

ViPNet Administrator Удостоверяющий и ключевой центр 3.2

Руководство администратора

1991–2012 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00006-05 32 02

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.....	9
О документе	10
Для кого предназначен документ	11
Соглашения документа.....	11
О программе.....	12
Лицензионное ограничение	14
Отсутствие функциональности программы в части Удостоверяющего центра ViPNet	15
Просмотр лицензионного ограничения.....	16
Настройка оповещения об окончании лицензии.....	17
Новые возможности	18
Что нового в версии 3.2.9	18
Что нового в версии 3.2.5	24
Что нового в версии 3.2.4	25
Что нового в версии 3.2.3	26
Что нового в версии 3.2.2	27
Что нового в версии 3.1.x	30
Системные требования.....	33
Требования к SQL-серверу для развертывания базы данных УКЦ.....	33
Информация о внешних устройствах хранения данных.....	35
Комплект поставки	40
Обратная связь	41
Глава 1. Установка и настройка программы ViPNet Удостоверяющий и ключевой центр	42
Варианты развертывания	43
Выбор необходимого дополнительного программного обеспечения ViPNet	44
Порядок развертывания	46
Установка программы	48
Проведение первичной инициализации программы	50
Возможные причины некорректной инициализации.....	56

Глава 2. Начало работы с программой ViPNet Удостоверяющий и ключевой центр.....	58
Запуск и завершение работы с программой.....	59
Подключение к SQL-серверу при запуске программы.....	62
Интерфейс программы ViPNet Удостоверяющий и ключевой центр	64
Глава 3. Основные действия администратора УКЦ	67
Создание ключевой информации при первоначальном развертывании сети.....	68
Рекомендации по созданию ключевой информации в связи с изменением структуры сети.....	70
Создание ключей при изменениях в структуре своей сети.....	70
Создание ключей при установлении взаимодействия с доверенной сетью ViPNet, а также при внесении изменений в это взаимодействие	73
Когда создавать обновление ключей?	75
Действия при плановой смене мастер-ключей	76
Плановая смена мастер-ключей.....	76
Плановая смена межсетевых мастер-ключа	77
Действия при компрометациях ключей.....	79
События, квалифицируемые как компрометация ключей	79
Действия при компрометации ключей пользователя.....	80
Действия при компрометации ключей УКЦ.....	82
Кросс-сертификация.....	83
Организация распределенной системы доверительных отношений между УЦ.....	86
Организация иерархической системы доверительных отношений между УЦ.....	86
Глава 4. Управление ключевой структурой ViPNet.....	88
Создание ключевой информации	89
Создание дистрибутивов ключей	91
Общие сведения	91
Особенности при создании дистрибутивов ключей	92
Процесс создания	93
Создание ключей узлов	95
Создание обновлений ключей узлов	97
Создание ключей пользователей	100
Создание резервных наборов персональных ключей	103
Создание ключей при компрометациях	105
Действия с созданной ключевой информацией.....	107

Действия с ключами пользователей	108
Действия с ключами узлов и обновлениями ключей для СУ.....	111
Действия с созданными дистрибутивами ключей.....	113
Действия с резервными персональными ключами	117
Создание мастер-ключей	119
Смена мастер-ключей своей сети	119
Создание межсетевых мастер-ключей	120
Логика выбора меж сетевого мастер-ключа.....	123
Экспорт и импорт межсетевых мастер-ключей.....	124
Экспорт межсетевых мастер-ключей	124
Импорт межсетевых мастер-ключей	126
Изменение статуса меж сетевого мастер-ключа	127
Пароль администратора сетевых узлов	129
Сохранение паролей пользователей и администраторов сетевых узлов.....	131
Смена паролей пользователей ViPNet.....	132
Просмотр свойств пользователя	133
Просмотр свойств сетевого узла	136
Просмотр свойств сетевой группы	139

Глава 5. Управление сертификатами в части Удостоверяющего центра..... 141

Издание сертификатов	143
Мастер редактирования полей сертификата.....	144
Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ.....	149
Издание (отклонение) сертификатов по запросам, поступившим с СУ пользователей сети ViPNet.....	149
Издание (отклонение) сертификатов по запросам, поступившим из ViPNet Registration Point	152
Издание (отклонение) сертификатов по запросам от внешних пользователей	154
Отзыв сертификатов, приостановление действия сертификатов, возобновление действия сертификатов	157
По запросу из ViPNet Registration Point	157
По инициативе администратора УКЦ	159
Импорт сертификатов администраторов доверенных сетей ViPNet	162
Импорт списков отзыванных сертификатов доверенных сетей ViPNet	165
Обновление списка отзыванных сертификатов своей сети.....	167

Обработка запросов на кросс-сертификаты (в том числе запросов на сертификаты из подчиненных УЦ)	169
Издание кросс-сертификатов	169
Описание окна Издание кросс-сертификатов.....	174
Описание окна Запрос на кросс-сертификат	175
Экспорт кросс-сертификатов	179
Просмотр запросов и сертификатов	180
Просмотр запросов на сертификаты пользователей	180
Просмотр запроса на сертификат	180
Просмотр сертификатов	182
Окно Сертификат	183
Просмотр истории сертификата.....	184
Просмотр списков отзыва сертификатов	185
Экспорт сертификатов	188
Форматы экспорта сертификатов	189
Проверка сертификатов	192
Публикация и прием опубликованных данных	193
Настройка программы УКЦ для взаимодействия с программой ViPNet Publication Service.....	194
Копирование данных для программы сервиса публикации	195
Прием данных из программы ViPNet Publication Service.....	195

Глава 6. Управление администраторами программы ViPNet Удостоверяющий и ключевой центр	197
Создание учетной записи администратора	199
Удаление учетной записи администратора	202
Смена текущей учетной записи администратора	203
Просмотр контейнера ключей администратора.....	204
Просмотр и изменение данных об администраторе	206
Обновление сертификата и закрытого ключа администратора	208
Выбор текущего сертификата администратора	216
Смена пароля администратора	217
Окно Пароль администратора	217
Смена ключа защиты УКЦ	218
Смена ключевого носителя администратора	219
Создание запроса на кросс-сертификат к вышестоящему УЦ и установка изданного сертификата в иерархической системе доверительных отношений.....	220

Создание запроса на кросс-сертификат к вышестоящему удостоверяющему центру.....	221
Ввод в действие кросс-сертификата, изданного в вышестоящем УЦ.....	224
Импорт сертификатов администраторов вышестоящего УЦ.....	226
Просмотр истории запросов на сертификат, сформированных к вышестоящему УЦ.....	227
Просмотр свойств запроса (окно Запрос на издание сертификата)	228
Создание запроса на кросс-сертификат к другому УЦ в распределенной системе доверительных отношений.....	230
Создание запроса на кросс-сертификат и отправка его в другой УЦ	230
Глава 7. Настройка программы ViPNet Удостоверяющий и ключевой центр.....	237
Настройка папок обмена.....	239
Настройка типа создаваемых паролей.....	242
Настройка параметров случайных паролей.....	243
Настройка паролей администраторов.....	245
Настройка параметров создания резервных наборов персональных ключей.....	247
Настройка параметров издания сертификатов и обработки запросов.....	250
Настройка параметров работы с сертификатами.....	253
Создание и редактирование шаблонов сертификатов.....	256
Настройка параметров работы со списками отозванных сертификатов	264
Расширенная настройка параметров обновления списков отозванных сертификатов на сетевых узлах.....	265
Настройка списка политик применения сертификата.....	268
Настройка параметров публикации данных	271
Настройка списка точек распространения	273
Глава 8. Административные функции	276
Создание и восстановление резервных копий конфигурации программы	277
Создание резервной копии текущей конфигурации	277
Восстановление конфигурации.....	279
Редактирование списка резервных копий.....	281
Отмена последнего восстановления конфигурации	282
Настройка параметров создания резервных копий.....	283
Работа с журналом событий ViPNet Удостоверяющий и ключевой центр	285
Просмотр журнала событий	285
Настройка параметров журнала событий	287
Проверка текущих данных	290

Ручная проверка текущих данных	294
Экспорт служебных данных	295
Ручной экспорт данных	295
Учет ключей Деловой сети РФ.....	296
Приложение А. Перенос базы данных УКЦ на SQL-сервер	299
Приложение В. Глоссарий	306
Приложение С. Указатель	323



Введение

О документе	10
О программе	12
Лицензионное ограничение	14
Новые возможности	18
Системные требования	33
Информация о внешних устройствах хранения данных	35
Комплект поставки	40
Обратная связь	41

О документе

Настоящий документ является подробным руководством по установке, настройке и использованию программы ViPNet Удостоверяющий и ключевой центр (далее — УКЦ) и организован следующим образом:

- В начале документа (во введении) приводятся общие сведения о программе: назначение, применение, функциональные возможности и лицензионное ограничение на использование УКЦ, а также список основных изменений и доработок программы, реализованных в версиях 3.1.x и 3.2.x.
- Далее (в первых двух главах) описывается порядок развертывания, установка и первичная инициализация УКЦ, начало работы с программой и полное описание ее графического интерфейса.
- В последующих главах (главы 3 — 6) содержится описание типовых сценариев работы администратора УКЦ, таких как: создание ключевой информации и ее обновление; смена основного мастер-ключа; создание, смена, экспорт, импорт межсетевых мастер-ключей; установление межсетевого взаимодействия с доверенной сетью; издание сертификатов пользователей ViPNet; импорт сертификатов администраторов и списков отозванных сертификатов из доверенных сетей ViPNet; обработка запросов на кросс-сертификаты и другие.
- В заключительных главах (главы 7, 8) приводится описание настройки программы и административных функций, которые можно в ней выполнить.
- В самом конце документа присутствуют краткий словарь терминов и определений (глоссарий) и указатель. Полная версия словаря приведена в документе «Основные термины и определения. Приложение к документации ViPNet CUSTOM» из комплекта поставки (см. [«Комплект поставки»](#) на стр. 40).

При изучении данного руководства рекомендуется дополнительно ознакомиться с остальной документацией из комплекта поставки. Это позволит получить общее представление об основных понятиях и структуре сети ViPNet и составить более полную картину взаимодействия УКЦ с программой ViPNet Центр управления сетью (см. [«Центр управления сетью \(ЦУС\)»](#)).

Для кого предназначен документ




Данное руководство предназначено для администраторов сетей ViPNet, отвечающих за организацию работы программы ViPNet Удостоверяющий и ключевой центр — администраторов УКЦ (см. «Администратор УКЦ»).

Предполагается, что читатель данного руководства предварительно прошел обучение по технологии ViPNet в учебном центре «ИнфоТеКС» <http://www.infotecs.ru/learning/> и имеет опыт организации и обслуживания виртуальных защищенных сетей 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.

О программе

ViPNet Удостоверяющий и ключевой центр — это административная программа, которая входит в состав программного обеспечения ViPNet Administrator, и предназначена для управления ключевой структурой сети ViPNet, а также для издания и обслуживания различных видов сертификатов открытого ключа подписи (см. «[Сертификат открытого ключа подписи пользователя](#)»).

В соответствии с основными функциями УКЦ условно можно разделить на два компонента: Ключевой центр и Удостоверяющий центр. Схематично данное деление представлено на рисунке ниже.



Рисунок 1: Условное деление УКЦ на компоненты

При работе УКЦ в роли Ключевого центра осуществляется создание ключей (дистрибутивов ключей (см. «[Дистрибутив ключей](#)»), ключей узлов (см. «[Ключи узла ViPNet](#)»), ключей пользователей сети ViPNet (см. «[Ключи пользователя ViPNet](#)») и других) на основе данных, поступающих из программы ViPNet Центр управления сетью. Созданные ключи впоследствии передаются пользователям и используются соответствующим программным обеспечением ViPNet для организации безопасного обмена конфиденциальной информацией. С помощью данного компонента также осуществляется формирование мастер-ключей (см. «[Мастер-ключ](#)»), в том числе, межсетевых мастер-ключей (см. «[Межсетевой мастер-ключ](#)»), необходимых при установлении взаимодействия с доверенными сетями.

При работе УКЦ в роли Удостоверяющего центра производится издание сертификатов открытого ключа подписи по запросам, поступающим от самих пользователей сети ViPNet либо из Центров регистрации (программ [ViPNet Registration Point](#)), а также отзыв выпущенных сертификатов, приостановление и возобновление их действия.



Примечание. Издание сертификатов осуществляется на базе алгоритма ГОСТ Р 34.10-2001. Описание алгоритма см. в RFC 4357
<http://www.ietf.org/rfc/rfc4357.txt>.

Кроме этого, с помощью данного компонента осуществляется:

- формирование корневых сертификатов администраторов (см. «[Корневой сертификат](#)»), списков отозванных сертификатов (см. «[Список отозванных сертификатов \(СОС\)](#)») и их распространение в своей и доверенных сетях;
- создание запросов на проведение кросс-сертификации с другими Удостоверяющими центрами либо издание кросс-сертификатов;
- импорт корневых сертификатов и СОС из внешних Удостоверяющих центров и другие всевозможные операции.

Лицензионное ограничение

Работа программы ViPNet Удостоверяющий и ключевой центр в части Удостоверяющего центра ViPNet осуществляется в соответствии с лицензией, содержащейся в файле `infotecs.re`, и может быть ограничена. Функциональность УКЦ в части Ключевого центра лицензией не ограничивается.

Лицензия в файле `infotecs.re` определяет максимальное число сертификатов, которое может быть издано в УКЦ для внутренних (см. «[Внутренний пользователь ViPNet](#)») и внешних пользователей ViPNet (см. «[Внешний пользователь ViPNet](#)»). При необходимости это число может быть неограниченно. Файл `infotecs.re` также может не содержать лицензии на издание сертификатов подписи. В таком случае УКЦ будет выполнять только функции Ключевого центра и не сможет работать в качестве Удостоверяющего центра (см. «[Отсутствие функциональности программы в части Удостоверяющего центра ViPNet](#)» на стр. 15).

О том, как узнать содержание предоставленной лицензии, см. раздел [Просмотр лицензионного ограничения](#) (на стр. 16).

Если лицензия на издание сертификатов ограничена и в процессе работы с программой число изданных сертификатов превысит или станет равным максимальному, издание нового сертификата будет невозможно. Об этом будет проинформировано в соответствующем предупреждении (см. «[Настройка оповещения об окончании лицензии](#)» на стр. 17). В данном случае потребуется расширение лицензии — увеличение максимально допустимого числа издаваемых сертификатов.

Для расширения лицензии обратитесь к представителю компании «ИнфоТеКс» и закажите новую лицензию, дополнительно сообщив ему номер сети ViPNet и желаемые параметры новой лицензии. Чтобы узнать номер сети, в УКЦ в меню **Справка** выберите пункт **О программе**. После обработки запроса на расширение лицензии вы получите новый файл `infotecs.re`. Поместите этот файл в папку установки УКЦ (см. «[Установка программы](#)» на стр. 48) и перезапустите программу. После перезапуска программы будет использоваться расширенная лицензия.



Примечание. Существует еще одно ограничение, но оно не является лицензионным и заключается в том, что если в программе ViPNet Центр управления сетью нет ни одного сетевого узла, зарегистрированного в задаче «Центр регистрации», то в УКЦ не отображаются элементы интерфейса, связанные с внешними пользователями. В частности, скрыты подразделы:

- **Удостоверяющий центр > Сертификаты пользователей > Внешние**
-

пользователи;

- **Удостоверяющий центр > Запросы на сертификаты > Входящие (Удовлетворенные, Отклоненные) > Внешние пользователи;**
 - **Удостоверяющий центр > Запросы на отзыв сертификатов > Входящие.**
-


Отсутствие функциональности программы в части Удостоверяющего центра ViPNet

При отсутствии в программе ViPNet Удостоверяющий и ключевой центр функциональности Удостоверяющего центра:

- Не производится загрузка сертификатов и проверка ключей подписи в ходе запуска программы.
- Не производятся проверки статуса списков отозванных сертификатов (СОС) и сертификатов администраторов, в связи с чем не отображаются соответствующие оповещения.
- При импорте межсетевой информации справочники сертификатов администраторов и СОС удаляются.
- Ключи узлов и обновления ключей не содержат справочники сертификатов администраторов и СОС.
- Все пользователи не имеют права подписи (поскольку для них не могут издаваться сертификаты открытого ключа подписи).
- В интерфейсе программы скрыты либо заблокированы соответствующие элементы:
 - В главном окне программы не отображается раздел **Удостоверяющий центр** со всеми вложенными подразделами.
 - В настройках программы не отображаются разделы **Сертификаты, Публикация, Лицензионное ограничение.**
 - В окне просмотра свойств пользователя и свойств администратора не отображается кнопка **Сертификаты**. В окне просмотра свойств администратора также отсутствуют вкладки **Сертификаты** и **Ключи**.
 - Не отображается пункт контекстного меню **Сертификат** для элементов списка в разделах **Ключевой центр > Своя сеть ViPNet > Пользователи и Администраторы**.
 - Недоступна часть пунктов меню **Сервис** и **Действия**.

Просмотр лицензионного ограничения

Чтобы ознакомиться с лицензией на работу программы ViPNet Удостоверяющий и ключевой центр в качестве Удостоверяющего центра ViPNet (при условии, что она выдана и содержится в файле `infotecs.re`):

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне перейдите в раздел **Лицензионное ограничение**.



Примечание. Данный раздел отображается, только если в файле `infotecs.re` содержится лицензия на издание сертификатов подписи (см. [Лицензионное ограничение](#) (на стр. 14)).

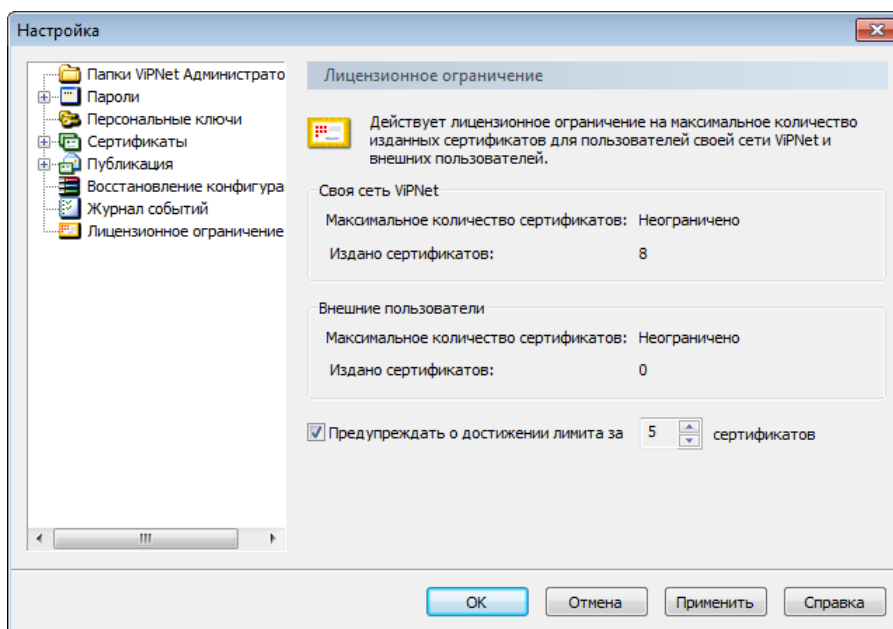


Рисунок 2: Просмотр лицензии

- 3 В разделе **Лицензионное ограничение** просмотрите следующие сведения:
 - В группе **Своя сеть**:
 - максимальное число сертификатов, которые лицензия позволяет издать в программе для пользователей сети ViPNet;
 - число уже изданных сертификатов.

- В группе **Внешние пользователи**:
 - максимальное число сертификатов, которые лицензия позволяет издать в программе для внешних пользователей ViPNet;
 - число уже изданных сертификатов для данной категории пользователей.

Настройка оповещения об окончании лицензии

Чтобы предупреждение о превышении числа издаваемых сертификатов (или так называемого лимита) не являлось неожиданным, при просмотре лицензии (см. [«Просмотр лицензионного ограничения»](#) на стр. 16) можно включить опцию предварительного оповещения о достижении лимита (за определенное число неизданных сертификатов).

Для включения данной опции в настройках программы в разделе **Лицензионное ограничение** установите флажок **Предупреждать о достижении лимита за** и в поле справа введите число сертификатов, которые должны оставаться неизданными до достижения лимита. По умолчанию опция включена, оповещение будет производиться за 5 сертификатов до достижения лимита.

Новые возможности

Что нового в версии 3.2.9

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Удостоверяющий и ключевой центр версии 3.2.9.

В соответствии с Федеральным законом 06.04.2011 N 63-ФЗ «Об электронной подписи» (текст закона <http://www.rg.ru/2011/04/08/podpis-dok.html>) сделаны следующие доработки:

- **Возможность просмотра истории сертификата**

Реализована возможность просмотра истории сертификатов пользователей, изданных и обслуживаемых в УКЦ. История сертификата содержит дату создания сертификата, а также даты всех операций, которые с ним производились (например, даты приостановления действия, возобновления действия, отзыва сертификата, если такие операции осуществлялись).

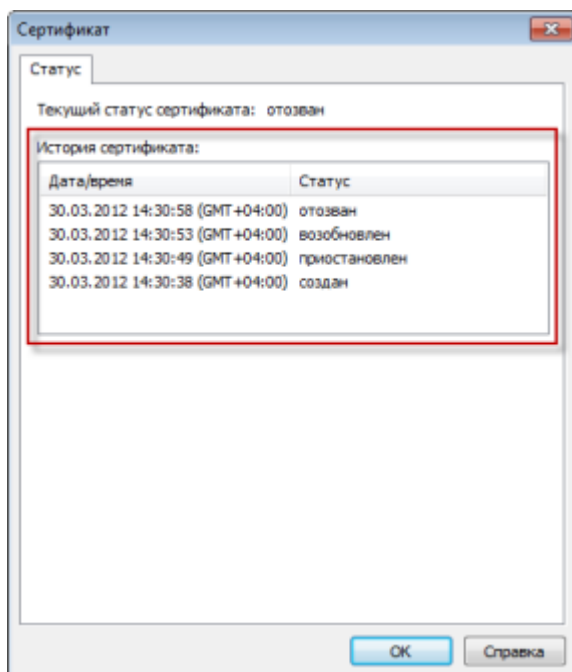


Рисунок 3: Просмотр истории сертификата

- Термин «электронная цифровая подпись» изменен на термин «электронная подпись»

Термин «электронная цифровая подпись» («цифровая подпись») в интерфейсе программы и документации изменен на термин «электронная подпись».

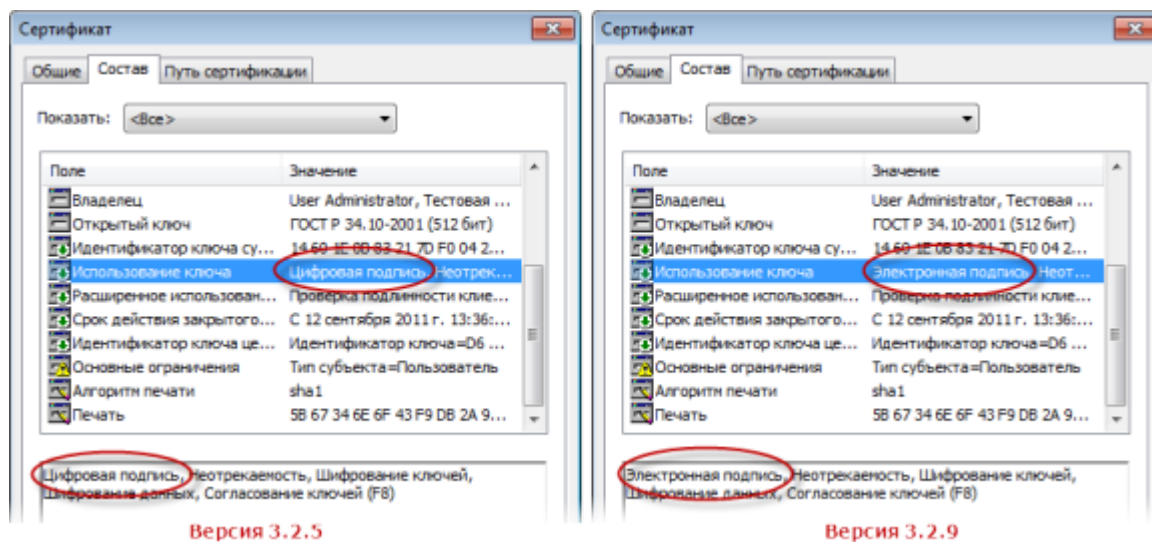


Рисунок 4: Изменение термина «цифровая подпись» на примере окна «Сертификат»

В соответствии с приказом ФСБ РФ 27.12.2011 №795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи» сделаны следующие доработки:

- **Поддержка дополнительных атрибутов имени владельца сертификата: ОГРН и СНИЛС**

В предыдущих версиях в сертификат подписи при издании мог быть добавлен только ИНН в качестве дополнительного атрибута его владельца. В новой версии реализована возможность добавления в сертификат также атрибутов СНИЛС (страховой номер индивидуального лицевого счета) и ОГРН (основной государственный регистрационный номер).

Кроме этого, при задании значений атрибутов ИНН, ОГРН и СНИЛС выполняется проверка допустимости вводимых символов.

Рисунок 5: Возможность задания дополнительных атрибутов имени

- **Атрибут PostalAddress заменен на streetAddress**

Теперь для задания в сертификате адреса его владельца вместо атрибута PostalAddress используется атрибут streetAddress. В связи с этим поле **Почтовый адрес** в мастерах издания сертификатов заменено на поле **Адрес, улица**.

Рисунок 6: Измененное поле ввода адреса владельца сертификата

- **Возможность задания средств электронной подписи Удостоверяющего центра и владельца сертификата**

Предусмотрена возможность указания в сертификате атрибутов, содержащих наименование средства электронной подписи и реквизитов заключения о его соответствии требованиям ФЗ N 63, наименование средства Удостоверяющего центра и реквизитов заключения о его соответствии требованиям ФЗ N 63, а также наименование средства электронной подписи владельца сертификата.

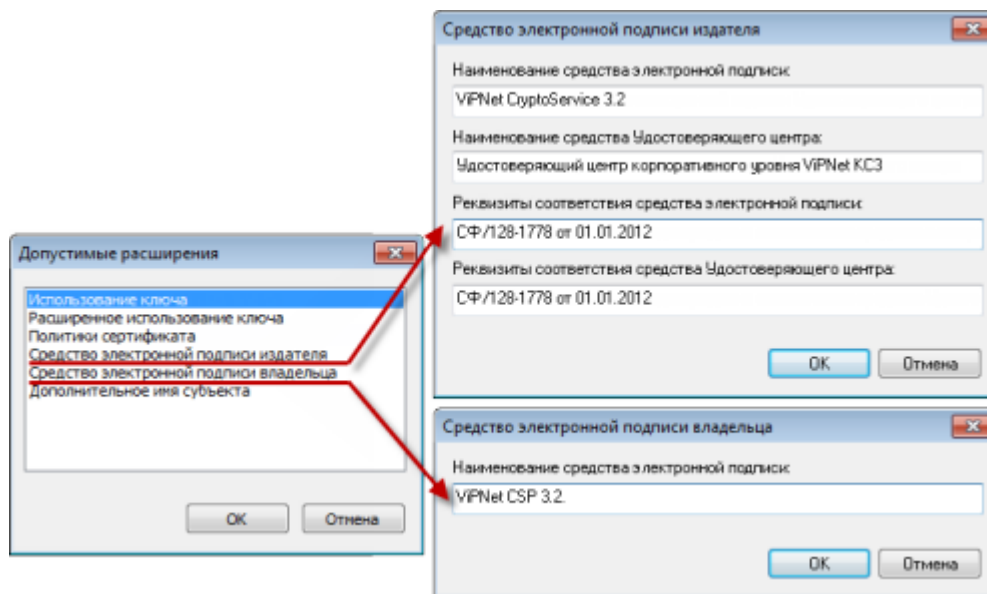


Рисунок 7: Возможность задания средств электронной подписи

- **Возможность выбора шаблона при издании сертификата пользователя**

В предыдущих версиях издание сертификатов пользователей производилось на основе шаблона сертификата, выбранного по умолчанию в настройках программы. Чтобы издание сертификатов производилось в соответствии с нужным шаблоном, шаблон приходилось предварительно задавать в настройках программы. Теперь издание сертификатов производится также в соответствии с параметрами шаблона по умолчанию, но при необходимости шаблон можно изменить в процессе издания сертификата.

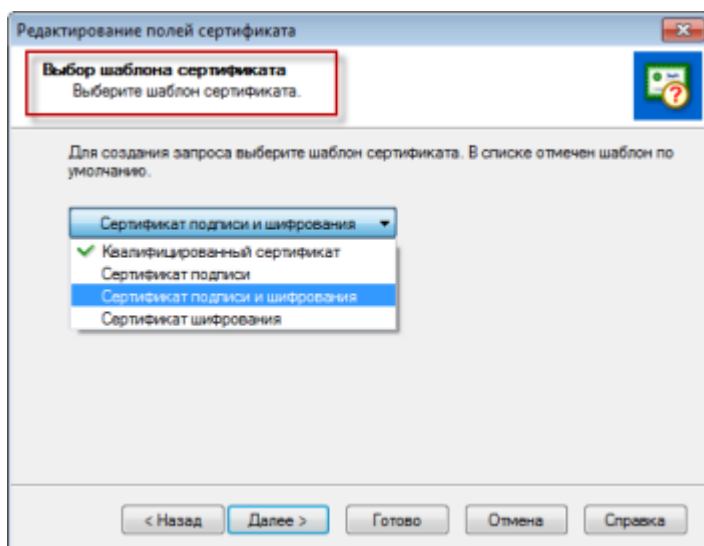


Рисунок 8: Возможность выбора шаблона при издании сертификата

- **Возможность использования шаблона сертификата «Квалифицированный сертификат»**

В конфигурацию программы добавлен новый шаблон сертификата, который может быть использован при издании квалифицированного сертификата (см. «Квалифицированный сертификат»). В данном шаблоне заданы все параметры, которые требуется учитывать при издании квалифицированного сертификата.

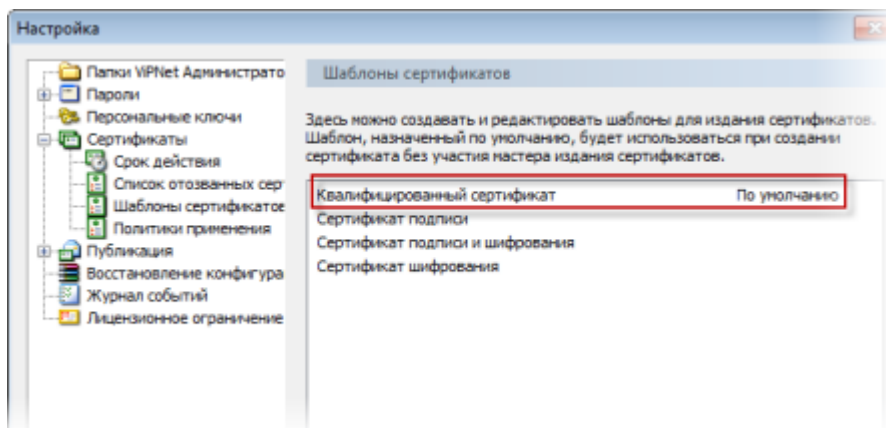


Рисунок 9: Возможность использования готового шаблона для издания квалифицированного сертификата

- **Политики применения, описывающие классы средств электронной подписи**

В конфигурацию программы добавлены политики применения сертификатов, описывающие различные классы средств электронной подписи.

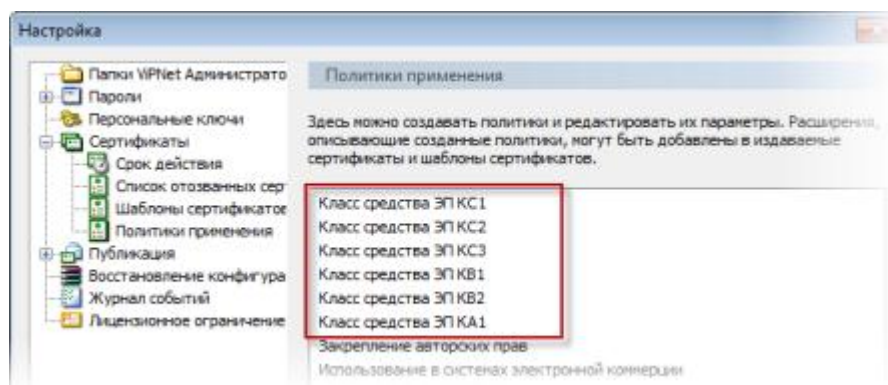


Рисунок 10: Политики применения сертификатов, описывающие классы средств электронной подписи

- **Механизм рассылки информации о политиках применения сертификатов и шаблонах сертификатов, создаваемых в УКЦ**

Реализован механизм рассылки информации о политиках применения и шаблонах сертификатов, задаваемых УКЦ, в Центры регистрации (узлы с программным обеспечением ViPNet Registration Point в сети ViPNet). Теперь после регистрации в УКЦ новой политики применения или после добавления нового шаблона сертификата можно сформировать обновления ключей узлов, с помощью которых в Центры регистрации будет передана информация о данной политике или шаблоне.

Кроме этого, были выполнены следующие доработки:

- **Возможность задания дополнительного имени пользователя**

Появилась возможность задания в сертификате дополнительного имени пользователя (владельца сертификата) в виде DNS-имени либо некоторого произвольного имени, определяемого администратором УКЦ. Необходимость добавления дополнительного имени может возникнуть при издании TLS/SSL-сертификата. Дополнительное имя в таком сертификате позволит расширить границы идентификации его владельца.

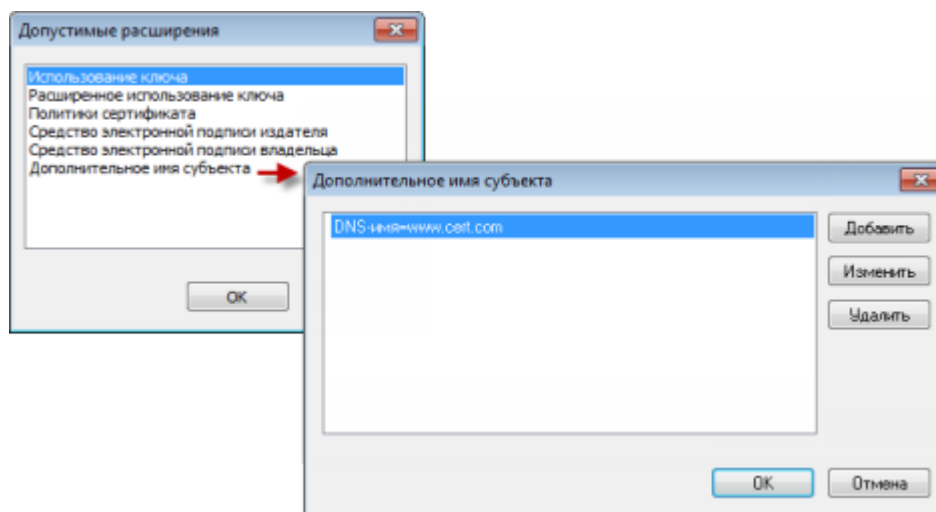


Рисунок 11: Возможность задания альтернативного имени пользователя

- **Расширен список поддерживаемых устройств аутентификации**

Реализована поддержка следующих устройств аутентификации: JaCarta, устройства компании Gemalto с апплетом «Аладдин Р.Д.», устройство Kaztoken с поддержкой казахстанского стандарта электронной подписи. Теперь эти устройства можно применять для хранения персональных ключей и ключей электронной подписи.

- **Усовершенствованная и дополненная документация и справка**

Частично переработаны документация и справка, улучшено их качество. При переработке документации акцент сделан на сценарный подход.

В руководство администратора ViPNet Удостоверяющий и ключевой центр также добавлен сценарий переноса базы данных УКЦ на SQL-сервер.

Что нового в версии 3.2.5

В версии 3.2.5 улучшена внутренняя функциональность программы, исправлены незначительные ошибки, выявленные в процессе эксплуатации версии 3.2.4. Значительно обновлена и актуализирована локализация пользовательского интерфейса программы на английский язык.

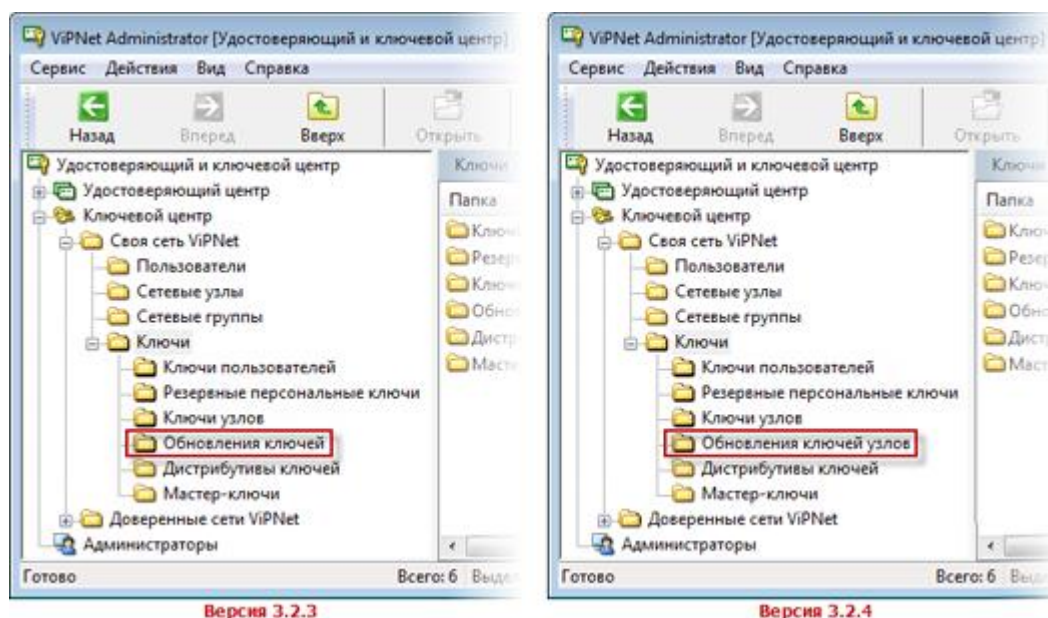
Что нового в версии 3.2.4

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Удостоверяющий и ключевой центр версии 3.2.4.

- **Изменены некоторые термины и названия элементов интерфейса, содержащие эти термины**

Старый термин	Новый термин
Контейнер ключей подписи, ключевой контейнер, контейнер закрытого ключа, контейнер с закрытым ключом, контейнер с открытым ключом	Контейнер ключей
Дистрибутив справочно-ключевой информации	Дистрибутив ключей
Обновления ключей	Обновления ключей узлов

В связи с изменениями переработан интерфейс программы.



- **Дополнена документация**

В руководство администратора ViPNet Удостоверяющий и ключевой центр добавлены два новых сценария: «Издание (отклонение) сертификатов по запросам

от внешних пользователей» и «Обновление сертификата и закрытого ключа администратора».

- **Локализация программы ViPNet Удостоверяющий и ключевой центр на испанский язык**

Пользовательский интерфейс, документация и справка для УКЦ переведены на испанский язык.

Что нового в версии 3.2.3

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Удостоверяющий и ключевой центр версии 3.2.3.

- **Изменены некоторые термины и названия элементов интерфейса, содержащие эти термины**

Старый термин	Новый термин
Ключевой диск (КД)	Ключи пользователя ViPNet
Ключевой набор (КН)	Ключи узла ViPNet

В связи с изменениями значительно переработан интерфейс программы.

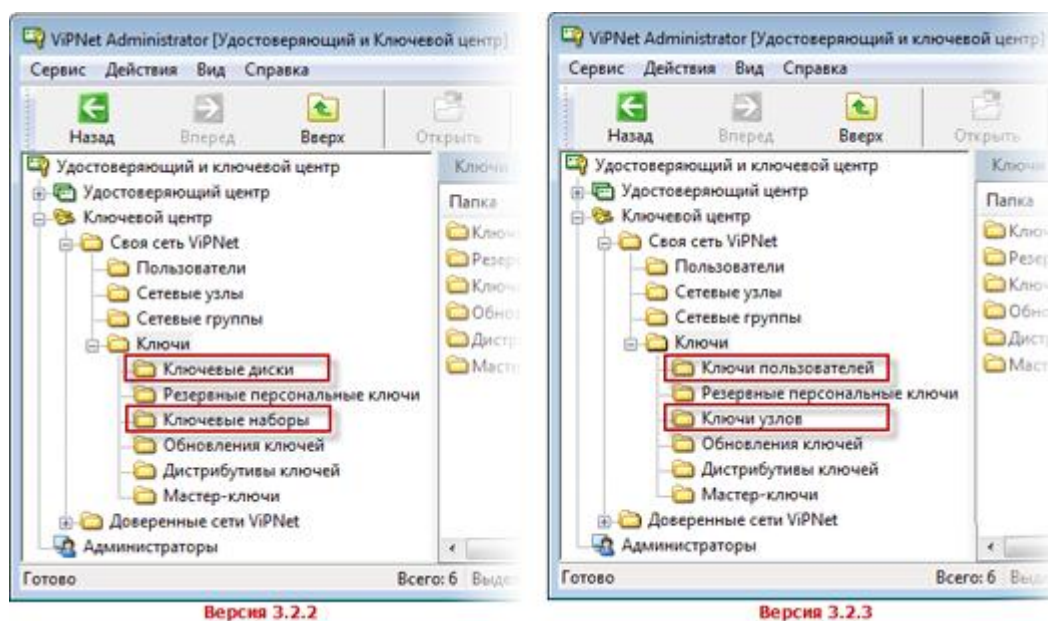


Рисунок 13: Измененный интерфейс программы

Также изменены названия пунктов главного и контекстных меню.

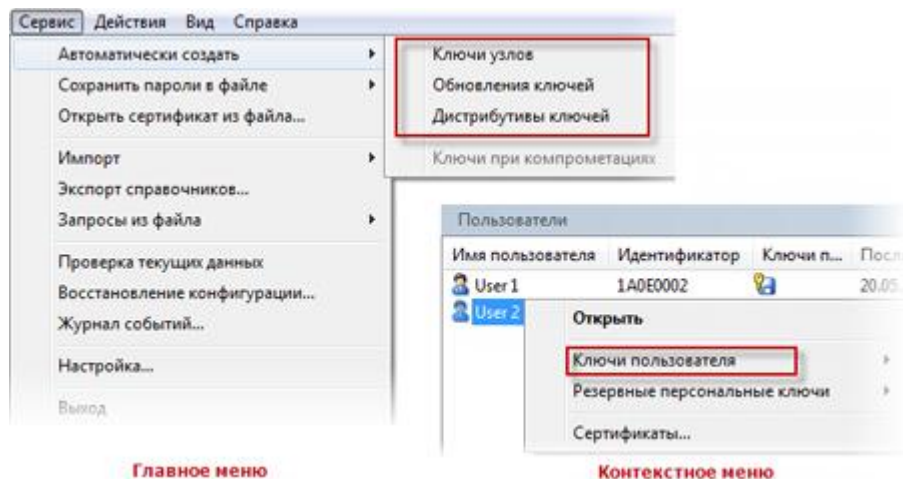


Рисунок 14: Измененные названия пунктов меню

- **Обновлена документация и справка**

В соответствии с заменой терминов обновилась справка и руководство администратора.

Что нового в версии 3.2.2

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Удостоверяющий и ключевой центр версии 3.2.2.

- **Возможность работы с политиками применения**

Появилась возможность регистрации и добавления в сертификат или шаблон сертификата политик применения (см. «[Политика применения сертификата](#)»), содержащих сведения об авторских правах, политиках выдачи сертификатов, ограничениях ответственности и другие данные.

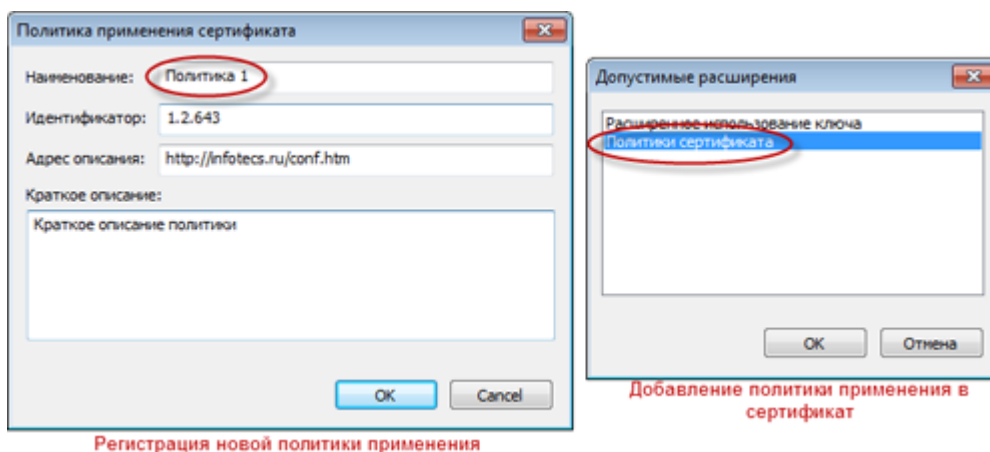


Рисунок 15: Возможность регистрации и добавления политик применения

Также теперь с помощью расширения «Сопоставление политики» можно устанавливать соответствие между политиками применения разных Удостоверяющих центров при издании кросс-сертификатов (см. «Кросс-сертификат»).

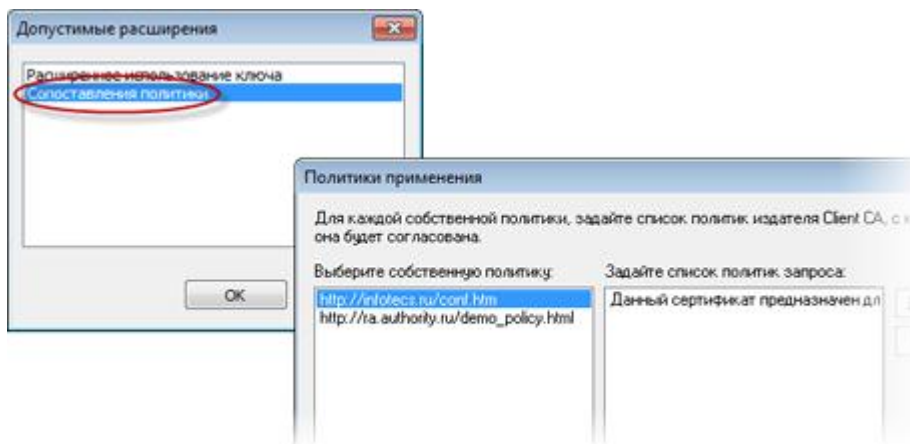


Рисунок 16: Возможность сопоставления политик применения

- **Издание сертификатов по запросам из внешних приложений**

Реализована поддержка запросов на издание сертификатов в форматах PKCS#10 и CMC, что позволяет издавать сертификаты по запросам ViPNet CSP или других приложений.

- **Изменен порядок работы со списками отозванных сертификатов**

Формирование списка отозванных сертификатов (см. «Список отозванных сертификатов (СОС)») осуществляется для каждого сертификата издателя (головного или подчиненного Удостоверяющего центра), в то время как ранее

список отозванных сертификатов мог соответствовать нескольким сертификатам. Обновление СОС производится администратором для соответствующего сертификата при наличии доступа к закрытому ключу.

- **Новые условия при обслуживании сертификатов и кросс-сертификатов**

Выполнять действия (отзыв, приостановление действия или возобновление приостановленного действия) с сертификатами пользователей сети ViPNet или внешних пользователей (см. «[Внешний пользователь ViPNet](#)»), а также отзывать изданные кросс-сертификаты администраторов других Удостоверяющих центров, может тот администратор УКЦ, который является их издателем. При невыполнении данного условия появляется соответствующее уведомление.

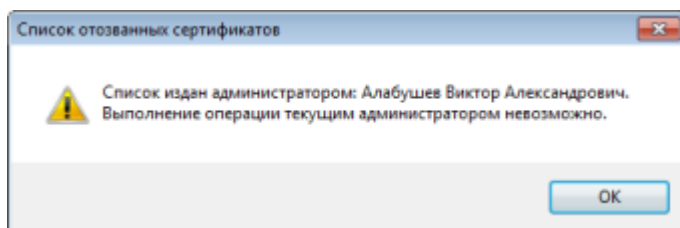


Рисунок 17: Сообщение о невозможности выполнения операции текущим администратором

- **Поддержка бесконтактных карт Mifare**

Реализована поддержка электронных бесконтактных карт Mifare и Mifare Standart 4K в качестве внешних устройств хранения контейнеров ключей.

- **Новый тип точки доступа к публикуемым данным**

Для онлайн проверки статуса сертификатов создан новый тип точки распространения данных — OCSP-сервер. При необходимости в сертификаты пользователей может добавляться расширение, содержащее информацию о данной точке распространения.

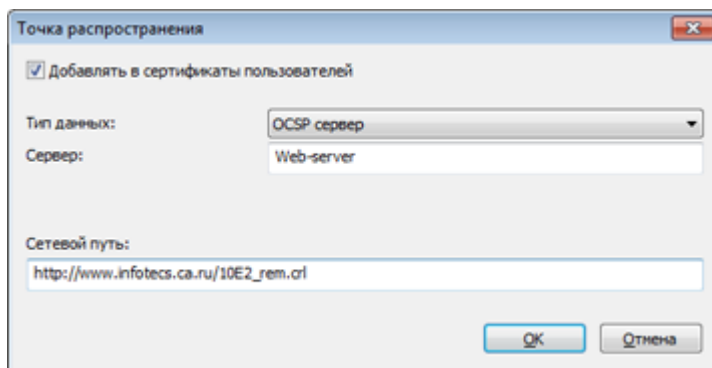


Рисунок 18: Использование нового типа точки распространения

- **Улучшен внешний вид документации и справки**

Изменился шаблон документации и справки, частично переработана структура руководства администратора ViPNet Удостоверяющий и ключевой центр.

Что нового в версии 3.1.x

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Удостоверяющий и ключевой центр версии 3.1.

- **Возможность создания иерархической системы доверительных отношений**

Появилась возможность построения иерархической системы Удостоверяющих центров ViPNet (см. [«Организация иерархической системы доверительных отношений между УЦ»](#) на стр. 86).

- **Изменился срок действия закрытого ключа подписи и сертификата открытого ключа**

Разделены сроки действия закрытого ключа подписи и соответствующего сертификата открытого ключа. Теперь срок действия закрытого ключа пользователя и уполномоченного лица Удостоверяющего центра (администратора УКЦ) составляет 1 год, максимальный срок действия сертификата пользователя увеличен до 5 лет, срок действия сертификата администратора УКЦ — до 6 лет. При истечении срока действия закрытого ключа появляется соответствующее уведомление. При истечении срока действия закрытого ключа на момент создания запроса на сертификат сообщается, что запрос не будет подписан и его корректность должен подтвердить администратор. В УКЦ такие запросы исключаются из автоматической обработки и издание сертификатов по данным запросам возможно только в ручном режиме.

- **Поддержка протокола TLS**

Реализована поддержка протокола TLS, необходимого для организации защищенного соединения. Также внесены изменения в логику формирования ключей и издания сертификатов открытого ключа подписи, которые позволили обеспечить совместимость реализации протокола TLS с криптопровайдером КриптоПро.

- **Другая процедура создания запроса на кросс-сертификат**

Изменился процесс создания запросов на кросс-сертификаты. Мастер создания запроса на кросс-сертификат теперь можно вызвать из контекстного меню при выборе текущего администратора УКЦ.

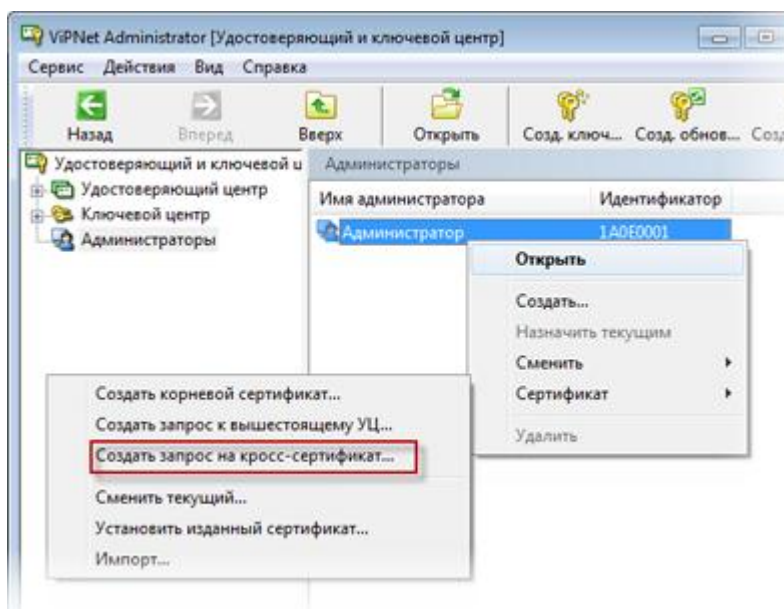


Рисунок 19: Измененный интерфейс при создании запроса на кросс-сертификат

- **Ограничение на функционирование программы в части Удостоверяющего центра ViPNet**

Реализовано лицензионное ограничение на работу УКЦ в качестве Удостоверяющего центра. При отсутствии лицензий на издание сертификатов в программе не будет выполняться ряд функций и отображаться раздел **Удостоверяющий центр** и другие элементы интерфейса (подробнее см. раздел [Отсутствие функциональности программы в части Удостоверяющего центра ViPNet](#) (на стр. 15)).

- **Дополнительные возможности при работе с запросами**

Добавлены возможности просмотра, удаления и повторного экспорта запросов на издание сертификатов к вышестоящему Удостоверяющему центру.

- **Формирование набора назначений при издании сертификата**

Появилась возможность при издании сертификатов задавать произвольный набор назначений, соответствующий выбранному типу сертификата (см. [Мастер редактирования полей сертификата](#) (на стр. 144)).

- **Возможность изменения данных пользователя при издании сертификата**

Реализована возможность редактирования дополнительных полей имени пользователя при издании сертификата (фамилия, имя, инициалы и другие).

- **Использование шаблонов для распечатки сертификатов**

Созданы шаблоны для распечатки сертификатов в установленном формате (файлы `cert_title.rtf` и `cert_signatures.rtf`). Теперь можно осуществлять редактирование шаблонов, указывать названия Удостоверяющего центра или Центра регистрации ViPNet, а также имена владельца сертификата и уполномоченного лица (администратора). Подробнее см. документ «Печать сертификатов. Приложение к документации ViPNet CUSTOM» из комплекта поставки (см. «Комплект поставки» на стр. 40).

- **Возможность автоматического обновления ключей**

Реализована возможность автоматического создания обновлений ключей в соответствии с указанным периодом. Период создания можно задать в настройках программы с помощью соответствующей опции. При включении данной опции УКЦ в течение заданного периода проверяет наличие файлов, принятых из программы ViPNet Центр управления сетью, и в случае их наличия формирует обновление ключей.

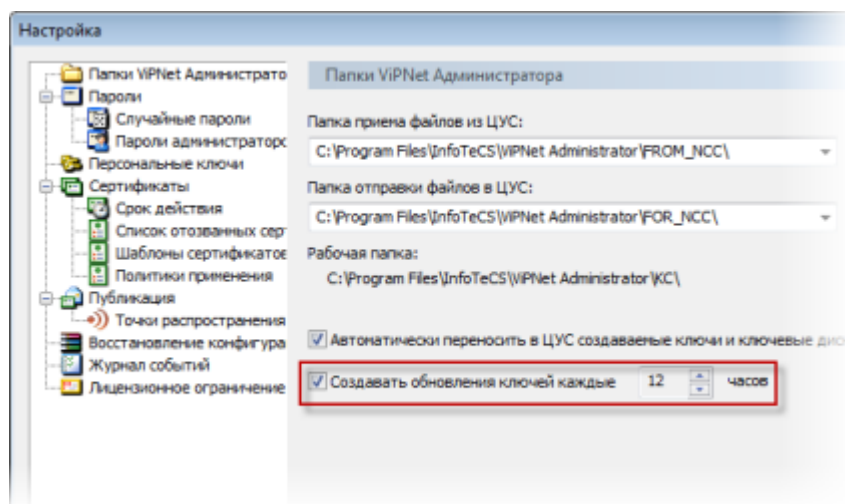


Рисунок 20: Возможность автоматического обновления ключей

- **Возможность изменения цепочки сертификации**

Появилась возможность при создании запроса на кросс-сертификат редактировать длину пути для цепочки сертификатов.

Системные требования

Требования к компьютеру для установки программы ViPNet Удостоверяющий и ключевой центр:

- Процессор — не менее Pentium IV или более производительный, x86-совместимый. Рекомендуется Intel Core 2 Duo E6400 или другой схожий по производительности x86-совместимый процессор с количеством ядер 2+.
- Объем оперативной памяти — не менее 1 Гбайт (при использовании 64-разрядных ОС Windows — не менее 2 Гбайт).
- Свободное место на жестком диске — не менее 1 Гбайт.
- Операционная система — Microsoft Windows XP SP3 (32-разрядная)/Server 2003 (32-разрядная)/Vista SP2 (32/64-разрядная)/Server 2008 (32/64-разрядная)/Windows 7 (32/64-разрядная)/Server 2008 R2 (64-разрядная).



Внимание! Установить УКЦ совместно с программой ViPNet Центр управления сетью можно только на компьютер с 32-разрядной операционной системой Windows.

- При использовании Internet Explorer — версия 6.0 и выше.

Требования к SQL-серверу для развертывания базы данных УКЦ

Программа ViPNet Удостоверяющий и ключевой центр имеет собственную базу данных, которую при необходимости можно развернуть на SQL-сервере. SQL-сервер в таком случае может быть размещен на одном компьютере вместе с УКЦ или на отдельном компьютере и должен быть одним из следующих версий:

- Microsoft SQL Server 2005;
- Microsoft SQL Server 2008;
- Microsoft SQL Server 2008 R2.



Примечание. Редакция перечисленного программного обеспечения может быть любой, в том числе и Express Edition. Но при использовании данной редакции SQL-сервер рекомендуется размещать на одном компьютере вместе с УКЦ (во избежание дополнительных и нестандартных настроек подключения к SQL-серверу с другого компьютера).

Информация о внешних устройствах хранения данных

В ПО ViPNet для записи и считывания персональной информации (паролей, ключей и так далее) имеется возможность использовать различные внешние устройства хранения данных.



Внимание! Хранение ключей нескольких пользователей на одном устройстве невозможно. Однако возможно хранение ключей подписи нескольких пользователей на одном устройстве.

Перед записью ключей на устройство убедитесь, что устройство отформатировано.

Ниже в таблице перечислены устройства и ключи, с которыми может работать ПО ViPNet. Приведенная таблица содержит следующие данные:

- в столбце **Тип устройства** представлены все типы устройств считывания, доступные для выбора в ПО ViPNet;
- в столбце **Тип ключа** представлены типы ключей, используемые для данных устройств;
- в столбце **Необходимые условия работы с ключом** описаны необходимые условия и важные моменты для использования каждого ключа;
- в последнем столбце содержится информация о поддержке стандарта PKCS#11.



Примечание. Стандарт PKCS#11 (также известный как Cryptoki) — один из стандартов семейства PKCS (Public Key Cryptography Standards — криптографические стандарты открытого ключа), разработанных компанией RSA Laboratories. Стандарт определяет независимый от платформы интерфейс API для работы с криптографическими устройствами идентификации и хранения данных.

Таблица 2. Поддерживаемые внешние устройства

Тип устройства	Тип ключа	Необходимые условия работы с ключом	Поддержка стандарта PKCS#11
eToken Aladdin	eToken PRO (персональные электронные ключи, eToken PRO (Java), eToken PRO, смарт-карты eToken PRO (Java), eToken PRO компании «Аладдин Р.Д.»)	<ul style="list-style-type: none"> • На компьютере должно быть установлено программное обеспечение PKI Client версии 5.1 и выше. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 SP2 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная), Server 2008 R2. • Замечание: Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC совместимым USB-устройством считывания с карт. 	Да
iButton	iButton (Dallas) (электронные ключи iButton типа DS1993, DS1994, DS1995 и DS1996)	<ul style="list-style-type: none"> • К компьютеру должно быть подключено устройство считывания. • На компьютере должно быть установлено программное обеспечение обмена информации с iButton, 1-Wire Drivers версии 3.6.2. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32-разрядная), Server 2008 (32-разрядная), Windows 7 (32-разрядная). 	Нет
Smartcard Athena	Смарт-карты с памятью типа I2C (ASE M4), синхронные смарт-карты с шиной 2/3 и защищенной памятью, удовлетворяющие стандарту ISO7816-3 (ASE MP42)	<ul style="list-style-type: none"> • Чтение и запись на смарт-карту осуществляется через считыватель ASEDrive III PRO-S компании Athena. • На компьютере должны быть установлены драйверы версии 2.5.0.0. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная). 	Нет
SmartCard RIK	Российская интеллектуальная	<ul style="list-style-type: none"> • Работа с картой ПО ViPNet может производиться через любой PS/CS- 	Нет

	карта компании «Атлас-Телеком»	совместимый считыватель.	
Shipka	ПСКЗИ ШИПКА компании ОКБ САПР	<ul style="list-style-type: none"> • Перед началом работы с устройством ШИПКА убедитесь, что на АП установлено программное обеспечение ACShipka Environment версии не ниже 3.3.2.6. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная). Проведите инициализацию устройства при помощи утилиты производителя «Параметры авторизации». 	Да
ruToken	Rutoken S, электронный идентификатор компании «Актив»	<ul style="list-style-type: none"> • На компьютере должны быть установлены драйверы Rutoken версий не ниже используемых в установочном комплекте версии 2.81.00.0424. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная). 	Да
ruTokenЕСР	Rutoken ЭЩП, электронный идентификатор компании «Актив»	<ul style="list-style-type: none"> • На компьютере должны быть установлены драйверы версии не ниже 2.81.00.0424. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная). 	Да
Аккорд-5MX	iButton типа DS1993, DS1994, DS1995 и DS1996	<ul style="list-style-type: none"> • На компьютере должен быть установлен драйвер версии не ниже 3.18.0.0. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32-разрядная), Server 2008 (32-разрядная). 	Нет

Siemens CardOS	Смарт-карты Siemens (CardOS/M4.01a, CardOS V4.3B, CardOS V4.2B, CardOS V4.2B DI, CardOS V4.2C, CardOS V4.4)	<ul style="list-style-type: none"> Для работы на компьютере должно быть установлено ПО Siemens CardOS API V5.0 или выше Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 EE SP2 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 SP2 (32/64-разрядная), Windows 7 (32/64-разрядная). 	Да
Mifare	Rosan Mifare	<ul style="list-style-type: none"> Для работы с устройством необходимо наличие COM-порта. Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista (32-разрядная), Windows 7 (32/64-разрядная). 	Нет
Mifare Standard4K	Mifare 4K	<ul style="list-style-type: none"> Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista (32-разрядная), Windows 7 (32/64-разрядная). Для работы с устройством используется интерфейс подключения USB 2.0 (совместимый с USB 1.1). Карта Mifare 4K поддерживается только через считыватель ACR128. 	Нет
еToken ГОСТ (не поддерживаетя ПО VipNet Удостоверяющий и ключевой центр)	еToken ГОСТ Aladdin	<ul style="list-style-type: none"> Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista (32-разрядная), Windows 7 (32/64-разрядная). Примечание: устройство поддерживает ГОСТ 34.10-2001. 	Да
JCDS	Смарт-карты Gemalto Optelio Contactless D72, KONA 131 72K	<ul style="list-style-type: none"> На карту должен быть загружен апплет, позволяющий модулю jcrkcs11ds.dll компании «Аладдин Р.Д.» работать с картой. Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 SP2 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная), Server 2008 R2. 	Да

JaCarta	Персональные электронные ключи JaCarta компании «Аладдин Р.Д.»	<ul style="list-style-type: none"> • На компьютере должно быть установлено программное обеспечение JC-Client компании «Аладдин Р.Д.». • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 SP2 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная), Server 2008 R2. 	Да
Kaztoken	Персональные электронные ключи Kaztoken	<ul style="list-style-type: none"> • На компьютере должны быть установлены драйверы Kaztoken версии не ниже 2.53.00.0365. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная). 	Да

Комплект поставки

Программа ViPNet Удостоверяющий и ключевой центр поставляется в рамках программного обеспечения ViPNet Administrator совместно с ViPNet Центр управления сетью.

В комплект поставки программного обеспечения ViPNet Administrator входит:

- Установочный файл `setup.exe`.
- Документация в формате PDF, в том числе:
 - «ViPNet Administrator Удостоверяющий и ключевой центр. Руководство администратора».
 - «ViPNet Administrator Центр управления сетью. Руководство администратора».
 - «Развертывание сети ViPNet. Руководство администратора».
 - «Классификация полномочий. Приложение к документации ViPNet CUSTOM».
 - «Печать сертификатов. Приложение к документации ViPNet CUSTOM».
 - «Основные термины и определения. Приложение к документации ViPNet CUSTOM».
 - «Порядок разбора конфликтных ситуаций, возникающих при использовании электронной подписи. Руководство администратора».
 - «Инструкция по установке и настройке защищённого рабочего места ViPNet Administrator. Приложение к документации ViPNet CUSTOM».
 - «Обновление ViPNet Administrator с версии 2.8.x до версии 3.2.x. Приложение к документации ViPNet CUSTOM 3.2».
 - «Обновление ViPNet Administrator с версии 3.1.x до версии 3.2.x. Приложение к документации ViPNet CUSTOM 3.2».

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/>.
- Форум компании «ИнфоТеКС» <http://www.infotecs.ru/forum>.
- 8 (495) 737-6196 — «горячая линия» службы поддержки.
- 8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).



1

Установка и настройка программы ViPNet Удостоверяющий и ключевой центр

Варианты развертывания	43
Выбор необходимого дополнительного программного обеспечения ViPNet	44
Порядок развертывания	46
Установка программы	48
Проведение первичной инициализации программы	50

Варианты развертывания

Программа ViPNet Удостоверяющий и ключевой центр может быть развернута на одном компьютере вместе со вторым компонентом программного обеспечения ViPNet Administrator — программой ViPNet Центр управления сетью (далее — ЦУС), либо на отдельном компьютере, если этого требует политика безопасности организации.

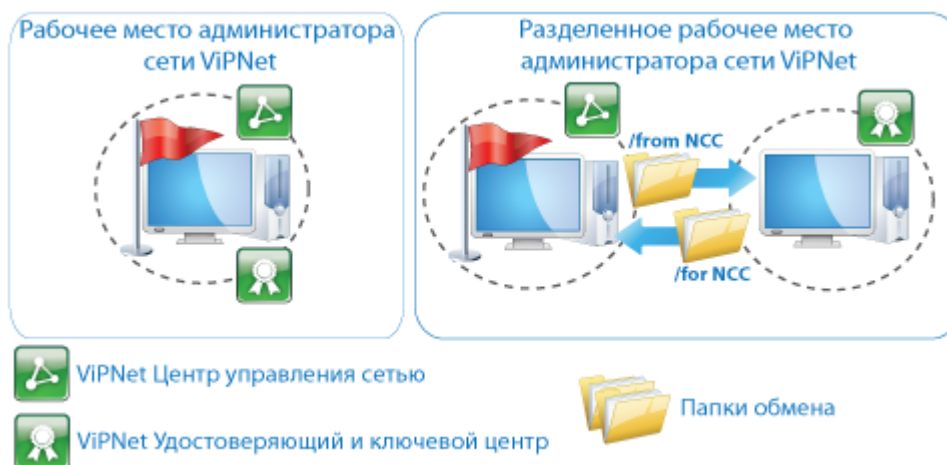


Рисунок 21: Варианты развертывания УКЦ

Первый вариант развертывания является типовым и достаточно распространенным. УКЦ и ЦУС совместно устанавливаются на компьютер, выделенный под рабочее место администратора сети ViPNet.

Во втором варианте развертывания установка ЦУС и УКЦ производится на разные компьютеры. При использовании данной схемы развертывания требуются дополнительные настройки:

- В ЦУСе должны быть созданы два абонентских пункта (один непосредственно для ЦУС, второй — для УКЦ).
- На компьютере, на котором установлен ЦУС, требуется задать папки обмена информацией между ЦУС и УКЦ.
- Для компьютера, на котором установлен УКЦ, требуется открыть сетевой доступ к заданным папкам обмена.

Выбор необходимого дополнительного программного обеспечения ViPNet

На рабочее место администратора сети ViPNet в обязательном порядке устанавливается дополнительное программное обеспечение ViPNet Client либо ViPNet CryptoService. При этом если программы ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр развернуты на разных компьютерах, то дополнительное программное обеспечение устанавливается на тот компьютер, на котором размещен ЦУС. На компьютер с УКЦ также можно установить дополнительное программное обеспечение, но в большинстве случаев это не требуется. В целях безопасности рекомендуется этот компьютер вообще не подключать к сети, соединив его только с компьютером, на котором установлен ЦУС.

Чаще всего в качестве дополнительного программного обеспечения выбирают ViPNet Client, поскольку он позволяет:

- Организовать защиту (шифрование) IP-трафика между рабочим местом администратора и другими узлами сети (см. схему ниже).
- Обеспечить защиту рабочего места администратора от несанкционированного доступа при работе в локальных и глобальных сетях с помощью встроенного межсетевого экрана.



