Обновление ПО ViPNet Administrator с версий 2.8.x до версий 3.1.x

Приложение к документации ViPNet CUSTOM 3.1

ViPNet
Virtual Private Network
infotecs

1991–2011 ОАО «Инфотекс», Москва, Россия

ФРКЕ.00006-04 90 08

Этот документ входит в комплект поставки программного обеспечения, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «Инфотекс».

ViPNet является зарегистрированной торговой маркой программного обеспечения, разрабатываемого ОАО «Инфотекс».

Все торговые марки и названия программ являются собственностью их владельцев.

ОАО «Инфотекс»

127287, г. Москва, Старый Петровско-Разумовский пр., дом 1/23, строение 1

Тел: (495) 737-61-96 (hotline), 737-61-92, факс 737-72-78

Сайт компании «Инфотекс»: http://www.infotecs.ru

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение **4**
О документе 5
Для кого предназначен документ 5
Соглашения документа 6
Используемые сокращения 6
Обратная связь 7
Дополнительная информация 7
Контактная информация 7

Глава 1. Обновление ПО ViPNet на СУ Администратора с версий 2.8.x до 3.1.x **8**
Подготовка к обновлению 9
Обновление ПО ViPNet Client 10
Обновление ПО ViPNet Administrator 11

Глава 2. Обновление сертификата пользователя, зарегистрированного на двух абонентских пунктах **22**
Постановка задачи 23
Для ViPNet Administrator версии 3.1 и ViPNet Client версии 3.0 (6.4059) 24
Обновление сертификата пользователя с помощью ЦУС 24
Обновление сертификата пользователя с помощью ПО ViPNet Client 35
Для ViPNet Administrator версии 3.1 и ViPNet Client версии 3.1 (2.6318) 42
Обновление сертификата пользователя с помощью ЦУС 42
Обновление сертификата пользователя с помощью ПО ViPNet Client 45

Введение

О документе 5

Обратная связь 7

О документе

Для кого предназначен документ

Настоящий документ описывает порядок обновления ПО ViPNet Administrator, установленного на АРМ Администраторов, с версии 2.8.x до 3.1.x, а также порядок обновления сертификата пользователя с использованием ПО ViPNet разных версий.

Документ предназначен для пользователя, имеющего квалификацию администратора сети ViPNet, т. е. обладающего знаниями и опытом в области конфигурирования, эксплуатации и управления сетью ViPNet.

Процесс обновления ПО ViPNet Administrator на АРМ Администраторов головной и подчиненных сетей идентичен и соответствует порядку, описанному в данном документе.

Обновление в сетях VPN производится согласно утвержденному графику.

Обновление ПО на АРМ Администраторов не затрагивает межсетевое взаимодействие, за исключением ограничений на модификацию сети VPN.

Внимание! Процедура обновления ПО ViPNet Administrator включает в себя не только обновление программного обеспечения непосредственно на АРМ Администратора, но и полное обновление ключей на всех сетевых узлах защищенной сети.

При этом в процессе обновления ПО межсетевые ключи не изменяются, что позволяет сохранить взаимодействие между узлами различных сетей.

При планировании работ по обновлению ПО ViPNet Администратор следует:

- проинформировать всех пользователей и администраторов сети о сроках проводимых работ;
- приостановить проведение работ, связанных с модификацией структуры защищенной сети (обработку импортов из других сетей, формирование и отправку экспортов в другие сети, регистрацию и удаление новых АП и СМ в сети и т. д);
- приостановить проведение работ по формированию и передаче пользователям дистрибутивов справочно-ключевой информации ПО ViPNet.

Соглашения документа

Соглашения данного документа представлены в таблице ниже.

Таблица 1. Условные обозначения

Указатель	Описание
	Внимание! Указывает на обязательное для исполнения или следования действие или информацию.
	Примечание. Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	Совет. Содержит дополнительную информацию общего характера.

Используемые сокращения

В данном документе используются следующие сокращения:

Сокращение	Термин
СУ	Сетевой узел
АП	Абонентский пункт
ЦУС	ViPNet Administrator Центр управления сетью
УКЦ	ViPNet Administrator Удостоверяющий и ключевой центр
ПО	Программное обеспечение
ПК	Программный комплекс
КД	Ключевой диск
КН	Ключевой набор
МК	Мастер-ключ
ММК	Межсетевой мастер-ключ
ИММК	Индивидуальный симметричный межсетевой мастер-ключ

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте компании «Инфотекс». По предложенным ссылкам можно найти ответы на многие вопросы, возникающие в процессе эксплуатации продуктов ViPNet.

- Описание комплекса ViPNet CUSTOM http://www.infotecs.ru/products/line/custom.php.
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Законодательная база в сфере защиты информации http://www.infotecs.ru/laws/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/vpn/.

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами компании «Инфотекс». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Электронный адрес службы поддержки hotline@infotecs.ru.
- Форма запроса по электронной почте в службу поддержки http://www.infotecs.ru/support/request/.
- 8 (495) 737-6196 — «горячая линия» службы поддержки.
- 8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

Обновление ПО ViPNet на СУ Администратора с версий 2.8.x до 3.1.x

Подготовка к обновлению 9

Обновление ПО ViPNet Client 10

Обновление ПО ViPNet Administrator 11

Подготовка к обновлению

Перед началом обновления:

1. Внимательно прочтите настоящую инструкцию. Для успешного обновления, во избежание проблем, необходимо строго выполнить последовательность указанных ниже действий.

Совет. В процедуре обновления целесообразно участие не менее двух человек, один из которых контролирует последовательность и корректность действий администратора безопасности, выполняющего обновление ПО ViPNet на СУ Администратора.

   Если результат операций по какому–либо разделу данной инструкции не соответствует указанному, не проводите дальнейших действий, так как это может привести к нарушению работоспособности всей защищенной сети. При возникновении ошибки приостановите дальнейшую работу и обратитесь в службу технической поддержки компании «Инфотекс».

2. Перед обновлением на СУ Администратора ПО ViPNet Client версии 2.8.x рекомендуется предварительно удалить ПО ViPNet Client версии 2.8.x с сохранением пользовательских файлов при деинсталляции.

3. Перед обновлением ПО ViPNet Administrator до версии 3.1 на всех СУ (кроме СУ Администратора) следует обновить ПО ViPNet Client и ViPNet Coordinator до версии 3.1 (2.6318) или выше. Это позволит сохранить работоспособность СУ и в дальнейшем решить проблему с запретом смены пароля на них.

Внимание! Если для связи с другими сетями ViPNet используются не индивидуальные симметричные межсетевые мастер-ключи (ИММК), то перед обновлением ПО ViPNet Administrator необходимо осуществить переход на использование ИММК.

Обновление ПО ViPNet Client

Внимание! Перед обновлением на СУ Администратора ПО ViPNet Client версии 2.8.x следует предварительно удалить ПО ViPNet Client версии 2.8.x с сохранением пользовательских файлов при переустановке.

Для обновления ПО ViPNet Client на СУ Администратора:

1. Сделайте резервную копию содержимого папки, в которой установлено ПО ViPNet Administrator версии 2.8 (рекомендуется полностью сохранить каталог `InfoTeCS`).
2. Проверьте наличие во вложенной папке `SS\Station\abn_AAAA` файла `AAAA.pk`, где `AAAA` — 16-ричный идентификатор пользователя в защищенной сети. Если этот файл отсутствует, перенесите его в указанную подпапку.
3. Выполните обновление ПО ViPNet Client на СУ Администратора с версии 2.8 до версии 3.1 (2.XXXX) путем запуска соответствующей программы установки.
4. Выполните проверку функционирования ПО ViPNet Client.
5. Проверьте защищенное соединение с узлами, с которыми связан СУ Администратора.

Внимание! Если связь не проверяется, приостановите обновление. Восстановите ПО ViPNet Client из резервной копии и повторите действия, указанные в п. 2.

Обновление ПО ViPNet Administrator

Внимание! Приведенные ниже действия описывают обновление ПО ViPNet Administrator ЦУС и УКЦ, установленного на одном сетевом узле.

Для обновления ПО ViPNet Administrator на СУ Администратора:

1. Создайте папку и перенесите в нее все файлы `*.pk` из вложенной папки `KC\P_KEYS` папки установки ПО ViPNet Administrator. Подпапка `KC\P_KEYS` должна стать пустой.

   Эти файлы могут потребоваться в том случае, если они не были переданы на какой-либо СУ.

2. Запустите программу установки ПО ViPNet Administrator версии 3.1.1.

   Появится окно с сообщением о том, что обнаружена установленная ранее версия ПО ViPNet Administrator.

   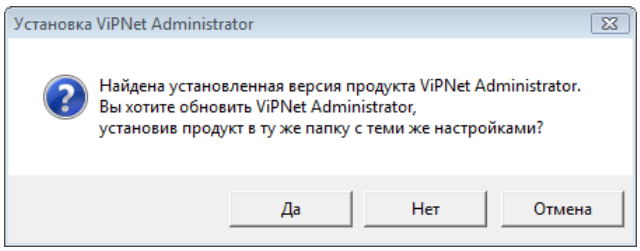

   Рисунок 1: Сообщение о наличии ранее установленного ПО

3. Чтобы начать немедленное обновление ПО, нажмите кнопку **Да**. Для запуска мастера установки нажмите кнопку **Нет**.

4. Дождитесь завершения процесса обновления.

5. Перезагрузите компьютер.

6. Запустите УКЦ и следуйте указаниям мастера первичной инициализации.

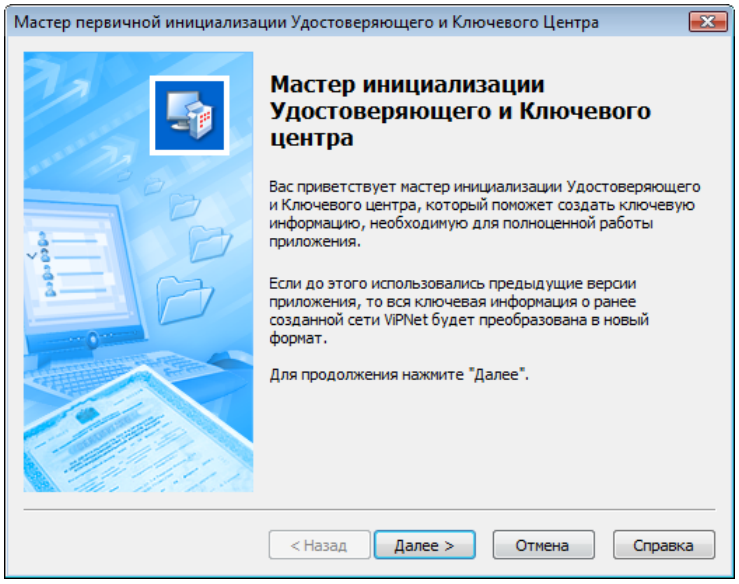

Рисунок 2: Стартовая страница мастера первичной инициализации УКЦ

Внимание! Ниже приведены действия, которые необходимо выполнить на отдельных страницах мастера. На остальных страницах рекомендуется оставить значения, предлагаемые по умолчанию. По завершении процесса обновления ПО эти значения можно изменить в настройках УКЦ.

Обратите особое внимание на следующие страницы мастера:

6.1 На странице **Выбор драйвера ODBC** выберите **Microsoft Access Driver (*.mdb)**.

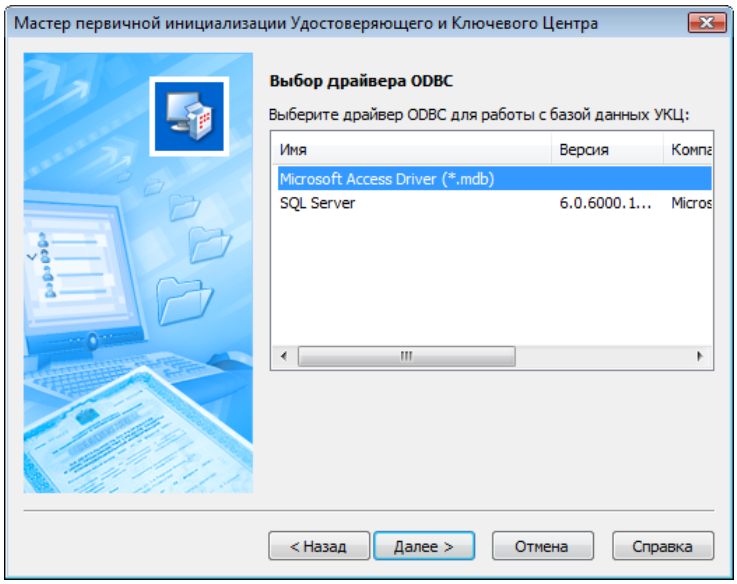

Рисунок 3: Страница выбора драйвера ODBC

6.2 На странице **Назначение администратора сети ViPNet** выберите пользователя (из числа зарегистрированных на данном АП), который будет выполнять функции администратора УКЦ.

