

Особенности эксплуатации компонентов ViPNet Администратор 4.x

Отдел технического сопровождения ИнфоТеКС сентябрь 2017 года

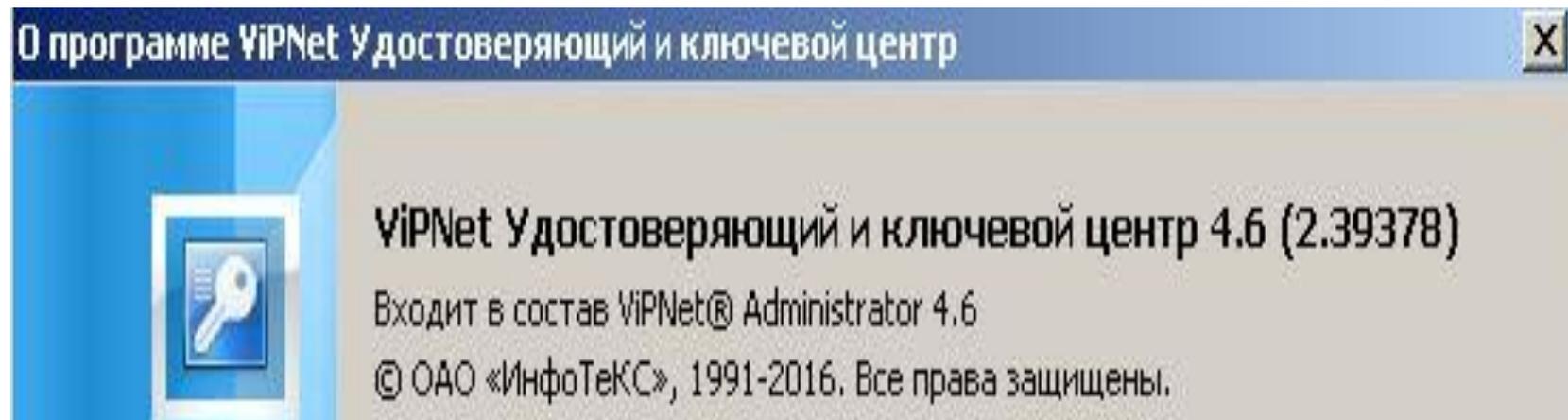
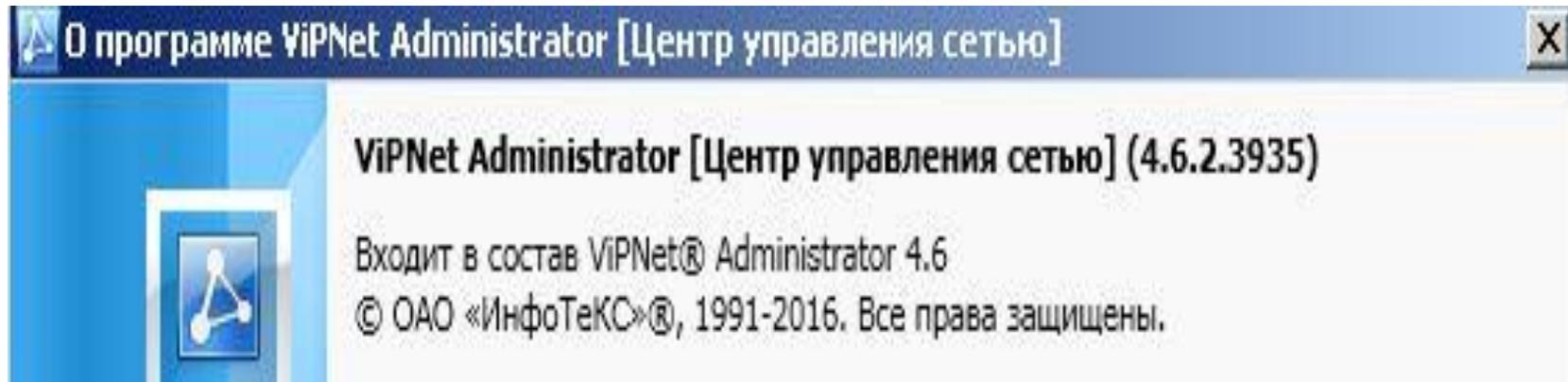
Темы:

1. Информация о текущих версиях, сборках
2. Обновление релизов 4.x
3. Взаимодействие компонентов
4. Архивирование данных
5. Восстановление из архива
6. Работа с доверенными сетями
7. Журналирование операций
8. Перенос компонентов на новое оборудование
9. Рассылка CRL
10. Формирование запроса в Минкомсвязь (ГУЦ)
11. Работа с группами
12. Настройки компонентов, добавление OID
13. Особенности смены мастер ключей своей сети ViPNet
14. Что делать не следует
15. Ответы на вопросы.

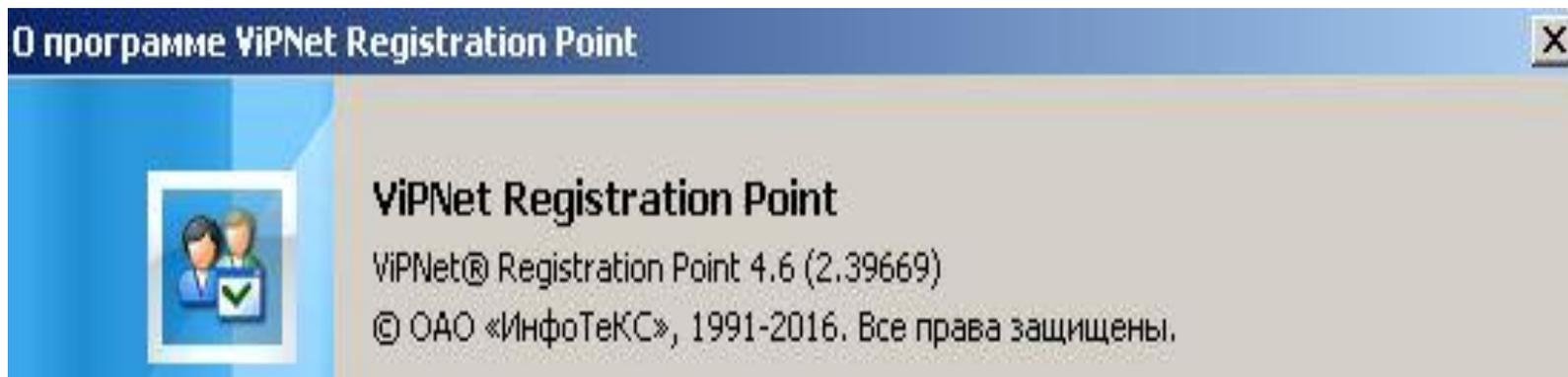
ViPNet Удостоверяющий и ключевой центр



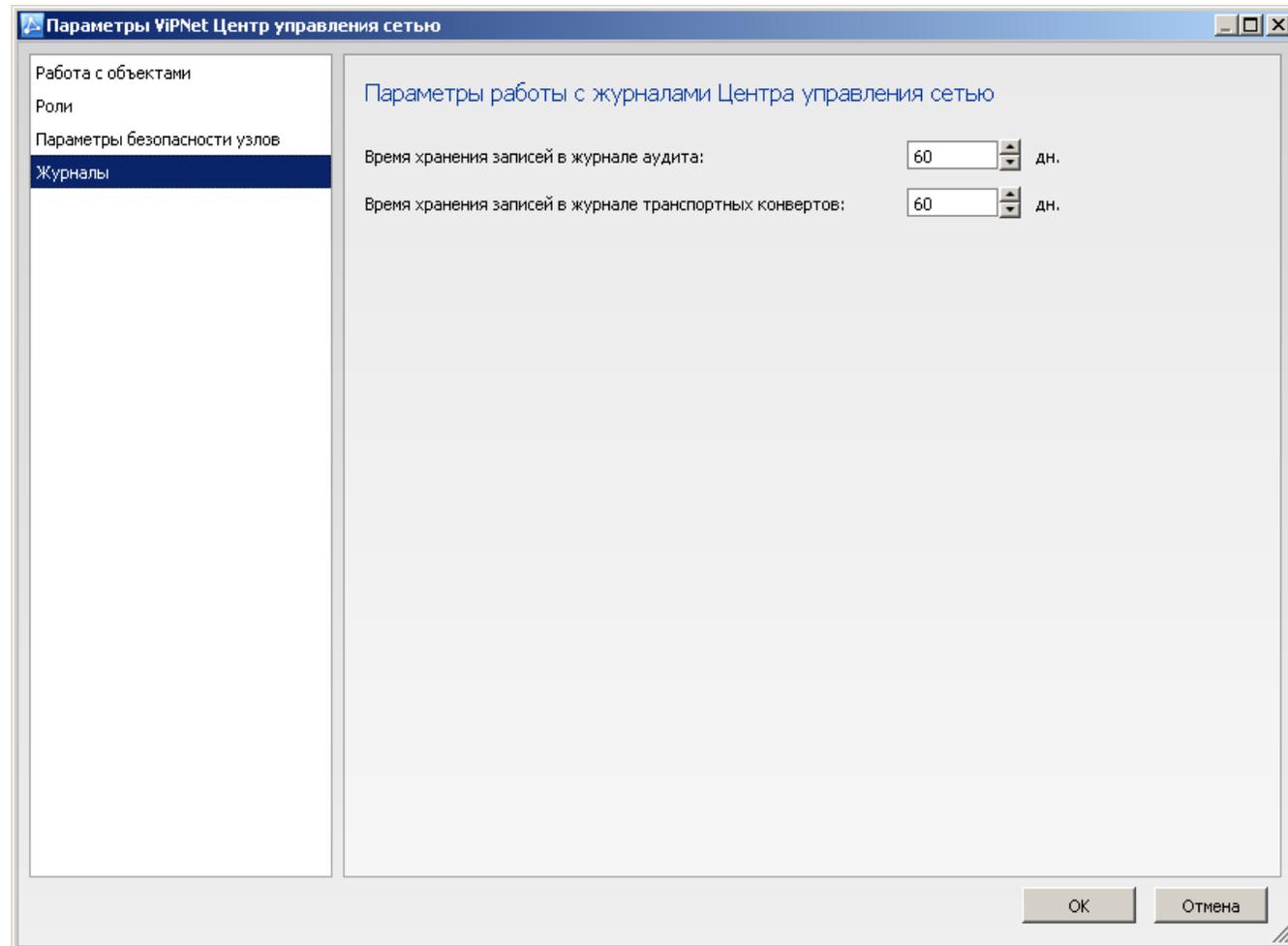
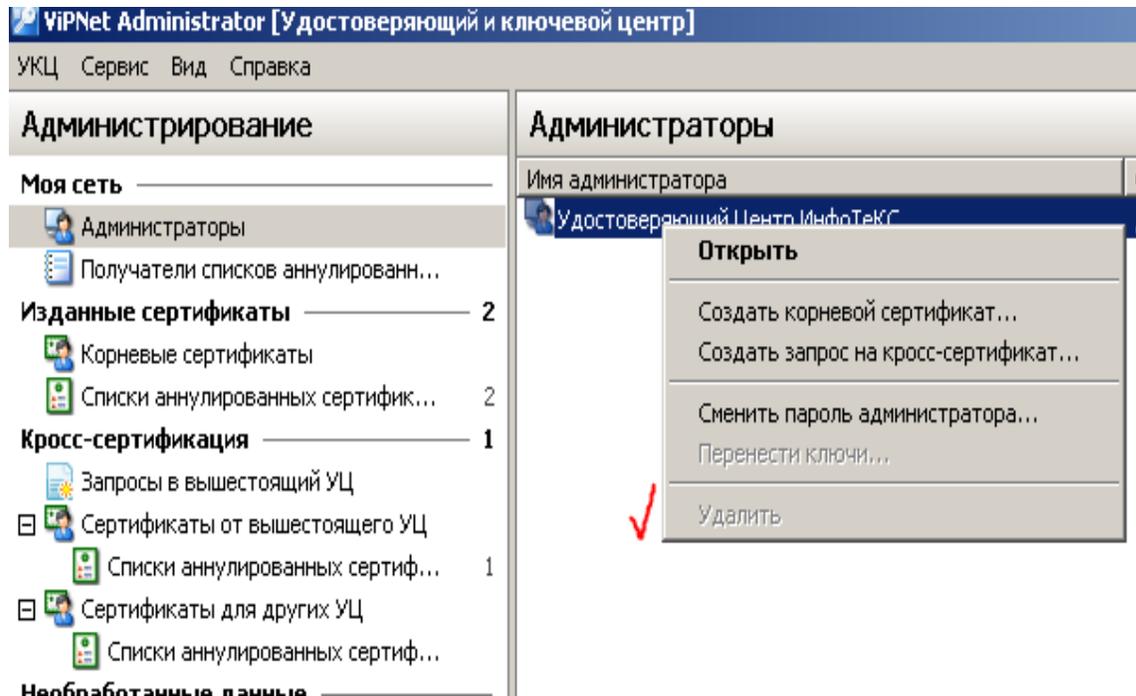
Версия ЦУС и УКЦ всегда должны применяться из одного инсталляционного комплекта, пример для версии 4.6.2:



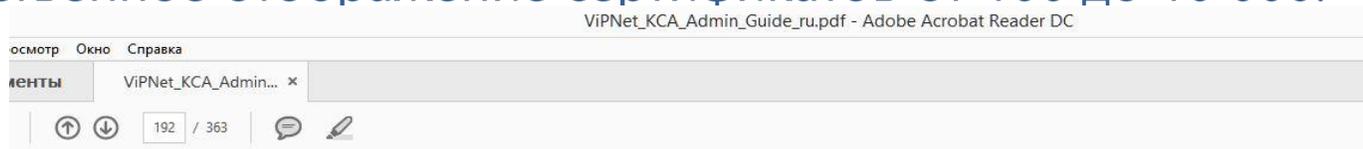
Такие приложения как Центр Регистрации, Сервис Публикации должны применяться версионностью 4.x, но не 3.2, например для комплекта 4.6.2 версия ЦР соответствует:



Возможность удалить учетные данные старых администраторов УКЦ и расширенное управление размерностью журналов ЦУС есть в релизе 4.6.3



Учены предложения пользователей и с версии 4.6.2 созданы настройки позволяющие изменить количественное отображение сертификатов от 100 до 10 000:



Настройка количества сертификатов, отображаемых в окне программы

По умолчанию в программе в списках сертификатов пользователей в подразделах раздела **Изданные сертификаты** отображается не более 100 сертификатов.