Рисунок 22: Разделенное рабочее место администратора с установленным ПО ViPNet Client

ViPNet CryptoService используется только в том случае, если защита трафика и дополнительная защита рабочего места администратора не требуется.



Порядок развертывания

Для успешного развертывания программы ViPNet Удостоверяющий и ключевой центр требуется выполнить все действия из приведенного ниже списка.

Действие	Ссылка
<ul style="list-style-type: none">□ Продумайте схему развертывания УКЦ. В зависимости от выбранной схемы развертывания подготовьте нужное количество компьютеров и организуйте их подключение к физической сети.	Варианты развертывания (на стр. 43)
<ul style="list-style-type: none">□ Выполните установку УКЦ с учетом выбранной схемы развертывания. Установите ЦУС на другом компьютере при условии, что он не был установлен вместе с УКЦ и должен быть размещен отдельно от него. Установка ЦУСа будет производиться аналогично установке УКЦ.	Установка программы (на стр. 48)
<ul style="list-style-type: none">□ Выполните установку программы ViPNet Client либо ViPNet CryptoService с учетом выбранной схемы развертывания и ваших потребностей.	См. соответствующие документы: «ViPNet Client Монитор. Руководство пользователя» «ViPNet CryptoService. Руководство администратора»
<ul style="list-style-type: none">□ Если ЦУС и УКЦ были установлены на разные компьютеры, на обоих компьютерах выполните настройку папок обмена информацией между ЦУСом и УКЦ.	См. документ «Развертывание сети ViPNet. Руководство администратора», главу «Подготовка к развертыванию сети ViPNet», раздел «Установка ViPNet Administrator» Настройка папок обмена в УКЦ также подробно описана в разделе Настройка папок обмена (на стр. 239) данного документа
<ul style="list-style-type: none">□ В ЦУСе создайте структуру защищенной сети ViPNet, выполните регистрацию пользователей и другие необходимые операции, после чего сформируйте справочники для УКЦ.	См. документ «Развертывание сети ViPNet. Руководство администратора», главу «Создание топологии сети в ViPNet Administrator»

- | | |
|---|---|
| <ul style="list-style-type: none">❑ Выполните процедуру первичной инициализации УКЦ. Предварительно разверните SQL-сервер, если база данных УКЦ будет размещена на нем.❑ После запуска УКЦ сформируйте дистрибутивы ключей ViPNet.❑ Проведите первичную инициализацию установленного программного обеспечения ViPNet Client либо ViPNet CryptoService (в зависимости от того, что было установлено). При инициализации используйте дистрибутив ключей, сформированный в УКЦ на предыдущем шаге. | <p>Проведение первичной инициализации программы (на стр. 50)</p> <p>Создание дистрибутивов ключей (на стр. 91)</p> <p>См. раздел «Установка и первичная инициализация» в соответствующих документах:</p> <p>«ViPNet Client Монитор. Руководство пользователя»</p> <p>«ViPNet CryptoService. Руководство администратора»</p> |
|---|---|
-



Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Развертывание УКЦ должен производить администратор сети ViPNet (администратор УКЦ).


Установка программы

Установку программы ViPNet Удостоверяющий и ключевой центр должен выполнять пользователь, обладающий правами администратора в операционной системе Windows.

Прежде чем начать установку программы:

- Убедитесь, что располагаете соответствующим установочным файлом `setup.exe` ViPNet Administrator.
УКЦ функционирует совместно с программой ViPNet Центр управления сетью в составе программного обеспечения ViPNet Administrator, поэтому для установки данных программ используется один установочный файл.
- Убедитесь, что располагаете файлами лицензии `infotecs.reg` и `infotecs.re`. Данные файлы предоставляют право на использование УКЦ и ЦУСа. Для работы с УКЦ файл `infotecs.reg` не требуется.
- Убедитесь, что на компьютере выполнены стандартные сетевые настройки, а также правильно заданы часовой пояс, дата и время.

Для установки программы выполните следующие действия:

- 1 Скопируйте файлы лицензии в одну папку с программой установки `setup.exe`. Тогда при установке они автоматически будут помещены в нужные папки (в папку установки УКЦ — файл `infotecs.re`, в папку установки ЦУСа — файлы `infotecs.re` и `infotecs.reg`). В противном случае после установки программы необходимо будет вручную поместить файлы лицензии в указанные папки.
- 2 Двойным щелчком запустите программу установки `setup.exe` .
- 3 Следуйте указаниям мастера установки.
- 4 Если на компьютер требуется установить только УКЦ (ЦУС будет размещен на другом компьютере (см. раздел [Варианты развертывания](#) (на стр. 43)), то в процессе установки выполните следующие действия:
 - На странице **Тип установки** выберите пункт **Выборочная установка**.
 - На странице **Компоненты программного продукта** снимите флажок **ViPNet Центр управления сетью**.
- 5 По окончании установки перезагрузите компьютер.

- 6 Если перед установкой программы файлы лицензии не были скопированы в одну папку с программой установки, поместите в папку установки УКЦ файл `infotecs.re`.



Примечание. По умолчанию УКЦ устанавливается в папку `C:\Program Files\InfoTeCS\ViPNet Administrator\КЦ` в 32-разрядных версиях Windows и в папку `C:\Program Files (x86)\InfoTeCS\ViPNet Administrator\КЦ` — в 64-разрядных версиях.

- 7 После этого выполните процедуру первичной инициализации (см. [«Проведение первичной инициализации программы»](#) на стр. 50).

Дополнительную информацию о развертывании УКЦ в типовой защищенной сети ViPNet можно узнать в документе «Развертывание сети ViPNet. Руководство администратора».

Проведение первичной инициализации программы

Процедура первичной инициализации программы ViPNet Удостоверяющий и ключевой центр проводится при ее первом запуске, после того, как в программе ViPNet Центр управления сетью была создана структура сети ViPNet и сформированы адресные справочники.



Примечание. Первичная инициализация УКЦ также проводится при обновлении программного обеспечения ViPNet Administrator с версии 2.8.x до версии 3.0.x и выше. В этом случае при проведении первичной инициализации требуется выполнить один дополнительный шаг — перенести ключи ViPNet из старой базы данных УКЦ (версии 2.8.x) в новую (версии 3.0.x и выше).


Подробное описание первичной инициализации в процессе обновления программного обеспечения приведено в документе «Обновление ViPNet Administrator с версии 2.8.x до версии 3.2.x. Приложение к документации ViPNet CUSTOM 3.2» из комплекта поставки (см. [«Комплект поставки»](#) на стр. 40).

При первичной инициализации осуществляется развертывание базы данных УКЦ и ее наполнение информацией, переданной ЦУСом в адресных справочниках. Базу данных УКЦ в процессе инициализации можно развернуть либо локально на компьютере на основе шаблона базы данных Microsoft Access, включенного в конфигурацию программы, либо на SQL-сервере.

В первом случае дополнительные действия не нужны, СУБД Microsoft Access устанавливать не требуется. Мастер первичной инициализации при выборе соответствующего драйвера ODBC (см. [«ODBC \(Open Database Connectivity\)»](#)) производит поиск шаблона базы Microsoft Access, после чего на его основе формирует базу данных (файл `kc.mdb`), размещает ее в указанной папке на компьютере и наполняет содержимым.

Во втором случае требуется предварительная установка SQL-сервера (см. [«Требования к SQL-серверу для развертывания базы данных УКЦ»](#) на стр. 33). На SQL-сервере в процессе инициализации мастер формирует базу данных «КС» и, также как и в первом случае, заполняет ее данными.

Чтобы провести процедуру первичной инициализации УКЦ, выполните следующие действия:

- 1 Запустите программу из меню **Пуск** или дважды щелкните значок  на рабочем столе (см. [Запуск и завершение работы с программой](#) (на стр. 59)). Будет запущен мастер первичной инициализации, следуйте его указаниям.
- 2 На странице **Выбор драйвера ODBC** в списке выберите драйвер ODBC для доступа и работы с базой данных УКЦ:
 - **Microsoft Access Driver (*.mdb)** — если база данных будет развернута локально на компьютере с использованием шаблона Microsoft Access (*.mdb). Microsoft Access Driver идет в составе операционной системы Windows.
 - **SQL Server** — если база данных будет развернута на SQL-сервере.

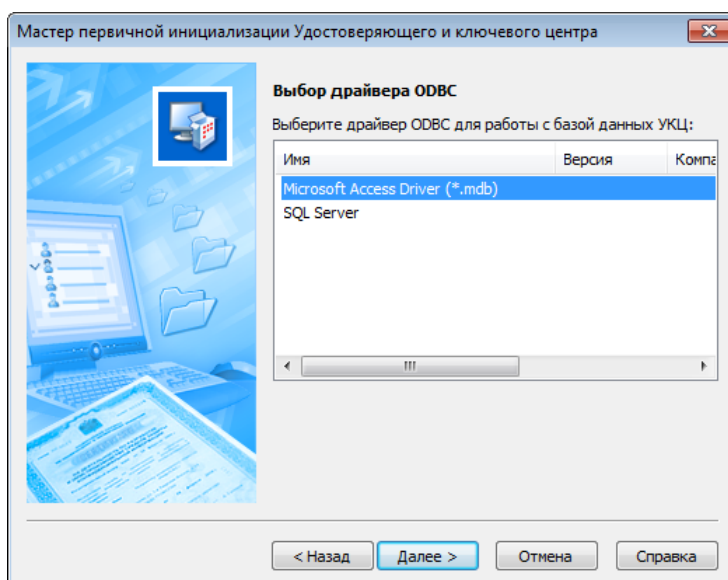


Рисунок 23: Выбор драйвера ODBC

Нажмите кнопку **Далее**.

- 3 Если в качестве драйвера ODBC был выбран **SQL Server**, укажите дополнительные параметры для работы с SQL-сервером:
 - На странице **Выбор SQL сервера** выберите (или введите) экземпляр SQL-сервера, на котором будет развернута база данных УКЦ, после чего нажмите кнопку **Далее**.
 - На странице **Проверка подлинности пользователя на SQL сервере** выберите тип аутентификации при подключении к SQL-серверу.

При выборе типа **По имени и паролю пользователя SQL сервера** укажите имя пользователя, под учетной записью которого будет осуществляться подключение к SQL-серверу, и пароль.



Примечание. Тип аутентификации **По сетевому имени пользователя Windows NT** может использоваться в том случае, если SQL-сервер размещен на одном компьютере с УКЦ. Тип **Проверка подлинности пользователя на SQL сервере** является рекомендуемым и используется при удаленном подключении к SQL-серверу.

Узнать параметры подключения к SQL-серверу и получить все необходимые учетные данные следует у его администратора.

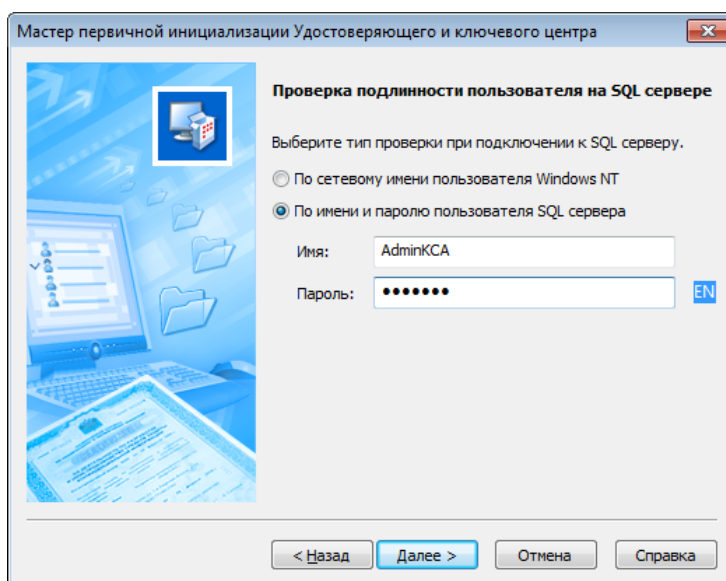



Рисунок 24: Выбор типа аутентификации при подключении к SQL-серверу

После этого нажмите кнопку **Далее**. Будет установлено соединение с SQL-сервером. При успешном соединении на сервере в соответствующем экземпляре будет создана база данных УКЦ, результат создания будет отображен на странице **Создание базы данных**.

Если установить соединение с сервером не получится, проверьте правильность всех ранее введенных параметров.

- 4 На странице **Папки Удостоверяющего и ключевого центра** выполните настройку папок, которые будут использоваться при работе УКЦ и ее взаимодействии с ЦУСом. С помощью кнопок  выберите:

- В поле **Папка для приема файлов из ЦУС** — папку, в которой будут находиться файлы, обработанные в ЦУСе. По умолчанию назначена папка: `\ViPNet Administrator\FROM_NCC`.
- В поле **Папка для отправки файлов в ЦУС** — папку, в которой будут находиться файлы, предназначенные для обработки в ЦУСе. По умолчанию назначена папка: `\ViPNet Administrator\FOR_NCC`.

Совет. Если УКЦ и ЦУС были установлены на одном компьютере, то не рекомендуется изменять папки приема и отправки файлов, предложенные по умолчанию. При изменении папок следует учитывать, что в настройках ЦУСа должны быть выбраны аналогичные папки, и доступ к этим папкам должен быть открыт для УКЦ.



О том, как настроить папки обмена в ЦУСе, см. документ «ViPNet Administrator Центр управления сетью. Руководство администратора», главу «Управление сетью», раздел «Настройка путей (пункт меню „Пути“)».

Папки приема и отправки файлов (или так называемые папки обмена) также можно изменить в процессе работы с УКЦ. Подробнее см. раздел [Настройка папок обмена](#) (на стр. 239).

- В поле **Рабочая папка** — папку, в которой будут сохраняться файлы, создаваемые УКЦ во время работы. Если база данных создается по типу Microsoft Access, то она также будет находиться в данной папке. По умолчанию выбрана папка установки УКЦ: `\ViPNet Administrator\КС`, рекомендуется ее сохранить и использовать по умолчанию.

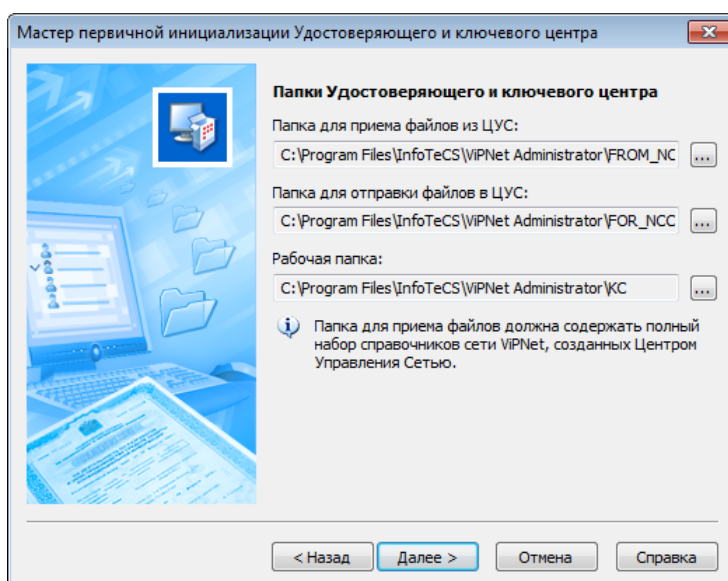


Рисунок 25: Выбор папок для работы УКЦ

Нажмите кнопку **Далее**. Если была задана неверная папка приема файлов из ЦУСа или в папке приема не будет нужных файлов адресных справочников (например, если в ЦУСе они не были сформированы), то появится сообщение с просьбой скопировать адресные справочники и переход на следующую страницу мастера будет невозможен.

- 5 Зарегистрируйте учетную запись администратора УКЦ, при регистрации укажите параметры его сертификата открытого ключа подписи. Описание всех необходимых для этого действий см. в разделе [Создание учетной записи администратора](#) (на стр. 199).



Примечание. При регистрации администратора потребуется создать пароль для работы с УКЦ. Можно создать случайный пароль с предварительной настройкой его параметров. В дальнейшем эти параметры по умолчанию будут использоваться для создания случайных паролей других пользователей, при необходимости их можно изменить (см. [«Настройка параметров случайных паролей»](#) на стр. 243).

- 6 После того как будет назначен администратор УКЦ и заданы параметры его сертификата подписи, на странице **Создание мастер-ключей** нажмите кнопку **Далее**. На данной странице отображаются названия и номера всех мастер-ключей, которые будут созданы при первичной инициализации.

Если в дальнейшем планируется устанавливать межсетевое взаимодействие с доверенными сетями ViPNet, создайте асимметричный межсетевой мастер-ключ для его последующего экспорта. Для этого установите соответствующий флажок. Создание межсетевых мастер-ключей можно выполнить и в процессе работы с УКЦ (см. раздел [Создание межсетевых мастер-ключей](#) (на стр. 120)).

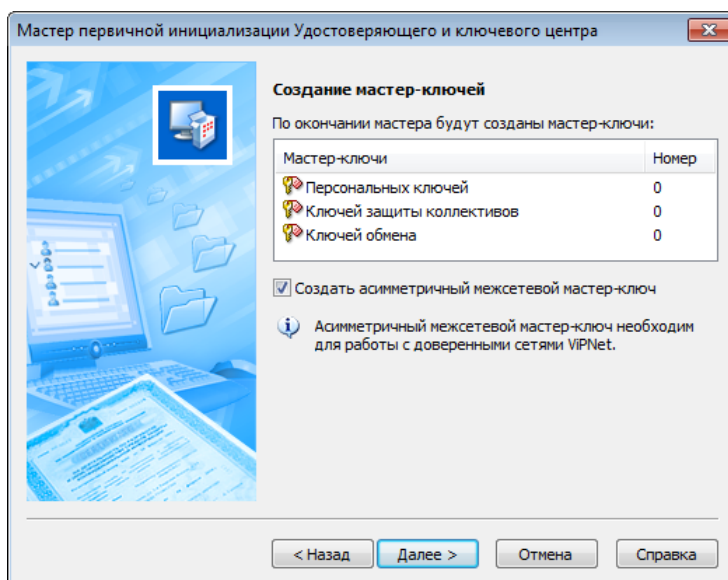


Рисунок 26: Создание мастер-ключей при первичной инициализации

7 Выполните действия, предлагаемые в окне **Электронная рулетка**.

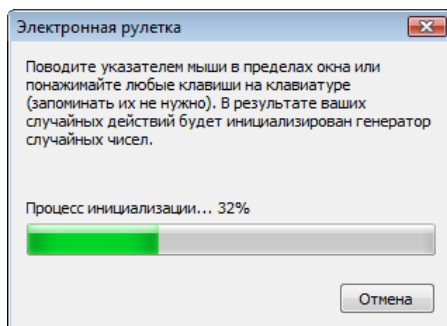


Рисунок 27: Электронная рулетка

Запустится процесс инициализации, при котором будут выполнены следующие операции:

- Создание учетной записи администратора программы (сети ViPNet).
- Издание сертификата администратора.
- Создание мастер-ключей. Создание межсетевого мастер-ключа при выборе соответствующей опции.
- Создание источника данных и частичное заполнение базы данных УКЦ (независимо от места ее размещения).

Результат проведения данных операций отобразится на последней странице мастера.

8 Убедитесь, что первичная инициализация успешно завершена, после чего нажмите кнопку **Готово**. При успешном завершении инициализации на последней странице

мастера появится соответствующее сообщение и напротив каждой выполненной операций будет значок ✓.

Если при инициализации какие-то операции будут выполнены с ошибками, то они будут отмечены значком ✗.

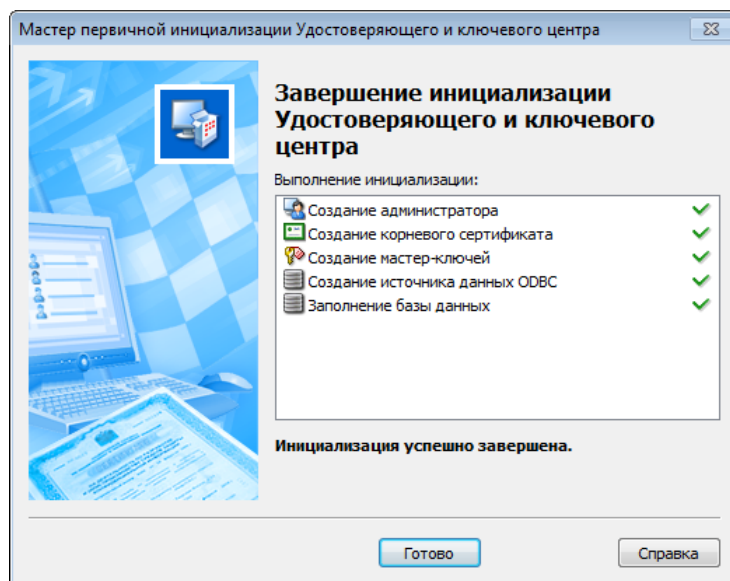


Рисунок 28: Завершение первичной инициализации

В случае корректной инициализации появится главное окно программы (см. «Интерфейс программы ViPNet Удостоверяющий и ключевой центр» на стр. 64). Можно приступать к работе с УКЦ.

Если инициализация была проведена некорректно, установите причину неудачи (см. «Возможные причины некорректной инициализации» на стр. 56) и выполните следующие действия:

- При развертывании базы на компьютере — переустановите УКЦ с предварительным удалением текущей версии программы и повторно проведите первичную инициализацию.
- При развертывании базы на SQL-сервере — удалите базу данных, созданную на SQL-сервере, после чего повторно проведите первичную инициализацию.

Возможные причины некорректной инициализации

Причинами некорректного проведения первичной инициализации могут быть:

- Поврежденные данные в адресных справочниках.
- Некорректная работа датчика случайных чисел (электронной рулетки).

- Повреждение при установке программы либо отсутствие необходимых динамически подгружаемых библиотек dll (dynamic load library).
- При развертывании базы данных на SQL-сервере — случайное или умышленное повреждение (удаление) базы данных.



2

Начало работы с программой ViPNet Удостоверяющий и ключевой центр


Запуск и завершение работы с программой	59
Подключение к SQL-серверу при запуске программы	62
Интерфейс программы ViPNet Удостоверяющий и ключевой центр	64

Запуск и завершение работы с программой

Чтобы запустить программу ViPNet Удостоверяющий и ключевой центр:

1 Выполните одно из действий:

- В меню **Пуск** выберите пункт **Все программы**, затем **ViPNet**, затем **Administrator** и щелкните **ViPNet Administrator Удостоверяющий и ключевой центр**. При установке путь к программе в меню **Пуск** мог быть изменен.

- Дважды щелкните значок  на рабочем столе (значок отображается, если при установке программы была выбрана соответствующая опция).



Примечание. Для запуска УКЦ также можно дважды щелкнуть по файлу `KeyCenter.exe` из папки установки программы (по умолчанию: `\ViPNet Administrator\KC`).

2 В появившемся окне выберите учетную запись администратора, под которой будет производиться вход в программу, и введите пароль (см. «[Пароль администратора УКЦ](#)»).

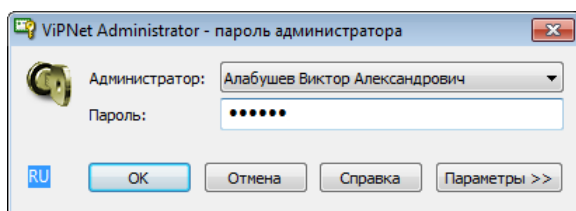



Рисунок 29: Окно входа в программу

3 Укажите место хранения ключей администратора, в том случае, если оно было изменено, либо если ключи находятся на внешнем устройстве хранения данных. Для этого в окне входа в программу нажмите кнопку **Параметры** и в скрытой ранее группе **Устройство хранения ключей** установите переключатель в положение:

- **Папка**, если ключи администратора хранятся в папке на компьютере. После этого с помощью кнопки  укажите путь к нужной папке с ключами.

- **Устройство**, если ключи администратора хранятся на внешнем устройстве (см. «[Информация о внешних устройствах хранения данных](#)» на стр. 35). После этого подключите устройство хранения ключей, выберите его в соответствующем списке и введите ПИН-код (если требуется).



Примечание. Необходимость ввода ПИН-кода зависит от типа используемого внешнего устройства. Чтобы сохранить ПИН-код и в дальнейшем не вводить его при аутентификации, в окне входа в УКЦ установите соответствующий флажок.

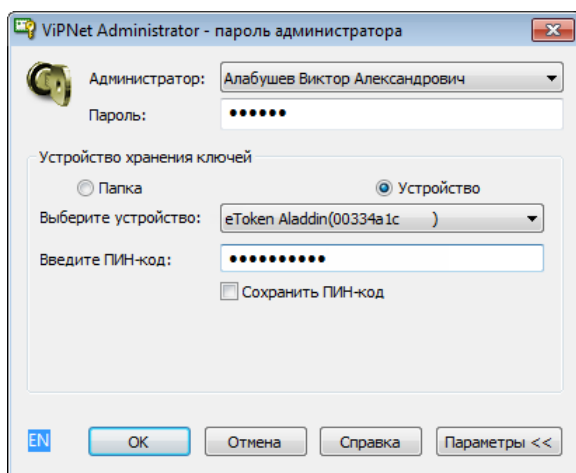



Рисунок 30: Окно входа в программу с указанием места хранения ключей


- 4 После ввода необходимых для аутентификации данных нажмите кнопку **ОК**.

Если база данных УКЦ находится локально на компьютере, появится главное окно программы (см. «[Интерфейс программы VIPNet Удостоверяющий и ключевой центр](#)» на стр. 64). Можно приступить к работе с УКЦ.

При размещении базы данных на SQL-сервере сначала будет выполнена проверка соединения с сервером. Если проверка пройдет успешно, произойдет вход в программу и появится главное окно УКЦ. В противном случае, появится окно подключения к SQL-серверу. Проверьте правильность параметров, заданных в данном окне, и при необходимости их измените. Подробнее см. раздел [Подключение к SQL-серверу при запуске программы](#) (на стр. 62).

Чтобы свернуть окно программы на панель задач, нажмите кнопку **Свернуть**  в правом верхнем углу окна.

Чтобы завершить работу с программой, выполните одно из действий:

- В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Выход**.
- Нажмите кнопку **Заккрыть**  в правом верхнем углу окна.

Если в настройках программы установлена опция автоматического создания резервных копий, то перед выходом из программы будет создана резервная копия ее текущей конфигурации (см. [«Создание и восстановление резервных копий конфигурации программы»](#) на стр. 277).

Подключение к SQL-серверу при запуске программы

Если база данных программы ViPNet Удостоверяющий и ключевой центр размещена на SQL-сервере, то при запуске УКЦ производится проверка подключения к этому серверу. Параметры подключения к SQL-серверу хранятся в файле `sqllogininfo.dat` и задаются, как правило, только при первичной инициализации (см. «[Проведение первичной инициализации программы](#)» на стр. 50) либо при первом соединении с SQL-сервером (например, после переноса на сервер базы данных УКЦ (см. «[Перенос базы данных УКЦ на SQL-сервер](#)» на стр. 299)).



Примечание. Для защиты от прочтения сторонними приложениями данные файла `sqllogininfo.dat` зашифрованы на ключе защиты УКЦ (см. «[Ключ защиты УКЦ](#)»).

Проверка подключения к выбранному SQL-серверу производится на основе параметров `sqllogininfo.dat` после ввода пароля администратора при каждом запуске программы (см. Запуск и завершение работы с программой (на стр. 59)). При успешной проверке осуществляется вход в программу, в случае возникновения ошибок в ходе проверки появляется диалоговое окно подключения к SQL-серверу (см. рисунок ниже).

Ошибки при проверке подключения к SQL-серверу могут возникать в следующих случаях:

- выбранный SQL-сервер не доступен;
- на SQL-сервере изменились учетные данные пользователя, имеющего доступ к базе УКЦ;
- изменились настройки подключения или настройки проверки подлинности SQL-сервера;
- изменился IP-адрес или имя SQL-сервера;
- удален или поврежден файл `sqllogininfo.dat` и прочее.

При возникновении ошибок соединения требуется установить их причину, проверить и, если требуется, изменить параметры подключения. Чтобы изменить параметры подключения к SQL-серверу:

- 1 В окне **Подключение к SQL серверу** в списке **Сервер** выберите или укажите SQL-сервер, на котором была развернута база данных УКЦ.

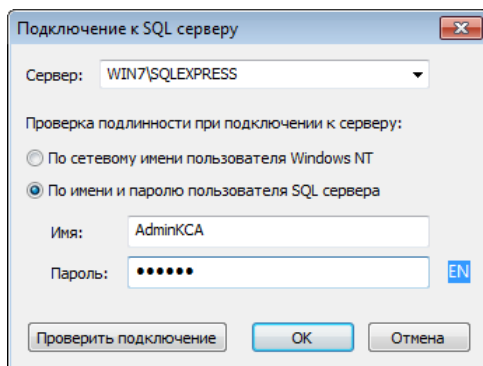


Рисунок 31: Подключение к SQL-серверу

- 2 Выберите тип аутентификации при подключении к SQL-серверу, установив переключатель в нужное положение.

При выборе типа **По имени и паролю пользователя SQL сервера** укажите имя пользователя, под учетной записью которого необходимо подключиться к SQL-серверу, и пароль. Данный пользователь должен иметь соответствующие права на работу с базой данных УКЦ.

- 3 Нажмите кнопку **Проверить подключение**. Если подключение к указанному SQL-серверу было проведено успешно, кнопка **ОК** станет активной. В противном случае, измените настройки подключения и нажмите кнопку **Повторить подключение** еще раз.
- 4 Нажмите кнопку **ОК**. В файл `sqllogininfo.dat` будут записаны изменившиеся настройки подключения к SQL-серверу.



Внимание! В случае возникновения проблем с подключением к SQL серверу, не пытайтесь устранить их самостоятельно, обратитесь к администратору используемого SQL-сервера.

Интерфейс программы ViPNet Удостоверяющий и ключевой центр

Внешний вид окна программы ViPNet Удостоверяющий и ключевой центр представлен на рисунке ниже:

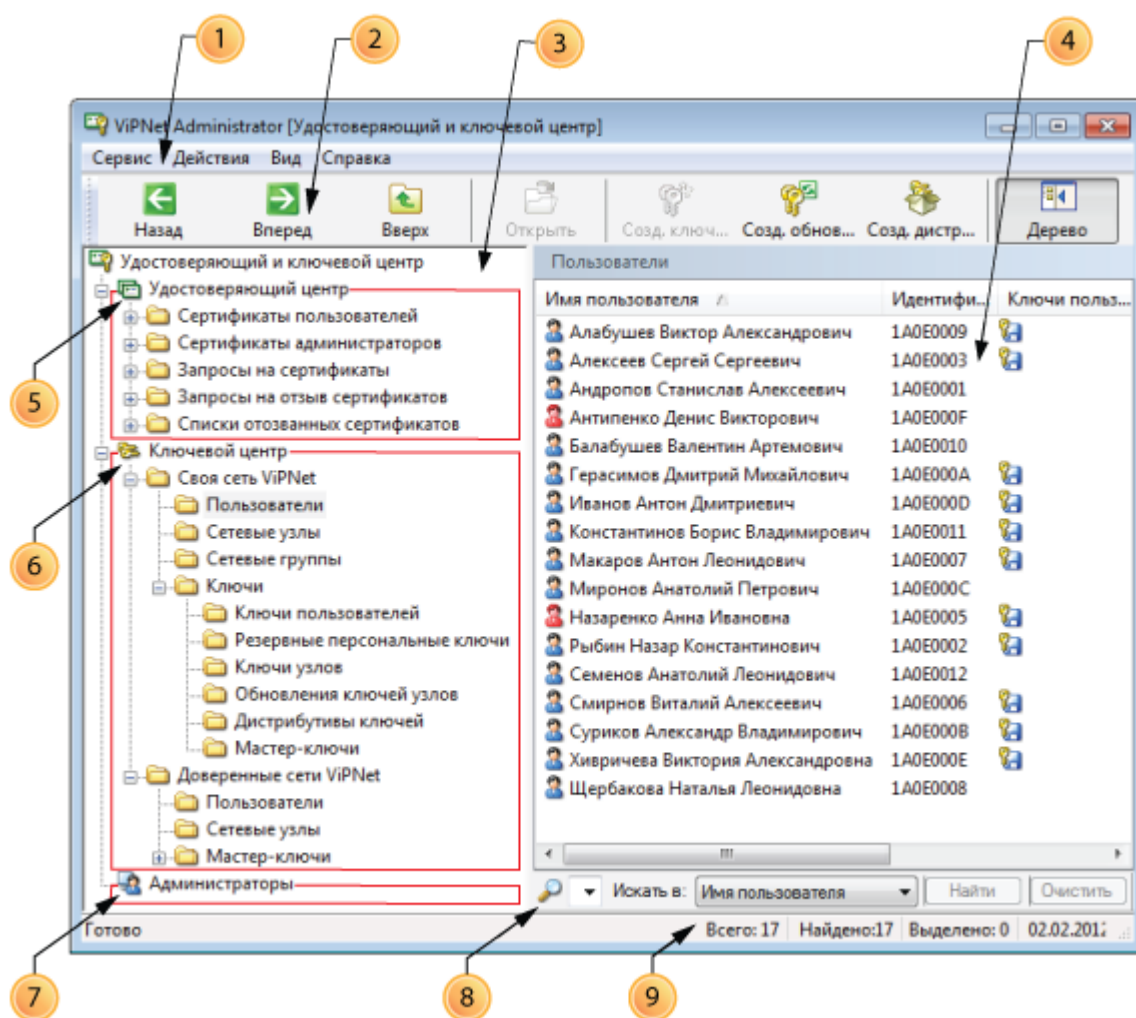




















Рисунок 32: Интерфейс программы ViPNet Удостоверяющий и ключевой центр

Цифрами на рисунке обозначены:

- 1 Главное меню программы.

- 2 Панель инструментов. Чтобы удалить или добавить кнопки на панель инструментов, в меню **Вид** выберите пункт **Панель инструментов**.
- 3 Панель навигации. Отображает в виде древовидного списка структуру элемента **Удостоверяющий и ключевой центр**, состоящего из трех основных разделов: **Удостоверяющий центр** (5), **Ключевой центр** (6) и **Администраторы** (7).
Чтобы показать или скрыть панель навигации, на панели инструментов нажмите кнопку **Дерево** .
- 4 Панель просмотра. Предназначена для отображения раздела, выбранного на панели навигации (3).
- 5 Раздел **Удостоверяющий центр** отображает работу программы в части Удостоверяющего центра ViPNet. Включает в себя вложенные подразделы:
 - **Сертификаты пользователей** — содержит сертификаты открытого ключа подписи внешних (см. «[Внешний пользователь ViPNet](#)») и внутренних пользователей ViPNet (см. «[Внутренний пользователь ViPNet](#)») .
 - **Сертификаты администраторов** — содержит сертификаты подписи администраторов своей и доверенных сетей ViPNet (уполномоченных лиц Удостоверяющих центров ViPNet) , а также изданные и импортированные кросс-сертификаты .
 - **Запросы на сертификаты** — содержит запросы на издание сертификатов внешних и внутренних пользователей ViPNet .
 - **Запросы на отзыв сертификатов** — содержит запросы на отзыв, приостановление и возобновление действия сертификатов пользователей , поступивших из Центров регистрации.
 - **Списки отозванных сертификатов** — содержит списки отозванных сертификатов (см. «[Список отозванных сертификатов \(СОС\)](#)») пользователей своей сети и доверенных сетей ViPNet .
- 6 Раздел **Ключевой центр** отображает работу программы в части Ключевого центра ViPNet. Включает в себя два подраздела:
 - **Своя сеть ViPNet** — содержит сведения об объектах своей сети ViPNet и их ключах. Данные сведения распределены по соответствующим вложенным подразделам следующим образом:
 - **Пользователи** — содержит список всех пользователей, зарегистрированных в своей сети ViPNet .
 - **Сетевые узлы** — содержит список всех сетевых узлов, имеющихся в своей сети ViPNet .

- **Сетевые группы** — содержит список групп узлов, организованных в своей сети ViPNet .
 - **Ключи** — содержит различные виды ключей, создаваемые для объектов своей сети ViPNet: ключи пользователей , резервные персональные ключи , ключи узлов , обновления ключей узлов , дистрибутивы ключей  и мастер-ключи .
 - **Доверенные сети ViPNet** — содержит сведения о пользователях и сетевых узлах доверенных сетей ViPNet, а также о межсетевых мастер-ключях, используемых для организации связи с доверенными сетями. Данные сведения также распределены по соответствующим вложенным подразделам.
- 7** Раздел **Администраторы** содержит список учетных записей администраторов УКЦ (уполномоченных лиц Удостоверяющего центра ViPNet) .
- 8** Строка состояния. Чтобы показать или скрыть строку состояния, в меню **Вид** выберите пункт **Строка состояния**.
- 9** Строка поиска . Присутствует в тех разделах, в которых содержатся непосредственно сами списки объектов: сертификатов, запросов, СОС, пользователей, сетевые узлов и групп, ключей пользователей и узлов, дистрибутивов ключей и других.



3

Основные действия администратора УКЦ

Создание ключевой информации при первоначальном развертывании сети	68
Рекомендации по созданию ключевой информации в связи с изменением структуры сети	70
Когда создавать обновление ключей?	75
Действия при плановой смене мастер-ключей	76
Действия при компрометациях ключей	79
Кросс-сертификация	83

Создание ключевой информации при первоначальном развертывании сети

Развертывание сети начинается с создания необходимой конфигурации в программе ЦУС, которая формирует набор различных справочников для программы УКЦ.

После того, как в папку приема файлов из ЦУС (по умолчанию это будет FROM_NCC, расположенная на уровне папки установки УКЦ) будут помещены сформированные программой ЦУС необходимые файлы связей, администратор УКЦ может произвести первичную инициализацию (см. «[Проведение первичной инициализации программы](#)» на стр. 50) программы УКЦ и начать создание ключевой информации для пользователей и узлов сети.

Создание ключевой информации может происходить в автоматическом и индивидуальном режимах.

Для первичного развертывания сети ViPNet рекомендуется создать дистрибутивы ключей для всех пользователей сети в режиме автоматического создания ключевой информации (см. «[Процесс создания](#)» на стр. 93), при этом обновления ключей высылать не следует.

При первичном создании ключей для СУ будет предложено создать пароль администратора (см. «[Пароль администратора сетевых узлов](#)» на стр. 129) для группы **Вся сеть**. Этот пароль можно создавать, а можно и отказаться от его создания сейчас и создать позже, можно и совсем не создавать.

После создания дистрибутивы отобразятся в папке **Ключевой центр > Своя сеть ViPNet > Ключи > Дистрибутивы ключей** (см. «[Действия с созданными дистрибутивами ключей](#)» на стр. 113), откуда их можно будет перенести в какую-либо папку или на внешние носители, и далее использовать для установки ПО ViPNet на сетевых узлах.



Примечание. В состав самого первого ключевого дистрибутива пользователя входит резервный набор персональных ключей (РПК). РПК понадобится пользователю для дистанционного обновления ключей при их компрометации. Подробнее об РПК читайте в разделе [Действия с резервными персональными ключами](#) (на стр. 117).

Для сохранения всех паролей пользователей в файле можно воспользоваться пунктом главного меню программы **Сервис > Сохранить пароли в файле > Пароли**

пользователей. Кроме того, программой предусмотрено и индивидуальное сохранение пароля и (или) персональной информации для выбранного пользователя в файл или на внешнее устройство хранения данных (из папки **Ключевой центр > Своя сеть ViPNet > Пользователи** выбрать пользователя, затем либо дважды щелкнуть мышью на выбранном пользователе, либо в контекстном меню выбрать пункт **Открыть**, далее из соответствующих вкладок открывшегося окна **Свойства пользователя** сохранить пароль и (или) персональную информацию (см. [Просмотр свойств пользователя](#) (на стр. 133))).

Ключевые дистрибутивы вместе с паролями пользователей нужно каким-либо защищенным способом передать соответствующим пользователям.

Рекомендации по созданию ключевой информации в связи с изменением структуры сети

Если в программе ЦУС структура сети ViPNet изменяется, то в УКЦ необходимо будет произвести ряд действий.

Структура сети может изменяться в следующих случаях:

- при добавлении или удалении объектов своей сети, изменении их связей, регистрации пользователей в других коллективах и др. (см. [Создание ключей при изменениях в структуре своей сети](#) (на стр. 70));
- при установлении межсетевого взаимодействия с другой сетью или изменениями структуры, связанными с другой сетью (см. [Создание ключей при установлении взаимодействия с доверенной сетью ViPNet, а также при внесении изменений в это взаимодействие](#) (на стр. 73)).

Создание ключей при изменениях в структуре своей сети

Рассмотрим возможные случаи изменений в структуре своей сети и действия администратора, связанные с ними:

- 1 Изменение связей объектов сети, удаление объекта сети и пользователя сети без компрометации. В этом случае, на основании поступившей информации из ЦУС об изменениях, необходимо создать ключи узлов (см. «[Ключи узла ViPNet](#)») для тех узлов сети, которые были затронуты этим изменением (в которых добавлена или наоборот исключена соответствующая ключевая информация). Это типовая и наиболее часто встречающаяся ситуация. Рекомендуется использовать автоматическое создание ключей узлов. Для этого выберите пункт главного меню **Сервис > Автоматически создать > Ключи узлов**. Подробнее о создании ключей узлов см. в разделе [Создание ключей узлов](#) (на стр. 95).

Созданные ключи узлов появятся в папке **Ключевой центр > Своя сеть ViPNet > Ключи > Ключи узлов**, откуда их нужно перенести в ЦУС для рассылки по сети и автоматического обновления на сетевых узлах (см. [Действия с ключами узлов и обновлениями ключей для СУ](#) (на стр. 111)).

- 2 Добавление нового узла своей сети. При добавлении в ЦУС нового узла сети, на основании поступившей из ЦУС информации об изменениях, необходимо создать измененные ключи узлов для тех узлов сети, которые были затронуты этим изменением (добавлены связи с новым узлом сети), а также дистрибутивы ключей (см. «[Дистрибутив ключей](#)») для начальной инсталляции для новых узлов сети. Рекомендуется использовать автоматическое создание ключей узлов и дистрибутивов ключей. Для создания ключей узлов выберите пункт главного меню **Сервис > Автоматически создать > Ключи узлов**. Для создания дистрибутивов ключей выберите пункт главного меню **Сервис > Автоматически создать > Дистрибутивы ключей**. Подробнее о создании дистрибутивов ключей см. в разделе [Создание дистрибутивов ключей](#) (на стр. 91).

Созданные ключи узлов появятся в папке **Ключевой центр > Своя сеть ViPNet > Ключи > Ключи узлов**, откуда их нужно перенести в ЦУС для рассылки по сети и автоматического обновления на сетевых узлах. Созданные дистрибутивы ключей появятся в папке **Ключевой центр > Своя сеть ViPNet > Ключи > Дистрибутивы ключей**, откуда их можно будет перенести в какой-либо каталог (см. [Действия с созданными дистрибутивами ключей](#) (на стр. 113)). Эти файлы вместе с паролями пользователей нужно каким-либо защищенным способом передать на соответствующие новые сетевые узлы.

- 3 Добавление нового пользователя или нового ТК и нового пользователя на уже существующий СУ. В этом случае, на основании поступившей информации из ЦУС об изменениях, необходимо создать ключи узлов для тех узлов сети, которые были затронуты этим изменением (если таковые были) и дистрибутивы ключей для добавленных пользователей. Рекомендуется использовать автоматическое создание ключей узлов и дистрибутивов ключей. Для создания ключей узлов выберите пункт главного меню **Сервис > Автоматически создать > Ключи узлов**. Для создания дистрибутивов ключей выберите пункт главного меню **Сервис > Автоматически создать > Дистрибутивы ключей**.

Созданные ключи узлов появятся в папке **Ключевой центр > Своя сеть ViPNet > Ключи > Ключи узлов**, откуда их нужно перенести в ЦУС для рассылки по сети и автоматического обновления на сетевых узлах. Созданные дистрибутивы ключей появятся в папке **Ключевой центр > Своя сеть ViPNet > Ключи > Дистрибутивы ключей**, откуда их можно будет перенести в какой-либо каталог. Эти файлы вместе с паролями пользователей нужно каким-либо защищенным способом передать соответствующим новым пользователям. Необходимо иметь в виду, что обновления на СУ, на которые были добавлены новые пользователи, должны пройти до того момента, как новый пользователь, получив дистрибутив ключей и пароль, будет активизироваться на этом СУ.

- 4 Изменение права подписи у пользователя. Если из ЦУС поступила информация о том, что у каких-то пользователей сети ViPNet удалено или добавлено право подписи, то нужно сформировать обновление ключей узлов (см. «[Обновление ключей узла](#)») для тех сетевых узлов, которые затронуло это изменение, поскольку

информация о праве иметь подпись содержится в составе обновления ключей узла. Рекомендуется использовать индивидуальное создание обновлений ключей. Для создания обновления ключей узла в папке **Ключевой центр > Своя сеть ViPNet > Сетевые узлы** выберите нужный сетевой узел и из контекстного меню по правой кнопке мыши выберите пункт **Ключи > Создать обновление**. Подробнее о создании обновлений ключей см. в разделе [Создание обновлений ключей узлов](#) (на стр. 97).

Созданные обновления ключей появятся в папке **Ключевой центр > Своя сеть ViPNet > Ключи > Обновления ключей узлов**, откуда их нужно перенести в ЦУС для рассылки по сети и автоматического обновления на сетевых узлах.

- 5 Регистрация пользователя в другом коллективе. Когда изменения касаются перерегистрации пользователя в другом коллективе, то из ЦУС поступают файлы связей для формирования его ключей (см. [«Ключи пользователя ViPNet»](#)). Для создания ключей пользователя в папке **Ключевой центр > Своя сеть ViPNet > Пользователи** выберите пользователя, для которого есть соответствующий файл связей из ЦУС, и из контекстного меню по правой кнопке мыши выберите пункт **Ключи пользователя > Создать**. Подробнее о создании ключей пользователя см. в разделе [Создание ключей пользователей](#) (на стр. 100).

Созданные ключи пользователя появятся в папке **Ключевой центр > Своя сеть ViPNet > Ключи > Ключи пользователя**, откуда их нужно перенести в ЦУС для рассылки по сети и автоматического обновления на сетевых узлах (см. [Действия с ключами пользователей](#) (на стр. 108)).

- 6 Удаление скомпрометированного пользователя из сети. При удалении пользователя в ЦУС, может возникнуть необходимость считать его ключи скомпрометированными. При наличии компрометации ключей (см. [«Компрометация ключей»](#)) в программе УКЦ станет доступен только пункт меню **Сервис > Автоматически создать > Ключи при компрометациях**, который и нужно выбрать. Подробнее о действиях администратора при компрометациях см. в разделе [Действия при компрометациях ключей](#) (на стр. 79).

Для сохранения всех паролей пользователей в файле можно воспользоваться пунктом главного меню программы **Сервис > Сохранить пароли в файле > Пароли пользователей**. Кроме того, программой предусмотрено и индивидуальное сохранение пароля и (или) персональной информации для выбранного пользователя в файл или на внешнее устройство хранения данных (из папки **Ключевой центр > Своя сеть ViPNet > Пользователи** выбрать пользователя, затем либо дважды щелкнуть мышью на выбранном пользователе, либо в контекстном меню выбрать пункт **Открыть**, далее из соответствующих вкладок открывшегося окна **Свойства пользователя** сохранить пароль и (или) персональную информацию (см. [Просмотр свойств пользователя](#) (на стр. 133))).

Создание ключей при установлении взаимодействия с доверенной сетью ViPNet, а также при внесении изменений в это взаимодействие

Если требуется организовать связь своей сети с объектами другой (доверенной сети ViPNet (см. «[Доверенная сеть](#)»)) сети, то необходимо осуществить ряд действий в ЦУС и УКЦ. Для полноты картины рассмотрим действия и в ЦУС, и в УКЦ. Рассмотрим на примере организации межсетевое взаимодействие между двумя сетями:

- 1 Администраторы двух ЦУС выполняют процедуру экспорта из своей сети информации об объектах, которые должны взаимодействовать с объектами другой сети. Экспортируется также по одному из координаторов каждой сети, через которые или с использованием которых будет осуществляться такое взаимодействие. Каким-либо защищенным способом производится обмен этой информацией и ее импорт в свой ЦУС.
- 2 Администраторам УКЦ необходимо создать один из межсетевых мастер-ключей (см. «[Межсетевой мастер-ключ](#)»). Следует заметить, что симметричные межсетевые мастер-ключи создаются только в одной сети, а в другую передаются, а асимметричный ключ — в обеих сетях, и администраторы двух сетей обмениваются открытыми частями своего ключа. Поэтому администраторам двух сетей предварительно нужно договориться, какие межсетевые мастер-ключи будут использоваться для связи между сетями. Предпочтительно использовать для связи двух сетей симметричный индивидуальный мастер-ключ, так как в этом случае безопасность хранения выше (об этом ключе знают администраторы только двух сетей, а при использовании универсального ключа — администраторы всех сетей, в которые он экспортирован). Стойкость же асимметричного ключа ниже (симметричного индивидуального и симметричного универсального ключа). Подробно о создании межсетевых мастер-ключей и о логике их выбора см. в разделе [Создание межсетевых мастер-ключей](#) (на стр. 120).
- 3 Администраторы двух УКЦ производят обмен межсетевыми мастер-ключами по симметричной или асимметричной схеме (см. [Экспорт и импорт межсетевых мастер-ключей](#) (на стр. 124)). Одновременно выполняется обмен справочниками сертификатов администраторов каждой сети и справочниками отозванных сертификатов пользователей каждой сети (даже если этот справочник пустой, то есть сертификаты в сети ни разу не отзывались).
- 4 В каждом из УКЦ производится импорт и заверение справочника сертификата администраторов другой сети подписью своего администратора в папке **Удостоверяющий центр > Сертификаты администраторов > Доверенные сети ViPNet > Входящие** и импорт справочника отозванных сертификатов пользователей другой сети в папке **Удостоверяющий центр > Списки отозванных сертификатов > Доверенные сети ViPNet** или автоматически после входе в УКЦ (см. [Импорт сертификатов администраторов доверенных сетей ViPNet](#) (на стр. 162)).

- 5 На основании информации, полученной из ЦУС каждой сети, в УКЦ каждой сети необходимо создать новые ключи узлов. На этом этапе будет создана новая ключевая информация только для своего ЦУС и координатора, так как информация о связях других объектов пока неизвестна. После обновления этой информации будет возможно установление соединения между ЦУС двух сетей.
- 6 Администраторы каждого из ЦУС устанавливают необходимые связи импортированных коллективов со своими экспортированными коллективами. Обмениваются уже автоматически через установленное соединение вновь сформированными экспортными данными и отправляют информацию о новых связях своих объектов в свои УКЦ.
- 7 На основании полученных данных в УКЦ необходимо создать новые ключи узлов для СУ, которых затронули изменения (ключи пользователей в этой ситуации не изменяются). Эти ключи узлов обычным образом отправляются в свой ЦУС для рассылки по своей сети и автоматического обновления.
- 8 Если в дальнейшем происходят изменения в конфигурации, касающейся объектов другой сети, то производятся действия, аналогичные действиям, описанным в разделах [Основные действия администратора УКЦ](#) (на стр. 67) и [Управление ключевой структурой ViPNet](#) (на стр. 88), а также:
 - При изменении в другой сети, связанной с объектами своей сети, сертификата администратора, то в ЦУС для УКЦ поступают новые справочники сертификатов подписей администраторов из доверенных сетей ViPNet, и их необходимо импортировать в свою сеть для замены старых в папке **Удостоверяющий центр > Сертификаты администраторов > Доверенные сети ViPNet** или автоматически после входа в УКЦ (см. [Импорт сертификатов администраторов доверенных сетей ViPNet](#) (на стр. 162)).
 - Если в другой сети, связанной с объектами своей сети, произошел отзыв сертификатов каких-либо пользователей, то в ЦУС для УКЦ поступают новые справочники отозванных сертификатов пользователей из доверенных сетей ViPNet и их нужно импортировать в свою сеть в папке **Удостоверяющий центр > Списки отозванных сертификатов > Доверенные сети ViPNet** или автоматически после входа в УКЦ (см. [Импорт списков отозванных сертификатов доверенных сетей ViPNet](#) (на стр. 165)).

Когда создавать обновление ключей?

Существуют ситуации, когда не нужно формировать полные ключи узла, а достаточно сформировать обновление ключей.

Обновление ключей производится в следующих случаях:

- Если произошла смена пароля администратора сетевой группы узлов (см. [«Пароль администратора сетевых узлов»](#) на стр. 129). В этом случае создайте обновления ключей самостоятельно (см. [Создание обновлений ключей узлов](#) (на стр. 97)).
- Если создана новая подпись администратора УКЦ. В этом случае обновление ключей создается автоматически на завершающем этапе работы мастера создания сертификата администратора.
- Если пришел экспорт справочников сертификатов администраторов (см. [«Импорт сертификатов администраторов доверенных сетей ViPNet»](#) на стр. 162) или СОС (см. [«Импорт списков отозванных сертификатов доверенных сетей ViPNet»](#) на стр. 165) из доверенных сетей ViPNet. В этом случае при импорте сертификатов администраторов или СОС предлагается создать обновление ключей. При отказе следует создать обновления ключей самостоятельно.
- Если из ЦУС поступила информация о том, что у каких-то пользователей сети ViPNet удалено или добавлено право подписи. В этом случае произведите создание обновлений ключей самостоятельно.

Действия при плановой смене мастер-ключей

Рекомендуется осуществлять плановую смену ключей — смену ключей с установленной в системе периодичностью, не вызванную компрометацией ключей.

Рекомендуется проводить плановую смену мастер-ключей (см. «[Плановая смена мастер-ключей](#)» на стр. 76) (персональных мастер-ключей, мастер-ключей защиты, мастер-ключей обмена) не реже одного раза в год.

Согласно установленному порядку, межсетевые мастер-ключи также должны обновляться не реже одного раза в год (см. «[Плановая смена межсетевого мастер-ключа](#)» на стр. 77).

Плановая смена мастер-ключей

Для смены какого-либо мастер-ключа выберите его в папке **Ключевой центр > Своя сеть ViPNet > Ключи > Мастер-ключи** и воспользуйтесь пунктом **Сменить** контекстного меню (подробнее см. [Смена мастер-ключей своей сети](#) (на стр. 119)).

После смены мастер-ключа необходимо произвести обновления ключей пользователей и ключей узлов для всех пользователей и СУ, для этого выполните следующие действия:

- 1 В ЦУС сформируйте все справочники.
- 2 Скопируйте из ЦУС в УКЦ справочники связей всех сетевых узлов и справочники связей всех пользователей.
- 3 Если в сети есть координаторы, на которые установлена Linux-версия ПО ViPNet, для этих координаторов скопируйте из ЦУС в УКЦ полный объем дистрибутивов.
- 4 В УКЦ создайте ключи пользователей (см. «[Создание ключей пользователей](#)» на стр. 100) и ключи узлов (см. «[Создание ключей узлов](#)» на стр. 95), затем перенесите их в ЦУС. Ключи узлов рекомендуется создавать в автоматическом режиме.
- 5 Для координаторов, на которые установлена Linux-версия ПО ViPNet, создайте дистрибутивы ключей (см. «[Создание дистрибутивов ключей](#)» на стр. 91). Затем перенесите созданные дистрибутивы в папку установки ViPNet Administrator, в подпапку `\FOR_NCC\DST`.

- 6 В ЦУС отправьте все обновления на сетевые узлы с отложенной датой (рекомендуемая дата обновления через 10 дней с момента отправки).



Внимание! Для того чтобы все обновления дошли на компьютеры всех СУ и прошли в автоматическом режиме, необходимо, чтобы за эти 10 дней все СУ и координаторы подключились к сети и СУ имели связь со своим координатором. Если это условие не будет выполнено, то для отключенных СУ обновления придется производить вручную!

Также следует иметь в виду, что в то время, пока не истек срок назначенного обновления, в УКЦ и ЦУС желательно не производить никаких действий. Если же что-то было изменено, то в ЦУС все обновления необходимо отсылать с более поздней датой, чем дата, указанная для обновления, отосланного в связи с плановой сменой основного мастер-ключа.

Перед обновлением ключей рекомендуется расшифровать письма программы «Деловая почта» на абонентских пунктах (см. «[Абонентский пункт \(АП\)](#)»). Если после обновления ключей на абонентский пункт придут письма, зашифрованные на старых ключах, они не будут приняты.

Более подробно об отправке обновлений см. в документации на программу ViPNet Центр управления сетью.

Плановая смена межсетевого мастер-ключа

Перед тем, как осуществлять плановую смену межсетевого мастер-ключа, следует договориться с администраторами доверенных сетей, для связи с которыми будет использоваться новый мастер-ключ, по следующим вопросам:

- при планировании изменения типа используемого межсетевого мастер-ключа следует договориться, какие межсетевые мастер-ключи будут использоваться для связи между сетями, и где эти ключи будут создаваться (см. [Создание межсетевых мастер-ключей](#) (на стр. 120));
- о времени проведения смены мастер-ключа и последующего обновления ключей узлов для СУ сетей.

Для создания нового межсетевого мастер-ключа в папке **Ключевой центр > Доверенные сети ViPNet > Мастер-ключи > Текущие** используйте пункт **Создать** контекстного меню.

После того, как была произведена смена межсетевого мастер-ключа и (или) выполнена операция экспорта (импорта) (см. «[Экспорт и импорт межсетевых мастер-ключей](#)» на стр. 124), необходимо также:

- 1 Ввести этот мастер-ключ в действие (см. «[Изменение статуса межсетевого мастер-ключа](#)» на стр. 127).
- 2 В ЦУС создать новые файлы связей для всех СУ, связанных с доверенной сетью на этом ключе.
- 3 В КЦ создать ключи узлов в режиме автоматического создания ключей (см. «[Создание ключей узлов](#)» на стр. 95).
- 4 В ЦУС отправить обновления на все СУ (дата обновления должна быть согласована с администраторами доверенных сетей, которых затрагивает данная плановая смена межсетевого мастер-ключа).



Внимание! Напомним, что после смены межсетевого мастер-ключа, связь между СУ разных сетей, использующих данный мастер-ключ, будет возможна только после обновления на всех соответствующих СУ данных сетей.

Действия при компрометациях ключей

Под компрометацией ключей подразумевается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Различают явную и неявную компрометацию ключей.

Явной называют компрометацию, факт которой становится известным на отрезке установленного времени действия данного ключа.

Неявной называют компрометацию ключа, факт которой остается неизвестным для лиц, являющихся законными пользователями данного ключа.

Наибольшую опасность представляют неявные компрометации ключей.

Решение задачи защиты ключей от компрометации направлено на исключение компрометаций вообще или, по крайней мере, на то, чтобы свести неявную компрометацию к явной.

События, квалифицируемые как компрометация ключей

Основные события, при которых ключи могут считаться скомпрометированными:

- 1 Посторонним лицам мог стать доступным файл ключевого дистрибутива.
- 2 Посторонним лицам мог стать доступным съемный носитель с ключевой информацией.
- 3 Посторонним лицам мог стать доступным пароль пользователя, и эти лица могли иметь доступ к компьютеру пользователя.
- 4 Посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на компьютере.
- 5 На компьютере, подключенном к сети, не установлен модуль ViPNet Монитор, или он устанавливался в 4 или 5 режим работы, а также:
 - в локальной сети считается возможным присутствие посторонних лиц;

- на границе локальной сети отсутствует (отключен) сертифицированный межсетевой экран.
- 6 Увольнение сотрудников имевших доступ к ключевой информации.
- 7 Нарушение печати на сейфе с ключевыми носителями.
- 8 Наличие в подписи под входящим документом сертификата, находящегося в списке отозванных сертификатов.
- 9 Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

К событиям, требующим расследования и принятия решения по компрометации, относятся возникновение подозрений по утечке или искажению информации в системе конфиденциальной связи.

При наступлении любого из перечисленных выше событий пользователь ViPNet должен немедленно прекратить работу на своем компьютере и сообщить о факте компрометации (или предполагаемом факте компрометации) администратору УКЦ своей сети.

По факту компрометации ключей должно быть проведено служебное расследование.

Действия при компрометации ключей пользователя

Для простоты изложения назовем пользователя, ключи которого скомпрометированы, скомпрометированным пользователем.

Компрометация ключей СУ имеет место только при компрометации какого-либо пользователя на данном СУ.

- 1 В случае компрометации ключей пользователя администратор УКЦ оповещает об этом ЦУС.
- 2 Оператор ЦУС объявляет ключи данного пользователя скомпрометированными и создает справочники связей при компрометациях с необходимой информацией для УКЦ, а именно:
 - программа ЦУС создает файлы связей для полной замены индивидуальной ключевой информации скомпрометированных пользователей и замены ключей сетевых узлов, где зарегистрированы данные пользователи;

- для всех сетевых узлов, с которыми связаны узлы, где зарегистрированы скомпрометированные пользователи, формируются файлы связей для частичного обновления ключевой информации;
- для пользователей (с нескомпрометированными ключами), зарегистрированных в коллективах, где имеются скомпрометированные пользователи, формируются файлы связей для частичного обновления индивидуальной ключевой информации.

Если скомпрометированы ключи координатора, на котором установлена Linux-версия ПО ViPNet, оператор ЦУС должен скопировать из ЦУС в УКЦ полный объем дистрибутивов для этого координатора.

- 3 Оператор ЦУС оповещает о факте компрометации ключей всех пользователей, связанных со скомпрометированным пользователем. После получения данного сообщения пользователи не должны использовать скомпрометированные ключи.
- 4 Далее в УКЦ необходимо сформировать новую ключевую информацию. Для этого станет доступен пункт меню **Сервис > Автоматически создать > Ключи при компрометациях**, который нужно выбрать для генерации ключей при компрометации (см. «[Создание ключей при компрометациях](#)» на стр. 105).

Если скомпрометированы ключи координатора, на котором установлена Linux-версия ПО ViPNet, в УКЦ необходимо создать дистрибутив ключей для этого координатора (см. «[Создание дистрибутивов ключей](#)» на стр. 91). Затем нужно перенести дистрибутив в папку установки ViPNet Administrator, в подпапку \FOR_NCC\DST.

Все сформированные файлы с новой ключевой информацией зашифрованы на нескомпрометированных ключах, поэтому могут передаваться на абонентский пункт и пользователю по любым каналам связи, в том числе и открытым.

- 5 В случае признания факта компрометации закрытого ключа подписи пользователя, УКЦ отзывает сертификат этого пользователя. Сертификат попадает в список отозванных сертификатов. Данный список должен быть отправлен всем пользователям сети ViPNet.
- 6 Отозванные сертификаты открытых ключей пользователя не удаляются из базы УКЦ и хранятся в течение установленного срока действия для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением электронной подписи.
- 7 Информация, содержащаяся на скомпрометированных съемных ключевых носителях, после проведения служебного расследования должна быть уничтожена с использованием утилиты `clean.exe`.



Внимание! Если были произведены действия, связанные с компрометацией ключей пользователя на одном из сетевых узлов, убедитесь в том, что все пользователи данного узла получили обновления. Обратите внимание, что если один из пользователей принял обновление, а другой (другие) нет, то при следующей смене ключей (компрометации, смене мастер-ключей) автоматическое обновление ключевой информации может оказаться невозможным. В таких случаях, для восстановления работоспособности потребуется проведение процедуры первичной установки сетевого узла с новым ключевым дистрибутивом. Это может привести к частичной или полной утере ранее принятой, зашифрованной корреспонденции в программе ViPNet Деловая почта на этом СУ.

Действия при компрометации ключей УКЦ

При компрометации ключей хотя бы одного администратора УКЦ вся ключевая информация в сети считается скомпрометированной. В этом случае должна быть немедленно остановлена работа на симметричных ключах шифрования.

Для восстановления работы системы необходимо:

- Удалить с жесткого диска все ключи с использованием утилиты `clean.exe`.
- Начать формирование ключевой системы с нулевой отметки (см. [«Создание ключевой информации при первоначальном развертывании сети»](#) на стр. 68).

До полного развертывания ключевой системы ключевая информация передается пользователям посредством личной встречи администраторов УКЦ, использования доверенных нарочных с документальным подтверждением отправки и приема, использования ведомственной или фирменной фельдъегерской связи и т.п.

Кросс-сертификация

Кросс-сертификация — это механизм установки доверительных отношений между удостоверяющими центрами.

Для администраторов удостоверяющих центров (см. «[Удостоверяющий центр](#)») могут быть сформированы следующие типы сертификатов:

- Корневые сертификаты — это сертификаты, в которых издатель сертификата является одновременно и владельцем сертификата. В таком сертификате совпадают поля **Издатель** и **Владелец**, определяющие администратора одного удостоверяющего центра.
- Кросс-сертификаты — это сертификаты, в которых издатель сертификата не является одновременно владельцем сертификата. В таком сертификате поля **Издатель** и **Владелец** не совпадают, и определяют администраторов различных удостоверяющих центров.

При помощи формирования кросс-сертификатов устанавливаются доверительные отношения между удостоверяющими центрами.

ViPNet УКЦ обеспечивает необходимую функциональность для организации доверительных отношений с УЦ различных производителей.

Доверительные отношения могут быть построены с использованием следующих принципов:

- Распределенная система доверительных отношений между УЦ. Распределенная система доверительных отношений подразумевает наличие самоподписанных сертификатов у администраторов всех УЦ, входящих в систему. Для установки доверительных отношений администраторы удостоверяющих центров издают кросс-сертификаты попарно по запросам друг друга. Таким образом, администратор каждого УЦ имеет не только самоподписанный сертификат, но и изданные кросс-сертификаты других УЦ, с кем были построены доверительные отношения.

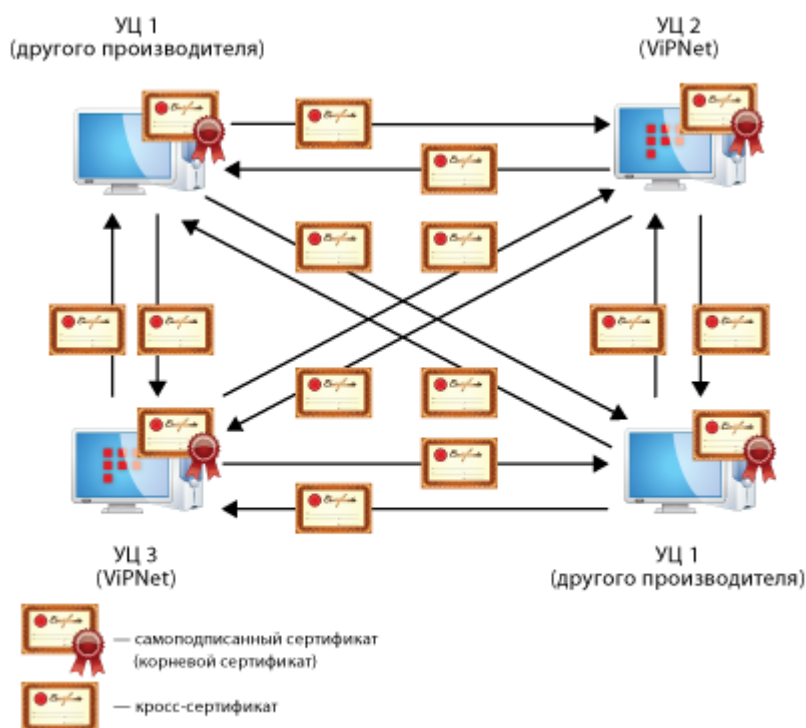


Рисунок 33: Распределенная модель доверительных отношений

- Иерархическая система доверительных отношений между УЦ. Иерархическая система доверительных отношений подразумевает наличие самоподписанного сертификата только у администратора головного УЦ (см. «[Вышестоящий удостоверяющий центр](#)»). Для установки доверительных отношений администраторы подчиненных УЦ (см. «[Подчиненный удостоверяющий центр](#)») формируют запросы на сертификат в вышестоящие УЦ. В вышестоящих УЦ по этим запросам издаются кросс-сертификаты и передаются обратно в подчиненные УЦ. Таким образом, администраторы подчиненных УЦ имеют кросс-сертификаты, изданные по их запросу в вышестоящем УЦ.