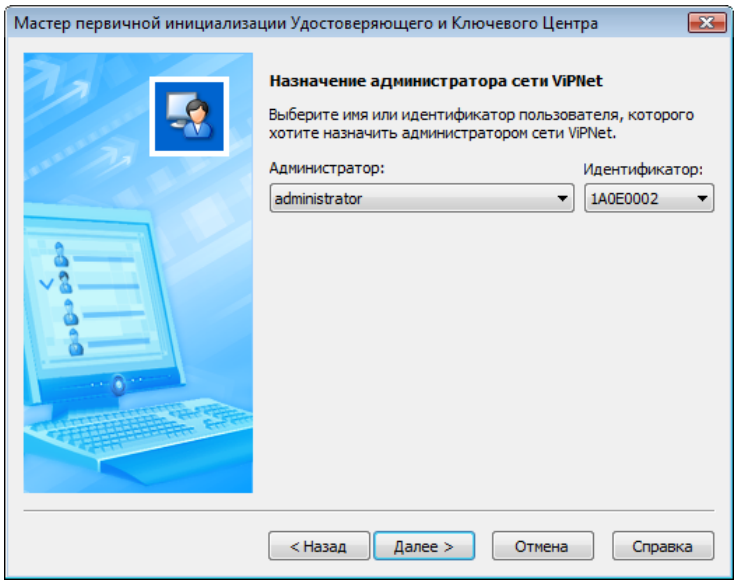

Рисунок 4: Страница выбора администратора сети ViPNet

6.3 На странице **Пароль администратора сети ViPNet** выберите тип пароля для входа в УКЦ.

Рекомендуется выбрать тип **Собственный**.

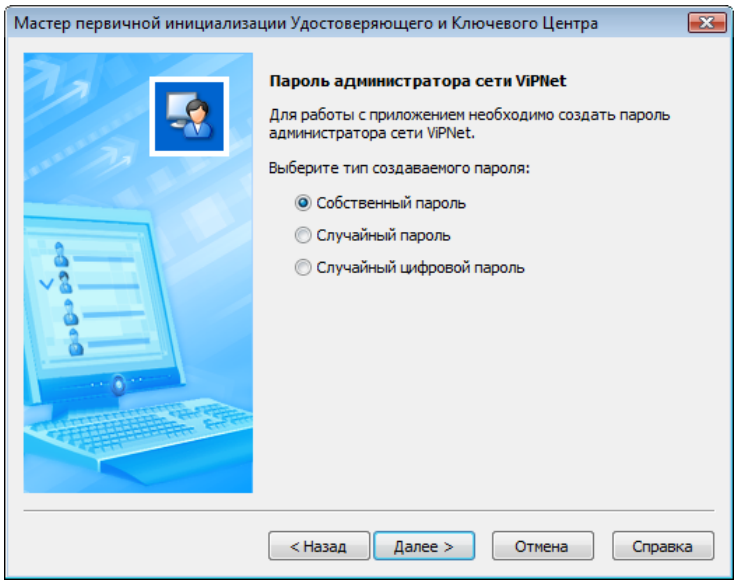

Рисунок 5: Страница выбора типа пароля администратора

Внимание! Запомните или запишите пароль! Без предварительного ввода пароля запуск УКЦ с текущей ключевой информацией невозможен.

6.4 На странице **База данных предыдущей версии УКЦ** в обязательном порядке установите флажок **Перенести ключевую информацию из обнаруженной базы данных в новую**.

Внимание! Если данное действие не будет выполнено, существующая ключевая информация будет проигнорирована. Это приведет к нарушению работоспособности сети, так как невозможно будет произвести обновление ключевой информации на сетевых узлах.

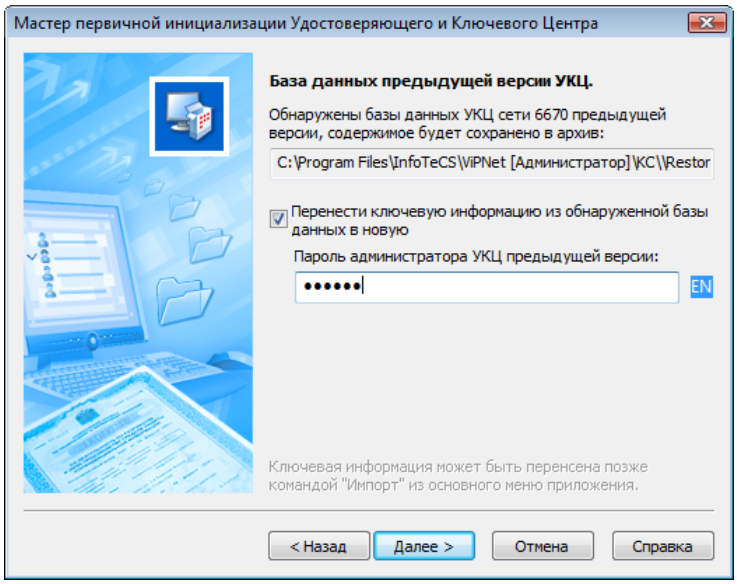

Рисунок 6: Страница выбора параметров работы с базой данных предыдущей версии УКЦ

7 Убедитесь в том, что по завершении работы мастера первичной инициализации запустился УКЦ.

8 Проверьте список отозванных сертификатов своей сети. Для этого:

8.1 В левой части главного окна УКЦ перейдите к разделу **Удостоверяющий центр** > **Списки отозванных сертификатов** > **Своя сеть ViPNet**.

8.2 Выделите запись с информацией о списке отозванных сертификатов (СОС) и выполните для нее команду контекстного меню **Проверить**. Если СОС не действителен, обновите его, но не формируйте при этом обновлений!

9 Создайте пароль администратора сетевой группы.

Внимание! Пароль администратора сетевой группы, который был задан в УКЦ версии 2.8, не переносится в УКЦ версии 3.1, поэтому пароль необходимо создать заново.

Пароль администратора сетевой группы не является паролем для входа администратора в УКЦ.

Для этого:

9.1 В левой части главного окна УКЦ перейдите к разделу **Ключевой центр** > **Своя сеть ViPNet** > **Сетевые группы**.

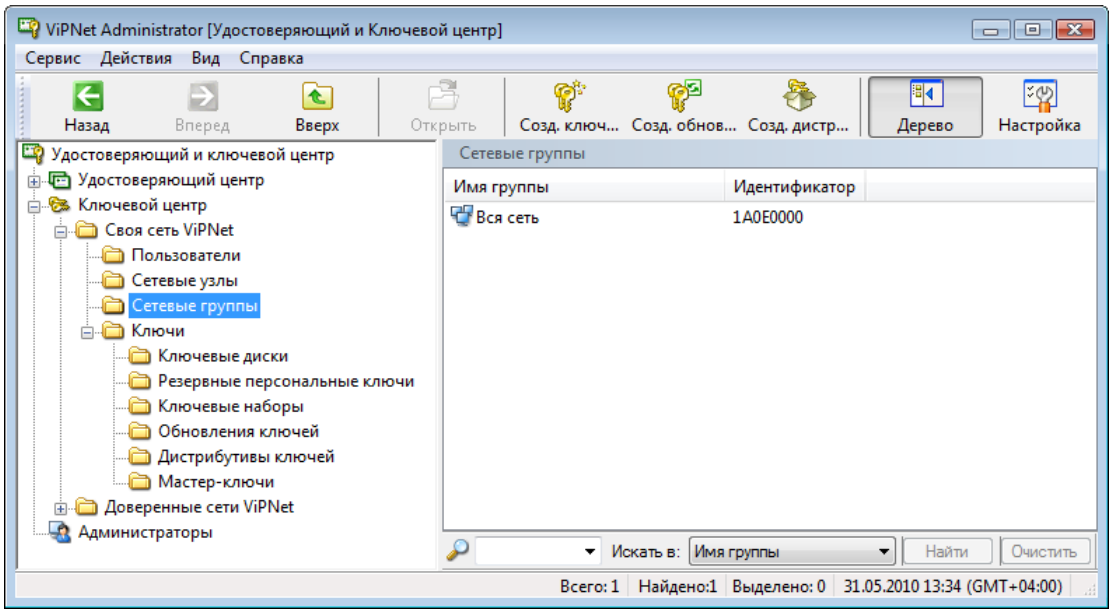

Рисунок 7: Просмотр параметров сетевых групп в УКЦ

9.2 Выполните двойной щелчок мыши по группе **Вся сеть**, после чего в появившемся окне **Свойства сетевой группы** перейдите на вкладку **Пароль администратора**.

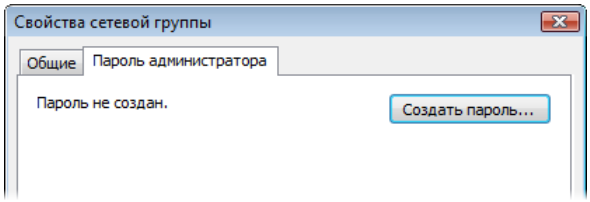

Рисунок 8: Просмотр пароля администратора

9.3 Нажмите кнопку **Создать пароль**.

9.4 В выпадающем списке появившегося окна задайте тип пароля.

Совет. Рекомендуется использовать тип **Случайный**.

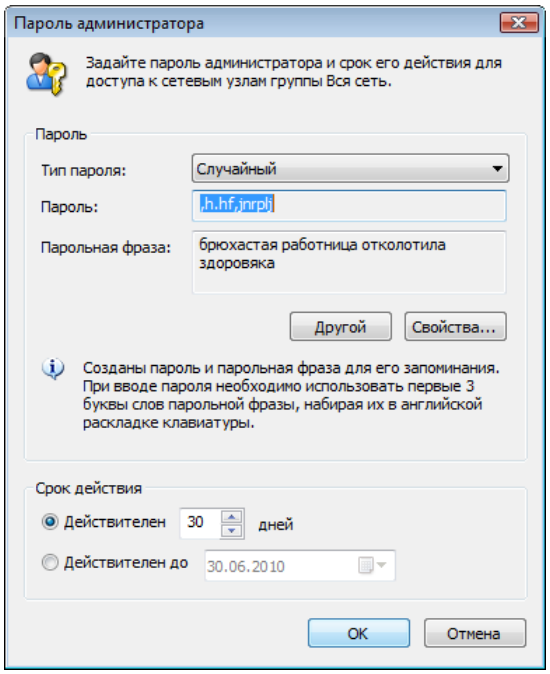

Рисунок 9: Указание пароля администратора и срока действия пароля

9.5 В группе параметров **Срок действия** определите продолжительность действия данного пароля.

Максимальный срок действия пароля администратора сетевых узлов составляет 365 дней.

10 Завершите работу программы УКЦ.

11 Запустите ЦУС.

12 Выберите в ЦУС меню **Службы** и в нем команду **Сформировать все справочники**.

13 Скопируйте из ЦУС в УКЦ справочники для всех пользователей. Для этого выберите меню **Службы**, в нем команду **Справочники для УКЦ**, а затем — **Справочники связей пользователей**.

14 Скопируйте из ЦУС в УКЦ справочники для всех СУ. Для этого выберите меню **Службы**, в нем команду **Справочники для УКЦ**, а затем — **Справочники связей сетевых узлов**.

Внимание! Если в вашей сети есть координаторы с Linux-версией, скопируйте из ЦУС в УКЦ справочники для таких координаторов с помощью команды меню **Службы** > **Справочники для УКЦ** > **Дистрибутивы** > **Полный объём**. При

этом категорически не рекомендуется копировать справочники дистрибутивов для других узлов.

15 Запустите УКЦ.

16 Прежде чем начать создание ключевых дисков (КД), обязательно выполните следующие действия:

- В меню **Сервис** выберите пункт **Настройки**.
- Если при создании КД будут формироваться новые пароли пользователей СУ, в окне **Настройка** в разделе **Пароли** выполните настройку параметров создаваемых паролей.
- Чтобы издание новых сертификатов пользователей при формировании КД происходило в автоматическом режиме, в окне **Настройка** в разделе **Сертификаты** установите флажок **На сертификаты, подписанные пользователями**.

17 Создайте ключевые диски для всех пользователей. Для этого в левой части главного окна УКЦ перейдите к разделу **Ключевой центр** > **Своя сеть ViPNet** > **Пользователи**, после чего выберите всех пользователей и выполните для них команду контекстного меню **Ключевой диск** > **Создать**. При создании ключевых дисков рекомендуется не изменять пароли пользователей.

Внимание! Создание ключевых дисков должно производиться только один раз! Если для СУ будет создано два и более КД, после обновления ключевой информации связь с данным узлом будет потеряна.

18 Сформируйте ключевые наборы (КН) для всех узлов. Для этого в УКЦ выберите меню **Сервис**, в нем команду **Автоматически создать**, а затем — **Ключевые наборы**.