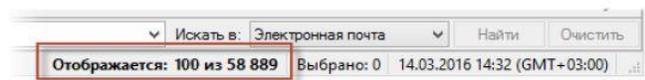


Рисунок 95: Количество сертификатов, отображаемых в программе по умолчанию

Если требуется, чтобы в списках сертификатов этих разделов отображалось большее количество сертификатов, выполните следующие действия:

- 1 В файле `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Ini\KC.ini` добавьте параметр `Certificates cache capacity` в секцию `[Certification]`.
- 2 В качестве значения параметра `certificates cache capacity` укажите количество сертификатов, которое должно отображаться. Возможные значения параметра `certificates cache capacity`: от 100 до 10000. Если будет задано значение меньше или больше возможного, то по умолчанию будет использоваться значение 100.

Выполняйте системные требования, они всегда есть в эксплуатационной документации:



Системные требования

Для установки программ, входящих в состав ПО ViPNet Administrator, компьютеры должны удовлетворять ряду требований.

Компьютер, на который будет установлено несколько программ ViPNet Administrator, должен соответствовать максимальным требованиям из числа указанных.

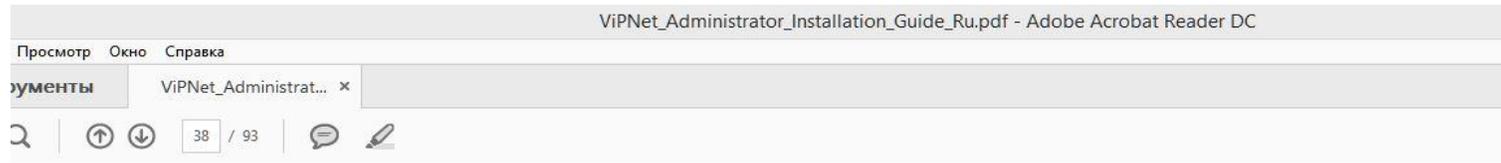
ViPNet Центр управления сетью

Серверное приложение

Требования к аппаратному обеспечению компьютера для установки серверного приложения ViPNet Центр управления сетью:

- Процессор — Intel Core 2 Quad или другой схожий по производительности x86-совместимый процессор с количеством ядер 4 и более.
- Объем оперативной памяти — не менее 4 Гбайт.

Перед обновлением компонентов установите критические обновления Microsoft



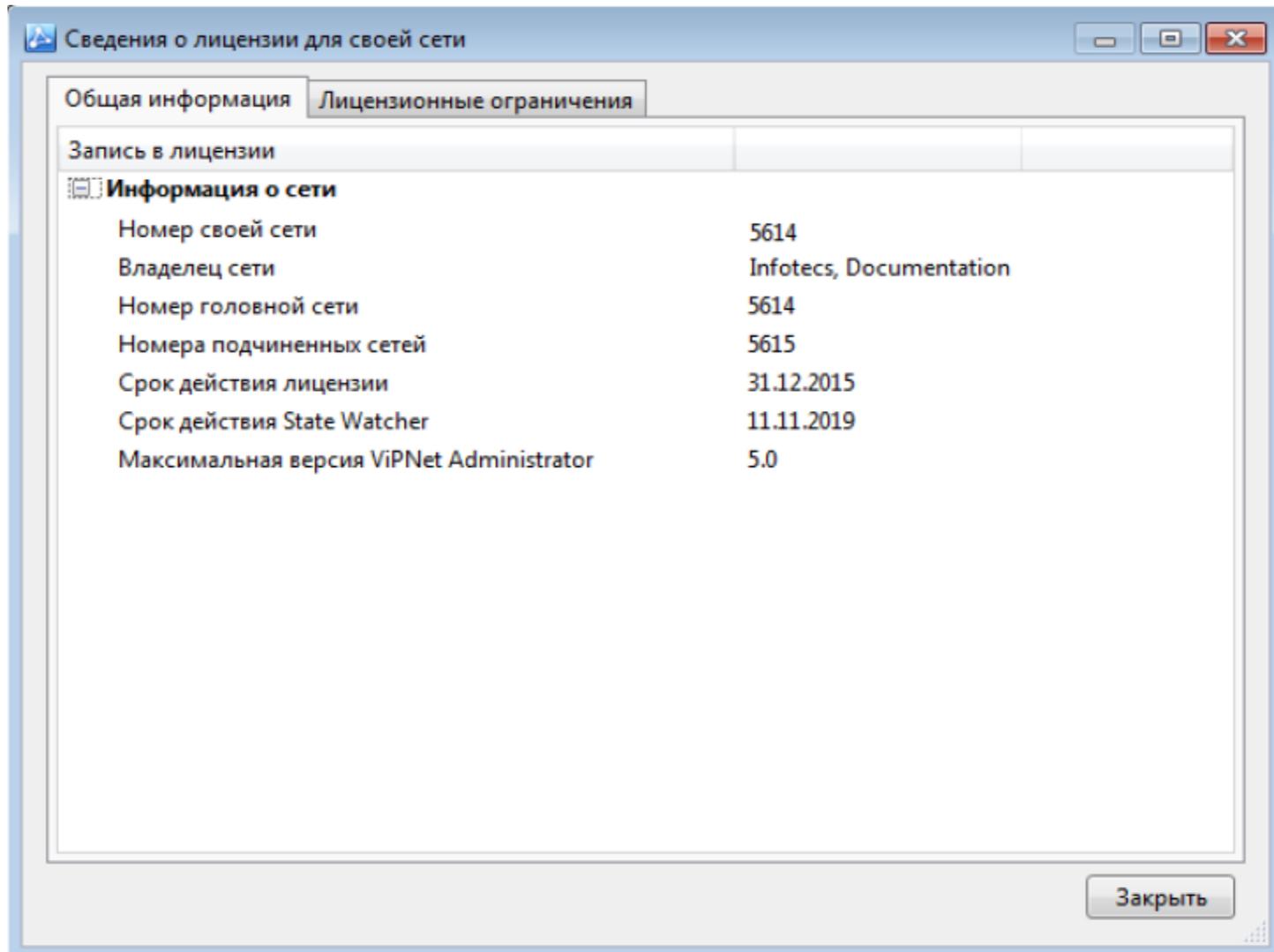
Установка обновлений для стороннего ПО

Программное обеспечение сторонних производителей, которое необходимо для работы программы ViPNet Центр управления сетью, может содержать уязвимости. Чтобы избежать влияния возможных уязвимостей на работу программы, необходимо своевременно устанавливать обновления безопасности, выпускаемые производителями стороннего ПО.

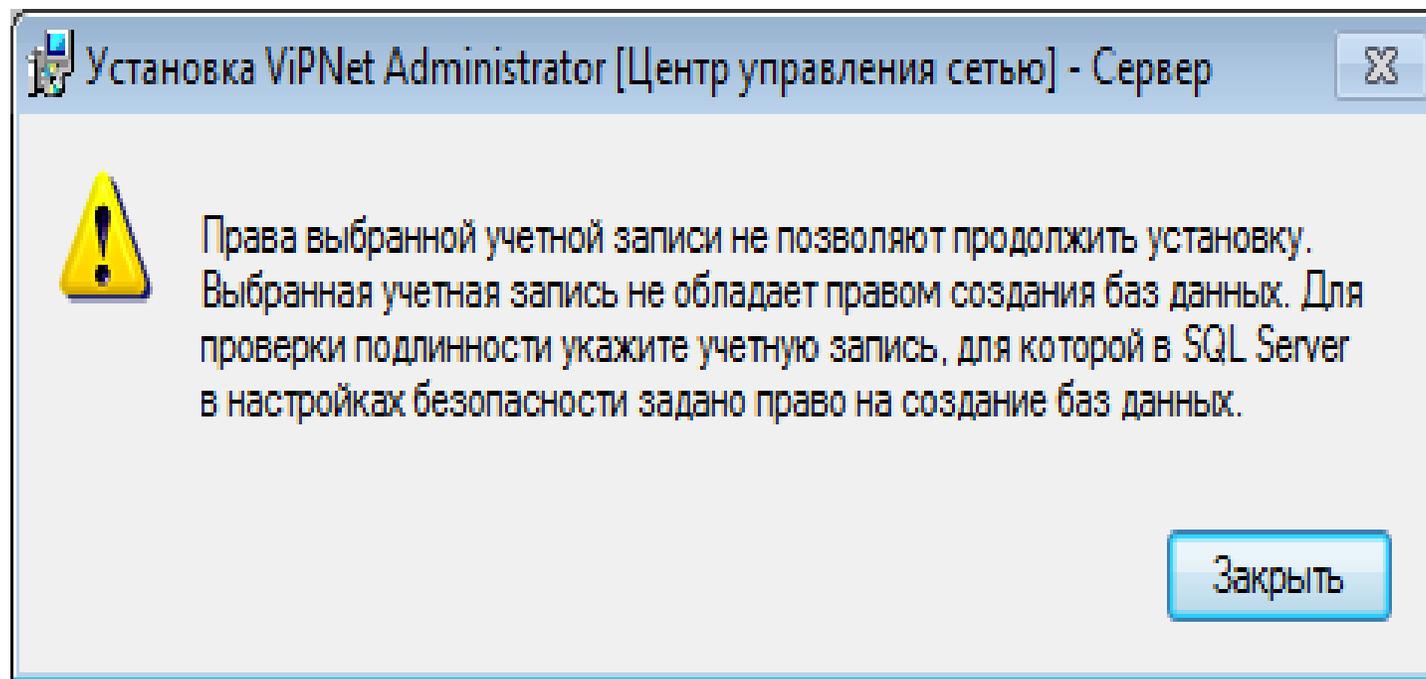
После установки серверного и клиентских приложений ViPNet Центр управления сетью выполните следующие действия:

- 1 Проверьте наличие обновлений безопасности или новых версий стороннего программного обеспечения:
 - Microsoft .NET Framework версии 4.5.
 - Visual C++ 2010 Redistributable Package.
 - Используемой версии Microsoft SQL Server.
- 2 При наличии обновлений установите их.
- 3 В процессе эксплуатации программы ViPNet Центр управления сетью регулярно устанавливайте выпускаемые обновления ПО сторонних производителей.