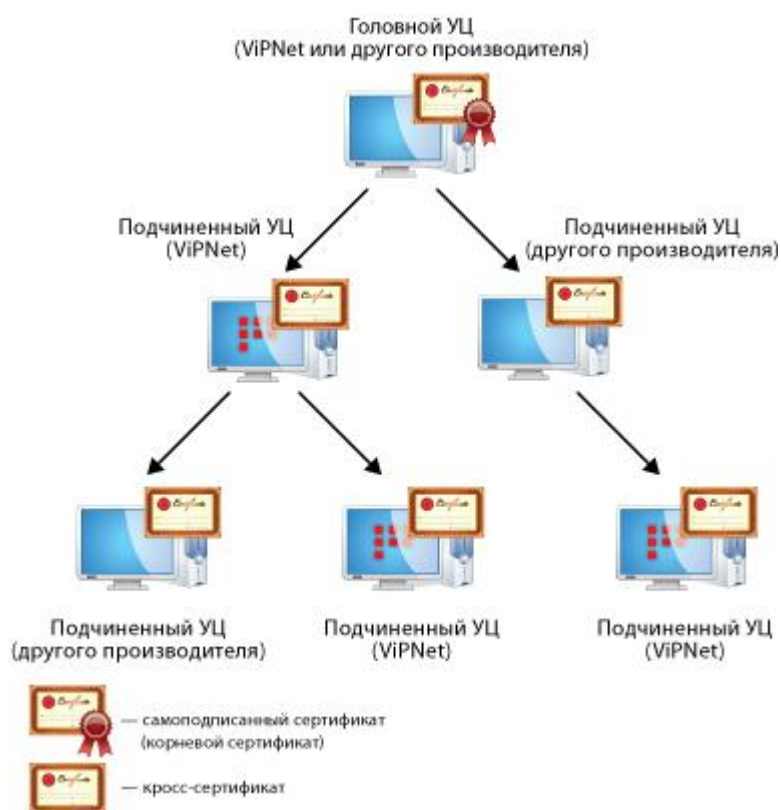


Рисунок 34: Иерархическая модель доверительных отношений

В ViPNet УКЦ предоставляется следующая функциональность по обеспечению кросс-сертификации:

- Создание запросов на кросс-сертификаты в другие УЦ (в том числе в вышестоящие УЦ).
- Прием запросов в формате PKCS#10 от других УЦ и проверку их целостности (подписи под запросом).
- Отображение и печать информации, содержащейся в запросе и результата проверки подписи под запросом.
- Издание кросс-сертификата на основании запроса (в том числе сертификатов администраторов подчиненных УЦ).
- Хранение изданных кросс-сертификатов, их экспорт в доверенные сети ViPNet и рассылку на сетевые узлы своей сети.
- Отзыв изданных кросс-сертификатов.

- Ввод в действие изданных в вышестоящем УЦ кросс-сертификатов.
- Импорт справочников, содержащих кросс-сертификаты от других УЦ.
- Разрешение конфликтов, связанных с наличием в хранилищах одновременно корневого и кросс-сертификата для одного и того же ключа подписи администратора.

Организация распределенной системы доверительных отношений между УЦ

УКЦ нескольких сетей ViPNet, а также УЦ других производителей, могут быть объединены в распределенную систему удостоверяющих центров (см. Рисунок 33 на стр. 84).

Для организации распределенной системы доверительных отношений между УЦ, для каждой пары УЦ должны быть выполнены следующие действия:

- 1 Администраторы двух УЦ в своих УЦ формируют запрос на кросс-сертификат и обмениваются файлами с запросами между собой. О выполнении этого действия в ViPNet УКЦ см. в разделе [Создание запроса на кросс-сертификат и отправка его в другой УЦ](#) (на стр. 230).
- 2 Администратор каждого УЦ издает кросс-сертификат для администратора другого УЦ, от которого получен запрос. О выполнении этого действия в ViPNet УКЦ см. в разделе [Обработка запросов на кросс-сертификаты \(в том числе запросов на сертификаты из подчиненных УЦ\)](#) (на стр. 169).

Эти действия должны быть выполнены для каждой парой УЦ, с кем организуется распределенная система доверительных отношений. После того как все УЦ издадут кросс-сертификаты друг другу, доверительные отношения между УЦ будут установлены.

Организация иерархической системы доверительных отношений между УЦ

УКЦ нескольких сетей ViPNet, а также УЦ других производителей, могут быть объединены в иерархическую систему удостоверяющих центров (см. Рисунок 34 на стр. 85).

Для организации иерархической системы доверительных отношений между УЦ, в подчиненном и вышестоящем УЦ, должны быть выполнены следующие действия:

- 1 Администратор подчиненного УЦ формирует запрос на кросс-сертификат в вышестоящий УЦ и передает файл с запросом администратору вышестоящего УЦ. О выполнении этого действия в ViPNet УКЦ см. в разделе [Создание запроса на кросс-сертификат к вышестоящему удостоверяющему центру](#) (на стр. 221).
- 2 Администратор вышестоящего УЦ издает кросс-сертификат для администратора подчиненного УЦ и передает файл с сертификатом обратно администратору подчиненного УЦ. О выполнении этого действия в ViPNet УКЦ см. в разделе [Обработка запросов на кросс-сертификаты \(в том числе запросов на сертификаты из подчиненных УЦ\)](#) (на стр. 169).
- 3 Администратор подчиненного УЦ вводит в действие изданный кросс-сертификат в своем УЦ. О выполнении этого действия в ViPNet УКЦ см. в разделе [Ввод в действие кросс-сертификата, изданного в вышестоящем УЦ](#) (на стр. 224).

Эти действия должны быть выполнены в тех УЦ, для которых организуется иерархическая система доверительных отношений. После того как все вышестоящие УЦ издадут кросс-сертификаты для подчиненных УЦ, доверительные отношения между УЦ будут установлены.



4

Управление ключевой структурой ViPNet

Создание ключевой информации	89
Действия с созданной ключевой информацией	107
Создание мастер-ключей	119
Пароль администратора сетевых узлов	129
Сохранение паролей пользователей и администраторов сетевых узлов	131
Смена паролей пользователей ViPNet	132
Просмотр свойств пользователя	133
Просмотр свойств сетевого узла	136
Просмотр свойств сетевой группы	139

Создание ключевой информации

В УКЦ существует возможность создавать следующие ключи для сетевых узлов (см. «Сетевой узел ViPNet (СУ)») и (или) пользователей сети ViPNet:

- Дистрибутив ключей — файл с расширением `.dst`, создаваемый в УКЦ для каждого пользователя сетевого узла. Файл необходим для обеспечения первичного запуска прикладной программы сети ViPNet на сетевом узле. В этом файле помещены адресные справочники (из ЦУСа), ключевая информация (ключи пользователя, ключи узла, резервный набор персональных ключей) и лицензионный файл.
- Ключи пользователя — набор файлов, создаваемый в УКЦ для каждого пользователя сетевого узла. Основное содержание ключей пользователя — информация, идентифицирующая пользователя и позволяющая работать с прикладными задачами сети ViPNet. Кроме того, в ключах пользователя находится электронная подпись данного пользователя, если администратор ЦУСа разрешил пользователю подписывать документы.
- Ключи узла — набор файлов, создаваемый в УКЦ для каждого сетевого узла. Основное содержание ключей узла — ключи для шифрования между коллективами и между сетевыми узлами, а также другие служебные файлы.
- Обновление ключей — набор файлов, создаваемый в УКЦ для каждого сетевого узла. Это урезанный вариант ключей узла, то есть содержит только справочники сертификатов администраторов УКЦ, списки отозванных сертификатов и контрольные суммы паролей администраторов.
- Резервный набор персональных ключей — несколько персональных ключей, создаваемых для каждого пользователя в УКЦ впрок (в виде файла `AAAA.pk`, где `AAAA` — идентификатор пользователя в рамках своей сети). Резервный набор персональных ключей (РНПК) пользователя используется для дистанционного обновления ключей пользователя при их компрометации. Файл РНПК входит в состав самого первого дистрибутива ключей и передается пользователю в его составе. Пользователи должны хранить РНПК в безопасном месте отдельно от ключей пользователя. Новые файлы РНПК создаются в УКЦ в случае необходимости.

При компрометации ключей пользователей УКЦ позволяет создать новые ключи для скомпрометированных пользователей. При этом действия по созданию других ключей становятся недоступны, пока не будут сформированы ключи при компрометациях.

Создание дистрибутивов ключей, ключей пользователей и ключей узлов доступно только для сетевых узлов и (или) пользователей, для которых есть соответствующие справочники связей из ЦУСа. Создание обновления ключей и резервных наборов персональных ключей доступно для всех вне зависимости от наличия файлов связи. Ключи при компрометации пользователей можно создать только при наличии специальных справочников связей из ЦУСа.

Создание ключей может происходить в автоматическом и индивидуальном режимах.

Автоматический режим подразумевает создание выбранного типа ключей сразу для всех сетевых узлов и (или) пользователей, для которых доступно создание ключей. В индивидуальном режиме можно выбрать из списка доступных, для кого следует создать выбранный тип ключей.

Создание ключей в автоматическом режиме используется для создания дистрибутивов (включая издание сертификатов пользователей), ключей узлов и обновлений ключей.

Создание ключей в индивидуальном режиме используется для создания ключей тех же типов, что и в автоматическом режиме, а также для создания ключей пользователей (включая издание сертификатов пользователей) для выбранных пользователей.

При самом первом создании ключей будет предложено создать пароль администратора сетевых узлов для группы **Вся сеть** (см. «[Пароль администратора сетевых узлов](#)» на стр. 129). Этот пароль можно создавать, а можно и отказаться от его создания сейчас и создать позже, можно и совсем не создавать.



Внимание! Если из ЦУСа поступила информация о пользователях и сетевых узлах, ключи которых скомпрометированы, то действия (соответствующие пункты меню) по созданию всех остальных типов ключей будут недоступны до тех пор, пока не будут созданы ключи после компрометации. Для этого воспользуйтесь пунктом меню **Сервис > Автоматически создать > Ключи при компрометациях**. Узнать о наличии скомпрометированных пользователей и сетевых узлов можно в папке **Ключевой центр > Своя сеть ViPNet > Пользователи** и папке **Ключевой центр > Своя сеть ViPNet > Сетевые узлы**, где в колонке **Статус** для скомпрометированных пользователей и узлов будет указано значение **Скомпрометирован**. Подробнее о действиях администратора при компрометациях см. в разделе [Действия при компрометациях ключей](#) (на стр. 79).

Создание дистрибутивов ключей

Общие сведения

Дистрибутив ключей — файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сетевого узла ViPNet. Состав дистрибутива ключей представлен на схеме ниже.



Рисунок 35: Состав дистрибутива ключей

Как правило, дистрибутив ключей для пользователя формируется при добавлении пользователя в сеть ViPNet (для развертывания узла, на котором зарегистрирован пользователь, в сети ViPNet).

В некоторых случаях дистрибутив ключей для пользователя может быть сформирован повторно, например, если произошел какой-либо сбой или возникли проблемы при обновлениях в сети ViPNet — пользователю не поступила обновленная информация, и нет возможности выполнить ее повторную отправку.



Внимание! Если для пользователя был повторно сформирован дистрибутив ключей, то перед его установкой на узле в программе ViPNet Деловая почта настоятельно рекомендуется расшифровать всю зашифрованную корреспонденцию. Это необходимо для предотвращения возможных проблем с ее прочтением после повторной инициализации дистрибутива ключей на узле.

Особенности при создании дистрибутивов ключей

При создании дистрибутивов ключей важно помнить о следующих особенностях:

- Если на сетевом узле зарегистрировано несколько пользователей, то независимо от способа дистрибутив будет сформирован сразу для всех пользователей узла. Количество дистрибутивов ключей, сформированных для пользователей узла, вы можете узнать в папке **Ключевой центр > Своя сеть ViPNet > Сетевые узлы** в списке сетевых узлов в столбце **Число дистрибутивов в комплекте** напротив соответствующего узла.
- Для пользователя, зарегистрированного на нескольких сетевых узлах, требуется формировать дистрибутив ключей на каждом из узлов.
- Если в процессе создания дистрибутива произошла какая-то ошибка (например, межсетевой мастер-ключ не был введен в действие при установке взаимодействия с доверенной сетью ViPNet), то появится соответствующее сообщение с предложением повторить, пропустить или отменить создание дистрибутива ключей для данного пользователя. В этом случае вам следует выбрать одно из предложенных действий и установить причину ошибки. После устранения ошибки вы сможете возобновить процесс создания дистрибутива ключей.
- Если дистрибутив ключей для пользователя создается повторно, то в процессе создания дистрибутива появится сообщение с предложением изменить пароль этого пользователя.

В данном случае вы можете изменить пароль пользователя. Для этого нажмите кнопку **Да**. Если в настройках программы по умолчанию выбран тип **Случайный пароль** или **Случайный цифровой пароль** (см. [Настройка типа создаваемых паролей](#) (на стр. 242)), то пароль будет изменен автоматически, в соответствии с параметрами, заданными для случайных паролей (см. раздел [Настройка параметров случайных паролей](#) (на стр. 243)). Если выбран тип **Собственный пароль**, задайте пароль вручную.



Примечание. Если дистрибутивы ключей создаются повторно для нескольких пользователей, то вы можете изменить пароли сразу для всех пользователей, установив соответствующий флажок в окне с сообщением.

- При повторном создании дистрибутива ключей в его состав не включается резервный набор персональных ключей пользователя (см. [«Резервный набор персональных ключей \(РНК\)»](#)). В связи с этим при передаче сформированного дистрибутива ключей пользователю также требуется любым доверенным способом предоставить соответствующий резервный набор персональных ключей. Если

резервный набор персональных ключей не будет передан пользователю, в дальнейшем у него возникнут проблемы с удаленным обновлением ключей при их компрометации или при смене мастер-ключа сети. В свою очередь, некорректное обновление приведет к потере всех зашифрованных писем пользователя.


Процесс создания

Чтобы сформировать дистрибутив ключей для пользователя, требуется наличие соответствующих справочников связей (файлов связей), полученных из программы ViPNet Центр управления сетью. О том, как отправить из ЦУСа файлы для создания дистрибутива ключей, см. в документе «ViPNet Administrator Центр управления сетью. Руководство администратора», в разделе «Формирование файлов для создания ключей в УКЦ».

Сформировать дистрибутив ключей можно в автоматическом или индивидуальном режиме.



Совет. Автоматический режим удобно использовать в том случае, если требуется сформировать дистрибутивы ключей сразу для всех пользователей, для которых были получены файлы связей (например, при первоначальном развертывании сети ViPNet). Если требуется сформировать дистрибутивы ключей для конкретных пользователей, то рекомендуется использовать индивидуальный режим (например, при добавлении одного или нескольких пользователей в сеть ViPNet или при повторном формировании дистрибутива ключей).

Чтобы создать дистрибутив ключей в автоматическом режиме, в окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Автоматически создать > Дистрибутивы ключей** или на панели инструментов нажмите кнопку **Создать дистрибутивы ключей** . В данном случае запустится процесс создания дистрибутивов ключей для всех пользователей, для которых имеются соответствующие файлы связей.

Для создания дистрибутива ключей в индивидуальном режиме выполните следующие действия:

- 1 В окне программы на панели навигации перейдите в папку **Ключевой центр > Своя сеть ViPNet > Сетевые узлы**.
- 2 В списке сетевых узлов на панели просмотра выберите узел, для пользователя которого требуется создать дистрибутив ключей. Если требуется сформировать дистрибутивы ключей одновременно для нескольких пользователей, то выберите соответственно несколько сетевых узлов (как показано на рисунке ниже).

- 3 Щелкните правой кнопкой мыши и в контекстном меню выберите пункт **Дистрибутивы ключей > Создать**.

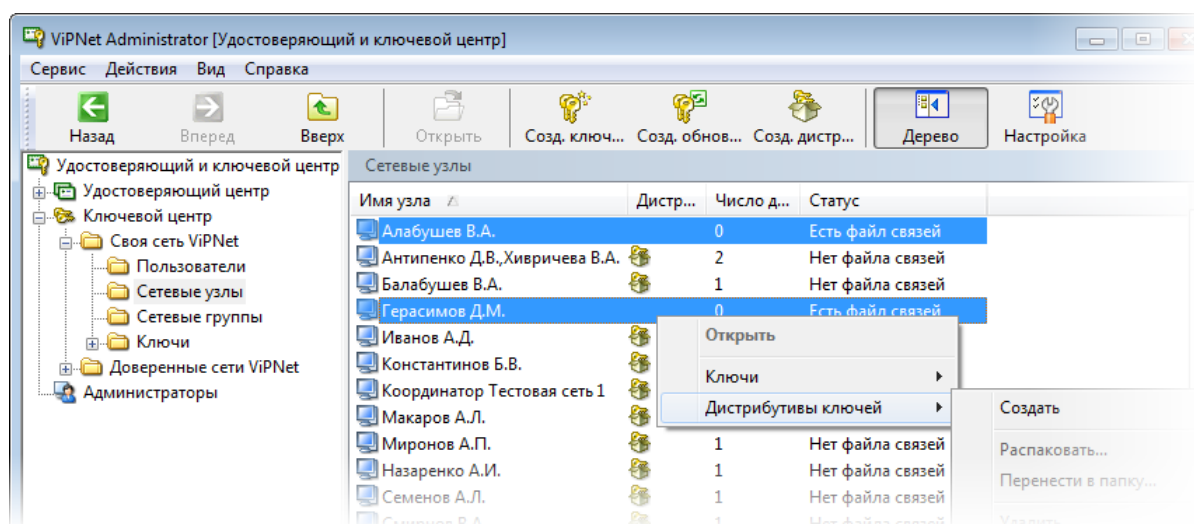


Рисунок 36: Создание дистрибутивов ключей для пользователей нескольких сетевых узлов

В результате запустится процесс создания дистрибутива ключей для пользователя выбранного сетевого узла (или пользователей, если было выбрано несколько узлов).


В процессе создания дистрибутива ключей:

- Появится электронная рулетка (см. Рисунок 27 на стр. 55), если она еще не запускалась в рамках текущей сессии. Поводите указателем в пределах окна **Электронная рулетка**.
- Будет произведена проверка текущих данных на наличие различных аномальных событий. Если при проверки данных будет установлен факт возникновения аномального события, появится соответствующее сообщение, и дальнейшее формирование дистрибутива будет невозможно. Подробнее см. раздел [Проверка текущих данных](#) (на стр. 290).
- Будет издан сертификат открытого ключа (и соответственно создан контейнер ключей), если пользователь, для которого создается дистрибутив ключей, имеет право подписи (задается в ЦУСе). Если пользователю сертификат не нужен (например, если пользователь является администратором координатора), то издание сертификата можно не производить, нажав кнопку **Отмена** в появившемся мастере редактирования полей сертификата.



Примечание. Мастер редактирования полей сертификата запускается в процессе формирования дистрибутива ключей при издании сертификата, только если в настройках программы установлена соответствующая опция: **При автоматическом создании сертификатов** или **При индивидуальном создании сертификатов** (в зависимости от используемого режима формирования дистрибутива). Подробнее см. раздел [Настройка параметров издания сертификатов и обработки запросов](#) (на стр. 250).

Если в процессе создания дистрибутива ключей мастер редактирования полей сертификата не запустится, отменить издание сертификата будет невозможно. Сертификат будет издан автоматически в соответствии параметрами шаблона, выбранного по умолчанию. Подробнее см. раздел [Создание и редактирование шаблонов сертификатов](#) (на стр. 256).

При успешном создании дистрибутивов ключей появится в папке **Ключевой центр > Своя сеть ViPNet > Ключи > Дистрибутивы ключей**. При этом в папке **Ключевой центр > Своя сеть ViPNet > Сетевые узлы** в списке сетевых узлов в столбце **Дистрибутив** появится значок  напротив узла, для пользователя которого был сформирован дистрибутив ключей.

Создание ключей узлов

Ключи узла — набор файлов, создаваемый в УКЦ для каждого сетевого узла. Основное содержание ключей узла — ключи для шифрования между коллективами и между сетевыми узлами, а также другие служебные файлы.

Ключи узла формируются, как правило, при изменениях в структуре своей сети или доверенной сети (например, при добавлении связей).



Внимание! Создание ключей узлов доступно только для сетевых узлов, для которых есть соответствующие справочники связей из ЦУС. То есть для сетевых узлов в папке **Ключевой центр > Своя сеть ViPNet > Сетевые узлы** в колонке **Статус** указано значение **Есть файл связей**.

Для создания ключей узлов воспользуйтесь одним из следующих способов:

- 1 Автоматическое создание ключей (когда нужно создать много ключей, то рекомендуем использовать этот способ).

Для создания ключей узлов сразу для всех сетевых узлов, для которых есть соответствующие файлы связей из ЦУС, воспользуйтесь пунктом главного меню

Сервис > Автоматически создать > Ключи узлов. Запустится процесс создания ключей (см. ниже).

2 Индивидуальное создание ключей.

Для создания ключей узлов для выбранных сетевых узлов выполните следующие действия:

2.1 В папке **Ключевой центр > Своя сеть ViPNet > Сетевые узлы** выберите сетевой узел (или несколько СУ).

2.2 Из контекстного меню по правой кнопке мыши выберите **Ключи > Создать ключи узла**.

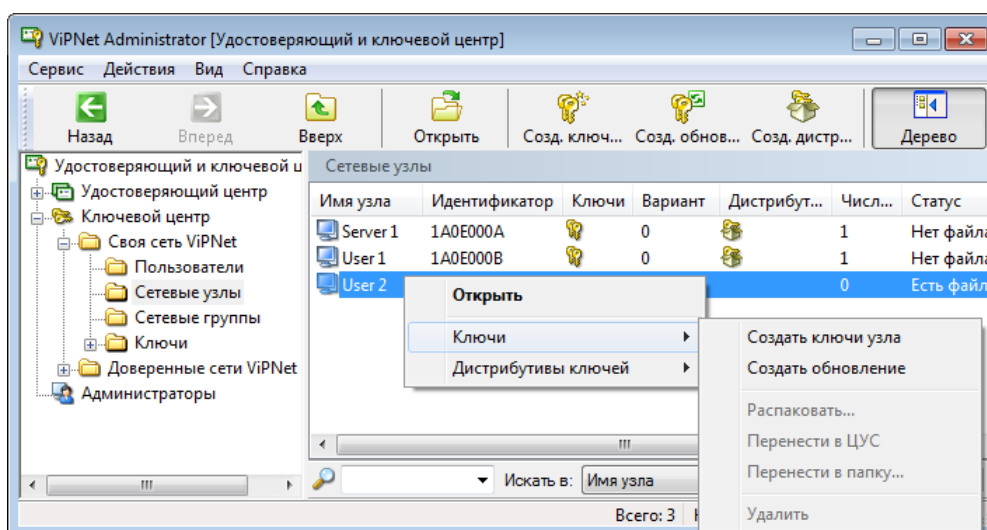


Рисунок 37: Создание ключей узлов

Запустится процесс создания ключей (см. ниже).

2.3 После запуска создания ключей узлов проверяются различные аномальные ситуации. Если аномальные ситуации будут найдены, то на экране появится подсказка, что нужно сделать.

2.4 Если никаких аномалий не обнаружено или они были устранены, то запустится процесс создания ключей.

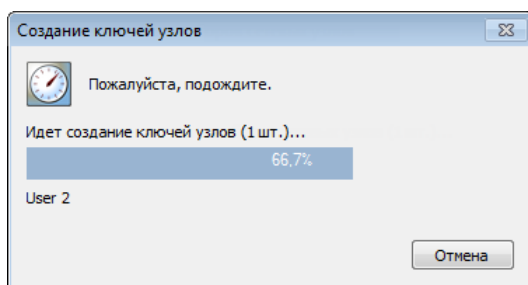



Рисунок 38: Выполнение процесса создания ключей узлов

2.5 После создания ключей узлов в папке **Ключевой центр** > **Своя сеть ViPNet** > **Сетевые узлы** в колонке **Ключи** появится значок .

2.6 Созданные ключи узлов появятся в папке **Ключевой центр** > **Своя сеть ViPNet** > **Ключи** > **Ключи узлов**, откуда их можно перенести в ЦУС для отправки автоматического обновления на СУ (см. [Действия с ключами узлов и обновлениями ключей для СУ](#) (на стр. 111)).



Внимание! Папка **Ключи узлов** будет пустой, если в настройках программы (открывается при помощи пункта главного меню **Сервис** > **Настройка**) в окне **Папки ViPNet Администратора** установлен флажок **Автоматически переносить в ЦУС создаваемые ключи пользователей и узлов** (см. [Настройка папок обмена](#) (на стр. 239)). В этом случае после создания все ключи узлов автоматически переносятся в ЦУС. Если этот флажок снят, то папка **Ключи узлов** будет содержать созданные ключи.

Создание обновлений ключей узлов

Создание обновления ключей узла всегда доступно для всех сетевых узлов ViPNet вне зависимости от наличия файлов связи из ЦУС.

Обновление ключей узла производится в следующих случаях:

- Если произошла смена пароля администратора сетевой группы узлов (см. [«Пароль администратора сетевых узлов»](#) на стр. 129). В этом случае создайте обновление ключей узла самостоятельно (см. ниже).
- Если создана новая подпись администратора УКЦ. В этом случае обновление ключей узла создается автоматически на завершающем этапе работы мастера создания сертификата администратора.

- Если пришел экспорт справочников сертификатов администраторов (см. «[Импорт сертификатов администраторов доверенных сетей ViPNet](#)» на стр. 162) или СОС из доверенных сетей ViPNet (см. «[Импорт списков отозванных сертификатов доверенных сетей ViPNet](#)» на стр. 165). В этом случае при импорте сертификатов администраторов или СОС предлагается создать обновление ключей узла. При отказе следует произвести создание обновлений ключей узла самостоятельно (см. ниже).
- Если из ЦУСа поступила информация о том, что у каких-то пользователей сети ViPNet удалено или добавлено право подписи. В этом случае создайте обновление ключей узла самостоятельно (см. ниже).

Для создания обновления ключей узла воспользуйтесь одним из следующих способов:

- 1 Автоматическое создание обновления (когда нужно создать обновление ключей для всех сетевых узлов, то рекомендуем использовать этот способ).

Для создания обновления ключей узла сразу для всех сетевых узлов воспользуйтесь пунктом главного меню **Сервис > Автоматически создать > Обновления ключей узлов**. Запустится процесс создания ключей узла (см. ниже).

- 2 Индивидуальное создание обновления.

Для создания обновления ключей для выбранных сетевых узлов выполните следующие действия:

- 2.1 В папке **Ключевой центр > Своя сеть ViPNet > Сетевые узлы** выберите сетевой узел (или несколько сетевых узлов).

- 2.2 Из контекстного меню по правой кнопке мыши выберите **Ключи > Создать обновление**.

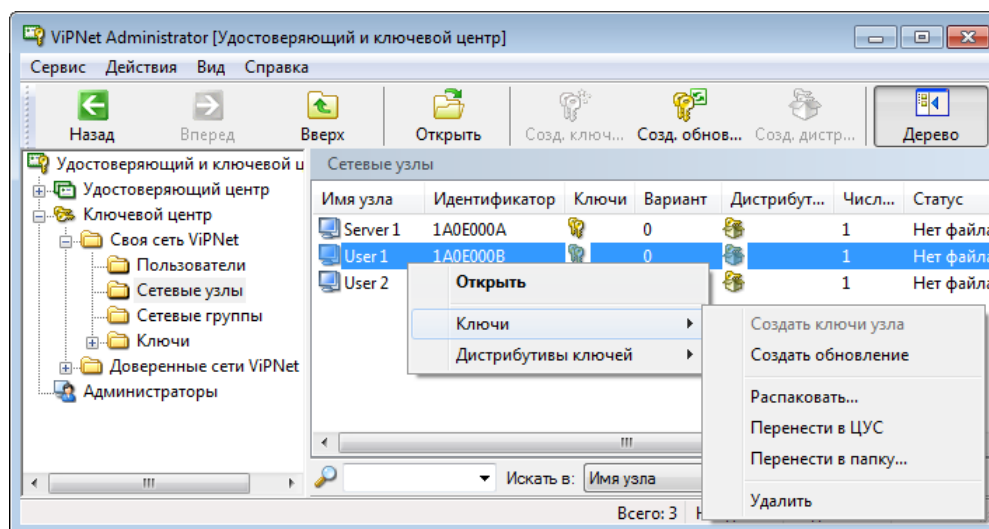


Рисунок 39: Создание обновлений ключей узла

Запустится процесс создания ключей узла (см. ниже).

- 2.3 После запуска создания обновления ключей узла проверяются различные аномальные ситуации. Если аномальные ситуации будут найдены, то на экране появится подсказка, что нужно сделать.
- 2.4 Если никаких аномалий не обнаружено или они были устранены, то запустится процесс создания обновлений.

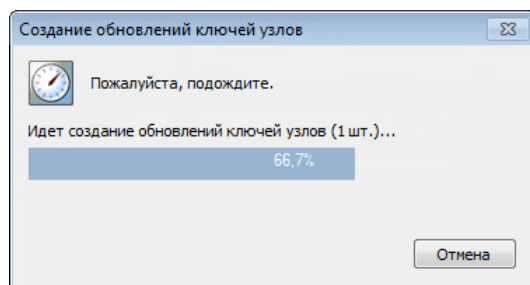



Рисунок 40: Выполнение процесса создания обновлений

- 2.5 После создания обновления ключей для сетевых узлов в папке **Ключевой центр > Своя сеть ViPNet > Сетевые узлы** в колонке **Ключи** появится значок .
- 2.6 Созданные обновления ключей узла появятся в папке **Ключевой центр > Своя сеть ViPNet > Ключи > Обновления ключей узлов**, откуда их можно перенести в ЦУС для отправки автоматического обновления на сетевые узлы ViPNet (см. [Действия с ключами узлов и обновлениями ключей для СУ](#) (на стр. 111)).



Внимание! Папка **Обновления ключей узлов** будет пустой, если в настройках программы (открывается при помощи пункта главного меню **Сервис > Настройка**) в окне **Папки ViPNet Администратора** установлен флажок **Автоматически переносить в ЦУС создаваемые ключи пользователей и узлов** (см. [Настройка папок обмена](#) (на стр. 239)). В этом случае после создания все обновления ключей узла автоматически переносятся в ЦУС. Если этот флажок снят, то папка **Обновления ключей узлов** будет содержать созданные обновления ключей узла.

Создание ключей пользователей

Ключи пользователя — набор файлов, создаваемый в УКЦ для каждого пользователя сетевого узла. Основное содержание ключей пользователя — информация, идентифицирующая пользователя и позволяющая работать с прикладными задачами сети ViPNet. Кроме того, в ключах пользователя находится электронная подпись данного пользователя, если администратор ЦУС разрешил пользователю подписывать документы.

Ключи пользователя формируются, как правило, если требуется создавать ключи для нового пользователя (ключи которого еще ни разу не создавались), при истечении срока действия сертификата пользователя, и, если требуется, изменить пароль пользователя.



Внимание! Создание ключей пользователей доступно только для пользователей, для которых есть соответствующие справочники связей из ЦУС. То есть для пользователей в папке **Ключевой центр > Своя сеть ViPNet > Пользователи** в колонке **Статус** указано значение **Есть файл связей**.

Создание ключей пользователей производится в соответствии с настройками программы, заданными в окне **Настройка**. Настройку можно осуществить при выборе пункта меню **Сервис > Настройка**.

Для создания ключей пользователей воспользуйтесь только индивидуальным способом создания ключей:

- 1** В папке **Ключевой центр > Своя сеть ViPNet > Пользователи** выберите пользователя (или несколько пользователей), для которых есть соответствующие файлы связей из ЦУС.
- 2** Из контекстного меню по правой кнопке мыши выберите **Ключи пользователя > Создать**.

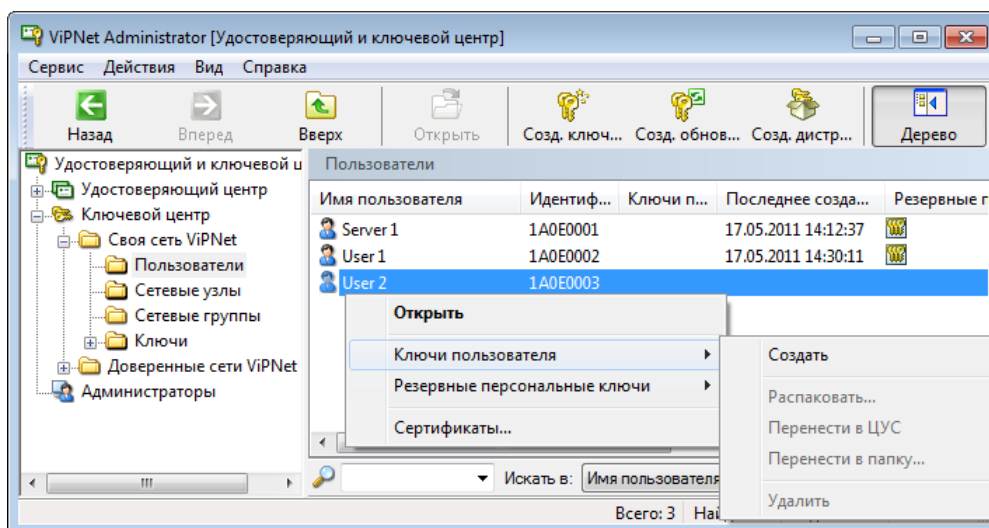


Рисунок 41: Создание ключей пользователя

Запустится процесс создания ключей (см. ниже).

- 3 После запуска создания ключей пользователя проверяются различные аномальные ситуации. Если аномальные ситуации будут найдены, то на экране появится подсказка, что нужно сделать.
- 4 Если никаких аномалий не обнаружено или они были устранены, то запустится процесс создания ключей.

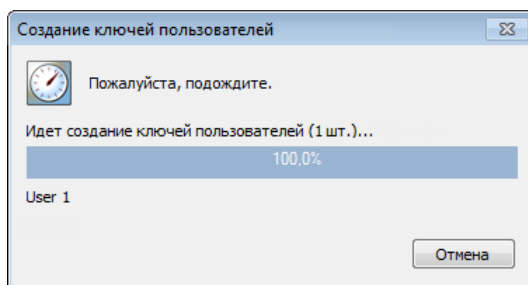


Рисунок 42: Процесс создания ключей пользователей

В процессе создания ключей может запуститься электронная рулетка (см. Рисунок 27 на стр. 55), если она еще не запускалась в данном сеансе работы УКЦ. Выполните действия, предлагаемые электронной рулеткой, после чего создание ключей пользователя продолжится.

В процессе создания ключей пользователя для каждого пользователя, у которого есть право подписи (определяется в ЦУС), создаются сертификаты. При этом может открываться окно **Редактирование полей сертификата** (см. «[Мастер редактирования полей сертификата](#)» на стр. 144), если в настройках программы в окне **Сертификаты** в


разделе **Отображать сертификаты для редактирования** установлен флажок **При индивидуальном создании сертификатов** (см. «[Настройка параметров издания сертификатов и обработки запросов](#)» на стр. 250). После заполнения полей (если это требуется) в этом окне нажмите **ОК** (означает издание сертификата для данного пользователя; при нажатии **Cancel** сертификат издан не будет), и создание ключевой информации продолжится.

Если срок действия издаваемого сертификата пользователя превышает срок действия сертификата текущего администратора УКЦ, то будет выдано сообщение об установке точно такого же срока действия издаваемого сертификата, как у текущего администратора УКЦ. Для создания сертификата нажмите **ОК** в окне с сообщением.

Если упомянутый флажок не установлен, то издание сертификата произойдет автоматически (равносильно нажатию кнопки **ОК**). При этом если срок действия издаваемого сертификата превышает срок действия сертификата текущего администратора УКЦ, то для издаваемого сертификата будет автоматически установлен срок действия, как у текущего администратора УКЦ.

Если ключи пользователя создаются не в первый раз, то на экране появится вопрос об изменении пароля пользователя: **Ввести новый пароль пользователя?**. Ответьте на вопрос. Чтобы применить выбранное действие для всех пользователей, установите флажок для всех. Создание ключей продолжится.

Если в процессе создания произойдет какая-то ошибка, то появится сообщение об ошибке и будет предложен выбор: Повторить, Пропустить, Отменить.

После создания ключей пользователей в папке **Ключевой центр > Своя сеть ViPNet > Пользователи** в колонке **Ключи пользователя** появится значок .

Созданные ключи пользователей можно посмотреть и обработать в окне **Ключевой центр > Своя сеть ViPNet > Ключи > Ключи пользователя**, откуда их можно перенести в ЦУС для отправки автоматического обновления на СУ (см. [Действия с ключами пользователей](#) (на стр. 108)).



Внимание! Папка **Ключи пользователей** будет пустой, если в настройках программы (открывается при помощи пункта главного меню **Сервис > Настройка**) в окне **Папки ViPNet Администратора** установлен флажок **Автоматически переносить в ЦУС создаваемые ключи пользователей и узлов** (см. [Настройка папок обмена](#) (на стр. 239)). В этом случае после создания все ключи пользователей автоматически переносятся в ЦУС. Если этот флажок снят, то папка будет содержать созданные ключи.

Просмотреть и сохранить пароль выбранного пользователя (в файл или на внешнее устройство хранения данных) можно из папки **Ключевой центр > Своя сеть ViPNet > Пользователи** в окне **Свойства пользователя** на вкладке **Пароль**. Для открытия окна **Свойства пользователя** выберите пользователя и два раза щелкните на нем левой кнопкой мыши (см. [Сохранение паролей пользователей и администраторов сетевых узлов](#) (на стр. 131)).

Просмотреть сертификаты пользователей можно из окна **Удостоверяющий центр > Сертификаты пользователей > Своя сеть ViPNet** (см. [Просмотр сертификатов](#) (на стр. 182)).

Создание резервных наборов персональных ключей

Резервные персональные ключи пользователя используется для дистанционного обновления ключей пользователя при их компрометации. Резервные наборы персональных ключей (РНПК) формируются для каждого пользователя. РНПК передается администратором УКЦ каждому пользователю некоторым защищенным способом (см. ниже). Пользователи должны хранить РНПК в безопасном месте. Если текущий персональный ключ пользователя скомпрометирован, то УКЦ высылает пользователю новые ключи, защищенные с использованием очередного варианта персонального ключа, который по сети передавать не нужно, так как он уже есть в РНПК, переданном пользователю заранее лично в руки.

Резервные персональные ключи пользователя автоматически формируется при создании самого первого ключевого дистрибутива (dst-файла) пользователя, и входят в его состав.

Число персональных ключей и минимальное число нескомпрометированных ключей в наборе определяется настройками УКЦ (см. «[Настройка параметров создания резервных наборов персональных ключей](#)» на стр. 247) (окно **Настройка > Персональные ключи**, параметры **Число персональных ключей в наборе пользователей** и **Минимальное число нескомпрометированных ключей в наборе пользователей** соответственно). Резервные персональные ключи пользователя имеют последовательно возрастающие варианты.

В дальнейшем резервные персональные ключи пользователя автоматически создаются и попадают в состав ключевого дистрибутива или ключей пользователя (в зависимости от того, что будет формироваться в момент создания нового набора резервных ключей) только в следующих случаях:

- При смене мастера персональных ключей.
- При компрометации, при условии, что оставшееся число нескомпрометированных персональных ключей в наборе пользователей меньше заданного числа в настройках УКЦ. Этот случай наступает в тот момент, когда для какого-то пользователя разница

между номером последнего персонального ключа в наборе и номером (вариантом) действующего персонального ключа становится меньше (на 1), чем значение опции **Минимальное число некомпрометированных ключей в наборе пользователей** в настройках УКЦ. РНПК создается в соответствии с параметром **Число персональных ключей в наборе пользователей** настроек УКЦ, при этом первый номер действующего ключа в новом наборе будет равен значению на 1 меньше номера последнего ключа в предыдущем наборе. Вариант персонального ключа пользователя меняется при компрометации его ключей. Увидеть информацию о варианте действующего персонального ключа пользователя и определить число оставшихся ключей можно в папке **Ключи > Резервные персональные ключи**.

Резервные персональные ключи можно создавать в индивидуальном режиме при помощи контекстного меню **Резервные персональные ключи > Создать** в папке **Ключевой центр > Своя сеть ViPNet > Пользователи**. В этом случае они не попадают в состав ключевого дистрибутива или ключей пользователя.

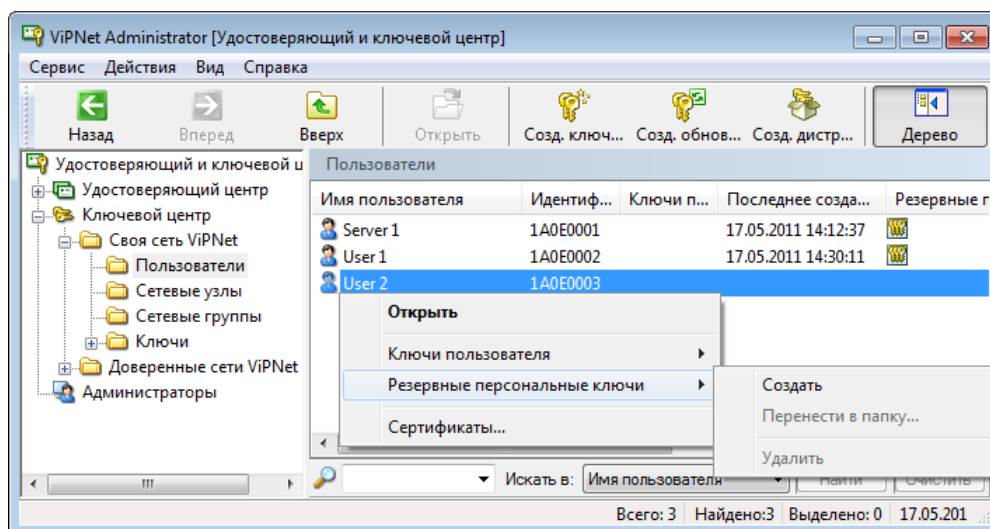



Рисунок 43: Создание резервных персональных ключей

О наличии резервных персональных ключей для пользователя свидетельствует значок  в колонке **Резервные персональные ключи**.

Все созданные резервные наборы ключей пользователей отображаются в папке **Ключи > Резервные персональные ключи**, откуда их можно перенести для передачи пользователю (см. [Действия с резервными персональными ключами](#) (на стр. 117)).

Администратору УКЦ необходимо выдавать резервные персональные ключи пользователю каждому пользователю сети ViPNet сразу после их формирования (то есть в случаях, указанных выше):

- Если резервные персональные ключи пользователя входят в состав ключевого дистрибутива или созданы в индивидуальном режиме, то для передачи пользователю запишите каждому пользователю на отдельный индивидуальный носитель его ключевой дистрибутив (см. «[Действия с созданными дистрибутивами ключей](#)» на стр. 113) или непосредственно сам файл с резервным набором (при помощи пункта меню **Перенести в папку** из окна **Ключи > Резервные персональные ключи**). Затем индивидуальные носители передаются пользователям лично в руки или по альтернативному защищенному каналу (например, с использованием доверенных нарочных с документальным подтверждением отправки и приема, использованием ведомственной или фирменной фельдъегерской связи и др.).
- Если резервные персональные ключи пользователя входят в состав ключей пользователя, то для передачи их пользователю необходимо отправить обновление ключей на СУ пользователя (см. «[Действия с ключами пользователей](#)» на стр. 108).







Внимание! При инициализации на СУ адресно-ключевой информации (при помощи dst-файла) мастер инициализации предложит пользователю сохранить файл РНПК в заданной папке. По умолчанию РНПК поместится в подпапку d_STATION\ABN_AAAA папки установки ПО ViPNet на СУ, и будет храниться там. Однако необходимо рекомендовать пользователям, для обеспечения большей безопасности, хранить переданные им файлы РНПК отдельно от ключей пользователя в безопасном месте, например, в сейфе. Пользователь несет личную ответственность за хранение в секрете от посторонних лиц переданного ему РНПК. Пользователи должны предъявлять файлы РНПК прикладной программе ViPNet по ее требованию.

Создание ключей при компрометациях

В случае компрометации ключей пользователя (см. «[Действия при компрометациях ключей](#)» на стр. 79) для формирования ключей становится доступным только пункт меню **Сервис > Автоматически создать > Ключи при компрометациях**. Этот пункт меню предназначен для создания ключевой информации для скомпрометированных пользователей и для создания ключевой информации пользователей и сетевых узлов, имеющих связи со скомпрометированным пользователем.

Если информации о скомпрометированных пользователях нет, то пункт меню **Ключи при компрометациях** будет недоступным.

Если из ЦУС поступили данные о компрометации ключей пользователей, то для скомпрометированных пользователей в папке **Ключевой центр > Своя сеть ViPNet > Пользователи** будет отображаться значок  вместо , а для сетевых узлов в папке **Ключевой центр > Своя сеть ViPNet > Сетевые узлы**, в которые входят эти пользователи, будет отображаться значок  вместо . В колонке **Статус** для скомпрометированных пользователей и узлов будет указано значение **Скомпрометирован**.

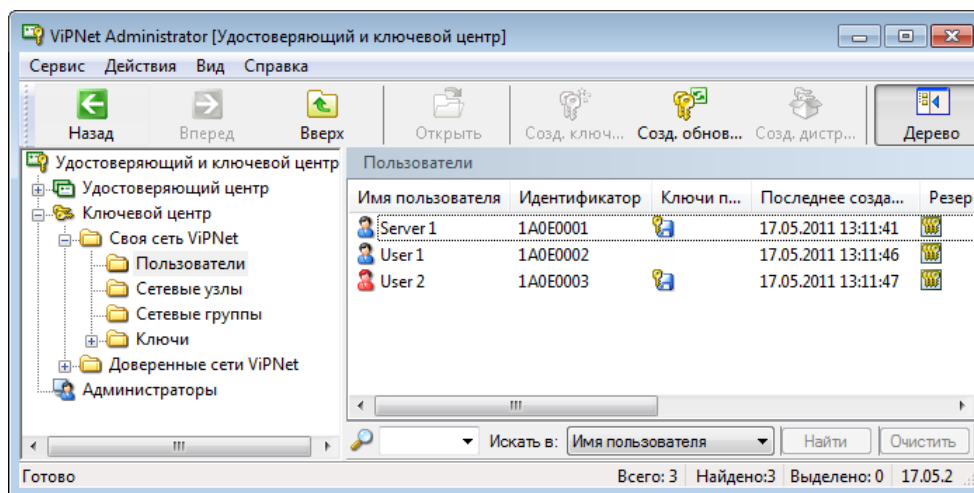


Рисунок 44: Пользователи сети ViPNet

Для формирования ключей при компрометации выберите пункт меню **Сервис > Автоматически создать > Ключи при компрометациях**. Будут созданы новые ключи пользователей и увеличен вариант персонального ключа для скомпрометированных пользователей. Для всех сетевых узлов, на которых зарегистрированы эти скомпрометированные пользователи, будет сформирован новый вариант сетевого узла. При формировании ключей скомпрометированных пользователей, новый пароль всегда будет создаваться случайным, независимо от настроек УКЦ (см. [«Настройка типа создаваемых паролей»](#) на стр. 242). Для всех СУ, где зарегистрированы скомпрометированные пользователи, и для всех СУ, с которыми связаны эти СУ, сформируется ключи узла.

Созданные ключи пользователей и ключи узлов появятся в соответствующих подпапках папки **Ключевой центр > Своя сеть ViPNet > Ключи**, откуда их необходимо перенести в ЦУС для отправки обновлений на СУ (см. [Действия с созданной ключевой информацией](#) (на стр. 107)).

Действия с созданной ключевой информацией

После того, как ключевая информация будет создана, она отобразится в папке **Ключевой центр > Своя сеть ViPNet > Ключи**. Созданная ключевая информация представляет собой ключи пользователей, ключи узлов или обновления ключей для сетевых узлов, дистрибутивы для начальной инсталляции и резервные наборы персональных ключей. Папка **Ключи** состоит, соответственно, из четырех папок: **Ключи пользователей**, **Ключи узлов**, **Дистрибутивы ключей** и **Резервные персональные ключи**. Все эти папки содержат списки элементов, соответствующих названиям папок.



Внимание! Папки **Ключи пользователей** и **Ключи узлов** будут пустыми, если в окне **Сервис > Настройка** в окне **Папки ViPNet Администратора** установлен флажок в опции **Автоматически переносить в ЦУС создаваемые ключи пользователей и узлов** (см. [Настройка папок обмена](#) (на стр. 239)). В этом случае после создания все ключи пользователей и узлов будут автоматически переноситься в ЦУС. Если этот флажок не установлен, то папки будут содержать соответствующую информацию (см. далее).

Папка **Ключи > Ключи пользователей** содержит список созданных ключей пользователей сети. С ключами пользователей можно производить следующие действия: удаление, перенос ключей в выбранную папку диска, перенос в ЦУС (для дальнейшего автоматического обновления из ЦУС), распаковку (то есть преобразование ключей к виду, готовому для работы — для ручного обновления) в папку диска и на различные носители информации. Подробно о действиях с созданной ключевой информацией пользователя см. раздел [Действия с ключами пользователей](#) (на стр. 108).

Папки **Ключи > Ключи узлов** и **Ключи > Обновления ключей узлов** содержат список созданных ключей узлов и обновлений ключей для каждого узла сети. С ключами узлов можно производить следующие действия: удаление, перенос ключей в папку диска, перенос в ЦУС (для дальнейшего автоматического обновления из ЦУС), распаковку в папку диска. Подробно о действиях с ключами узлов см. раздел [Действия с ключами узлов и обновлениями ключей для СУ](#) (на стр. 111).

Папка **Ключи > Дистрибутивы ключей** содержит список созданных дистрибутивов. С готовыми дистрибутивами можно производить следующие действия: просмотр информации о дистрибутиве, удаление, перенос и распаковку в выбранную папку на диске и на различные носители информации с выбором типа аутентификации

пользователя. Подробно о действиях с дистрибутивами см. раздел [Действия с созданными дистрибутивами ключей](#) (на стр. 113).

Папка **Ключи** > **Резервные персональные ключи** содержит список созданных резервных наборов ПК для каждого пользователя (см. раздел [Действия с резервными персональными ключами](#) (на стр. 117)).



Внимание! Созданная ключевая информация будет работоспособна только после выполнения в программе УКЦ действий либо по распаковке или переносу ее в ЦУС или папку. Переносить созданные ключи (например, в УКЦ вручную перенести дистрибутивы из папки `\DISTRIB`), не используя действия УКЦ, нельзя.

Действия с ключами пользователей

Папка **Ключи** > **Ключи пользователей** содержит список созданных ключей пользователей сети.

С ключами пользователей можно производить следующие действия:

- Распаковка в выбранную папку на диске и на различные носители информации.
- Перенос в ЦУС (для дальнейшего автоматического обновления из ЦУС).
- Перенос ключей в выбранную папку на диске.
- Удаление.

Все действия можно осуществить, если воспользоваться контекстным меню. Рассмотрим все действия подробно и по порядку.

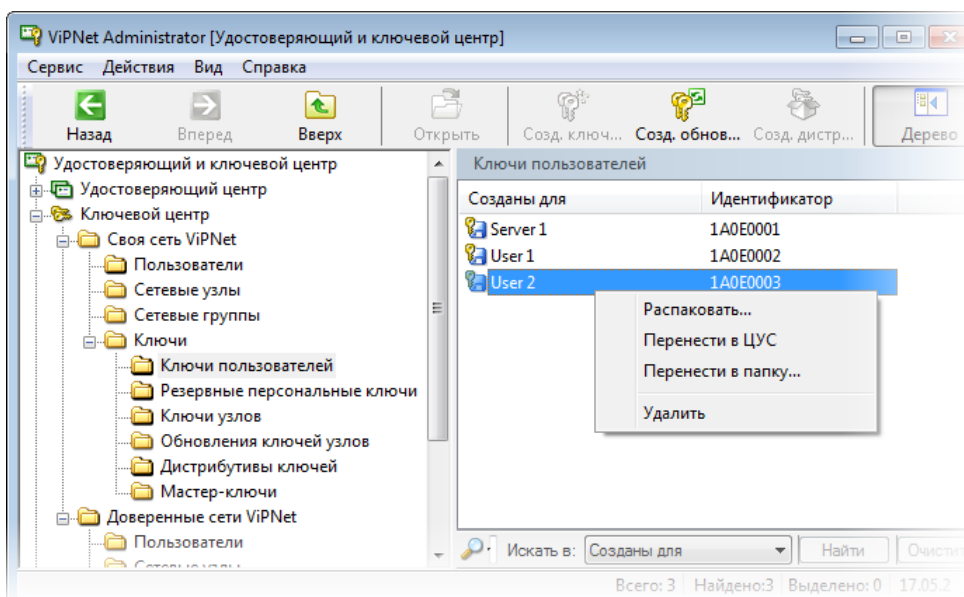


Рисунок 45: Возможные действия с ключами пользователей

Для распаковки ключей пользователей необходимо выбрать один или несколько комплектов ключей и из контекстного меню — пункт **Распаковать**. Откроется окно **Распаковка ключевой информации**.

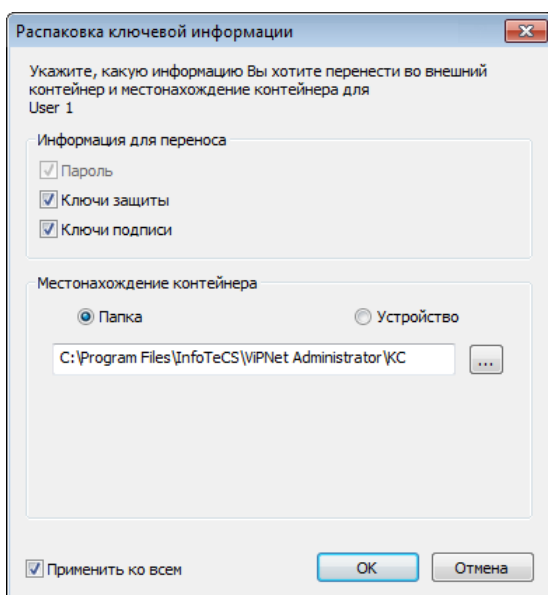


Рисунок 46: Распаковка ключевой информации

В этом окне можно указать, какую информацию, и на какой носитель необходимо ее перенести. В папку на диске можно перенести ключи защиты и ключи подписи

пользователя, а на внешнее устройство хранения данных также можно перенести и пароль.



Внимание! Ключи защиты, перенесенные на внешние устройства хранения данных с помощью ViPNet Administrator Удостоверяющий и ключевой центр версии 3.2.0 нельзя использовать для аутентификации и первичной инициализации в продуктах, входящих в пакет ViPNet CUSTOM 3.0.6. Данный функционал поддерживается в версиях ViPNet CUSTOM и ViPNet CryptoService, начиная с версии 3.1.x.

Для переноса ключей:

- Выберите переключатель для указания местонахождения контейнера в разделе **Местонахождение контейнера**:
 - **Папка** – в этом случае укажите папку для переноса контейнера.
 - **Устройство** – в этом случае выберите считыватель или внешнее устройство из списка установленных доступных устройств хранения данных (не забудьте обеспечить контакт ключа с выбранным устройством). При необходимости введите ПИН. Подробную информацию о поддерживаемых внешних устройствах хранения данных и особенностях работы с ними см. в разделе [Информация о внешних устройствах хранения данных](#) (на стр. 35).
- Выберите соответствующие опции для указания ключевой информации для переноса (распаковки) в разделе **Информация для переноса**:
 - При выборе **Устройство** будут доступны опции **Пароль** и **Ключи** подписи.
 - При выборе **Папка** будут доступны опции **Ключи защиты** и **Ключи** подписи.
- Опция **Применить ко всем** доступна только в том случае, если выбрано несколько комплектов ключей пользователей и в качестве местонахождения контейнера выбрана **Папка**. Включение данной опции означает, что все настройки применимы ко всем комплектам. По умолчанию опция выключена. Это означает, что данное окно будет появляться последовательно для настроек параметров переноса для каждого комплекта ключей. При этом будет меняться имя пользователя, для которого переносится ключи.
- Далее нажмите **ОК**.

Начнется процесс переноса информации, если было отмечено устройство хранения данных, то программа предложит обеспечить контакт ключа с выбранным устройством для каждого пользователя (если их несколько).

После распаковки ключевой информации в указанную папку информация о данном пользователе исчезнет из списка созданных ключей. Путь к файлам распакованных ключей пользователя будет: <указанная папка>\<имя пользователя>\Key_disk\dom*.*.

Сохранение паролей возможно также и из окна **Свойства пользователя** (см. раздел [Просмотр свойств пользователя](#) (на стр. 133)).

Для переноса в ЦУС (переноса в папку для файлов, подлежащих обработке ЦУС для последующей централизованной отправки автоматического обновления ключей пользователей из ЦУС) созданных ключей пользователей необходимо выбрать один или несколько комплектов ключей и из контекстного меню по правой клавише мыши выбрать пункт **Перенести в ЦУС**.

Для переноса в какую-либо папку созданных ключей пользователей необходимо выбрать один или несколько комплектов ключей и из контекстного меню выбрать пункт **Перенести в папку**. Откроется окно в котором нужно выбрать папку и нажать **ОК**. Ключи пользователей будут перенесены в выбранную папку в подпапки с именами соответствующих пользователей (в виде файлов *.ke). Для обновления ключей пользователя на СУ нужно на СУ положить этот файл в подпапку ccc\key папки установки ПО ViPNet.

Для удаления ключей пользователей выберите один или несколько комплектов ключей и воспользуйтесь пунктом **Удалить** контекстного меню. В результате этого действия выбранные ключи пользователей исчезнут из списка.

Действия с ключами узлов и обновлениями ключей для СУ

Папка **Ключи** > **Ключи узлов** содержит список созданных ключей для каждого сетевого узла.

Папка **Ключи** > **Обновление ключей** содержит список созданных обновлений ключей для каждого сетевого узла.

С ключами можно производить следующие действия:

- Распаковка в выбранную папку на диске.
- Перенос в ЦУС для отправки автоматического обновления на сетевые узлы.
- Перенос ключей узла в выбранную папку на диске.
- Удаление.

Все действия можно осуществить, если воспользоваться контекстным меню. Рассмотрим все действия подробно и по порядку.

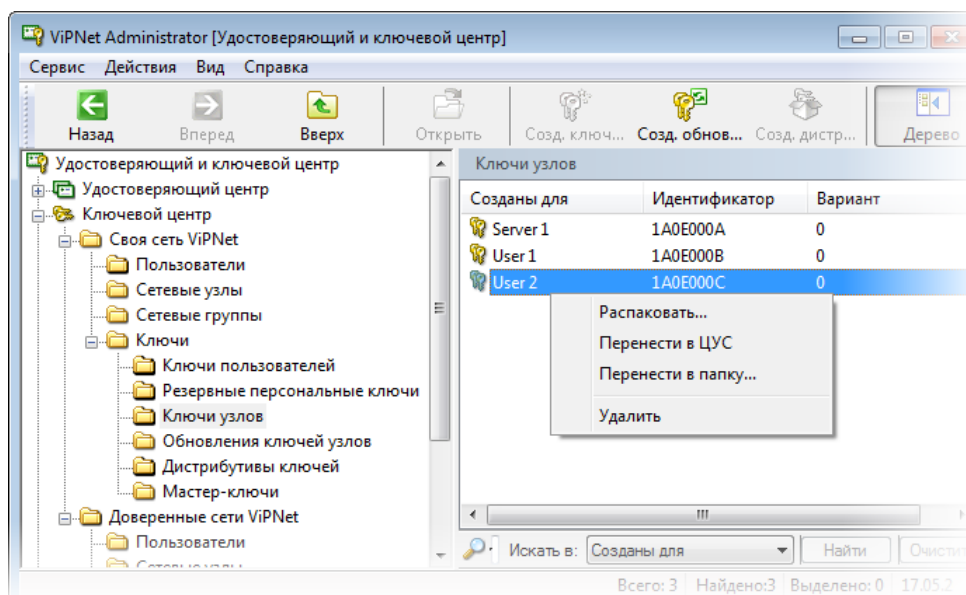


Рисунок 47: Возможные действия с КН и обновлениями ключей

Для распаковки ключей узлов необходимо выбрать один или несколько комплектов ключей и из контекстного меню выбрать пункт **Распаковать**. Далее выберите папку, куда будут распакованы ключи узла и нажмите **ОК**. После распаковки информация о данном СУ исчезает из списка созданных ключей.

Для переноса в ЦУС (переноса в папку для файлов, подлежащих обработке ЦУС для последующей централизованной отправки автоматического обновления ключей узлов из ЦУС) созданных ключей узлов необходимо выбрать один или несколько комплектов ключей узлов и из контекстного меню выбрать пункт **Перенести в ЦУС**. После переноса ключей в ЦУС они исчезнут из списка созданных ключей.

Для переноса в какую-либо папку созданных ключей узлов необходимо выбрать один или несколько комплектов ключей и из контекстного меню по правой клавише мыши выбрать пункт **Перенести в папку**. Откроется окно, в котором нужно выбрать папку и нажать **ОК**. Ключи узла будут перенесены в выбранную папку в подпапки с именами соответствующих СУ (в виде файлов *.ke) и исчезнут из списка созданных.

Для обновления ключей узла нужно на СУ положить этот файл в подпапку `CCC\key` папки установки ПО ViPNet на СУ.

Для удаления ключей узлов выберите один или несколько комплектов ключей и воспользуйтесь пунктом **Удалить** контекстного меню. В результате этого действия выбранные комплекты ключей узлов исчезнут из списка.

Действия с созданными дистрибутивами ключей

Папка **Ключи > Дистрибутивы ключей** содержит список сетевых узлов, для которых созданы дистрибутивы ключей.

С дистрибутивами можно производить следующие действия:

- Открыть.
- Распаковка дистрибутива в выбранную папку на диске и на различные носители информации с выбором типа аутентификации пользователя.
- Перенос в выбранную папку на диске и на различные носители информации с выбором типа аутентификации пользователя. Это действие следует выбрать для переноса дистрибутивов ключей в ЦУС для дальнейшей отправки обновления из ЦУС.
- Удаление.

Все эти действия можно осуществить, если воспользоваться контекстным меню, если выбрать соответствующий пункт.

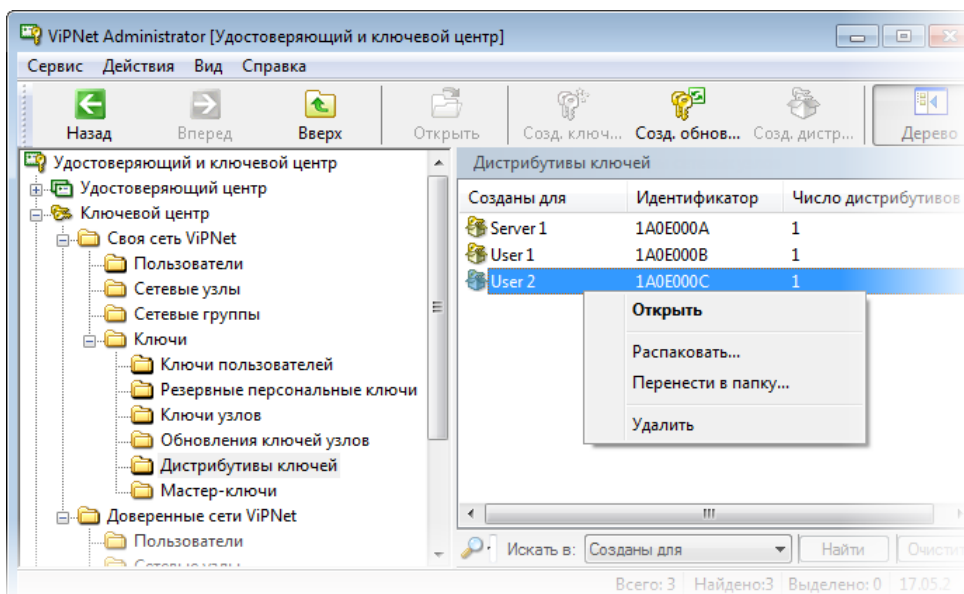


Рисунок 48: Возможные действия с дистрибутивами ключей

Выбор пункта **Открыть** (или двойной щелчок на выбранном СУ) откроет диалоговое окно **Свойства сетевого узла**, где на вкладке **Дистрибутивы** (см. «[Просмотр свойств сетевого узла](#)» на стр. 136) можно выполнить все перечисленные выше действия с дистрибутивом каждого пользователя выбранного сетевого узла (на СУ может быть несколько пользователей) с помощью кнопок, соответствующих действиям контекстного меню.

Кроме того, те же самые действия для созданных дистрибутивов будут доступны также из контекстного меню на выбранном узле (узлах) папки **Ключевой центр > Своя сеть ViPNet > Сетевые узлы**, а также из вкладки **Дистрибутивы** при открытии свойств выбранного узла в этой же папке.

Рассмотрим все действия подробно и по порядку.

Для распаковки в какую-либо папку созданных дистрибутивов сетевого узла выберите из списка соответствующий сетевой узел и используйте действие **Распаковать** (любым из вышеперечисленных способов). Откроется окно **Перенос дистрибутивов ключей**.

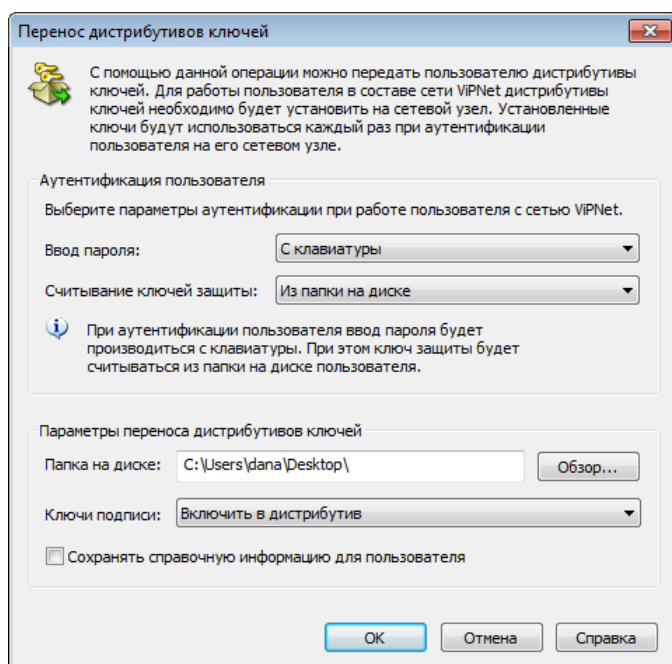


Рисунок 49: Перенос дистрибутивов ключей

Распаковать дистрибутив означает получить весь набор файлов, необходимых пользователю для первичного запуска прикладной программы сети ViPNet на СУ – набор ключей для пользователей и сетевого узла, лицензионный файл (infotecs.re), а также адресные справочники.

Распаковка дистрибутива аналогична функции перенос лишь с той разницей, что при переносе файлы дистрибутивов переносятся в заданную папку как файлы *.dst, а при распаковке файлы дистрибутивов распаковываются в заданную папку для распаковки, и путь к ним выглядит для каждого узла и дистрибутива следующим образом: <заданная папка> \ <папка с именем выбранного узла > \ <папка с именем пользователя выбранного узла> \.<папка ключей пользователя – Key_disk (папка для СУ – D_STATION; файлы-справочники, infotecs.re и др. файлы)>.

Для переноса в какую-либо папку созданных дистрибутивов сетевых узлов необходимо выбрать из списка один или несколько сетевых узлов и использовать действие **Перенести в папку** любым из вышеперечисленных способов. Откроется окно **Перенос дистрибутивов ключей** (см. Рисунок 49 на стр. 114).

В данном окне задайте параметры для переноса дистрибутива ключей:

- В группе **Авторизация пользователя** выбираются параметры для авторизации пользователя при его работе на узле сети ViPNet:
 - **Ввод пароля** – выберите из списка, откуда пользователь будет производить ввод пароля: с клавиатуры (значение по умолчанию) или с внешнего устройства. При выборе параметра ввода пароля с клавиатуры ключи защиты могут быть считаны либо с внешнего устройства, либо из папки на диске (см. след. параметр авторизации). При выборе параметра ввода пароля с внешнего устройства ключи защиты могут быть считаны только из папки на диске (см. след. параметр авторизации).
 - **Считывание ключей защиты** – выберите из списка, откуда будут считываться ключи защиты пользователя: из папки на диске (значение по умолчанию) или с внешнего устройства. При этом значение из списка можно выбрать только в том случае, если в списке **Ввод пароля** выбрано значение **С клавиатуры**.
- В группе **Параметры переноса дистрибутивов ключей** указываются:
 - **Папка на диске** – укажите папку на диске для переноса файлов дистрибутивов (файлы *.dst) для всех пользователей выбранного сетевого узла (или узлов). Указать папку можно при помощи кнопки **Обзор**. Эти файлы будут располагаться по следующему пути: <заданная папка> \ <папка с именем выбранного узла> \ <папка с именем пользователя выбранного узла >. Например, при условии задания папки C:\Distr путь к файлу дистрибутива abn_0001.dst пользователя A1 сетевого узла S1 будет таким: C:\Distr\S1\A1\.



Примечание. Для переноса дистрибутивов ключей для отправки из ЦУС задайте папку DST в папке отправки файлов в ЦУС (по умолчанию FOR_NCC). Следует учитывать, что дистрибутивы ключей пользователей можно отправить только на сетевые узлы (с ПО ViPNet), работающие под ОС Linux. На сетевых узлах (с ПО ViPNet), работающих под ОС Windows, обновление дистрибутивов ключей

пользователей не обрабатывается.

- **Ключи подписи** – выберите из списка, куда перенести ключи подписи пользователя: включить их в дистрибутив или перенести на внешнее устройство. По умолчанию ключи подписи будут включены в дистрибутив.



Внимание! Если ключи подписи будут включены в дистрибутив, а ключ защиты при этом будет сохранен на внешнем устройстве, подпись и расшифрование в сторонних приложениях (например, в MS Office) будут невозможны. Во избежание проблем доступа к ключу защиты в сторонних приложениях рекомендуется ключи подписи сохранять там же где и их ключ защиты.