Внимание! Если в вашей сети есть координаторы с Linux-версией, в левой части главного окна УКЦ перейдите к разделу **Ключевой центр** > **Своя сеть ViPNet** > **Сетевые узлы**. Выберите координаторы с Linux-версией и выполните для них команду контекстного меню **Дистрибутивы ключей** > **Создать**.

Внимание! Если до выполнения следующего пункта вы считаете, что допустили какие-либо ошибки, то следует удалить новую версию ViPNet Administrator, восстановить сохраненную копию версии 2.8 и повторить все действия настоящей

инструкции.

После выполнения п. 19 ключевая информация будет отправлена на узлы защищенной сети! Если в ходе выполнения предыдущих пунктов были допущены ошибки, то после наступления времени обновления работоспособность защищенной сети может быть нарушена!

Восстановление функционирования сети будет возможно только с использованием ключевых дистрибутивов, сформированных в ПО ViPNet Administrator версии 3.1.

19 Перенесите КД всех пользователей и КН всех сетевых узлов из УКЦ в ЦУС. Для этого:

- В левой части главного окна УКЦ перейдите к разделу **Ключевой центр** > **Своя сеть ViPNet** > **Ключи** > **Ключевые диски**, после чего выберите всех пользователей и выполните для них команду контекстного меню **Перенести в ЦУС**.
- В левой части главного окна УКЦ перейдите к разделу **Ключевой центр** > **Своя сеть ViPNet** > **Ключи** > **Ключевые наборы**, после чего выберите все СУ и выполните для них команду контекстного меню **Перенести в ЦУС**.

Внимание! Из УКЦ перенесите DST-файлы для координаторов с Linux-версией в папку на жестком диске. Для этого выполните одно из действий:

- В левой части главного окна перейдите к разделу **Ключевой центр** > **Своя сеть ViPNet** > **Ключи** > **Ключевые дистрибутивы**, выберите все дистрибутивы и выполните для них команду контекстного меню **Перенести в ЦУС**.
- Создайте в папке установки ПО ViPNet Administrator вложенную папку `\FOR_NCC\DST` и скопируйте в нее вручную DST-файлы для координаторов с Linux-версией.

20 Перейдите в программу ЦУС.

21 Подтвердите запросы об отправке поступившей ключевой информации, после чего в списке узлов защищенной сети выберите все узлы.

22 В появившемся окне с параметрами даты и времени отправки обновлений:

- Задайте отложенную дату. Это гарантирует получение обновлений ключевой информации всеми узлами защищенной сети до вступления этих обновлений в действие.

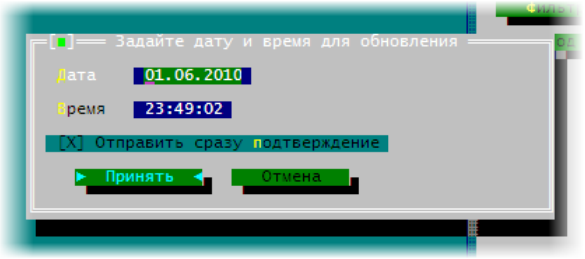

Рисунок 10: Указание в ЦУС даты и времени отправки обновлений

Рекомендуется указывать дату, на 2 дня (или более) превосходящую текущую дату. Установите дату ближайшего выходного дня (субботы или воскресенья) — если работа по обновлению проводится не позднее среды.

В течение рабочих дней до указанного выходного дня все узлы сети, на которых установлено ПО ViPNet Client или ViPNet Coordinator, должны функционировать, причем ПО ViPNet должно быть запущено хотя бы один раз. Это необходимо для того, чтобы файлы обновлений поступили на узел.

- Установите флажок **Отправить сразу подтверждение**. В данном случае вместе с отправкой обновления произойдет отправка подтверждения обновления.

Внимание! До наступления назначенной даты обновления администраторам безопасности сетей следует:

- Контролировать в ЦУС в базе запросов и ответов процесс получения обновлений всеми сетевыми узлами, особенно координаторами.
- Если какие-либо узлы защищенной сети не получат обновления до назначенной даты, то после обновления ключей на других СУ связь с ними будет утеряна. В этом случае связь может быть восстановлена только вручную с помощью дистрибутива справочно-ключевой информации (dst-файла), сформированного в ПО ViPNet Administrator версии 3.1.
- Не изменять конфигурацию сети с помощью ЦУС (а именно не выполнять регистрацию СУ, пользователей, удаление СУ, изменение связей и т. д.) и не рассылать обновления.
- Не обрабатывать импорт, полученный из других сетей.
- Не отправлять экспорт в другие сети.

---

23 При наступлении назначенной даты на включенных узлах обновления вступят в силу. При этом между включенными узлами установится связь на основе новых ключей.

На узлах, которые будут включены в первый рабочий день (или позднее) после назначенной даты, через 1–7 минут после включения и запуска ПО ViPNet произойдет обновление ключей и установится связь со всеми другими узлами сети, получившими и принявшими обновление.

При этом связь с узлами других защищенных сетей ViPNet сохранится, так как межсетевые ключи не изменятся.

Внимание! Если на СУ предупреждение об обновлении ключевой информации появилось в момент, когда запущена программа «Деловая почта», следует закрыть все файлы, открытые из вложений корреспонденции, завершить работу «Деловой почты» и выполнить прием обновления.

24 При появлении окна с предложением указать путь к файлу с резервным набором персональных ключей (имеется в виду файл `AAAA.pk`, где AAAA — 16-ричный идентификатор пользователя в защищенной сети) укажите путь к папке, в которой расположен данный файл.

2

Обновление сертификата пользователя, зарегистрированного на двух абонентских пунктах

Постановка задачи	23
Для ViPNet Administrator версии 3.1 и ViPNet Client версии 3.0 (6.4059)	24
Для ViPNet Administrator версии 3.1 и ViPNet Client версии 3.1 (2.6318)	42

Постановка задачи

В данном разделе описана процедура формирования и получения обновлений ключевой информации для пользователя сети ViPNet, обладающей следующими характеристиками:

- Пользователь User_1 зарегистрирован на абонентских пунктах АП1 и АП2.

  Причем, тип коллектива АП1 является главным для этого пользователя.

- Сертификат и персональные ключи пользователя User_1 совпадают на обоих АП, на которых он зарегистрирован.

- Пользователь User_2 зарегистрирован на АП2.

Действия, которые необходимо выполнить для передачи и получения обновлений, зависят от версий ПО ViPNet, используемого на сетевом узле администратора и на абонентских пунктах. В данном разделе приведено описание действий для продуктов следующих версий:

- ViPNet Administrator версии 3.1 и ViPNet Client версии 3.0 (6.4059);

- ViPNet Administrator версии 3.1 и ViPNet Client версии 3.1 (2.6318).

Для того чтобы просмотреть версию ПО ViPNet:

1 Выберите меню **Справка** и в нем команду **О программе**.

2 В верхней части открывшегося окна просмотрите номер версии программы.

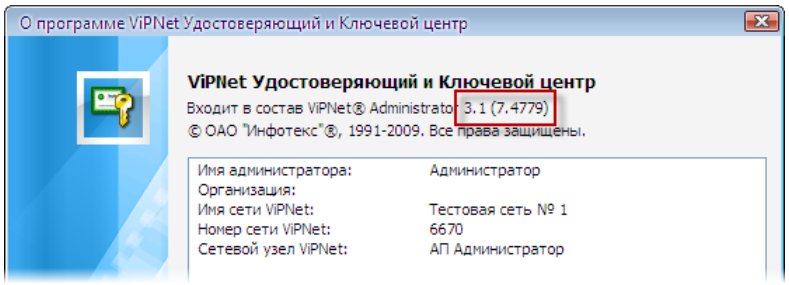

Рисунок 11: Определение версии продукта

Для ViPNet Administrator версии 3.1 и ViPNet Client версии 3.0 (6.4059)

Обновление сертификата пользователя с помощью ЦУС

При обновлении сертификата пользователя с помощью программы ViPNet Administrator Центр управления сетью (далее — ЦУС) это обновление передается на АП в составе ключевой дискеты (КД).

Процедура обновления КД пользователя, зарегистрированного на двух АП (в данном случае — пользователя User_1), выполняется следующим образом:

1. Администратор формирует обновление в программах ЦУС и ViPNet Administrator Удостоверяющий и ключевой центр (далее — УКЦ).
2. Администратор отправляет по сети сформированное обновление.

Примечание. Обновление будет отправлено на тот АП, ТК которого является главным для пользователя (в данном случае — на АП1).

3. Пользователь User_1 принимает обновление с помощью ПО ViPNet Client.
4. Пользователь вручную передает информацию о сертификатах и ключах подписи с АП1 на другой АП (в данном случае — на АП2), на котором он также зарегистрирован. Автоматическая передача не возможна, поскольку тип коллектива АП2 не является главным для пользователя (см. «Постановка задачи» на стр. 23).

Для обновления сертификата пользователя User_1 с помощью ЦУС:

1. В программе ЦУС, используемой на сетевом узле Администратора:

1.1 Выполните команду меню **Службы** > **Справочники для УКЦ** > **Справочники связей пользователей**.

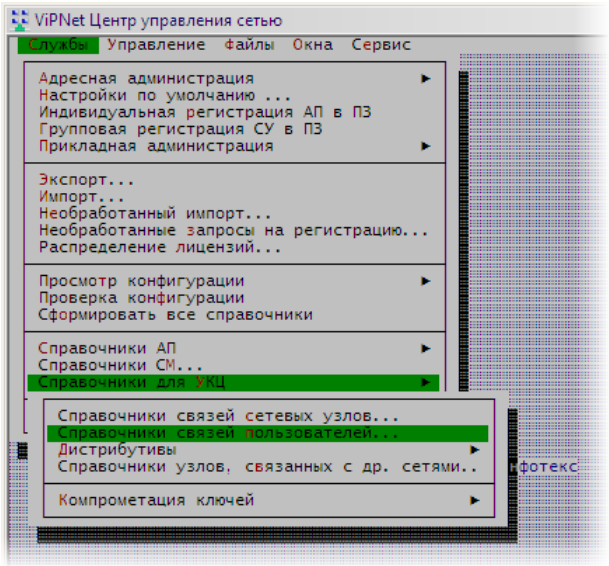

Рисунок 12: Копирование справочников связей пользователя

1.1 В появившемся окне выберите пользователя, сертификат которого необходимо обновить (в данном случае — User_1), после чего нажмите кнопку **Копировать**.

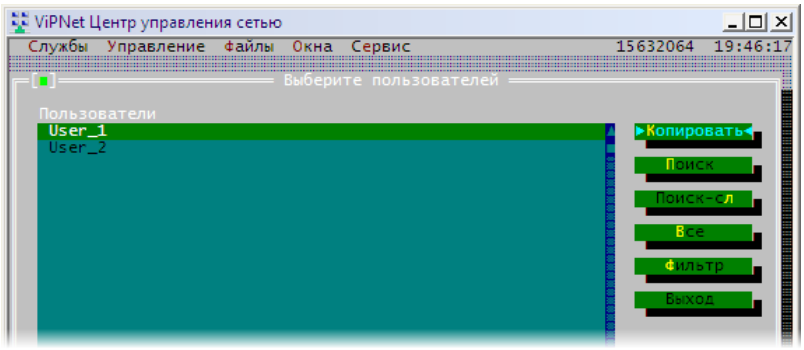

Рисунок 13: Выбор пользователя

1.2 При появлении диалогового окна с сообщением об успешном копировании справочников нажмите любую клавишу.

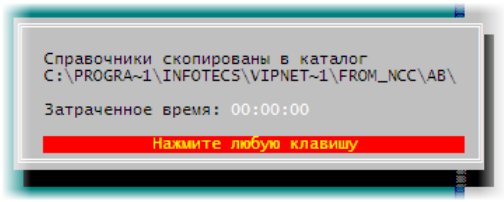

Рисунок 14: Диалоговое окно ЦУС

2 В программе УКЦ, используемой на сетевом узле Администратора:

2.1 В главном окне перейдите к разделу **Ключевой центр** > **Своя сеть ViPNet** > **Пользователи**.

2.2 На правой панели выберите пользователя (в данном случае — User_1), КД которого необходимо обновить.

