора УКЦ».



Подготовка ViPNet Client/Coordinator Linux

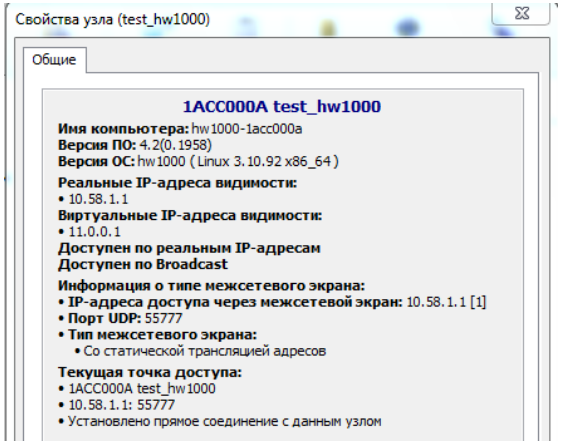
- Необходимо обновить ПО до версии 4.1.4 или выше
- Проверить версию установленного ПО можно средствами команды failover info
- РНПК размещается в каталоге /etc/vipnet/d_station/abn_AAAA

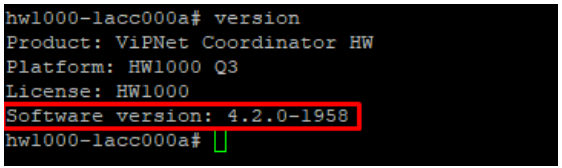
```
linux-coordinator-1:~ # failover info
Running failover info
Versions: ViPNet 4.1.4 (10954), daemon 1.5 (1)
Workstation configured for ID 1ACC000F (Coordinator Linux)
The workstation works in a single mode of protection against failures
Workstation time (utc: 1532094529) Fri Jul 20 17:48:49 2018
```



Обновление ПО ПАК HW

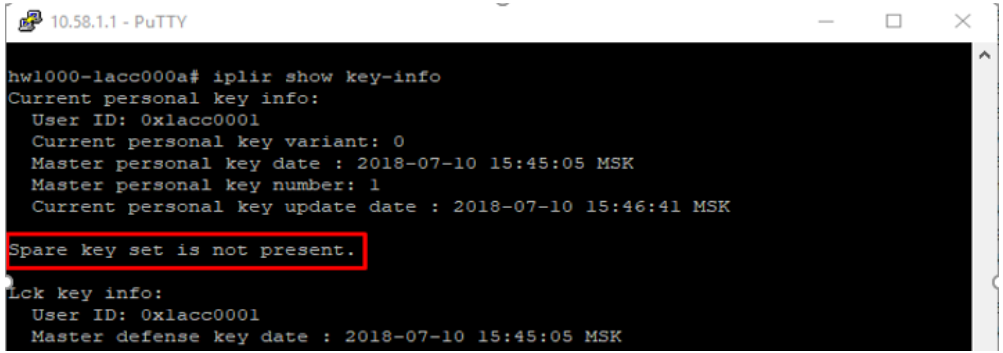
- Для корректного обновления ключей при смене мастер-ключей на ViPNet Coordinator HW должно быть установлено ПО версии не ниже 4.2.0
- Проверку установленной версии ПО можно выполнить непосредственно в консоли ПАК средствами команды «version», или с узла администратора.
- Обновление ключей для более ранних версий ПО, или ПАК HW, работающих в кластере горячего резервирования, следует производить развертыванием актуального дистрибутива ключей.

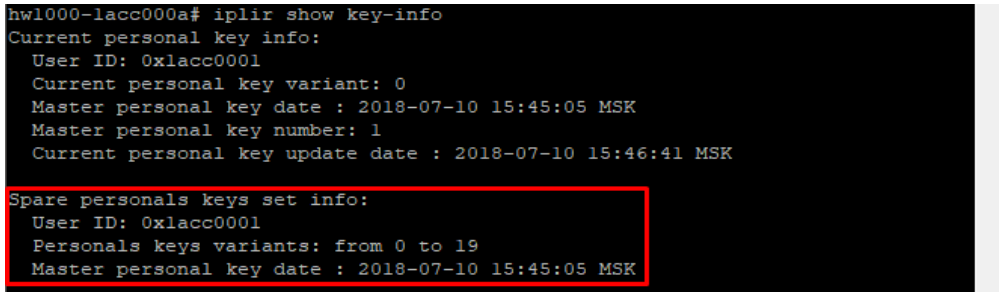




ПАК HW. Проверка наличия РНПК

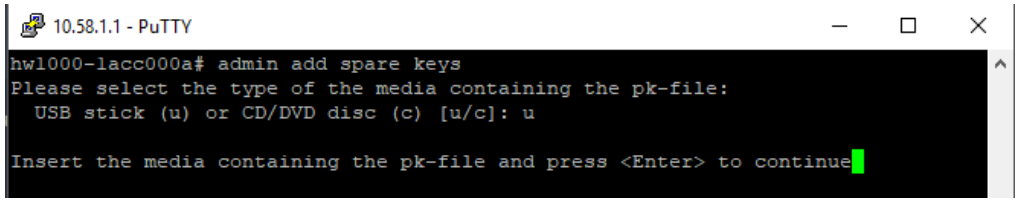
- Проверка выполняется средствами консоли при помощи команды **iplir show key-info**
- В случае отсутствия РНПК на ПАК, в выводе будет присутствовать строка **Spare key set is not present.**

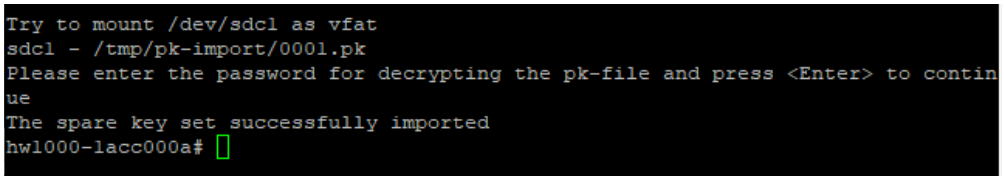




ПАК HW. Импорт РНПК

- Ранее сформированный РНПК следует записать на USB носитель.
- Импорт РНПК на ПАК HW производится при помощи команды **admin add spare keys**
- После приглашения консоли следует вставить подготовленный USB носитель и нажать «Enter»
- Монтирование носителя и поиск *.pk файла происходит автоматически.
- После ввода пароля пользователя РНПК будет установлен, о чем свидетельствует сообщение в консоли «**The spare key set successfully imported**»