- **Сохранять справочную информацию для пользователя** – установите флажок, чтобы в папке переноса (распаковки) дистрибутива ключей также сохранить парольную информацию.
- Опция **Применить ко всем** будет доступна только в том случае, если выбрано несколько сетевых узлов и (или) на одном СУ имеется несколько пользователей, и следовательно, несколько дистрибутивов. Если включить опцию, то все заданные в окне **Перенос дистрибутивов ключей** параметры будут применены ко всем дистрибутивам выбранных СУ. По умолчанию опция выключена. Это означает, что данное окно будет появляться последовательно для настроек параметров переноса для каждого дистрибутива. При этом будет меняться имя пользователя, для которого переносится дистрибутив.
- После выбора необходимых параметров нажмите **ОК**. Начнется процесс переноса дистрибутивов. Если были выбраны параметры переноса некоторых данных пользователя (пароля, ключей защиты и (или) ключей подписи) на внешнее устройство, то появится окно выбора внешнего устройства для сохранения данных пользователя.
- Обеспечьте контакт ключа с устройством, выберите доступный считыватель и устройство, а также при необходимости введите ПИН. Нажмите **ОК**. Начнется процесс переноса данных для указанного пользователя. Если было выбрано несколько СУ или на СУ несколько пользователей, то окно выбора внешнего устройства будет появляться для каждого пользователя, соответственно для каждого пользователя нужно выполнить указанные действия. Данные каждого пользователя необходимо записывать на отдельные ключи.

Подробную информацию о поддерживаемых внешних устройствах хранения данных и особенностях работы с ними см. в разделе [Информация о внешних устройствах хранения данных](#) (на стр. 35).

- Дистрибутивы ключей вместе с паролями пользователей и ключами (если при переносе дистрибутивов какие-то данные были перенесены на внешнее устройство хранения данных) нужно каким-либо защищенным способом передать соответствующим пользователям.

Для удаления какого-либо дистрибутива или нескольких дистрибутивов выберите нужные и воспользуйтесь пунктом **Удалить** контекстного меню (см. Рисунок 48 на стр. 113). Для удаления из окна **Свойства сетевого узла** на вкладке **Дистрибутивы** воспользуйтесь кнопкой **Удалить**. В результате этого действия выбранные дистрибутивы исчезнут из списка.

Действия с резервными персональными ключами

Все созданные резервные наборы ключей пользователей отображаются в папке **Ключи > Резервные персональные ключи**.

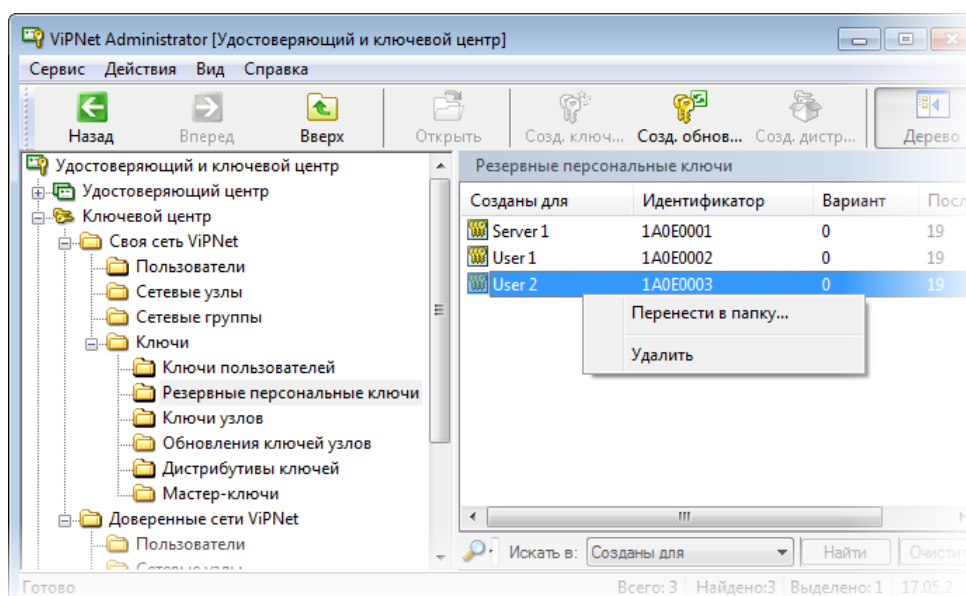


Рисунок 50: Возможные действия с резервными ключами

Для каждого РНПК отображается имя пользователя (колонка **Созданы для**), идентификатор, номер действующего персонального ключа (колонка **Вариант**) и номер последнего ключа в наборе (колонка **Последний ключ**).

С резервными персональными ключами можно производить следующие действия:

- Перенести в папку. Для переноса ключа (ключей) в папку выберите один или несколько ключей и воспользуйтесь пунктом контекстного меню **Перенести в папку**. Откроется окно **Перенос резервных наборов ПК**.

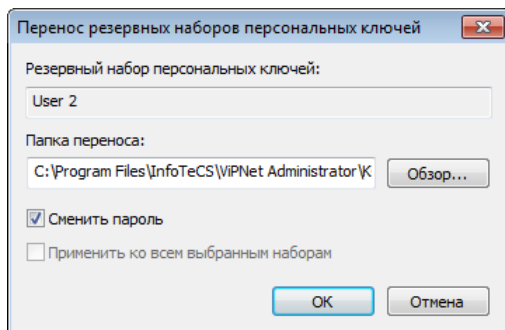


Рисунок 51: Перенос резервных ключей в папку

В данном окне нужно указать папку для переноса ключей, воспользовавшись кнопкой **Обзор**. Флажок **Сменить пароль** предназначен для смены пароля к резервным персональным ключам. Установив флажок, пароль можно сменить только на собственный (появится окно для ввода и подтверждения нового собственного пароля). Флажок **Применить ко всем выбранным наборам** предназначен для применения флажка **Сменить пароль** для всех выбранных наборов. После переноса в папку выбранные резервные наборы исчезнут из списка и появятся в заданной папке в подпапках с именами соответствующих пользователей (в виде файлов с расширением .pk).

- Удалить. Для удаления ключа (ключей) выберите один или несколько ключей и воспользуйтесь пунктом контекстного меню **Удалить**. Программа попросит подтверждения. При положительном ответе ключи будут удалены и исчезнут из списка. Удалять РНПК можно только в том случае, если есть уверенность, что этот набор хранится у пользователя.

Создание мастер-ключей

В каждой сети должны быть созданы три различных мастер-ключа своей сети:

- для создания ключей обмена коллективов (мастер-ключ ключей обмена);
- для создания ключей защиты ключей обмена (мастер-ключ ключей защиты);
- для создания персональных ключей для каждого пользователя (мастер-ключ персональных ключей).

Все эти три ключа формируются при первичной инициализации УКЦ (см. «[Проведение первичной инициализации программы](#)» на стр. 50). При необходимости их можно сменить (см. «[Смена мастер-ключей своей сети](#)» на стр. 119).

Для образования связей между коллективами двух разных сетей и СУ двух разных сетей используется межсетевой мастер-ключ для заданной пары сетей (см. «[Создание межсетевых мастер-ключей](#)» на стр. 120). Создание межсетевых мастер-ключей в настоящей системе возможно двумя способами:

- Мастер-ключ для взаимодействия двух сетей создается в одной из сетей и секретным образом передается в УКЦ другой сети (симметричный способ создания мастер-ключей).
- В каждом из УКЦ на базе своего закрытого и чужого открытого создается общий ключ. Этот способ называется асимметричной схемой создания межсетевых мастер-ключей.

Смена мастер-ключей своей сети

Для смены какого-либо мастер-ключа в папке **Ключевой центр > Своя сеть ViPNet > Ключи > Мастер-ключи** воспользуйтесь контекстным меню и выберите пункт **Сменить**, находясь на строке с названием мастер-ключа, который необходимо сменить. Программа выдаст окно с предупреждением. Для смены мастер-ключа, в окне с сообщением включите флажок опции **Сменить ключ Мастер-ключ обмена** (защиты или персональных ключей в зависимости от выбора) и нажмите кнопку **Продолжить**, которая после включения этого флажка станет активной. После нажатия на кнопку мастер-ключ будет сменен.

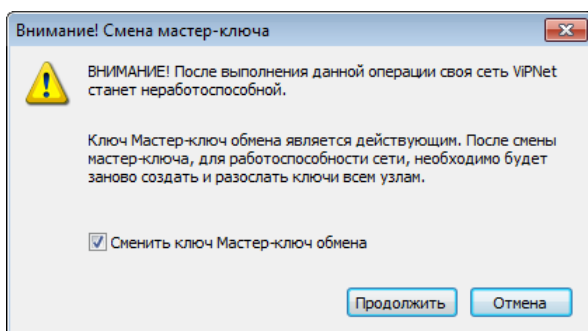



Рисунок 52: Предупреждение при смене мастер-ключей

Для смены всех трех мастер-ключей это действие необходимо повторить для каждого мастер-ключа.

 **Внимание!** Следует помнить, что после создания нового мастер-ключа, создаваемые ключи пользователей и узлов будут несовместимы с действующими ключами. Это означает, что все ключи пользователей и узлов, созданные на новом мастер-ключе будут несовместимы с созданными на предыдущем. Например, если после обновления ключей на абонентский пункт придут письма, зашифрованные на старых ключах, они не будут приняты. Поэтому операция по смене мастер-ключей своей сети применяется только при создании сети или плановой смене всех ключей пользователей и узлов.

Подробную информацию см. в разделе [Плановая смена мастер-ключей](#) (на стр. 76).

Создание межсетевых мастер-ключей

Если планируются связи своей сети с объектами доверенных сетей ViPNet, то необходимо наличие межсетевого мастер-ключа. Межсетевые мастер-ключи могут быть трех видов:

- Индивидуальный симметричный межсетевого мастер-ключ — ключ используется для создания классических ключей между объектами двух сетей (своей и конкретной чужой). Следует отметить, что данный ключ для каждой пары сетей должен быть один и тот же, следовательно, создаваться он должен только в одной сети, а в другую он должен быть каким-то образом передан, естественно, с исключением возможности доступа к нему посторонних лиц.
- Универсальный симметричный межсетевого мастер-ключ — ключ используется для создания классических ключей между объектами разных сетей, если нет индивидуального. Следует отметить, что данный ключ во всех сетях должен быть

один и тот же, следовательно, создаваться он должен только в одной сети, а в другие он должен быть каким-то образом передан, естественно, с исключением возможности доступа к нему посторонних лиц.

- Асимметричный межсетевой мастер-ключ — такой ключ используется при организации связи между двумя сетями как альтернативный классическому межсетевому мастер-ключу. Для каждой сети он свой. Закрытый асимметричный межсетевой мастер-ключ хранится в УКЦ своей сети, а соответствующий открытый асимметричный межсетевой мастер-ключ делается общедоступным и может быть использован в УКЦ любой доверенной сети для организации связи между двумя сетями. Следует отметить, чтобы асимметричный ключ использовался при создании ключевой информации, необходимо наличие закрытого асимметричного ключа своей сети и открытого асимметричного ключа доверенной сети. На их основе формируется общий ключ, имеющий ту же структуру, и используемый точно так же, как и симметричный межсетевой мастер-ключ.

Для связи двух сетей (или при плановой смене меж сетевого мастер-ключа) необходимо создать какой-либо один мастер-ключ и осуществить операции экспорта и (или) импорта мастер-ключа для обмена межсетевыми мастер-ключами по симметричной или асимметричной схеме, а также ввести этот ключ в действие (см. «[Изменение статуса меж сетевого мастер-ключа](#)» на стр. 127). Логика выбора меж сетевого мастер-ключа, при наличии нескольких введенных в действие ключей разного типа описана в разделе [Логика выбора меж сетевого мастер-ключа](#) (на стр. 123). Подробнее об экспорте и импорте см. далее в разделе [Экспорт и импорт меж сетевых мастер-ключей](#) (на стр. 124).

Межсетевые мастер-ключи создаются в папке **Ключевой центр > Доверенные сети ViPNet > Мастер-ключи > Текущие**.

Внимание! Следует помнить, что если создать новый меж сетевой мастер-ключ, то создаваемые ключи узлов для связи с доверенными сетями будут несовместимы с действующими ключами. Поэтому, такая операция используется только при:



- начальном установлении связи с доверенными сетями;
- компрометации универсального меж сетевого мастер-ключа;
- плановой согласованной смене универсального симметричного мастер-ключа во всех сетях, связанных со своей сетью.

Не рекомендуется создавать меж сетевые мастер-ключи без необходимости.

Для создания меж сетевого мастер-ключа используйте пункт **Создать** контекстного меню по правой кнопке мыши, даже, если это окно пусто. Откроется окно **Создание мастер-ключа для доверенных сетей ViPNet**.

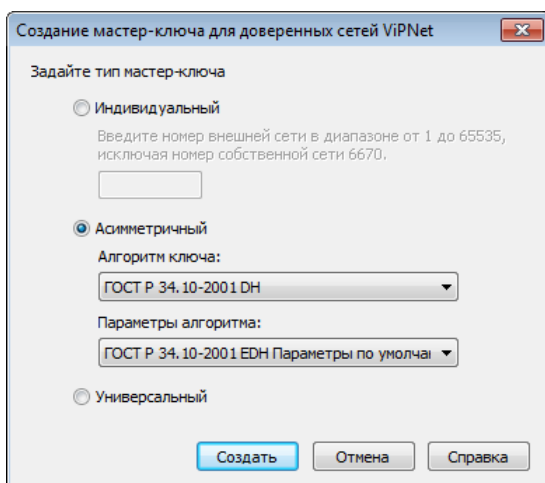


Рисунок 53: Создание мастер-ключа

В окне **Создание мастер-ключа для доверенных сетей ViPNet** выберите один из следующих типов ключей:

- **Индивидуальный** – введите номер другой (доверенной) сети (в пределах 0 – 65535) в поле для сети. Необходимо ввести номер той доверенной сети, для связи с которой создается межсетевой мастер-ключ.
- **Асимметричный** – выберите алгоритм ключа и параметры алгоритма.
- **Универсальный** – никаких дополнительных параметров настраивать не надо.

После выбора нажмите кнопку **Создать**. После нажатия кнопки откроется окно с предупреждением, соответствующим выбранному типу создаваемого мастер-ключа.

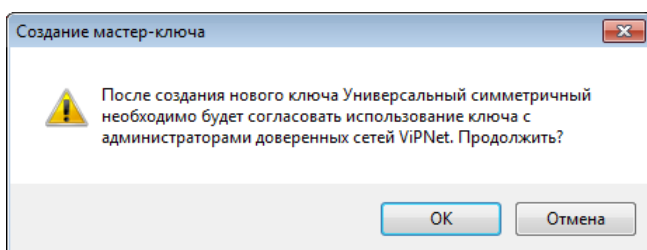


Рисунок 54: Предупреждение при создании мастер-ключа

Для создания ключа в данном окне нажмите **ОК**.

После создания мастер-ключа (индивидуального или универсального) его необходимо экспортировать (см. «[Экспорт межсетевых мастер-ключей](#)» на стр. 124) и передать

администраторам тех сетей, с которыми будет устанавливаться связь своей сети на данном ключе. Администратор другого УКЦ должен поместить этот мастер-ключ в подпапку `.\import` папки, где установлен УКЦ, и импортировать его (см. «[Импорт межсетевых мастер-ключей](#)» на стр. 126).

В случае асимметричного мастер-ключа помимо действий, описанных выше, администраторы доверенных сетей ViPNet также должны сформировать у себя асимметричные межсетевые мастер-ключи, экспортировать и передать их в свою сеть. При получении ключи необходимо импортировать.



Примечание. Экспортируется только открытая часть ключа.

Для того, чтобы межсетевой мастер-ключ использовался для формирования ключей после экспорта (импорта) необходимо ввести в действие (см. «[Изменение статуса межсетевого мастер-ключа](#)» на стр. 127).

Если была произведена плановая согласованная смена мастер-ключа, то обязательно прочитайте раздел [Плановая смена межсетевого мастер-ключа](#) (на стр. 77).

Внимание! Поскольку формат ключевой информации, начиная с версии 3.0, изменен (по сравнению с версией 2.8), то при организации процедуры обмена межсетевыми мастер-ключами с УКЦ версии 2.8 и ниже необходимо учитывать следующие особенности:



- Обмен асимметричными мастер-ключами с данными сетями невозможен.
- Импорт ключей, сформированных в версии 3.0 и выше, в УКЦ младших версий, невозможен.

Таким образом, для организации межсетевого взаимодействия с сетями версии 2.8 и ниже необходимо импортировать индивидуальный межсетевой мастер-ключ, созданный в версии 2.8, или использовать ключ, импортированный из баз данных УКЦ предыдущей версии.

Логика выбора межсетевого мастер-ключа

Если в УКЦ создано (или импортировано) и введено в действие несколько межсетевых мастер-ключей разного вида, то выбор мастер-ключа при формировании ключа между объектом данной сети (например, сеть с номером 1111 {0457 hex}) и объектом другой сети (например, сеть с номером 2222 {08AE hex}) происходит по логике, описанной ниже. Объектами могут являться коллективы или СУ.

Сначала программа ищет действующий индивидуальный мастер-ключ для данной сети. Если ключ найден, то он и будет использоваться при формировании ключей связи сетевых объектов.

При отсутствии индивидуального мастер-ключа программа ищет действующий закрытый асимметричный межсетевой мастер-ключ сети 1111 и открытый асимметричный межсетевой мастер-ключ сети 2222. Если они есть, то на их основе создается симметричный ключ, который и используется при формировании ключей связи сетевых объектов.

Если асимметричного межсетевого мастер-ключа тоже нет, то программа ищет действующий универсальный ключ, который и используется при формировании ключей связи сетевых объектов.

Если и универсального ключа нет, то выдается сообщение об ошибке.

Экспорт и импорт межсетевых мастер-ключей

Для обеспечения связи между сетями необходимо создать межсетевой мастер-ключ и экспортировать его в доверенные сети и (или) импортировать к себе созданные в доверенных сетях межсетевые мастер-ключи.

Экспорт межсетевых мастер-ключей

Если в своей сети был создан какой-либо из межсетевых мастер-ключей, его необходимо экспортировать в доверенные сети, с которыми связана своя сеть.

Для этого откройте папку **Ключевой центр > Доверенные сети ViPNet > Мастер-ключи > Текущие**.

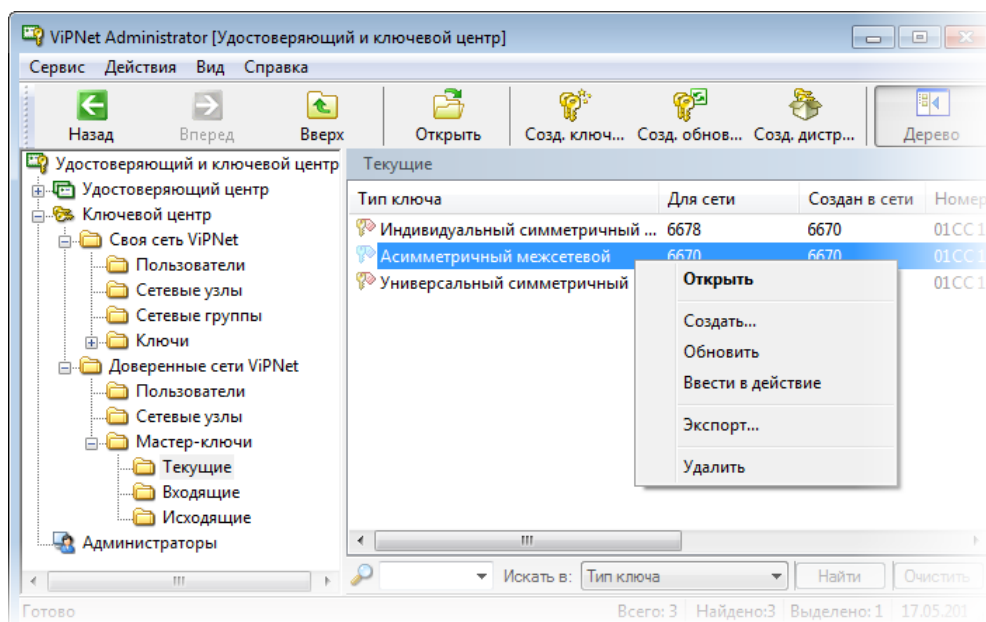


Рисунок 55: Экспорт межсетевого мастер-ключа

В этом окне представлен список межсетевых мастер-ключей из разных сетей и их номера. Для того чтобы экспортировать созданный в своей сети мастер-ключ, необходимо выбрать ключ для экспорта и воспользоваться либо контекстным меню, выбрав пункт **Экспорт**, либо выбрать одноименный пункт из меню **Действия**. После этого:

- Если межсетевой ключ симметричный, программа предложит задать пароль для экспорта мастер-ключа. Заданный пароль должен отличаться от пароля в УКЦ. Затем ключ будет помещен в папку `.\export` (файл `NNNN0000.key`, если ключ универсальный или `NNNNMMMM.key`, если ключ индивидуальный, где `NNNN` — номер своей сети, `MMMM` — номер доверенной сети). Необходимо запомнить пароль, заданный при экспорте межсетевого мастер-ключа, а затем каким-либо защищенным способом (вне программы УКЦ) передать его в другую сеть вместе с мастер-ключом из папки `.\export`.
- Если ключ асимметричный, то экспорт произойдет сразу — открытая часть ключа (файл `mst_NNNN.cer`, где `NNNN` — номер своей сети) будет помещена в папку `.\export`. После чего этот файл каким-либо защищенным способом (вне программы УКЦ) необходимо передать в другую сеть.

После экспорта межсетевой мастер-ключ необходимо ввести в действие (см. [«Изменение статуса межсетевого мастер-ключа»](#) на стр. 127).

После экспорта ключ также будет помещен в папку **Ключевой центр > Доверенные сети ViPNet > Мастер-ключи > Исходящие**.

Администратор другой сети должен поместить полученный файл с межсетевым мастер-ключом в подпапку `.\import` папки, где установлен УКЦ, и импортировать его (см. «Импорт межсетевых мастер-ключей» на стр. 126).

Импорт межсетевых мастер-ключей

Если в какой-то сети, имеющей связи со своей сетью, был создан и передан какой-либо из межсетевых мастер-ключей, то его необходимо импортировать. Для этого он должен быть помещен в папку `.\import`.

Для импорта откройте окно **Ключевой центр > Доверенные сети ViPNet > Мастер-ключи > Входящие**.

В этом окне представлен список межсетевых мастер-ключей, предназначенных для импорта, и их номера. Для того чтобы импортировать мастер-ключ, необходимо выбрать ключ для импорта и воспользоваться либо контекстным меню, выбрав пункт **Импорт**, либо выбрать одноименный пункт из меню **Действия**. При этом запросится пароль, на котором был зашифрован данный межсетевой ключ (если он симметричный). Этот пароль должен был быть передан из другой сети некоторым защищенным способом. Если мастер-ключ асимметричный, то будет произведена проверка подписи под данным ключом. Если подпись и сертификат администратора будут признаны действительными, то мастер-ключ будет импортирован. В связи с этим при одновременном импорте справочников сертификатов администраторов, списков отозванных сертификатов и мастер-ключей следует придерживаться следующего порядка импорта:

- Справочники сертификатов администраторов.
- Списки отозванных сертификатов.
- Асимметричный мастер-ключ.

Перед импортом мастер-ключа доверенной сети рекомендуется проверить целостность файла, в котором он содержится. Чтобы выполнить проверку:

- 1 В контекстном меню для данного межсетевого мастер-ключа выберите пункт **Проверить**.
- 2 В окне **Ввод пароля** введите пароль, на котором был зашифрован данный мастер-ключ.

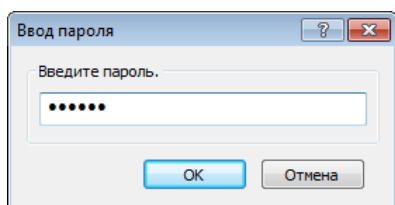


Рисунок 56: Ввод пароля при проверке мастер-ключа

При сохранении целостности файла мастер-ключа, появится сообщение об успешной проверке.

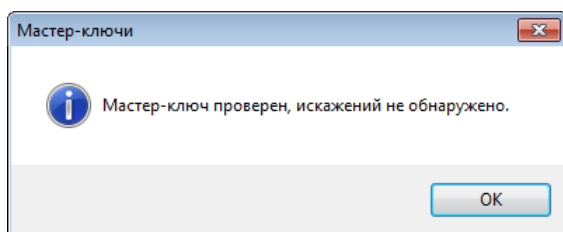


Рисунок 57: Сообщение об успешной проверке мастер-ключа доверенной сети ViPNet

После импорта межсетевой мастер-ключ необходимо ввести в действие (см. [«Изменение статуса межсетевого мастер-ключа»](#) на стр. 127).

После импорта ключ будет помещен в папку **Ключевой центр > Доверенные сети ViPNet > Мастер-ключи > Текущие**.



Внимание! Если была произведена плановая согласованная смена мастер-ключа, то необходимо также произвести обновления ключей узлов для всех СУ, связанных с доверенными сетями на этом ключе.

Изменение статуса межсетевого мастер-ключа

Для того чтобы мастер-ключ использовался при создании ключей связи сетевых объектов доверенных сетей, необходимо ввести его в действие. Для этого в папке **Ключевой центр > Доверенные сети ViPNet > Мастер-ключи > Текущие** выберите ключ, не введенный еще в действие (в колонке **Статус** должно быть либо **Экспортирован**, либо **Импортирован**) и воспользуйтесь контекстным меню, выбрав пункт **Ввести в действие**, мастер-ключ будет введен в действие (в колонке **Статус** появится значение **Действует**). Для данного ключа пункт контекстного меню поменяется на **Не использовать**. Если выбрать этот пункт, то программа запросит подтверждение на это изменение, и при положительном ответе, статус ключа изменится на предыдущий, а пункт контекстного меню **Не использовать** изменится на **Ввести в действие**.

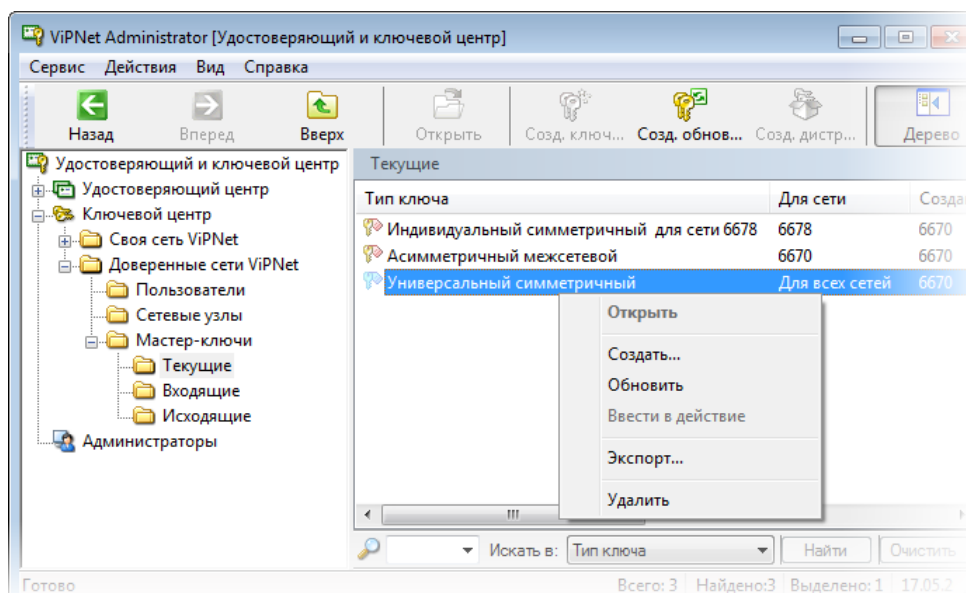


Рисунок 58: Ввод в действие межсетевого мастер-ключа

Для каждой сети в текущий момент может быть действующим единственный мастер-ключ каждого типа (один индивидуальный или один асимметричный). Так же может быть действующим только один универсальный мастер-ключ.

Логика выбора межсетевого мастер-ключа, при наличии нескольких введенных в действие ключей разного типа описана в разделе [Логика выбора межсетевого мастер-ключа](#) (на стр. 123).

Пароль администратора сетевых узлов

Администратор сетевых узлов ViPNet — лицо, ответственное за настройку и функционирование программного обеспечения ViPNet на компьютерах локальной сети (сетевых узлах). Администратор сетевых узлов ViPNet имеет специальный пароль для входа в ПО ViPNet на сетевых узлах для возможности производить дополнительные настройки ПО ViPNet.

Пароль администраторов сетевых узлов может создаваться для каждого узла, а также для групп сетевых узлов, заданных в программе ЦУС. При создании сети ViPNet в программе ЦУС автоматически создается группа **Вся сеть**, в которую входят все узлы сети ViPNet. Если других групп не задано, то в УКЦ будет отображаться только группа **Вся сеть**.

Пароль для администраторов группы **Вся сеть** называется общесетевым, для любой другой группы узлов — групповым, для одного узла — индивидуальным.

Пароль администраторов сетевых узлов для группы **Вся сеть** предлагается создать при первичном создании ключей для сетевых узлов. При отказе его можно создать позднее.



Внимание! Если не создавать пароли администраторов сетевых узлов, в этом случае будет невозможно получить доступ к дополнительным настройкам ПО ViPNet на сетевых узлах.

Для создания или смены пароля администраторов сетевых узлов выполните следующие действия в зависимости от типа пароля:

- Для создания или смены общесетевого или группового пароля администратора сетевых узлов выберите нужную группу в папке **Ключевой центр > Своя сеть ViPNet > Сетевые группы** и дважды щелкните на ней левой кнопкой мыши. Откроется окно **Свойства сетевой группы** (см. «[Просмотр свойств сетевой группы](#)» на стр. 139).
- Для создания или смены индивидуального пароля администратора сетевых узлов выберите нужный сетевой узел в папке **Ключевой центр > Своя сеть ViPNet > Сетевые узлы** и дважды щелкните на нем левой кнопкой мыши. Откроется окно **Свойства сетевого узла** (см. «[Просмотр свойств сетевого узла](#)» на стр. 136).

Перейдите на вкладку **Пароль администратора**. Если пароль не создан, то для создания пароля нажмите кнопку **Создать пароль**. Если пароль создан, то он будет отображаться на вкладке. Для смены пароля нажмите кнопку **Сменить пароль**.

Если созданы пароли разных типов, то администратору сетевых узлов необходимо сообщить тот пароль, который соответствует его уровню полномочий: общесетевой, групповой или индивидуальный.

После смены пароля администратора СУ следует сформировать обновления ключей (см. «Создание обновлений ключей узлов» на стр. 97) и выслать их на СУ. После обновления на сетевых узлах старый пароль администратора СУ того же типа станет недействительным.

В окне **Свойства сетевой группы** и **Свойства сетевого узла** на вкладке **Общие** можно посмотреть также подробную информацию о свойствах сетевых групп и сетевых узлов соответственно.

Сохранение паролей пользователей и администраторов сетевых узлов

В программе УКЦ можно сохранить пароли пользователей и пароли администраторов сетевых узлов в файл и (или) на произвольный носитель.

Для сохранения всех паролей пользователей в файле можно воспользоваться пунктом главного меню программы **Сервис > Сохранить пароли в файле > Пароли пользователей**. Кроме того, программой предусмотрено и индивидуальное сохранение пароля и (или) персональной информации для выбранного пользователя в файл или на внешнее устройство хранения данных. Для этого из папки **Ключевой центр > Своя сеть ViPNet > Пользователи** нужно выбрать пользователя, затем в контекстном меню выбрать пункт **Открыть**, далее из соответствующих вкладок открывшегося окна **Свойства пользователя** сохранить пароль и (или) персональную информацию (см. [Просмотр свойств пользователя](#) (на стр. 133)).

Для сохранения всех паролей администраторов сетевых узлов или групп сетевых узлов в файле можно воспользоваться, соответственно, пунктами главного меню программы **Сервис > Сохранить пароли в файле > Пароли администраторов сетевых узлов** или **Сервис > Сохранить пароли в файле > Пароли администраторов сетевых групп**.

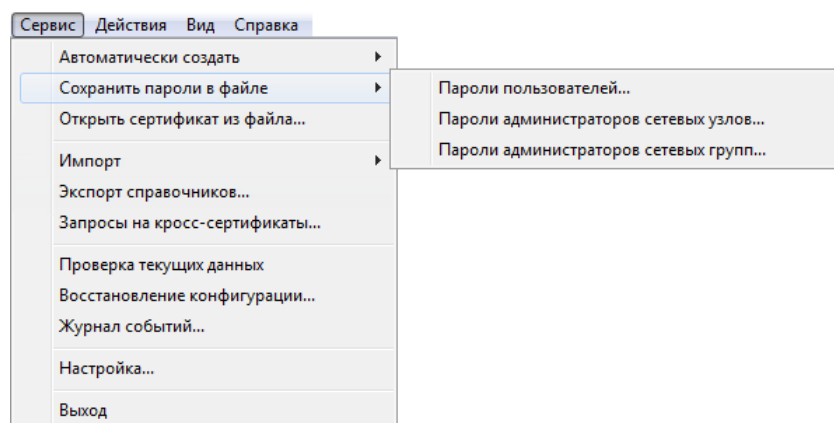


Рисунок 59: Пункт меню «Сохранить пароли в файле»

Смена паролей пользователей ViPNet

Смена паролей пользователей в УКЦ носит рекомендательный характер, то есть после смены пароля пользователя в УКЦ и отправки обновления на сетевой узел, у пользователя сетевого узла появится предупреждение о необходимости сменить пароль. После чего пользователь должен сменить свой пароль самостоятельно.

Для того чтобы инициировать процедуру смены пароля пользователей на сетевых узлах в УКЦ необходимо сформировать ключи пользователей, а именно выполнить следующие действия:

- 1 Из ЦУС скопировать в УКЦ справочники связей для пользователей, которым рекомендовано сменить пароль.
- 2 В УКЦ создать новые ключи пользователей (см. [«Создание ключей пользователей»](#) на стр. 100). При этом будет задан вопрос о желании сменить пароль. Для смены пароля ответьте положительно.
- 3 Из ЦУС отправить созданные ключи на сетевые узлы, пользователям которых был изменен пароль.

Если обновление пройдет успешно, то на сетевом узле появится предупреждение о том, что в соответствии с политиками безопасности сети ViPNet пароль недействителен, и его необходимо сменить. Пользователь сможет сменить пароль прямо из окна с предупреждением. Новый пароль будет сформирован в соответствии с параметрами, заданными в настройках параметров безопасности на сетевом узле.



Внимание! После смены пароля пользователя на сетевом узле будет произведена попытка перешифровать на новом пароле имеющийся файл резервного набора персональных ключей (файл с расширением *.pk) (см. [«Действия с резервными персональными ключами»](#) на стр. 117). Если файл не будет найден, и если в будущем произойдет компрометация ключей пользователя, то не удастся дистанционно выслать ему новые ключи. В этом случае для пользователя придется сформировать новый ключевой дистрибутив.

Просмотр свойств пользователя

Окно **Свойства пользователя** открывается выбором пункта контекстного меню **Открыть** для выбранного пользователя в папке **Ключевой центр > Своя сеть ViPNet > Пользователи**.

Окно имеет 3 вкладки:

- **Общие** – содержит следующую информацию о пользователе: имя пользователя, идентификатор (из ЦУС), вариант используемого ключа и список сетевых узлов, на которых зарегистрирован пользователь. На вкладке также имеются 2 кнопки: **Печать** (для печати персональной информации о пользователе, которая включает в себя содержание вкладки), **Сохранить в файле** (для сохранения информации в файле).

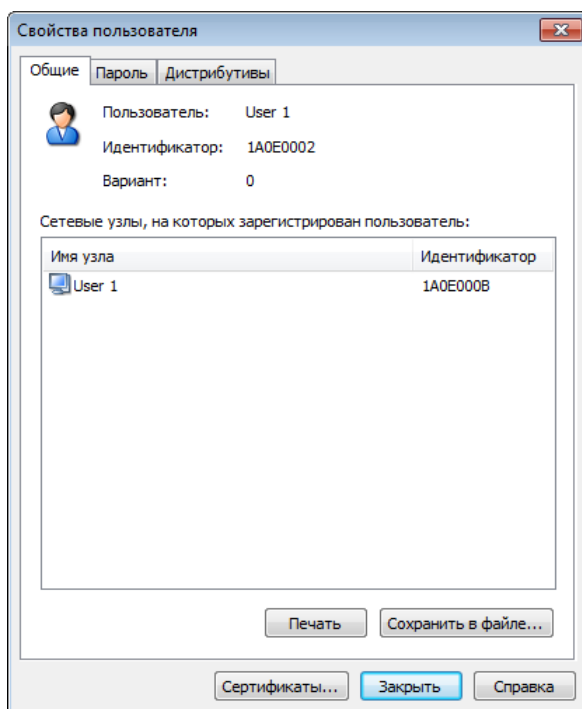


Рисунок 60: Общие свойства пользователя сети ViPNet

- **Пароль** – если созданы ключи пользователя, то на вкладке отображается пароль, который можно сохранить в файле или на внешнем устройстве хранения данных (кнопка **Сохранить в файле**). Если пароля нет, то можно создать ключи пользователя.

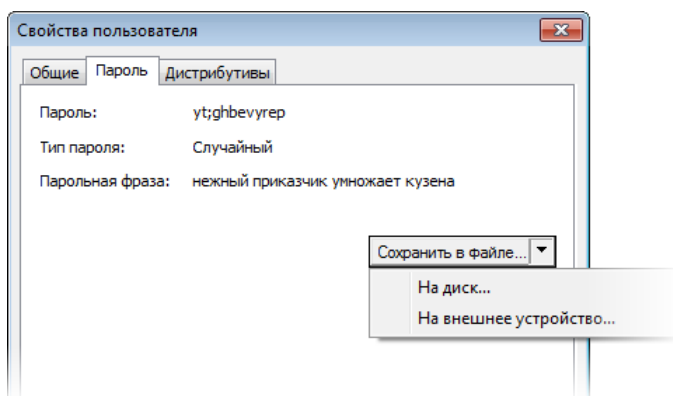


Рисунок 61: Пароль пользователя

- **Дистрибутивы** – отображается имя файлов дистрибутивов и список сетевых узлов, для которых созданы дистрибутивы. Внизу вкладки имеются 4 кнопки: **Выделить все** (выделяются все элементы списка), **Распаковать**, **Перенести** (выбранные дистрибутивы будут соответственно распакованы или перенесены в папку или на устройство, при этом откроется окно **Перенос дистрибутивов ключей**), **Удалить** (выбранные дистрибутивы будут удалены).

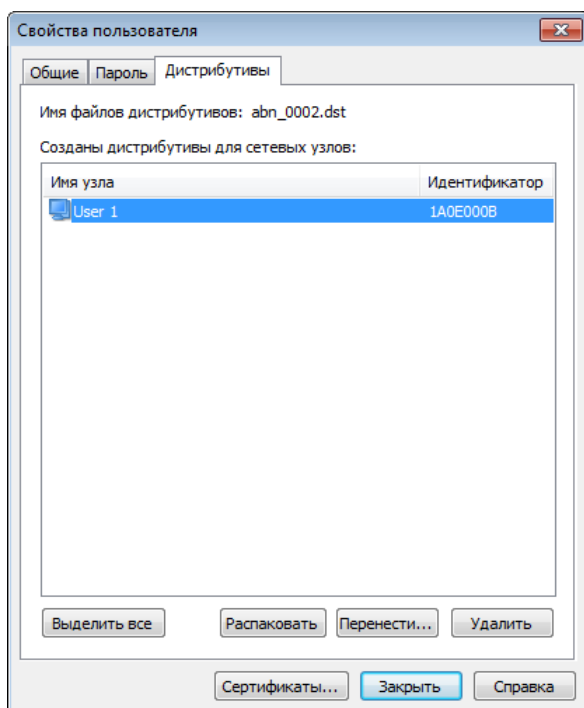


Рисунок 62: Созданные дистрибутивы для сетевого узла пользователя

В нижней части окна расположены следующие кнопки:

- **Сертификаты** – для просмотра сертификатов пользователя. При отсутствии сертификатов у пользователя, окно со списком сертификатов не вызывается и выдается сообщение, что сертификатов не обнаружено. Кнопка может отсутствовать при наличии лицензионных ограничений на работу УКЦ в части Удостоверяющего центра.
- **Заккрыть** – чтобы закрыть данное окно.
- **Справка** – для получения справки.

Просмотр свойств сетевого узла

В программе УКЦ можно посмотреть информацию о сетевых узлах своей сети. Для этого в папке **Ключевой центр** > **Своя сеть ViPNet** > **Сетевые узлы** выберите необходимый узел и воспользуйтесь пунктом **Открыть** контекстного меню.

Откроется окно **Свойства сетевого узла**.

Окно содержит 3 вкладки:

- **Общие** – содержит следующую информацию об узле: имя, идентификатор (из ЦУС), вариант используемого ключа и список пользователей, зарегистрированных в коллективах данного узла.

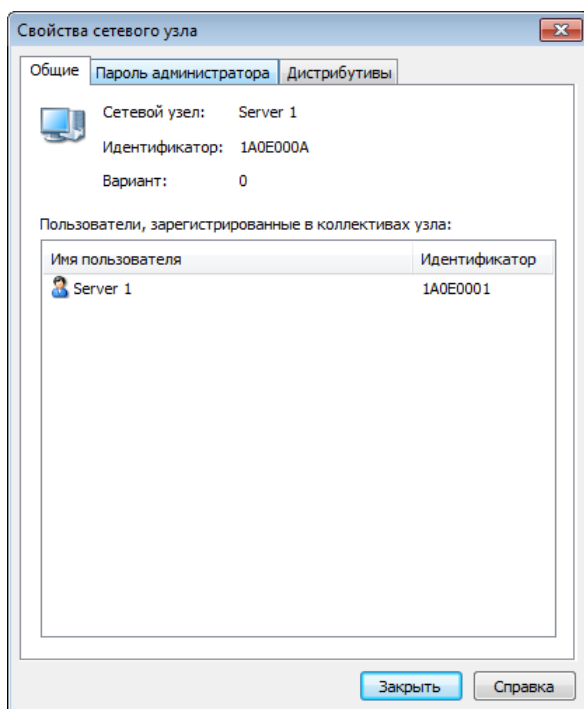


Рисунок 63: Общие свойства сетевого узла

- **Пароль администратора** (сетевого узла) – на вкладке отображается пароль, если вы его создали, также можно его сменить. Если пароля нет, то можно его создать.

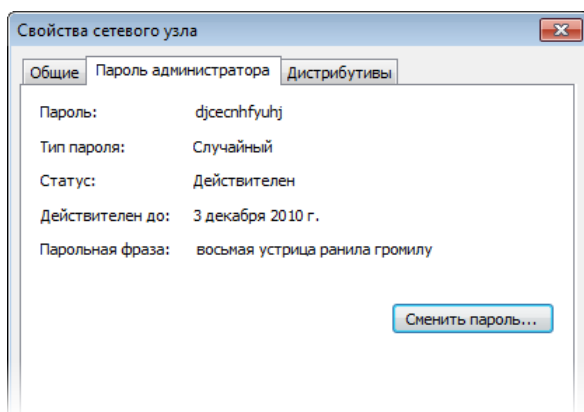


Рисунок 64: Пароль администратора сетевого узла

- **Дистрибутивы** – эта вкладка отображается только в случае наличия созданных и необработанных дистрибутивов ключей. Отображается путь к файлу дистрибутивов и список пользователей, для которых созданы дистрибутивы. На вкладке имеется 4 кнопки: **Выделить все** (выделяются все элементы списка), **Распаковать**, **Перенести** (выбранные дистрибутивы будут соответственно распакованы или перенесены в папку или на устройство, при этом откроется окно **Перенос дистрибутивов ключей**), **Удалить** (выбранные дистрибутивы будут удалены).

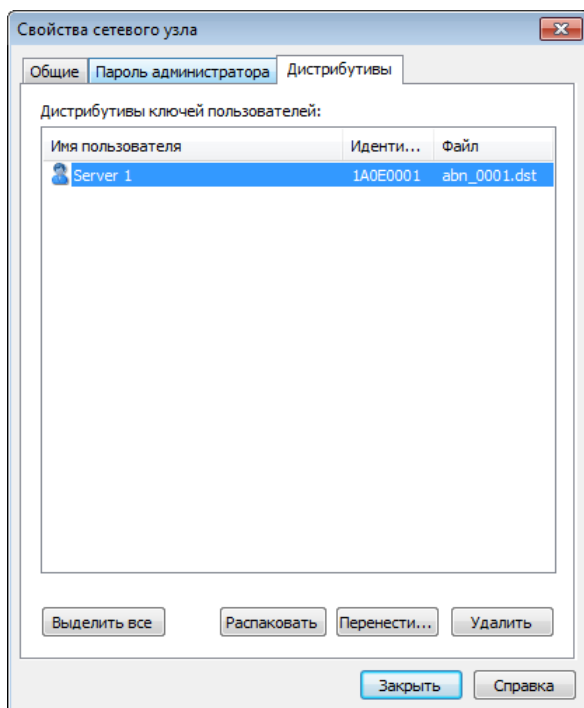


Рисунок 65: Дистрибутивы ключей пользователя сетевого узла

В нижней части окна расположены кнопка **Закрыть** и кнопка **Справка**, чтобы закрыть окно или получить справку соответственно.

Просмотр свойств сетевой группы

В программе УКЦ можно посмотреть информацию о сетевой группе узлов своей сети. Для этого в папке **Ключевой центр** > **Своя сеть ViPNet** > **Сетевые группы** выберите необходимую группу (в том числе можно выбрать и группу **Вся сеть**) и воспользуйтесь пунктом **Открыть** контекстного меню. Откроется окно **Свойства сетевой группы**.

Окно имеет 2 вкладки:

- **Общие** – содержит следующую информацию о сетевой группе: имя, идентификатор (из ЦУС), список сетевых узлов, на которых зарегистрирована группа.

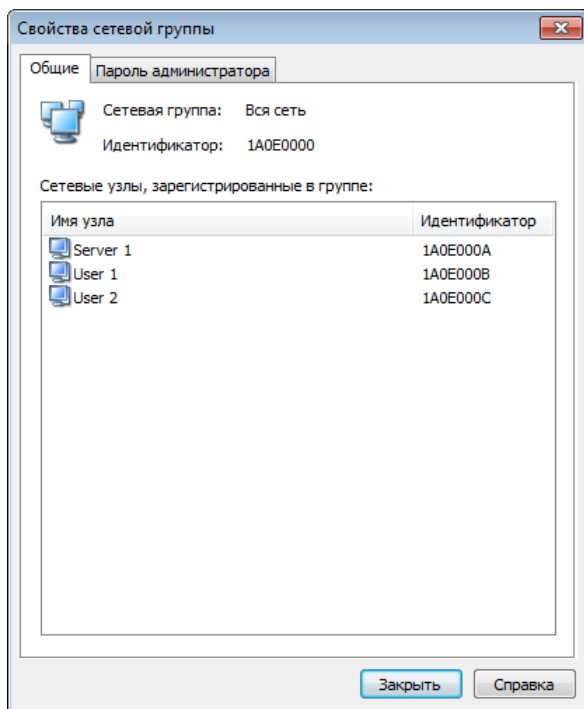


Рисунок 66: Общие свойства сетевой группы

- **Пароль администратора** (сетевой группы) – на вкладке отображается пароль (аналогично сетевому узлу), если он создан, то его можно сменить. Если пароля нет, то его можно создать (аналогично сетевому узлу).

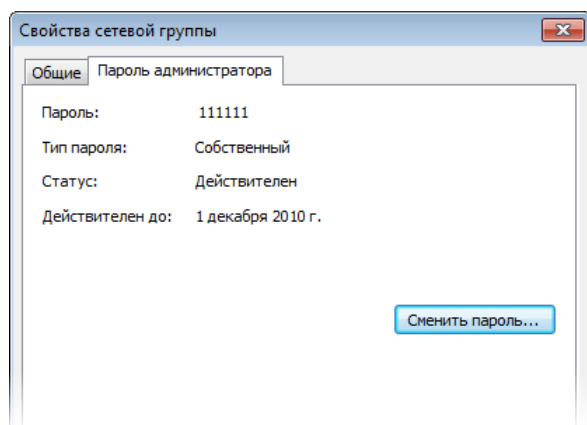


Рисунок 67: Пароль администратора сетевой группы

В нижней части окна расположены кнопка **Закреть** и кнопка **Справка**, чтобы закрыть окно или получить справку соответственно.



5

Управление сертификатами в части Удостоверяющего центра

Издание сертификатов	143
Отзыв сертификатов, приостановление действия сертификатов, возобновление действия сертификатов	157
Импорт сертификатов администраторов доверенных сетей ViPNet	162
Импорт списков отозванных сертификатов доверенных сетей ViPNet	165
Обновление списка отозванных сертификатов своей сети	167
Обработка запросов на кросс-сертификаты (в том числе запросов на сертификаты из подчиненных УЦ)	169
Просмотр запросов и сертификатов	180
Экспорт сертификатов	188
Проверка сертификатов	192

Издание сертификатов

Первое издание сертификата для пользователей своей сети ViPNet происходит в УКЦ во время первого создания ключей пользователя, имеющего право подписи (это право определяется в ЦУС). Ключи пользователя формируются при создании дистрибутива для начальной инсталляции (см. «[Создание дистрибутивов ключей](#)» на стр. 91). Также ключи пользователя можно сформировать отдельно от создания дистрибутива ключей (см. [Создание ключей пользователей](#) (на стр. 100)).

Дальнейшее переиздание сертификата может происходить в УКЦ, как при формировании ключей пользователя (см. «[Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ](#)» на стр. 149), так и по запросу пользователя, сформированному на СУ (см. «[Издание \(отклонение\) сертификатов по запросам, поступившим с СУ пользователей сети ViPNet](#)» на стр. 149).

Запросы на сертификаты из ViPNet Registration Point могут поступать для зарегистрированных внешних пользователей и для пользователей сети ViPNet (см. [Издание \(отклонение\) сертификатов по запросам, поступившим из ViPNet Registration Point](#) (на стр. 152)).

Издание сертификатов производится на основе шаблонов, создаваемых в окне **Настройка > Сертификаты > Шаблоны сертификатов**. В комплекте поставки имеется несколько шаблонов. О том, как создать, или изменить шаблон см. в разделе [Создание и редактирование шаблонов сертификатов](#) (на стр. 256).

Если в настройках задано, что во время издания сертификата он не будет отображаться для редактирования (см. «[Настройка параметров издания сертификатов и обработки запросов](#)» на стр. 250), то:

- При издании сертификатов во время создания ключей пользователя или дистрибутивов используется шаблон, выбранный по умолчанию (устанавливается в настройках (см. «[Создание и редактирование шаблонов сертификатов](#)» на стр. 256)).
- При издании сертификатов по запросам используются параметры сертификата, заданные в запросе.

Если в настройках задано, что во время издания сертификата он будет отображаться для редактирования, то редактирование сертификата производится в мастере редактирования полей сертификата (см. «[Мастер редактирования полей сертификата](#)» на стр. 144).

Мастер редактирования полей сертификата

Как было отмечено выше, мастер редактирования полей сертификата запускается в процессе издания сертификата в том случае, если в настройках программы установлена соответствующая опция (см. «[Настройка параметров издания сертификатов и обработки запросов](#)» на стр. 250). Перед запуском мастера появляется сообщение с вопросом о необходимости редактирования полей сертификата. При положительном ответе открывается первая страница мастера редактирования полей сертификата. При отказе от редактирования сертификат издается без участия мастера.



Примечание. При издании сертификата учитываются параметры шаблона, выбранного в настройках по умолчанию. Некоторые параметры из шаблона заимствуются полностью и без возможности изменения (поскольку не отображаются в мастере редактирования полей сертификата). К ним относится алгоритм и параметры открытого ключа. В связи с этим перед изданием сертификата убедитесь, что назначен нужный шаблон по умолчанию (см. раздел [Создание и редактирование шаблонов сертификатов](#) (на стр. 256)).

При издании квалифицированного сертификата (см. «[Квалифицированный сертификат](#)») используйте соответствующий шаблон «Квалифицированный сертификат».

При запуске мастера редактирования полей сертификата выполните в нем следующие действия:

- 1 На странице **Сведения о владельце сертификата** укажите имя и другие необходимые данные о владельце сертификата и нажмите кнопку **Далее**.

Имя:	Михайлова Антонина Петровна
Должность:	Бухгалтер
Подразделение:	Бухгалтерия
Организация:	ООО «Ветка»
ИНН:	7452052871
ОГРН:	8754215725566
СНИПС:	02324423703

Рисунок 68: Заполнение основных сведений о владельце сертификата

- 2 Если требуется, на следующей странице мастера, укажите такие данные владельца, как город, страна, адрес и так далее. Затем нажмите кнопку **Далее**.

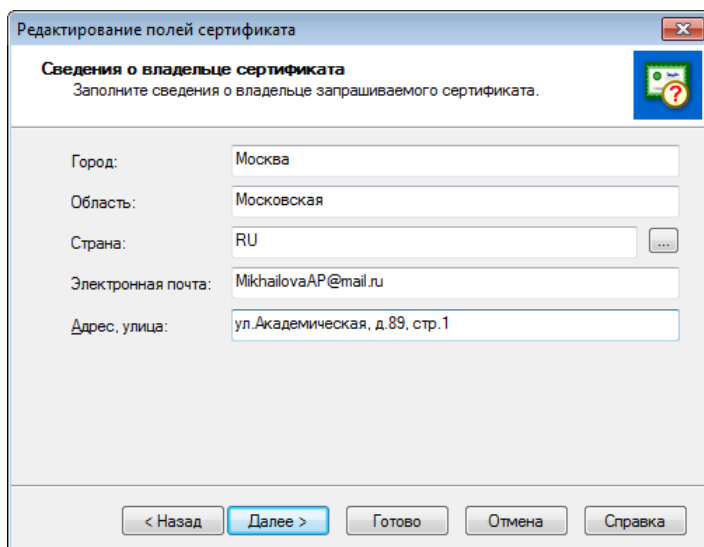



Рисунок 69: Заполнение сведений об адресе владельца сертификата



Совет. В поле **Страна** следует указать страну с помощью кнопки  или вручную ввести ее код в соответствии с ISO 3166. В поле **Электронная почта** рекомендуется указывать только правильный адрес электронной почты владельца сертификата.

- 3 На следующей странице мастера с помощью кнопки **Изменить** отредактируйте дополнительные сведения о владельце и нажмите кнопку **Далее**.

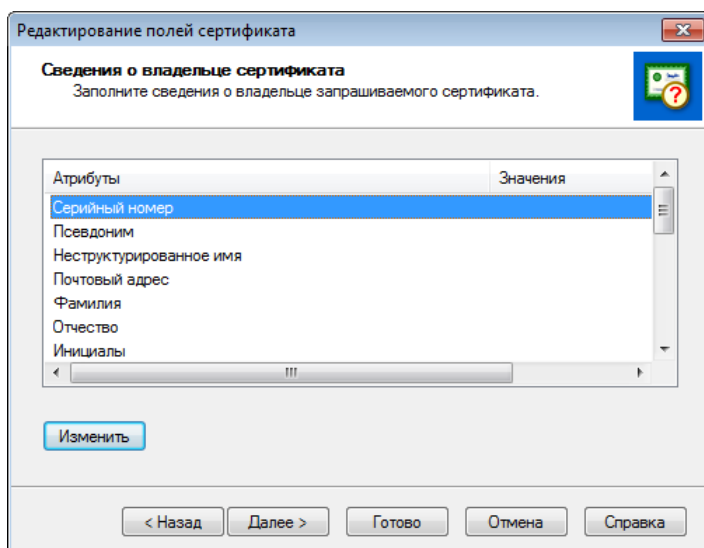


Рисунок 70: Заполнение дополнительных сведений о владельце сертификата

- 4 При необходимости на странице **Выбор шаблона сертификата** измените шаблон, в соответствии с которым будет производиться издание сертификата. Шаблон, отмеченный в списке значком ✓, является шаблоном по умолчанию.

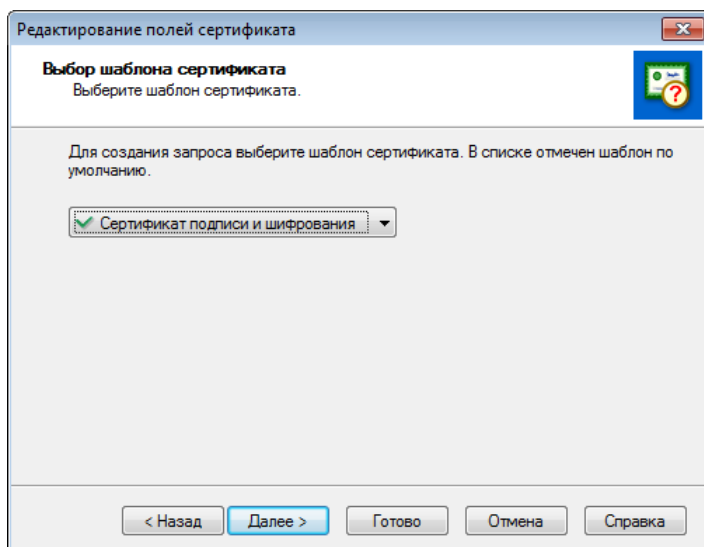


Рисунок 71: Выбор шаблона сертификата

- 5 На странице **Срок действия сертификата** задайте желаемый срок действия издаваемого сертификата любым удобным способом, после чего нажмите кнопку **Далее**.

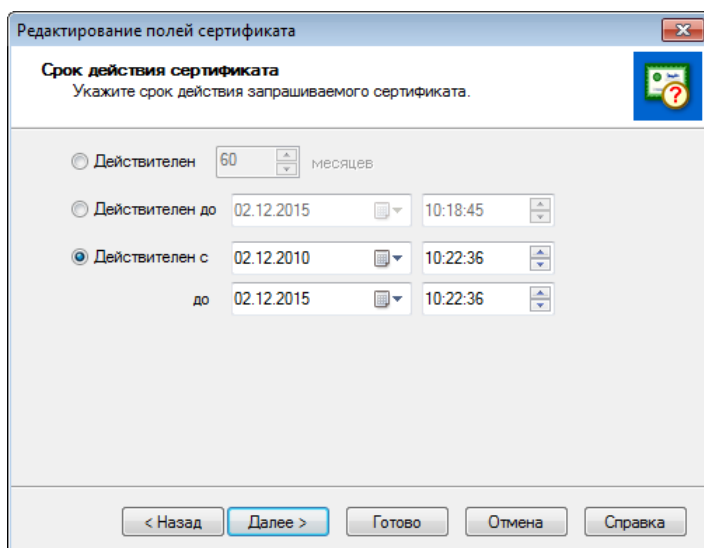


Рисунок 72: Указание желаемого срока действия сертификата



Примечание. При задании срока действия сертификата автоматически определяется срок действия закрытого ключа. Если срок действия сертификата задается меньше или равным 12 месяцам (1 году), то срок действия закрытого ключа будет равен заданному сроку действия сертификата. Если заданный срок действия сертификата больше 1 года, то срок действия закрытого ключа устанавливается равным 1 году. Только в этом случае при издании сертификата будет указан срок действия закрытого ключа (1 год). Максимальный срок действия сертификата пользователя составляет 5 лет.

- 6 На страница **Назначение сертификата** при необходимости добавьте расширения и политики применения сертификата, а также задайте атрибуты, содержащие наименование средства электронной подписи издателя, наименование средства электронной подписи владельца, дополнительное имя владельца.



Примечание. На странице **Назначения сертификата** присутствуют расширения, политики применения и атрибуты, которые заданы в используемом шаблоне сертификата. См. раздел [Создание и редактирование шаблонов сертификатов](#) (на стр. 256).

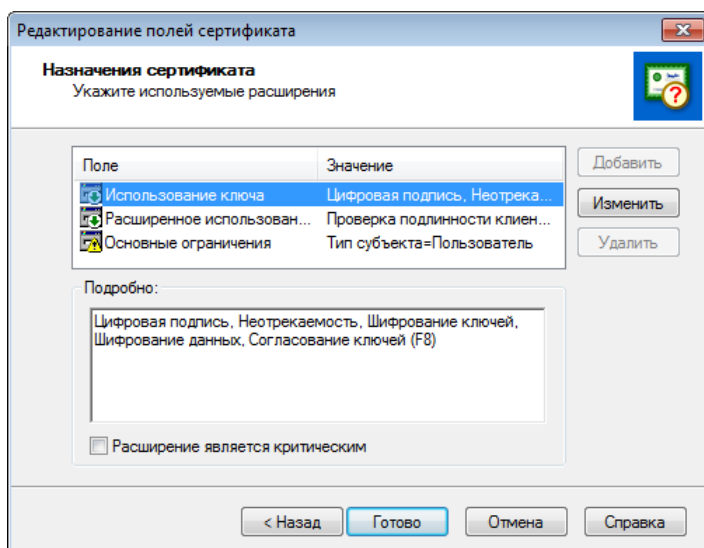


Рисунок 73: Формирование назначений сертификата

- По завершении задания параметров издаваемого сертификата нажмите кнопку **Готово**.

Запустится процесс издания сертификата, в результате которого будет сформирован сертификат открытого ключа подписи пользователя.

Если срок действия, заданный для издаваемого сертификата, будет превышать срок действия сертификата текущего администратора УКЦ, то в процессе издания появится соответствующее сообщение. В окне с сообщением нажмите **ОК**.

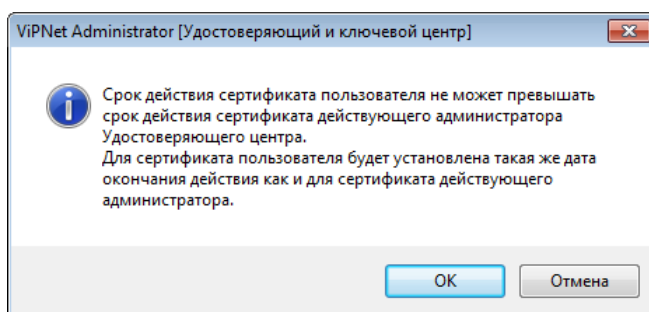


Рисунок 74: Сообщение о превышении срока действия издаваемого сертификата

В данном случае будет издан сертификат, срок действия которого будет таким же как и у сертификата текущего администратора УКЦ.

Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ

Администратор может по своей инициативе переиздать сертификаты каких-либо пользователей сети ViPNet, для этого необходимо выполнить следующие действия:

- 1 В ЦУС скопировать файлы связей для таких пользователей.
- 2 В УКЦ при индивидуальном формировании ключей создать ключи пользователей (см. «Создание ключей пользователей» на стр. 100), при этом будут обновлены сертификаты пользователей.
- 3 В ЦУС отправить обновления ключей пользователей на СУ, пользователям которых переиздали сертификаты.

Издание (отклонение) сертификатов по запросам, поступившим с СУ пользователей сети ViPNet

Когда срок действия сертификата пользователя заканчивается, или пользователь по каким-либо причинам хочет завести себе новый сертификат, этот пользователь может на своем СУ создать запрос на новый сертификат и отправить его в ЦУС. ЦУС передаст этот запрос в УКЦ.

Запрос на сертификат представляет собой шаблон сертификата, содержащий информацию о пользователе, его новый открытый ключ подписи, предполагаемый срок действия сертификата, а также некоторые дополнительные параметры, соответствующие стандарту X.509.

Когда в УКЦ от какого-либо пользователя поступает запрос на сертификат, необходимо принять решение по этому запросу — удовлетворить запрос и издать сертификат, либо отклонить запрос. Если принято решение издать сертификат, то на основании распечатки запроса на сертификат, заверенной рукописной подписью пользователя, удовлетворяется запрос и издается сертификат для данного пользователя. При этом сертификат также регистрируется в справочнике действующих сертификатов пользователей сети. Изданный сертификат будет выслан пользователю на СУ. Когда пользователь получит его и введет в действие, он сможет производить подпись документов, используя свой новый сертификат. Если принято решение не издавать сертификат, то запрос отклоняется (не подписывается администратором).

Удовлетворение запроса и издание сертификата произойдет только в том случае, если пользователь, приславший запрос, в ЦУС имеет право подписи и подпись действительна. В противном случае запрос будет предложено удалить (в случае отсутствия права подписи в ЦУС), либо отклонить (в случае недействительности подписи).

При поступлении запроса на сертификат может быть два варианта обработки запроса – ручной и автоматический, в зависимости от настроек в окне **Настройки > Сертификаты** (см. «[Настройка параметров издания сертификатов и обработки запросов](#)» на стр. 250). По умолчанию, после установки УКЦ, запросы на сертификат, подписанные пользователем, обрабатываются в ручном режиме. Отклонить запросы можно только в ручном режиме. Если подпись запроса недействительна, то такие запросы обрабатываются только в ручном режиме.

Примечание. Создание запросов на сертификаты по истечении срока действия закрытого ключа:



- Если на момент создания запроса на сертификат срок действия закрытого ключа истек, то программа сообщает пользователю, что его запрос не будет подписан, и в этом случае пользователь должен будет подтвердить корректность запроса администратору согласно регламенту, принятому в УКЦ.
- Несмотря на это сообщение, запрос будет подписан с использованием того же закрытого ключа, для которого формируется запрос. Однако эта подпись используется не для подтверждения авторства, а только для проверки целостности запроса. При просмотре свойств таких запросов на сертификаты указывается признак **Не подписан**.
- Издание таких сертификатов (с признаком **Не подписан**) возможно только в ручном режиме обработки запроса (см. ниже).

Обработка запроса на сертификат вручную происходит в случае, если в окне **Настройки > Сертификаты** в группе **Автоматически удовлетворять запросы** снят флажок **На сертификаты, подписанные пользователем**.

При поступлении нового запроса на сертификат на экране появится сообщение об этом. Нажмите **ОК**. Обработать запросы можно в папке **Удостоверяющий центр > Запросы на сертификаты > Входящие > Своя сеть ViPNet**.

Для удовлетворения запроса и издания сертификата выберите строку с запросом (можно выделить несколько запросов) и воспользоваться либо контекстным меню, выбрав пункт **Удовлетворить**, либо выбрать пункт **Удовлетворить запрос** из главного меню **Действия**.

Если пользователь имеет право подписи и подпись действительна, то программа предложит отредактировать издаваемый сертификат. При согласии откроется мастер **Редактирование полей сертификата** (см. «[Мастер редактирования полей сертификата](#)» на стр. 144), в котором просматриваются, подтверждаются (на основании распечатки запроса на сертификат, заверенной рукописной подписью пользователя) и при необходимости редактируются данные о пользователе, срок действия сертификата и открытый ключ подписи.

По завершении редактирования и нажатия кнопки **Готово** в мастере **Редактирование полей сертификата** для данного пользователя издается сертификат. При нажатии кнопки **Отмена** в мастере **Редактирование полей сертификата** операция издания сертификата отменяется.

Если срок действия издаваемого сертификата в запросе превышает срок действия сертификата текущего администратора УКЦ, то будет выдано сообщение об установке точно такого же срока действия издаваемого сертификата, как у текущего администратора УКЦ. Для создания сертификата нажмите **ОК** в окне с сообщением.



Примечание. В случае группы редактируемых сертификатов их окна появляются последовательно (после нажатия кнопки **Готово**). Если в каком-либо окне редактирования сертификата нажата кнопка **Отмена**, то издание обрабатываемого сертификата, а также еще необработанных сертификатов отменяется.

При отказе от предложения отредактировать сертификат, он издается без редактирования.

После издания сертификата пользователю будет выслан новый сертификат.

Администратор может отказать в сертификации. Для этого на строке с запросом (можно выделить несколько запросов) нужно воспользоваться либо контекстным меню, выбрав пункт **Отклонить**, либо выбрать пункт **Отклонить запрос** из главного меню **Действия**. После подтверждения желания отклонить запрос или запросы, запросы будут отклонены. При этом файл с запросом отправляется в исходном виде на СУ, где отсутствие подписи администратора интерпретируется как отказ в сертификации. Отклоненные запросы переместятся в папку **Удостоверяющий центр > Запросы на сертификаты > Отклоненные > Своя сеть ViPNet**.

Автоматическая обработка запроса на сертификат происходит в случае, если в окне **Настройки > Сертификаты** (см. «[Настройка параметров издания сертификатов и обработки запросов](#)» на стр. 250) в группе **Автоматически удовлетворять запросы** установлен флажок **На сертификаты, подписанные пользователем**.

В этом случае при поступлении нового запроса на сертификат, запрос будет автоматически удовлетворен и издан сертификат, если в ЦУС пользователь имеет право подписи и подпись действительна.



Внимание! Если срок действия издаваемого сертификата в запросе превышает срок действия сертификата текущего администратора УКЦ, то для издаваемого сертификата будет установлен срок действия, как у текущего администратора УКЦ.

Изданный сертификат будет помещен в общий список сертификатов пользователей своей сети — в папку **Удостоверяющий центр > Сертификаты пользователей > Своя сеть ViPNet**, где можно просмотреть (см. [«Просмотр сертификатов»](#) на стр. 182), отозвать сертификат, приостановить действие сертификата или возобновить действие приостановленного ранее сертификата (см. [Отзыв сертификатов, приостановление действия сертификатов, возобновление действия сертификатов](#) (на стр. 157)).

Удовлетворенный запрос переместится в папку **Удостоверяющий центр > Запросы на сертификаты > Удовлетворенные > Своя сеть ViPNet**, где его можно в любой момент просмотреть (см. [Просмотр запросов на сертификаты пользователей](#) (на стр. 180)).