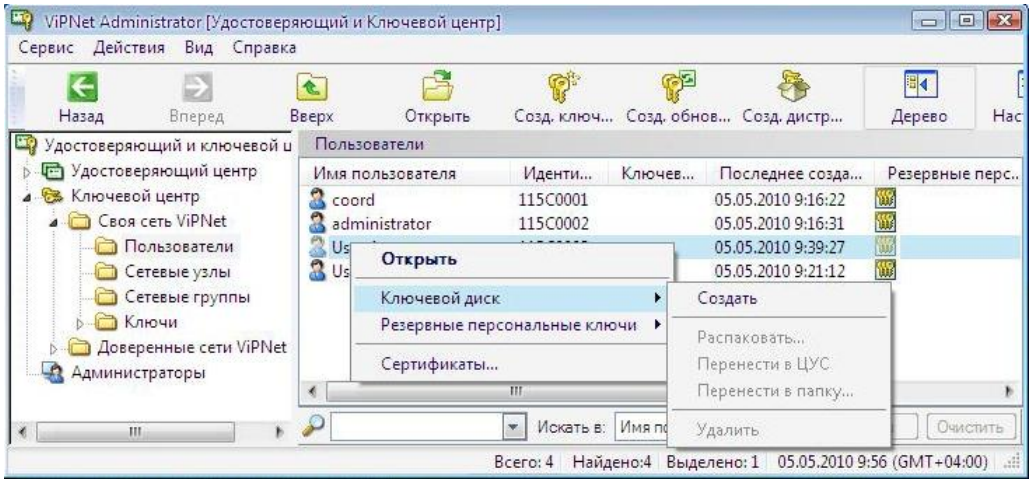

Рисунок 15: Создание КД для пользователя

2.3 При появлении электронной рулетки поводите указателем мыши в пределах появившегося окна.

Примечание. В случае, если в рамках текущей сессии электронная рулетка уже была запущена, данное окно не появится.

2.4 В окне с предложением ввести новый пароль:

- При необходимости сменить пароль для КД нажмите кнопку **Да**, после чего введите новый пароль.
- При необходимости сохранения прежнего пароля нажмите кнопку **Нет**.

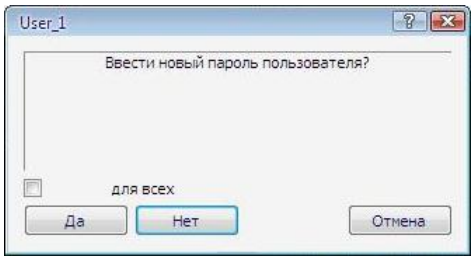

Рисунок 16: Смена пароля пользователя

2.5 На странице **Сведения о владельце сертификата** мастера редактирования полей сертификата укажите и (или) измените информацию о пользователе, для которого формируется обновление информации.

- Если требуется дальнейшее редактирование полей сертификата, нажмите кнопку **Далее** и перейдите к действию 2.6.
- Если информацию редактировать не требуется, нажмите кнопку **Готово** и перейдите к действию 2.10.

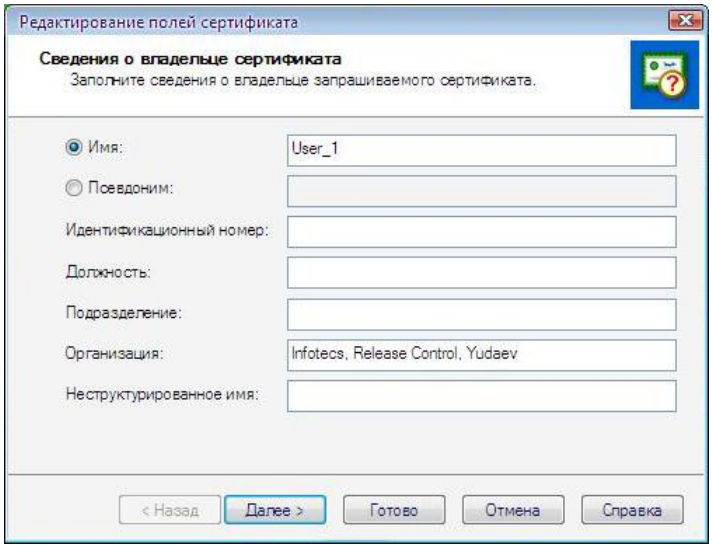

Рисунок 17: Редактирование сведений о владельце сертификата

2.6 На второй странице **Сведения о владельце сертификата** укажите и (или) измените контактные данные пользователя:

- Если требуется дальнейшее редактирование полей сертификата, нажмите кнопку **Далее** и перейдите к действию 2.7.

- Если информацию редактировать не требуется, нажмите кнопку **Готово** и перейдите к действию 2.10.

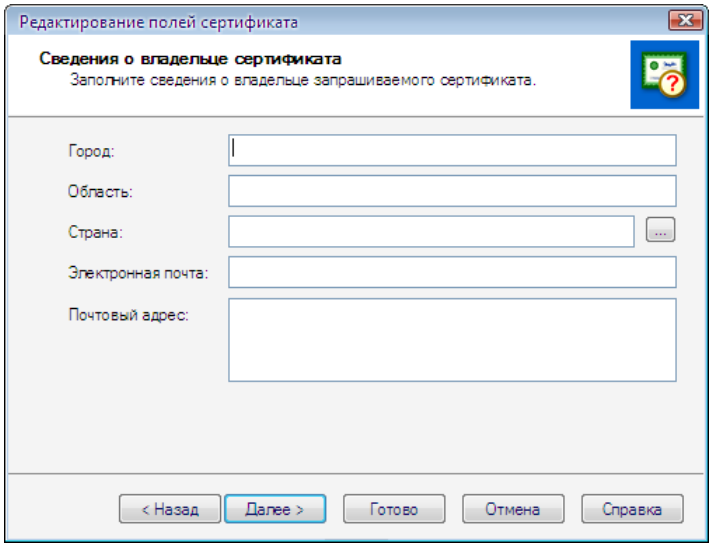

Рисунок 18: Редактирование контактных данных владельца сертификата

2.7 На третьей странице **Сведения о владельце сертификата** убедитесь в правильности сведений, указанных на предыдущих страницах мастера. При необходимости, отредактируйте в окне, вызываемом с помощью кнопки **Изменить**.

- Если требуется дальнейшее редактирование полей сертификата нажмите кнопку **Далее** и перейдите к действию 2.8.

- Если информацию редактировать не требуется, нажмите кнопку **Готово** и перейдите к действию 2.10.

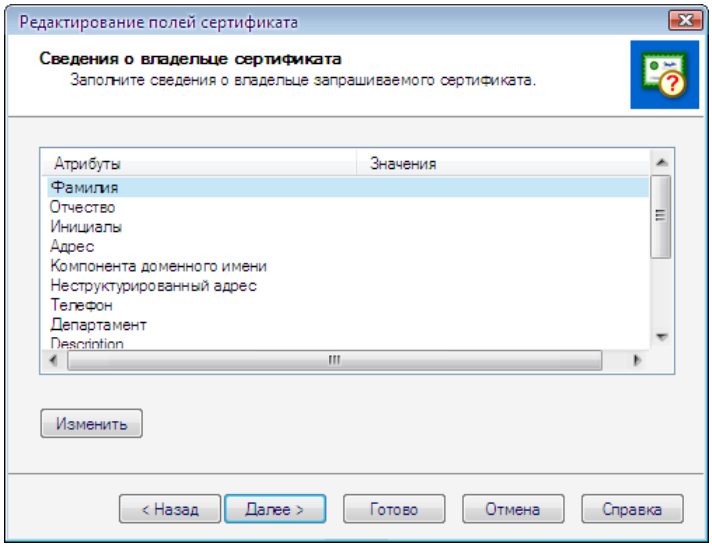

Рисунок 19: Проверка сведений о владельце сертификата

2.8 На странице **Срок действия сертификата** задайте желаемый срок действия сертификата удобным для Вас способом.

- Если требуется дальнейшее редактирование полей сертификата, нажмите кнопку **Далее** и перейдите к действию 2.9.
- Если информацию редактировать не требуется, нажмите кнопку **Готово** и перейдите к действию 2.10.

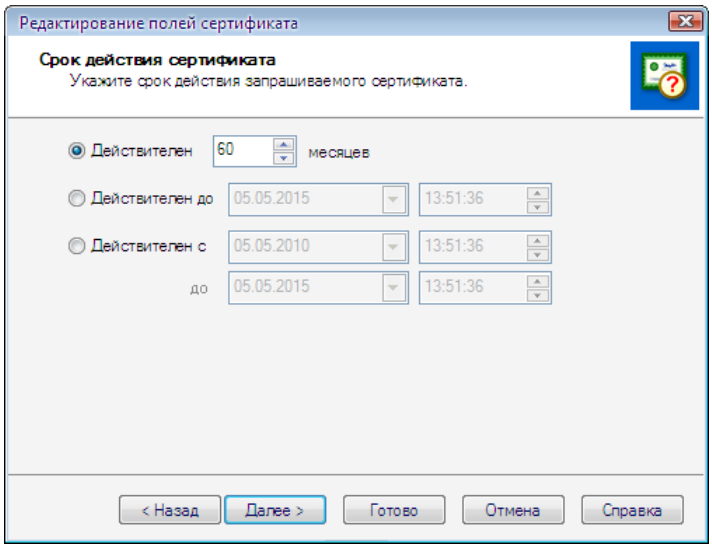

Рисунок 20: Указание желаемого срока действия сертификата

2.9 На странице **Назначения сертификата**:

- Задайте длину цепочки сертификатов. Для этого выберите пункт **Основные ограничения**, после чего нажмите кнопку **Изменить** и задайте в появившемся окне **Основные ограничения** нужное значение.
- Измените функции ключа. Для этого выберите пункт **Использование ключа**, после чего нажмите кнопку **Изменить** и исключите в окне **Использование ключа** ненужные функции.
- Расширьте функциональность ключа. Для этого нажмите кнопку **Добавить**, после чего в появившемся окне выберите нужное расширение (**Расширенное использование ключа** или **Политики безопасности**) и нажмите кнопку **ОК**. Появится окно настроек, соответствующее выбранному расширению.
- Признайте то или иное расширение критическим. Для этого выберите нужный пункт и установите (снимите) флажок **Расширение является критическим**.

Примечание. Если критическое расширение оказывается не распознанным и не обработанным прикладным ПО, то сертификат признается недействительным.

- Для завершения работы с мастером редактирования полей сертификата нажмите кнопку **Готово**.

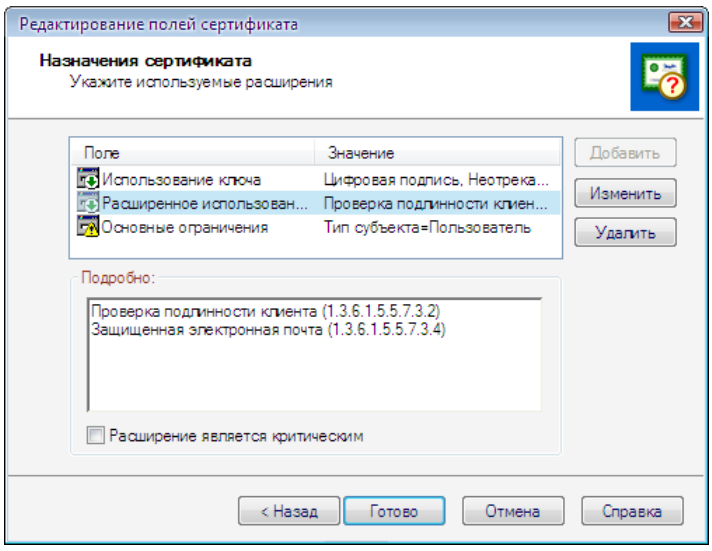

Рисунок 21: Редактирование назначений сертификата

2.10 В появившемся диалоговом окне **Создание ключевых дисков пользователей** нажмите кнопку **ОК**.

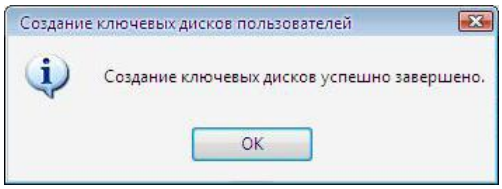

Рисунок 22: Диалоговое окно с сообщением об успешном создании КД

2.11 В главном окне перейдите к разделу **Ключевой центр** > **Своя сеть ViPNet** > **Ключи** > **Ключевые диски**.

2.12 На правой панели выберите пользователя, для которого сформирована КД (в данном случае — User_1), и выполните команду контекстного меню **Перенести в ЦУС**.