ПАК HW. Создание резервной копии конфигурации (VBE)

- Остановите работу модулей iplir, mftp при помощи команд **iplir stop** и **mftp stop**
- Запустите процедуру создания резервной копии при помощи команды **admin export keys binary-encrypted usb**
- Подключите подготовленный ранее USB-носитель и нажмите «Enter»
- При наличии нескольких носителей, укажите порядковый номер требуемого из списка
- Дождитесь сообщение консоли «**You may remove the USB drive**» и извлеките носитель с готовым VBE
- Запустите модули iplir, mftp при помощи команд **iplir start** и **mftp start**

```
hw1000-1acc000a# iplir stop
Shutting down IpLir
hw1000-1acc000a# mftp stop
Shutting down MFTP daemon
hw1000-1acc000a# admin export keys binary-encrypted usb
Configuration file will be saved to /tmp/vipnet/hw1000-1acc000a-2018-07-12.vbe
Put hw1000-1acc000a-2018-07-12.vbe file onto USB drive.
Insert USB drive and press Enter
```

```
1) Generic Flash Disk partition 7680Mb
Select target partition [1-1] or 0 to abort: 1
Try to mount /dev/sdc1 as vfat
Partition /dev/sdc1 was successfully mounted on /usb.
File hw1000-1acc000a-2018-07-12.vbe to be copied onto the USB drive.
File hw1000-1acc000a-2018-07-12.vbe was successfully copied onto the USB drive.
You may remove the USB drive.
hw1000-1acc000a#
```

Подготовка узлов с ПО ViPNet

- Процедура подготовки РМ с ViPNet CryptoService и ViPNet «Деловая почта» аналогична ViPNet Client 4.x
- Пользователям, использующим ПО ViPNet SafeDisk-V следует рекомендовать создать резервную копию ключей контейнера данных, для возможности восстановления доступа к ранее зашифрованным данным

ViPNet «Деловая почта»

ViPNet SafeDisk-V

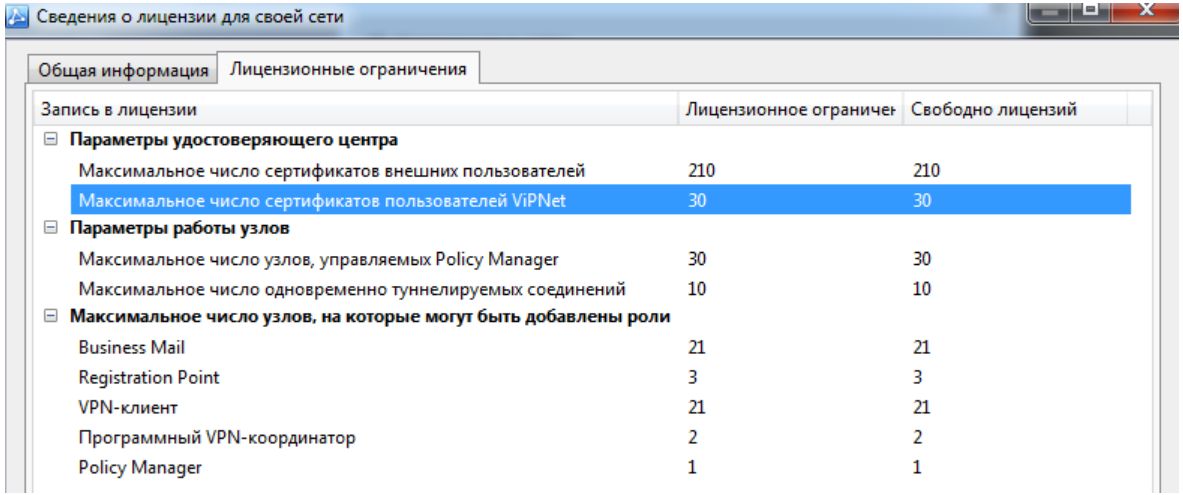
ViPNet CryptoService

Подготовка ПО ViPNet Client на мобильных устройствах

ViPNet Client Mobile

- На мобильные клиенты рекомендуется отправить актуальные версии ПО, известные на момент подготовки к обновлению мастер-ключей
- Проверку наличия РНПК на данных устройствах выполнить невозможно

Актуализация лицензии *.itcslic/*.reg



- Следует заранее обеспечить достаточное количество лицензий на максимальное число сертификатов пользователей ViPNet, обратившись в ОАО «ИнфоТеКС» для обновления лицензии на сеть ViPNet, заполнив форму на сайте: https://infotecs.ru/personal-offer/

Реализация резервного защищенного канала на примере использования программного координатора Windows.

Условия для реализации

- Для реализации потребуется одна свободная лицензия «Программный VPN координатор»
- Временный технологический координатор должен быть доступен напрямую из публичной сети Интернет и иметь проверенные связи со всеми пользовательскими узлами до начала обновления мастер-ключей
- Внутренний интерфейс координатора должен быть напрямую доступен с узла администратора ViPNet сети
- На технологический координатор не отправляются обновления ключей после смены мастер-ключей
- Минимально-необходимая версия ПО ViPNet Coordinator – 3.2.x
- ОС из списка поддерживаемых, согласно эксплуатационной документации к устанавливаемой версии ПО ViPNet Coordinator

Использование

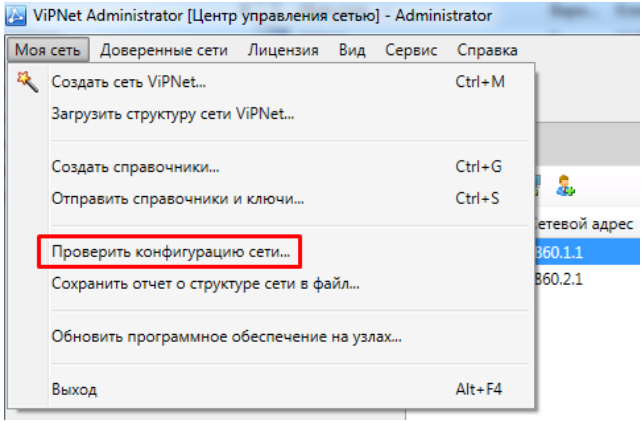
- Передача актуальных дистрибутивов ключей после смены мастер-ключей средствами компонента «Файловый обмен»
- Возможность удаленного доступа к пользовательским узлам, на которых обновление ключевой информации по каким-либо причинам не было выполнено.