Проверка ограничения допустимой версии доступно из текущего Клиента ЦУС:



Проблема при обновлении:



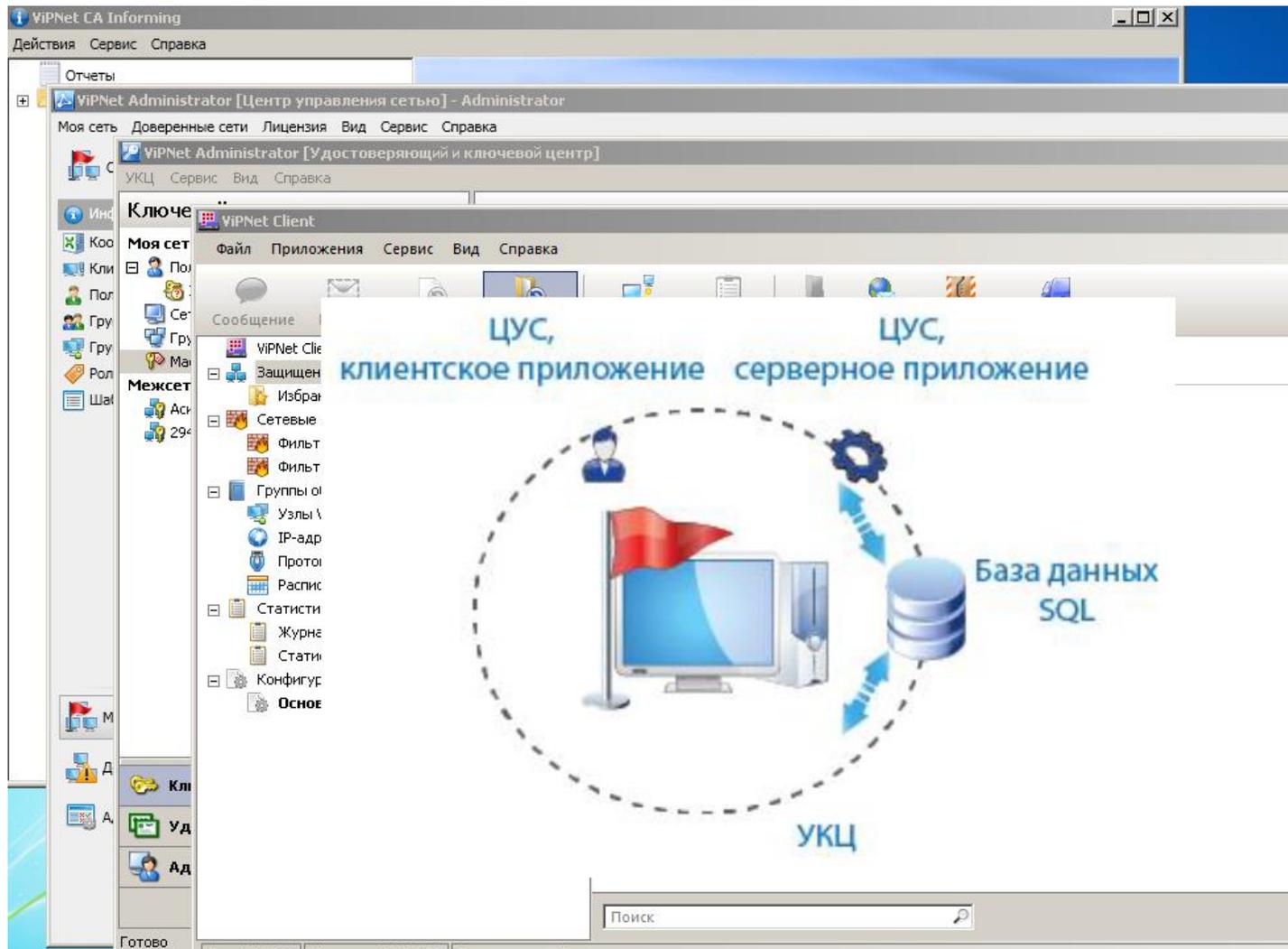
/ Решение детально излагается в разделе документа «Руководство по установке»
/ "VIPNet_Administrator_Installation_Guide_Ru.pdf"

Порядок обновления компонентов из документа «Руководство по установке»:

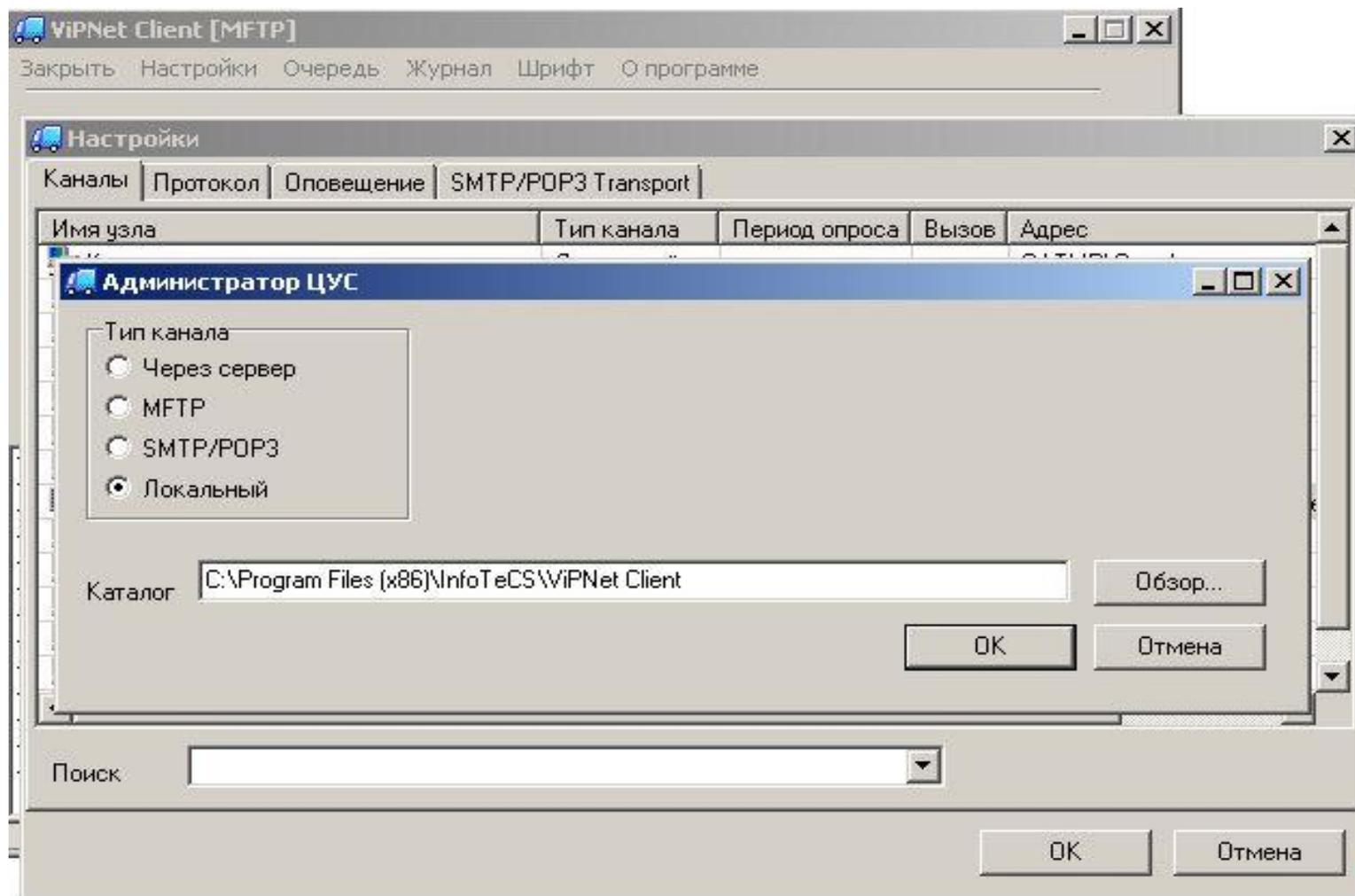
Обновление компонентов программного обеспечения ViPNet Administrator рекомендуется выполнять в следующем порядке:

- 1 Обновите серверное приложение ViPNet Центр управления сетью (см. «Обновление приложений ViPNet Центр управления сетью» на стр. 59).
- 2 Обновите клиентское приложение ViPNet Центр управления сетью (см. «Обновление приложений ViPNet Центр управления сетью» на стр. 59).
- 3 Обновите программу ViPNet Удостоверяющий и ключевой центр (см. «Обновление программы ViPNet Удостоверяющий и ключевой центр» на стр. 61).

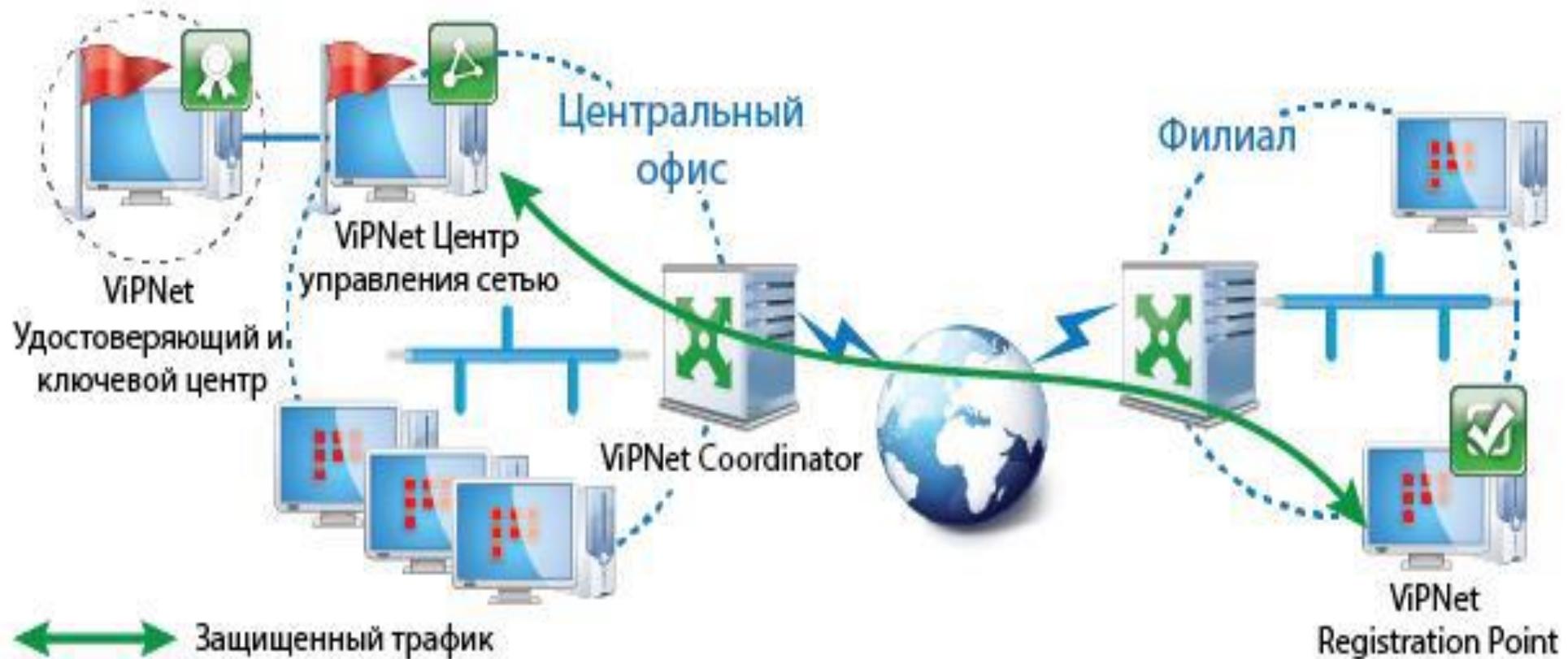
Все компоненты на одном компьютере:



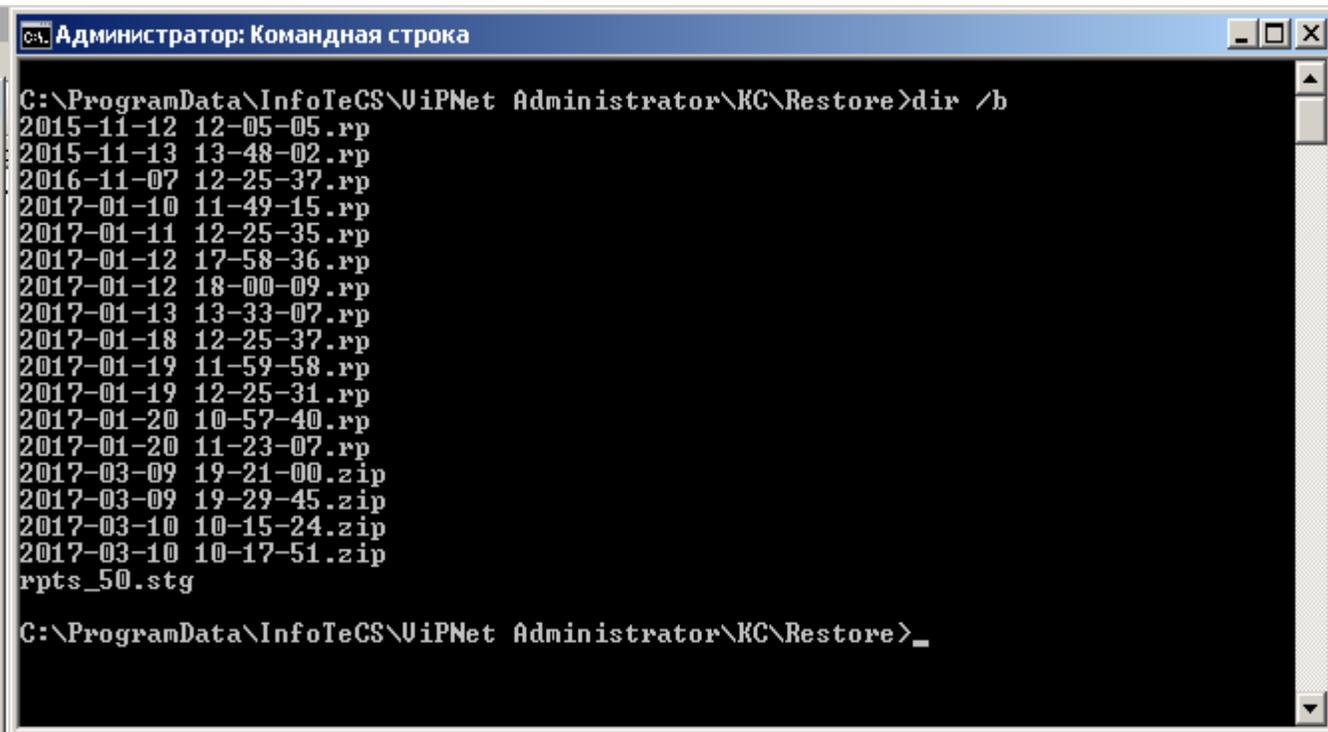
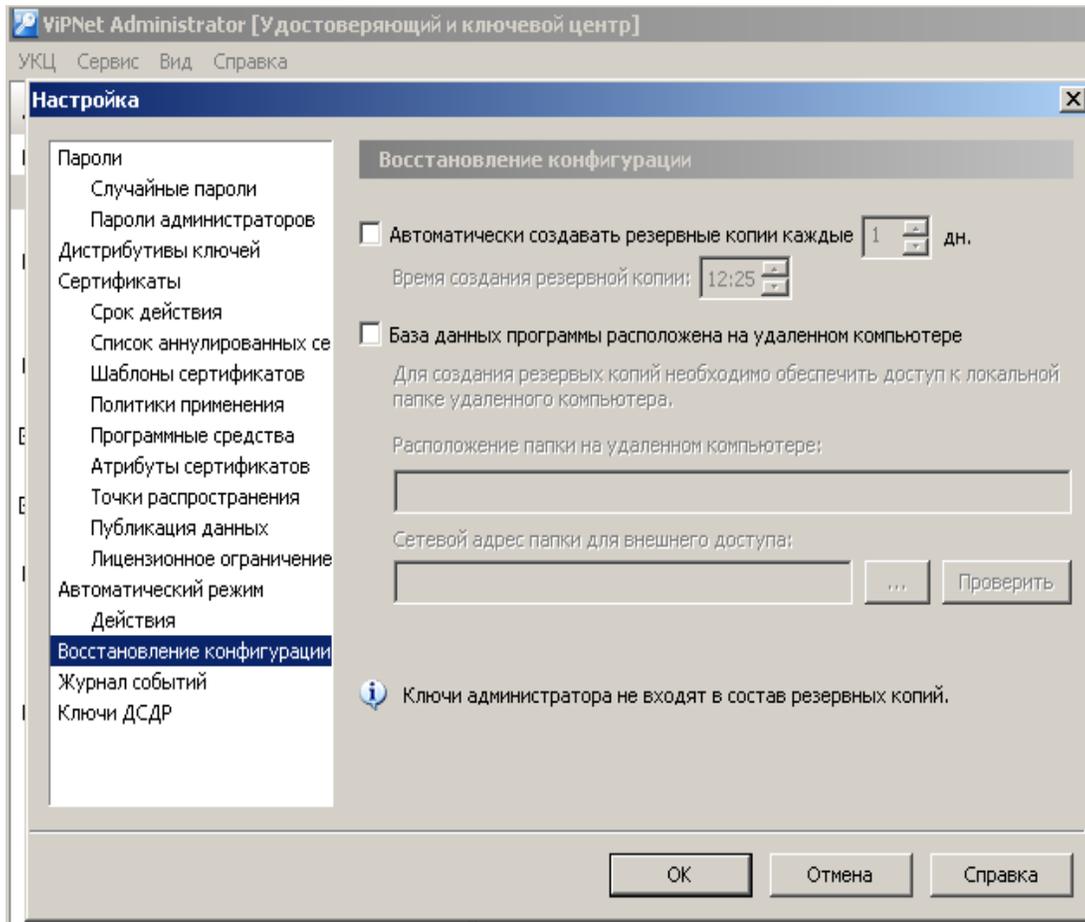
Настройка канала MFTP ViPNet Клиента на ЦУС:



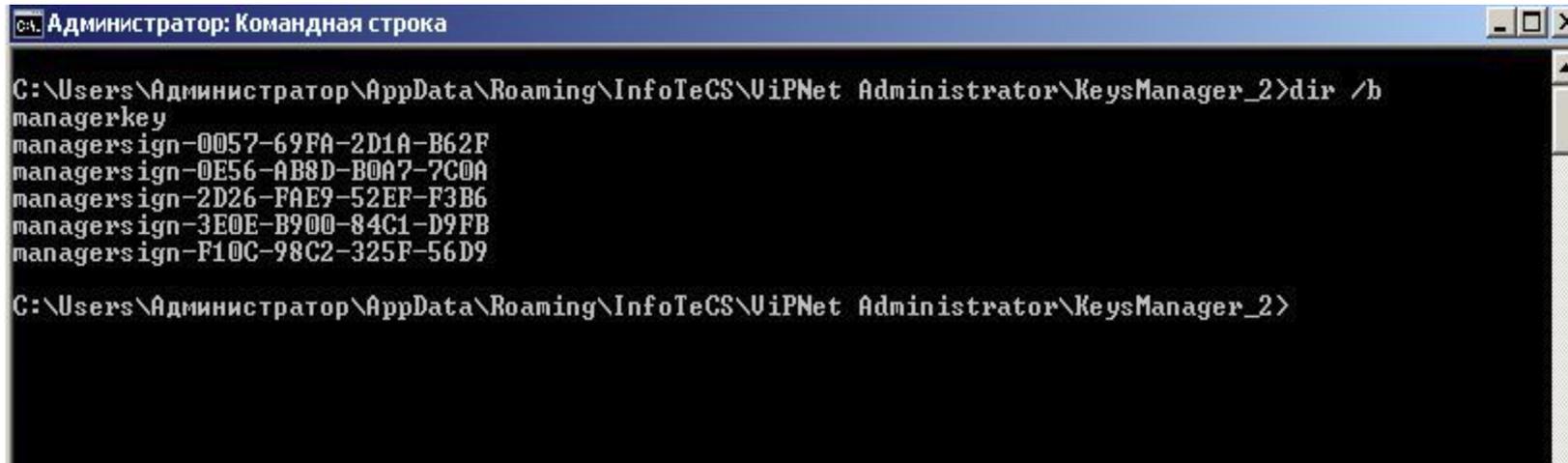
Установка Центра регистрации совместно с ViPNet Client как один сетевой узел:



Архивирование данных (меню настроек УКЦ и целевой каталог по умолчанию):

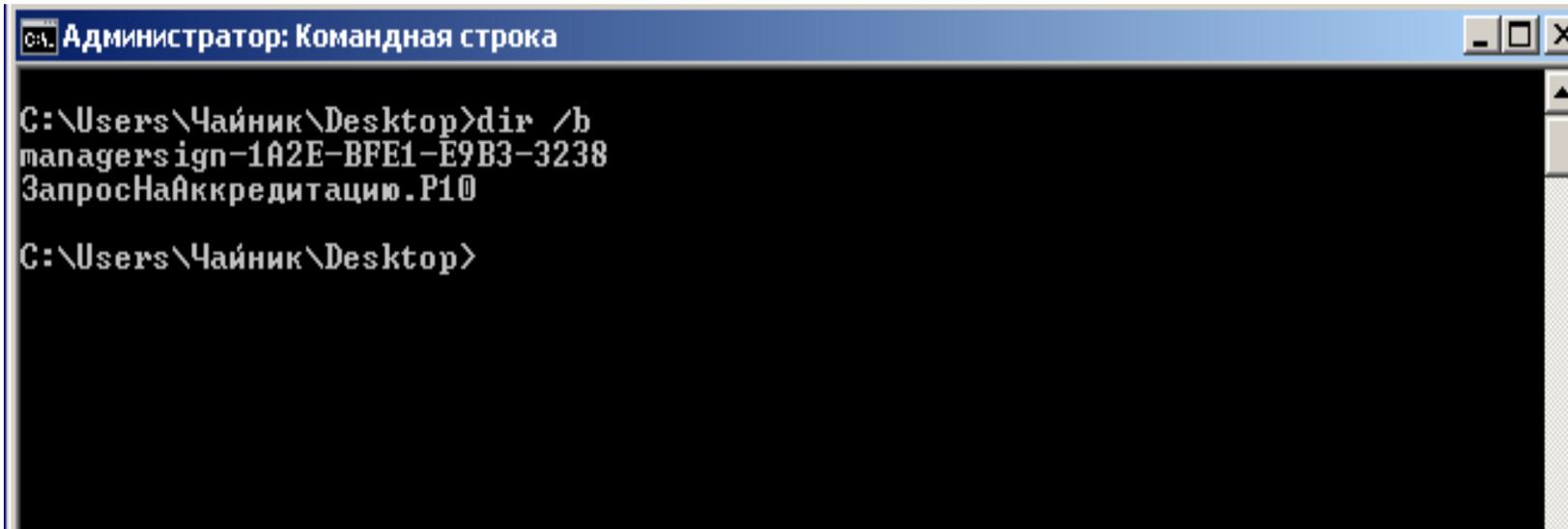


Расположение контейнеров закрытого ключа:



```
Администратор: Командная строка
C:\Users\Администратор\AppData\Roaming\InfoTeCS\VipNet Administrator\KeysManager_2>dir /b
managerkey
managersign-0057-69FA-2D1A-B62F
managersign-0E56-AB8D-B0A7-7C0A
managersign-2D26-FAE9-52EF-F3B6
managersign-3E0E-B900-84C1-D9FB
managersign-F10C-98C2-325F-56D9

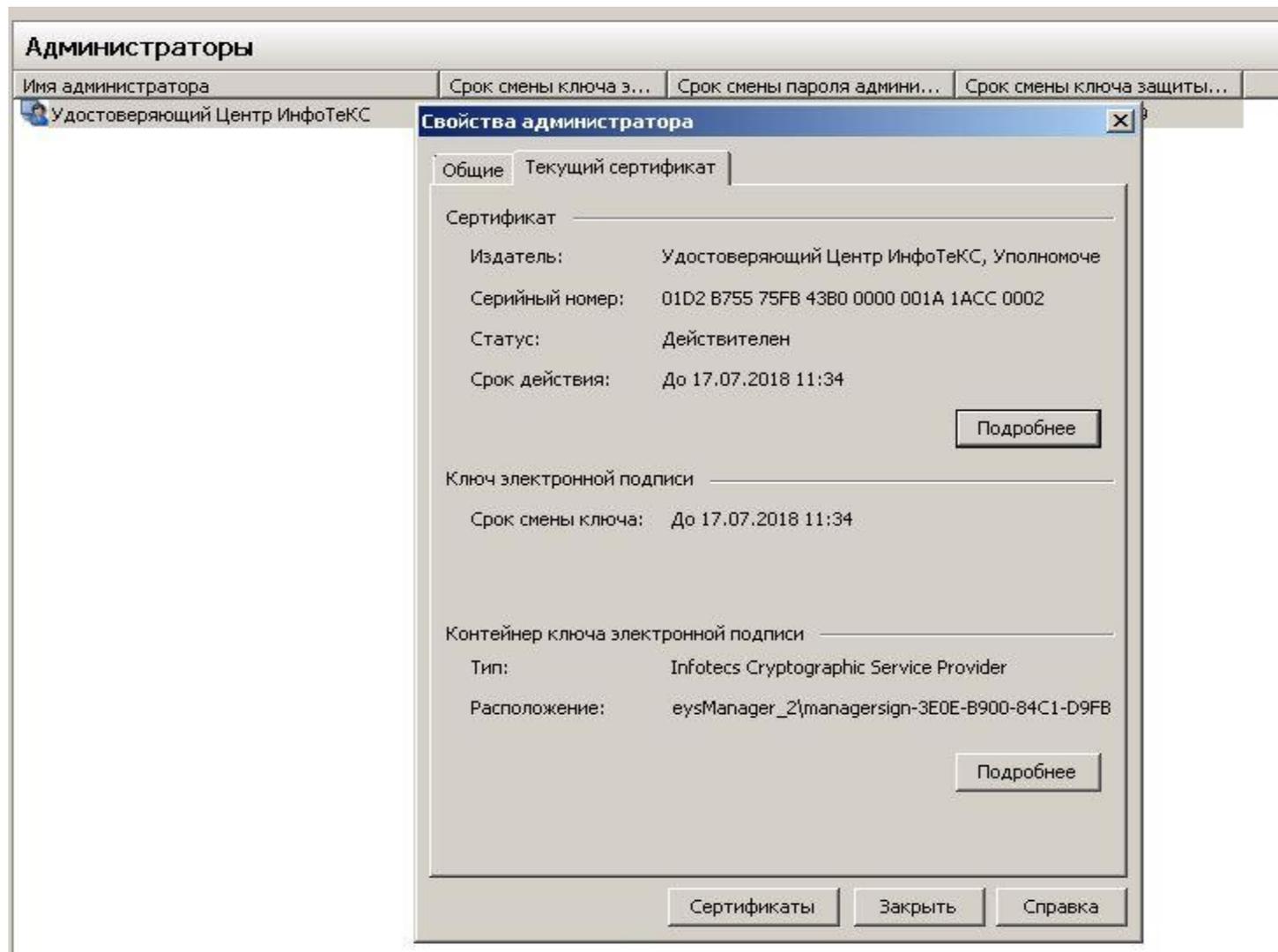
C:\Users\Администратор\AppData\Roaming\InfoTeCS\VipNet Administrator\KeysManager_2>
```