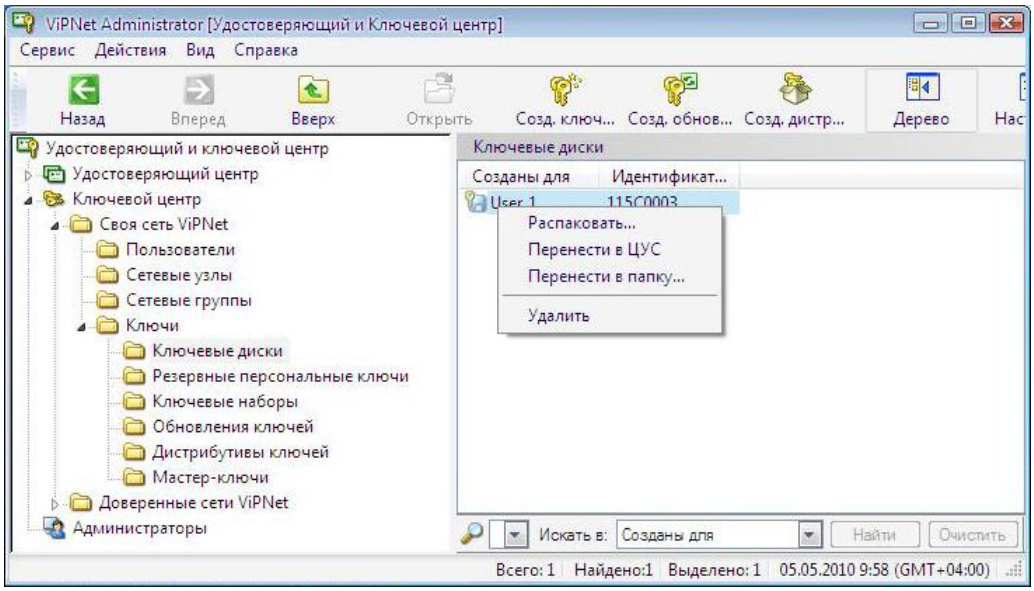

Рисунок 23: Передача КД из УКЦ в ЦУС

3 В программе ЦУС, используемой на сетевом узле Администратора:

3.1 При появлении окна с вопросом об отправке ключей нажмите кнопку **Да**.

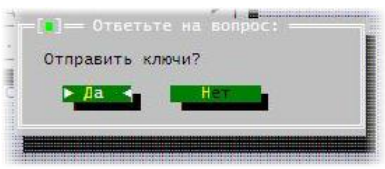

Рисунок 24: Подтверждение отправки ключевой информации на АП

3.2 Задайте дату и время отправки обновлений, после чего нажмите кнопку **Принять**.

По умолчанию дата и время отправки отличаются от текущих на сутки вперед.

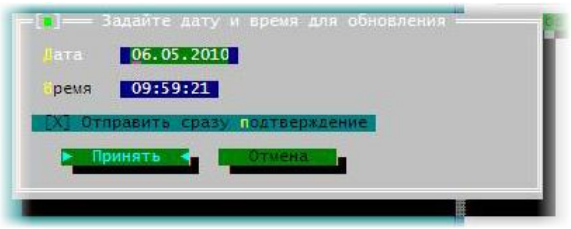

Рисунок 25: Указание даты и времени отправки обновлений из ЦУС

4 В ПО ViPNet Client, используемом на АП1:

4.1 При появлении окна с сообщением о поступлении обновлений ключевой информации нажмите кнопку **ОК**.

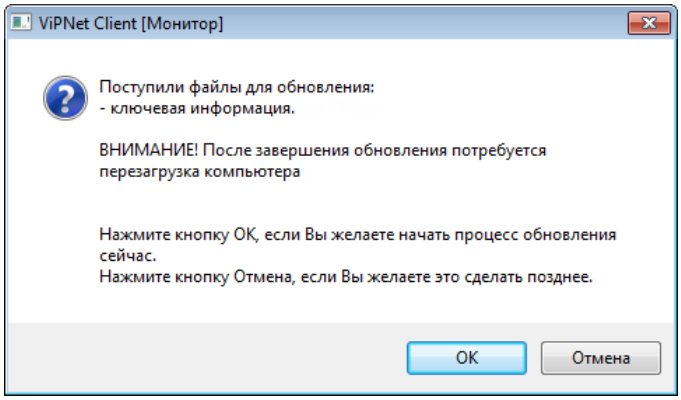

Рисунок 26: Диалоговое окно с сообщением о поступлении обновлений на данный АП

4.2 Убедитесь в том, что обновление успешно принято.

Для этого:

1. Выберите меню **Сервис** и в нем команду **Настройка параметров безопасности**.

2. В окне **Настройка параметров безопасности** перейдите на вкладку **Подпись**.

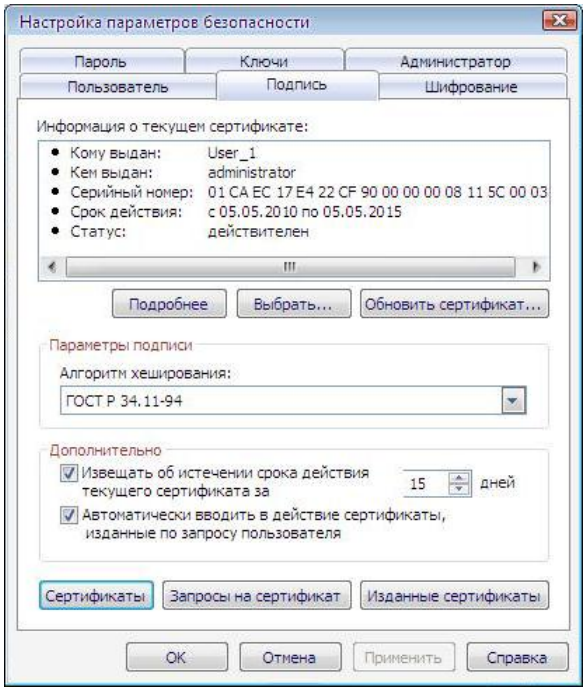

Рисунок 27: Информация об ЭЦП пользователя

3. Нажмите кнопку **Сертификаты**. В окне **Менеджер сертификатов** на вкладке **Личные сертификаты** отображается текущий сертификат пользователя, а также сертификаты, полученные в составе обновлений.

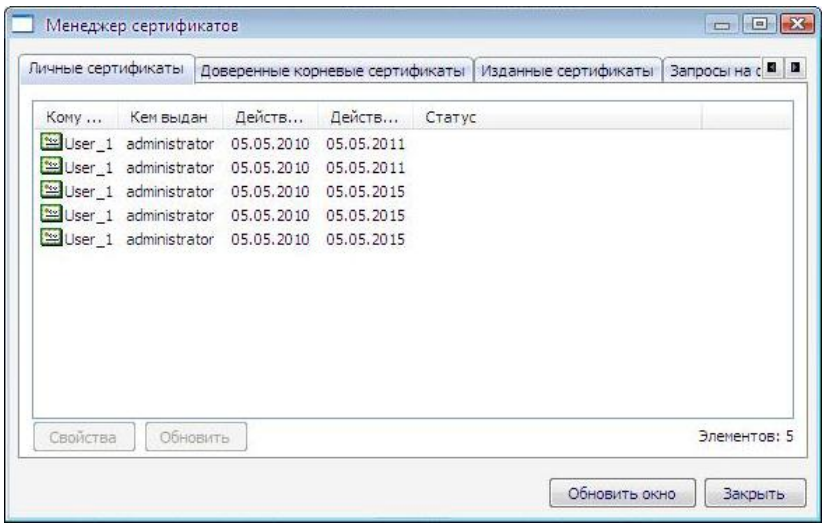

Рисунок 28: Личные сертификаты пользователя

4.3 Для использования полученного сертификата в качестве текущего в окне **Настройка параметров безопасности** на вкладке **Подпись** нажмите кнопку **Выбрать**.

4.4 В окне **Выбор сертификата** выберите обновленный сертификат, после чего нажмите кнопку **ОК**.

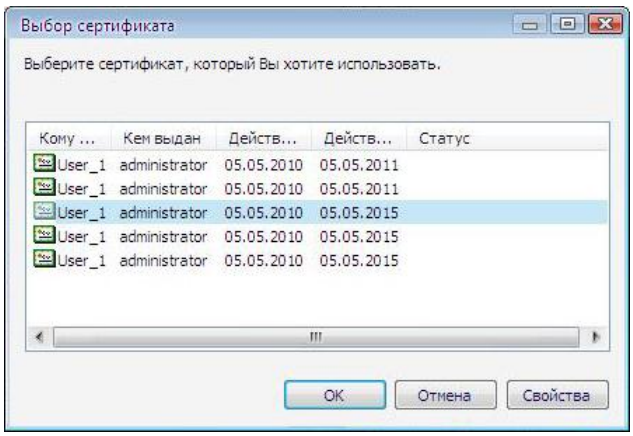

Рисунок 29: Выбор текущего сертификата

5 На АП1 скопируйте папку `sgn_cont`, в которой хранится информация о личных сертификатах пользователя и о ключах подписи.

Папка sgn_cont расположена в папке установки продукта ViPNet Client. По умолчанию это `C:\Program Files\InfoTeCS\ViPNet Client\user_XXXX\key_disc\dom\sgn_cont`.

6 Передайте надежным способом эту папку на АП2.

7 На АП2 замените папку `sgn_cont`, которая соответствует тому же пользователю User_1 и которая расположена по умолчанию по тому же пути, на полученную папку `sgn_cont`.

8 При запуске на АП2 в ПО ViPNet Client выполните действия, описанные в п. 4.2–4.4 текущего подраздела.

Обновление сертификата пользователя с помощью ПО ViPNet Client

Процедура обновления сертификата пользователя, зарегистрированного на двух АП (в данном случае — пользователя User_1), с помощью ПО ViPNet Client выглядит следующим образом:

1 Пользователь User_1 формирует запрос на обновление сертификата и отправляет этот запрос по сети на сетевой узел Администратора.

Внимание! Формирование запроса на обновление сертификата выполняется с использованием ПО ViPNet Client, установленного на том АП, ТК которого является главным для пользователя (в данном случае — на АП1).

2 Администратор получает запрос в УКЦ и издает сертификат по запросу.

3 Пользователь вручную передает информацию о сертификатах и ключах подписи с АП1 на другой АП (в данном случае — на АП2), на котором он также зарегистрирован. Автоматическая передача не возможна, поскольку тип коллектива АП2 не является главным для пользователя (см. «Постановка задачи» на стр. 23).

Для обновления сертификата пользователя с помощью ПО ViPNet Client, установленного на АП1:

1 В ПО ViPNet Client:

1.1 Вызовите окно **Настройка параметров безопасности** (см. Рисунок 27 на стр. 33):

- В программе ViPNet Client Монитор — выберите меню **Сервис** и в нем команду **Настройка параметров безопасности**.
- В программе ViPNet Client Деловая почта — выберите меню **Инструменты** и в нем команду **Настройка параметров безопасности**.

1.1 В окне **Настройка параметров безопасности** перейдите на вкладку **Подпись**, после чего нажмите кнопку **Обновить сертификат**.

1.2 На стартовой странице мастера обновления сертификата нажмите кнопку **Далее**.

1.3 На странице **Открытый ключ** укажите параметры открытого ключа, после чего нажмите кнопку **Далее**.

Примечание. Параметры, используемые по умолчанию, являются рекомендуемыми.

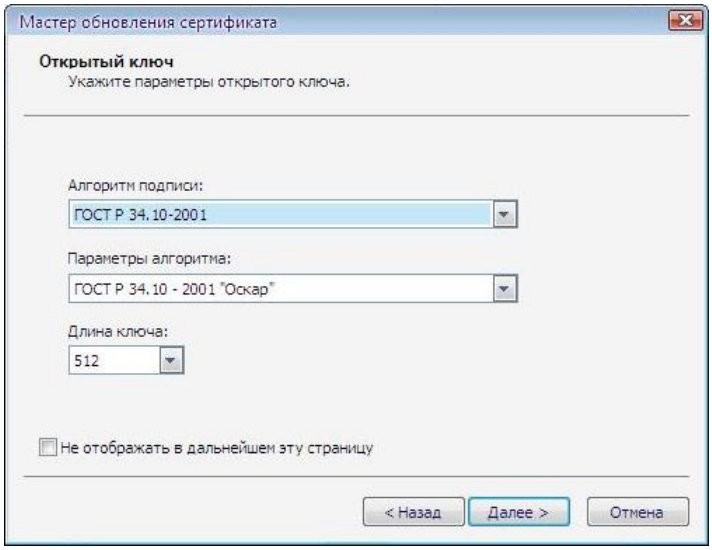

Рисунок 30: Указание параметров открытого ключа

1.4 На странице **Срок действия сертификата** задайте желаемый срок действия сертификата удобным для Вас способом, после чего нажмите кнопку **Далее**.

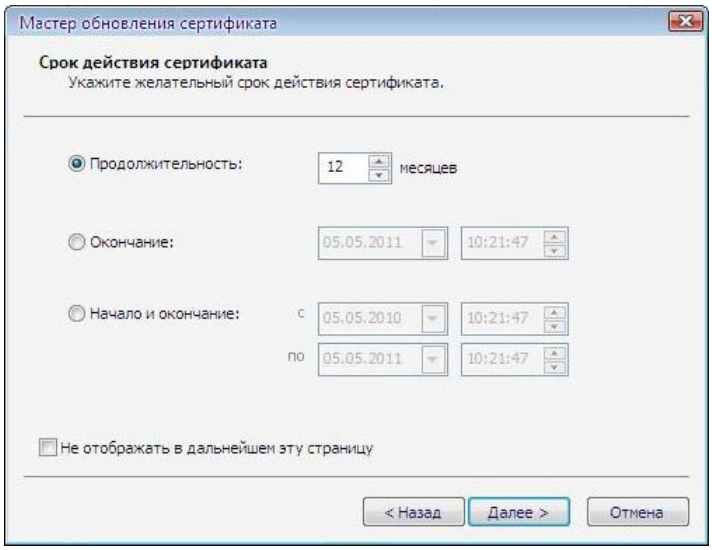

Рисунок 31: Указание срока действия сертификата

1.5 На странице **Готовность к созданию запроса на сертификат** убедитесь в правильности параметров, заданных на предыдущих страницах мастера.