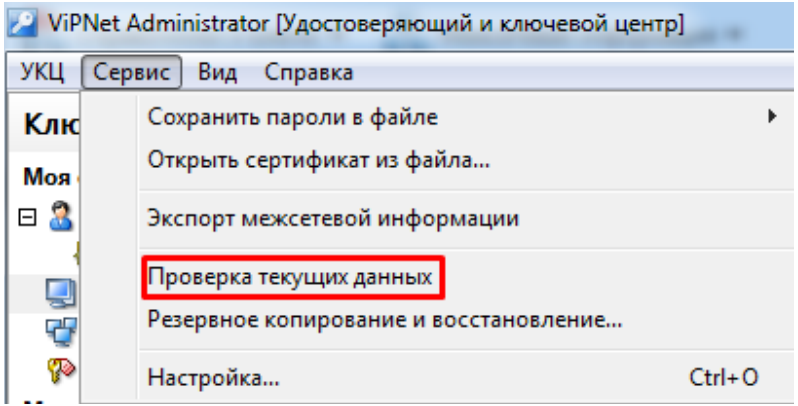
Подготовка ЦУС и УКЦ

ViPNet Administrator

- Временно остановите поступление данных из приложений ViPNet Publication Service, ViPNet Registration Point, ViPNet CA Web Service
- Находящиеся в стадии импорта или удовлетворения запросов данные должны быть обработаны
- Следует обработать всю межсетевую информацию, поступившую на момент начала смены мастер-ключей
- Ожидающая отправки справочная и ключевая информация должна быть отправлена на узлы

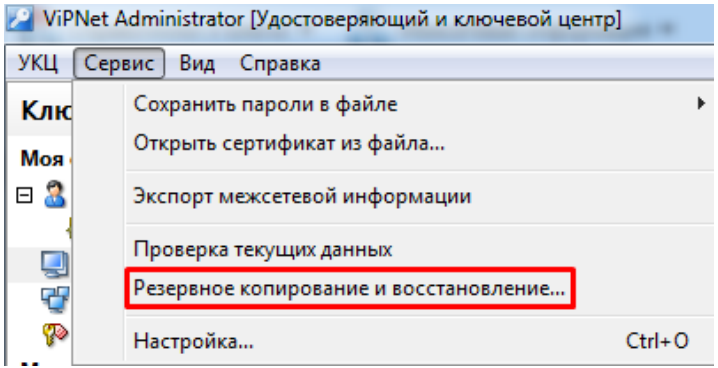
Проверка конфигурации ЦУС и УКЦ

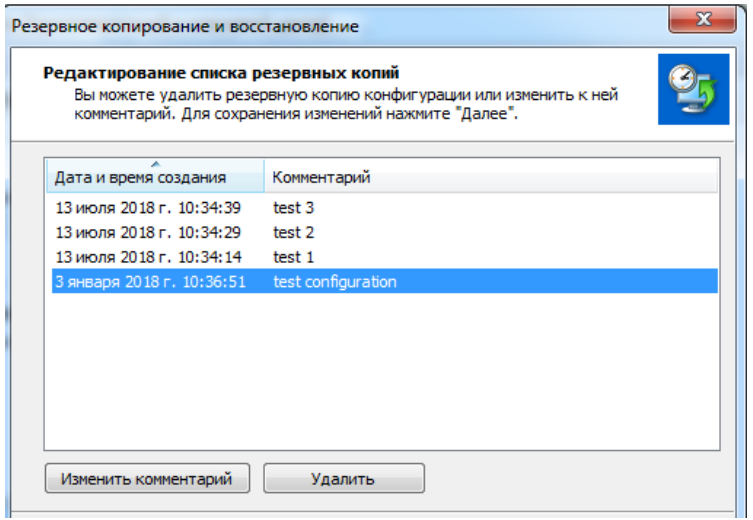




- При положительном результате проверки конфигурации сети ЦУС отображает сообщение «Конфликтных или неполных данных не обнаружено»
- При положительном результате проверки текущих данных УКЦ отображает сообщение «Ошибок в ходе проверки текущих данных не обнаружено»
- Аномалии, выявленные при проверке конфигурации рекомендуется устранить перед процедурой обновления мастер-ключей

Удаление неактуальных резервных копий УКЦ





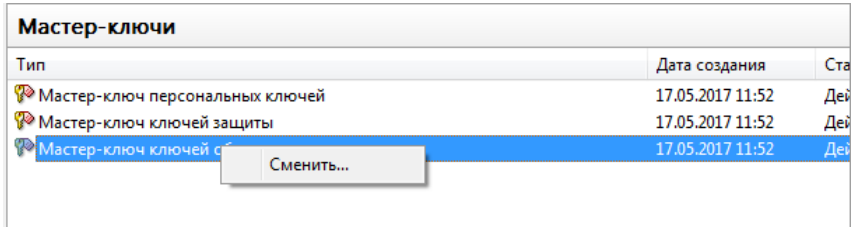
- Рекомендуется удалить неактуальные резервные копии УКЦ, в частности, созданные в ранних версиях ПО ViPNet Administrator

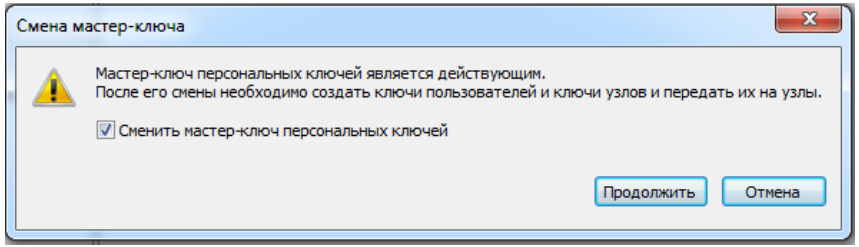
Создание полной резервной копии набора данных ViPNet Administrator

- Процедура создания полной резервной копии набора данных описана в разделе «**Подготовка данных для миграции ПО ViPNet Administrator**» документа «**ViPNet Administrator 4 Руководство по миграции ПО**»
- В состав полной резервной копии входят:
  - резервная копия конфигурации сети (файл *.rp или *.zip)
  - копия архива, содержащего список всех резервных копий, созданных при эксплуатации сети (файл rpts_50.stg, расположен в каталоге **C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore**
  - копия лицензионного файла (infotecs.reg или *.itcslic)
  - копия каталога с контейнерами ключей администратора УКЦ: **C:\Users\<имя учетной записи локального администратора Windows, от лица которого была произведена установка УКЦ>\AppData\Roaming\Infotecs\ViPNet Administrator**
  - Список учетных записей администраторов ЦУС и УКЦ, с помощью которых осуществляется аутентификация в указанных программах, и пароли к каждой из них.
  - Справочники и ключи для восстановления работоспособности ПО ViPNet Client.