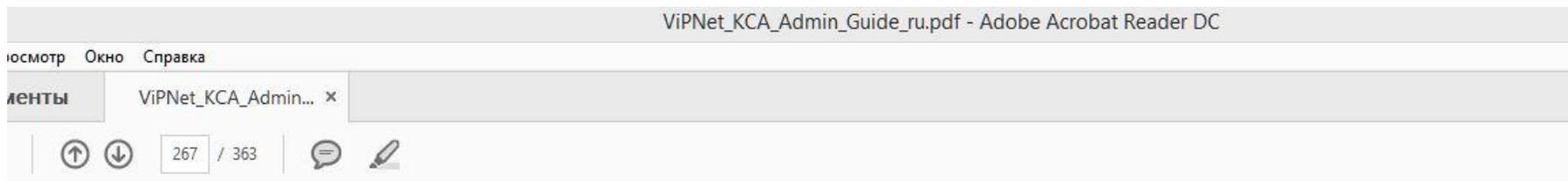
```
Администратор: Командная строка
C:\Users\Чайник\Desktop>dir /b
managersign-1A2E-BFE1-E9B3-3238
ЗапросНаАккредитацию.P10

C:\Users\Чайник\Desktop>
```

Определение контейнера закрытого ключа подписи по строке «Расположение»:



Новые настройки каталога сохранения архива, детали в документации:



При необходимости вы можете изменить папку сохранения резервных копий по умолчанию, выполните следующие действия:

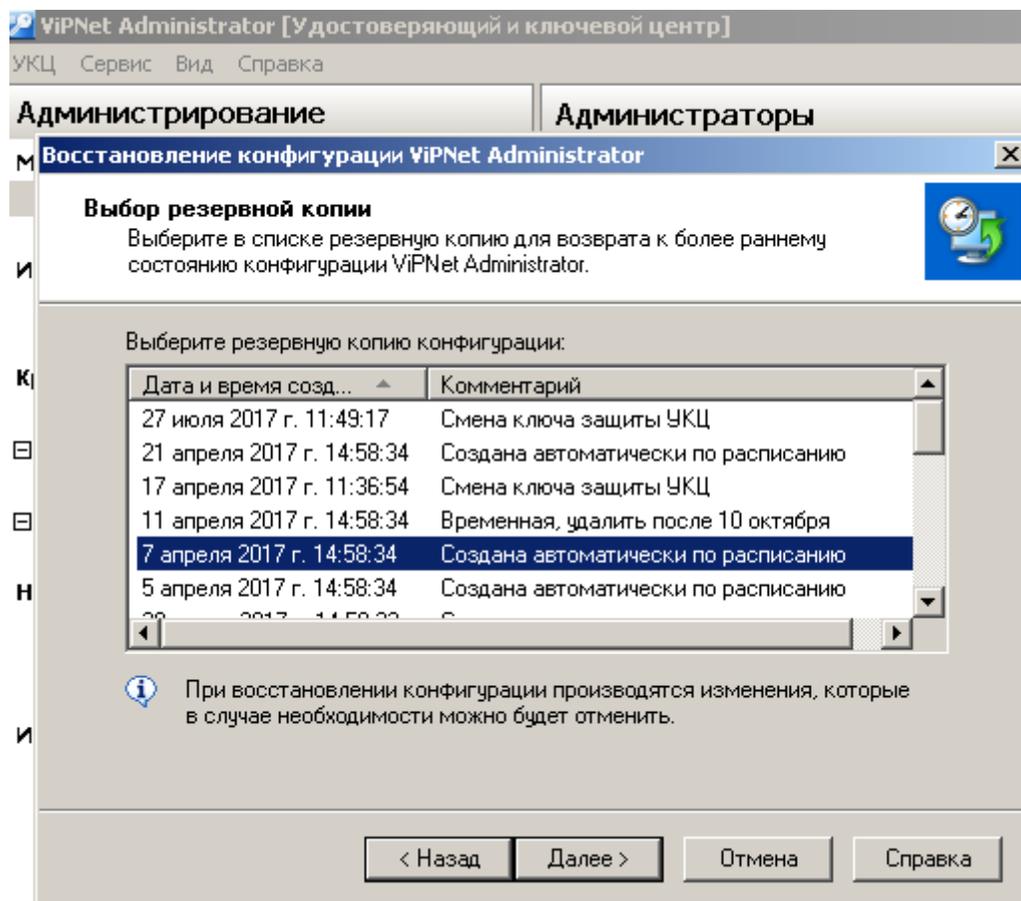
- 1 Откройте файл конфигурации УКЦ `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\ini\KC.ini`.
- 2 В секции `[Archive]` добавьте строку следующего вида: `Configuration backup folder=<Путь к папке сохранения резервных копий>`.

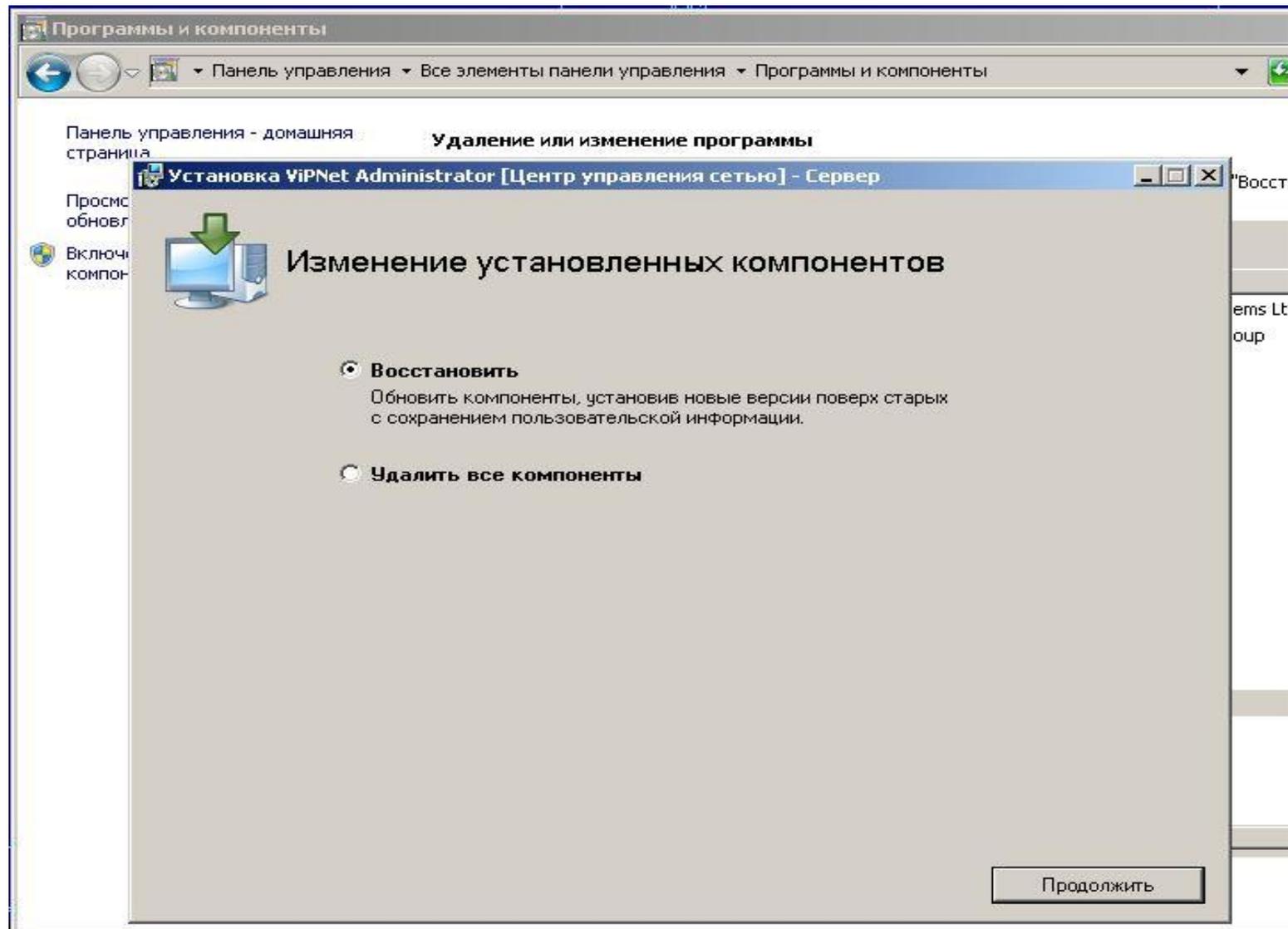


Примечание. Чтобы сохранить текущий список резервных копий конфигурации сети, необходимо перенести все содержимое папки `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore` в папку сохранения резервных копий по новому пути.

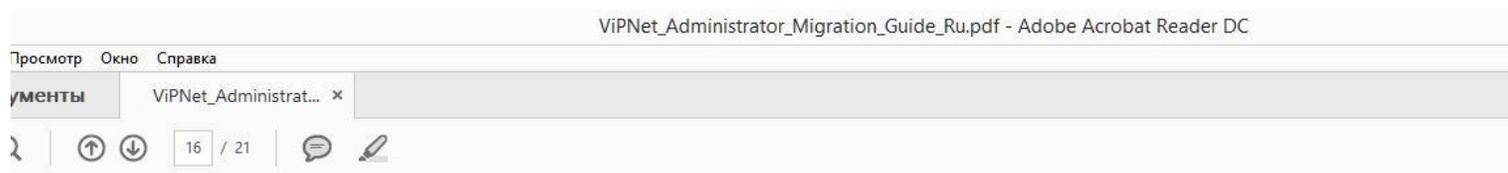
Резервная копия конфигурации сети записывается в файл списка резервных копий с расширением `*.stg`, который потом отображается при редактировании списка резервных копий.

Восстановление из архива:





Раздел документа «ViPNet_Administrator_Migration_Guide_Ru.pdf»



Восстановление конфигурации сети из резервной копии

После развертывания ПО ViPNet Administrator на новом компьютере требуется восстановить резервную копию конфигурации сети, созданную перед началом миграции.

Для восстановления резервной копии выполните следующие действия:

- 1 Скопируйте резервную копию конфигурации сети (файл *.zip или *.rp) и копию архива со списком всех созданных резервных копий (файл rpts_50.stg), которые были сделаны перед началом миграции, в папку `C:\ProgramData\InfoTeCS\ViPNet Administrator\КЦ\Restore` (см. «Подготовка данных для миграции ПО ViPNet Administrator» на стр. 14).
- 2 Войдите в программу ViPNet Удостоверяющий и ключевой центр с помощью учетной записи администратора, которая была создана во время первичной инициализации УКЦ на новом компьютере.
- 3 В окне программы в меню **Сервис** выберите пункт **Восстановление конфигурации**.
- 4 В появившемся окне мастера восстановления конфигурации выберите **Восстановить конфигурацию ViPNet Удостоверяющий и ключевой центр** и нажмите кнопку **Далее**.
- 5 На странице **Выбор резервной копии** укажите копию, из которой будет восстановлена

Раздел документа «Руководство по миграции программного обеспечения на другой компьютер»:



Восстановление учетной записи администратора УКЦ

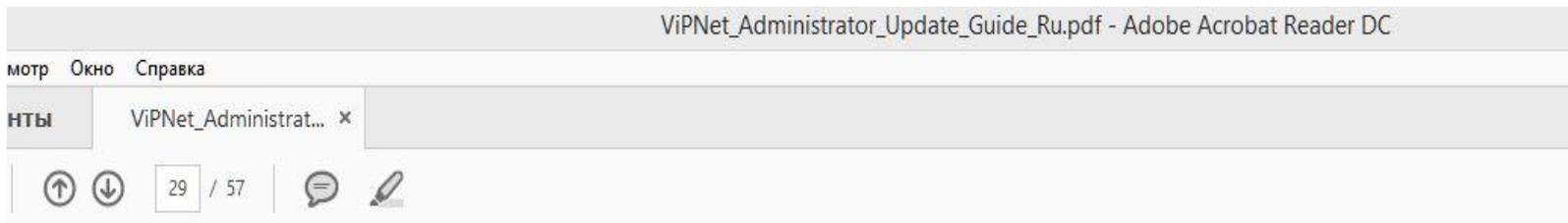
Чтобы администратор УКЦ мог продолжить работу со своей учетной записью на новом компьютере, необходимо перенести на новый компьютер ключи администратора УКЦ. Для этого выполните следующие действия:

- 1 На новом компьютере с УКЦ удалите данные о подключении к SQL-серверу, восстановленные из резервной копии. Для этого удалите из папки `C:\ProgramData\InfoTeCS\ViPNet Administrator\КЦ\Ini` файл `sqlloginfo.dat`.
- 2 Удалите контейнер ключей администратора, созданный при первичной инициализации УКЦ. Для этого удалите папку `C:\Users\<имя локального администратора Windows>`, от лица которого установлена программа `УКЦ>\AppData\Roaming\Infotecs\ViPNet Administrator`.
- 3 Перенесите на новый компьютер копию папки с контейнерами ключей администратора, которая была создана перед миграцией, в папку `C:\Users\<имя локального администратора Windows>`, от лица которого была установлена программа УКЦ до миграции `>\AppData\Roaming\Infotecs\ViPNet Administrator`.