При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.

Если все параметры верны, нажмите кнопку **Далее**.

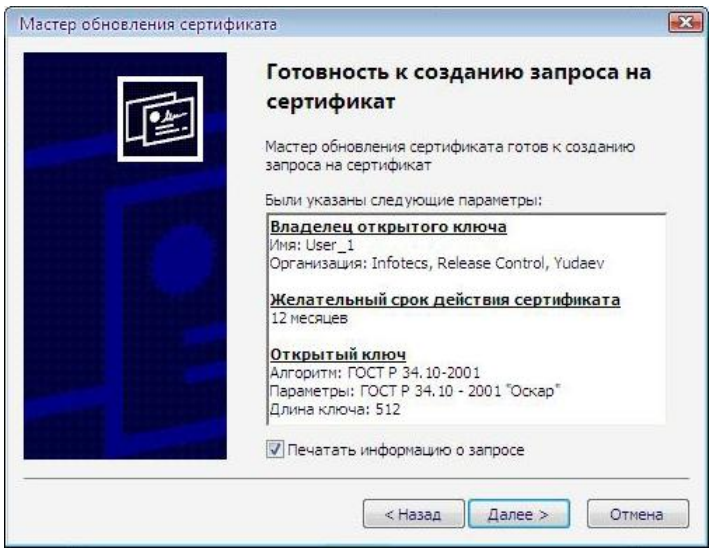

Рисунок 32: Проверка указанных параметров сертификата

1.6 При появлении электронной рулетки поводите указателем мыши в пределах появившегося окна.

Примечание. В случае, если в рамках текущей сессии электронная рулетка уже была запущена, данное окно не появится.

1.7 На странице **Завершение работы мастера обновления сертификата** оставьте параметры, используемые по умолчанию, после чего нажмите кнопку **Готово**.

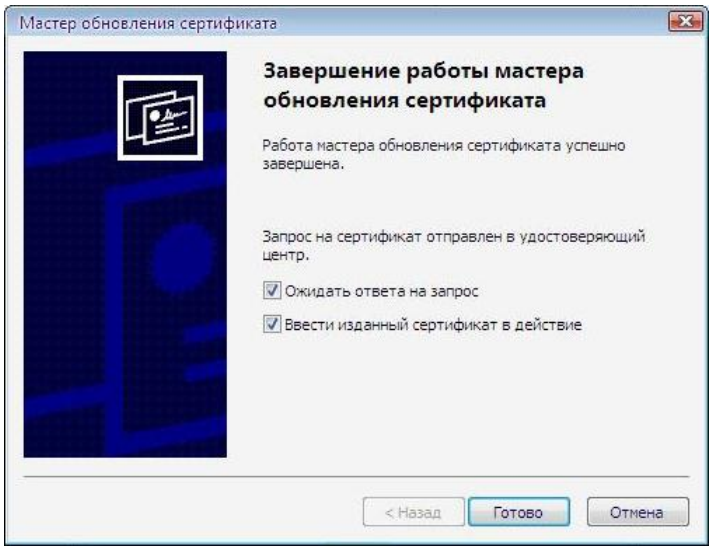

Рисунок 33: Завершение работы мастера обновления сертификата

1.8 Появившееся окно будет закрыто при получении ответа от УКЦ.

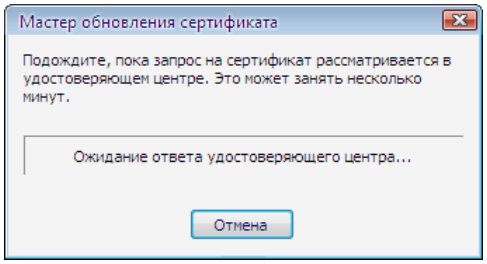

Рисунок 34: Ожидание ответа на запрос от УКЦ

2 В программе УКЦ, используемой на сетевом узле администратора:

2.1 При появлении окна с сообщением о получении запроса на обновление сертификата нажмите кнопку **ОК**.

Примечание. Данное окно появляется в том случае, если в программе УКЦ в окне **Настройки** в разделе **Сертификаты** установлен флажок **На сертификаты, подписанные пользователями**.

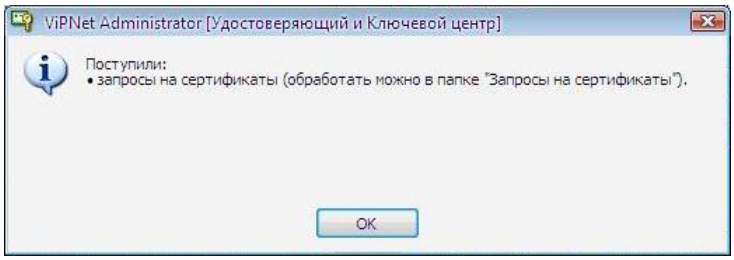

Рисунок 35: Получение в УКЦ запроса на сертификат

2.2 В главном окне УКЦ перейдите к разделу **Удостоверяющий центр** > **Запросы на сертификаты** > **Входящие** > **Своя сеть ViPNet**.

2.3 Выберите полученный запрос и выполните для него команду **Удовлетворить** контекстного меню.

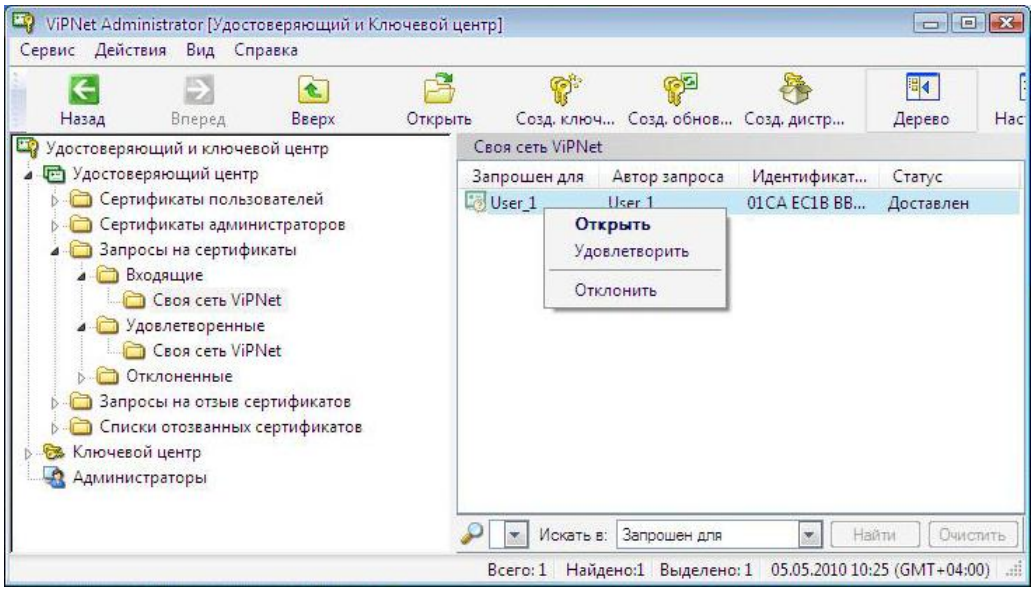

Рисунок 36: Издание сертификата по полученному запросу

2.4 При появлении электронной рулетки поводите указателем мыши в пределах появившегося окна.

Примечание. В случае, если в рамках текущей сессии электронная рулетка уже была запущена, данное окно не появится.

2.5 В появившемся окне с вопросом о редактировании полей издаваемого сертификата:

- При необходимости редактирования полей нажмите кнопку **Yes**, после чего перейдите к действию 2.6.
- Для отказа от редактирования нажмите кнопку **No**, после чего перейдите к п. 3.

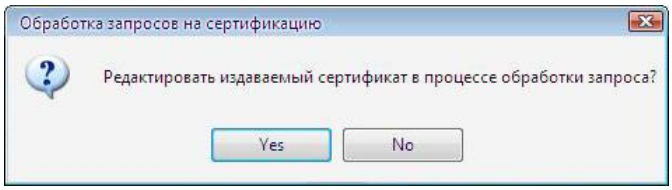

Рисунок 37: Подтверждение редактирования издаваемого сертификата

2.6 Укажите и (или) измените сведения о владельце сертификата, а также о назначениях сертификата на страницах мастера редактирования полей сертификата (см. «Обновление сертификата пользователя с помощью ЦУС» на стр. 24).

3 В ПО ViPNet Client, установленном на АП1:

3.1 В появившемся окне с сообщением об успешном вводе сертификата в действие нажмите кнопку **ОК**.

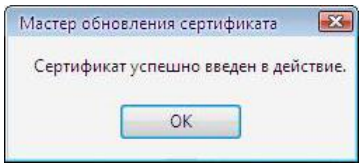

Рисунок 38: Диалоговое окно с сообщением об успешном вводе сертификата в действие

3.2 Вызовите окно **Настройка параметров безопасности** и перейдите в нем на вкладку **Подпись**.

3.3 Нажмите кнопку **Выбрать**.

3.4 В появившемся окне **Выбор сертификата** (см. Рисунок 29 на стр. 34) выберите полученный сертификат, после чего нажмите кнопку **ОК**.

Данный сертификат будет назначен текущим.

4 На АП1 скопируйте папку `sgn_cont`, в которой хранится информация о личных сертификатах пользователя и о ключах подписи.

Папка `sgn_cont` расположена в каталоге установки продукта ViPNet Client. По умолчанию это `C:\Program Files\InfoTeCS\ViPNet Client\user_XXXX\key_disc\dom\sgn_cont`.

5 Передайте надежным способом эту папку на АП2.

6 На АП2 замените папку sgn_cont, которая соответствует тому же пользователю User_1 и которая расположена по умолчанию по тому же пути, на полученную папку sgn_cont.

Для ViPNet Administrator версии 3.1 и ViPNet Client версии 3.1 (2.6318)

Обновление сертификата пользователя с помощью ЦУС

При обновлении сертификата пользователя с помощью программы ViPNet Administrator Центр управления сетью (далее — ЦУС) это обновление передается на АП в составе ключевой дискеты (КД).

Процедура обновления КД пользователя, зарегистрированного на двух АП (в данном случае — пользователя User_1) выглядит следующим образом:

1. Администратор формирует обновление в программах ЦУС и ViPNet Administrator Удостоверяющий и ключевой центр (далее — УКЦ)
2. Администратор отправляет по сети сформированное обновление.

Примечание. Обновление будет отправлено на тот АП, ТК которого является главным для пользователя (в данном случае — на АП1).

3. Пользователь User_1 принимает обновление с помощью ПО ViPNet Client.
4. Пользователь вручную передает информацию о сертификатах и ключах подписи с АП1 на другой АП (в данном случае — на АП2), на котором он также зарегистрирован. Автоматическая передача не возможна, поскольку тип коллектива АП2 не является главным для пользователя (см. «Постановка задачи» на стр. 23).

Для обновления сертификата пользователя User_1 с помощью ЦУС:

1. В программе ЦУС, используемой на сетевом узле Администратора, выполните действия, описанные в п. 1 (см. «Обновление сертификата пользователя с помощью ЦУС» на стр. 24).
2. В программе УКЦ, используемой на сетевом узле Администратора, выполните действия, описанные в п. 2 (см. «Обновление сертификата пользователя с помощью ЦУС» на стр. 24).

3 В программе ЦУС, используемой на сетевом узле Администратора, выполните действия, описанные в п. 3 (см. «Обновление сертификата пользователя с помощью ЦУС» на стр. 24).

4 В ПО ViPNet Client, используемом на АП1, выполните действия, описанные в п. 4 (см. «Обновление сертификата пользователя с помощью ЦУС» на стр. 24).

5 В ПО ViPNet Client в окне **Настройка параметров безопасности** перейдите на вкладку **Ключи**.

На панели **Контейнер ключей подписи** отображается имя используемого контейнера, а также полный путь к папке контейнера.