Смена мастер-ключей в УКЦ

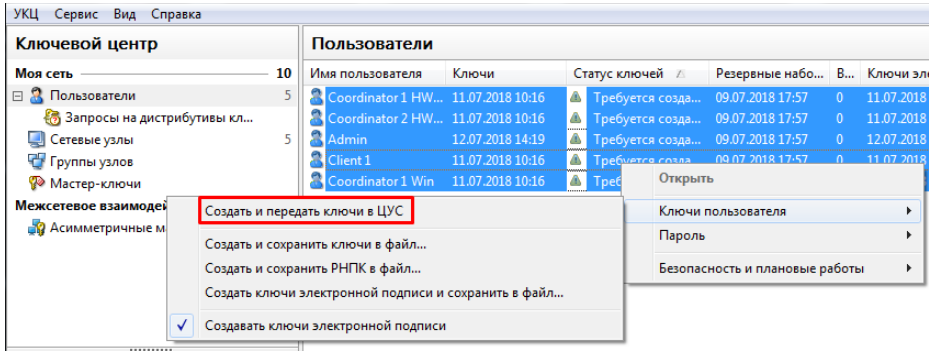
- Порядок обновления мастер-ключей в УКЦ аналогичен для 3.x и 4.x
- Последовательно сменяются все три мастер-ключа:
  - мастер-ключ персональных ключей
  - мастер-ключ ключей защиты
  - мастер-ключ ключей обмена

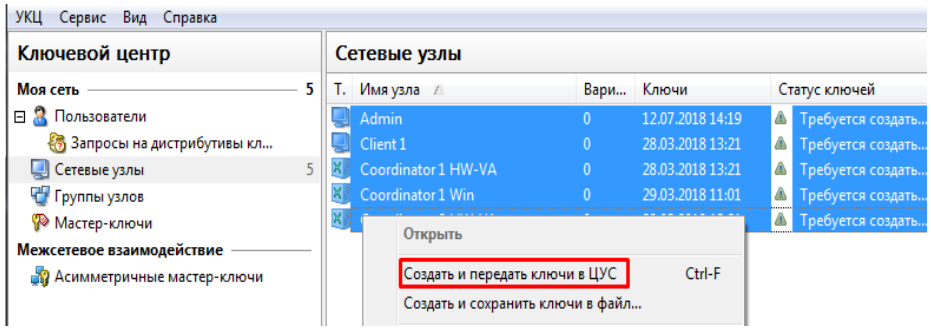




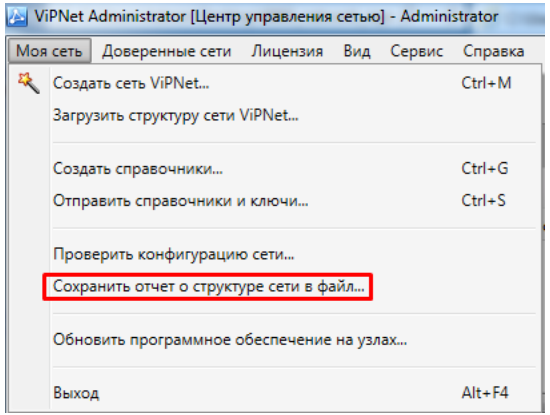
Создание обновлений ключей пользователей и узлов

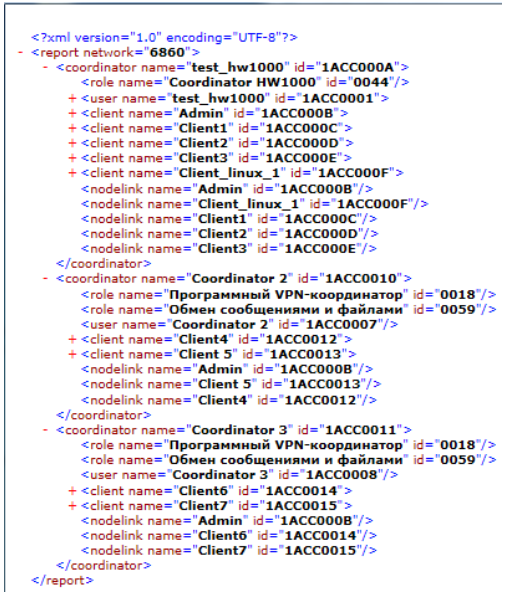
- Процедура создания обновлений ключей имеет строгую последовательность как для 4.x, так и для 3.x:
  1. Создание ключей пользователей, передача в ЦУС
  2. Создание ключей узлов, передача в ЦУС

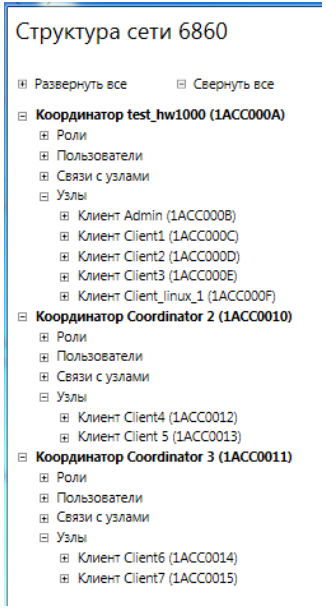




Экспорт отчета о структуре сети в файл



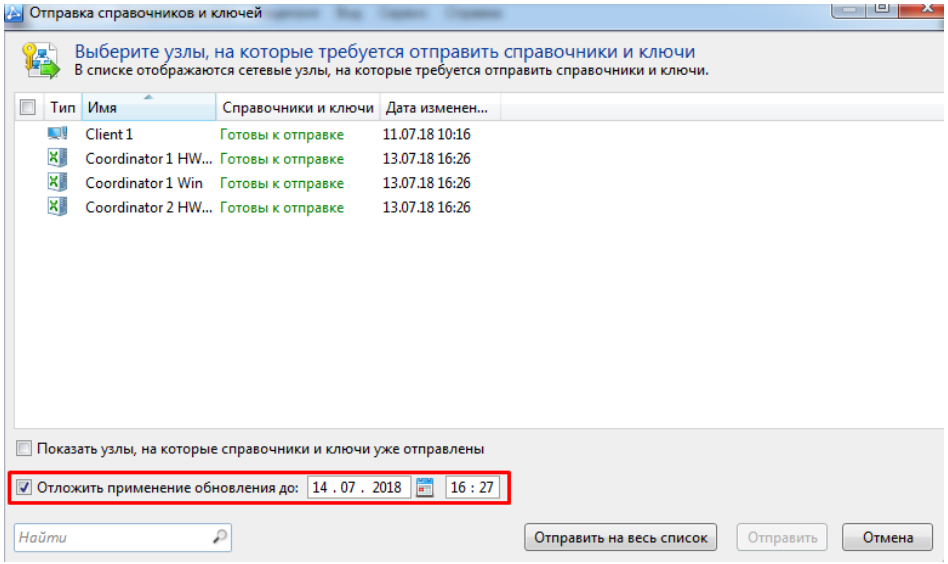




- Рекомендуется сохранить отчет о структуре сети для удобства выбора узлов при планировании рассылки отложенных обновлений и просмотра информации, за каким координатором они расположены.
- Присутствует возможность сохранения структуры в XML и HTML формате.