Примечание. Если название папки в `C:\Users\` будет содержать неправильное имя локального администратора Windows, то учетная запись не сможет быть восстановлена. Если все контейнеры ключей администраторов размещаются на внешних устройствах, то пропустите этот шаг.

Межсетевое взаимодействие:



Особенности преобразования связей при конвертации

В ViPNet Центр управления сетью версии 3.2.x объекты сети (см. глоссарий, стр. 55) связаны между собой на уровне типов коллективов (ТК). В программе ViPNet Центр управления сетью версии 4.x образуются связи других видов, при этом во внутренних механизмах работы программы связи между ТК остаются. При конвертации данных ЦУСа 3.2.x появляются связи между узлами сети (см. глоссарий, стр. 55), связи между ТК преобразуются в связи следующего типа:

- связи между пользователями;
- связи между пользователями и группами пользователей.

g [Центр управления сетью] - Administrator

ети Лицензия Вид Сервис Справка

ючи ▾ Межсетевая информация ▾

Свойства сетей

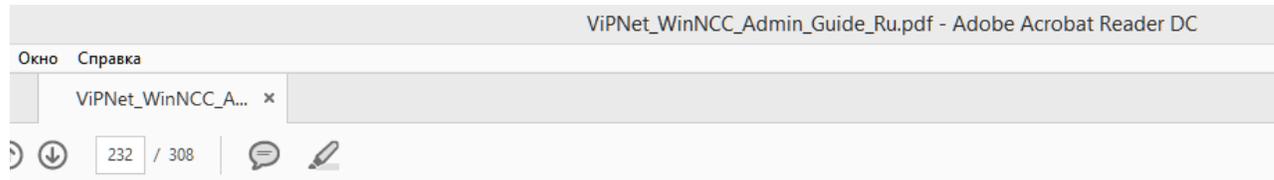
Установить взаимодействие Загрузить межсетевую информацию Сохранить лицензию

<input checked="" type="checkbox"/>	Тип сети	Имя	▲	Номер сети	Шлюз моей сети	Шлюз доверенной се
<input checked="" type="checkbox"/>		test		2012	Корреспондент	Корреспондент (6) СД

- Свойства
- Создать межсетевую информацию...
- Отправить межсетевую информацию...
- Сохранить межсетевую информацию в файл...
- Загрузить межсетевую информацию из файла...
- Обработать межсетевую информацию...
- Отклонить межсетевую информацию
- Прекратить взаимодействие
- Очистить кэш межсетевой информации
- Автоматическая обработка межсетевой информации...

✓

Экспорт справочников из 3.2 для передачи в сеть версии 4.*

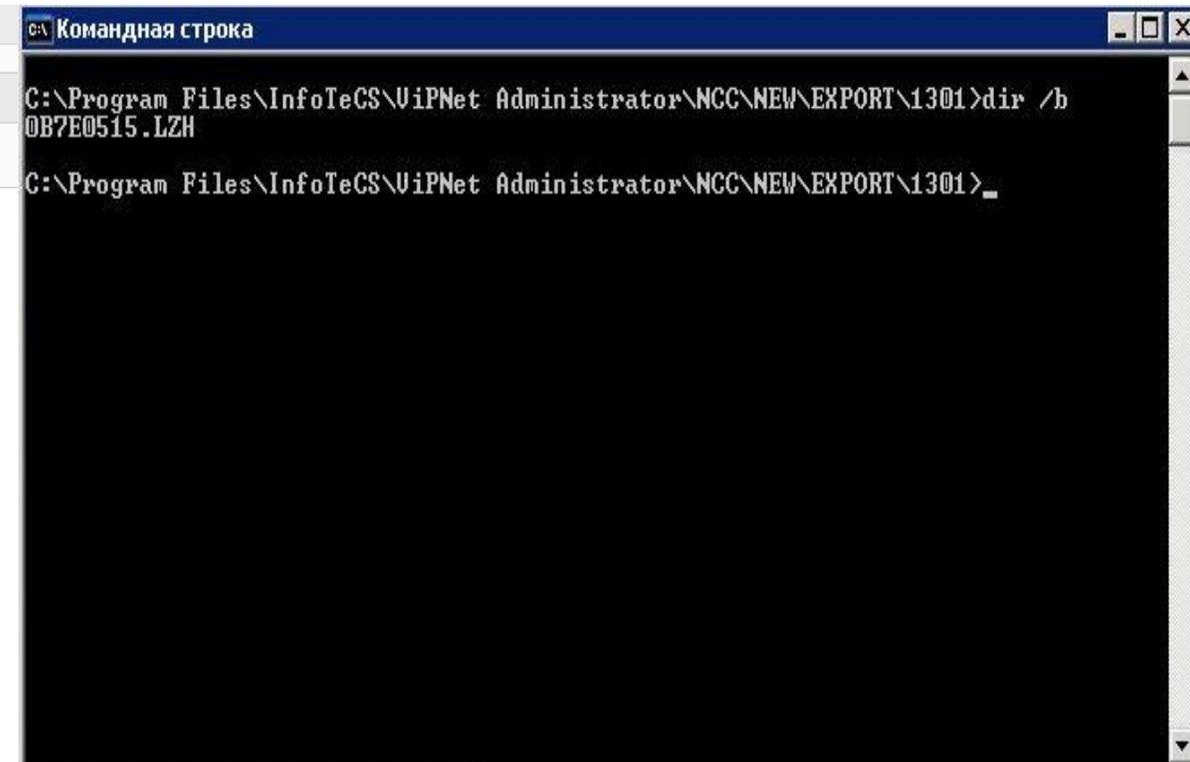


Особенности создания межсетевой информации в ПО VIPNet Administrator 3.x

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 **Задать 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.



<HexNumFROM><HexNumFOR>.lzh

Из документа «ViPNet Центр управления сетью 4. Руководство администратора»:

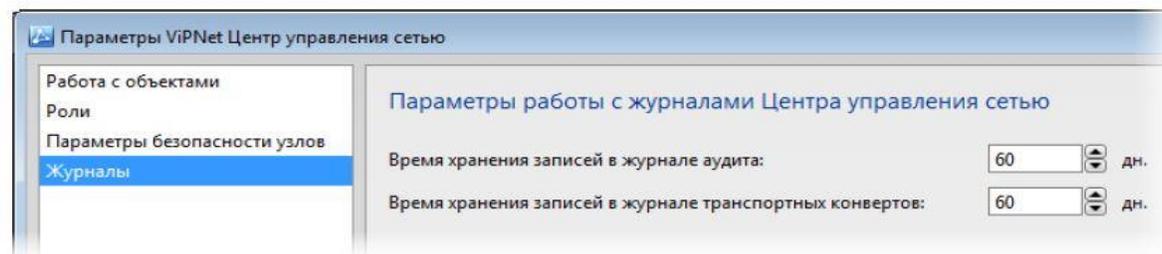
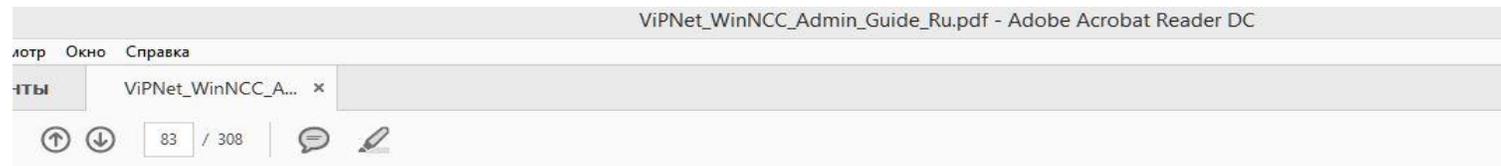


Рисунок 39. Параметры журналов

- 3 Чтобы задать время хранения записей в журналах аудита, в соответствующем поле установите необходимое число дней. Минимальное время хранения 7 дней, максимальное — 365 дней. По умолчанию записи хранятся 60 дней.
Записи с истекшим временем хранения автоматически удаляются из журналов.
- 4 Чтобы задать время хранения записей в журнале транспортных конвертов, в соответствующем поле установите необходимое число дней. Минимальное время хранения 1 день, максимальное — 365 дней. По умолчанию записи хранятся 60 дней.
Записи со сроком хранения более установленного значения автоматически удаляются из журналов в 00:00 часов следующего дня.
- 5 Для сохранения настроек нажмите кнопку **ОК**.

Распаковка ключевого файла из транспортного журнала ЦУС:

The screenshot shows a software interface for viewing network traffic logs. On the left, there are filters for 'Тип' (Type), 'Дата получения' (Date received), 'Дата обработки' (Date processed), 'Статус' (Status), 'Имя узла' (Node name), 'Идентификатор узла' (Node identifier), 'Имя исходного конверта' (Original filename), and 'Имя транспортного конверта' (Transport filename). The main area displays a table of log entries with columns: 'Дата отправки' (Send date), 'Имя узла' (Node name), 'Статус' (Status), 'Имя исходного конверта' (Original filename), 'Содержимое конверта' (Content), and 'Имя транспортного конверта' (Transport filename). A 'Обзор папок' (Folder view) window is open over the log, showing a folder named 'MFTP.tempo'. A 'Командная строка' (Command prompt) window is also open, showing the following commands and output:

```

C:\MFTP.tempo\m%hqw8}8.ct1>dir /b
keaf8fa6.cnf
keaf8fa6.dtm
keaf8fa6.lzh

C:\MFTP.tempo\m%hqw8}8.ct1>lha l keaf8fa6.lzh

Listing of archive : keaf8fa6.lzh

  Name           Original      Packed  Ratio  Date       Time      Attr Type  CRC
-----
apn_000C.ke     29349        7306   24.9%  16-12-08   17:38:13  a-w  -lh5-  96E6
  1 files       29349        7306   24.9%  17-09-12   11:57:58
C:\MFTP.tempo\m%hqw8}8.ct1>
    
```

At the bottom of the application window, there are buttons for 'Сбросить' (Reset), 'Обновить журнал' (Refresh log), 'Сохранить в файл...' (Save to file...), and 'Закрыть' (Close).

Журнал УКЦ доступен в Windows:

The screenshot shows the Windows Event Viewer interface. The left pane displays the tree view with 'VIPNet Administrator KCA' selected under 'Журналы приложений и служб'. The right pane shows the details for event ID 16650, titled 'Событие 16650, Key and Certification Authority'.