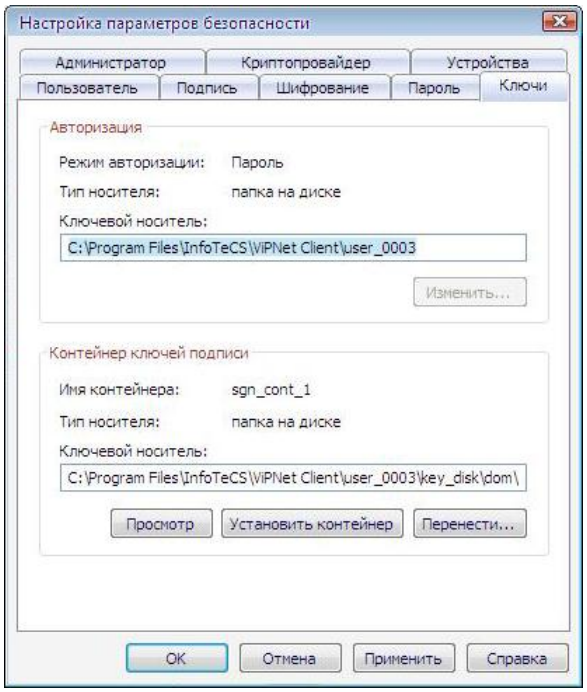

Рисунок 39: Просмотр информации о размещении контейнера ключей подписи

6 Перейдите к этой папке, скопируйте ее и передайте надежным способом на АП2.

7 На АП2 поместите полученную папку по тому же пути, по которому она располагается на АП1.

8 В ПО ViPNet Client, используемом на АП2:

8.1 Вызовите окно **Настройка параметров безопасности**, после чего перейдите на вкладку **Ключи**.

8.2 Нажмите кнопку **Установить контейнер**.

8.3 В появившемся окне укажите имя полученного контейнера и его расположение, после чего нажмите кнопку **ОК**.

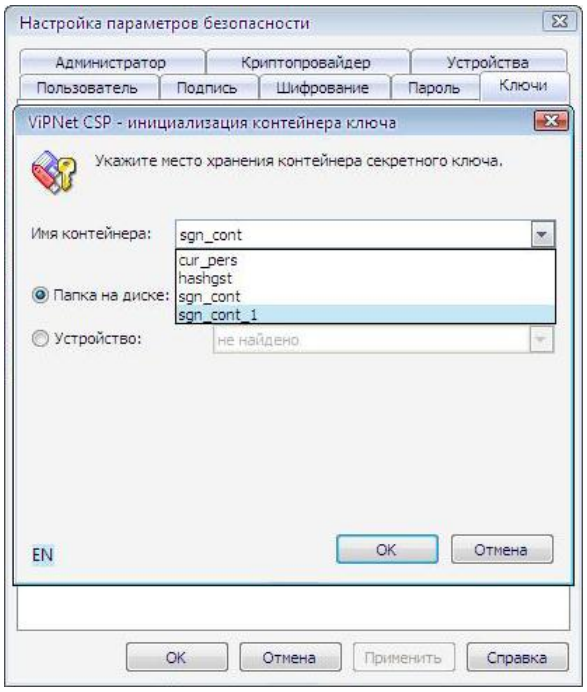

Рисунок 40: Выбор контейнера ключей подписи

8.4 В появившемся окне **Выбор сертификата** выберите предложенный сертификат, который хранится в выбранном контейнере, после чего нажмите кнопку **ОК**.

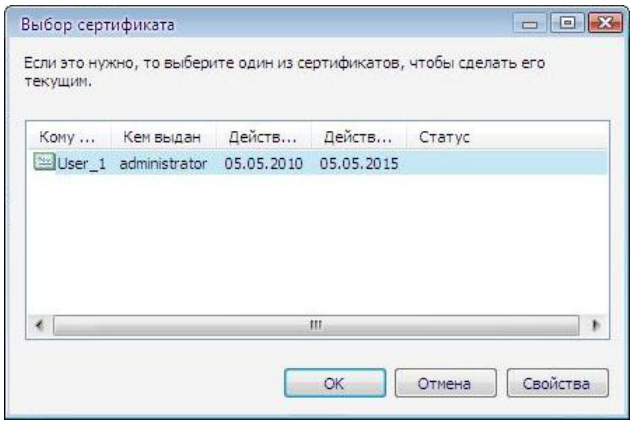

Рисунок 41: Выбор сертификата, который хранится в контейнере

8.5 В окне **Настройка параметров безопасности** перейдите на вкладку **Подпись**, после чего нажмите кнопку **Выбрать**.

8.6 В появившемся окне **Выбор сертификата** выберите тот же сертификат, после чего нажмите кнопку **ОК**.

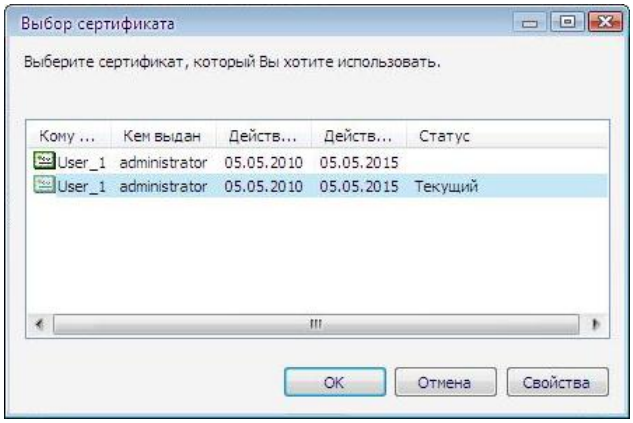

Рисунок 42: Выбор текущего сертификата в ПО версии 3.1 (1.5030 и выше)

Данный сертификат будет назначен текущим (в колонке **Статус** для этого сертификата отобразится сообщение **Текущий**).

Обновление сертификата пользователя с помощью ПО ViPNet Client

Процедура обновления сертификата пользователя, зарегистрированного на двух АП (в данном случае — пользователя User_1), с помощью ПО ViPNet Client выглядит следующим образом:

1 Пользователь User_1 формирует запрос на обновление сертификата и отправляет этот запрос по сети на сетевой узел Администратора.

Внимание! Формирование запроса на обновление сертификата выполняется с использованием ПО ViPNet Client, установленного на том АП, ТК которого является главным для пользователя (в данном случае — на АП1).

2 Администратор получает запрос в УКЦ и издает сертификат по запросу.

3 Пользователь вручную передает информацию о сертификатах и ключах подписи с АП1 на другой АП (в данном случае — на АП2), на котором он также зарегистрирован. Автоматическая передача не возможна, поскольку тип коллектива АП2 не является главным для пользователя (см. «Постановка задачи» на стр. 23).

Для обновления сертификата пользователя с помощью ПО ViPNet Client, установленного на АП1:

1 В ПО ViPNet Client:

1.1 Вызовите окно **Настройка параметров безопасности**:

- В программе ViPNet Client Монитор — выберите меню **Сервис** и в нем команду **Настройка параметров безопасности**.
- В программе ViPNet Client Деловая почта —выберите меню **Инструменты** и в нем команду **Настройка параметров безопасности**.

1.1 В окне **Настройка параметров безопасности** перейдите на вкладку **Подпись**, после чего нажмите кнопку **Обновить сертификат**.

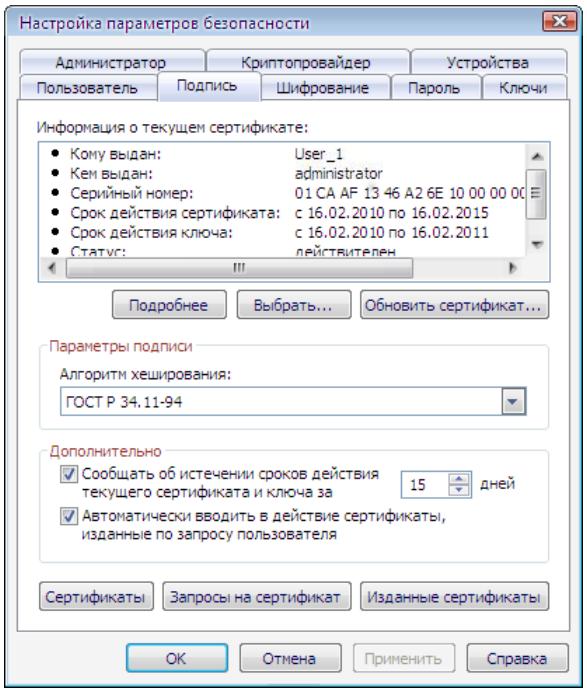

Рисунок 43: Информация об ЭЦП пользователя для ПО версии 3.1 (1.5030 и выше)

1.2 На стартовой странице мастера обновления сертификата нажмите кнопку **Далее**.

1.3 На странице **Открытый ключ** укажите параметры открытого ключа, после чего нажмите кнопку **Далее**.

Примечание. Параметры, используемые по умолчанию, являются рекомендуемыми

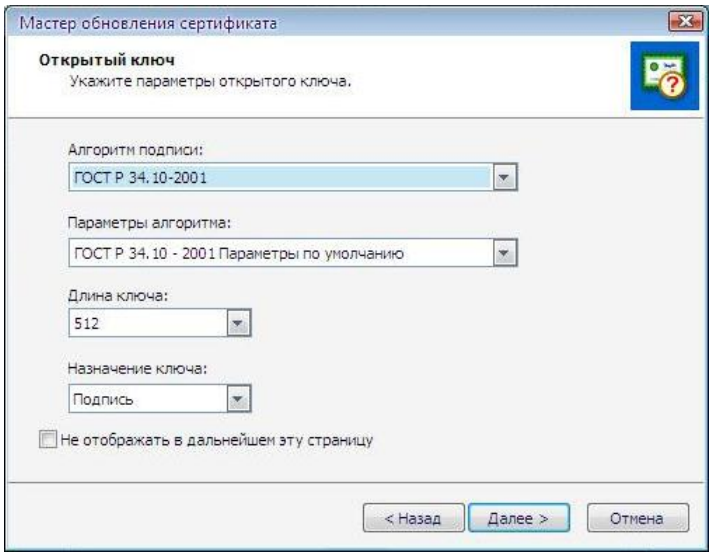

Рисунок 44: Указание параметров открытого ключа

1.4 На странице **Контейнер с секретным ключом** укажите место сохранения контейнера с закрытым ключом: папку на диске или устройство с указанием его параметров и при необходимости ПИН-кода (если ПИН-код не был сохранен ранее). Если выбрано устройство, то подключите внешнее устройство в компьютеру.

Нажмите кнопку **ОК**.

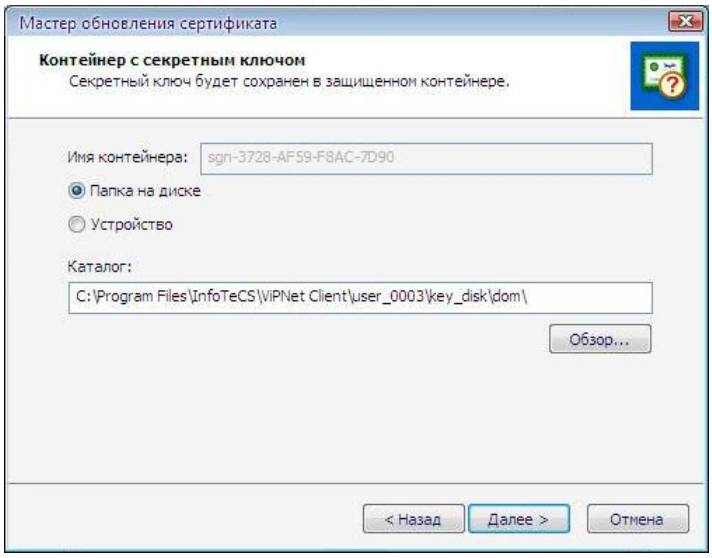

Рисунок 45: Указание папки для сохранения контейнера с закрытым ключом

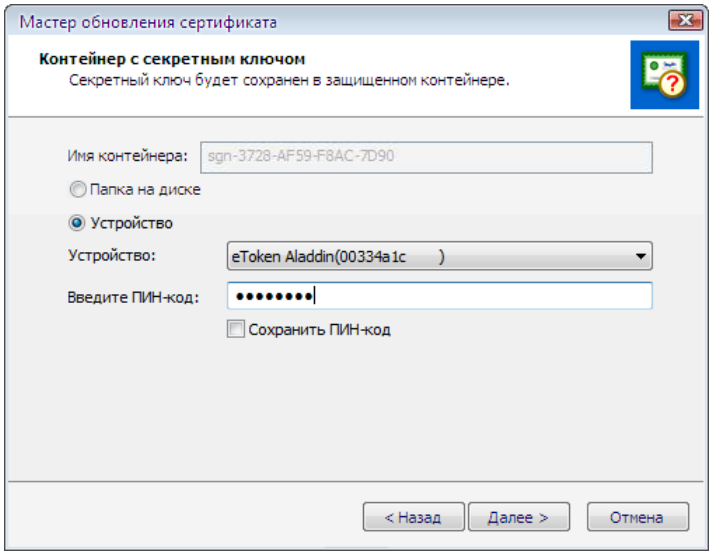

Рисунок 46: Подключение к устройству для сохранения контейнера с закрытым ключом

1.5 На странице **Срок действия сертификата** задайте желаемый срок действия сертификата удобным для Вас способом, после чего нажмите кнопку **Далее**.