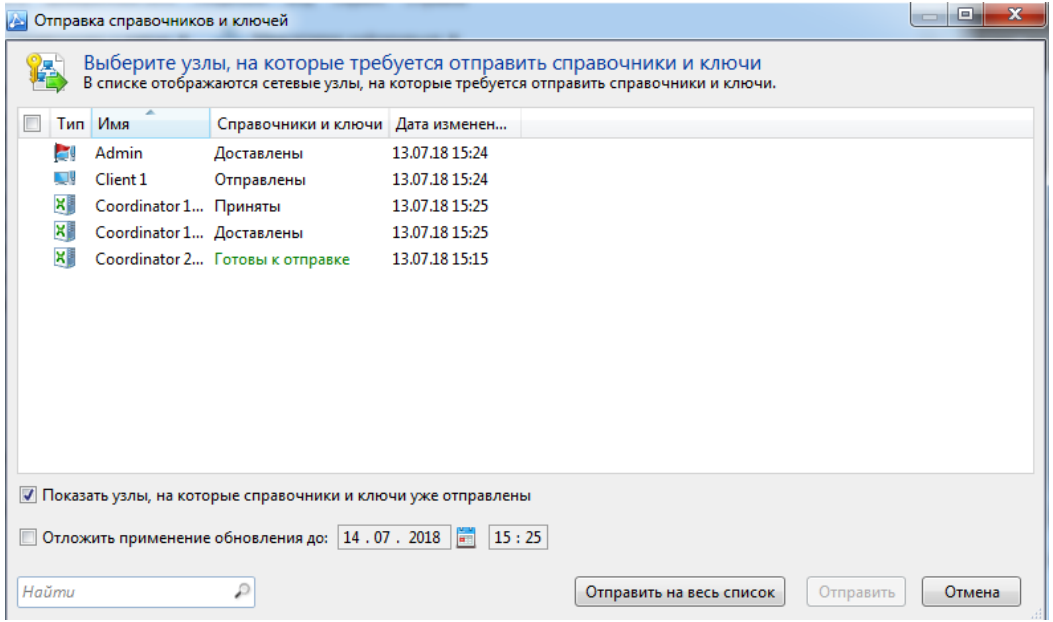
Рассылка обновлений из ЦУС

- Рассылка обновлений на узлы производится с отложенным временем применения.
- Применение обновлений на оконечных узлах должно производиться раньше координаторов, за которыми зарегистрированы данные узлы
- До окончания передачи конвертов из ЦУС в очередь MFTP не следует производить формирование дистрибутивов ключей в УКЦ

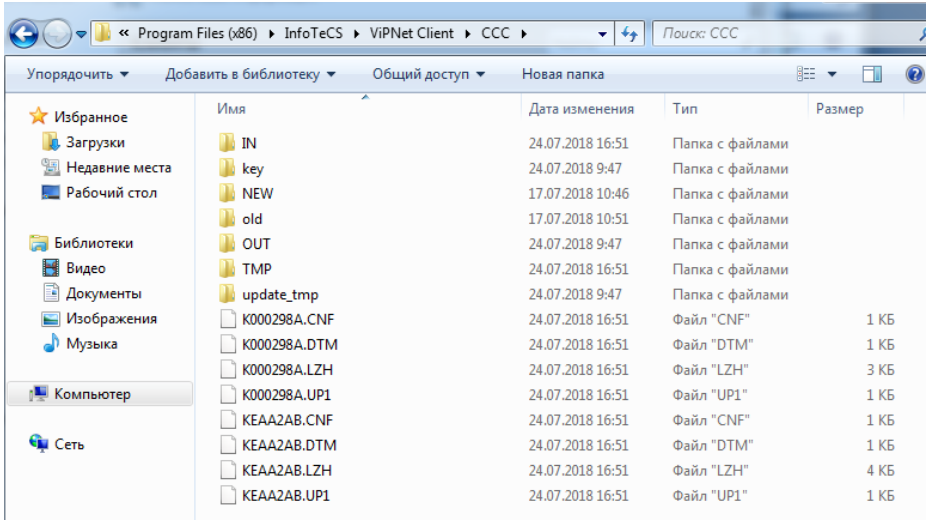


Контроль доставки конвертов из ЦУС

- Статус **Отправлены** указывает, что справочники и ключи отправлены на сетевой узел
- Статус **Доставлены** указывает, что отправленные справочники и ключи были доставлены на сетевой узел
- Статус **Приняты** указывает, что справочники и ключи на сетевом узле были успешно обновлены. Если обновление не удалось, появится статус **Не приняты**