Издание (отклонение) сертификатов по запросам, поступившим из ViPNet Registration Point

Запросы на сертификаты из ViPNet Registration Point могут поступать для зарегистрированных внешних пользователей и для пользователей сети ViPNet.

При поступлении запроса на сертификат может быть два варианта обработки запроса — ручной и автоматический, в зависимости от настроек в окне **Настройки > Сертификаты** (см. [«Настройка параметров издания сертификатов и обработки запросов»](#) на стр. 250).

По умолчанию, после установки УКЦ, запросы на сертификат, подписанные пользователем ViPNet Registration Point, обрабатываются в автоматическом режиме.

Отклонить запросы можно только в ручном режиме. Если подпись запроса недействительна, то такие запросы обрабатываются только в ручном режиме.

Если действие сертификата пользователя было приостановлено в УКЦ, но обновление еще не отправлено, то при поступлении из ViPNet Registration Point запросов на сертификаты каких-либо пользователей, произвести их обработку можно только в ручном режиме. В такой ситуации можно только отклонить запросы, поскольку сертификаты пользователей считаются недействительными. При попытке удовлетворить запрос появится сообщение о том, что сертификат неверный и предложение отклонить запрос.

Автоматическая обработка запроса на сертификат происходит в случае, если в окне **Настройки > Сертификаты** в группе **Автоматически удовлетворять запросы** установлен флажок **На сертификаты, подписанные в Центрах регистрации**.

В этом случае при поступлении нового запроса на сертификат, запрос будет автоматически удовлетворен и издан сертификат, если в ЦУС пользователь имеет право подписи и подпись действительна.



Внимание! Если срок действия издаваемого сертификата в запросе превышает срок действия сертификата текущего администратора УКЦ, то для издаваемого сертификата будет установлен срок действия, как у текущего администратора УКЦ.

Обработка запроса на сертификат вручную происходит в случае, если в окне **Настройки > Сертификаты** в группе **Автоматически удовлетворять запросы** снят флажок **На сертификаты, подписанные в Центрах регистрации**.

При поступлении нового запроса на сертификат на экране появится сообщение об этом. Нажмите **ОК**. Обработать запросы для пользователей ViPNet можно в папке **Удостоверяющий центр > Запросы на сертификаты > Входящие > Своя сеть ViPNet**.

Обработать запросы для внешних пользователей можно в папке **Удостоверяющий центр > Запросы на сертификаты > Входящие > Внешние пользователи**.

Для удовлетворения запроса и издания сертификата нужно выбрать строку с запросом (можно выделить несколько запросов) и воспользоваться либо контекстным меню, выбрав пункт **Удовлетворить**, либо выбрать пункт **Удовлетворить запрос** из главного меню **Действия**.

Если пользователь имеет право подписи и подпись действительна, то программа предложит отредактировать издаваемый сертификат. При согласии откроется мастер **Редактирование полей сертификата** (см. «[Мастер редактирования полей сертификата](#)» на стр. 144), в котором просматриваются, подтверждаются (на основании распечатки запроса на сертификат, заверенной рукописной подписью пользователя) и при необходимости редактируются данные о пользователе, срок действия сертификата и открытый ключ подписи.

По завершении редактирования и нажатия кнопки **Готово** в мастере **Редактирование полей сертификата** для данного пользователя издается сертификат. При нажатии кнопки **Отмена** операция издания сертификата отменяется.

Если срок действия издаваемого сертификата в запросе превышает срок действия сертификата текущего администратора УКЦ, то будет выдано сообщение об установке точно такого же срока действия издаваемого сертификата, как у текущего администратора УКЦ. Для создания сертификата нажмите **ОК** в окне с сообщением.



Примечание. В случае группы редактируемых сертификатов их окна появляются последовательно (после нажатия кнопки **Готово**). Если в каком-либо окне редактирования сертификата нажата кнопка **Отмена**, то издание обрабатываемого сертификата, а также еще необработанных сертификатов отменяется.

При отказе от предложения отредактировать сертификат, он издается без редактирования.

После издания сертификата пользователю будет выслан новый сертификат.

Администратор может отказать в сертификации. Для этого на строке с запросом (можно выделить несколько запросов) нужно воспользоваться либо контекстным меню, выбрав пункт **Отклонить**, либо выбрать пункт **Отклонить запрос** из главного меню **Действия**. После подтверждения желая отклонить запрос или запросы, запросы будут отклонены. При этом файл с запросом отправляется в исходном виде на СУ, где отсутствие подписи администратора интерпретируется как отказ в сертификации. Отклоненные запросы для пользователей ViPNet переместятся в папку **Удостоверяющий центр > Запросы на сертификаты > Отклоненные > Своя сеть ViPNet**. Отклоненные запросы для внешних пользователей переместятся в папку **Удостоверяющий центр > Запросы на сертификаты > Отклоненные > Внешние пользователи**.

Изданный сертификат для пользователя сети ViPNet будет помещен в общий список сертификатов пользователей своей сети — в папку **Удостоверяющий центр > Сертификаты пользователей > Своя сеть ViPNet**. Изданный сертификат для внешнего пользователя будет помещен в общий список сертификатов внешних пользователей — в папку **Удостоверяющий центр > Сертификаты пользователей > Внешние пользователи**. В этих папках можно просмотреть (см. [«Просмотр сертификатов»](#) на стр. 182), отозвать сертификат, приостановить действие сертификата или возобновить действие приостановленного ранее сертификата (см. [Отзыв сертификатов, приостановление действия сертификатов, возобновление действия сертификатов](#) (на стр. 157)).

Удовлетворенный запрос для пользователя сети ViPNet переместится в папку **Удостоверяющий центр > Запросы на сертификаты > Удовлетворенные > Своя сеть ViPNet**, где его можно в любой момент просмотреть, а для внешнего пользователя — в папку **Удостоверяющий центр > Запросы на сертификаты > Удовлетворенные > Внешние пользователи** (см. [Просмотр запросов на сертификат пользователей](#) (см. [«Просмотр запросов на сертификаты пользователей»](#) на стр. 180)).

Издание (отклонение) сертификатов по запросам от внешних пользователей



Внимание! Возможность создания сертификата пользователя по запросу из файла доступна в программе ViPNet Administrator Удостоверяющий и ключевой центр (УКЦ) версии 3.2.2 и выше.

Запросы на издание сертификата открытого ключа могут поступать от внешних пользователей в виде файла запроса. Файл запроса на сертификат передается в одном из двух форматов:

- PKCS #10 (файл с расширением *.p10) — широко распространенный формат запросов на сертификат, поддерживаемый большинством удостоверяющих центров. Подробнее см. на странице PKCS #10 веб-узла RSA Labs <http://www.rsa.com/rsalabs/node.asp?id=2132>.
- CMC (файл с расширением *.cmc) — менее распространенный формат запросов на сертификат. Подробнее см. на странице CMC веб-узла Википедия http://en.wikipedia.org/wiki/Certificate_Management_over_CMS.

Для издания сертификатов по запросам от внешних пользователей:

- 1 В меню **Сервис** выберите пункт **Запросы из файла**, затем **Сертификаты пользователей**.
- 2 В окне выбора файла запроса выделите нужные файлы запросов с расширением *.p10 или *.cmc и нажмите кнопку **Открыть**.
- 3 В окне **Запросы на сертификаты пользователей**, если необходимо, просмотрите параметры переданных запросов. Для этого выберите нужный запрос и нажмите кнопку **Свойства запроса**.
- 4 Для того, чтобы выполнить издание сертификата, выберите нужные запросы и нажмите кнопку **Издать сертификат**.
- 5 В окне вопроса о редактировании издаваемых сертификатов нажмите кнопку **Да**, чтобы иметь возможность изменить параметры нового сертификата, или кнопку **Нет**, если эти изменения не требуются.
- 6 При необходимости, измените параметры сертификата в окне **Редактирование полей сертификата**. По окончании изменений нажмите кнопку **Готово**.
Выполните данное действие для всех издаваемых сертификатов.
- 7 В окне сообщения об успешном издании сертификатов нажмите кнопку **ОК**.

После издания сертификатов сохраните файлы сертификатов на диске и передайте их пользователям. Для этого:

- 1 В разделе **Удостоверяющий центр** выберите **Сертификаты пользователей** и далее **Внешние пользователи**.

- 2 Выберите нужный сертификат и в контекстном меню нажмите пункт **Экспорт**.
- 3 На страницах мастера экспорта сертификата укажите формат экспорта и расположение файла сертификата.
- 4 Выполните экспорт сертификатов для всех пользователей, после чего передайте пользователям изданные файлы сертификатов.



Примечание. Если предполагается, что несколько сертификатов будут использоваться на одном компьютере (например, чтобы пользователь имел возможность проверять ЭЦП и выполнять шифрование писем электронной почты для других пользователей, или когда для одного пользователя было издано несколько сертификатов), можно экспортировать несколько сертификатов в один файл формата PKCS #7. Для этого выберите сертификаты нужных пользователей и в контекстном меню нажмите пункт **Экспорт**, после чего укажите место расположение файла сертификатов. Все выбранные сертификаты будут помещены в один файл с расширением *.p7b.

Отзыв сертификатов, приостановление действия сертификатов, возобновление действия сертификатов

В некоторых случаях может возникнуть необходимость отзыва или приостановления действия сертификата пользователя, например, при утере клиентом своего ключевого носителя.

Отзыв, приостановление действия, возобновления действия сертификата пользователя может происходить как [по запросу из ViPNet Registration Point](#) (на стр. 157) для пользователей (сети ViPNet и внешних), зарегистрированных в центре регистрации, так и [по инициативе администратора УКЦ](#) (на стр. 159).



Примечание. Возобновить действие можно только приостановленного сертификата.

Иногда также может возникнуть необходимость отзыва изданных кросс-сертификатов администраторов других УЦ.

По запросу из ViPNet Registration Point

Запрос (на отзыв, приостановление действия, возобновление действия сертификата) из ViPNet Registration Point может поступить только для сертификатов зарегистрированных пользователей (сети ViPNet и внешних).

Удовлетворение запроса произойдет только в том случае, если пользователь, приславший запрос, в ЦУС имеет право подписи и подпись действительна. В противном случае запрос будет предложено удалить (в случае отсутствия права подписи в ЦУС) либо отклонить (в случае недействительности подписи).

При поступлении запроса может быть два варианта обработки запроса — ручной и автоматический, в зависимости от настроек в окне **Настройки > Сертификаты** (см. [«Настройка параметров издания сертификатов и обработки запросов»](#) на стр. 250). По

умолчанию, после установки УКЦ, запросы обрабатываются в автоматическом режиме. Отклонить запросы можно только в ручном режиме.

Автоматическая обработка запросов (на отзыв, приостановление действия, возобновление действия сертификата) происходит в случае, если в окне **Настройки > Сертификаты** в группе **Автоматически удовлетворять запросы** установлен флажок **На отзыв сертификатов**.

В этом случае при поступлении нового запроса, запрос будет автоматически удовлетворен, если в ЦУС пользователь ViPNet Registration Point имеет право подписи и подпись действительна.

Обработка запроса вручную происходит в случае, если в окне **Настройки > Сертификаты** в группе **Автоматически удовлетворять запросы** снят флажок **На отзыв сертификатов**.

При поступлении нового запроса на экране появится сообщение об этом. Нажмите **ОК**. Обработать запросы можно в папке **Удостоверяющий центр > Запросы на отзыв сертификатов > Входящие**.

Для удовлетворения запроса нужно выбрать строку с запросом и воспользоваться либо контекстным меню, выбрав пункт **Удовлетворить**, либо выбрать пункт **Удовлетворить запрос** из главного меню **Действия**.

Если пользователь ViPNet Registration Point имеет право подписи и подпись действительна, то после подтверждения желаяния удовлетворить запрос откроется окно **Список отзыва сертификатов (Certificate Revocation List)**, в котором просматривается и подтверждается список отзыва, и, если все верно, то нажимается кнопка **ОК**, запрос будет удовлетворен.

Удовлетворенный запрос будет перемещен в папку **Удостоверяющий центр > Запросы на отзыв сертификатов > Удовлетворенные**.

Для отклонения запроса на строке с запросом нужно воспользоваться либо контекстным меню, выбрав пункт **Отклонить**, либо выбрать пункт **Отклонить запрос** из главного меню **Действия**. После подтверждения желаяния отклонить запрос, запрос будет отклонен. При этом файл с запросом отправляется в исходном виде на СУ, где отсутствие подписи администратора интерпретируется как отказ в сертификации. Отклоненные запросы переместятся в папку **Удостоверяющий центр > Запросы на отзыв сертификатов > Отклоненные**.

Отозванные и приостановленные сертификаты попадут в папку **Удостоверяющий центр > Списки отозванных сертификатов > Своя сеть ViPNet** в список отозванных сертификатов (см. «[Просмотр списков отзыва сертификатов](#)» на стр. 185) под именем издателя соответствующего списка отзыва (пользователя ViPNet Registration Point или

администратора УКЦ). А после возобновления действия приостановленного сертификата, он исчезнет из списка отозванных сертификатов для своего издателя.

После отзыва, приостановления или возобновления действия сертификата изменится и информация на вкладке **Общие** окна **Сертификат** (см. «[Просмотр сертификатов](#)» на стр. 182) для данного пользователя, открывающегося для пользователя ViPNet из папки **Удостоверяющий центр > Сертификаты пользователей > Своя сеть ViPNet**, для внешнего пользователя из папки **Удостоверяющий центр > Сертификаты пользователей > Внешние пользователи**.

Измененные СОС должны быть отправлены на СУ.

Если в настройках программы в окне **Списки отозванных сертификатов** (см. «[Настройка параметров работы со списками отозванных сертификатов](#)» на стр. 264) включена опция **Копировать в ЦУС при наличии изменений каждые**, то СОС в случае их изменения отправятся в ЦУС автоматически, и далее будут отправлены на те СУ, для которых это настроено в ЦУС. Для всех остальных СУ или, если вышеописанная опция выключена, необходимо создать ключи узлов (см. «[Создание ключей узлов](#)» на стр. 95) в индивидуальном режиме. Далее ключи узлов передаются в ЦУС для рассылки и автоматического обновления ключей на СУ.

По инициативе администратора УКЦ

Администратор УКЦ может отзывать, приостанавливать действие или возобновлять приостановленное действие сертификатов пользователей сети ViPNet или внешних пользователей, а также отзывать изданные кросс-сертификаты администраторов других УЦ, в случае, если он является их издателем. В противном случае, выполнение данных операций будет невозможно, о чем сообщит окно с предупреждением.

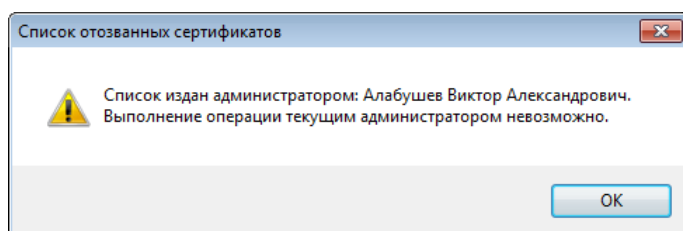


Рисунок 75: Сообщение о невозможности выполнения операции текущим администратором

Для выполнения данных операций с сертификатами:

- 1 В разделе **Удостоверяющий центр** главного окна программы выберите:
 - Подраздел **Сертификаты пользователей > Своя сеть ViPNet** для действий с сертификатами пользователей сети ViPNet.

- Подраздел **Сертификаты пользователей** > **Внешние пользователи** для действий с сертификатами внешних пользователей.
 - Подраздел **Сертификаты администраторов** > **Кросс-сертификаты** > **Изданные** для действий с изданными кросс-сертификатами администраторов других УЦ.
- 2 Для указанного сертификата в меню **Действия** или в контекстном меню выберите:
- пункт **Отозвать** для отзыва сертификата пользователя или кросс-сертификата.
 - пункт **Приостановить** для приостановления действия сертификата пользователя.
 - пункт **Возобновить** для возобновления действия ранее приостановленного сертификата пользователя.



Примечание. Возобновить действие сертификата пользователя можно только, если его действие было ранее приостановлено. Для отозванного сертификата возобновить его действие нельзя.

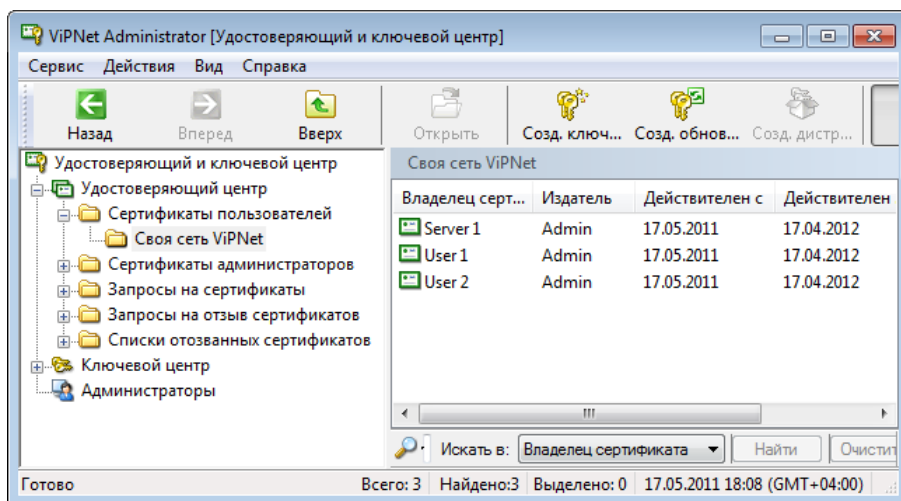


Рисунок 76: Возможные действия с сертификатами пользователей

- 3 После отзыва или приостановления действия сертификата в колонке **Статус** для данного сертификата появится соответствующее значение. В окне **Сертификат** на вкладке **Общие** (см. «[Просмотр сертификатов](#)» на стр. 182) также изменится информация.

Отозванные и приостановленные в действии сертификаты попадут в подраздел **Удостоверяющий центр** > **Списки отозванных сертификатов** > **Своя сеть ViPNet** в

список отозванных сертификатов (см. «[Просмотр списков отзыва сертификатов](#)» на стр. 185) издателя соответствующего списка отзыва:

- Пользователя ViPNet Registration Point для внешних пользователей.
- Администратора УКЦ для пользователей ViPNet и администраторов других УЦ.

При возобновлении действия приостановленного сертификата пользователя, он исчезнет из списка отозванных сертификатов для своего издателя.

Измененные СОС должны быть отправлены на СУ. Если в настройках программы включена опция **Автоматически копировать список в ЦУС каждые**, то СОС отправятся в ЦУС автоматически, и далее будут отправлены на те СУ, для которых это настроено в ЦУС (см. раздел [Настройка параметров работы со списками отозванных сертификатов](#) (на стр. 264)). Для всех остальных СУ или, если вышеописанная опция выключена, следует создать обновление ключей (см. «[Создание обновлений ключей узлов](#)» на стр. 97) в индивидуальном режиме. Далее ключи узлов передаются в ЦУС для рассылки и автоматического обновления ключей на СУ.

Импорт сертификатов администраторов доверенных сетей ViPNet

Сертификаты администраторов доверенных сетей ViPNet используются для проверки сертификатов пользователей доверенных сетей ViPNet, приславших подписанную информацию на какой-либо СУ своей сети. Сертификаты администраторов доверенных сетей должны быть заверены (подписаны) администратором своей сети. Для этого их нужно импортировать.

Если в папке для УКЦ из ЦУС есть файлы-сертификаты администраторов доверенных сетей ViPNet, то появится сообщение о поступлении справочников сертификатов администраторов из доверенной сети ViPNet с информацией, где их можно обработать.

Сертификаты администраторов из доверенных сетей ViPNet отобразятся в папке **Удостоверяющий центр > Сертификаты администраторов > Доверенные сети ViPNet > Входящие**. Для импорта выберите эту папку, а далее строку с нужным сертификатом и воспользуйтесь контекстным меню **Импорт**. На экране появится окно со списком всех имеющихся справочников сертификатов.

Примечание. Если файлы-сертификаты администраторов других сетей были переданы вручную (не средствами ПО ViPNet), то для импорта выполните следующие действия:



- В главном меню программы выберите **Сервис > Импорт > Сертификатов администраторов других сетей**.
 - Укажите папку, где лежит справочник сертификатов администраторов другой сети.
 - В окне **Импорт сертификатов администраторов других сетей** для выбранного сертификата нажмите кнопку **Импорт сертификата**.
-

В левой части окна отображены номера сети и имена администраторов этих сетей, сертификаты которых, необходимо импортировать. В правой части отображен список всех сертификатов каждого администратора.

Можно настроить фильтр просмотра списка сертификатов, выбрав в списке **Показывать** необходимый тип сертификатов:

- **Все сертификаты** — для отображения всех сертификатов.
- **Новые сертификаты** — для отображения только новых сертификатов.
- **Действующие сертификаты** — для отображения только действующих сертификатов.

Для того чтобы импортировать сертификаты администраторов доверенных сетей ViPNet, необходимо просмотреть, проверить и подтвердить сертификаты для каждого администратора (сертификат для каждого администратора в бумажном виде должен быть передан из доверенных сетей ViPNet некоторым защищенным способом). Для проверки и подтверждения действительности сертификата необходимо в левой части окна **Импорт сертификатов администраторов других сетей** выбрать администратора, а затем в правой части какой-либо из сертификатов (или все сертификаты) и нажать кнопку **Сертификат** или дважды щелкнуть на выбранном сертификате. Откроется окно **Сертификат**.

Сертификаты, предназначенные для импорта не являются действительными, поскольку они еще не находятся в системном хранилище сертификатов УКЦ. В связи с этим, при просмотре и проверке этих сертификатов на вкладке **Путь сертификации** отображается ошибка проверки **Нет доверия к этому корневому сертификату центра сертификации**. Данное сообщение не является препятствием для импорта сертификата. При отсутствии других ошибок и совпадении содержимого полей сертификата с имеющейся распечаткой, сертификат может быть импортирован. После завершения процедуры регистрации он становится «доверенным» и действительным сертификатом.

Кроме этого, при первом импорте сертификатов из некоторой сети, УКЦ не располагает списками отозванных сертификатов (СОС) из данной сети. (Регистрация СОС возможна только в том случае, если сертификат ключа подписи администратора, заверившего данный СОС, успешно импортирован.) В этом случае при просмотре сертификатов администраторов на вкладке **Путь сертификации** отображается ошибка проверки сертификата **Не удалось проверить этот сертификат, поскольку не получен правильный список отзыва сертификатов от центра сертификации, выпустившего этот сертификат**. При первом импорте сертификатов данная ситуация не является препятствием для регистрации справочника. Если аналогичное сообщение возникает при повторном импорте (после регистрации хотя бы одного СОС из данной сети), необходимо обратиться к администратору данной сети для получения правильных СОС и справочников сертификатов администраторов.

Появление других ошибок и сообщений свидетельствует о нарушении целостности принимаемого сертификата, и его импорт недопустим.

Если все условия выполнены, то нажмите кнопку **ОК** (для данного администратора данный сертификат проверен). Все описанные действия производятся для всех сертификатов из окна **Импорт сертификатов администраторов других сетей**. После того, как произойдет сверка всех поступивших сертификатов администраторов из доверенных сетей ViPNet, можно произвести импорт этих сертификатов. Выберите их и нажмите кнопку **Импорт сертификатов**.

Если сертификаты администраторов доверенных сетей ViPNet были переданы в виде файлов *.p7*, то импортировать их нужно с помощью пункта главного меню **Сервис > Импорт > Сертификатов администраторов доверенных сетей**.

После импорта сертификатов администраторов доверенных сетей появится сообщение о необходимости сформировать обновление ключей для сетевых узлов. При согласии с предложением запустится автоматическое формирование обновлений ключей для всех СУ, связанных с сетью, откуда пришли сертификаты администраторов. При отказе следует произвести создание обновлений ключей самостоятельно (см. [«Создание обновлений ключей узлов»](#) на стр. 97).

Сформированные ключи узлов появятся в окне **Ключевой центр > Своя сеть ViPNet > Ключи > Ключи узлов**, откуда их необходимо перенести в ЦУС для отправки обновлений на СУ (см. [Действия с ключами узлов и обновлениями ключей для СУ](#) (на стр. 111)).

Импортированные сертификаты будут помещены в папку **Удостоверяющий центр > Сертификаты администраторов > Доверенные сети ViPNet > Текущие**, где их можно просмотреть (см. [«Просмотр сертификатов»](#) на стр. 182).

Импорт списков отозванных сертификатов доверенных сетей ViPNet

Импорт списков отозванных сертификатов пользователей доверенных сетей ViPNet необходим, так как на основании информации из этих списков, на СУ выполняется следующая проверка: если поступило сообщение с подписью, присутствующей в этом списке, и дата подписи более поздняя, чем дата отзыва сертификата, то сообщение признается недействительным. Импорт обязателен даже в том случае, если СОС пустые, то есть пользователи в сети ни разу не удалялись.

При приходе новых СОС доверенных сетей осуществляется автоматический импорт данных списков. Если СОС доверенных сетей ViPNet были переданы в виде файлов *.p7s, то импортировать их нужно с помощью пункта главного меню **Сервис > Импорт > Списков отозванных сертификатов**.

Импорт списка отозванных сертификатов пользователей доверенной сети не требуется и не будет выполнен в том случае, если ранее уже был импортирован список с таким же номером и более поздней датой издания. Об этом уведомит соответствующее сообщение.

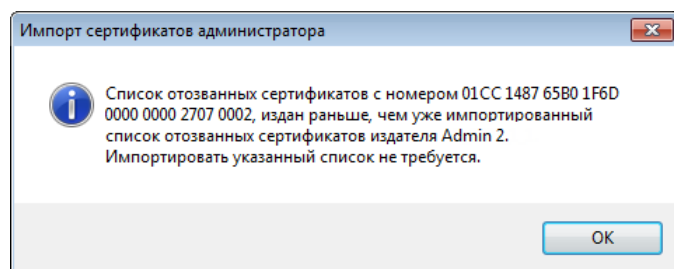


Рисунок 77: Сообщение о невозможности импорта списка отозванных сертификатов

При успешном импорте СОС появится сообщение о необходимости сформировать обновление ключей узлов. При согласии запустится автоматическое формирование обновлений ключей тех узлов, которые связаны с сетью, откуда пришли СОС.



Примечание. Ключи узлов будут формироваться только в том случае, если для этой сети не создавался кросс-сертификат. В противном случае ключи узлов формироваться не будут.

При отказе следует произвести создание обновлений ключей самостоятельно (см. [«Создание обновлений ключей узлов»](#) на стр. 97).

Сформированные ключи узлов появятся в папке **Ключевой центр > Своя сеть ViPNet > Ключи > Ключи узлов**, откуда их необходимо перенести в ЦУС для отправки обновлений на СУ (см. [Действия с ключами узлов и обновлениями ключей для СУ](#) (на стр. 111)).

Импортированные СОС попадут в папку **Удостоверяющий центр > Списки отозванных сертификатов > Доверенные сети ViPNet** в список для своей сети (см. [Просмотр списков отзыва сертификатов](#) (на стр. 185)).

Обновление списка отозванных сертификатов своей сети

Список отзыва сертификатов создается при издании корневого сертификата администратора, а затем автоматически обновляется при отзыве или приостановлении действия сертификатов пользователей.

СОС своей сети хранятся в папке **Удостоверяющий центр > Списки отозванных сертификатов > Своя сеть ViPNet** под именем издателей списков отзыва – администраторов сети ViPNet (см. [Просмотр списков отзыва сертификатов](#) (на стр. 185)).

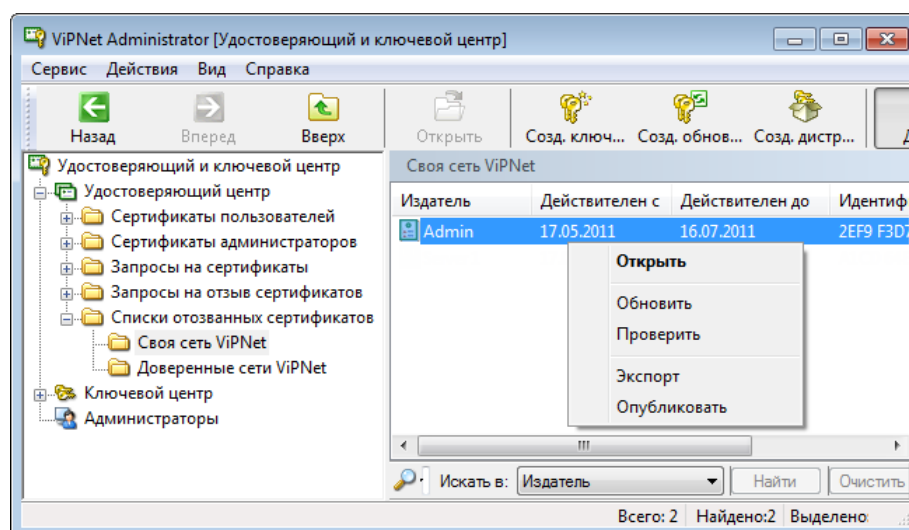


Рисунок 78: Возможные действия с отозванными сертификатами

Если срок действия СОС своей сети закончился, то для обновления СОС вручную выберите нужную строку с именем издателя СОС своей сети и из контекстного меню по правой кнопке мыши (или из меню **Действия**) выберите **Обновить**. Срок действия СОС формируется в соответствии с настройками на вкладке **Списки отозванных сертификатов** окна **Настройки** (см. «[Настройка параметров работы со списками отозванных сертификатов](#)» на стр. 264).

При наличии доверительных отношений обновленные СОС необходимо вручную отправить в другие сети. Чтобы вручную отправить СОС в доверенные сети ViPNet, щелкните необходимые для отправки СОС своей сети и контекстном меню выберите пункт **Экспорт**, после чего в появившемся окне нажмите кнопку **Сохранить**.

Измененные СОС будут отправлены автоматически на те сетевые узлы, для которых в ЦУС настроена необходимость такой отправки, и только в случае, если в УКЦ в настройках программы в окне **Списки отозванных сертификатов** включена опция **Копировать в ЦУС при наличии изменений каждые**.

Для остальных СУ или, для всех СУ, если опция **Автоматически копировать список в ЦУС каждые** выключена, следует создать обновление ключей в индивидуальном режиме (см. «[Создание обновлений ключей узлов](#)» на стр. 97).

Обработка запросов на кросс-сертификаты (в том числе запросов на сертификаты из подчиненных УЦ)

Для построения распределенной (или иерархической) системы доверительных отношений между УЦ следует произвести обработку запросов на кросс-сертификаты из других УЦ.

После получения запросов на кросс-сертификаты следует выполнить следующие действия в своем УКЦ:

- Издать кросс-сертификаты по полученным запросам (см. [«Издание кросс-сертификатов»](#) на стр. 169).
- Экспортировать сертификаты, изданные для администраторов подчиненных УЦ, и передать их администраторам подчиненных УЦ, от которых поступили запросы на сертификат (см. [Экспорт кросс-сертификатов](#) (на стр. 179)).

Издание кросс-сертификатов

Для обработки запросов на кросс-сертификаты в меню **Сервис** выберите **Запросы из файла > Кросс-сертификаты**. Откроется окно для выбора файлов с запросами на кросс-сертификат. Выберите файл с запросом (с расширением `.p10`), переданный из другого УЦ, и нажмите **Открыть**. Можно выбрать сразу несколько файлов с запросами.

После выбора файлов проверяется их содержимое на соответствие стандарту PKCS#10. Запросы, структура которых соответствует формату PKCS#10, отобразятся в окне **Издание кросс-сертификатов**.

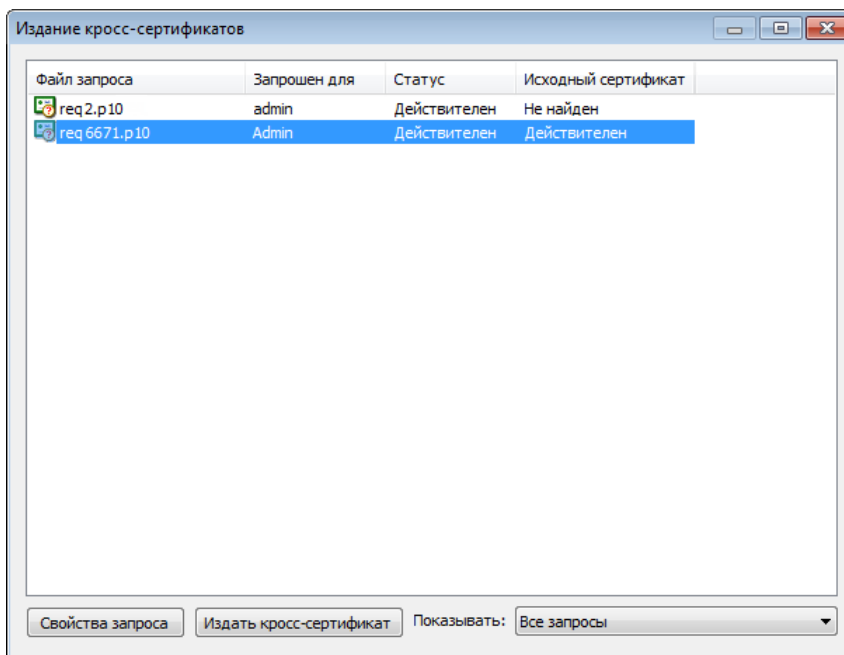


Рисунок 79: Издание кросс-сертификатов

Описание структуры окна **Издание кросс-сертификатов** см. в разделе [Описание окна Издание кросс-сертификатов](#) (на стр. 174).

Для просмотра параметров запроса выберите запрос и нажмите на кнопку **Свойства запроса** (см. «[Описание окна Запрос на кросс-сертификат](#)» на стр. 175).

Для издания кросс-сертификата выберите запрос и нажмите на кнопку **Издатель кросс-сертификат**.



Примечание. Кнопка **Издатель кросс-сертификат** недоступна, если запрос принадлежит администратору данного УКЦ или подпись на запросе искажена (статус **Искажен**).

На экране появится окно с вопросом о том, редактировать ли издаваемый сертификат:

- При отказе от редактирования сертификат будет издан, о чем появится сообщение. При этом срок действия изданного кросс-сертификата назначается как срок действия для сертификатов администраторов из настроек УКЦ, но не превышающий срока действия текущего администратора УКЦ (см. [Настройка параметров работы с сертификатами](#) (на стр. 253)).

- При положительном ответе откроется страница мастера **Шаблон сертификата**, на которой нужно указать срок действия издаваемого кросс-сертификата.

Рисунок 80: Указание срока действия сертификата

Укажите желаемый срок действия издаваемого сертификата, установив переключатель в одно из трех положений. По умолчанию срок действия сертификата составляет 6 лет и является максимальным сроком действия. Минимальный срок действия составляет 1 месяц. Воспользуйтесь одним из следующих способов задания срока действия сертификата:

- **Действителен** – указывается продолжительность срока действия в месяцах с данного момента времени.
- **Действителен до** – указываются дата и время окончания срока действия сертификата.
- **Действителен с** – указываются дата и время начала и окончания срока действия сертификата (выбрано по умолчанию).

Для переключения на следующую страницу используйте кнопку **Далее**. Откроется следующая страница **Назначение сертификата** для указания назначений сертификата.



Примечание. На каждой странице мастера доступна кнопка **Готово**, которую можно нажать в случае, если нет необходимости в дальнейшем редактировании параметров издаваемого сертификата. После нажатия кнопки **Готово** сертификат будет издан.

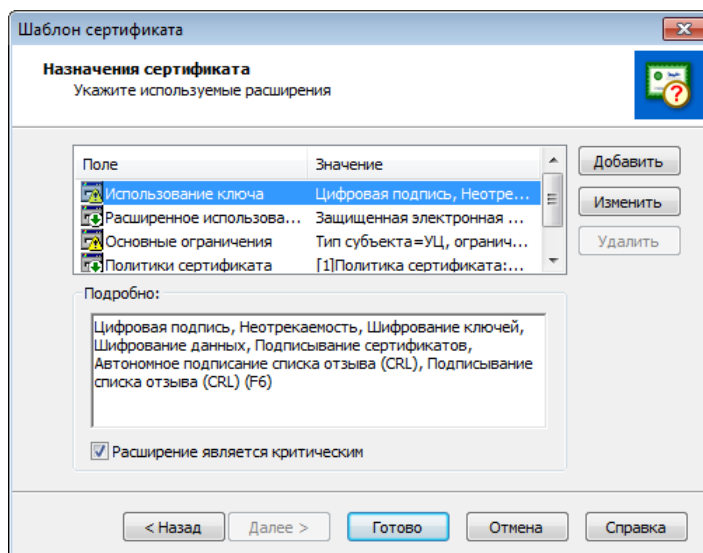


Рисунок 81: Формирование назначений сертификата

Задайте необходимые расширения или политики применения сертификата при помощи кнопок **Добавить** и **Изменить**.



Примечание. Подробно об изменении назначений сертификата см. раздел [Создание запроса на кросс-сертификат и отправка его в другой УЦ](#) (на стр. 230), в котором описаны следующие действия: добавление списка функций использования ключа, изменение, удаление используемых расширений, а также редактирования длины пути цепочки сертификатов.

Если сертификат администратора, на основе которого был создан запрос на кросс-сертификат, включает политики применения, можно добавить расширение **Сопоставления политики**. Это расширение позволяет установить соответствие между политиками, содержащимися в запросе, и собственными политиками данного удостоверяющего центра. Для этого нажмите кнопку **Добавить**, в окне **Допустимые расширения** выберите **Сопоставления политики** и нажмите **ОК**. Откроется окно **Политики применения**.

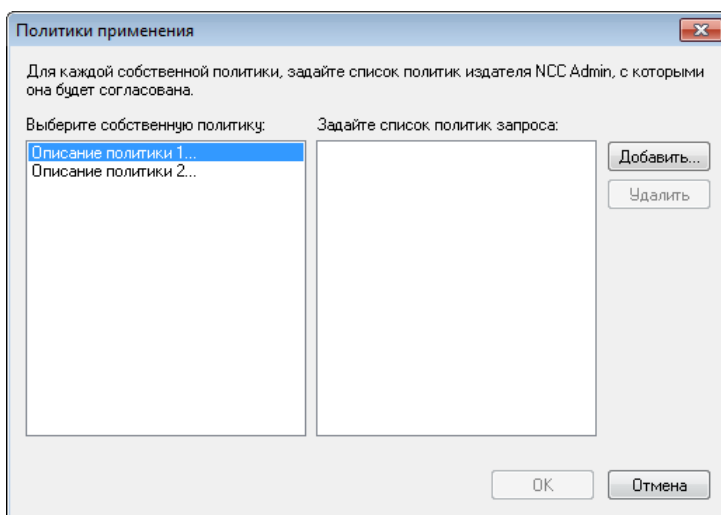


Рисунок 82: Согласование политик применения сертификата

На левой панели окна **Политики применения** выберите собственную политику, затем нажмите кнопку **Добавить**. Из списка политик запроса укажите ту политику, которую требуется поставить в соответствие выбранной собственной политике, затем нажмите **ОК**.

По завершении настроек нажмите кнопку **Готово** для издания сертификата.

Если срок действия издаваемого сертификата в запросе превышает срок действия сертификата текущего администратора УКЦ, то будет выдано сообщение об установке точно такого же срока действия издаваемого сертификата, как у текущего администратора УКЦ. Для создания сертификата нажмите **ОК** в окне с сообщением.

Сертификат будет издан, о чем появится сообщение.

Изданный кросс-сертификат помещается в папку **Удостоверяющий центр > Сертификаты администраторов > Кросс-сертификаты > Изданные**.

Сертификаты, изданные для администраторов подчиненных УЦ, далее следует экспортировать (см. «[Экспорт кросс-сертификатов](#)» на стр. 179) для передачи администратору подчиненного УЦ, от которого поступил запрос на сертификат.

Также изданные в своем УКЦ кросс-сертификаты помещаются в справочник `NNNN.tr1` вместе с сертификатами администраторов своего УКЦ (где `NNNN` — номер сети) для экспорта в другие сети ViPNet. Это происходит при изменении сертификата администратора своего УКЦ или при использовании главного меню **Сервис > Экспорт справочников** (см. раздел [Экспорт служебных данных](#) (на стр. 295)).

После издания кросс-сертификата или сертификата подчиненного внешнего УЦ (не ViPNet) производится их рассылка на сетевые узлы обычным порядком в файле 0000_tr1.p7s.

Описание окна Издание кросс-сертификатов

Опишем структуру окна **Издание кросс-сертификатов**. О том, как открыть это окно читайте в разделе [Издание кросс-сертификатов](#) (на стр. 169).

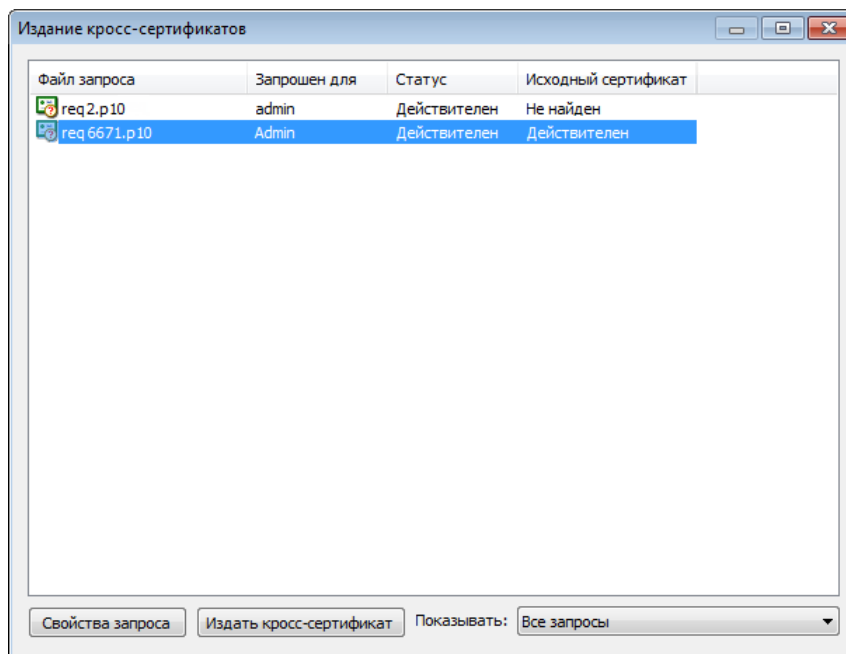


Рисунок 83: Издание кросс-сертификатов

Окно состоит из таблицы со списком выбранных запросов на кросс-сертификаты и кнопок.

Таблица имеет следующие колонки:

- **Файл запроса** – имя файла, содержащего запрос на кросс-сертификат.
- **Запрошен для** – имя владельца издаваемого сертификата.
- **Статус** – результат проверки подписи запроса. Колонка **Статус** может иметь одно из трех значений:
 - **Действителен** – если проверка подписи прошла успешно.
 - **Искажен** – если при проверке подписи была обнаружена ошибка.


- **Неверный набор атрибутов** – в случае отсутствия или неверного состава критических расширений (назначение ключа, основные ограничения) или при наличии в запросе открытого ключа совпадающего с ключом администратора своей сети.
- **Исходный сертификат** – отражает факт наличия и действительности исходного сертификата. Возможные значения:
 - **Не найден.**
 - **Недействителен.**
 - **Действителен.**

В нижней части окна из списка с названием **Показывать** можно выбрать следующие значения:

- **Все запросы.**
- **Действительные** (запросы, подпись под которыми верна).
- **Новые** (нет сертификатов с таким же открытым ключом).

В нижней части окна располагаются следующие кнопки:

- **Свойства запроса** – для просмотра запроса на кросс-сертификат (можно дважды щелкнуть мышью на выбранном запросе для вызова окна). Кнопка активна всегда при выборе какого-либо запроса.
- **Издать кросс-сертификат** – для издания кросс-сертификата по выбранному запросу. Данная кнопка будет неактивна, если запрос либо искажен, либо неверен по назначению, либо обнаружен аналогичный корневой сертификат администратора своей сети.

Для того чтобы закрыть окно, нажмите  в верхнем правом углу.

Описание окна Запрос на кросс-сертификат

Для просмотра параметров запроса выберите запрос в окне **Издание кросс-сертификатов** и нажмите на кнопку **Свойства запроса**.

Окно **Запрос на кросс-сертификат** имеет пять вкладок: **Общие**, **Владелец ключа**, **Открытый ключ**, **Состав** и **Сертификаты**.

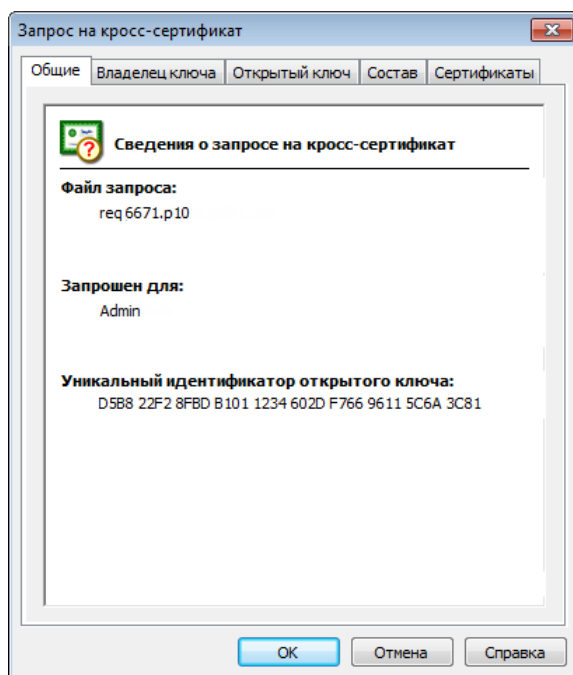




Рисунок 84: Просмотр запроса на кросс-сертификат

На вкладке **Общие** отображаются следующие сведения о запросе на кросс-сертификат: имя файла запроса, для кого сделан запрос, уникальный идентификатор открытого ключа, а также, если при проверке подписи была обнаружена ошибка, то внизу вкладки будет ее описание. Кроме того, вместо значка сертификата с успешной проверкой подписи  появится значок .

Вкладки **Открытый ключ** и **Владелец** содержат такую же информацию, как и одноименные вкладки запроса на сертификат.

Вкладка **Состав** содержит значения полей запроса, включая атрибуты и расширения. Форматирование информации осуществляется аналогично одноименной вкладке в окне **Сертификат**.

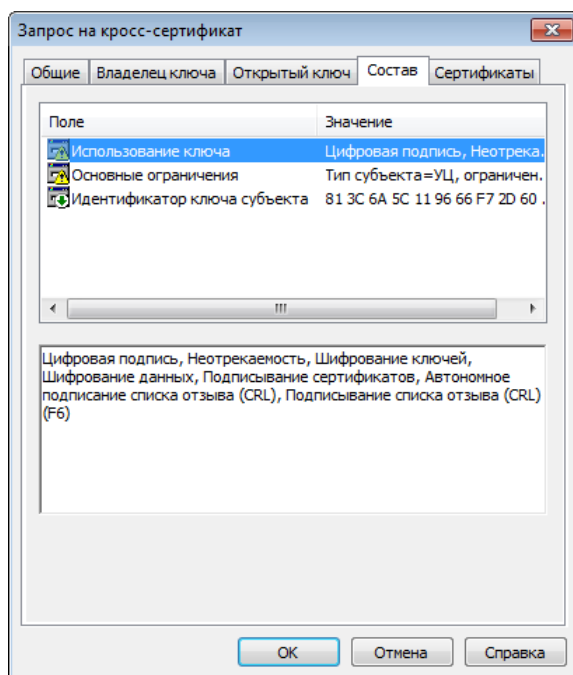


Рисунок 85: Состав запроса на кросс-сертификат

Вкладка **Сертификаты** отображает следующую информацию:

- Под заголовком **Корневой сертификат** указываются:
 - **Серийный номер** корневого сертификата, если он найден.
 - **Действителен до:** – до какой даты действителен этот сертификат.
 - Статус проверки принимает значения: действителен, недействителен, не найден.
- Если статус корневого сертификата имеет значение **Не найден**, то активна кнопка **Найти**. При нажатии на эту кнопку вызывается окно выбора файла, в котором нужно найти и указать исходный корневой сертификат. Выбираются файлы, имеющие следующие стандартные расширения: *.cer (по умолчанию), *.p7b, *.p7s, *.* - все файлы. Если выбранный файл содержит сертификат с тем же открытым ключом, что и запрос, то информация о нем отображается, в противном случае выдается сообщение **Исходный сертификат в указанном файле не найден**.

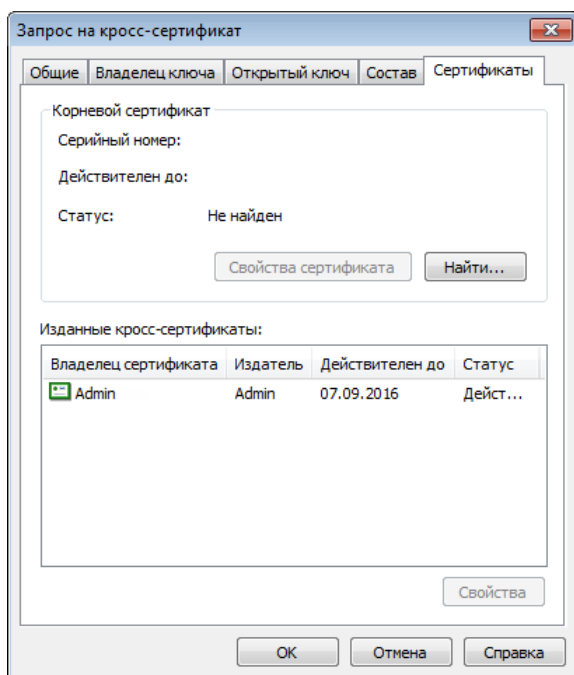


Рисунок 86: Просмотр изданных сертификатов

- Если статус корневого сертификата имеет значение **Действителен** или **Недействителен**, то активна кнопка **Свойства сертификата**, при нажатии на которую будет вызвано окно стандартного диалога просмотра сертификата.

В нижней части страницы представлен список **Изданные кросс-сертификаты**. В данном списке отображается информация о всех ранее изданных кросс-сертификатах с тем же открытым ключом. Состав колонок списка:

- **Владелец сертификата** (имя).
- **Издатель** (имя).
- **Действителен до:** (дата, до которой сертификат действителен).
- **Статус** (действителен, недействителен).

Для выделенного объекта можно просмотреть свойства сертификата по нажатию кнопки **Свойства**.

Просмотр запросов и сертификатов

В программе УКЦ возможен просмотр любых запросов и сертификатов. В данном разделе документа подробно описано, в какой папке можно открыть тот или иной запрос или сертификат.

Просмотр запросов на сертификаты пользователей

Если в настройках не указано автоматически удовлетворять запрос на сертификат (см. «[Настройка параметров издания сертификатов и обработки запросов](#)» на стр. 250), то при поступлении запроса он попадает в следующую папку (в зависимости от того, кем был создан запрос):

- Запрос создан пользователем своей сети – папка **Удостоверяющий центр > Запросы на сертификаты > Входящие > Своя сеть ViPNet.**
- Запрос создан внешним пользователем – папка **Удостоверяющий центр > Запросы на сертификаты > Входящие > Внешние пользователи.**

После того, как запрос на сертификат будет удовлетворен (вручную или автоматически) в вышеназванных папках, он попадает в следующую папку (в зависимости от того, кем был создан запрос):

- Запрос создан пользователем своей сети – папка **Удостоверяющий центр > Запросы на сертификаты > Удовлетворенные > Своя сеть ViPNet.**
- Запрос создан внешним пользователем – папка **Удостоверяющий центр > Запросы на сертификаты > Удовлетворенные > Внешние пользователи.**

Просмотр запроса на сертификат

Чтобы посмотреть подробную информацию о запросе на сертификат (см. «[Запрос на сертификат](#)»), в соответствующем подразделе раздела **Запросы на сертификаты** дважды щелкните нужный запрос правой кнопкой мыши или в контекстном меню запроса выберите пункт **Открыть**.

В окне просмотра параметров запроса содержится ряд вкладок, на которых отображается следующая информация:

- **Общие** — основная информация о запросе:

- для запросов, сформированных в программах ViPNet Client и ViPNet Registration Point — номер запроса; имя администратора, заверившего запрос; имя владельца открытого ключа; желательный срок действия сертификата; статус запроса и подписи;
 - для запросов, сформированных во внешних приложениях (например, в ViPNet CSP) — имя файла запроса; назначение сертификата; имя пользователя, для которого запрошен сертификат; идентификатор открытого ключа.
- **Владелец ключа** — сведения о пользователе ViPNet, для которого создан запрос на сертификат.
 - **Срок действия** — срок действия сертификата, заявленный в запросе.
 - **Открытый ключ** — параметры открытого ключа.
 - **Состав** — список расширений, определяющих назначение сертификата.
 - **Информация о запросе** — дополнительные сведения о владельце открытого ключа.
 - **Статус** — текущий статус запроса и история запроса (дата и время создания, отправки, доставки и других статусов запроса).
 - **Подпись** — информация о подписи, заверившей запрос, и контрольной сумме запроса. На вкладке также с помощью кнопки **Просмотр сертификата** можно просмотреть сведения о сертификате, которым был подписан запрос.



Примечание. В зависимости от того, где был сформирован запрос на сертификат (в программе ViPNet Client, в программе ViPNet Registration Point или во внешнем приложении), набор вкладок может быть различным.

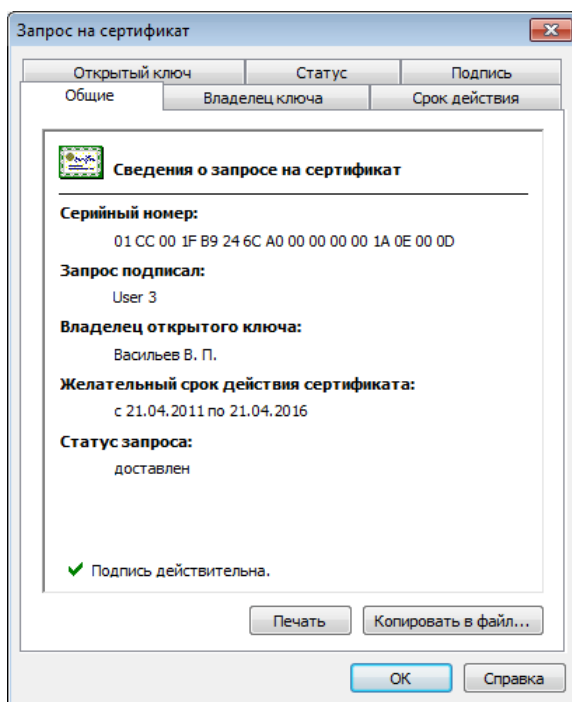


Рисунок 88: Просмотр общей информации о запросе

Просмотр сертификатов

После издания сертификата пользователя, или регистрации сертификата администратора из доверенной сети ViPNet, такой сертификат всегда можно посмотреть:

- Для пользователя своей сети в папке **Удостоверяющий центр > Сертификаты пользователей > Своя сеть ViPNet**.
- Для внешнего пользователя в папке **Удостоверяющий центр > Сертификаты пользователей > Внешние пользователи**.
- Для администратора своей сети в папке **Удостоверяющий центр > Сертификаты администраторов > Своя сеть ViPNet**.
- Для зарегистрированных сертификатов администраторов из доверенных сетей в папке **Удостоверяющий центр > Сертификаты администраторов > Доверенные сети ViPNet > Текущие**.
- Изданные кросс-сертификаты администраторов других УЦ в папке **Удостоверяющий центр > Сертификаты администраторов > Кросс-сертификаты > Изданные**.

Для просмотра сертификата пользователя нужно выбрать пользователя и из контекстного меню по правой кнопке мыши выбрать **Открыть**. После этого (если для данного пользователя был сформирован сертификат) откроется окно **Сертификат**.

Окно Сертификат

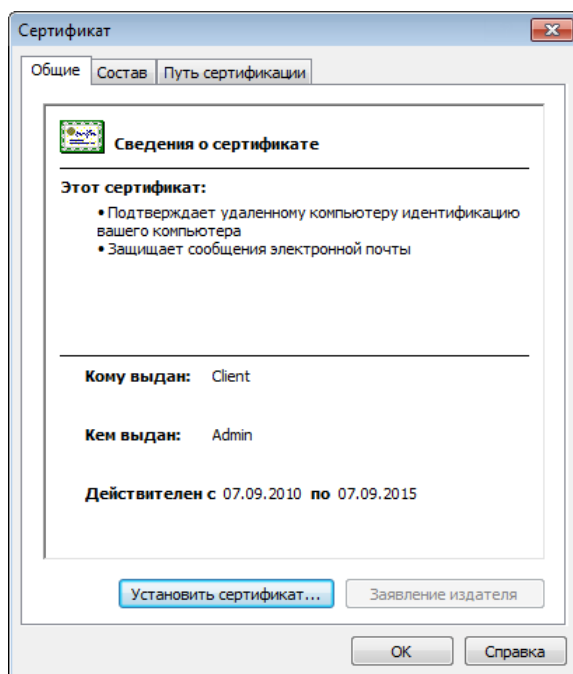


Рисунок 89: Просмотр сведений о сертификате

Вкладка **Общие** содержит общие сведения о сертификате: список применения сертификата, имя пользователя, кому он выдан, имя администратора, заверившего сертификат, а также срок действия. Кнопка **Установить сертификат** в УКЦ не используется. Если нажать на кнопку **Заявление издателя**, откроется окно **Заявление об отказе**, содержащее описание политики применения сертификата.

Вкладка **Состав** включает в себя вывод списка всех полей по стандарту X.509, расширений и связанных свойств, найденных в сертификате. Информацию из этого окна можно распечатать с помощью кнопки **Печать**, и сохранить в файл с помощью кнопки **Копировать в файл** (с помощью этой кнопки сертификат открытого ключа подписи можно экспортировать в файл различных форматов по выбору пользователя, подробности см. в разделе [Экспорт сертификатов](#) (на стр. 188)).

Сертификат распечатывается в специальном формате с заголовком, данными сертификата, с именами владельца сертификата и уполномоченного лица (более подробно см. в документе «Печать сертификатов»). Данные сертификата включают в себя следующую информацию:

- Имя владельца сертификата.
- Информацию, относящуюся к стандарту X 509.
- Название алгоритма подписи.
- Имя издателя сертификата.
- Срок действия сертификата.
- Информацию о ключе владельца сертификата.
- Информацию о ключе центра сертификации.
- Информацию о проверке сертификата, где отражается:
 - Статус сертификата: действителен или недействителен.
 - Время проверки: дата и время.



Примечание. Время проверки — это время открытия данного сертификата и другая информация.

При нажатии кнопки **Копировать в файл** сертификат открытого ключа подписи будет сохранен в файле с расширением *.cer. Впоследствии сертификат может быть проверен (подробно см. раздел [Проверка сертификатов](#) (на стр. 192)) открытием данного файла с помощью пункта меню **Действия > Проверить сертификат**.

Вкладка **Путь сертификации** используется для просмотра пути данного сертификата и состояния сертификата. Путь сертификата представляет собой цепочку связанных сертификатов. В этом окне можно подробно просмотреть выбранный сертификат из цепочки, используя кнопку **Просмотр сертификата** на этой вкладке.

Просмотр истории сертификата

Операции, которые производились с сертификатом пользователя в УКЦ с момента его издания, зафиксированы в так называемой истории сертификата. Историю каждого изданного сертификата пользователя при необходимости можно просмотреть.

Чтобы просмотреть историю сертификата:

- 1 В окне программы на панели навигации перейдите в папку:
 - **Удостоверяющий центр > Сертификаты пользователей > Своя сеть ViPNet** — для просмотра истории сертификата пользователя своей сети ViPNet (внутреннего пользователя);
 - **Удостоверяющий центр > Сертификаты пользователей > Внешние пользователи** — для просмотра истории сертификата внешнего пользователя.
- 2 Щелкните нужный сертификат правой кнопкой мыши и в контекстном меню выберите пункт **Статус**.
- 3 В появившемся окне ознакомьтесь с операциями, которые производились с сертификатом, а также датами их проведения.

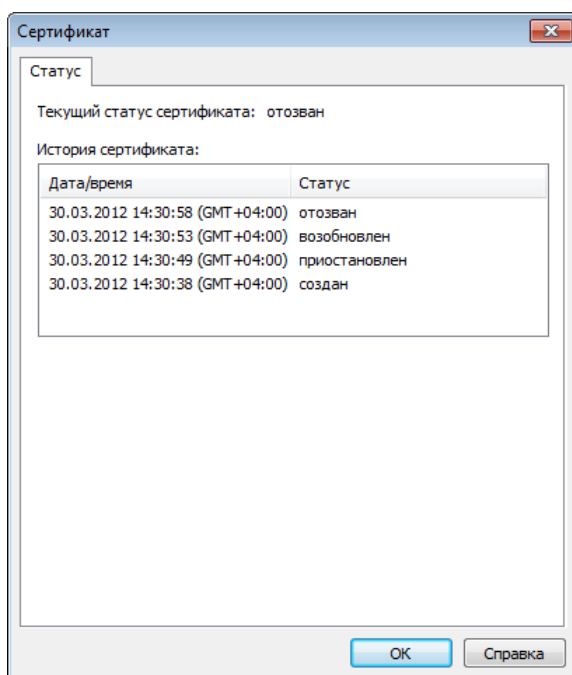


Рисунок 90: Просмотр истории сертификата

Просмотр списков отзыва сертификатов

Папка **Удостоверяющий центр > Списки отозванных сертификатов** (для своей сети) содержит списки отозванных сертификатов своей сети и доверенных сетей ViPNet (соответственно), запросы на отзыв и приостановление которых были удовлетворены в УКЦ.

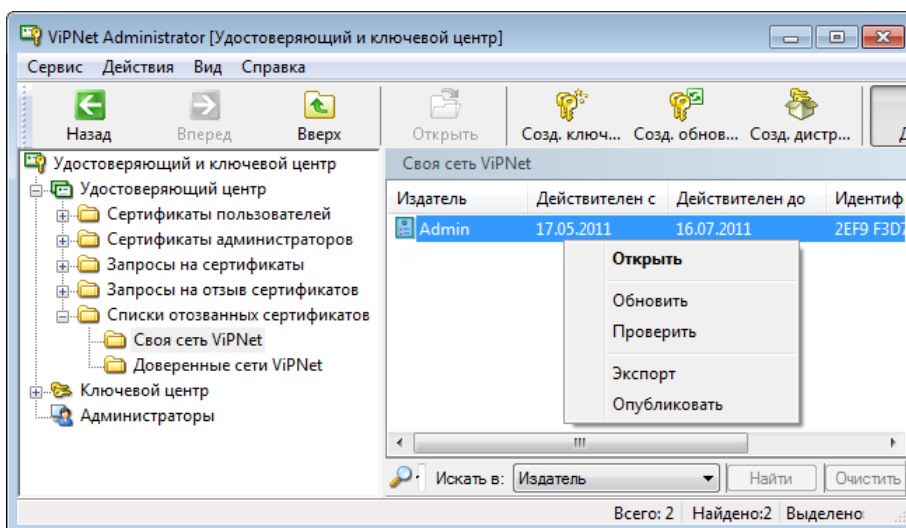


Рисунок 91: Возможные действия с отозванными сертификатами

Для просмотра списка отозванных сертификатов выберите из контекстного меню (или из главного меню **Действия**) пункт **Открыть**. После этого откроется окно **Список отзыва сертификатов**.

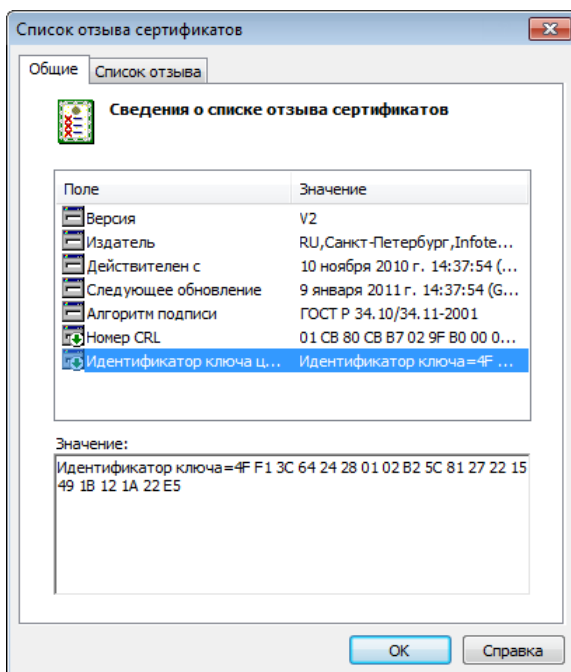


Рисунок 92: Просмотр списка отзыва сертификатов

Вкладка **Общие** включает в себя вывод списка атрибутов и связанных свойств, найденных в СОС (данные об администраторе, алгоритме подписи и т.д.).

Вкладка **Список отзыва** содержит сам список отозванных и приостановленных сертификатов. Просмотреть любой сертификат из списка можно с помощью кнопки **Просмотр сертификата**. Если приходит запрос на возобновление действия сертификата, входящего в этот список, то при удовлетворении этого запроса, данный сертификат будет удален из списка.

Экспорт сертификатов

Изданные сертификаты (пользователей сети ViPNet, внешних пользователей, администраторов своей сети, кросс-сертификаты) могут быть экспортированы в файл. Для этого выберите сертификат в папке расположения сертификата нужного типа (**Удостоверяющий и ключевой центр > Удостоверяющий центр > Сертификаты пользователей > Своя сеть ViPNet** или **Внешние пользователи, Удостоверяющий и ключевой центр > Удостоверяющий центр > Сертификаты администраторов > Своя сеть ViPNet** или **Кросс-сертификаты > Изданные**) и в контекстном меню выберите **Экспорт**.

Экспорт сертификата можно осуществить и из окна просмотра сертификата **Сертификат** (см. «[Просмотр сертификатов](#)» на стр. 182). Для этого выберите вкладку **Состав** и нажмите кнопку **Копировать в файл**.

Откроется первая страница мастера экспорта сертификатов с приветствием. Нажмите кнопку **Далее**. Откроется следующая страница мастера для выбора формата экспортируемого файла.

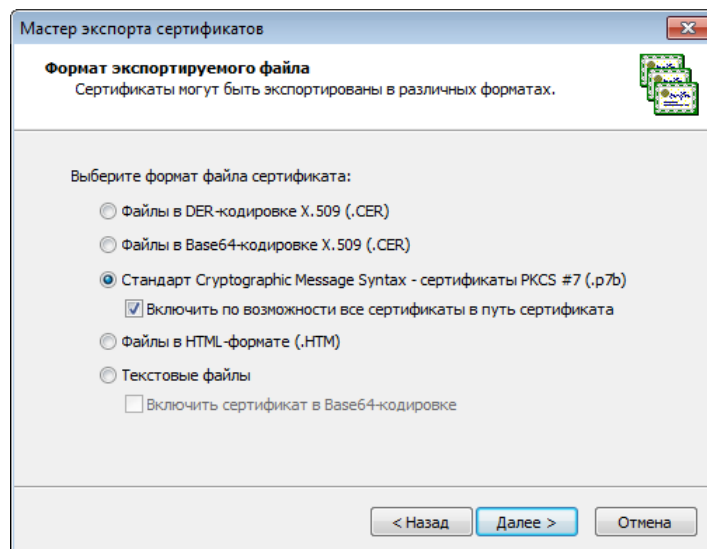


Рисунок 93: Выбор формата экспортируемого файла

Выберите один из следующих форматов файла сертификата для экспорта (в скобках указано расширение файла):

- Файлы в DER-кодировке X.509 (расширение * .CER).

- Файлы в Base64-кодировке X.509 (расширение *.cer).
- Стандарт Cryptographic Message Syntax —сертификаты PKCS #7 (расширение .p7b) — для этого формата можно установить флажок **Включить по возможности все сертификаты в путь сертификата**.
- Файлы в HTML-формате (расширение *.htm).
- Текстовые файлы (расширение *.txt). Для этого формата можно установить флажок **Включить сертификат в Base64-кодировке**.

После выбора формата файла нажмите кнопку **Далее**. Появится страница, где нужно указать путь и имя файла. Можно указать только имя, расширение файла будет добавлено автоматически в соответствии с выбранным форматом. В этом окне нажмите кнопку **Далее**. Появится страница мастера с указанием заданных параметров экспортируемого файла. Нажмите кнопку **Готово**. Появится сообщение об успешном экспорте файла.

В результате экспорта сертификат будет сохранен в файле заданного формата с заданным именем по заданному пути. Теперь можно просмотреть файл сертификата в среде, соответствующей расширению файла экспорта. Этот файл можно передавать в другие УЦ.

Форматы экспорта сертификатов

При выборе формата экспорта сертификата следует руководствоваться перечисленными положениями.

- При экспорте сертификатов для импорта на компьютер с ОС Windows наиболее предпочтительный формат экспорта — PKCS #7, в первую очередь потому, что этот формат обеспечивает сохранение цепочки центров сертификации, или пути сертификации любого сертификата. Некоторые приложения требуют при импорте сертификата из файла представления в виде DER или Base64. Поэтому формат экспорта необходимо выбирать в соответствии с требованиями приложения или системы, в которую этот сертификат предполагается импортировать.
- Для просмотра сертификата и вывода его на печать используются текстовый и HTML-форматы.