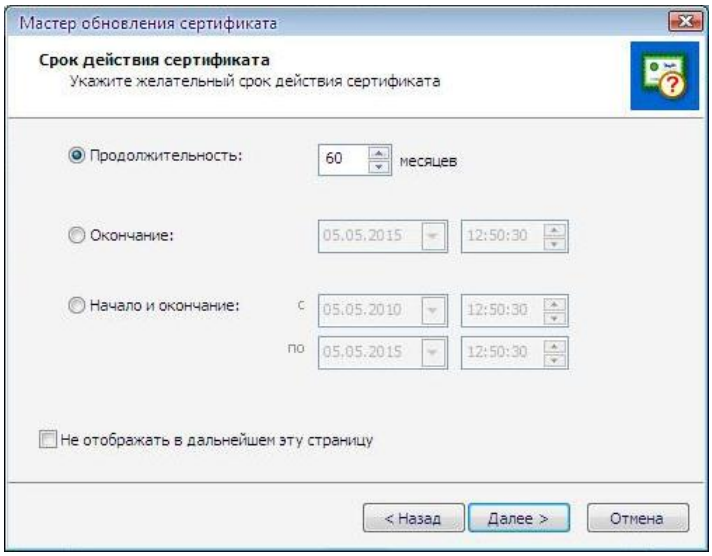

Рисунок 47: Указание желательного срока действия сертификата

1.6 На странице **Способ передачи сертификата** убедитесь в том, что переключатель установлен в положение **Передать через транспортный модуль**, после чего нажмите кнопку **Далее**.

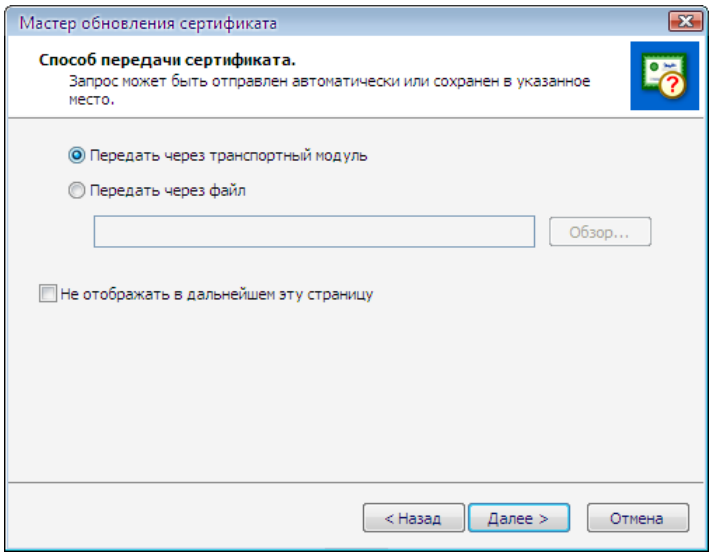

Рисунок 48: Выбор способа передачи сертификата в УКЦ

1.7 На странице **Готовность к созданию запроса на сертификат** убедитесь в правильности параметров, заданных на предыдущих страницах мастера. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.

Если все параметры верны, нажмите кнопку **Далее**.

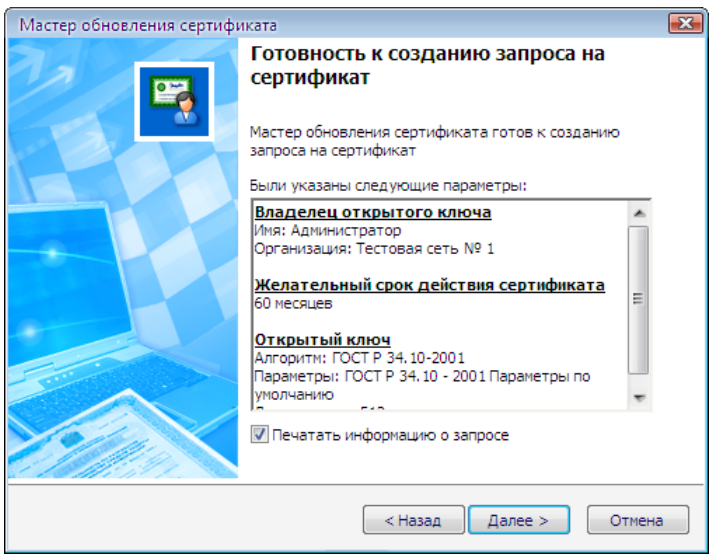

Рисунок 49: Проверка указанных параметров запроса

1.8 При появлении электронной рулетки поводите указателем мыши в пределах появившегося окна.

Примечание. В случае, если в рамках текущей сессии электронная рулетка уже была запущена, данное окно не появится.

1.9 На странице **Завершение работы мастера обновления сертификата** оставьте параметры, используемые по умолчанию, после чего нажмите кнопку **Готово**.

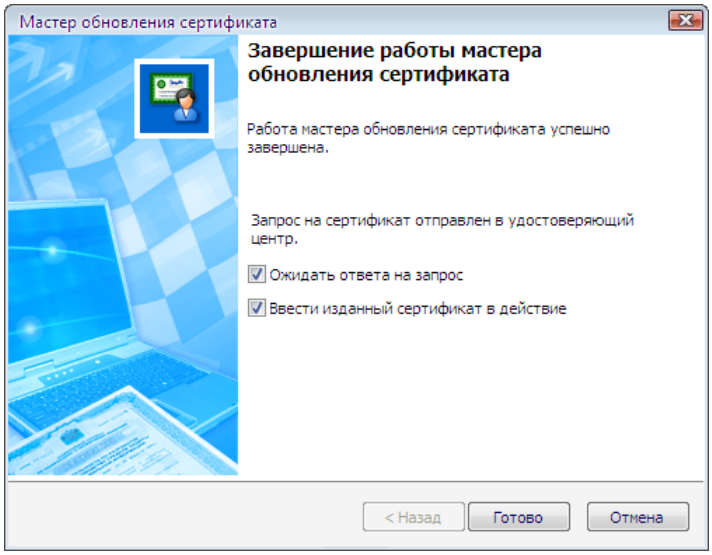

Рисунок 50: Завершение работы мастера обновления сертификата

1.10 Появившееся окно будет закрыто при получении от УКЦ ответа на запрос.

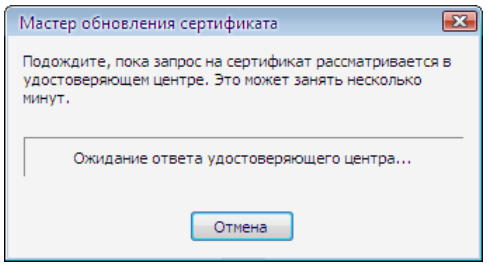

Рисунок 51: Ожидание ответа на запрос от УКЦ

2 В программе УКЦ, используемой на сетевом узле администратора, выполните действия, описанные в п. 2 (см. «Обновление сертификата пользователя с помощью ПО ViPNet Client» на стр. 35).

3 В ПО ViPNet Client, установленном на АП1:

3.1 В появившемся диалоговом окне с сообщением об успешном вводе сертификата в действие нажмите кнопку **ОК**.

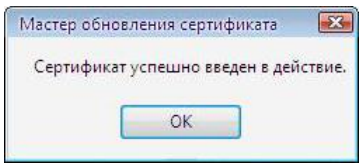

Рисунок 52: Диалоговое окно с сообщением об успешном вводе сертификата в действие

3.2 Вызовите окно **Настройка параметров безопасности** и перейдите в нем на вкладку **Подпись** (см. Рисунок 43 на стр. 46).

3.3 Нажмите кнопку **Выбрать**.

3.4 В появившемся окне **Выбор сертификата** выберите полученный сертификат, после чего нажмите кнопку **ОК**.

Данный сертификат будет назначен текущим (в колонке **Статус** для этого сертификата отобразится сообщение **Текущий**).

3.5 В окне **Настройка параметров безопасности** перейдите на вкладку **Ключи**.

На панели **Контейнер ключей подписи** отображается имя используемого контейнера, а также полный путь к папке контейнера.

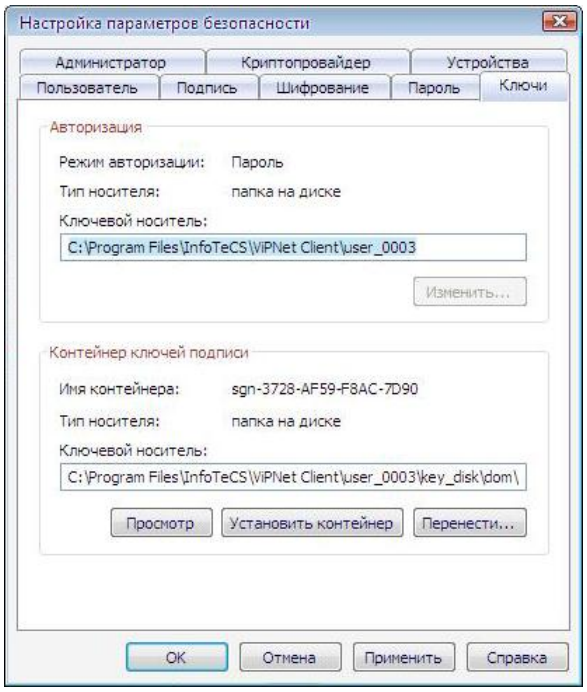

Рисунок 53: Просмотр информации о размещении контейнера ключей подписи в ПО версии 3.1 (1.5030 и выше)

4 Перейдите к этой папке, скопируйте ее и передайте надежным способом на АП2.

5 На АП2 поместите полученную папку по тому же пути, по которому она располагается на АП1.

6 В ПО ViPNet Client, используемом на АП2:

6.1 Вызовите окно **Настройка параметров безопасности**, после чего перейдите на вкладку **Ключи**.

6.2 Нажмите кнопку **Установить контейнер**.

6.3 В появившемся окне укажите имя полученного контейнера и его расположение, после чего нажмите кнопку **ОК**.

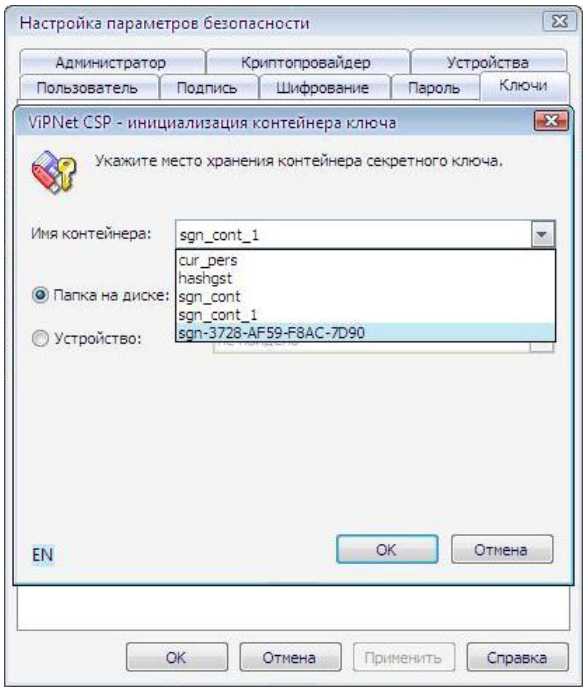

Рисунок 54: Выбор контейнера ключей подписи

6.4 В появившемся окне **Выбор сертификата** выберите предложенный сертификат, который хранится в выбранном контейнере, после чего нажмите кнопку **ОК**.

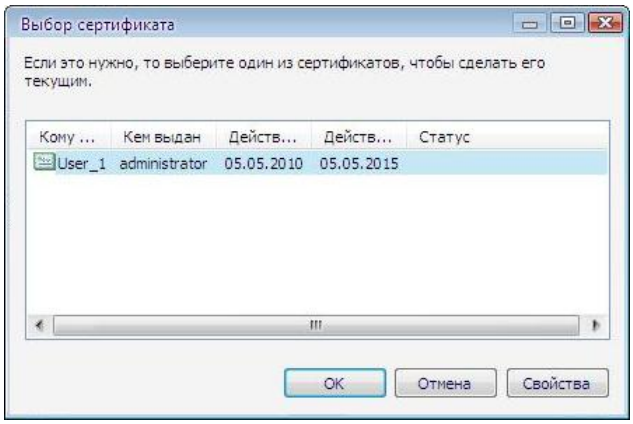

Рисунок 55: Выбор сертификата, который хранится в контейнере

6.5 В окне **Настройка параметров безопасности** перейдите на вкладку **Подпись**, после чего нажмите кнопку **Выбрать**.

6.6 В появившемся окне **Выбор сертификата** выберите тот же сертификат, после чего нажмите кнопку **ОК**.

Данный сертификат будет назначен текущим (в колонке **Статус** для этого сертификата отобразится сообщение **Текущий**).