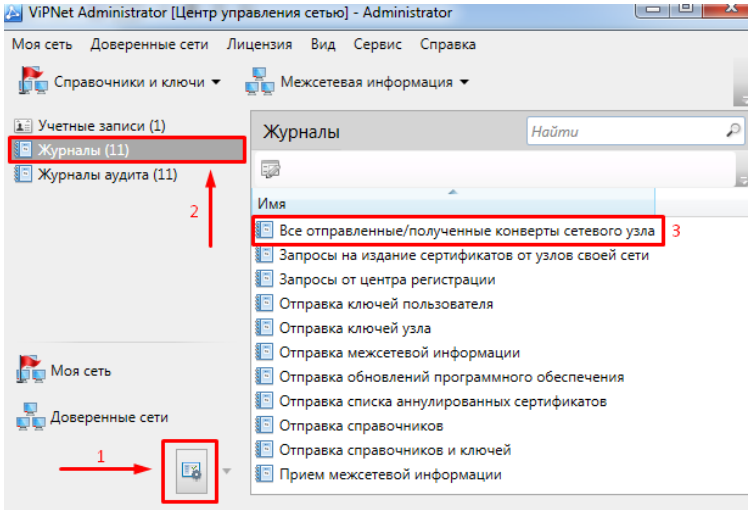


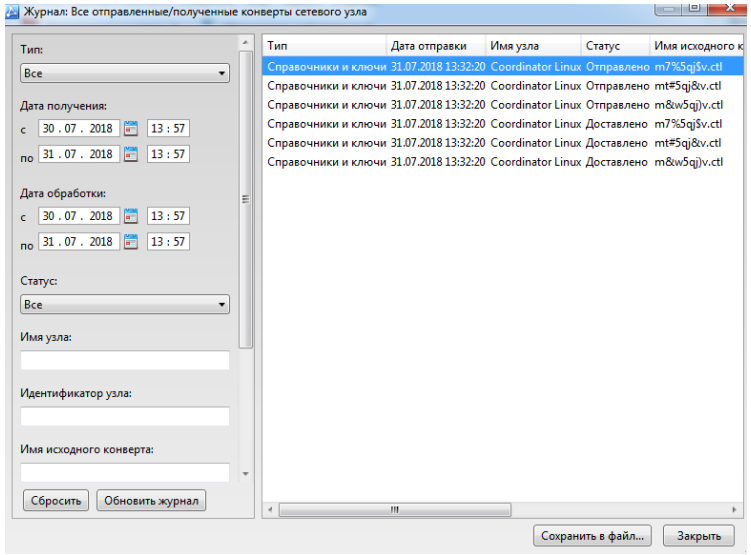
Контроль доставки конвертов из ЦУС



На узлах с ПО ViPNet Client и Coordinator Windows/Linux, обновления помещаются в подкаталог /CCC, расположенный в корневом каталоге установки ПО (*.cnf, *.dtm, *.lzh, *.up1). Здесь они будут находиться до наступления даты применения, заданного в ЦУС. По содержимому каталога и датам создания файлов можно убедиться, что отложенные обновления доставлены на узел.

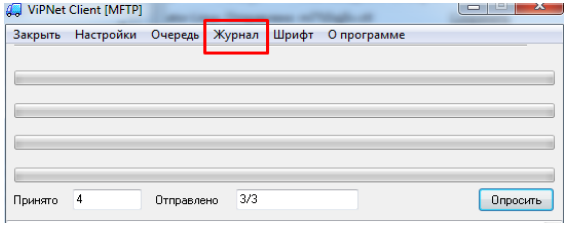
Контроль доставки конвертов из ЦУС

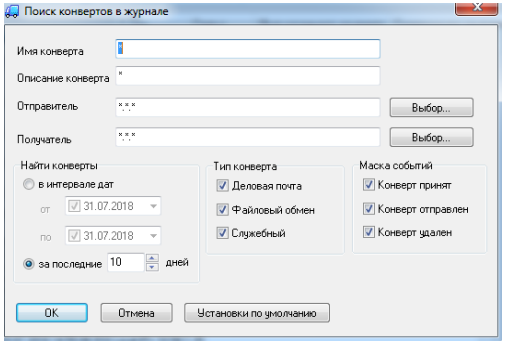


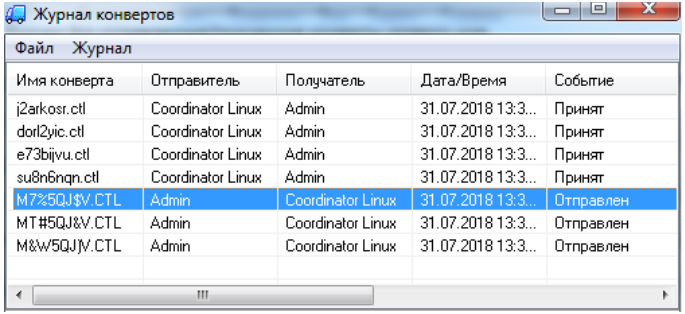


- Если в течение длительного времени после рассылки обновлений, на узле отсутствуют файлы, следует отследить маршрут доставки конверта.
- Имя исходного конверта можно посмотреть в ЦУС. Для этого следует перейти в раздел «Администрирование» -> «Журналы» -> «Все отправленные/полученные конверты сетевого узла». Далее задайте требуемые фильтры и нажмите «Обновить журнал». В списке найдите конверт с обновлениями, направленными на узел и зафиксируйте имя конверта, из столбца «Имя исходного конверта»

Контроль доставки конвертов из ЦУС



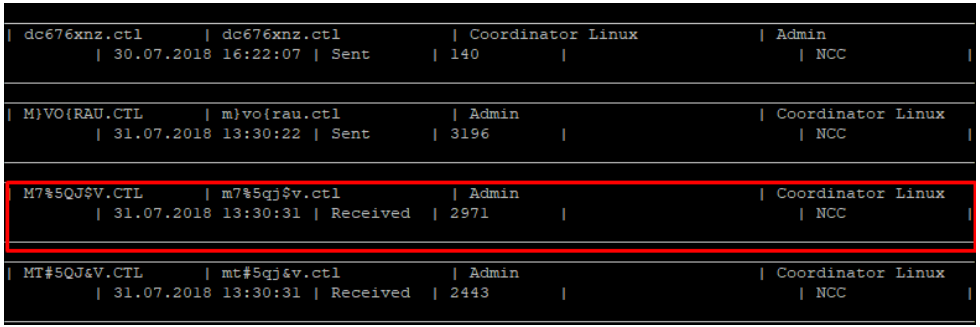


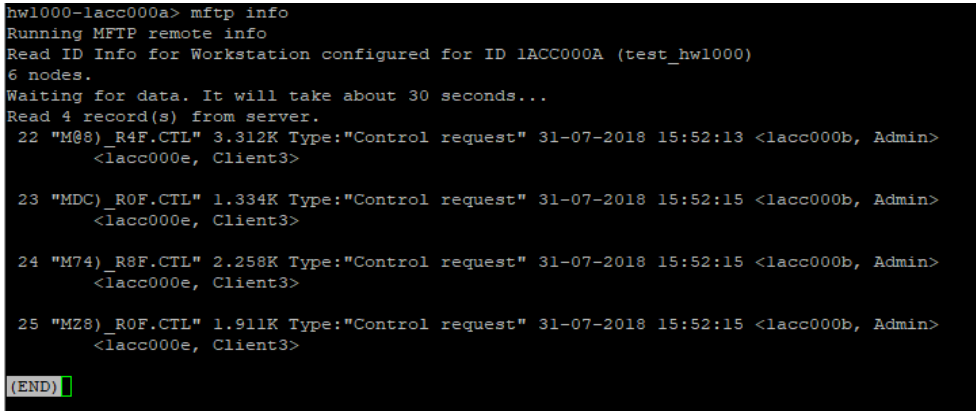


- Для просмотра журнала конвертов следует открыть интерфейс транспортного модуля и выбрать пункт меню «Журнал». Далее при необходимости задайте значения фильтров и нажмите OK.
- Отобразится информация о всех конвертах и их статусах согласно предустановленным фильтрам