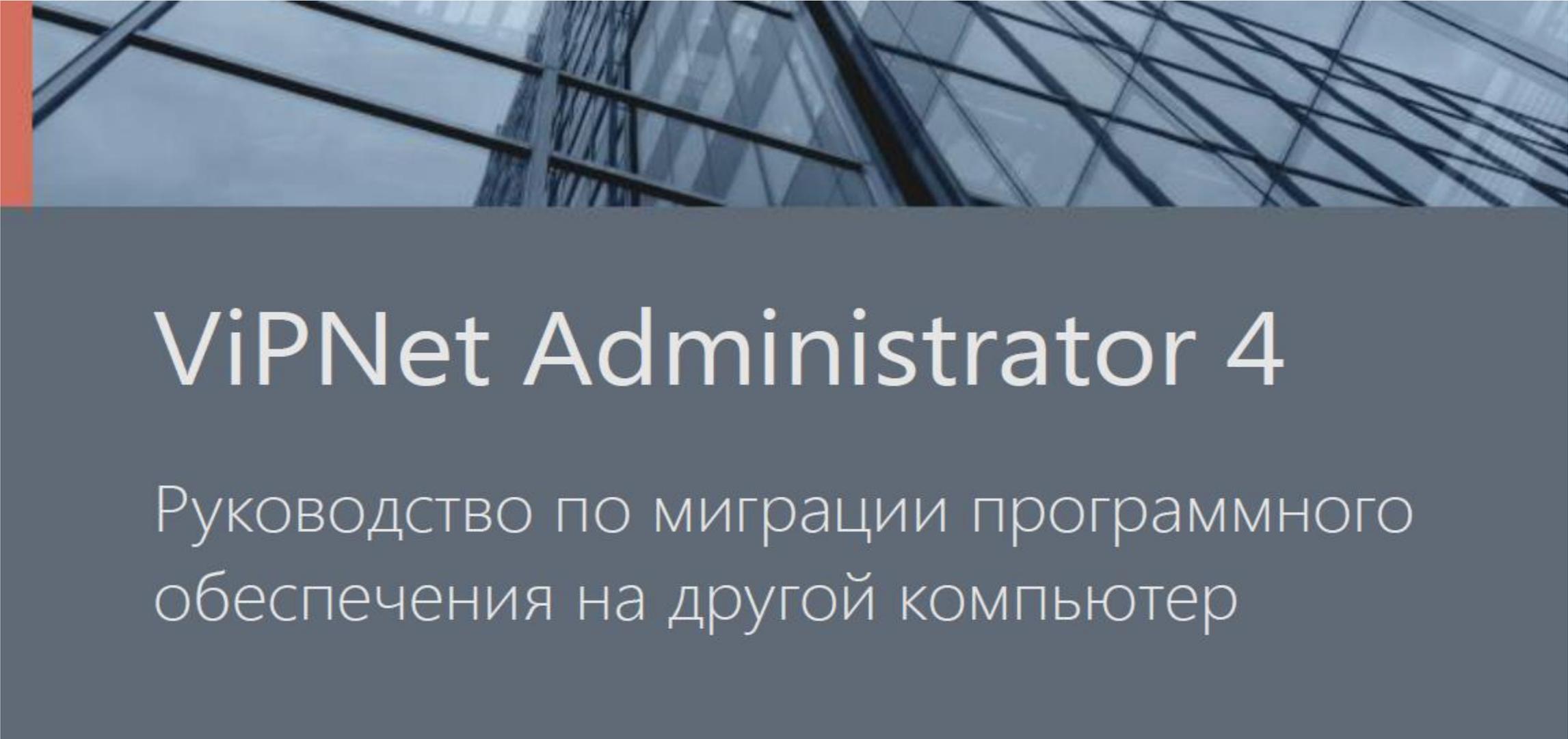
Уровень	Дата и время	Источник	Код события	Категория з...
И	07.09.2017 15:25:48	Key and Certi...	16650	Отсутствует

Событие 16650, Key and Certification Authority

Общие | Подробности

Издан CRL.
 Серийный номер CRL: 01 D3 27 D4 6F 5C 6D 2B 00 00 17 1A CC 00 02
 Имя издателя CRL: Удостоверяющий Центр ИнфоТеКС, Уполномоченное лицо, Отдел технического сопровождения, ОАО «ИнфоТеКС», hotline@infotecs.ru, Москва, RU, 7710013769, 10277391850, "Москва, Старый Петровско-Разумовский проезд, дом 1/23, строение 1", 1027739185066, 8-800-250-0-260, Тестовый УЦ версии 4.6, 127287
 Основание: Инициатива администратора

Документ «ViPNet_Administrator_Migration_Guide_Ru.pdf»



ViPNet Administrator 4

Руководство по миграции программного обеспечения на другой компьютер

Настройка списка получателей CRL своей сети:

The screenshot shows the 'VIPNet Administrator' window with the 'Администрирование' (Administration) menu open. The 'Получатели списков аннулированных сертификатов' (CRL Recipients) option is selected. The main pane displays a table with two columns: 'Тип' (Type) and 'Имя узла' (Node Name). Two entries are listed: 'Администратор ЦУС' (CA Administrator) and 'Центр регистрации' (Registration Center).

Тип	Имя узла
	Администратор ЦУС
	Центр регистрации

Передать CRL в ЦУС:

The screenshot shows the ViPNet Administrator interface. The main window title is "ViPNet Administrator [Удостоверяющий и ключевой центр]". The menu bar includes "УКЦ", "Сервис", "Вид", and "Справка".

The left pane is titled "Ключевой центр" and contains a tree view with the following items:

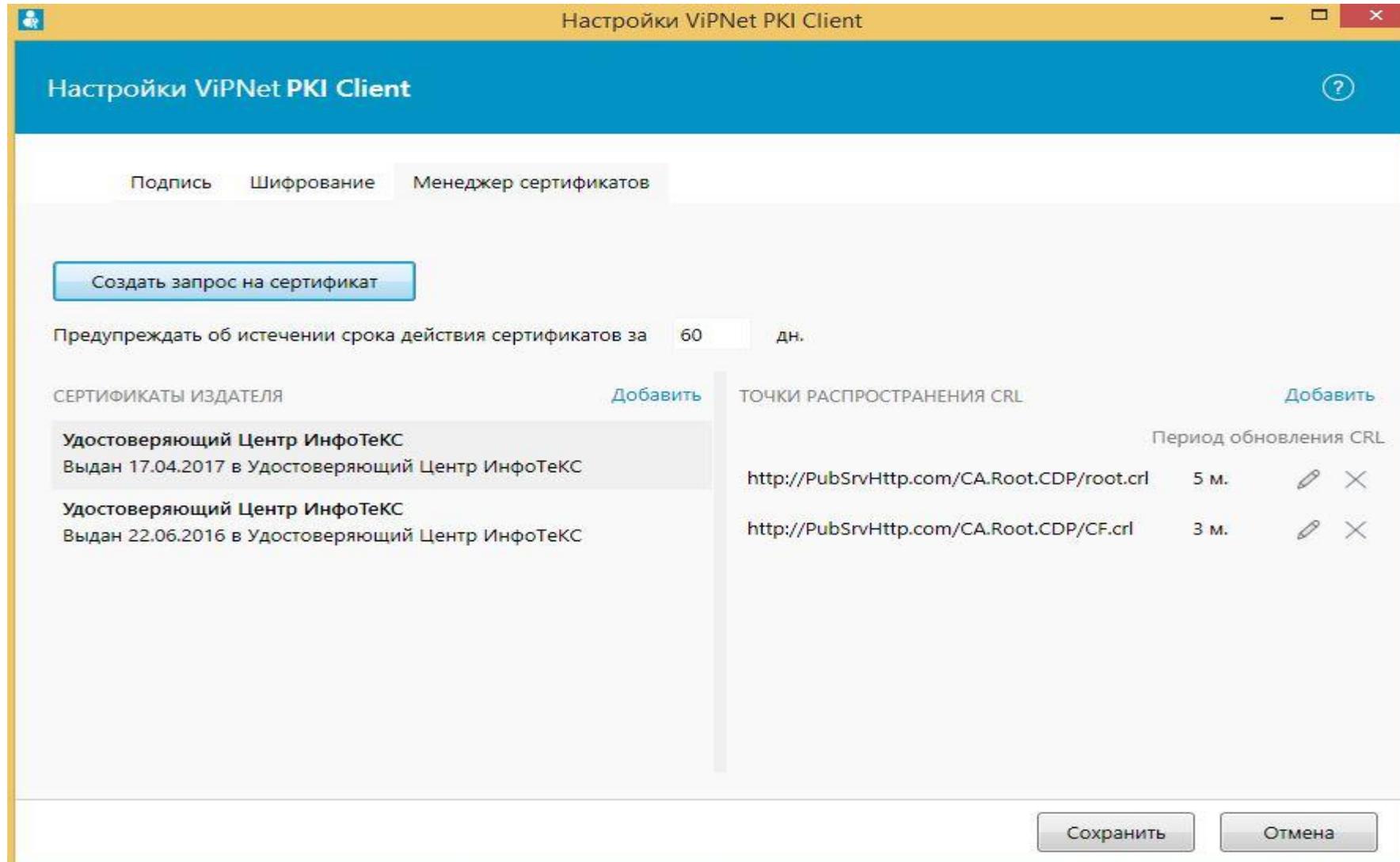
- Моя сеть — 12
 - Пользователи
 - Запросы на дистрибутивы ключей — 1
 - Сетевые узлы — 11
 - Группы узлов
 - Мастер-ключи
- Межсетевое взаимодействие —
 - Асимметричные мастер-ключи
 - 2943 - test

The right pane is titled "Сетевые узлы" and contains a table with columns: "Т...", "Имя узла /", "Ключи", and "CRL". The table has one row: "Центр регис..." with a value of "15" in the "CRL" column.

A context menu is open over the "Центр регис..." node. The menu items are:

- Открыть
- Создать и передать ключи в ЦУС Ctrl-F
- Создать и сохранить ключи в файл...
- Применить новый вариант ключей
- Передать CRL в ЦУС
- Сохранить CRL в файл...
- Выдать новый дистрибутив ключей...
- Пароль администратора ▶
- ✓ Получать текущий CRL

Реализация в PKI клиенте:



Обработка запроса на аккредитацию в

[О министерстве](#)[События](#)[Деятельность](#)[Документы](#)[Контакты](#)[Обращения граждан](#)[Eng](#)

Минкомсвязь России

[Написать в редакцию об ошибках](#)

[Деятельность](#) / [Государственные услуги](#) / [Государственные услуги Минкомсвязи](#)

Аккредитация удостоверяющих центров

Последнее обновление: 9 июня 2017

Список аккредитованных удостоверяющих центров

[Найдите ближайший удостоверяющий центр.](#)

Список аккредитованных организаций



Перечень аккредитованных удостоверяющих центров (по состоянию на 28.08.2017), XLS, 250,0 КБ



Перечень аккредитованных удостоверяющих центров, аккредитация которых приостановлена, XLS, 38,0 КБ



Перечень аккредитованных удостоверяющих центров, аккредитация которых досрочно прекращена, XLS, 33,5 КБ

[Список аккредитованных удостоверяющих центров](#)

[Список аккредитованных организаций](#)

[Описание услуги](#)

[Формы документов, необходимых для получения государственной услуги](#)

[Ответственные лица](#)