Ниже находится подробная информация о каждом из форматов экспорта сертификатов, поддерживаемыми ПО VipNet

- **Стандарт Cryptographic Message Syntax (PKCS #7)**

Формат PKCS #7 позволяет передавать сертификат и все сертификаты в цепочке сертификации с одного компьютера на другой или с компьютера на внешнее устройство. Файлы PKCS #7 обычно имеют расширение .p7b и совместимы со стандартом ITU-T X.509. Формат PKCS#7 разрешает такие атрибуты, как удостоверяющие подписи, связанные с обычными подписями. Для таких атрибутов, как метка времени, можно выполнить проверку подлинности вместе с содержимым сообщения. Дополнительные сведения о формате PKCS #7 см. на странице PKCS #7 веб-узла RSA Labs <http://www.rsa.com/rsalabs/node.asp?id=2129>.

- **Файлы в DER-кодировке X.509**

DER (Distinguished Encoding Rules) для ASN.1, как определено в рекомендации ITU-T Recommendation X.509, — более ограниченный стандарт кодирования, чем альтернативный BER (Basic Encoding Rules) для ASN.1, определенный в рекомендации ITU-T Recommendation X.209, на котором основан DER. И BER, и DER обеспечивают независимый от платформы метод кодирования объектов, таких как сертификаты и сообщения, для передачи между устройствами и приложениями.

При кодировании сертификата большинство приложений используют стандарт DER, так как сертификат (сведения о запросе на сертификат) должен быть закодирован с помощью DER и подписан. Файлы сертификатов DER имеют расширение .cer.

Дополнительные сведения см. в документе «ITU-T Recommendation X.509, Information Technology — Open Systems Interconnection — The Directory: Authentication Framework» на веб-узле International Telecommunication Union (ITU) <http://www.itu.int/ru/Pages/default.aspx>.

- **Файлы в Base64-кодировке X.509**

Этот метод кодирования создан для работы с протоколом S/MIME, который популярен при передаче бинарных файлов через Интернет. Base64 кодирует файлы в текстовый формат ASCII, при этом в процессе прохождения через шлюз файлы практически не повреждаются. Протокол S/MIME обеспечивает работу некоторых криптографических служб безопасности для приложений электронной почты, включая механизм неотрекаемости (с помощью электронных подписей), секретность и безопасность данных (с помощью кодирования, процесса проверки подлинности и целостности сообщений). Файлы сертификатов Base64 имеют расширение .cer.

MIME (Multipurpose Internet Mail Extensions) спецификации (RFC 1341 and successors) определяет механизмы кодирования произвольных двоичных данных для передачи по электронной почте.

Дополнительные сведения см. в документе «RFC 2633 S/MIME Version 3 Message Specification, 1999» на веб-узле Internet Engineering Task Force (IETF) <http://www.ietf.org/rfc/rfc2633.txt?number=2633>.

- **Файлы в HTML-формате**

Файлы для просмотра и печати в любом веб-браузере, а также офисных и других программах, поддерживающих язык разметки гипертекста HTML.

- **Текстовые файлы**

Файлы кодировки ANSI для просмотра в любом текстовом редакторе и вывода на печать.

Проверка сертификатов

В УЦ есть возможность проверить сертификат открытого ключа подписи любого зарегистрированного в УЦ пользователя. Для проверки сертификата пользователь должен обратиться в УЦ с заявлением либо в простой письменной форме, либо в электронном виде (с использованием ViPNet Деловая почта). При подаче заявления в электронном виде оно должно быть подписано действующим ключом подписи пользователя. Приложением к заявлению на подтверждение подлинности сертификата открытого ключа является файл (в виде вложения ViPNet Деловая почта), содержащий сертификат открытого ключа зарегистрированного пользователя УЦ, подвергающийся процедуре проверки.

Для того, чтобы получить такой файл, нужно в окне **Сертификат** нажать кнопку **Копировать в файл**, и сертификат открытого ключа подписи будет сохранен в выбранном папке в файле с расширением *.cer.

Публикация и прием опубликованных данных

Публикация — это распространение сформированной в УЦ информации на источниках данных, доступных по общеизвестным протоколам. Публикация имеет целью упростить интеграцию ViPNet приложений с приложениями других разработчиков. Публикацией информации занимается программа ViPNet Publication Service.

В УЦ создаются сертификаты пользователей, администраторов, СОС. Исходя из требований безопасности, сетевой узел УКЦ, как правило, не имеет выхода во внешние сети. Вместе с тем, при взаимодействии с внешними УЦ актуализация списков отозванных сертификатов этих УЦ производится путем обращения к так называемым точкам распространения СОС. Для обеспечения нормального взаимодействия с внешними УЦ необходимо периодически обращаться к внешним точкам распространения, извлекать оттуда информацию о СОС и обеспечивать их рассылку на сетевые узлы ViPNet в составе обновлений ключей узлов.

Опрос точек распространения СОС осуществляет ViPNet Publication Service в соответствии со своими настройками. Publication Service передает полученные списки в УЦ, используя при этом папки обмена информацией с УКЦ. УКЦ принимает полученные СОС, импортирует их, затем они рассылаются на СУ в составе обновлений.

Таким образом, в программе УКЦ обеспечиваются следующие возможности:

- 1 Настройка состава информации, подлежащей публикации.
- 2 Автоматическое копирование информации в соответствии с настройками для Publication Service.
- 3 Выборочное копирование информации для Publication Service по команде администратора.
- 4 Сканирование каталога с ответами от ViPNet Publication Service, сохранение информации о точках доступа к опубликованной информации.
- 5 Редактирование информации о точках доступа к опубликованной информации.
- 6 Размещение данных о точках доступа в сертификатах пользователей.

Путь к точке распространения может быть получен программой ViPNet Publication Service либо от УКЦ, либо администратор должен ввести путь к точке распространения вручную в программе ViPNet Publication Service.

Для работы программы ViPNet Publication Service в УЦ должны быть сделаны соответствующие настройки папок обмена с программой ЦУС и другие (см. разделы [Настройка папок обмена](#) (на стр. 239) и [Настройка параметров публикации данных](#) (на стр. 271)). Ниже описано более детально, как настроить программу УКЦ для взаимодействия с программой ViPNet Publication Service, как подготовиться к публикации и автоматической публикации, и как получить опубликованные данные.

При издании сертификатов пользователей в расширение CrlDistributionPoint добавляется информация обо всех включенных точках доступа к СОС, а в расширение AuthorityInfoAccess добавляется информация обо всех включенных точках доступа к текущему сертификату администратора (по серийному номеру).

Настройка программы УКЦ для взаимодействия с программой ViPNet Publication Service

Для того чтобы программа ViPNet Publication Service смогла опубликовать данные, произведите следующие настройки:

- 1 Прежде всего, нужно либо настроить папки приема (получения) данных от ViPNet Publication Service, либо воспользоваться папкой по умолчанию. По умолчанию, это папка администратора в каталоге установки УКЦ `for_NCC (from_NCC)\pubserv\`. Настраивается только папка приема (получения) файлов для (из) ЦУС, подпапка `pubserv\` задана программой.



Примечание. Если УКЦ и ViPNet Publication Service установлены на разных компьютерах, то на компьютере с УКЦ, используя средства операционной системы, откройте сетевой доступ к настроенным папкам приема (получения) файлов для компьютера, где установлен ViPNet Publication Service.

- 2 В настройках УКЦ выбрать пункт главного меню **Сервис > Настройка > Публикация** (см. «[Настройка параметров публикации данных](#)» на стр. 271) и указать, какие данные подлежат публикации.
- 3 Настроить список точек распространения (пункт главного меню **Сервис > Настройка > Публикация > Точки распространения** (см. «[Настройка списка точек распространения](#)» на стр. 273)) — добавить, удалить и отредактировать элементы списка точек распространения.

Копирование данных для программы сервиса публикации

После задания настроек публикация будет производиться либо автоматически (в соответствии с настройками), либо вручную, по команде меню **Опубликовать** в соответствующих окнах для следующих выделенных элементов:

- сертификатов администраторов своей сети;
- кросс-сертификатов, изданных в своей сети;
- сертификатов пользователей;
- списка отозванных сертификатов своей сети.



Внимание! Автоматическое копирование данных в папку для ViPNet Publication Service осуществляется при издании новых сертификатов или при обновлении СОС своей сети.

При копировании сертификатов администраторов программа формирует случайное имя файла для копирования в папку для ViPNet Publication Service.

При публикации СОС копирование производится в виде файлов `NNNN_rem.crl`.

Прием данных из программы ViPNet Publication Service

ПО ViPNet Publication Service принимает информацию от программы УКЦ в виде файлов с расширениями `*.cer` (сертификат), `*.crt` (кросс-сертификат), `*.crl` (список отзыва) и публикует их в соответствии со своими настройками. В случае полностью успешной или частично успешной публикации ViPNet Publication Service отправляет отчет о результатах публикации в программу УКЦ.

Полностью успешная публикация означает, что данные опубликованы на всех выбранных пользователем серверах доступа (настраивается в программе ViPNet Publication Service).

Частично успешная публикация означает, что данные опубликованы не на всех выбранных пользователем серверах доступа, но хотя бы на одном из них.

Неудачная публикация означает, что данные вообще нигде не удалось опубликовать. Файлы, которые не удалось опубликовать, попадут в подпапку папки отправки файлов в УКЦ `Unpublished`.

Результаты публикации отправляются в УКЦ. Они создаются в виде специальных файлов и называются отчетами о публикации. Эти отчеты содержат информацию о точках доступа к опубликованным данным. Форматы отчетов о публикации сертификатов и СОС имеют структуру ini-файла и схожи по содержанию.



6

Управление администраторами программы ViPNet Удостоверяющий и ключевой центр

Создание учетной записи администратора	199
Удаление учетной записи администратора	202
Смена текущей учетной записи администратора	203
Просмотр контейнера ключей администратора	204
Просмотр и изменение данных об администраторе	206
Обновление сертификата и закрытого ключа администратора	208
Выбор текущего сертификата администратора	216
Смена пароля администратора	217
Смена ключа защиты УКЦ	218

Смена ключевого носителя администратора	219
Создание запроса на кросс-сертификат к вышестоящему УЦ и установка изданного сертификата в иерархической системе доверительных отношений	220
Создание запроса на кросс-сертификат к другому УЦ в распределенной системе доверительных отношений	230

Создание учетной записи администратора

В программе ViPNet Удостоверяющий и ключевой центр может использоваться несколько учетных записей администраторов (см. «[Администратор УКЦ](#)»). Самая первая учетная запись администратора создается в процессе первичной инициализации программы (см. «[Проведение первичной инициализации программы](#)» на стр. 50). Для организации многопользовательской работы в программе с целью распределения прав по управлению сертификатами и ключами сети ViPNet вы можете создать дополнительные учетные записи администраторов УКЦ.

Следует учесть, что при создании учетной записи администратора автоматически в соответствии с заданными параметрами издается сертификат администратора (корневой сертификат, если Удостоверяющий центр, в роли которого выступает УКЦ, является головным (см. «[Головной удостоверяющий центр](#)»)), который становится сертификатом издателя (см. «[Сертификат издателя](#)»).

Для создания новой учетной записи администратора:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в разделе **Администраторы** правой кнопкой мыши щелкните по текущей учетной записи администратора и в контекстном меню выберите пункт **Создать**. Будет запущен мастер создания администратора сети ViPNet.
- 2 На странице **Назначение администратора сети ViPNet** выберите пользователя, который будет выполнять функции администратора.



Примечание. Выбор пользователя сети ViPNet при создании администратора является номинальным. Выбранный пользователь может не обладать особыми правами, чтобы выполнять функции администратора сети ViPNet.

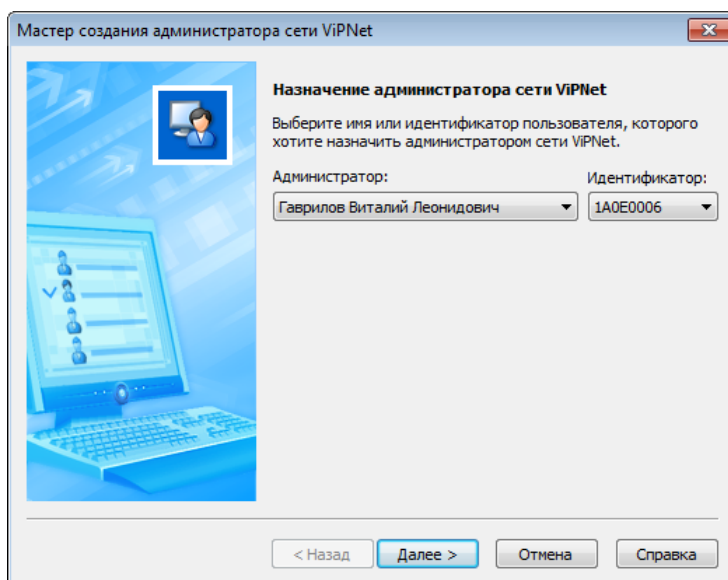


Рисунок 94: Выбор пользователя, назначаемого администратором УКЦ

- 3 На последующих страницах мастера задайте параметры сертификата администратора, который будет издан по завершении создания его учетной записи. Подробнее см. раздел [Обновление сертификата и закрытого ключа администратора](#) (на стр. 208).
- 4 На странице **Место хранения контейнеров ключа подписи и ключа защиты УКЦ** выберите способ хранения ключей администратора.
- 5 На странице **Пароль администратора сети ViPNet** выберите тип пароля и задайте сам пароль администратора для входа в программу.
- 6 На последней странице мастера ознакомьтесь с результатом создания новой учетной записи администратора, после чего нажмите кнопку **Готово**. При создании учетной записи администратора кроме издания сертификата также производится экспорт служебных данных (на стр. 295) и создание обновлений ключей узлов.

При успешном создании учетной записи администратора и выполнении всех сопутствующих операций на последней странице мастера появится соответствующее сообщение, и напротив каждой операции будет отображаться значок . Если какие-то операции были выполнены с ошибками, то они будут отмечены значком .

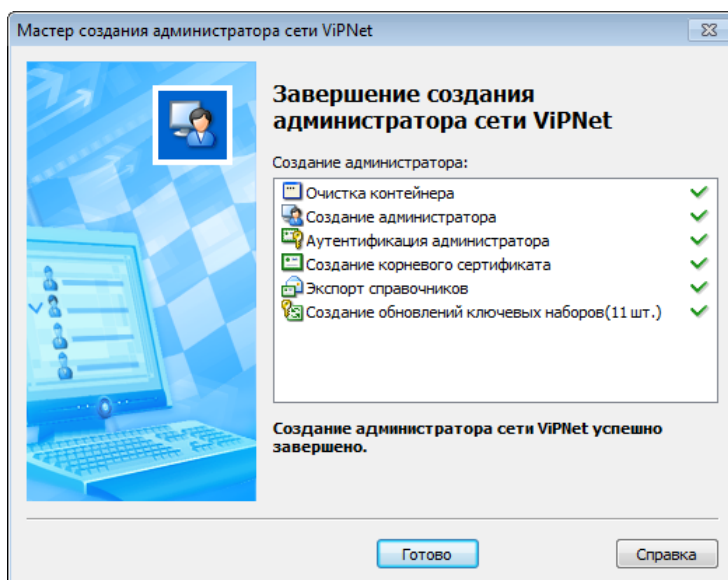


Рисунок 95: Результат создания учетной записи нового администратора

В результате созданная учетная запись появится в списке в разделе **Администраторы** и автоматически станет текущей. При необходимости текущую учетную запись администратора можно сменить (см. «[Смена текущей учетной записи администратора](#)» на стр. 203). В разделе **Сертификаты администраторов > Своя сеть ViPNet** появится изданный сертификат администратора.

После создания учетной записи выполните следующие действия:

- 1 Удостоверьтесь, что в УКЦ можно выполнить вход под учетной записью нового администратора (см. «[Запуск и завершение работы с программой](#)» на стр. 59).
- 2 Если УКЦ выступает в роли подчиненного Удостоверяющего центра, то изданный сертификат будет не корневым, а только самоподписанным. Если в соответствии с регламентом такой сертификат нельзя использовать (для подписи издаваемых сертификатов пользователей), то получите другой сертификат в вышестоящем Удостоверяющем центре по специальному запросу. О том, как получить сертификат в вышестоящем Удостоверяющем центре, см. раздел [Создание запроса на кросс-сертификат к вышестоящему УЦ и установка изданного сертификата в иерархической системе доверительных отношений](#) (на стр. 220).
- 3 Перенесите созданные обновления ключей узлов в программу ViPNet Центр управления сетью для их дальнейшей отправки на узлы своей сети и в доверенные сети ViPNet (при наличии межсетевого взаимодействия). Если планируется получение сертификата в вышестоящем Удостоверяющем центре, то обновления ключей рекомендуется перенести в ЦУС после выдачи сертификата и повторного экспорта служебных данных.

Удаление учетной записи администратора

Если в программе ViPNet Удостоверяющий и ключевой центр зарегистрировано несколько учетных записей администраторов (см. [«Создание учетной записи администратора»](#) на стр. 199) и какие-то учетные записи стали непригодными (например, в случае увольнения администратора), то их можно удалить.

Учетную запись можно удалить только в том случае, если она не является текущей. При необходимости можно удалить сразу несколько учетных записей.



Внимание! В текущей версии УКЦ учетную запись администратора не следует удалять до тех пор, пока не истечет срок действия всех его сертификатов открытого ключа подписи.



В противном случае обновление списков отозванных сертификатов (СОС), соответствующих действующим сертификатам подписи администратора, учетная запись которого была удалена, будет невозможно.

Чтобы удалить учетную запись администратора:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в разделе **Администраторы** выберите нужную учетную запись.
- 2 Щелкните выбранную запись правой кнопкой мыши и в контекстном меню выберите пункт **Удалить**.
- 3 В появившемся окне подтвердите удаление учетной записи.
- 4 Убедитесь, что учетная запись пропала из списка в разделе **Администраторы**.

Если у администратора, учетная запись которого была удалена, останется возможность доступа к программе, настоятельно рекомендуется сменить ключ защиты УКЦ (см. [«Смена ключа защиты УКЦ»](#) на стр. 218).

Смена текущей учетной записи администратора

Под текущей учетной записью администратора понимается учетная запись, под которой производился вход в программу ViPNet Удостоверяющий и ключевой центр при ее запуске (см. «[Запуск и завершение работы с программой](#)» на стр. 59) либо при смене текущей учетной записи непосредственно в самом сеансе работы с программой (см. ниже). Только одна учетная запись из имеющихся может являться текущей. Список зарегистрированных учетных записей администраторов содержится в разделе **Администраторы**, текущая учетная запись администратора в списке обозначена значком , остальные учетные записи — значком .

Если в УКЦ зарегистрировано несколько учетных записей администраторов, сменить текущую учетную запись (текущего администратора) можно, не выходя из программы. Для этого:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в разделе **Администраторы** выполните следующие действия:
 - В списке правой кнопкой мыши щелкните учетную запись, которую предполагается использовать в качестве текущей, и в контекстном меню выберите пункт **Назначить текущим**.
 - Дважды щелкните учетную запись, которую предполагается использовать в качестве текущей, после чего в появившемся окне **Свойства администратора** установите флажок **Назначить текущим** и нажмите кнопку **ОК** (см. [Просмотр и изменение данных об администраторе](#) (на стр. 206)).
- 2 В появившемся окне входа в программу введите пароль, соответствующий выбранной учетной записи, и нажмите кнопку **ОК**.

В результате произойдет смена текущей учетной записи администратора и все операции в программе будут осуществляться от имени администратора с текущей учетной записью.

Просмотр контейнера ключей администратора

При каждом издании сертификата администратора или создании запроса на сертификат к вышестоящему Удостоверяющему центру создается закрытый ключ, который помещается в специальный контейнер ключей. Контейнер ключей при этом сохраняется либо локально на компьютере (в заданной папке на диске), либо на внешнем устройстве хранения данных. Подробнее см. раздел [Обновление сертификата и закрытого ключа администратора](#) (на стр. 208).

В программе ViPNet Удостоверяющий и ключевой центр можно просмотреть подробную информацию о контейнере ключей администратора: имя и место хранения (путь к файлу контейнера ключей, если контейнер размещен в папке на компьютере) и его содержимое: серийный номер, алгоритм и дату создание закрытого ключа.

Внимание! Просмотреть информацию можно только о контейнере ключей:



- текущего администратора (см. [«Смена текущей учетной записи администратора»](#) на стр. 203);
 - закрытый ключ в котором соответствует текущему сертификату администратора.
-

Для просмотра контейнера ключей текущего администратора:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в разделе **Администраторы** дважды щелкните учетную запись текущего администратора.
- 2 В окне **Свойства администратора** перейдите на вкладку **Ключи** и нажмите кнопку **Свойства контейнера**.
- 3 В появившемся окне **Свойства контейнера ключей** ознакомьтесь с содержимым контейнера ключей.

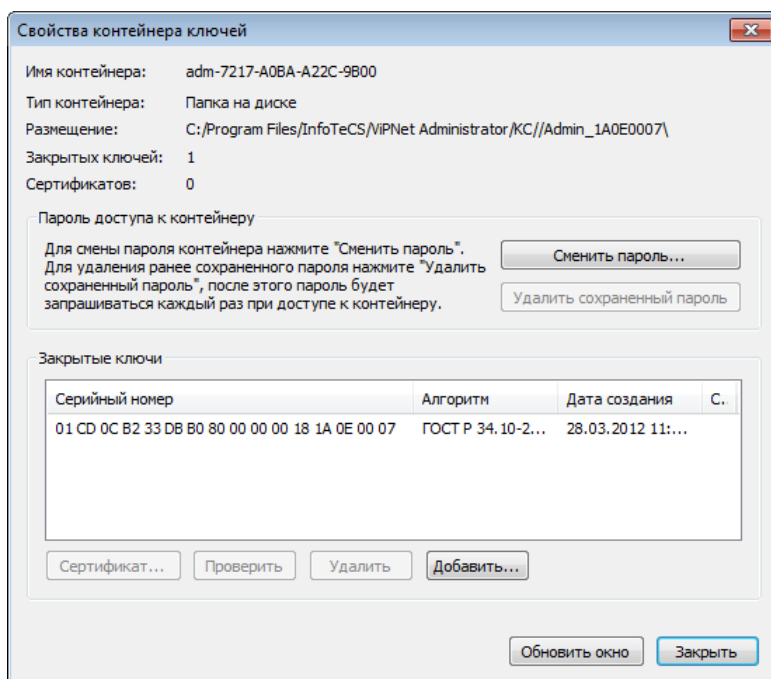


Рисунок 96: Информация о контейнере ключей администратора



Внимание! Не производите никаких действий в данном окне. Это запрещено регламентом работы Удостоверяющего центра.

Просмотр и изменение данных об администраторе

Можно просмотреть и изменить различную информацию об администраторах. Для этого в папке **Администраторы** установите указатель мыши на строку с администратором, информацию о котором Вы хотите посмотреть, и воспользуйтесь пунктом **Открыть** контекстного меню или дважды щелкните на строке в выбранном администратором.

Откроется окно **Свойства администратора**.

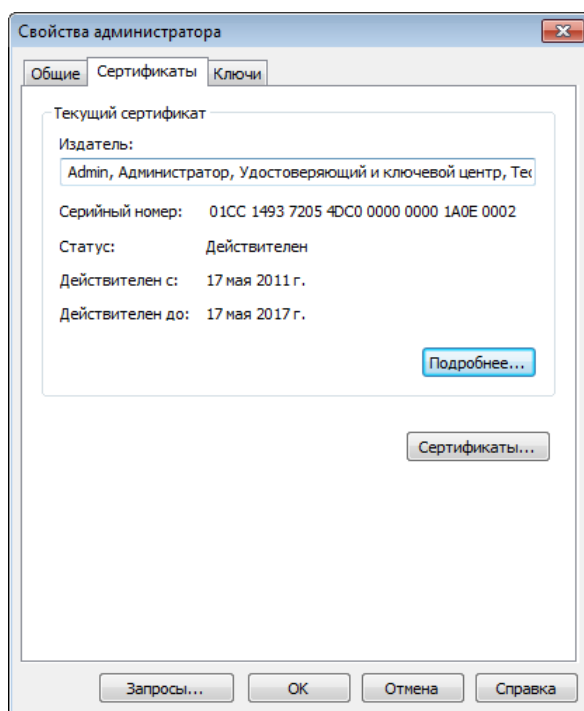


Рисунок 97: Свойства действующего администратора

В этом окне имеется 3 вкладки: **Общие**, **Сертификаты** и **Ключи**. Вкладки **Сертификаты** и **Ключи** могут отсутствовать, если:

- Открыты свойства администратора, который не является текущим.
- Лицензия накладывает ограничения на работу УКЦ в части Удостоверяющего центра.

На вкладке **Общие** отображаются имя и идентификатор администратора, является ли администратор текущим. Кнопка **Сменить пароль** предназначена для смены пароля администратора. Опция **Назначить текущим** будет активна и не включена для администратора, не являющегося текущим. При включении данной опции этот администратор становится текущим. Опция **Назначить текущим** будет неактивна и включена для текущего администратора.

На вкладке **Сертификаты** отображаются сведения о текущем сертификате (том сертификате, который действует в данный момент) администратора (издатель, серийный номер, статус, срок действия). Нажатие на кнопку **Подробнее** откроет окно **Сертификат**. Нажатие на кнопку **Сертификаты** откроет окно со списком сертификатов выбранного администратора (см. «[Выбор текущего сертификата администратора](#)» на стр. 216). Кнопка **Сертификаты** может отсутствовать при наличии лицензионных ограничений на работу УКЦ в части Удостоверяющего центра. Если администратор текущий и имеет несколько сертификатов, то из списка сертификатов можно выбрать сертификат, который будет являться текущим сертификатом. Для администратора, не являющегося текущим, можно только просмотреть список его сертификатов.

На вкладке **Ключи** указано место хранения ключей администратора (папка на диске или устройство). Нажатие на кнопку **Свойства контейнера** откроет окно **Свойства контейнера**.

В нижней части окна располагаются следующие кнопки: **Запросы**, **ОК**, **Отмена** и **Справка**.

Для просмотра информации о запросах на сертификат, сформированных к вышестоящему УЦ, нажмите кнопку **Запросы**.

Обновление сертификата и закрытого ключа администратора

Сертификат открытого ключа и закрытый ключ любого администратора программы ViPNet Удостоверяющий и ключевой центр имеют ограниченный срок действия, поэтому их требуется регулярно обновлять. Закрытый ключ формируется при создании сертификата администратора УКЦ, его срок действия зависит от заданного срока действия сертификата и не может превышать 1 год.

После истечения срока действия закрытый ключ администратора станет недействительным, и подписание сертификатов пользователей будет невозможно. Программа заблаговременно оповещает о приближении даты окончания действия закрытого ключа: за несколько дней до истечения срока действия программа выводит сообщение о количестве оставшихся дней, а также напоминание о необходимости обновить сертификат администратора. Время начала оповещений о скором окончании срока действия закрытого ключа зависит от настроек программы (см. [«Настройка параметров работы с сертификатами»](#) на стр. 253).



Внимание! Проверка срока действия закрытого ключа и (в случае необходимости) оповещения о его истечении выполняются только для текущего администратора УКЦ. Если в УКЦ зарегистрированы несколько администраторов, то проверить срок действия закрытого ключа конкретного администратора можно только при назначении этого администратора текущим.

При появлении оповещений рекомендуется создать новый сертификат администратора УКЦ, не дожидаясь окончания срока действия закрытого ключа.

Для издания нового сертификата администратора УКЦ выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр на левой панели выберите раздел **Администраторы**.
- 2 В разделе **Администраторы** выполните одно из действий:
 - Если текущий корневой сертификат издан администратором УКЦ, на правой панели щелкните текущего администратора правой кнопкой мыши, в контекстном меню выберите **Сертификат**, затем щелкните команду **Создать корневой сертификат**. Будет запущен **Мастер создания сертификата администратора сети ViPNet**.

- Если корневой сертификат издан вышестоящим Удостоверяющим центром, на правой панели щелкните текущего администратора правой кнопкой мыши, в контекстном меню выберите **Сертификат**, затем щелкните команду **Создать запрос к вышестоящему УЦ**. Будет запущен **Мастер создания запроса на сертификат в вышестоящий УЦ**.
- 3 На первой и второй страницах мастера укажите имя администратора и другие необходимые данные, которые впоследствии будут добавлены в его сертификат, и нажмите кнопку **Далее**.

Мастер создания сертификата администратора сети ViPNet

Владелец сертификата

Имя:
Гаврилов Виталий Леонидович

Должность:
Администратор

Подразделение:
Удостоверяющий и ключевой центр

Организация:
ООО «Ветка»

ИНН:
543454456546

ОГРН:

СНИЛС:
56567678888

< Назад Далее > Отмена Справка

Рисунок 98: Первая страница мастера создания сертификата администратора

- 4 На следующей странице мастера с помощью кнопки **Изменить** отредактируйте дополнительные сведения об администраторе и нажмите кнопку **Далее**.

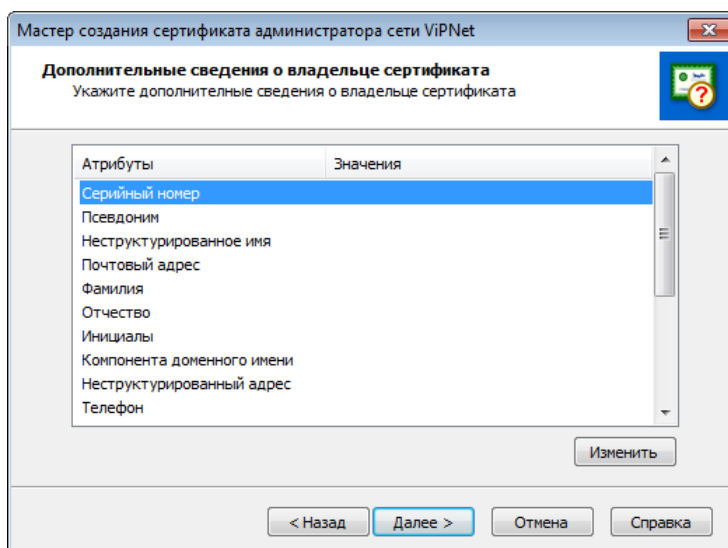


Рисунок 99: Дополнительные сведения об администраторе

- 5 На странице **Параметры ключа подписи** задайте параметры ключа подписи в соответствии с приведенной ниже таблицей:

Таблица 3. Характеристики алгоритма ГОСТ Р 34.10-2001

Алгоритм подписи	Описание	Параметры алгоритма	Описание параметров	Длина ключа
ГОСТ Р 34.10-2001	Новый стандарт электронной подписи, основанный на арифметике эллиптических кривых.	ГОСТ Р 34.10-2001	Параметры по умолчанию (рекомендуется). OID «1.2.643.2.2. 35.1»	512
	OID «1.2.643.2.2.19»	ГОСТ Р 34.10-2001	Параметры подписи 3 (в соответствии с RFC 4357 http://www.ietf.org/rfc/rfc4357.txt). OID «1.2.643.2.2. 35.3»	



Совет. Рекомендуется использовать параметры алгоритма, предлагаемые по умолчанию. Данные параметры характеризуются наибольшей скоростью вычисления и проверки подписи.

После этого нажмите кнопку **Далее**.

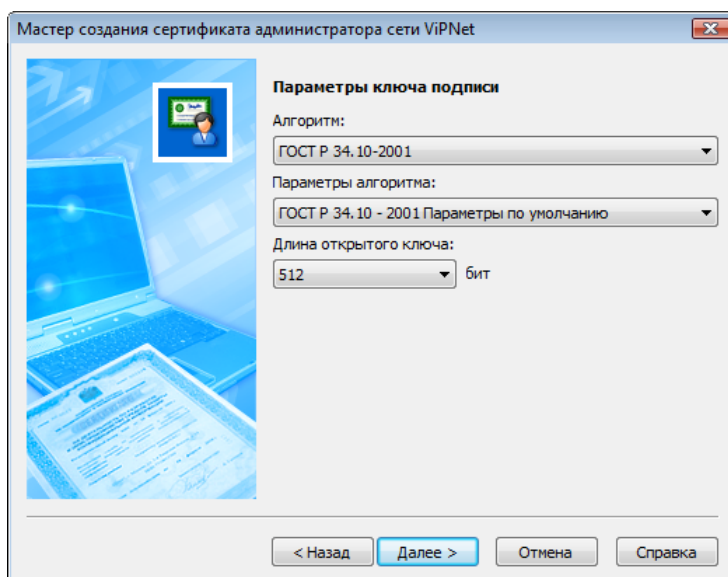


Рисунок 100: Параметры ключа подписи

- 6 На странице **Срок действия сертификата** задайте желаемый срок действия сертификата администратора, после чего нажмите кнопку **Далее**.



Примечание. При задании срока действия сертификата автоматически определяется срок действия закрытого ключа. Если срок действия сертификата задается меньше или равным 12 месяцам (1 году), то срок действия закрытого ключа будет равен заданному сроку действия сертификата. Если заданный срок действия сертификата больше 1 года, то срок действия закрытого ключа устанавливается равным 1 году. Только в этом случае при издании сертификата будет указан срок действия закрытого ключа (1 год).

Минимальный срок действия сертификата администратора составляет 1 месяц, максимальный — 6 лет. По умолчанию установлен срок действия 6 лет.

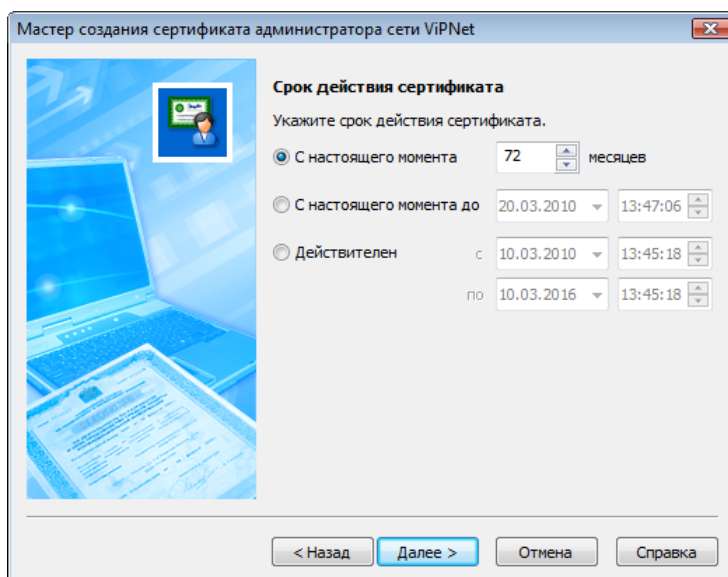


Рисунок 101: Срок действия сертификата

- 7 На странице **Назначение сертификата** укажите используемые расширения и нажмите кнопку **Далее**.

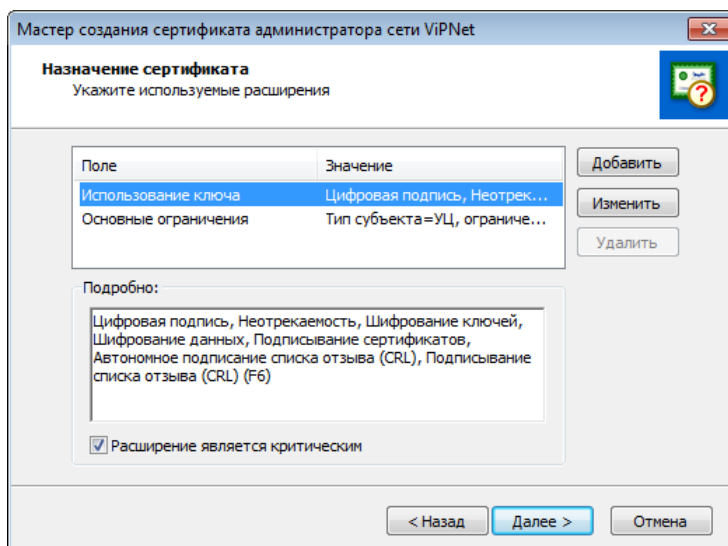


Рисунок 102: Указание назначения сертификата

- 8 На странице **Место хранения контейнера ключей** укажите место хранения контейнера ключей: **В файле** или **На внешнем устройстве**. Нажмите кнопку **Далее**.

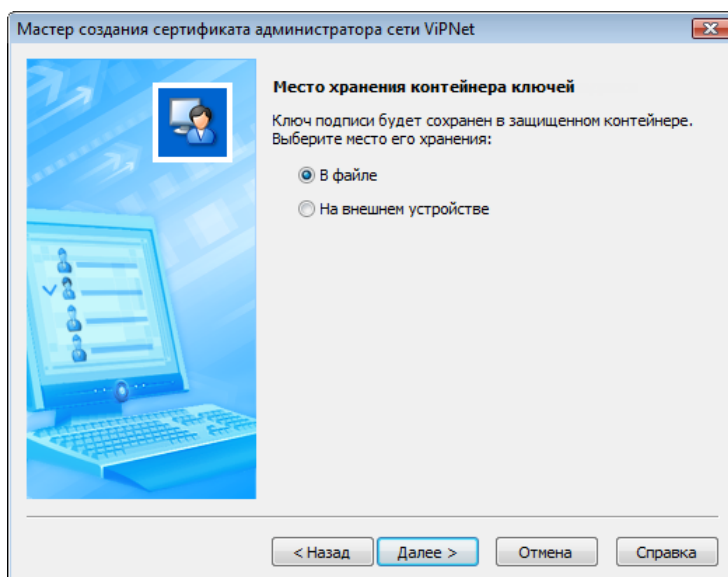


Рисунок 103: Выбор места хранения контейнера ключей

- 9 Если выбрано хранение ключа в файле, на странице **Папка хранения контейнера ключей** укажите папку для контейнера.

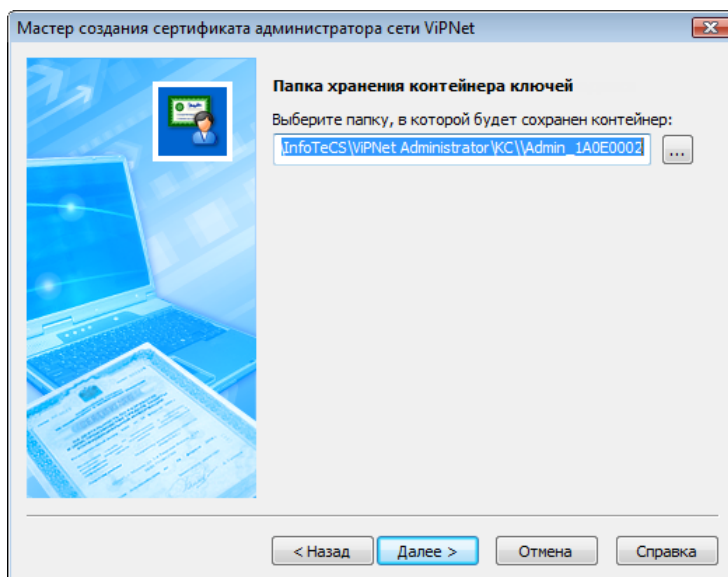


Рисунок 104: Выбор папки контейнера ключей

Если выбрано хранение ключа на внешнем устройстве, на странице **Место хранения контейнеров ключа подписи и ключа защиты УКЦ** выберите внешнее устройство хранения данных.

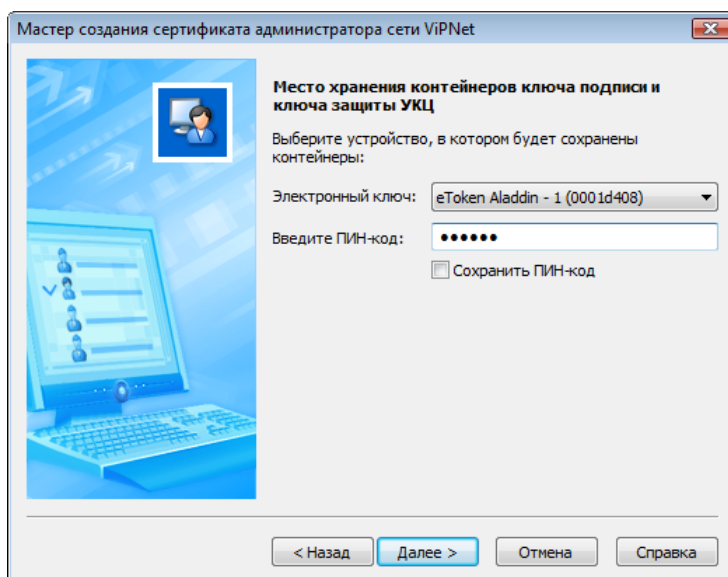


Рисунок 105: Выбор внешнего устройства

Нажмите кнопку **Далее**.

- 10 Если создается запрос в вышестоящий Удостоверяющий центр, на странице **Файл запроса на сертификат в вышестоящий УЦ** укажите путь и имя файла запроса.
- 11 На странице **Готовность к созданию корневого сертификата** (или **Готовность к созданию запроса на сертификат**) проверьте указанные параметры и нажмите кнопку **Далее**.
- 12 При появлении электронной рулетки поведите указателем в пределах окна.



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

- 13 Если издается корневой сертификат, на странице **Завершение создания корневого сертификата** будет выведено уведомление о создании корневого сертификата, справочников и обновлений ключевых наборов.

Если создается запрос в вышестоящий Удостоверяющий центр, на странице **Завершение создания запроса на сертификат** будет выведено уведомление о создании запроса. Созданный файл запроса нужно передать администратору вышестоящего Удостоверяющего центра. После издания этот сертификат нужно ввести в действие в УКЦ.

- 14 Нажмите кнопку **Готово**.

После издания сертификата администратора автоматически создаются обновления ключей узлов. Если сертификат администратора УКЦ был издан в вышестоящем Удостоверяющем центре и введен в действие в УКЦ, обновления ключей необходимо создать и отправить на сетевые узлы вручную (подробнее см. раздел [Создание обновлений ключей узлов](#) (на стр. 97)).

Если в УКЦ установлены доверительные отношения с каким-либо другим Удостоверяющим центром (на основе распределенной модели), то после обновления сертификата администратора УКЦ требуется также обновить кросс-сертификат администратора УКЦ. Для этого необходимо создать запрос на новый кросс-сертификат и передать файл с созданным запросом администратору Удостоверяющего центра, с которым установлены доверительные отношения (подробнее см. раздел [Создание запроса на кросс-сертификат к вышестоящему удостоверяющему центру](#) (на стр. 221)). По этому запросу администратор данного Удостоверяющего центра издаст новый кросс-сертификат.

Выбор текущего сертификата администратора

Для каждого текущего администратора можно выбрать сертификат, который будет текущим, то есть будет использоваться для подписи и заверения различных данных УКЦ. Для этого нужно открыть окно **Свойства администратора** (см. «[Просмотр и изменение данных об администраторе](#)» на стр. 206) для текущего администратора (выбрав пункт контекстного меню **Открыть**) и нажать кнопку **Сертификаты**, откроется окно со списком сертификатов этого текущего администратора. Если администратор текущий и имеет несколько сертификатов, то из списка сертификатов можно выбрать сертификат, который будет являться текущим сертификатом. Для администратора, не являющегося текущим, можно только просмотреть список его сертификатов.

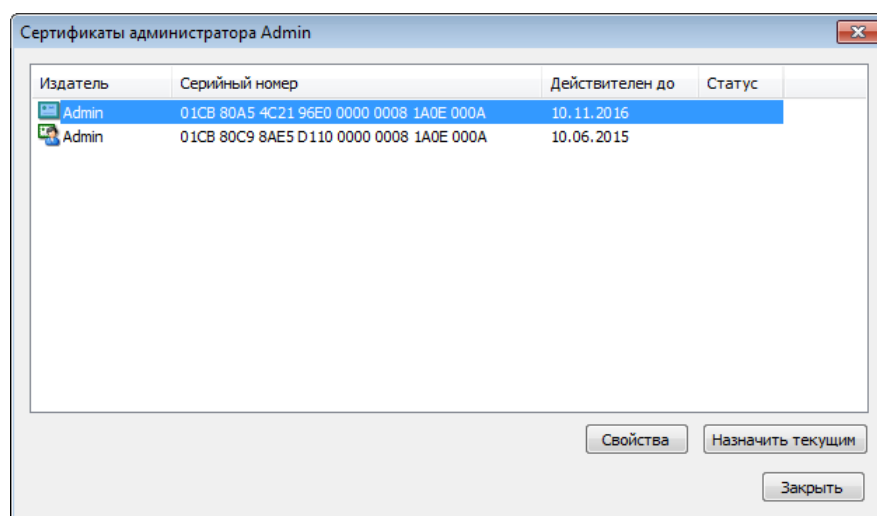


Рисунок 106: Просмотр сертификатов текущего администратора

В этом окне можно просмотреть каждый сертификат с помощью кнопки **Свойства**.

Для выбора текущего сертификата текущего администратора установите курсор на нужный сертификат и нажмите кнопку **Назначить текущим**. Сертификат будет выбран текущим для данного администратора, и информация об этом отобразится в окне **Свойства администратора**. Кнопка **Назначить текущим** будет активна только для сертификата, не являющегося текущим.

Смена пароля администратора

Для дополнительной безопасности текущий администратор имеет возможность в любой момент сменить свой пароль. Для этого нужно в окне **Свойства администратора** на вкладке **Общие** нажать кнопку **Сменить пароль**, после чего откроется окно для задания пароля.

Окно Пароль администратора

При нажатии на кнопку **Сменить пароль** на вкладке **Общие** свойств администратора (см. Рисунок 97 на стр. 206) откроется окно для создания нового пароля администратора.

В этом окне для смены пароля администратора нужно сначала задать тип пароля. Если выбран собственный тип пароля, то нужно ввести пароль и подтвердить его (пароль должен быть не менее 6 символов). Если выбран тип пароля случайный или случайный цифровой, то сначала запустится электронная рулетка (см. Рисунок 27 на стр. 55), если она еще не запускалась в этом сеансе работы программы УКЦ, а потом в окне появится пароль (при выборе случайного пароля на основе парольной фразы будет дана еще и парольная фраза для запоминания пароля). Для создания другого случайного или случайного цифрового пароля можно воспользоваться кнопкой **Другой**. Для случайного пароля на основе парольной фразы можно изменить параметры случайного пароля, воспользовавшись кнопкой **Свойства**. Для случайного цифрового можно задать количество цифр.

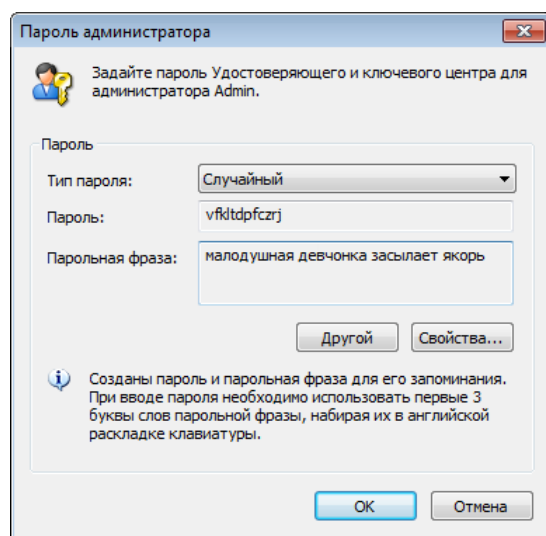


Рисунок 107: Изменение пароля администратора

Смена ключа защиты УКЦ

Ключ защиты УКЦ используется для шифрования других ключей, создаваемых в УКЦ.



Совет. Рекомендуется проводить плановую смену ключа защиты УКЦ не реже одного раза в год.

Также рекомендуется сменить ключ защиты УКЦ после удаления администратора УКЦ.

Для смены ключа защиты УКЦ выполните следующие действия:

- В папке **Администраторы** выберите строку с именем текущего администратора и воспользуйтесь контекстным меню **Сменить > Ключ защиты УКЦ**.
Появится сообщение для подтверждения смены ключа защиты УКЦ.
 - Для смены ключа нажмите **Да** в окне подтверждения. Ключ защиты УКЦ будет сменен.
-



Внимание! После смены ключа защиты следует обеспечить ввод пароля в УКЦ всех администраторов УКЦ, если их несколько. Это нужно для того, чтобы все администраторы УКЦ имели доступ к новому ключу защиты. При вводе пароля администратора ключ защиты будет зашифрован на персональном ключе каждого администратора. Для этого назначьте текущим поочередно каждого администратора при помощи контекстного меню **Назначить текущим** (см. «Смена текущей учетной записи администратора» на стр. 203).

Смена ключевого носителя администратора

При необходимости возможна смена места хранения закрытого ключа администратора УКЦ.

Чтобы сменить место хранения выполните следующие действия:

- В папке **Администраторы** выберите строку с именем текущего администратора и воспользуйтесь контекстным меню **Сменить > Ключевой носитель**.

Откроется окно ввода пароля администратора УКЦ.

- Введите пароль и нажмите **ОК**. Откроется окно для указания места сохранения контейнера ключей.

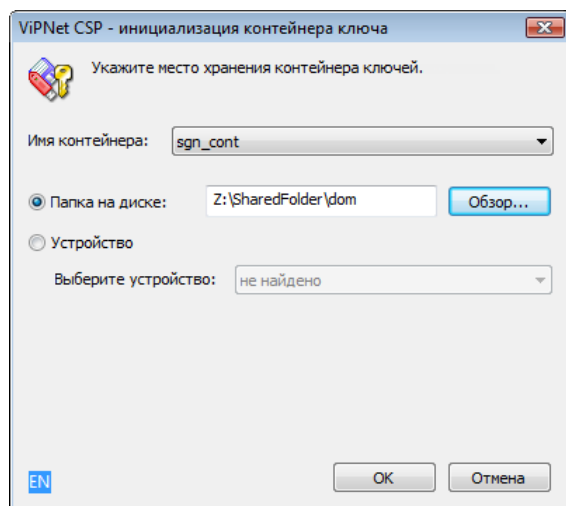


Рисунок 108: Инициализация контейнера ключа из папки

- В этом окне укажите место хранения контейнера ключей: папку на диске, используя кнопку **Обзор**, или устройство с указанием его параметров и при необходимости ПИН-кода (если ПИН-код не был сохранен ранее). Если выбрано устройство, то обеспечьте контакт ключа с внешним устройством хранения данных (информацию о внешних устройствах и особенностях работы с ними см. в [Информация о внешних устройствах хранения данных](#) (на стр. 35)).
- Нажмите **ОК**. Контейнер будет перенесен, о чем появится соответствующее сообщение.

Создание запроса на кросс-сертификат к вышестоящему УЦ и установка изданного сертификата в иерархической системе доверительных отношений

Если свой УКЦ является подчиненным, то для построения иерархической системы доверительных отношений с другими УЦ следует выполнить следующие действия в своем (подчиненном) УКЦ:

- 1 Создать запрос на кросс-сертификат администратора к вышестоящему (или головному) УЦ (см. [«Создание запроса на кросс-сертификат к вышестоящему УЦ и установка изданного сертификата в иерархической системе доверительных отношений»](#) на стр. 220) и передать его каким-либо защищенным способом администратору этого УЦ для издания кросс-сертификата.
- 2 После получения изданного в вышестоящем УЦ кросс-сертификата ввести его в действие в своем УКЦ (см. [«Ввод в действие кросс-сертификата, изданного в вышестоящем УЦ»](#) на стр. 224).



Примечание. Если не импортирован справочник сертификатов администраторов вышестоящего УЦ, то перед вводом в действие кросс-сертификата необходимо произвести его импорт (см. [«Импорт сертификатов администраторов вышестоящего УЦ»](#) на стр. 226).

Создание запроса на кросс-сертификат к вышестоящему удостоверяющему центру

Для создания запроса на кросс-сертификат текущего администратора в вышестоящий Удостоверяющий центр выполните следующие действия:

- В папке **Администраторы** выберите строку с именем текущего администратора и воспользуйтесь контекстным меню **Сертификат > Создать запрос к вышестоящему УЦ**.

Запустится мастер создания сертификата администратора (см. Рисунок 98 на стр. 209).

- Заполните сведения о владельце сертификата, то есть сведения об администраторе. В поле **Имя** уже подставлено имя администратора, но его можно отредактировать. Если нужно использовать имя в качестве псевдонима, то установите флажок **Использовать имя в качестве псевдонима**. Имя является обязательным полем, которое должно быть задано. Далее можно заполнить поля по желанию. Можно задать, дополнительно неструктурированное имя в поле с одноименным названием (можно задать любые символы, длина поля ограничена 255 символами).
- Для продолжения нажмите кнопку **Далее**, откроется следующая страница **Владелец сертификата**, где можно заполнить сведения о местонахождении владельца сертификата.

Поля являются необязательными, поэтому их можно заполнить по желанию. Введите необходимые данные.

- Нажмите кнопку **Далее**. Откроется следующая страница **Параметры ключа подписи** (см. Рисунок 100 на стр. 211) для выбора параметров ключа подписи.

По умолчанию в этом окне уже заданы рекомендуемые параметры ключа подписи: алгоритм, параметры алгоритма и длина открытого ключа. Если требуется изменить параметры.

- Нажмите кнопку **Далее**. Откроется следующая страница **Срок действия сертификата** (см. Рисунок 101 на стр. 212) для указания срока действия запрашиваемого сертификата.

Укажите желаемый срок действия сертификата администратора, установив переключатель в одно из трех положений. По умолчанию срок действия сертификата администратора составляет 6 лет и является максимальным сроком действия. Минимальный срок действия составляет 1 месяц. Воспользуйтесь одним из следующих способов задания срока действия сертификата:

- **С настоящего момента** – указывается продолжительность срока действия в месяцах с данного момента времени.

- **С настоящего момента до** – указываются дата и время окончания срока действия сертификата.
- **Действителен** – указываются дата и время начала и окончания срока действия сертификата (выбрано по умолчанию).
- Для продолжения нажмите кнопку **Далее**. Откроется страница **Назначение сертификата** (см. Рисунок 102 на стр. 212). Чтобы добавить расширенное использование ключа или политику сертификата, нажмите кнопку **Добавить**. В окне **Допустимые расширения** выберите тип расширения и нажмите **ОК**. Откроется окно для добавления соответствующих расширений.
- Для продолжения нажмите кнопку **Далее**. Откроется следующая страница **Место хранения контейнера ключей** (см. Рисунок 103 на стр. 213).

Ключ подписи будут сохранен в защищенном контейнере. Выберите тип контейнера — файл или внешнее устройство хранения данных.
- После выбора нажмите кнопку **Далее**. Откроется следующая страница мастера. На данной странице укажите место хранения контейнера:
 - Если на предыдущем шаге был выбран тип контейнера **В файле**, то укажите папку на диске.
 - Если на предыдущем шаге был выбран тип контейнера **На внешнем устройстве**, то:
 - Обеспечьте контакт ключа с устройством.
 - Выберите электронный ключ, если его значение не подставилось автоматически.
 - Если запрашивается ПИН-код, то введите его. Если следует сохранить ПИН-код для последующих запусков, то установите флажок **Сохранить ПИН-код**.



Примечание. Если устройство не было отформатировано ранее, то может быть отображено окно с предложением отформатировать устройство. В этом случае согласитесь с предложением, и дождитесь окончания форматирования.

Подробную информацию о поддерживаемых внешних устройствах хранения данных и особенностях работы с ними читайте в разделе [Информация о внешних устройствах хранения данных](#) (на стр. 35).

- Для продолжения нажмите кнопку **Далее**. Откроется страница мастера для указания места создания файла с запросом на сертификат.

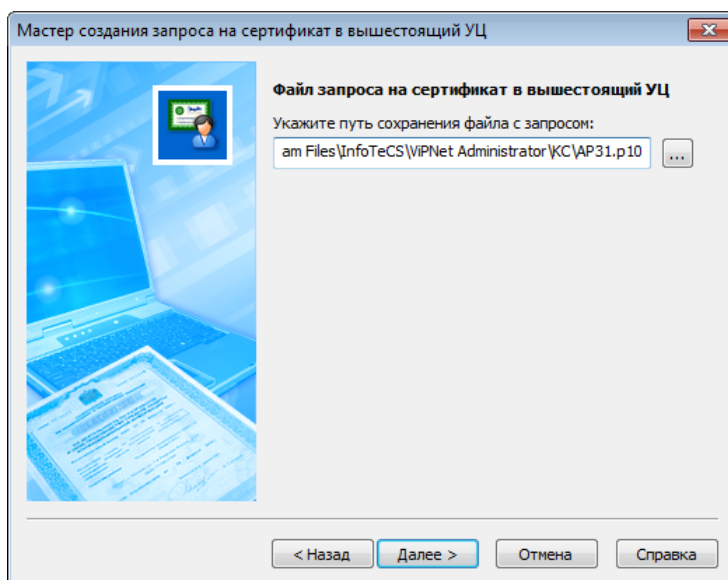


Рисунок 109: Указание места хранения файла с запросом

- Укажите путь сохранения файла с запросом. Запрос сохраняется в файле формата PKCS#10 (файл с расширением .p10).
- Нажмите кнопку **Далее**. Откроется страница **Готовность к созданию сертификата для проверки введенных данных**.

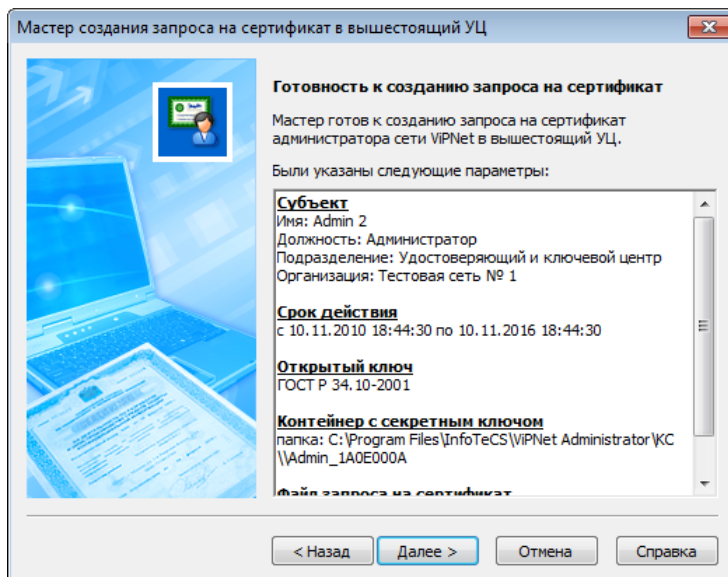


Рисунок 110: Обзор параметров перед созданием запроса

- Проверьте указанные данные и нажмите кнопку **Далее**, откроется завершающая страница мастера и запустится процесс создания запроса на сертификат администратора.

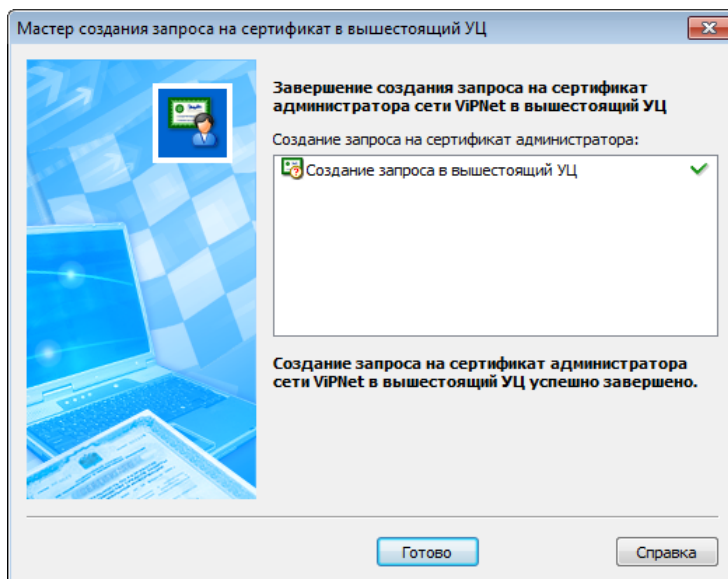



Рисунок 111: Завершение создания запроса на сертификат

По завершении процесса создания запроса на сертификат в окне отобразится статус выполненных действий. Если запрос сформировался, то все действия будут помечены значком  и станет доступна кнопка **Готово**.

- Для завершения работы мастера нажмите кнопку **Готово**. Сформированный файл с запросом (файл с расширением .p10) каким-либо защищенным способом передайте администратору вышестоящего УЦ.

После издания сертификата в вышестоящем УЦ и передаче его в подчиненный УКЦ, сертификат необходимо ввести в действие в своем УКЦ (см. [«Ввод в действие кросс-сертификата, изданного в вышестоящем УЦ»](#) на стр. 224).

Ввод в действие кросс-сертификата, изданного в вышестоящем УЦ

Изданный в вышестоящем УЦ сертификат администратора следует ввести в действие (импортировать) в своем УКЦ.



Внимание! Наряду с импортом самого сертификата осуществляется импорт цепочки сертификатов вышестоящего УЦ–издателя. Поэтому перед тем, как

вводить в действие изданный в вышестоящем УЦ сертификат администратора убедитесь, что импортирован справочник сертификатов администраторов вышестоящего УЦ. До осуществления импорта справочника сертификатов администраторов вышестоящего УЦ импортированный сертификат администратора не является достоверным и не может использоваться администратором в своем УКЦ. Импортированные сертификаты администраторов других сетей отображаются в папке **Удостоверяющий центр > Сертификаты администраторов > Доверенные сети ViPNet > Текущие** (см. раздел [Просмотр сертификатов](#) (на стр. 182)). Если справочник сертификатов администраторов вышестоящего УЦ не импортирован, то необходимо произвести его импорт (см. раздел [Импорт сертификатов администраторов вышестоящего УЦ](#) (на стр. 226)).

Для введения в действие (импорта) изданного в вышестоящем УЦ сертификата администратора выполните следующие действия:

- В папке **Администраторы** выберите строку с именем администратора, для которого был издан кросс-сертификат, и воспользуйтесь контекстным меню **Сертификат > Установить изданный сертификат**.



Внимание! Проверьте, что этот администратор является текущим (см. «[Смена текущей учетной записи администратора](#)» на стр. 203).

Откроется окно для выбора файла с изданным кросс-сертификатом.

- Укажите путь к файлу с сертификатом (с расширением `.p7b`, `.cer` или `.crt`), переданному из вышестоящего УЦ, и нажмите **Открыть**. После успешной проверки содержимого файла с сертификатом откроется окно **Импорт сертификатов, изданных по запросу**.

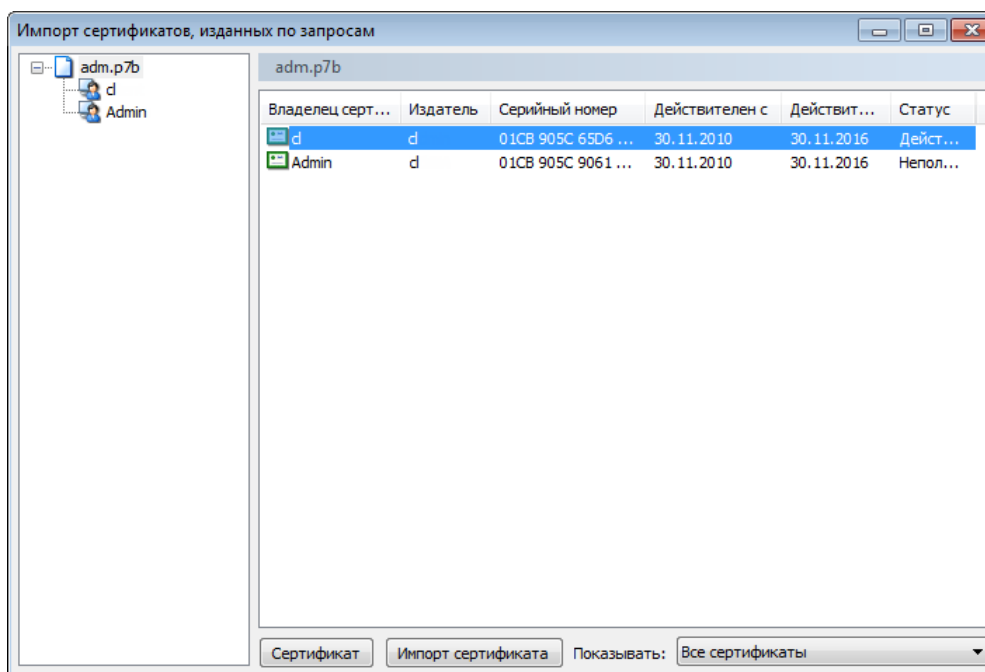


Рисунок 112: Импорт кросс-сертификата

В этом окне перед тем, как импортировать необходимо, просмотреть, проверить и подтвердить (при помощи кнопки **Сертификат**) каждый сертификат из цепочки сертификатов УЦ-издателя (сертификаты в бумажном виде должны быть переданы некоторым защищенным способом).

- Для ввода кросс-сертификата в действие выберите сертификат и нажмите кнопку **Импорт сертификата**. Если импорт произошел успешно, то появится соответствующее сообщение. С этого момента кросс-сертификат считается введенным в действие и становится текущим для администратора, информация о новом сертификате отобразится в окне **Свойства администратора** на вкладке **Сертификаты**.

Импорт сертификатов администраторов вышестоящего УЦ

Если не импортирован справочник сертификатов администраторов вышестоящего УЦ, то перед вводом в действие кросс-сертификата необходимо произвести его импорт.

Для импорта в главном меню программы выберите **Сервис > Импорт > Сертификатов администраторов других сетей** и укажите папку, где лежит справочник сертификатов администраторов другой сети. Откроется окно **Импорт сертификатов администраторов других сетей**. Произведите импорт (см. «[Импорт сертификатов администраторов доверенных сетей ViPNet](#)» на стр. 162).



Примечание. Произвести импорт сертификатов можно и при помощи контекстного меню. В папке **Администраторы** выберите строку с именем текущего администратора и воспользуйтесь контекстным меню **Сертификат > Открыть**.

Просмотр истории запросов на сертификат, сформированных к вышестоящему УЦ

Для просмотра истории запросов на сертификат, сформированных к вышестоящему УЦ, выполните следующие действия:

- В папке **Администраторы** выберите строку с именем текущего администратора и воспользуйтесь контекстным меню **Открыть**. Откроется окно **Свойства администратора** (см. Рисунок 97 на стр. 206).
- В окне **Свойства администратора** нажмите кнопку **Запросы**. Откроется окно **Запросы на сертификаты администратора к вышестоящему УЦ** со списком всех сформированных текущим администратором запросов.

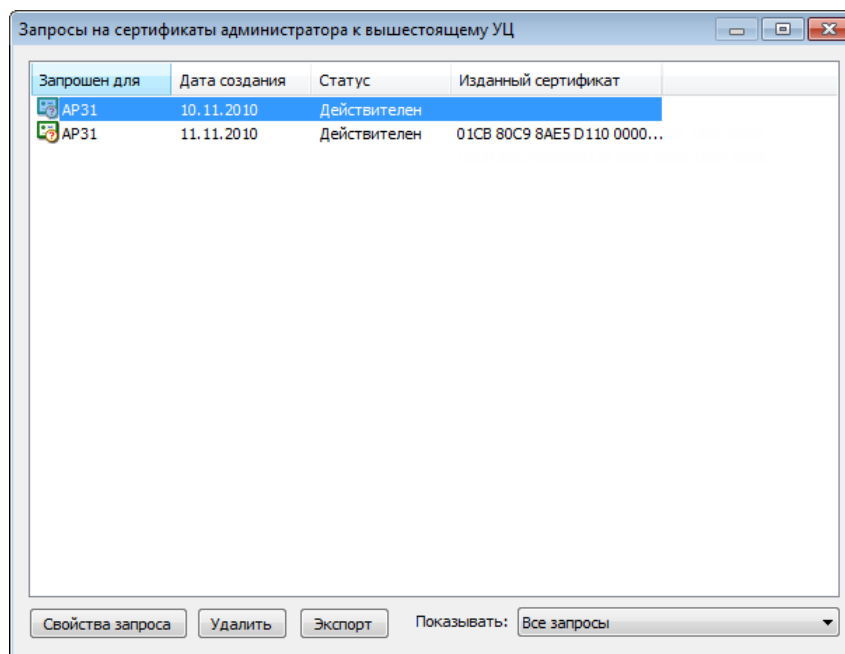


Рисунок 113: Просмотр запросов на издание сертификатов

В этом окне отображается список сформированных запросов на кросс-сертификат к вышестоящему УЦ. Для каждого запроса отображается следующая информация:

- Кем сделан запрос (в колонке **Запрос для**).
 - Дата создания запроса (в колонке **Дата создания**).
 - Статус запроса — действителен или недействителен (в колонке **Статус**).
 - Введен ли в действие изданный по данному запросу кросс-сертификат (в колонке **Изданный сертификат**). Если сертификат введен в действие, то в колонке отображается серийный номер сертификата.
- Для просмотра свойств запроса выберите запрос и нажмите кнопку **Свойства запроса** (см. [Просмотр свойств запроса \(окно Запрос на издание сертификата\)](#) (на стр. 228)).
 - Для экспорта в файл формата PKCS#10 (с расширением .p10) выберите запрос и нажмите кнопку **Экспорт**.
 - Если требуется удалить запрос, то выберите запрос и нажмите кнопку **Удалить**.