Контроль доставки конвертов из ЦУС

- На программно-аппаратных комплексах HW просмотреть журнал MFTP конвертов в консоли можно при помощи команды **mftp view**
- Если конверт находится в очереди, просмотреть данную информацию можно при помощи команды **mftp info**





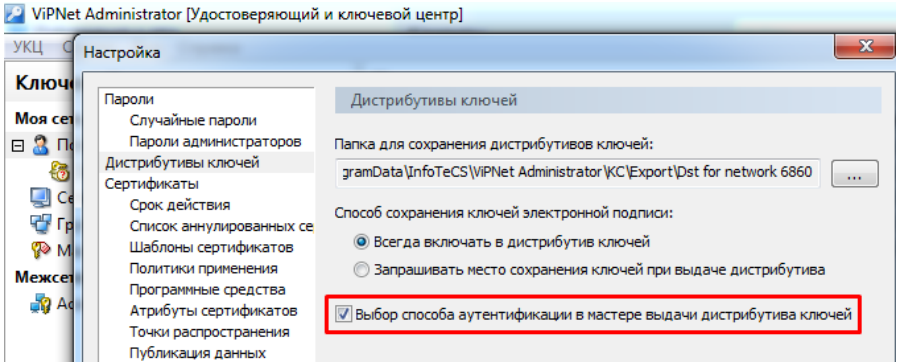
Формирование актуальных дистрибутивов ключей

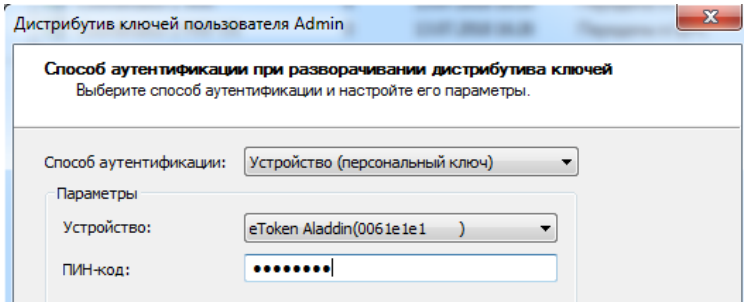
- В случае возникновения проблем после применения обновлений, сформируйте актуальные дистрибутивы ключей
- Не следует формировать ключевые дистрибутивы до завершения помещения отправленных обновлений в очередь MFTP
- Дистрибутивы следует вручную развернуть на узлах, где по каким-либо причинам обновление не прошло
- Актуальные дистрибутивы также потребуются для обновления ключей на ViPNet Terminal и устаревших версиях ПО ViPNet, где обновление ключевой информации технически невозможно.
- Передачу дистрибутивов можно осуществить по резервному защищенному каналу, с использованием технологического координатора, работающего на старых мастер-ключах
- Определить, связаны ли проблемы соединения с узлом из за неприменившихся обновлений на одном из них можно средствами журнала IP-пакетов. Пакеты от узла, работающего на старых ключах, будут заблокированы с событием №2 – «Неверное значение имито» («Events: 2 - Message authentication code is incorrect» для ПАК HW)

Использование внешних устройств аутентификации на узлах

Для узлов, использующих внешние устройства аутентификации потребуется обновить персональный ключ:

- Перед формированием дистрибутива ключей следует убедиться, что в параметрах УКЦ установлен флаг «Выбор способа аутентификации в мастере выдачи дистрибутива ключей»
- В процессе создания нового дистрибутива ключей следует заменить персональный ключ на внешнем устройстве
- В случае нехватки свободного места на устройстве допустимо произвести его полную инициализацию средствами драйвера производителя





Завершение процедуры обновления мастер-ключей

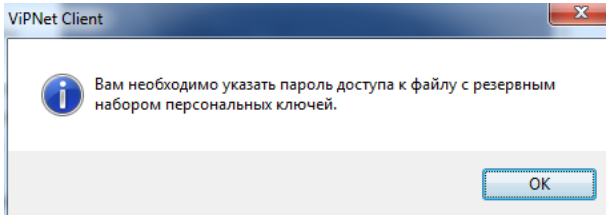
- Удаление неактуальных дистрибутивов ключей
- Удаление неактуальных РНПК
- Удаление неактуальных резервных копий УКЦ
- Удаление неактуальных резервных копий VBE координаторов HW
- Вывод из эксплуатации резервного технологического координатора
- При необходимости, сформируйте и отправьте межсетевую информацию в доверенные сети

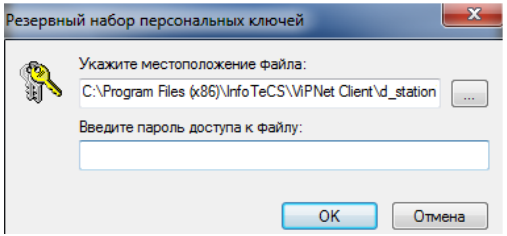
Возможные неполадки и способы их устранения

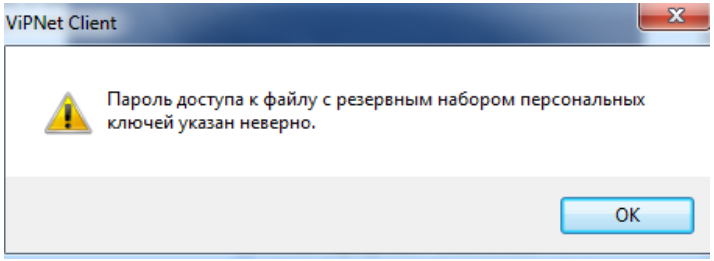
После применения обновлений ПО ViPNet Client запрашивается пароль от РНПК. Пользовательский пароль не принимается

Проблема возникает, если пользовательский пароль ранее был изменен в настройках параметров безопасности ПО ViPNet Client непосредственно самим пользователем.