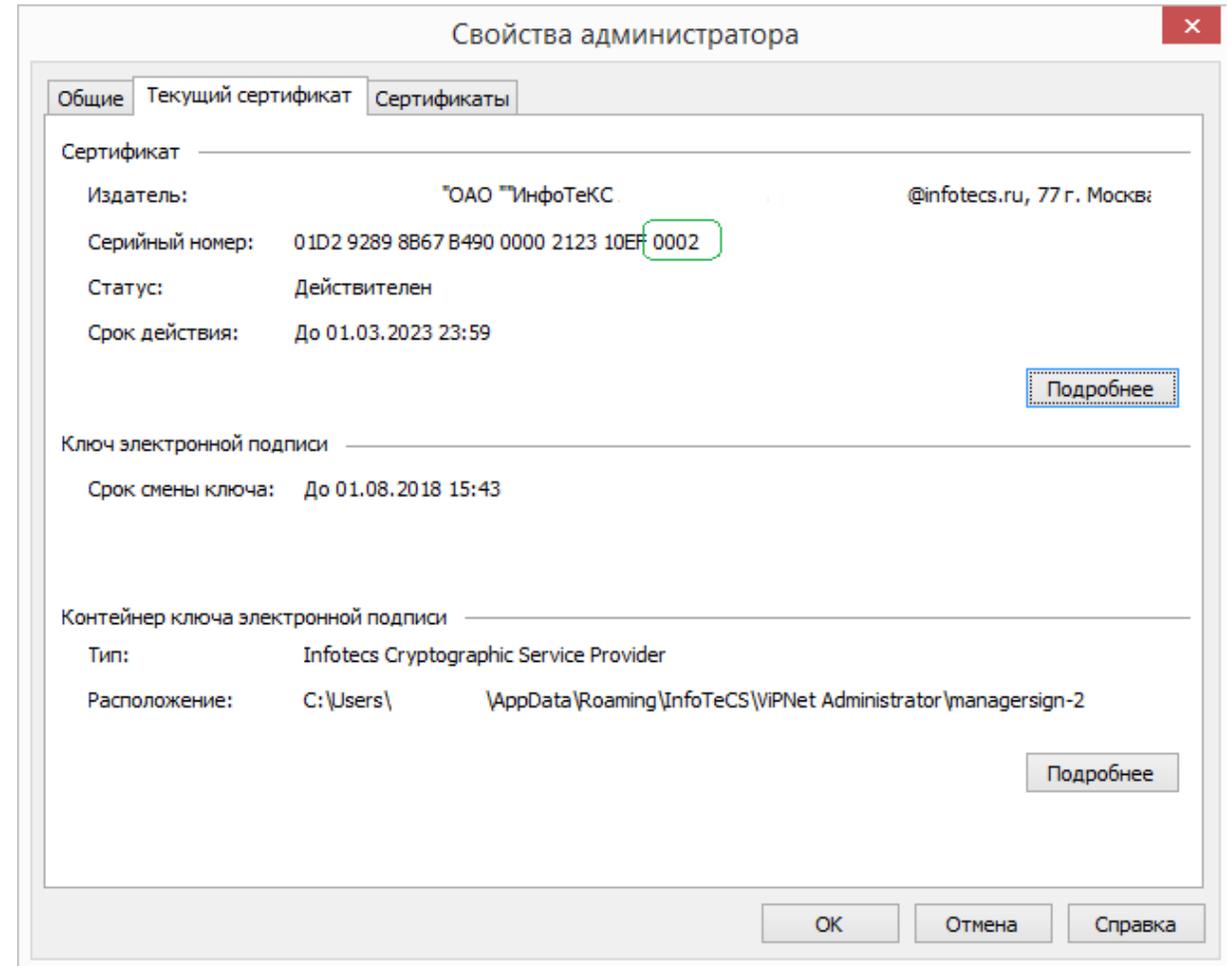
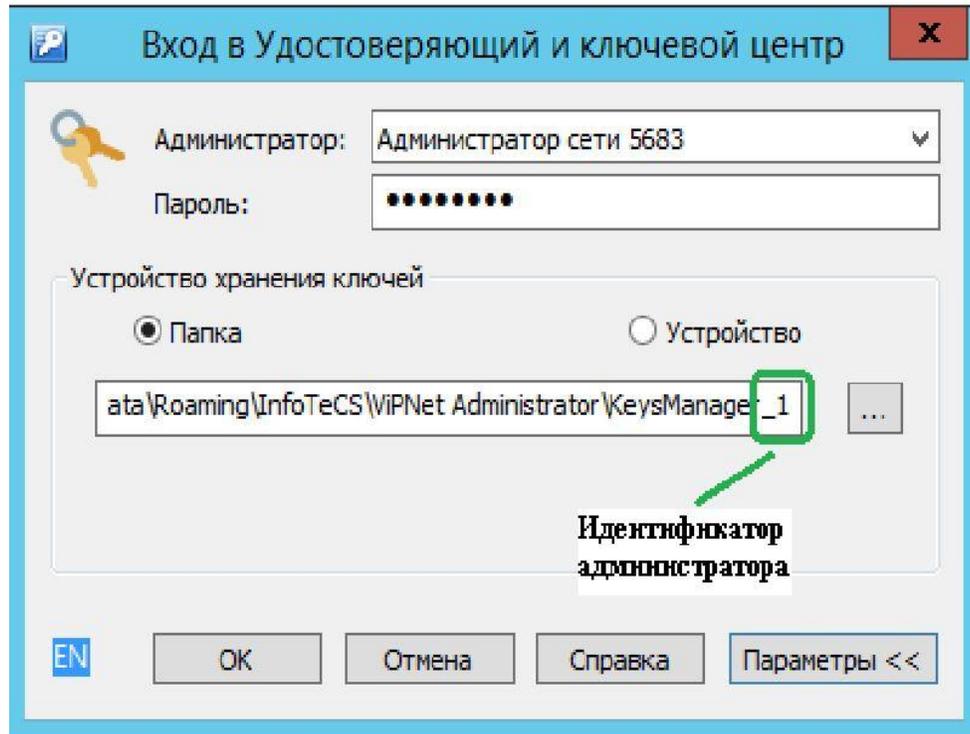
[Подать заявление через портал государственных услуг](#)

[События](#)

[Документы](#)

[Часто задаваемые вопросы](#)

Определение идентификатора для работы утилиты:

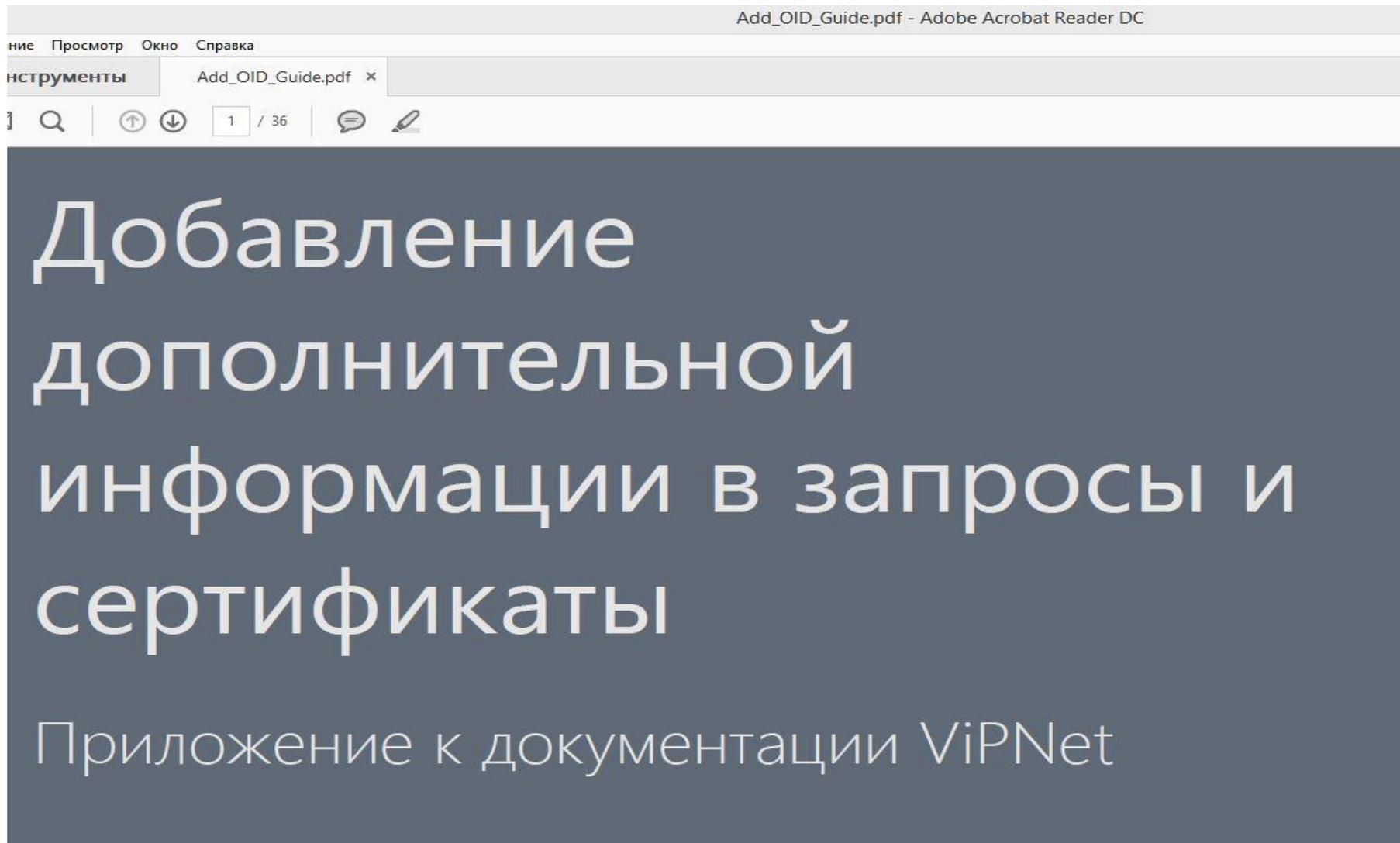


Дополнение по использованию групп узлов и пользователей:



/ из "Особенности преобразования связей при конвертации" документа "Руководство по обновлению с версии 3.2.x до версии 4.x"
/ (ViPNet_Administrator_Update_Guide_Ru.pdf)

Документ «Add_OID_Guide.pdf»:



Учитывать разрядность операционной системы:



2 В окне **Редактор реестра** на панели навигации создайте новый подраздел реестра в разделе:

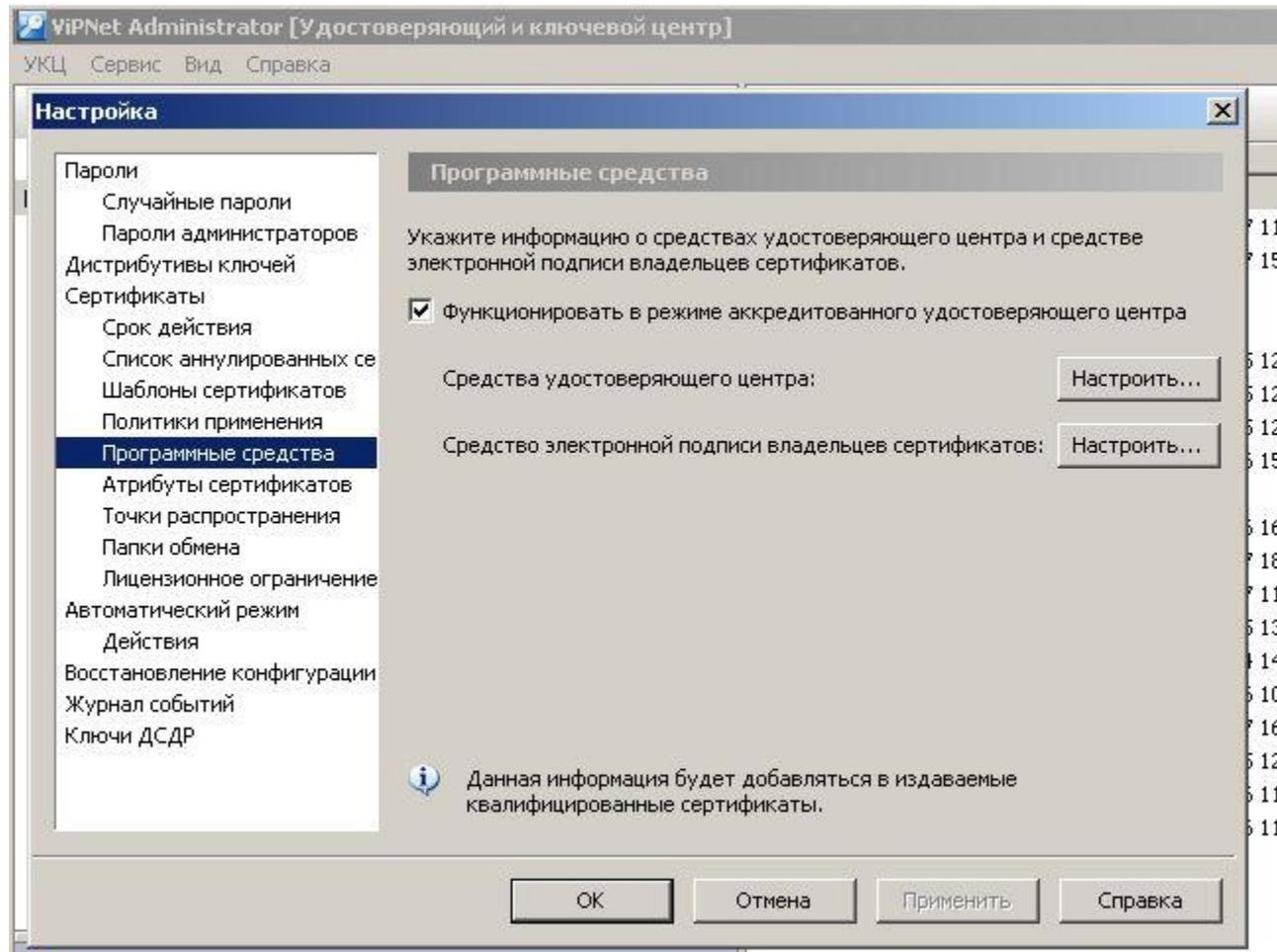
- \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo — при использовании 32-разрядной операционной системы Windows.
- \HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo и \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo — при использовании 64-разрядной операционной системы Windows.

Для создания нового подраздела:

2.1 На панели навигации правой кнопкой мыши щелкните по разделу `CryptDllFindOIDInfo` и в контекстном меню выберите пункт **Создать > Раздел**.

Введите название подраздела, состоящее из полного идентификатора объекта (например, для атрибута «Подпись пакетов информационного обмена между системами» —

Включение флага в настройках УКЦ:



Смена мастер-ключей:

ViPNet Administrator [Удостоверяющий и ключевой центр]

УКЦ Сервис Вид Справка

Ключевой центр

Моя сеть _____ **12**

- [-] Пользователи
- [-] Запросы на дистрибутивы ключей 1
- [-] Сетевые узлы 11
- [-] Группы узлов
- [-] **Мастер-ключи**

Межсетевое взаимодействие

- [-] Асимметричные мастер-ключи
- [-] 2943 - test

Мастер-ключи

Тип	Дата создания	Статус
[-] Мастер-ключ персональных ключей	14.05.2014 10:53	Действует
[-] Мастер-ключ ключей защиты	14.05.2014 10:53	Действует
[-] Мастер-ключ ключей обмена	14.05.2014 10:53	Действует

Сменить...

Вопросы?
Предложения?
Комментарии?