Просмотр свойств запроса (окно Запрос на издание сертификата)

Окно **Запрос на издание сертификата** содержит информацию об администраторе, создавшем запрос, открытом ключе, назначении сертификата, а также информацию об изданном в вышестоящем УЦ сертификате.

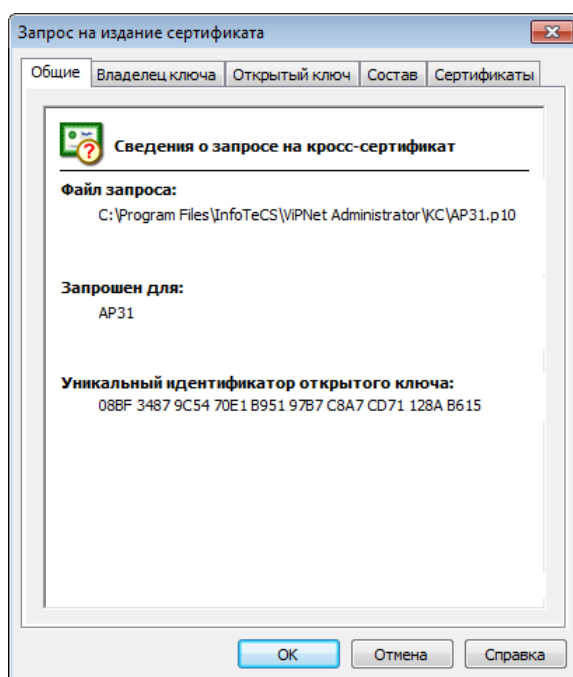


Рисунок 114: Общие свойства запроса на сертификат

Окно **Запрос на издание сертификата** содержит следующие вкладки:

- Вкладка **Общие** содержит сведения о запросе на сертификат.
- Вкладка **Владелец ключа** содержит данные администратора, создавшего запрос.
- Вкладка **Открытый ключ** содержит сведения об алгоритме и длине ключа.
- Вкладка **Состав** отображает все назначения сертификата.
- Вкладка **Сертификаты** отображает текущий сертификат, если он есть, а также список всех изданных для администратора сертификатов.

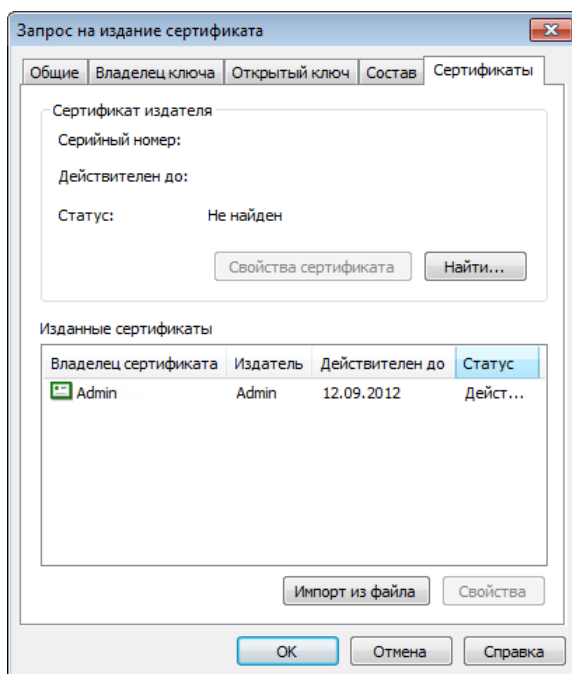


Рисунок 115: Просмотр изданных сертификатов

В этом окне можно выполнить следующие действия:

- Просмотреть свойства текущего сертификата при помощи кнопки **Свойства сертификата** (см. раздел [Окно Сертификат](#)).
- Если текущий сертификат не найден, то можно выбрать его при помощи кнопки **Найти**.
- Если из вышестоящего УЦ был передан файл с изданным сертификатом, то его можете импортировать при помощи кнопки **Импорт из файла** (откроется окно **Импорт сертификатов**, изданных по запросу (см. «[Ввод в действие кросс-сертификата, изданного в вышестоящем УЦ](#)» на стр. 224)).
- Просмотреть свойства изданных сертификатов при помощи кнопки **Свойства**.

Создание запроса на кросс-сертификат к другому УЦ в распределенной системе доверительных отношений

Для построения распределенной системы доверительных отношений между УЦ следует в своем УКЦ создать запрос на кросс-сертификат администратора и передать его каким-либо защищенным способом администратору другого УЦ (с кем устанавливаются доверительные отношения) для издания кросс-сертификата.

Создание запроса на кросс-сертификат и отправка его в другой УЦ

Для создания запроса на кросс-сертификат текущего администратора в папке Администраторы воспользуйтесь контекстным меню **Сертификат > Создать запрос на кросс-сертификат**. Будет запущен **Мастер создания запроса на кросс-сертификат**.

На странице **Сертификат администратора** укажите сертификат, для которого требуется создать запрос на кросс-сертификат.

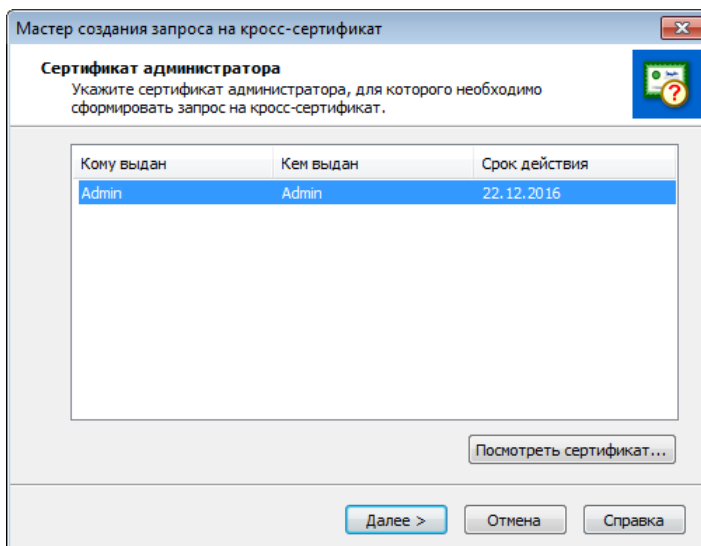


Рисунок 116: Выбор сертификата администратора

Выберите сертификат и нажмите **Далее**, откроется окно **Назначение кросс-сертификата**.

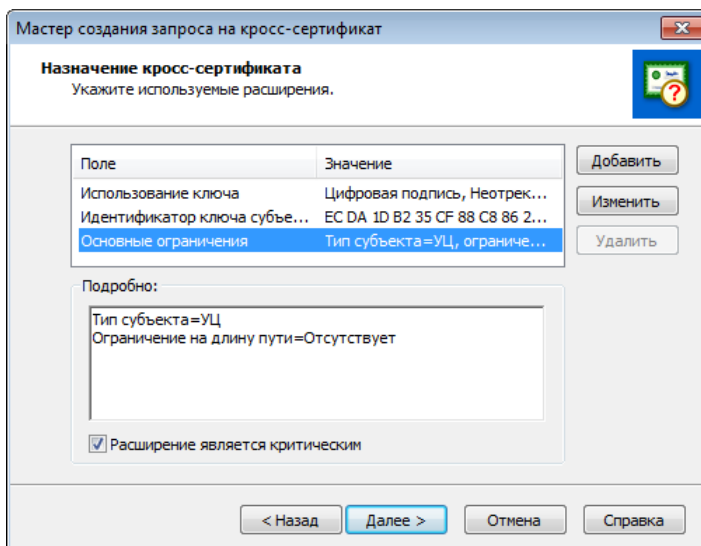


Рисунок 117: Назначение сертификата

В данном окне перед созданием запроса на кросс-сертификат можно выполнить следующие действия:

- Редактирование длины пути для цепочки сертификатов. Для этого в верхней части окна выберите **Основные ограничения** и нажмите кнопку **Изменить**. Откроется

окно **Основные ограничения**, в котором установите флажок **Ограничение на длину пути** (значения 0-255) и задайте длину пути. Нажмите **ОК**.

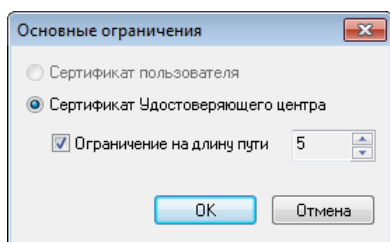


Рисунок 118: Указание основных ограничений

Заданное значение, появится в поле **Ограничение на длину пути**=<заданное значение>. При снятии флажка **Ограничение на длину пути** ограничения снимаются, и значение **Ограничение на длину пути** будет равно **Отсутствует**.



Внимание! Если в исходном сертификате была задана длина цепочки, то при создании запроса на кросс-сертификат возможно задание длины цепочки, не больше длины цепочки исходного сертификата (то есть можно изменить длину только на меньшую).

- Изменение списка функций использования ключа. Для этого нужно выбрать позицию **Использование ключа**. В нижней части окна отобразятся названия функций использования ключа.

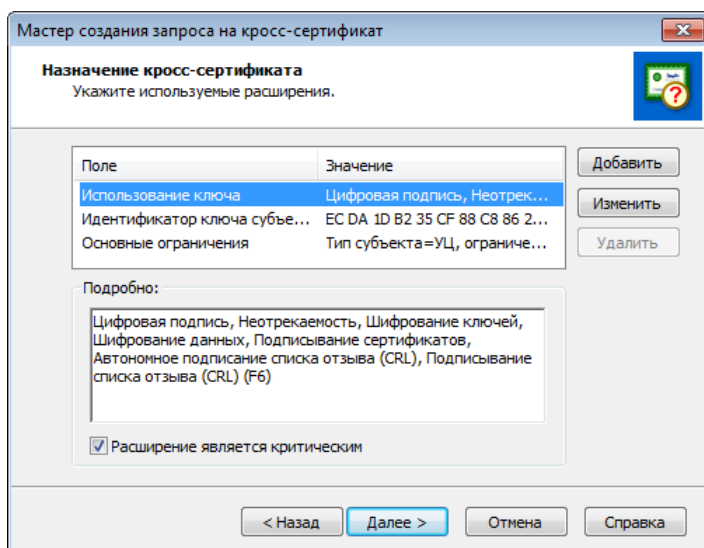


Рисунок 119: Использование ключа сертификата

Для изменения списка функций нажмите кнопку **Изменить**. Откроется окно **Использование ключа**.

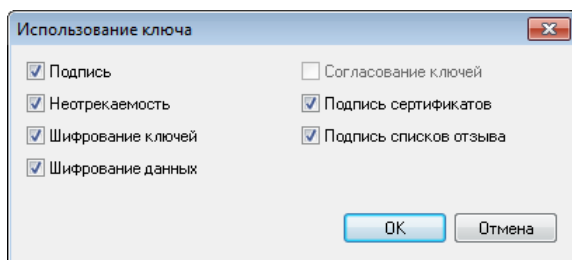


Рисунок 120: Настройка параметров использования ключа

В этом окне можно добавить (удалить) функции, установив (сняв) соответствующие флажки. После изменений нажмите **ОК** и список функций в окне **Назначение кросс-сертификата** изменится.



Внимание! Хотя бы одна функция должна быть выбрана, то есть нельзя удалить все функции использования ключа: в этом случае кнопка **ОК** будет недоступна.

- Добавление расширения. Для добавления расширения в окне **Назначение кросс-сертификата** нажмите кнопку **Добавить**. Откроется окно **Допустимые расширения**.

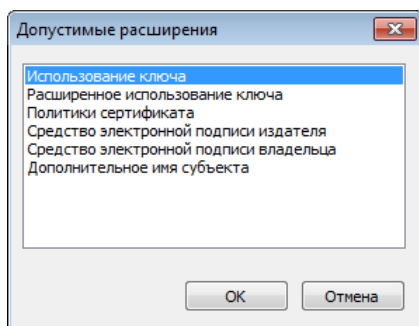


Рисунок 121: Выбор допустимого расширения

Выберите допустимое расширение (например, **Расширенное использование ключа** или **Политики сертификата**) и нажмите **ОК**. Откроется окно, соответствующее выбранному допустимому расширению, например, **Расширенное использование ключа**. Первоначально список выбранных расширений в окне пуст (в исходном сертификате нет никаких добавлений).

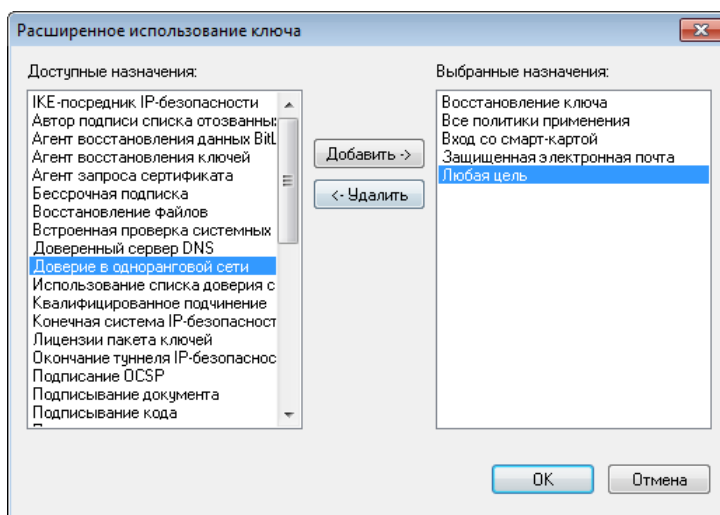


Рисунок 122: Выбор назначений расширенного использования ключа

В этом окне с помощью кнопок **Добавить** и **Удалить** добавьте или удалите назначения ключа, которые необходимы.



Внимание! Если уже было добавлено несколько назначений ключа, то нельзя будет удалить все выбранные значения расширенного использования ключа: если останется одно значение, то кнопка **ОК** будет недоступна. Для удаления всех выбранных значений нужно воспользоваться кнопкой **Удалить** (кнопка станет доступной, если выбрать добавленное расширение) в окне **Назначение кросс-сертификата**.

После добавления назначений ключа нажмите **ОК**. Расширения использования ключа появятся в окне **Назначение кросс-сертификата**.

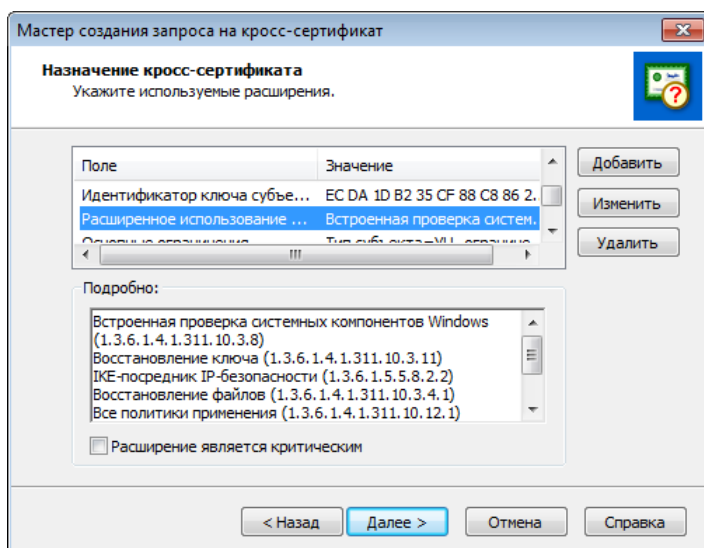


Рисунок 123: Результат добавления нового назначения сертификата

В окне **Назначение кросс-сертификата** можно установить (снять) флажок **Расширение является критическим**, если это необходимо. Если флажок установлен, то расширение будет помечено, как критическое. Это означает, если прикладное ПО не может обработать такое расширение, то сертификат признается недействительным. Для некритических расширений в этом случае расширение игнорируется.

Кнопка **Вернуть** отменяет сделанные изменения (добавления) в окне **Назначение кросс-сертификата**. Кнопка **Отмена** отменяет создание кросс-сертификата.

По завершении настроек в окне **Назначение кросс-сертификата** нажмите кнопку **Далее**. На странице **Файл запроса** задайте путь и имя файла запроса (с расширением `.p10`), затем нажмите кнопку **Готово**. В указанной папке будет создан файл запроса на кросс-сертификат.

Сформированный файл с запросом (файл с расширением `.p10`) каким-либо защищенным способом передайте администратору другого УЦ (с кем устанавливаются доверительные отношения) для издания кросс-сертификата.

Администратор другого УЦ по запросу издаст кросс-сертификат. Для установки доверительных отношений администратор другого УЦ должен сформировать и передать в данный УЦ свой запрос на кросс-сертификат. По этому запросу в данном УЦ должен быть издан кросс-сертификат (см. «[Обработка запросов на кросс-сертификаты \(в том числе запросов на сертификаты из подчиненных УЦ\)](#)» на стр. 169). С этого момента доверительные отношения между двумя УЦ установлены.



Примечание. Если доверительные отношения устанавливаются по так называемой «мостовой схеме», то изданные в «мостовом» УЦ сертификаты,

необходимо импортировать в остальных УЦ, участвующих в схеме. Это можно сделать при помощи главного меню **Сервис > Импорт > Сертификатов администраторов других сетей** (см. раздел [Импорт сертификатов администраторов вышестоящего УЦ](#) (на стр. 226)). После импорта эти сертификаты отобразятся в папке **Удостоверяющий центр > Сертификаты администраторов > Кросс-сертификаты > Импортированные**.



Настройка программы ViPNet Удостоверяющий и ключевой центр

Настройка папок обмена	239
Настройка типа создаваемых паролей	242
Настройка паролей администраторов	245
Настройка параметров создания резервных наборов персональных ключей	247
Настройка параметров издания сертификатов и обработки запросов	250
Настройка параметров работы с сертификатами	253
Создание и редактирование шаблонов сертификатов	256
Настройка параметров работы со списками отозванных сертификатов	264
Настройка списка политик применения сертификата	268
Настройка параметров публикации данных	271


Настройка папок обмена

Взаимодействие программы ViPNet Удостоверяющий и ключевой центр с программой ViPNet Центр управления сетью, в процессе которого происходит автоматический обмен необходимой информацией, осуществляется при помощи папок на диске (или сетевых папок). Для организации данного взаимодействия в ЦУСе и УКЦ требуется настроить соответствующие папки обмена.



Примечание. Настройка папок обмена требуется в том случае, если УКЦ и ЦУС были установлены на разные компьютеры (см. «[Установка программы](#)» на стр. 48). При установке программ на один компьютер папки обмена назначаются автоматически, и не рекомендуется их изменять.

Обычно папки обмена настраиваются в процессе первичной инициализации программы (см. «[Проведение первичной инициализации программы](#)» на стр. 50), но при необходимости их также можно настроить уже в процессе работы с УКЦ. Для настройки папок обмена в УКЦ выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Папки ViPNet Администратора**.

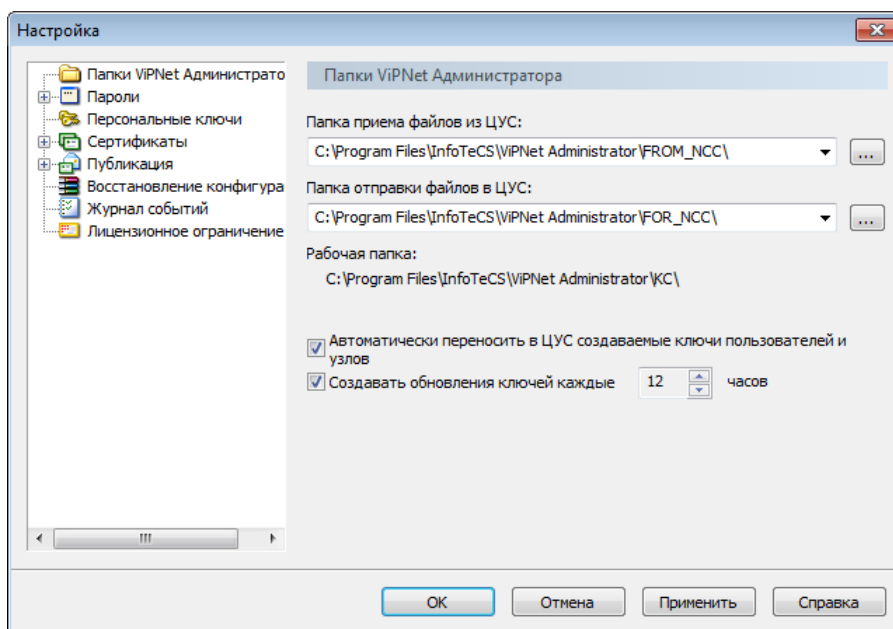


Рисунок 124: Настройки параметров программы

3 В разделе **Папки VIPNet Администратора** с помощью кнопок  укажите нужные папки обмена:

- В поле **Папка приема файлов из ЦУС** — папку, в которой будут находиться файлы, обработанные в ЦУСе. По умолчанию используется папка: \VIPNet Administrator\FROM_NCC.
- В поле **Папка отправки файлов в ЦУС** — папку, в которой будут находиться файлы, предназначенные для обработки в ЦУСе. По умолчанию используется папка: \VIPNet Administrator\FOR_NCC.



Внимание! В ЦУСе должны быть указаны аналогичные папки обмена. Сетевой доступ к этим папкам должен быть открыт для УКЦ.

О том, как настроить папки обмена в ЦУСе, см. документ «VIPNet Administrator Центр управления сетью. Руководство администратора», главу «Управление сетью», раздел «Настройка путей (пункт меню „Пути“)».

4 Для сохранения указанных папок нажмите кнопку **Применить** и (или) **ОК**.


В разделе **Папки ViPNet Администратора** также можно:

- В поле **Рабочая папка** посмотреть путь к папке, в которой хранятся база данных (если она была развернута по типу Microsoft Access) и различные данные, создаваемые в процессе работы УКЦ (например, дистрибутивы ключей, резервные наборы ключей и другие). Чаще всего данная папка также является и папкой установки программы.
- Включить опцию автоматического переноса ключей из УКЦ в ЦУС, установив флажок **Автоматически переносить в ЦУС создаваемые ключи пользователей и узлов**.
- Включить опцию автоматического создания ключей узлов в заданный период времени при наличии файлов для их создания из ЦУСа. Для этого установите флажок **Создавать обновления ключей каждые** и в поле справа введите период создания новых ключей узлов (в часах, по умолчанию установлено 12 часов). Данная опция доступна для редактирования только если включена функция автоматического переноса ключей в ЦУС (установлен флажок **Автоматически переносить в ЦУС создаваемые ключи пользователей и узлов**).

При включении опции автоматического создания ключей узлов по истечении заданного времени с момента последнего автоматического создания ключей и при наличии файлов для их создания из ЦУСа появится сообщение с предложением сформировать новые ключи узлов. В случае положительного ответа запустится процесс создания ключей узлов, в случае отрицательного ответа данное сообщение снова появится спустя 1 час.

Настройка типа создаваемых паролей

При выполнении некоторых операций в программе ViPNet Удостоверяющий и ключевой центр (например, при формировании ключей пользователя или дистрибутивов ключей) создание паролей производится на основе типа, выбранного в настройках программы по умолчанию, и без возможности его смены. Чтобы в процессе данных операций по умолчанию создавались пароли нужного типа, предварительно выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Пароли**.

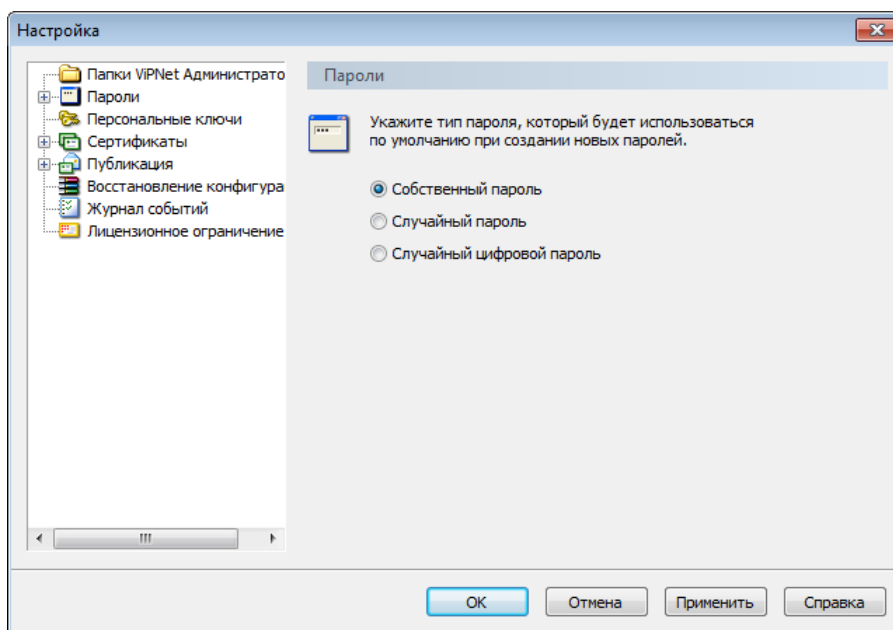


Рисунок 125: Выбор типа создаваемых паролей

- 3 В разделе **Пароли** выберите тип пароля, который будет использоваться по умолчанию при создании новых паролей:
 - **Собственный пароль** — для создания паролей, определяемых администратором УКЦ. При вводе длина таких паролей должна быть не менее 6 символов.
 - **Случайный пароль** — для создания паролей, формируемых автоматически на основе парольных фраз по заданным параметрам.

- **Случайный цифровой пароль** — для создания паролей, формируемых автоматически из заданного числа цифр.



Примечание. При выборе типа **Случайный пароль** или **Случайный цифровой пароль** дополнительно настройте параметры случайных паролей (см. «[Настройка параметров случайных паролей](#)» на стр. 243).

- 4 Нажмите кнопку **Применить** и (или) **ОК**.

В результате создание паролей будет производиться в соответствии с выбранным типом.


Настройка параметров случайных паролей

Если в процессе работы в программе ViPNet Удостоверяющий и ключевой центр при выполнении каких-либо операций будут создаваться случайные цифровые пароли или пароли на основе парольных фраз, предварительно настройте параметры их создания.



Примечание. Параметры случайных паролей первоначально могут быть заданы в процессе выполнения первичной инициализации (см. «[Проведение первичной инициализации программы](#)» на стр. 50).

Чтобы настроить параметры создания случайных паролей:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Пароли > Случайные пароли**.

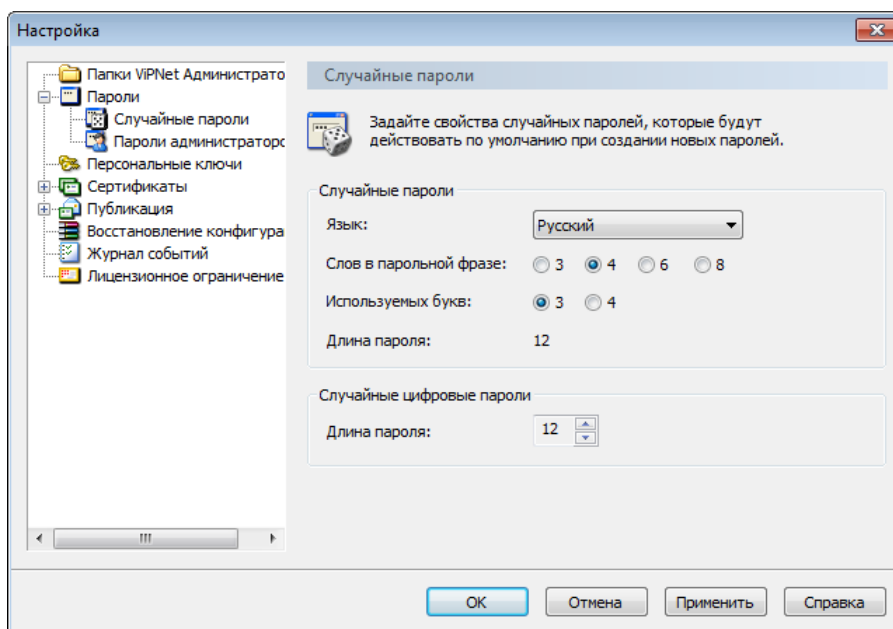


Рисунок 126: Настройка параметров случайных паролей

- 3 При настройке параметров случайных паролей на основе парольных фраз в группе **Случайные пароли**:
 - В списке **Язык** выберите язык парольной фразы.
 - В списке **Слов в парольной фразе** выберите число слов (3, 4, 6 или 8), из которых будет состоять парольная фраза. Чем больше число слов, тем длиннее и, соответственно, надежнее будет пароль.
 - В списке **Используемых букв** выберите число начальных букв каждого слова (3 или 4), которые войдут в пароль.


В строке **Длина пароля** отобразится количество букв в пароле, который будет сформирован с учетом указанных параметров.

- 4 При настройке параметров случайных паролей в группе **Случайные цифровые пароли** укажите длину пароля (от 6 до 32 цифр).
- 5 Для сохранения параметров нажмите кнопку **Применить** и (или) **ОК**.

В результате создание случайных паролей будет производиться в соответствии с указанными параметрами.

Настройка паролей администраторов

В программе ViPNet Удостоверяющий и ключевой центр задаются пароли администраторов сетевых узлов и сетевых групп, и они имеют ограниченный срок действия. Чтобы по истечении срока действия таких паролей производилось специальное оповещение, выполните следующие настройки:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Пароли > Пароли администраторов**.

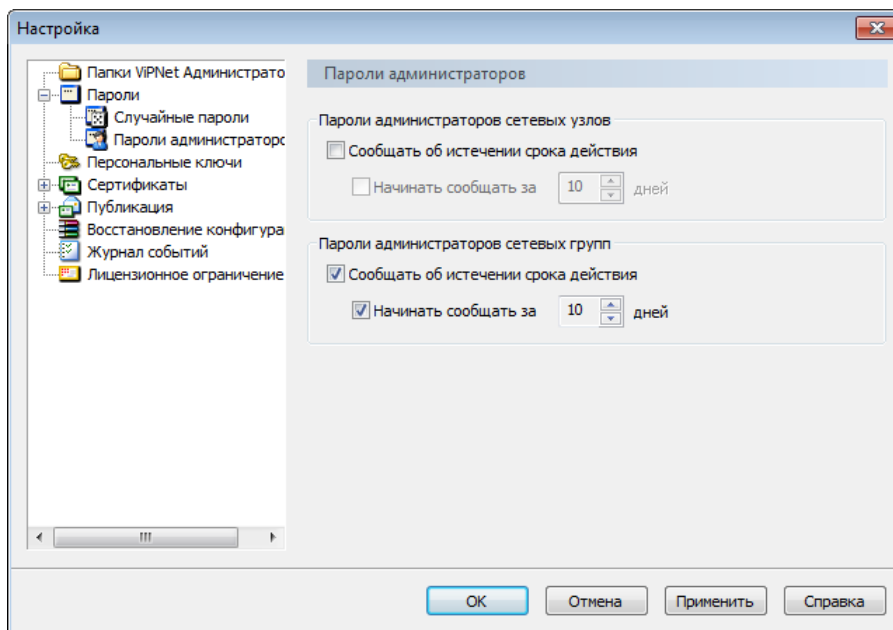


Рисунок 127: Настройка параметров паролей администраторов

- 3 В разделе **Пароли администраторов**:
 - Для предварительного оповещения об истечении срока действия паролей администраторов сетевых узлов в группе **Пароли администраторов сетевых узлов** установите флажки **Сообщать об истечении срока действия** и **Начинать сообщать за** и в поле справа введите количество дней, за которое следует производить оповещение.

Если будет установлен только флажок **Сообщать об истечении срока действия**, то оповещение будет производиться уже после истечения срока действия пароля.

- Для предварительного оповещения об истечении срока действия паролей администраторов сетевых групп аналогичным образом укажите необходимые параметры в группе **Пароли администраторов сетевых групп**.



Примечание. По умолчанию в настройках включена опция оповещения об истечении срока действия паролей администраторов сетевых групп (за 10 дней до его истечения).


- 4 Для сохранения настроек нажмите кнопку **Применить** и (или) **ОК**.

Настройка параметров создания резервных наборов персональных ключей

При формировании самого первого дистрибутива ключей пользователя создается резервный набор его персональных ключей. Резервный набор ключей необходим для дистанционного обновления ключей пользователя при их компрометации или при смене мастер-ключа персональных ключей и входит в состав дистрибутива ключей (см. [Резервный набор персональных ключей \(РНПК\)](#)). Впоследствии резервные наборы ключей создаются при смене мастера персональных ключей либо при компрометации последнего допустимого персонального ключа пользователя из текущего резервного набора ключей пользователя.

Создание резервных наборов персональных ключей производится в соответствии с параметрами, заданными в настройках программы.

Для настройки параметров создания резервных наборов персональных ключей выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Персональные ключи**.

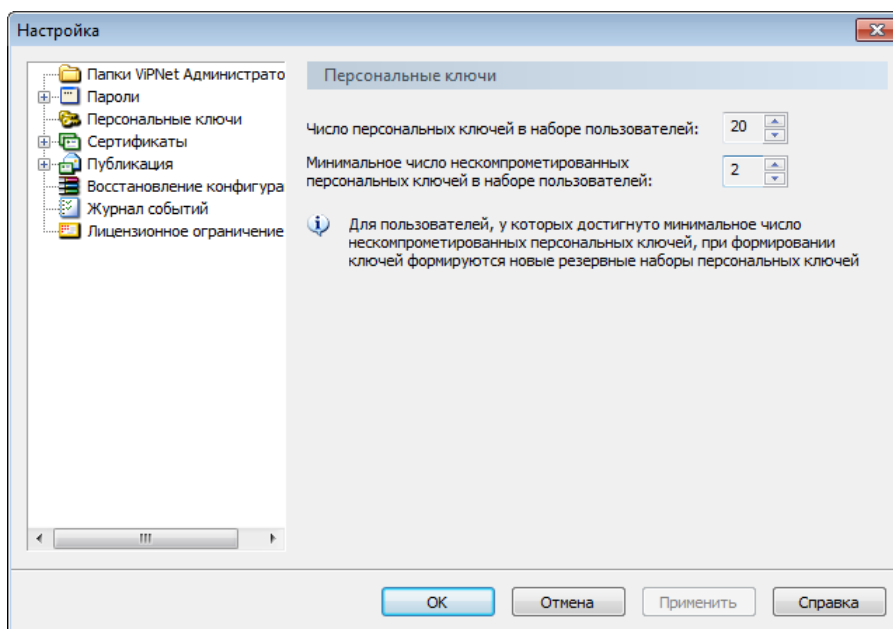


Рисунок 128: Настройка параметров персональных ключей

3 В разделе **Персональные ключи**:

- В поле **Число персональных ключей в наборе пользователей** укажите количество персональных ключей, из которых будет состоять создаваемый резервный набор. В резервном наборе может быть не более 20 персональных ключей.
- В поле **Минимальное число некомпromетированных персональных ключей в наборе пользователей** укажите минимальное количество персональных ключей, которые должны оставаться некомпromетированными в создаваемом наборе. Количество некомпromетированных ключей не может быть меньше 2 и больше 18.

Данный параметр определяет необходимость формирования нового резервного набора персональных ключей, а именно: создание нового резервного набора ключей производится при компрометации последнего допустимого персонального ключа пользователя из текущего набора. При этом один из некомпromетированных ключей текущего набора используется для шифрования нового резервного набора, остальные некомпromетированные ключи переходят в состав создаваемого набора.

В качестве примера рассмотрим следующую ситуацию. Допустим, в резервном наборе количество персональных ключей равно 20, а минимальное количество некомпromетированных ключей — 2. Формирование нового резервного набора ключей в таком случае произойдет при компрометации персонального ключа пользователя под номером 18, причем новый набор будет зашифрован на

персональном ключе под номером 19 из старого набора, а персональный ключ под номером 20 войдет в состав нового набора ключей.



Совет. Настоятельно рекомендуется использовать параметры, установленные по умолчанию.


- 4 Для сохранения параметров нажмите кнопку **Применить** и (или) **ОК**.
В результате создание резервных наборов персональных ключей будет производиться в соответствии с указанными параметрами.

Настройка параметров издания сертификатов и обработки запросов

При отсутствии лицензионных ограничений (см. «[Лицензионное ограничение](#)» на стр. 14) программа ViPNet Удостоверяющий и ключевой центр работает в качестве Удостоверяющего центра ViPNet и осуществляет издание сертификатов открытого ключа подписи пользователей и обслуживание изданных сертификатов (отзыв, приостановка и возобновление действия сертификатов).

Издание сертификатов происходит как при формировании ключей ViPNet, так и по запросам от пользователей либо из Центров регистрации ViPNet. Обслуживание изданных сертификатов производится либо по инициативе администратора УКЦ, либо в соответствии с запросами из Центров регистрации.

Чтобы издание сертификатов в ходе различных операций и обслуживание сертификатов по запросам из Центров регистрации ViPNet могли осуществляться в автоматическом режиме, выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Сертификаты**.

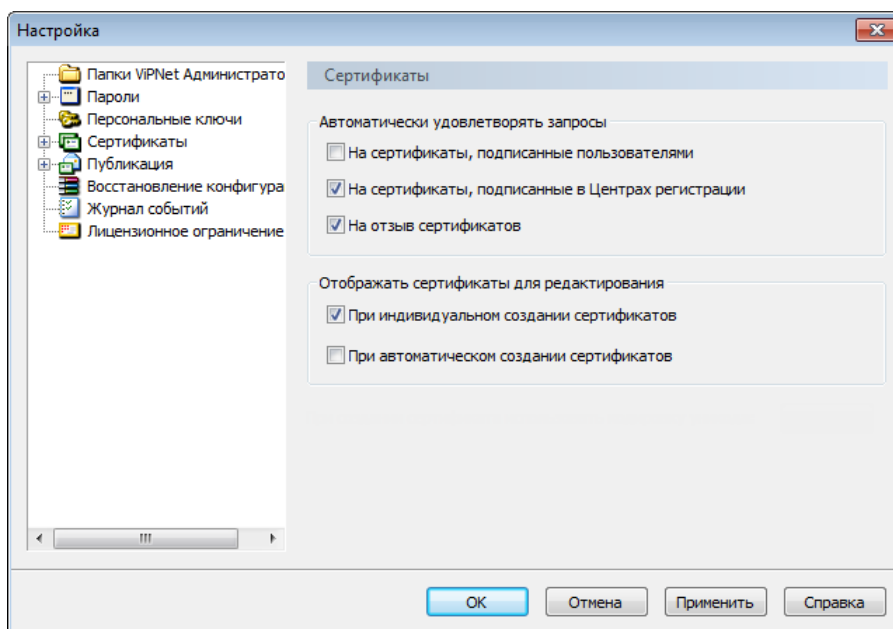


Рисунок 129: Настройка параметров издания сертификатов и обработки запросов

3 В разделе Сертификаты:


- Для автоматического издания сертификатов подписи по запросам, полученным от пользователей сетевых узлов VipNet (подписанным действующим ключом пользователя) установите флажок **На сертификаты, подписанные пользователями**.
- Для автоматического издания сертификатов подписи по запросам, полученным из Центров регистрации VipNet (подписанным действующим ключом администратора Центра регистрации) убедитесь, что установлен флажок **На сертификаты, подписанные в Центрах регистрации**.

Внимание! Сертификаты по запросам не будут изданы в автоматическом режиме в том случае, если:



- Истек срок действия списка отозванных сертификатов. Требуется обновить СОС своей сети.
- Подпись под запросом неверна, или права пользователя, подписавшего запрос, недостаточны для выполнения данной операции.
- Срок действия сертификата в запросе превышает срок действия, указанный в шаблоне. Требуется корректировка срока действия сертификата.

Запросы на издание сертификатов переместятся в раздел **Запросы на сертификаты > Входящие > Своя сеть VipNet (Внешние пользователи)** для обработки вручную администратором.

- Для автоматического издания сертификатов пользователей в процессе создания новых ключей пользователей (см. «[Создание ключей пользователей](#)» на стр. 100) или выборочных дистрибутивов ключей (см. «[Процесс создания](#)» на стр. 93) убедитесь, что установлен флажок **При индивидуальном создании сертификатов**.
- Для автоматического издания сертификатов пользователей в процессе массового создания дистрибутивов ключей (при выборе пункта меню **Сервис > Автоматически создать > Дистрибутивы ключей** или по нажатию кнопки **Создать дистрибутивы ключей**  на панели инструментов) установите флажок **При автоматическом создании сертификатов**.



Примечание. Издание сертификатов во всех вышеуказанных случаях будет производиться без участия администратора УКЦ, без редактирования параметров и на основе шаблона сертификата, заданного в настройках по умолчанию (см. [Создание и редактирование шаблонов сертификатов](#) (на стр. 256)).

- Для автоматической обработки запросов на отзыв, приостановление и возобновление действия сертификатов, полученных из Центров регистрации ViPNet, убедитесь, что установлен флажок **На отзыв сертификатов**.
- 4** Для сохранения настроек нажмите кнопку **Применить** и (или) **ОК**.

Настройка параметров работы с сертификатами


Сертификаты открытого ключа подписи пользователей и администраторов имеют ограниченный срок действия, который задается при их издании.



Примечание. При задании срока действия сертификата автоматически определяется срок действия закрытого ключа. Если срок действия сертификата задается меньше или равным 12 месяцам (1 году), то срок действия закрытого ключа будет равен заданному сроку действия сертификата. Если заданный срок действия сертификата больше 1 года, то срок действия закрытого ключа устанавливается равным 1 году. Только в этом случае при издании сертификата будет указан срок действия закрытого ключа (1 год). Максимальный срок действия сертификата пользователя составляет 5 лет, сертификата администратора — 6 лет.

В программе ViPNet Удостоверяющий и ключевой центр предусмотрена возможность оповещения об истечении срока действия изданных сертификатов (а точнее, соответствующих им закрытых ключей) с помощью специальных сообщений. При истечении срока действия закрытого ключа любого администратора за определенное количество дней, указанное в настройках программы, появляется соответствующее сообщение с рекомендацией его обновить. Данная опция предназначена для того, чтобы администратор мог своевременно узнать об истечении срока действия сертификата и его обновить, и отключить ее невозможно. При необходимости также может производиться оповещение об истечении срока действия сертификатов пользователей. В этом случае в зависимости от настроек программы сообщения могут появляться за несколько дней до истечения срока действия либо уже после его истечения.

Чтобы настроить параметры оповещения об истечении срока действия изданных сертификатов, выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Сертификаты > Срок действия**.

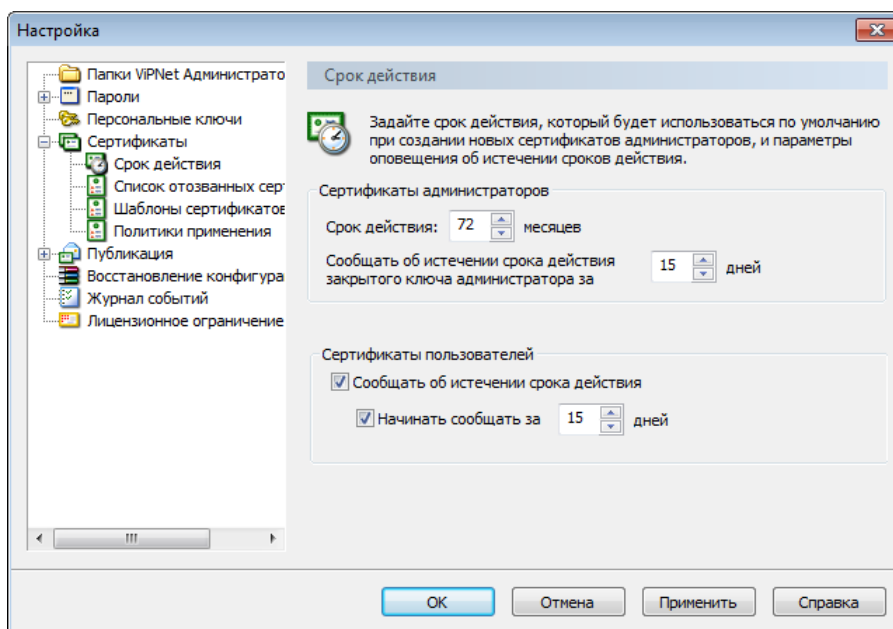


Рисунок 130: Настройка параметров работы с сертификатами

3 В разделе **Срок действия**:

- В группе **Сертификаты администраторов** в поле **Сообщать об истечении срока действия закрытого ключа администратора за** введите количество дней (не более 30), за которое следует производить оповещение об истечении срока действия закрытого ключа администратора с рекомендацией обновить его сертификат.
- Для предварительного оповещения об истечении срока действия сертификатов пользователей, в группе **Сертификаты пользователей** установите флажки **Сообщать об истечении срока действия** и **Начинать сообщать за** и в поле справа введите количество дней (не более 30), за которое требуется производить оповещение.

Если будет установлен только флажок **Сообщать об истечении срока действия**, то оповещение будет производиться уже после истечения срока действия сертификатов пользователей.

4 Для сохранения указанных настроек нажмите кнопку **Применить** и (или) **ОК**.



Примечание. В данном разделе в группе **Сертификаты администраторов** в поле **Срок действия** также можно указать срок действия сертификатов администраторов (в месяцах), который по умолчанию будет указываться в процессе их издания. Срок действия сертификата администратора не может превышать 72 месяца (6 лет).

Как правило, данная опция полезна в том случае, если при издании сертификатов

администраторов не осуществляется редактирование параметров на страницах мастера.

Создание и редактирование шаблонов сертификатов


В программе ViPNet Удостоверяющий и ключевой центр издание сертификатов открытого ключа подписи производится на основе специальных шаблонов сертификатов (см. «[Шаблон сертификата](#)»), а точнее, в соответствии с параметрами того шаблона сертификата, который выбран по умолчанию (см. ниже). В зависимости от настроек программы (см. «[Настройка параметров издания сертификатов и обработки запросов](#)» на стр. 250) во время издания сертификатов данные параметры могут из шаблона заимствоваться полностью без возможности изменения либо дополняться и изменяться (за исключением алгоритма и параметров открытого ключа, которые всегда берутся из шаблона по умолчанию).



Примечание. Параметры всех шаблонов сертификатов хранятся в файле `cert_tem.ini` папки установки программы. При обновлении программного обеспечения существующие шаблоны не изменяются и не удаляются.

В конфигурацию программы входит несколько стандартных шаблонов сертификатов подписи и шифрования, в том числе и шаблон для издания квалифицированного сертификата (см. «[Квалифицированный сертификат](#)»). При необходимости администратор УКЦ может с помощью мастера создать другие шаблоны сертификатов или отредактировать существующие.

Для создания нового шаблона сертификата:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Сертификаты > Шаблоны сертификатов**.

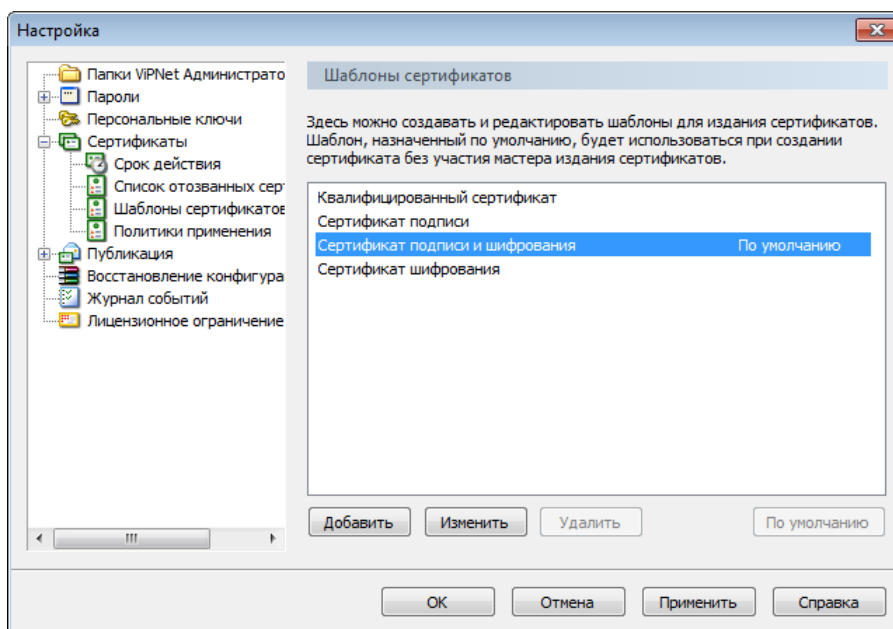


Рисунок 131: Управление шаблонами сертификатов

- 3 В разделе **Шаблоны сертификатов** нажмите кнопку **Добавить** и следуйте указаниям мастера создания шаблона сертификата.
- 4 На первой странице мастера введите имя шаблона и нажмите кнопку **Далее**. Имя шаблона должно быть уникальным.
- 5 На странице **Алгоритм и параметры ключа** укажите параметры открытого ключа в соответствии с приведенной ниже таблицей:

Таблица 4. Характеристики алгоритма ГОСТ Р 34.10-2001

Алгоритм подписи	Описание	Параметры алгоритма	Описание параметров	Длина ключа
ГОСТ Р 34.10-2001	Новый стандарт электронной подписи, основанный на арифметике эллиптических кривых.	ГОСТ Р 34.10-2001	Параметры по умолчанию (рекомендуется). OID «1.2.643.2.2. 35.1»	512
	OID «1.2.643.2.2.19»	ГОСТ Р 34.10-2001	Параметры подписи 3 (в соответствии с RFC 4357 http://www.ietf.org/rfc/rfc4357.txt). OID «1.2.643.2.2. 35.3»	



Совет. Рекомендуется использовать параметры алгоритма, предлагаемые по умолчанию. Данные параметры характеризуются наибольшей скоростью вычисления и проверки подписи.

После этого нажмите кнопку **Далее**.

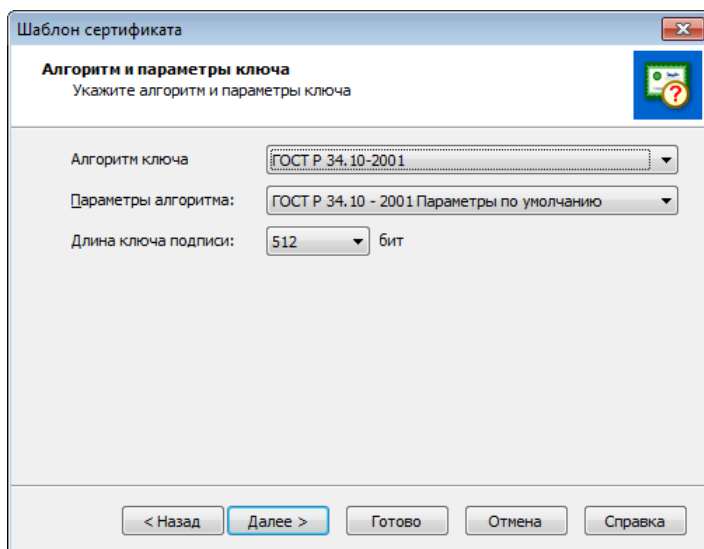


Рисунок 132: Выбор алгоритма и настройка параметров ключа

- 6 На следующей странице задайте срок действия сертификата, после чего нажмите кнопку **Далее**.



Примечание. При задании срока действия сертификата автоматически определяется срок действия закрытого ключа. Если срок действия сертификата задается меньше или равным 12 месяцам (1 году), то срок действия закрытого ключа будет равен заданному сроку действия сертификата. Если заданный срок действия сертификата больше 1 года, то срок действия закрытого ключа устанавливается равным 1 году. Только в этом случае при издании сертификата будет указан срок действия закрытого ключа (1 год). Максимальный срок действия сертификата пользователя составляет 5 лет.

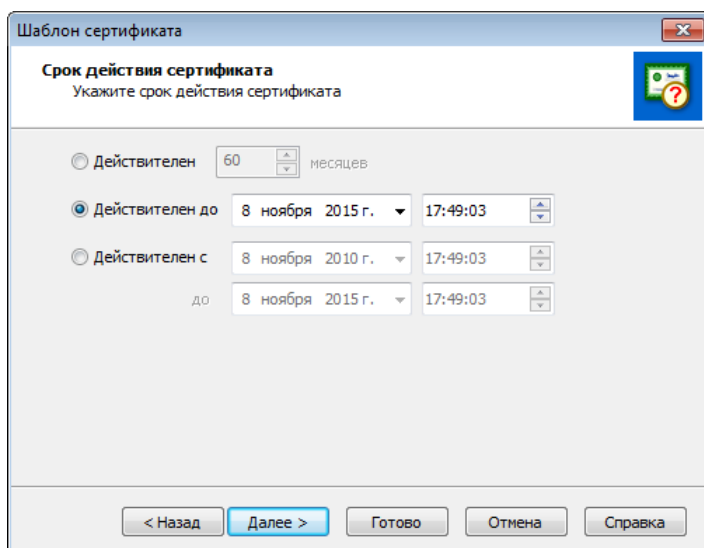


Рисунок 133: Указание срока действия сертификата

- 7 На странице **Назначения сертификата** укажите расширения сертификата, которые будут добавлены в новый шаблон.

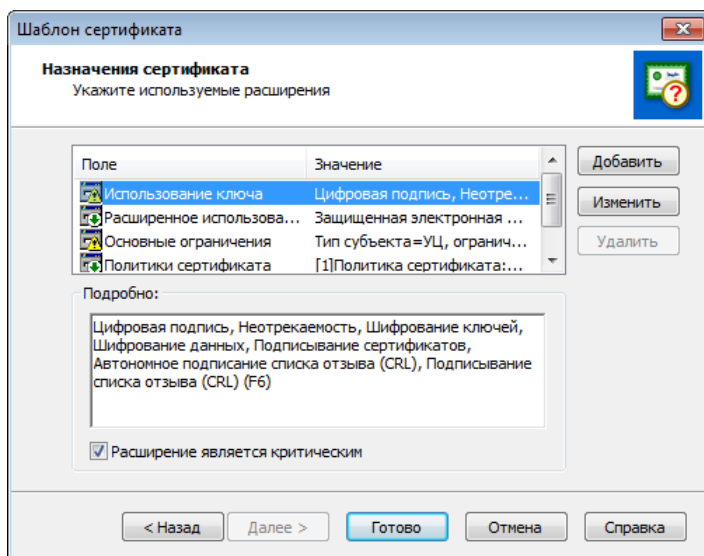


Рисунок 134: Формирование назначений сертификата

Для добавления расширения нажмите кнопку **Добавить** и в окне **Допустимые расширения** выберите одно из расширений:

- **Использование ключа.** В появившемся окне настройте параметры использования ключа и нажмите кнопку **ОК**.

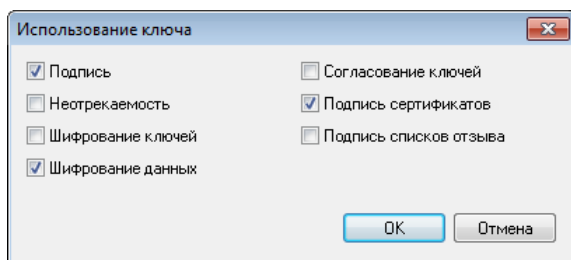


Рисунок 135: Настройка параметров использования ключа

- **Расширенное использование ключа.** В появившемся окне с помощью кнопок **Добавить** и **Удалить** сформируйте список назначений ключа и нажмите кнопку **ОК**.

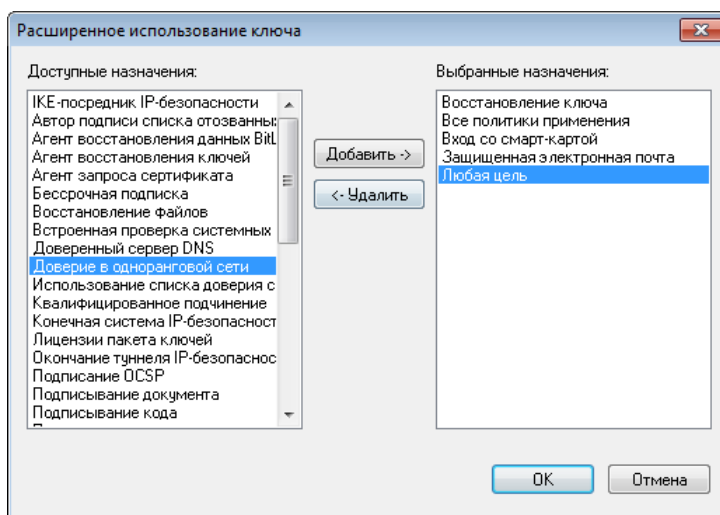


Рисунок 136: Выбор назначений расширенного использования ключа

- **Политики сертификата.** В появившемся окне с помощью кнопок **Добавить** и **Удалить** выберите политики применения сертификата, которые будут включены в данный шаблон, и нажмите кнопку **ОК**. При необходимости предварительно выполните настройку списка политик применения (см. «[Настройка списка политик применения сертификата](#)» на стр. 268).

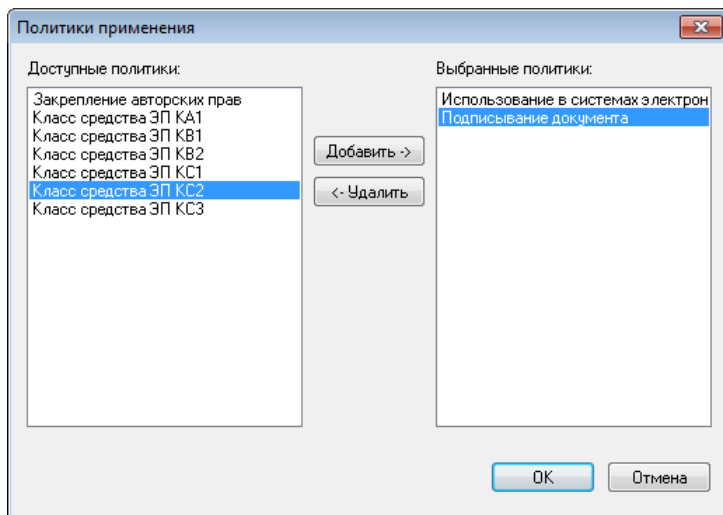


Рисунок 137: Выбор политик применения сертификата

- **Средство электронной подписи издателя.** В появившемся окне укажите сведения о средстве электронной подписи, которое используется издателем для создания ключей электронной подписи и сертификата, и нажмите кнопку **ОК**.

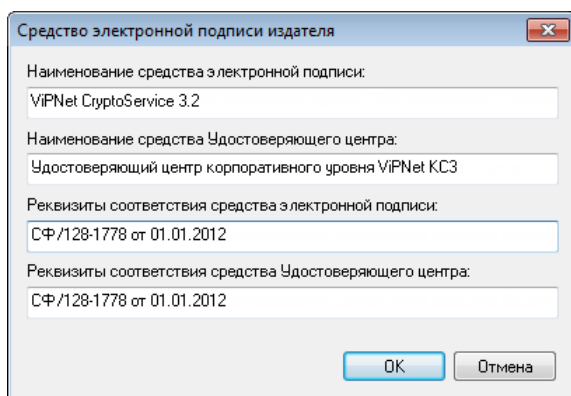


Рисунок 138: Задание средства электронной подписи Удостоверяющего центра

- **Средство электронной подписи владельца.** В появившемся окне укажите наименование средства формирования электронной подписи, которое используется владельцем сертификата, и нажмите кнопку **ОК**.

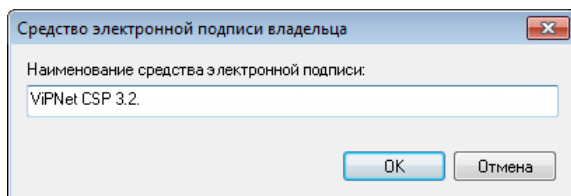


Рисунок 139: Задание средства электронной подписи владельца сертификата

- **Дополнительное имя субъекта.** Для указания дополнительного имени пользователя нажмите кнопку **Добавить**, в появившемся окне задайте тип имени и его значение, затем нажмите кнопку **ОК**.

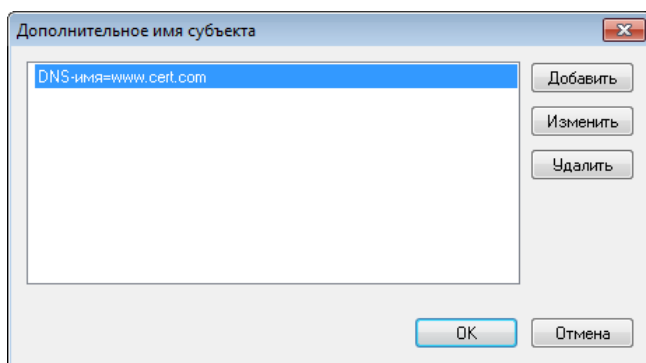


Рисунок 140: Задание средства электронной подписи владельца сертификата

Для изменения параметров используемого расширения воспользуйтесь кнопкой **Изменить**, для удаления ненужного расширения — кнопкой **Удалить**.

При необходимости для выбранного расширения установите флажок **Расширение является критическим**. При включении данной опции расширение будет отмечено как критическое. Это означает, что если прикладное ПО не сможет обработать такое расширение, то сертификат будет признан недействительным.

- 8 После формирования назначений сертификата нажмите кнопку **Готово**. При необходимости изменения параметров шаблона вернитесь на нужную страницу с помощью кнопки **Назад**.
- 9 В результате в списке шаблонов сертификатов появится новый шаблон. Для сохранения созданного шаблона нажмите кнопку **Применить** и (или) **ОК**.

Чтобы изменить параметры шаблона сертификата, выберите его в списке и нажмите кнопку **Изменить**, затем на страницах мастера внесите необходимые коррективы (см. выше) и нажмите кнопку **ОК**.

Чтобы удалить ненужный шаблон, выберите его в списке и нажмите кнопку **Удалить**.




Примечание. При взаимодействии с Центрами регистрации (узлами с программным обеспечением ViPNet Registration Point) после добавления, изменения или удаления шаблонов сертификатов сформируйте и отправьте обновления ключей узлов. Данная операция требуется для того, чтобы в Центры регистрации поступила актуальная информация о шаблонах сертификатов, сформированных в УКЦ.

Чтобы издание сертификатов подписи производилось в соответствии с параметрами нужного шаблона, выберите его в списке и нажмите кнопку **По умолчанию**.

Настройка параметров работы со списками отозванных сертификатов

При издании сертификатов администраторов создаются списки отозванных сертификатов (см. «Список отозванных сертификатов (СОС)»). Для удобства работы с данными списками можно настроить ряд параметров.

Чтобы выполнить настройку параметров работы со списками отозванных сертификатов своей сети:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Сертификаты > Список отозванных сертификатов**.

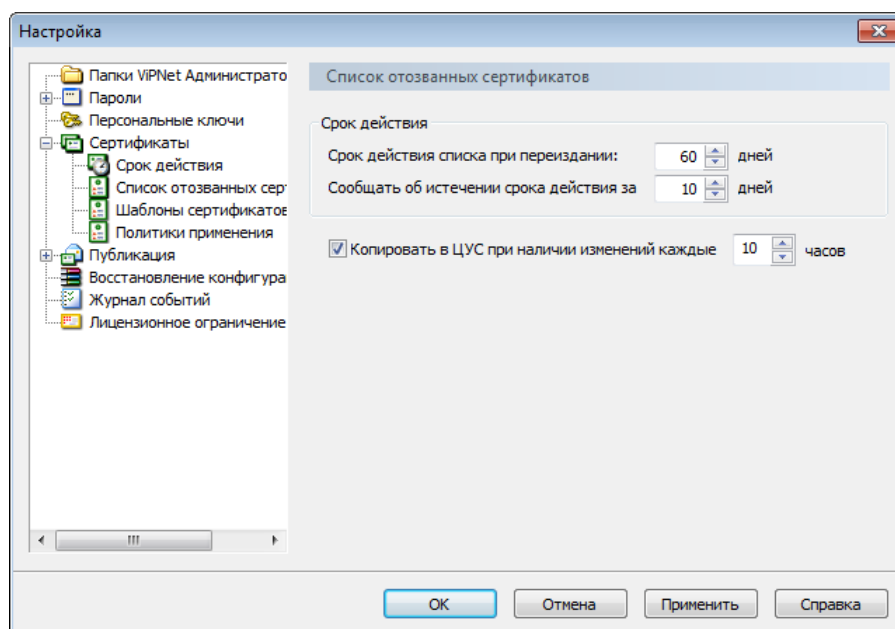


Рисунок 141: Настройка параметров работы со списками отозванных сертификатов

- 3 В разделе **Список отозванных сертификатов**:
 - В поле **Срок действия списка при переиздании** введите срок действия СОС (в днях), в течение которого он будет действителен после своего обновления (см.

«[Обновление списка отозванных сертификатов своей сети](#)» на стр. 167). Срок действия не может превышать 365 дней (1 год), по умолчанию установлено 60 дней.

- В поле **Сообщать об истечении срока действия** за укажите количество дней (не более 10), за которое следует выдавать предупреждение об истечении срока действия СОС с рекомендацией его обновить.
- Чтобы СОС автоматически копировались в папку обмена для последующей отправки в программу ViPNet Центр управления сетью (при наличии изменений в заданный интервал времени), установите флажок **Копировать в ЦУС при наличии изменений каждые** и в поле справа введите интервал (в часах, в диапазоне от 0 до 30), в течение которого будет проверяться наличие изменений СОС.

Если значение параметра будет равно 0, то при изменении СОС будет сразу копироваться в папку.

- 4 Для сохранения указанных настроек нажмите кнопку **Применить** и (или) **ОК**.

Расширенная настройка параметров обновления списков отозванных сертификатов на сетевых узлах

Обновление списков отозванных сертификатов (СОС) на сетевых узлах осуществляется в соответствии с параметрами, указанными в файле `crl-update-settings.ini`. Первоначально данный файл формируется при первом запуске программы ViPNet Удостоверяющий и ключевой центр, а затем рассылается на сетевые узлы вместе с обновлениями ключей. Значения параметров файла `crl-update-settings.ini` могут изменяться при добавлении или удалении точек доступа к СОС в настройках программы (см. «[Настройка списка точек распространения](#)» на стр. 273).

При необходимости можно выполнить расширенную настройку параметров обновления СОС. Для этого:

- 1 В текстовом редакторе откройте файл `crl-update-settings.ini`, который по умолчанию расположен в папке установки ViPNet Удостоверяющий и ключевой центр (по умолчанию: `\ViPNet Administrator\KC`).
- 2 В секции `[CrlUpdateAtSigVerification]` задайте параметры обновления СОС при проверке электронной подписи:
 - Для возможности обновления СОС во время проверки электронной подписи укажите значение параметра `AllowCrlUpdate` равным 1, в случае запрета обновления СОС укажите значение 0. По умолчанию `AllowCrlUpdate=1`.
 - Для игнорирования действительного СОС при проверке электронной подписи укажите значение параметра `ForceCrlUpdate` равным 1; чтобы принимать во

внимание действительный сертификат, укажите 0. По умолчанию установлено значение 0.

Примечание. Если параметр `AllowCrlUpdate=0`, а `ForceCrlUpdate=0` или 1, то обновление СОС при проверке подписи не произойдет.

Если `AllowCrlUpdate=1`, а значение параметра `ForceCrlUpdate=0`, то обновление СОС при проверке подписи будет выполнено при следующих условиях:



- Действительный СОС локально недоступен.
- В сертификате пользователя прописана точка распространения СОС.

Если параметры `AllowCrlUpdate=1` и `ForceCrlUpdate=1`, то обновление СОС при проверке электронной подписи выполнится при условии, что в сертификате пользователя указана точка распространения СОС.

3 В секции `[PeriodicallyCrlUpdate]` задайте параметры периодического обновления СОС:

- Для выполнения периодического обновления СОС укажите значение параметра `AllowCrlUpdate` равным 1, при запрете периодического обновления укажите значение 0. По умолчанию в файле значение параметра равно 1.
- Для автоматического добавления найденных при проверке электронной подписи точек распространения в список опроса укажите значение параметра `CollectLocallyDetectedCdp` равным 1, для запрета добавления новых точек укажите значение 0. По умолчанию в файле `CollectLocallyDetectedCdp=0`.



Примечание. Кроме точек распространения, заданных администратором в Удостоверяющем центре (описанных в данном файле в секциях `[cdp-n]`), в сертификатах могут встретиться и другие точки распространения. Данный параметр позволяет накапливать точки распространения СОС, найденные при проверке подписи и отсутствующие в основном списке опроса.

4 В секции `[cdp-n]`, где `n` — номер точки распространения, укажите параметры опроса точки доступа. Для этого задайте параметры из списка, приведённого ниже:

- `Name` — название точки распространения.
- `Url` — сетевой путь, по которому доступен СОС.

- `IntervalInMinutes` — интервал опроса данной точки распространения (в минутах). По умолчанию значение параметра равно 1440 (1 сутки), минимальное значение равно 1.
 - `NextUpdate` — дата и время следующего опроса.
 - `LastSuccessfulAccess` — дата и время последней успешной загрузки СОС с точки распространения.
 - `Enabled` — параметр отключения, либо включения точки распространения в момент опроса. Если `Enabled=1`, то точка доступа будет опрашиваться. Если `Enabled=0`, то опрос данной точки осуществляться не будет.
 - `IssuerName` — имя издателя СОС в формате X.500.
- 5** Задайте параметр `BadCdpIgnoreIntervalInSec` — интервал (в секундах), в течение которого не опрашивается проблемная точка распространения — точка, с которой не удалось получить доступ к СОС. Если параметр имеет нулевое значение, то проблемные точки не учитываются.
- 6** Задайте параметр `MaxTimeDownloadingCrllnSec` — максимальное время (в секундах) загрузки СОС во время проверки электронной подписи. Если данный параметр равен 0, то время загрузки СОС не ограничено.