Следует сообщить пользователю старый пароль из УКЦ доверенным способом.







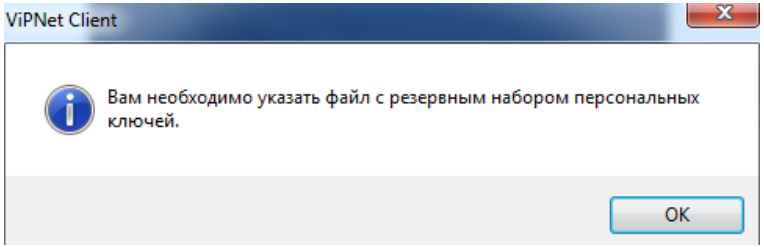
Возможные неполадки и способы их устранения

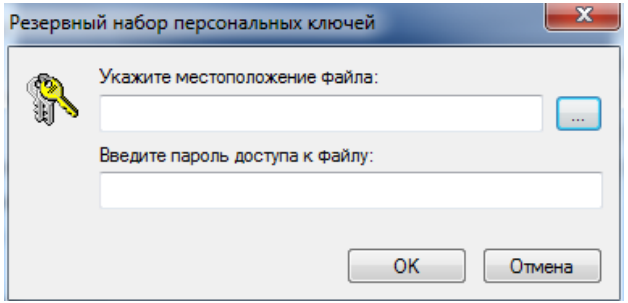
Запрошен путь к местоположению файла резервного набора персональных ключей

Проблема возникает, если *.pk-файл не был размещен в требуемых каталогах перед применением обновлений.

Следует передать пользователю РНПК, ранее выгруженный из УКЦ до смены мастер-ключей.

Также, допустимо развернуть актуальный дистрибутив ключей





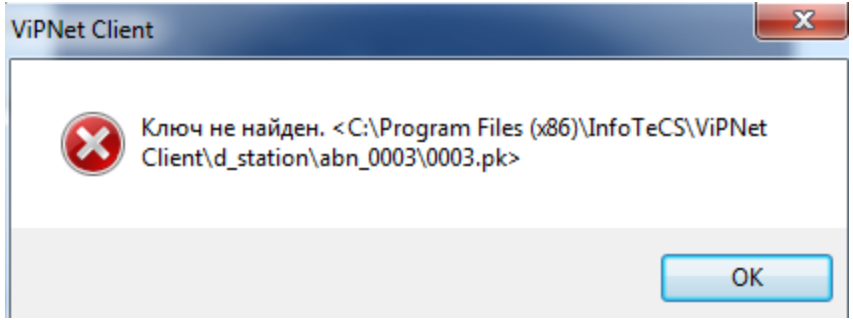
Возможные неполадки и способы их устранения

При указании пути к РНПК и вводе пароля, возникает ошибка «Ключ не найден»

Проблема наблюдается в двух случаях:

1. РНПК не соответствует пользователю, зарегистрированному на данном узле

2. РНПК выгружен из УКЦ после смены мастер-ключей. Данный файл не будет принят при применении обновлений.



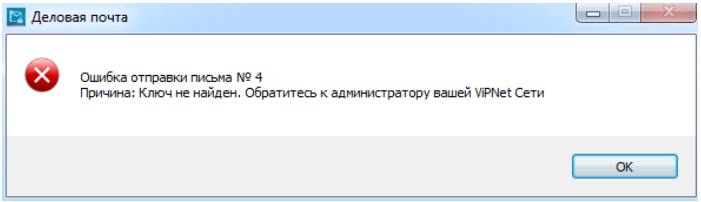
Следует передать пользователю корректный РНПК, либо актуальный дистрибутив ключей.

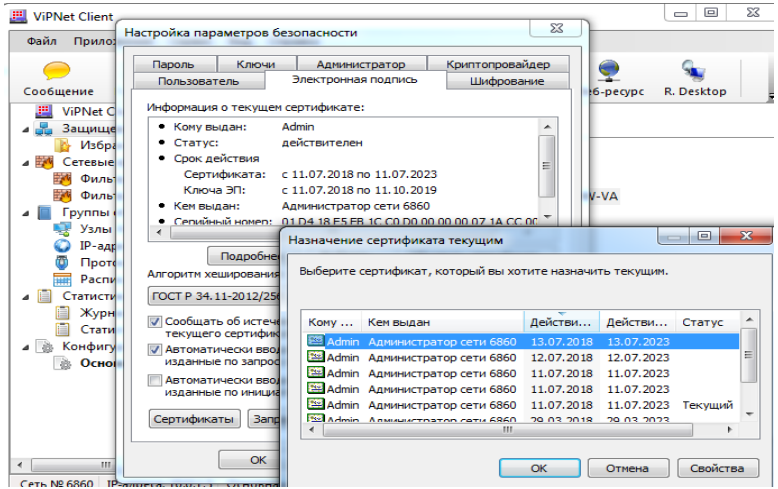
Возможные неполадки и способы их устранения

При попытке отправки писем в деловой почте возникает ошибка «Ключ не найден»

Проблема возникает, если при обновлении ключей не был введен в действие новый сертификат.

Для решения проблемы следует назначить текущим актуальный сертификат в параметрах электронной подписи ПО ViPNet Client





Возможные неполадки и способы их устранения

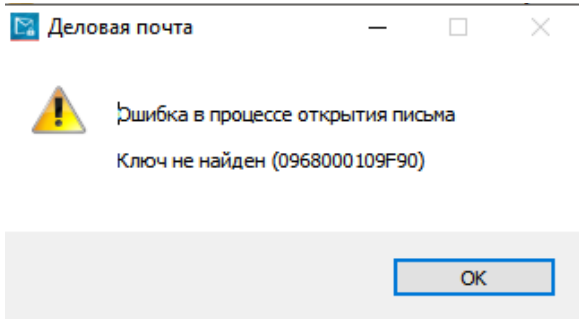
При попытке открытия ранее полученных писем возникает ошибка «Ключ не найден». Новые сообщения открываются корректно.

Пользователь не расшифровал письма в своих рабочих хранилищах. Т.к. обновления ключей применены – доступ к информации, зашифрованной на старых ключах, утерян.

Для решения проблемы следует передать пользователю два дистрибутива ключей, созданные до и после смены мастер-ключей.

Последовательность:

1. Установка DST, созданного до смены мастер-ключей
2. Расшифровка хранилищ деловой почты
3. Установка актуального DST
4. Шифрование имеющихся хранилищ деловой почты на новых ключах



Спасибо за внимание

hotline@infotecs.ru