В результате после рассылки данного файла обновление СОС на сетевых узлах будет выполняться в соответствии с указанными параметрами.

Настройка списка политик применения сертификата

Область использования и применения сертификата открытого ключа подписи можно определить путем добавления в него специального расширения — политики применения (см. «[Политика применения сертификата](#)»). То есть, если сертификат следует использовать для каких-то определенных целей, например, только на торговой площадке или только для подписи отчетной документации, то при его издании можно добавить соответствующую политику, которая будет определять сферу его действия (подробнее см. RFC 5280 <http://tools.ietf.org/html/rfc5280>).

Примечание. Политика применения может быть представлена в виде текста или ссылки на веб-страницу.


С политикой применения изданного сертификата подписи можно ознакомиться, нажав кнопку **Заявление издателя** в окне просмотра сертификата.



В конфигурации программы имеется готовый список политик применения, описывающих классы средств электронной подписи. Данные политики в обязательном порядке должны добавляться в издаваемые квалифицированные сертификаты (а именно, в те сертификаты, в которых указаны наименования средств электронной подписи издателя и владельца сертификата).

Политики применения также можно добавлять в шаблоны сертификатов. Подробнее см. раздел [Создание и редактирование шаблонов сертификатов](#) (на стр. 256).

Прежде чем добавить политику применения в издаваемый сертификат или шаблон сертификата, ее предварительно требуется создать. Чтобы создать политику применения, выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Сертификаты > Политики применения**.

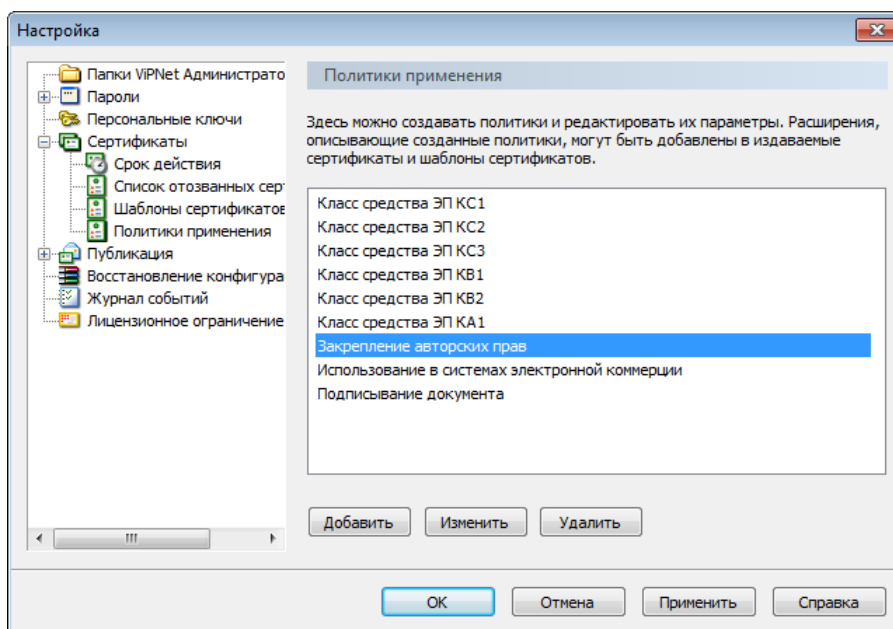


Рисунок 142: Управление политиками применения сертификатов

3 В разделе **Политики применения** нажмите кнопку **Добавить**.

4 В окне **Политика применения сертификата**:

- В поле **Наименование** введите название политики.
- В поле **Идентификатор** введите идентификатор политики. Идентификатор должен состоять из набора десятичных чисел, разделенных точками. Длина идентификатора должна быть не более 64 символов.



Внимание! Идентификатор политики применения должен начинаться с корневого идентификатора организации, зарегистрированного в мировом пространстве идентификаторов объектов. Российский сегмент этого пространства имеет корневой идентификатор 1.2.643.

Поля **Наименование** и **Идентификатор** обязательно должны быть заполнены. Кроме того, идентификатор должен иметь уникальное значение в пределах данного Удостоверяющего центра.

- В поле **Адрес описания** введите URL-адрес документа, содержащего описание политики (в виде HTTP, FTP, файла или адреса LDAP).
- В поле **Краткое описание** введите краткое описание политики сертификации.

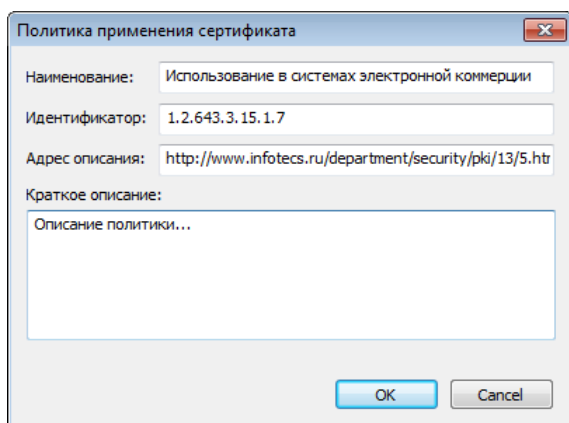


Рисунок 143: Добавление политики применения

- 5 По окончании ввода данных нажмите кнопку **ОК**. Созданная политика появится в списке в разделе **Политики применения**.
- 6 Для сохранения новой политики применения нажмите кнопку **Применить** и (или) **ОК**.

Чтобы редактировать политику, выберите ее в списке и нажмите кнопку **Изменить**, затем в окне **Политика применения сертификата** внесите необходимые коррективы (см. выше) и нажмите кнопку **ОК**.

Чтобы удалить политику, выберите ее в списке и нажмите кнопку **Удалить**.



Примечание. При взаимодействии с Центрами регистрации (узлами с программным обеспечением ViPNet Registration Point) после добавления, изменения или удаления политик применения сертификатов сформируйте и отправьте обновления ключей узлов. Данная операция требуется для того, чтобы в Центры регистрации поступила актуальная информация о политиках применения, заданных в УКЦ.

Настройка параметров публикации данных

Сертификаты пользователей, сертификаты администраторов и списки отозванных сертификатов (СОС), изданные в программе ViPNet Удостоверяющий и ключевой центр, могут быть опубликованы в общедоступных хранилищах данных (например, если в корпоративной сети организована система доменного управления) или в различных точках распространения (см. «[Точка распространения данных](#)»).




Примечание. В точки распространения могут публиковаться только СОС и сертификаты издателей. См. раздел [Настройка списка точек распространения](#) (на стр. 273).

Публикация данных производится с помощью Сервиса публикации (программы ViPNet Publication Service): ViPNet Publication Service получает данные для публикации из УКЦ, после чего размещает их в заданных хранилищах или точках распространения. Подробнее см. документ «ViPNet Publication Service. Руководство администратора».

Передача данных для публикации в программу ViPNet Publication Service осуществляется через специальную папку обмена `for_NCC\PubSRV` и может производиться как в автоматическом, так и в ручном режиме.

Чтобы все необходимые для публикации данные передавались УКЦ автоматически, выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Публикация**.

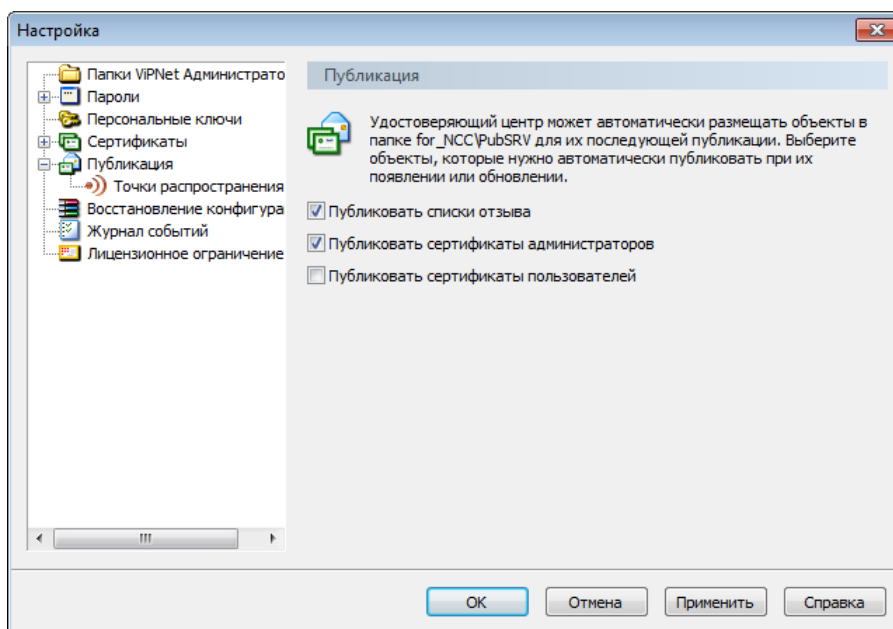


Рисунок 144: Настройка параметров публикации данных

3 В разделе **Публикация** установите флажки:

- **Публиковать списки отзыва** — для передачи на публикацию СОС.
- **Публиковать сертификаты администраторов** — для передачи сертификатов администраторов (в том числе и кросс-сертификатов администраторов).
- **Публиковать сертификаты пользователей** — для передачи издаваемых сертификатов пользователей.

4 Для сохранения настроек нажмите кнопку **Применить** и (или) **ОК**.

Таким образом, при появлении или обновлении данные, в соответствии с указанными настройками, будут автоматически помещаться в папку `for_NCC\PubSRV` для последующей передачи в программу ViPNet Publication Service.



Примечание. В программе ViPNet Publication Service папка `for_NCC\PubSRV` должна быть задана в качестве папки приема файлов из УКЦ. См. документ «ViPNet Publication Service. Руководство администратора», глава «Настройка взаимодействия УКЦ и Сервиса публикации», раздел «Настройка папок обмена».

Подробнее о публикации см. раздел [Публикация и прием опубликованных данных](#) (на стр. 193).

Настройка списка точек распространения


Списки отозванных сертификатов (СОС) и сертификаты администраторов с помощью Сервиса публикации (программы ViPNet Publication Service) могут публиковаться в так называемых точках распространения данных (см. «[Точка распространения данных](#)»). Точкой распространения данных может быть, например, FTP или OSCP-сервер.

Список точек распространения, в которых требуется размещать публикуемые данные, может быть сформирован как в программе ViPNet Publication Service, так и в программе ViPNet Удостоверяющий и ключевой центр.



Примечание. Если список точек распространения формируется в УКЦ, то информация о заданных точках помещается в издаваемые сертификаты пользователей (в соответствии с настройками, см. ниже).

Чтобы в УКЦ добавить точку распространения, выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Публикация > Точки распространения**.

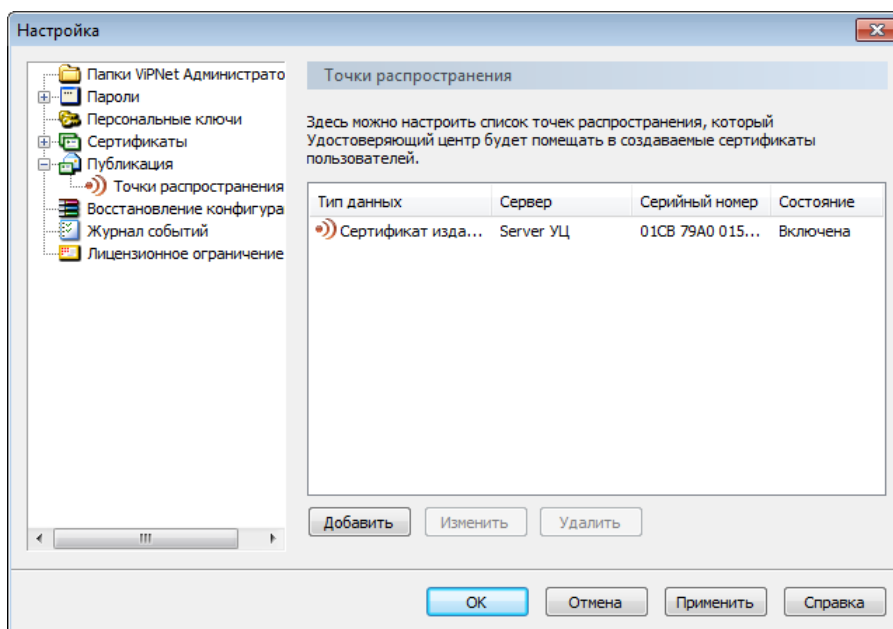


Рисунок 145: Настройка списка точек распространения

3 В разделе **Точки распространения** нажмите кнопку **Добавить**.

4 В окне **Точка распространения**:

- Установите флажок **Добавлять в сертификаты пользователей** для добавления информации о точке распространения в издаваемые сертификаты пользователей. Данная опция позволяет помещать в сертификат при издании адрес точки распространения, в которой опубликован сертификат его издателя или СОС.
- В списке **Тип данных** выберите тип данных, публикуемых в данной точке:
 - **Сертификат издателя** — для публикации сертификата издателя.
 - **Список отозванных сертификатов** — для публикации СОС.
 - **ОСРР сервер** — если в данной точке будет размещаться сервер онлайн-проверки статуса сертификатов (ОСРР-сервер).
- В поле **Сервер** введите имя точки распространения.
- Если в точке распространения будут публиковаться сертификаты издателей или СОС, с помощью кнопки **Выбрать** укажите сертификат издателя или сертификат, соответствующий списку отозванных сертификатов, который будет опубликован в данной точке.



Примечание. В сертификаты пользователей будут добавляться только те точки распространения, в которых указан соответствующий сертификат их издателя

(если включена опция **Добавлять в сертификаты пользователей**).

- В поле **Сетевой путь** введите URL-адрес сетевого ресурса (в виде HTTP, FTP или адреса LDAP), на котором будет размещаться данная точка распространения.

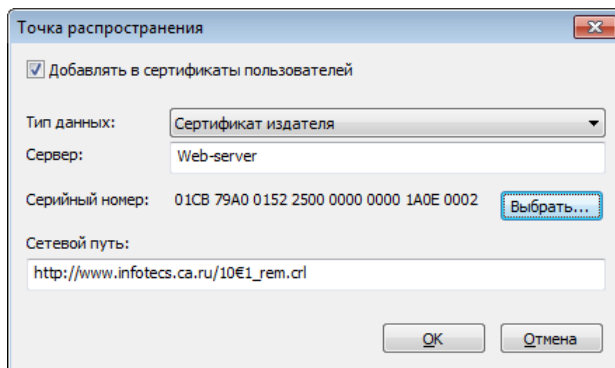


Рисунок 146: Добавление точки распространения

- 5 Нажмите кнопку **ОК**. Созданная точка распространения появится в списке в разделе **Точки распространения**.
- 6 Для сохранения новой точки распространения нажмите кнопку **Применить** и (или) **ОК**.

Чтобы изменить параметры точки распространения, выберите ее в списке и нажмите кнопку **Изменить**, затем в окне **Точка распространения** внесите необходимые коррективы (см. выше) и нажмите кнопку **ОК**.

Чтобы удалить точку распространения, выберите ее в списке и нажмите кнопку **Удалить**.



8

Административные функции

Создание и восстановление резервных копий конфигурации программы	277
Работа с журналом событий ViPNet Удостоверяющий и ключевой центр	285
Проверка текущих данных	290
Экспорт служебных данных	295
Учет ключей Деловой сети РФ	296

Создание и восстановление резервных копий конфигурации программы

В программе ViPNet Удостоверяющий и ключевой центр существует возможность возврата к предыдущим конфигурациям. Для восстановления конфигурации используются резервные копии, которые автоматически создаются программой или вручную администратором. Каждая резервная копия конфигурации включает в себя базу данных и настройки программы.

Автоматическое создание резервных копии текущей конфигурации (без участия администратора) осуществляется в том случае, если в настройках программы установлена соответствующая опция (см. «[Настройка параметров создания резервных копий](#)» на стр. 283). При ручном создании резервных копий используется мастер восстановления конфигурации.

Внимание! Следует иметь в виду, что:



- Восстановление резервных копий невозможно при смене пароля администратора либо ключа защиты УКЦ (см. «[Ключ защиты УКЦ](#)»).
 - Если в программе регистрируется новый администратор (который становится текущим), то он не сможет восстановить резервные копии на те моменты времени, в которые он администратором не являлся. Поэтому для восстановления конфигураций из таких резервных копий следует назначать текущим соответствующего администратора.
 - При удалении одной из учетных записей администратора рекомендуется сменить ключ защиты УКЦ и удалить те резервные копии, которые были сделаны в ходе работы данного администратора.
-

Создание резервной копии текущей конфигурации

Резервная копия конфигурации создается для того, чтобы можно было восстановить определенную конфигурацию программы.



Примечание. Если для создания резервной копии конфигурации недостаточно свободного пространства на диске, программа выдаст сообщение об этом. Для создания резервной копии необходимо освободить больше пространства на диске.

Чтобы создать резервную копию текущей конфигурации:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Восстановление конфигурации**. Будет запущен мастер **Восстановление конфигурации ViPNet Удостоверяющий и ключевой центр**.
- 2 На странице **Восстановление конфигурации ViPNet Удостоверяющий и ключевой центр** выберите **Создать резервную копию текущей конфигурации**, затем нажмите кнопку **Далее**.
- 3 На странице **Создание резервной копии** в поле **Комментарий к резервной копии** введите комментарий с описанием конфигурации. Добавление комментария необязательно, но он поможет быстрее найти нужную резервную копию в списке. Комментарий должен содержать не более 200 символов.

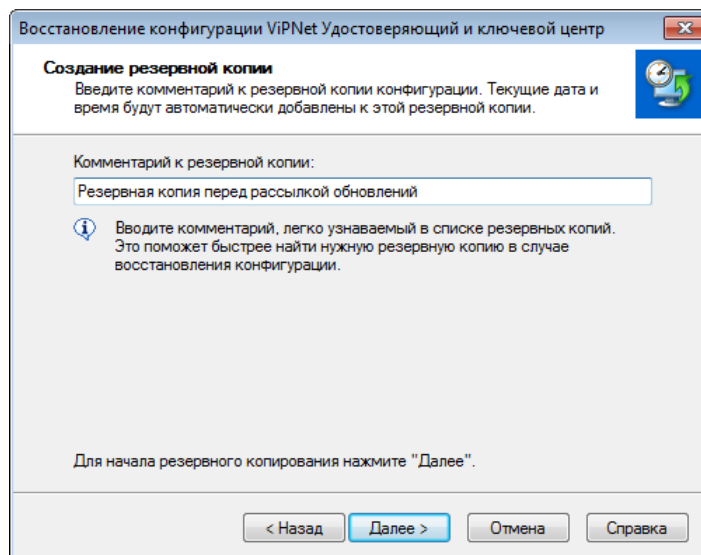


Рисунок 147: Создание резервной копии

- 4 Нажмите кнопку **Далее**. Будет создана резервная копия конфигурации. Созданная резервная копия конфигурации будет сохранена в подпапке `\Restore` папки установки программы.
- 5 Чтобы закончить работу мастера, на странице **Завершение создания резервной копии конфигурации** нажмите кнопку **Готово**.

Чтобы выполнить новую операцию с резервными копиями, нажмите кнопку **В начало**.

Восстановление конфигурации

Чтобы восстановить конфигурацию из ранее созданной резервной копии:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Восстановление конфигурации**. Будет запущен мастер **Восстановление конфигурации ViPNet Удостоверяющий и ключевой центр**.
- 2 На странице **Восстановление конфигурации ViPNet Удостоверяющий и ключевой центр** выберите **Восстановить конфигурацию ViPNet Удостоверяющий и ключевой центр**, затем нажмите кнопку **Далее**.

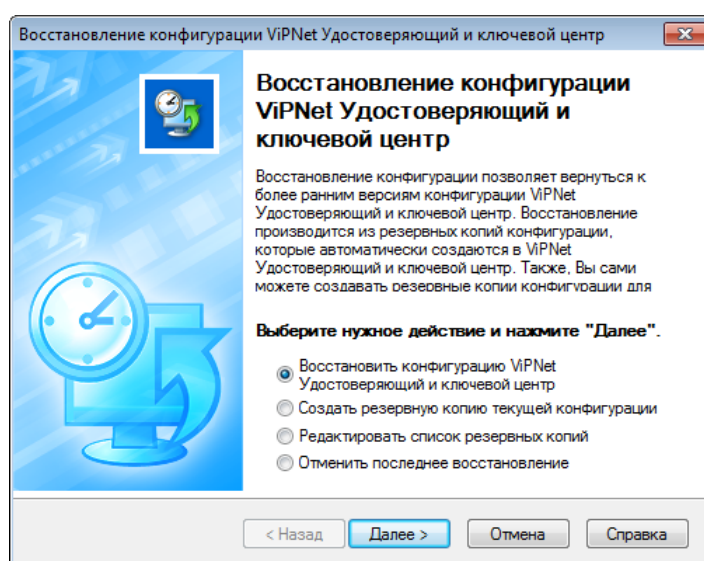


Рисунок 148: Запуск мастера создания и восстановления конфигурации

- 3 На странице **Выбор резервной копии** представлен список резервных копий конфигурации.

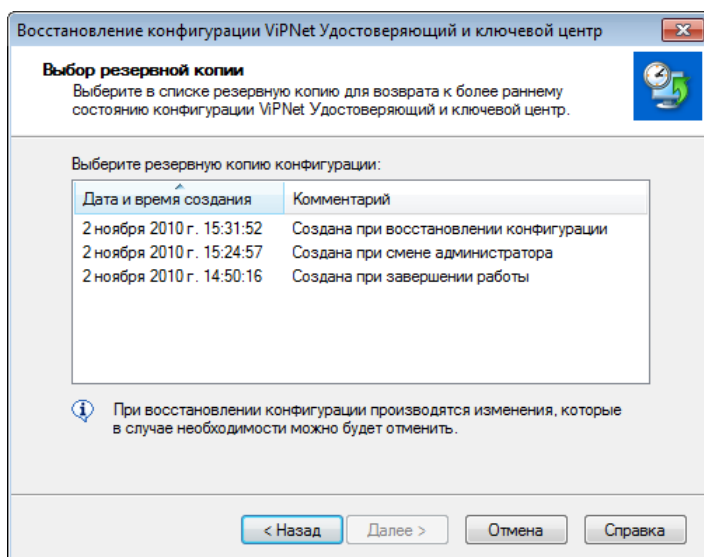


Рисунок 149: Восстановление резервной копии

Резервные копии, созданные автоматически, могут иметь следующие комментарии:

- Создана при завершении работы.
- Создана при восстановлении конфигурации.

Резервные копии конфигурации автоматически сортируются по дате и времени создания. Чтобы изменить порядок сортировки, щелкните заголовок столбца **Дата и время создания** или **Комментарий**.

Выберите резервную копию конфигурации, которую требуется восстановить, и нажмите кнопку **Далее**.

- 4 Начнется процесс восстановления выбранной конфигурации. При восстановлении конфигурации текущий пароль администратора для входа в ViPNet Удостоверяющий и ключевой центр не изменится.
- 5 Чтобы закончить работу мастера, на странице **Завершение восстановления конфигурации ViPNet Удостоверяющий и ключевой центр** нажмите кнопку **Готово**.

Чтобы выполнить другую операцию с резервными копиями, нажмите кнопку **В начало**.



Примечание. Всегда можно отменить последнее восстановление или восстановить конфигурацию из другой резервной копии, вернувшись на первую страницу мастера. Если мастер уже закрыт, заново запустите его.

В том случае если в процессе работы с программой изменялась папка ее установки (например, содержимое папки установки было перенесено в другую папку либо папка установки была переименована), после восстановления конфигурации следует проверить, правильно ли заданы папки обмена файлами с программой ViPNet Центр управления сетью (см. раздел [Настройка папок обмена](#) (на стр. 239)).

Редактирование списка резервных копий

Список резервных копий конфигурации можно редактировать: удалять резервные копии или изменять комментарии.

Для редактирования списка резервных копий конфигурации:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Восстановление конфигурации**. Будет запущен мастер **Восстановление конфигурации ViPNet Удостоверяющий и ключевой центр**.
- 2 На странице **Восстановление конфигурации ViPNet Удостоверяющий и ключевой центр** выберите **Редактировать список резервных копий** и нажмите кнопку **Далее**.
- 3 На странице **Редактирование списка резервных копий** выберите резервную копию, которую необходимо изменить. Чтобы изменить комментарий, нажмите кнопку **Редактировать комментарий**. Для удаления резервной копии нажмите кнопку **Удалить**.

Резервные копии конфигурации автоматически сортируются по дате и времени создания. Чтобы изменить порядок сортировки, щелкните заголовок столбца **Дата и время создания** или **Комментарий**.

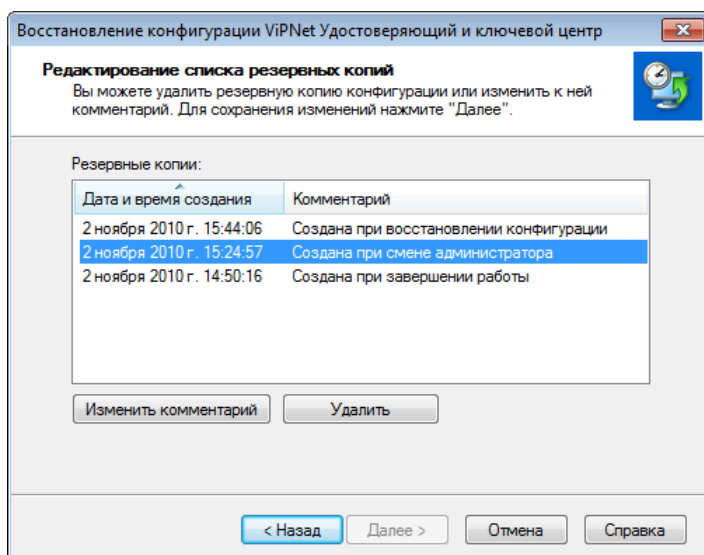


Рисунок 150: Редактирование списка резервных копий

- 4 Чтобы завершить редактирование, нажмите кнопку **Далее**.
 - 5 Чтобы закончить работу мастера, на странице **Завершение создания резервной копии конфигурации** нажмите кнопку **Готово**.
- Чтобы выполнить новую операцию с резервными копиями, нажмите кнопку **В начало**.

Отмена последнего восстановления конфигурации



Примечание. Это действие возможно только после восстановления конфигурации из резервной копии, если после этого не были созданы новые резервные копии конфигурации.

Чтобы отменить последнее восстановление конфигурации:

- 1 Выполните одно из действий:
 - В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Восстановление конфигурации**.
 - На последней странице мастера **Восстановление конфигурации ViPNet Удостоверяющий и ключевой центр** нажмите кнопку **В начало**.

- 2 На странице **Восстановление конфигурации ViPNet Удостоверяющий и ключевой центр** выберите **Отменить последнее восстановление**, затем нажмите кнопку **Далее**.

Начнется процесс отмены последнего восстановления конфигурации.


- 3 Чтобы закончить работу мастера, на странице **Завершение отмены последнего восстановления конфигурации** нажмите кнопку **Готово**.

Чтобы выполнить другую операцию с резервными копиями, нажмите кнопку **В начало**.

Настройка параметров создания резервных копий

В зависимости от настроек создание резервных копий конфигурации программы ViPNet Удостоверяющий и ключевой центр может осуществляться в автоматическом режиме и с заданной периодичностью.

Для настройки параметров создания резервных копий конфигурации:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Восстановление конфигурации**.

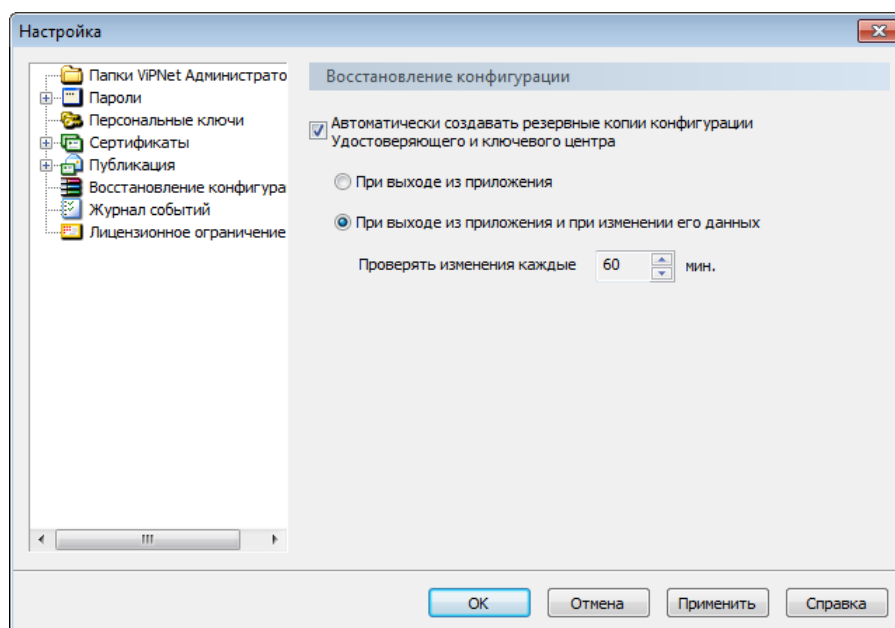


Рисунок 151: Настройка параметров восстановления конфигурации

- 3 Чтобы создание резервных копий осуществлялось в автоматическом режиме без участия администратора, установите флажок **Автоматически создавать резервные копии конфигурации Удостоверяющего и ключевого центра**, при этом:
- Для создания резервной копии при каждом выходе из программы ViPNet Удостоверяющий и ключевой центр выберите режим **При выходе из приложения**.
 - Для создания резервной копии не только при завершении работы с программой, но и с учетом вносимых изменений, выберите режим **При выходе из приложения и при изменении его данных** и в поле **Проверять изменения каждые** укажите интервал проверки изменений (в минутах).



Совет. Рекомендуется использовать данный режим при длительных сеансах работы с программой, в ходе которых она не закрывается.

- 4 Для сохранения настроек нажмите кнопку **Применить** и (или) **ОК**.

Работа с журналом событий ViPNet Удостоверяющий и ключевой центр

Информация о событиях, возникающих при работе программы ViPNet Удостоверяющий и ключевой центр, фиксируется в журнале событий. Настройка журнала событий описана в разделе [Настройка параметров журнала событий](#) (на стр. 287).

Просмотр журнала событий



Совет. Для корректного отображения записей журнала событий рекомендуется использовать Internet Explorer версии 6.0 и выше.

Для просмотра журнала событий выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Журнал событий**. Откроется окно **Просмотр журналов**.

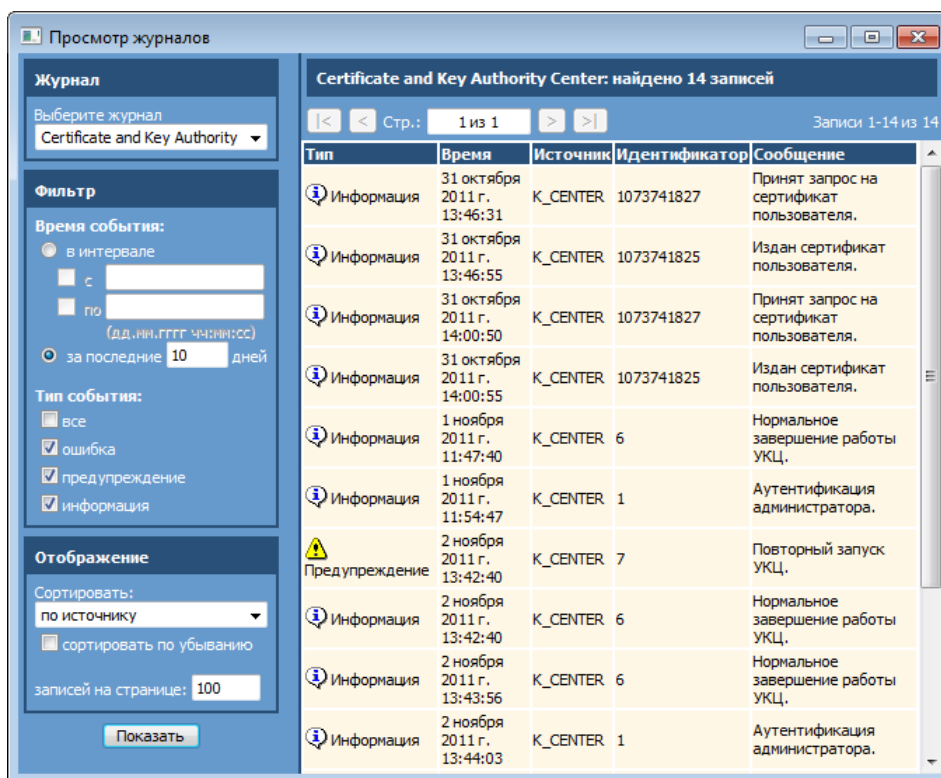


Рисунок 152: Просмотр журнала событий

2 В левой части окна **Просмотр журналов** на панели **Фильтр** задайте параметры поиска событий в журнале:

- Задайте время события одним из двух способов:
 - Для поиска событий, произошедших в определенном интервале времени, выберите пункт **в интервале**. Чтобы указать начало и конец интервала, установите соответствующие флажки **с** и **по** и в поле справа введите дату и время в формате `дд.мм.гггг чч:мм:сс`.
 - Для поиска событий, произошедших за последние несколько дней, выберите пункт **за последние** и в поле справа введите количество дней.

По умолчанию задан поиск событий за последние 10 дней.

- Задайте тип события, установив или сняв флажки **все**, **ошибка**, **предупреждение**, **информация**. По умолчанию задан поиск всех событий.

3 На панели **Отображение**:

- Из списка **Сортировать** выберите порядок сортировки. По умолчанию выбран пункт **< не сортировать >**.

- Если требуется изменить порядок сортировки событий, установите флажок **сортировать по убыванию** (этот флажок недоступен, если в списке **Сортировать** выбран пункт **< не сортировать >**).
 - В поле **Записей на странице** укажите число событий, отображаемых на одной странице (по умолчанию 100).
- 4 Задав параметры поиска, нажмите кнопку **Показать**. На правой панели окна **Просмотр журналов** отобразится список найденных событий (см. Рисунок 152 на стр. 286).
 - 5 Если результаты поиска отображаются на нескольких страницах, для переключения между страницами используйте кнопки, расположенные над списком событий.
 - 6 Чтобы просмотреть подробную информацию о каком-либо событии, щелкните строку этого события. Откроется окно **Информация о событии**.

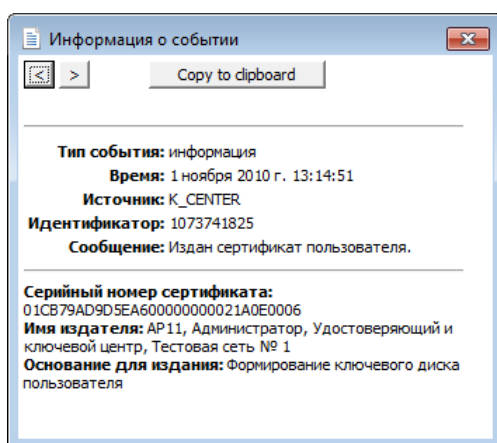





Рисунок 153: Подробная информация о событии

Чтобы перейти к предыдущему событию в списке, нажмите кнопку  в верхней части окна **Информация о событии**. Чтобы перейти к следующему событию, нажмите кнопку .

Настройка параметров журнала событий

С помощью настройки журнала событий можно включить или отключить опцию ведения журнала событий, определить его размер и другие параметры (в частности, детализацию и срок хранения архива журнала).

Для настройки параметров журнала событий выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Журнал событий**.

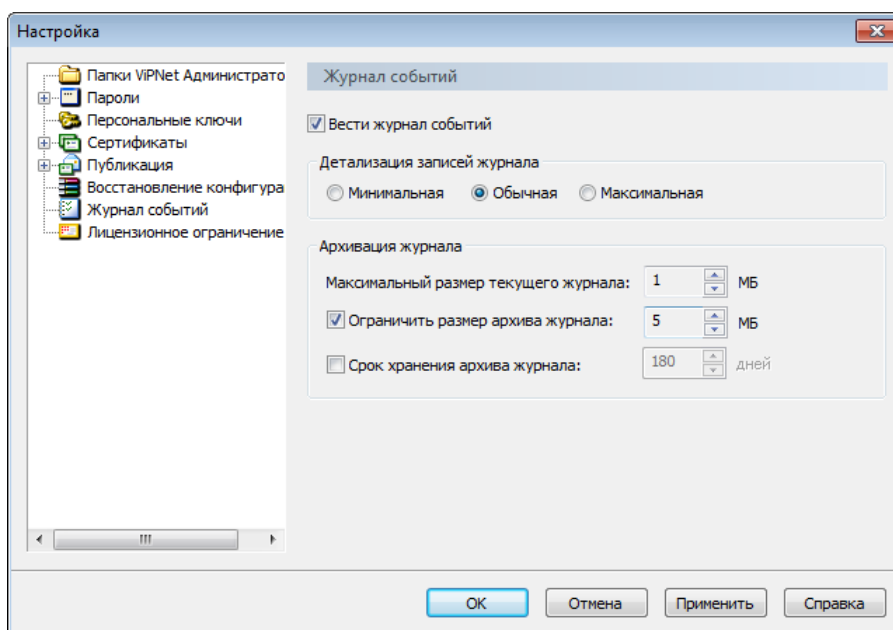


Рисунок 154: Настройка параметров журнала событий

- 3 Если требуется отключить ведение журнала событий, снимите флажок **Вести журнал событий**.
Если данный флажок снят, настройка остальных параметров журнала событий недоступна.
- 4 В группе **Детализация записей журнала** выберите один из пунктов:
 - **Минимальная** — фиксируются основные события, такие как: аутентификация администратора УКЦ, регистрация нового администратора, издание сертификата администратора, создание мастер-ключа своей сети, завершение работы УКЦ.
 - **Обычная** (выбран по умолчанию) — фиксируется наиболее важная информация, например: издание сертификата подписи, издание списка отозванных сертификатов, удовлетворение либо отклонение запроса на сертификат или его отзыв.
 - **Максимальная** — фиксируется вся информация.
- 5 В группе **Архивация журнала** задайте следующие параметры:

- В поле **Максимальный размер текущего журнала** введите размер журнала в мегабайтах (по умолчанию 1).

Если размер текущего файла журнала превышает заданное значение, файлу присваивается статус архивного и создается новый текущий файл журнала.

- Чтобы задать ограничение по размеру архива журнала, установите флажок **Ограничить размер архива журнала** и в поле справа введите размер архива в мегабайтах (по умолчанию 5).

Если суммарный размер архивных файлов журнала превысил заданное значение, последовательно удаляются самые старые архивные файлы до тех пор, пока суммарный размер архивов не станет меньше или равен заданному значению.

- Чтобы задать ограничение по времени хранения архива, установите флажок **Срок хранения архива журнала** и в поле справа введите максимальное время хранения архива в днях (по умолчанию 180).

Если время хранения архивного файла журнала (разница между текущим временем и временем перевода файла в архив) превышает заданное значение, такой файл удаляется.



Примечание. Если установлен флажок **Срок хранения архива журнала**, не рекомендуется изменять системное время, так как это может иметь негативные последствия.

- 6 Чтобы сохранить настройки, нажмите кнопку **Применить** и (или) **ОК**.

Проверка текущих данных

При запуске и в процессе работы программы ViPNet Удостоверяющий и ключевой центр автоматически производится проверка текущих данных на наличие следующих событий:

- **Критические** — события, при которых программа не может продолжать свою работу и закрывается.
- **Аномальные** — события, при которых осуществляется некорректная работа программы в части Удостоверяющего центра: все операции с сертификатами (издание, отзыв, импорт и прочее) либо недоступны, либо неуспешны. Функциональность программы в части Ключевого центра при этом полностью доступна и в целом программа остается работоспособной.



Примечание. Проверку данных на наличие аномальных ситуаций также можно выполнить вручную (см. [Ручная проверка текущих данных](#) (на стр. 294)).

- **Рабочие** — события, возникающие в рабочем порядке и не влияющие на функциональность программы.

Если в ходе проверки данных будет установлен факт возникновения какого-либо события, будет выдано соответствующее сообщение с его описанием.

Перечень возможных критических, аномальных и рабочих событий, а также описание действий администратора при возникновении данных событий приведены ниже в таблице.

Тип события	Описание события и форма оповещения	Рекомендуемые действия администратора программы
Критические события	<p>Нарушение целостности или повреждение исполняемых модулей программы, лицензионного файла <code>infotecs.re</code>.</p>	<p>Следует поставить в известность должностное лицо, ответственное за безопасность эксплуатации сети ViPNet и выявить причины появления данного события. Особое внимание рекомендуется уделить исключению возможностей несанкционированного доступа к компьютеру и умышленного искажения файлов. Восстановление работоспособности программы в данном случае возможно только путем переустановки программного обеспечения.</p>
	<p>Нарушение целостности ключей ViPNet (ключа защиты УКЦ, закрытого ключа текущего администратора).</p> <p>При обнаружении события появляется сообщение об ошибке инициализации администратора.</p>	<p>Следует выявить причины возникновения подобного события. В зависимости от того, какой ключ был поврежден, устранение ошибок возможно будет либо путем восстановления резервной копии конфигурации программы, либо путем переиздания сертификата администратора.</p>
Аномальные события	<p>Истечение срока действия закрытого ключа и соответствующего ему сертификата текущего администратора.</p> <p>За определенное количество дней до истечения срока действия (если установлена опция в настройках программы) либо при истечении срока действия появляется сообщение о том, что истекает (истек) срок действия закрытого ключа или сертификата текущего администратора.</p>	<p>Настоятельно рекомендуется издать новый сертификат администратора.</p>

Тип события	Описание события и форма оповещения	Рекомендуемые действия администратора программы
	<p>Истечение срока действия списка отозванных сертификатов.</p> <p>За определенное количество дней до истечения срока действия (если установлена опция в настройках программы) либо при истечении срока действия появляется соответствующее сообщение с предложением сформировать новый список отозванных сертификатов.</p> <p>Несоответствие номера сети в УКЦ.</p> <p>При запуске программы выдается сообщение, что отсутствует нужный файл.</p>	<p>Рекомендуется сформировать новый список отозванных сертификатов.</p> <p>Следует заменить файл <code>infotecs.re</code> идентичным файлом из программы ViPNet Центр управления сетью.</p>
Рабочие события	<p>Истечение срока действия закрытого ключа и соответствующего ему сертификата пользователя.</p> <p>За определенное количество дней до истечения срока действия (если установлена опция в настройках программы) либо при истечении срока действия появляется сообщение о том, что истекает (истек) срок действия закрытого ключа или соответствующего ему сертификата для следующего пользователя (списка пользователей).</p> <p>Наличие искажений в сертификатах администраторов доверенных сетей ViPNet, информации о пользователях и сетевых узлах, межсетевых мастер-ключях и прочем.</p> <p>При обнаружении искажений в процессе обращения к соответствующей информации появляется соответствующее сообщение об ошибке и выполнение ряда операций в программе будет невозможно до устранения неполадок.</p>	<p>Рекомендуется для пользователя, указанного в сообщении, сформировать новые ключи, предварительно получив файлы для создания ключей из ЦУСа.</p>

Тип события	Описание события и форма оповещения	Рекомендуемые действия администратора программы
	<p>Закончились лицензии на издание сертификатов пользователей в соответствии с лицензионным файлом <code>infotecs.re</code>.</p>	<p>Следует обратиться к представителю компании «ИнфоТеКС» с запросом на расширение текущей лицензии.</p>
	<p>Если число изданных сертификатов станет равным числу, указанному в настройках программы, либо максимальному числу, заявленному в лицензионном файле, появляется соответствующее сообщение. При достижении лимита издание сертификатов становится невозможным. Подробнее см. раздел Лицензионное ограничение (на стр. 14).</p>	
	<p>В папке <code>FROM_NCC</code> появились файлы сертификатов администраторов доверенных сетей ViPNet.</p>	<p>Рекомендуется выполнить импорт сертификатов.</p>
	<p>Выдается сообщение с предложением импортировать поступившие сертификаты администраторов.</p>	<p>При отказе от импорта поступившие сертификаты перемещаются в раздел Сертификаты администраторов > Доверенные сети ViPNet > Входящие.</p>
	<p>В папке <code>FROM_NCC</code> появились файлы с запросами на издание сертификатов от пользователей либо из Центра регистрации или файлы с запросами на отзыв сертификатов.</p>	<p>Рекомендуется обработать поступившие запросы.</p> <p>При отказе от обработки запросы на издание сертификатов перемещаются в раздел Запросы на сертификаты > Входящие > Своя сеть ViPNet (Внешние пользователи), запросы на отзыв сертификатов — Запросы на отзыв сертификатов > Входящие.</p>
	<p>Выдается сообщение с предложением обработать поступившие запросы.</p>	
	<p>В папке <code>FROM_NCC</code> появились файлы с информацией о новых сетевых узлах доверенной сети ViPNet и их связях.</p>	<p>Рекомендуется сформировать и отправить новые ключи узлов.</p>
	<p>Выдается сообщение о том, что требуется создать ключи узлов, связанных с новыми узлами доверенной сети.</p>	

Ручная проверка текущих данных

В программе ViPNet Удостоверяющий и ключевой центр предусмотрена возможность ручной проверки данных на наличие аномальных событий (описание возможных событий приведено в разделе [Проверка текущих данных](#) (на стр. 290)).

Чтобы вручную выполнить проверку данных, в окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Проверка текущих данных**. При успешной проверке появится сообщение, что аномальных ситуаций не обнаружено.

Экспорт служебных данных

Для организации межсетевого взаимодействия с доверенными сетями требуется набор служебных данных. Часть этих данных содержится в программе ViPNet Удостоверяющий и ключевой центр и при установке межсетевого взаимодействия должна быть экспортирована и отправлена в соответствующие доверенные сети с помощью программы ViPNet Центр управления сетью.

Из УКЦ экспортируются следующие служебные данные:

- список сертификатов администраторов;
- списки отозванных сертификатов пользователей своей сети ViPNet;
- имеющиеся кросс-сертификаты.

Экспорт указанных данных производится автоматически каждый раз при их изменении (например, при издании нового сертификата администратора, создании кросс-сертификата, обновлении списка отозванных сертификатов), но также может быть выполнен и вручную (см. «[Ручной экспорт данных](#)» на стр. 295).


Ручной экспорт данных

При необходимости выполните экспорт межсетевых служебных данных вручную. Для этого в окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Экспорт справочников**. По завершении экспорта появится соответствующее сообщение с указанием папки, в которую были скопированы служебные данные.

Учет ключей Деловой сети РФ

Возможны ситуации, когда в сети ViPNet в качестве координаторов используются программно-аппаратные комплексы (ПАК) ViPNet Linux Coordinator KB2. В составе ключевой структуры данных ПАКов используется ключи Деловой сети РФ (ДСРФ), формируемые сторонней уполномоченной организацией. При получении и перед вводом в действие полученные ключи ДСРФ в обязательном порядке регистрируются в программе ViPNet Удостоверяющий и ключевой центр — каждому ключу присваиваются соответствующие серия и номер.

Для регистрации ключей ДСРФ выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
- 2 В появившемся окне на панели навигации выберите раздел **Ключи Деловой сети РФ**.



Примечание. Раздел **Ключи Деловой сети РФ** в настройках программы отображается только в том случае, если в программе ViPNet Центр управления сетью в конфигурации сети имеются ПАКи ViPNet Linux Coordinator KB2 (координаторы, зарегистрированные в прикладной задаче «VPN-координатор KB2»). Подробнее см. документ «ViPNet Administrator Центр управления сетью. Руководство администратора», главу «Регистрация АП и СМ в прикладных задачах».

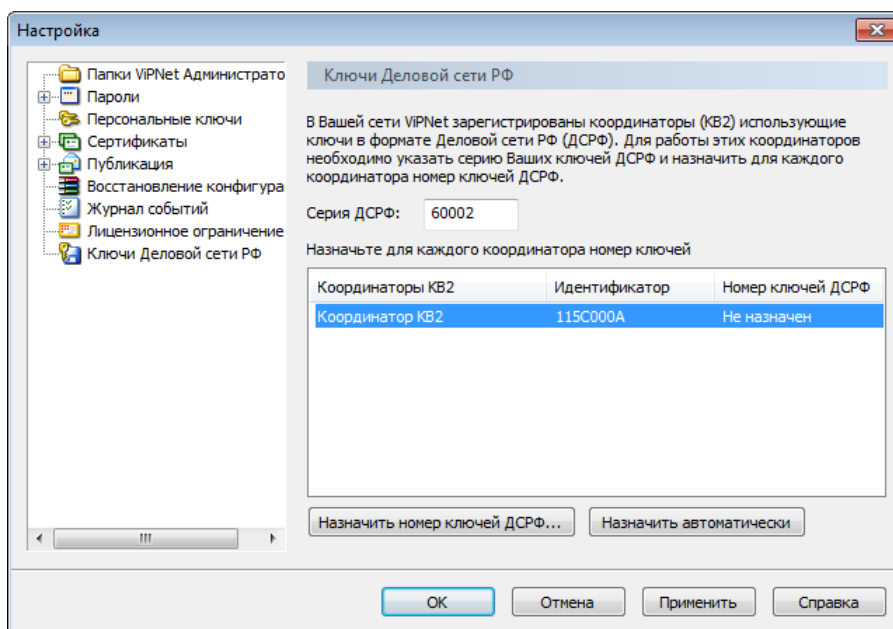


Рисунок 155: Управление ключами ДСРФ

- 3 В поле **Серия ДСРФ** введите серию ключей ДСРФ. Серия должна быть представлена в числовом формате и может содержать не более 6 символов.
- 4 Ключам каждого координатора из списка назначьте уникальный номер одним из следующих способов:



Примечание. В списке отображаются имена и идентификаторы всех зарегистрированных ПАКов ViPNet Linux Coordinator KB2. По умолчанию номера ключей не заданы.

- Чтобы вручную присвоить номер ключам ДСРФ, в списке выберите координатор и нажмите кнопку **Назначить номер диска ДСРФ**, после чего в появившемся окне введите номер ключей (в диапазоне от 1 до 9999) и нажмите кнопку **ОК**. В том случае если введенный номер уже используется, появится сообщение с предложением указать другой номер.
 - Чтобы автоматически присвоить номера одновременно ключам всех координаторов, нажмите кнопку **Назначить автоматически**. Присвоение номеров произойдет для ключей всех координаторов в порядке, соответствующем порядку сортировки координаторов по возрастанию. Новый номер будет назначен в том числе и для тех ключей координаторов, у которых он уже был.
- 5 По завершении ввода данных нажмите кнопку **Применить** и (или) **ОК**.

После задания серии и номеров ключей координаторов можно выполнить обновление ключей.



A

Перенос базы данных УКЦ на SQL-сервер

Возможна ситуация, при которой может потребоваться перенос базы данных программы ViPNet Удостоверяющий и ключевой центр, первоначально сформированной локально на компьютере средствами Microsoft Access, на SQL-сервер (например, при увеличении ее объема либо для повышения скорости выполняемых в УКЦ операций).



Внимание! Перенос базы данных УКЦ на SQL-сервер должен производить администратор SQL-сервера совместно с администратором УКЦ. Для успешного переноса следует выполнить все перечисленные ниже действия.

Если в наличии нет готового к использованию SQL-сервера, то перед переносом базы данных требуется его развернуть. SQL-сервер должен соответствовать требованиям, описанным в разделе [Требования к SQL-серверу для развертывания базы данных УКЦ](#) (на стр. 33). Если SQL-сервер будет размещен не на одном компьютере с УКЦ, то также потребуются предоставить к нему доступ для подключения с компьютера, на котором установлен УКЦ.

Для переноса уже развернутой базы данных УКЦ на SQL-сервер выполните следующие действия:

- 1 На развернутом SQL-сервере в соответствующем экземпляре вручную создайте базу данных «КС».

- 2 В сформированную базу «КС» импортируйте данные из начальной базы УКЦ, созданной по шаблону Microsoft Access (с расширением `.mdb`, по умолчанию `kc.mdb`). Для импорта потребуется доступ к папке хранения исходной базы данных. При отсутствии доступа к указанной папке файл исходной базы можно непосредственно скопировать на SQL-сервер.



Примечание. По умолчанию папкой хранения считается рабочая папка, заданная при первичной инициализации (см. «[Проведение первичной инициализации программы](#)» на стр. 50). Посмотреть путь к рабочей папке можно в настройках программы, в разделе **Папки ViPNet Администратора** (см. раздел [Настройка папок обмена](#) (на стр. 239)).

- 3 В службе технической поддержки компании «ИнфоТеКС» (см. «[Обратная связь](#)» на стр. 41) получите файл `kc add primary key.sql` и запустите скрипт, который в нем содержится.

В данном файле содержится скрипт добавления признака первичного ключа атрибуту **ID** в таблицах базы данных «КС», в которых он присутствует. По умолчанию этот атрибут присутствует во всех таблицах, кроме: `dbo.History`, `dbo.NetworkGroupAbonent`, `dbo.RelationShipGroup`, `dbo.RNodeGroup`.

- 4 Во всех таблицах базы данных «КС» вручную измените свойство **Спецификация идентификатора** атрибута **ID**.
- 5 На компьютере с установленным УКЦ в файле настроек `kc.ini` измените тип драйвера ODBC для доступа и работы с базой данных УКЦ. Файл `kc.ini` хранится в папке установки УКЦ (см. «[Установка программы](#)» на стр. 48).
- 6 По окончании всех операций запустите УКЦ (см. «[Запуск и завершение работы с программой](#)» на стр. 59).
- 7 После ввода пароля администратора УКЦ появится окно подключения к SQL-серверу. Укажите в нем необходимые параметры подключения (см. раздел [Подключение к SQL-серверу при запуске программы](#) (на стр. 62)).
- 8 Проверьте корректность работы программы и наличие данных.
После этого перенос данных на SQL-сервер можно считать завершённым.

Чтобы создать базу данных «КС»:

- 1 Запустите программу Microsoft SQL Server Management Studio. В окне соединения с сервером укажите имя SQL-сервера, экземпляр и режим аутентификации.

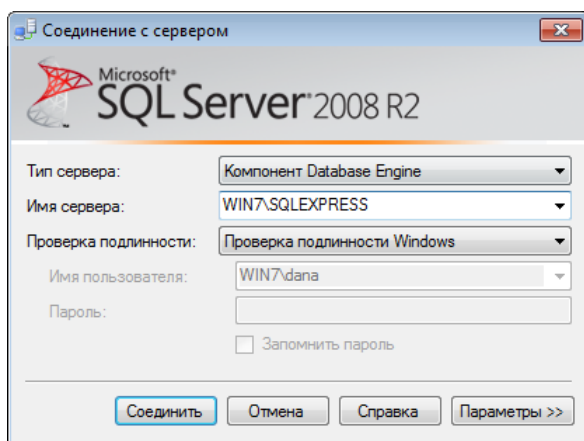


Рисунок 156: Задание параметров подключения к SQL-серверу

- 2 На панели навигации щелкните правой кнопкой мыши раздел **Базы данных** и в контекстном меню выберите пункт **Создать базу данных**.
- 3 В появившемся окне введите имя базы данных (в нашем случае — «КС») и нажмите кнопку **ОК**.

Созданная база данных отобразится на панели навигации в разделе **Базы данных**.

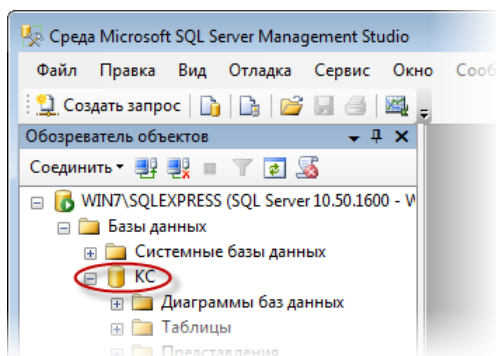


Рисунок 157: Результат создания базы данных

Чтобы импортировать данные из начальной базы в новую базу на SQL-сервере:

- 1 Щелкните правой кнопкой мыши по созданной базе данных «КС» и в контекстном меню выберите пункт **Задачи > Импорт данных**. Запустится мастер импорта и экспорта данных, следуйте его указаниям.
- 2 На странице **Выбор источника данных** в списке **Источник данных** выберите **Microsoft Access** и с помощью кнопки **Обзор** укажите файл начальной базы данных.

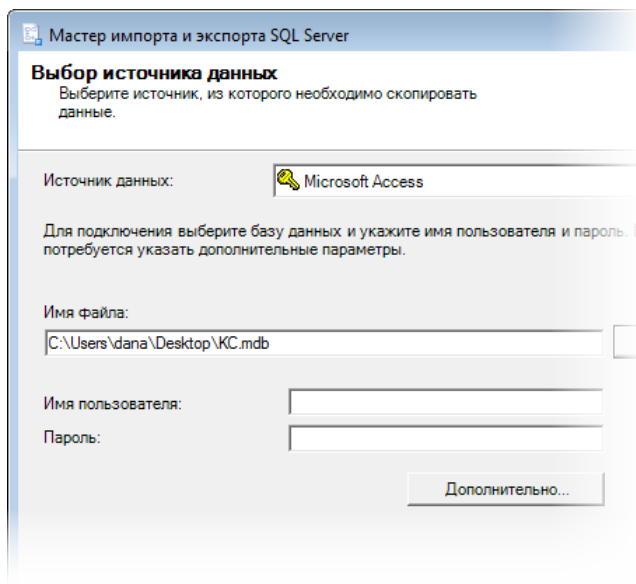


Рисунок 158: Выбор первичной базы данных для переноса данных

- 3 На странице **Выбор назначения** укажите имя и экземпляр SQL-сервера, тип аутентификации и выберите базу данных. По умолчанию уже установлены все необходимые значения, не рекомендуется их изменять.

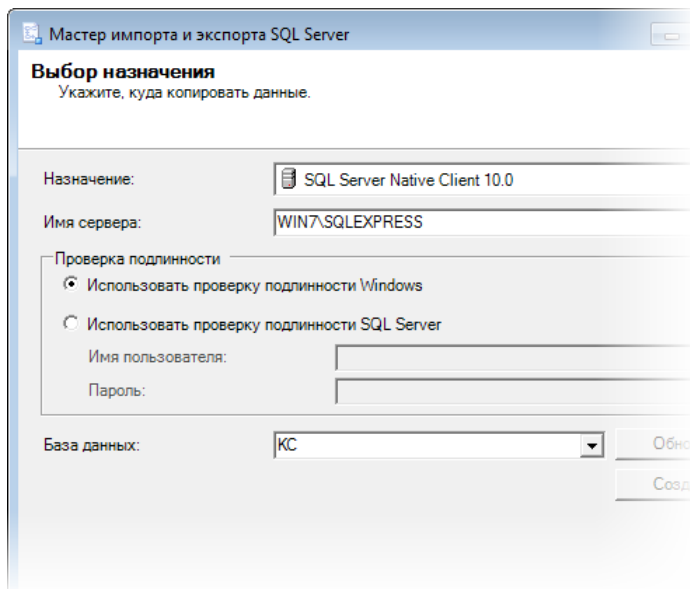


Рисунок 159: Выбор базы данных на SQL-сервере для переноса данных

- 4 На странице **Выбор копирования таблицы или запроса** установите переключатель в положение **Скопировать данные из одной или нескольких таблиц или представлений.**

- 5 На странице **Выбор исходных таблиц и представлений** в списке выберите все имеющиеся таблицы, установив флажок в поле **Источник** в заголовке списка.

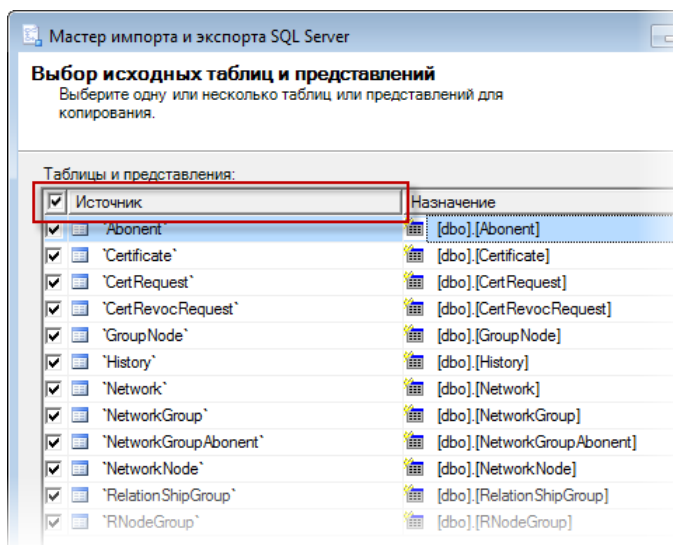


Рисунок 160: Редактирование свойств таблиц исходной базы данных

- 6 На странице **Завершение работы мастера** нажмите кнопку **Готово**. Начнется процесс переноса данных.

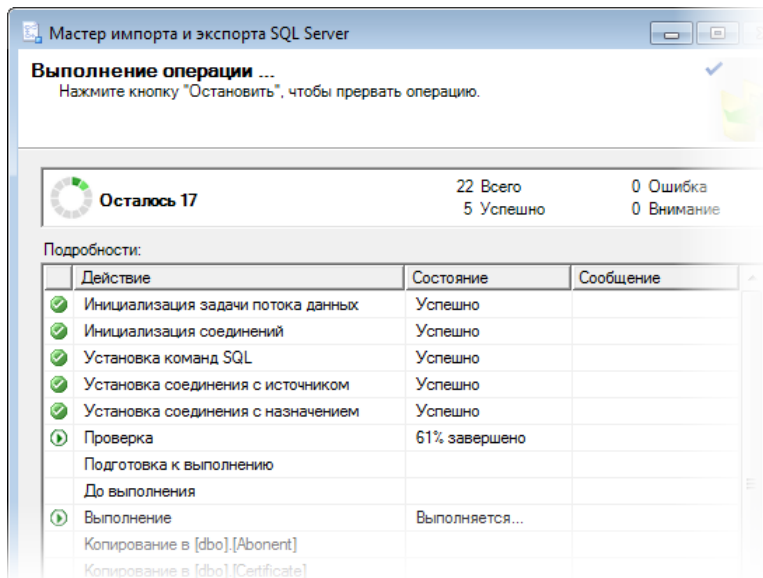



Рисунок 161: Результат переноса данных в базу данных на SQL-сервере

- 7 На последней странице мастера ознакомьтесь с результатами переноса данных в SQL-базу и нажмите кнопку **Закреть**.

Все операции по переносу данных должны быть выполнены успешно. Если какие-то операции были выполнены с ошибками, удалите базу данных «КС», создайте новую с таким же именем и повторите процедуру импорта.

Чтобы запустить скрипт, содержащийся в файле `kc add primary key.sql`:

- 1 Файл `kc add primary key.sql` поместите на компьютер с развернутым SQL-сервером.
- 2 Дважды щелкните по данному файлу. Текст скрипта отобразится на отдельной вкладке в программе Microsoft SQL Server Management Studio.
- 3 В окне программы на панели инструментов нажмите кнопку  **Выполнить**.

При успешном завершении работы скрипта атрибуту **ID** в соответствующих таблицах базы данных будет присвоен признак первичного ключа.

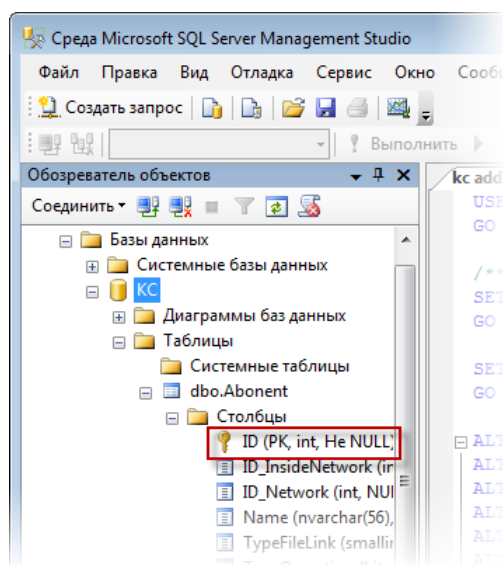


Рисунок 162: Результат создания первичных ключей

Чтобы в таблице базы данных «КС» изменить свойство **Спецификация идентификатора** атрибута **ID**:

- 1 Щелкните по таблице правой кнопкой мыши и в контекстном меню выберите пункт **Проект**.
- 2 В появившемся списке атрибутов таблицы выберите **ID**.
- 3 На вкладке свойств атрибута раскройте свойство **Спецификация идентификатора** и для параметра (**Идентификатор**) установите значение **Да**.

- 4 На панели инструментов нажмите кнопку **Сохранить** <название таблицы>.



Внимание! Перед сохранением изменений в таблице убедитесь, что в окне настройки параметров (Сервис > Параметры) в разделе **Конструкторы** снят флажок **Запретить сохранение изменений, требующих повторного создания таблицы**. В противном случае, сохранение изменений будет невозможно.

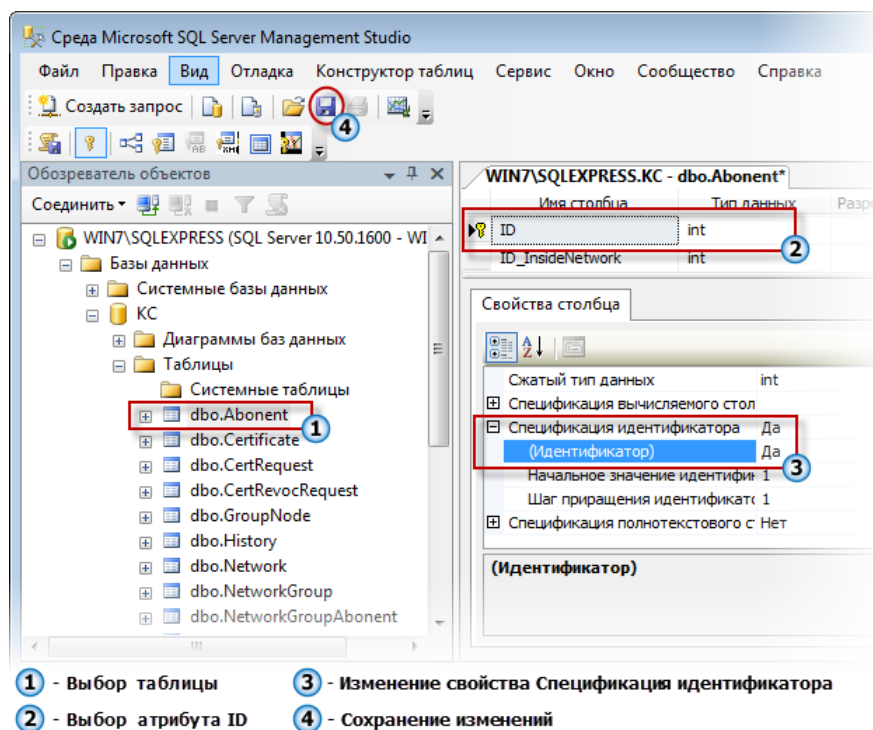


Рисунок 163: Изменение свойства атрибута ID

Чтобы изменить тип выбранного драйвера ODBC:

- 1 С помощью текстового редактора откройте файл настроек `kc.ini`.
- 2 В секции `[Database]` параметру `ODBC Driver` присвойте значение 1. Значение 1 данного параметра означает выбор драйвера **SQL Server** для работы с базой данных УКЦ на SQL-сервере.
- 3 Сохраните внесенные изменения.



В

Глоссарий

О

ODBC (Open Database Connectivity)

Стандартный программный интерфейс (Application Programming Interface, API) доступа к различным источникам данных (базам данных), разработанный компанией Microsoft.

Р

PKI (инфраструктура открытых ключей)

PKI (инфраструктура открытых ключей) — комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам в распределенных системах через создание сертификатов открытых ключей и поддержание их жизненного цикла.

См. также: [Открытый ключ](#).

У

ViPNet Administrator

Набор программного обеспечения для администрирования сети ViPNet, включающий в себя ЦУС и УКЦ.

См. также: [Сеть ViPNet](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#), [Центр управления сетью \(ЦУС\)](#).

ViPNet Publication Service

Программное обеспечение для публикации сертификатов пользователей, издателей (администраторов) и списков отозванных сертификатов в общедоступных хранилищах данных.

См. также: [Список отозванных сертификатов \(СОС\)](#).

ViPNet Registration Point

Программное обеспечение, предназначенное для регистрации пользователей ViPNet и хранения их регистрационных данных, а также для выдачи сертификатов подписи и дистрибутивов ключей, создаваемых в программе ViPNet Удостоверяющий и ключевой центр по соответствующим запросам.

См. также: [Дистрибутив ключей](#), [Пользователь ViPNet](#), [Сертификат открытого ключа подписи пользователя](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#).

A

Абонентский пункт (АП)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора абонентский пункт не выполняет функции маршрутизации трафика и служебной информации.

См. также: [Координатор \(ViPNet-координатор\)](#), [Маршрутизация](#), [Сетевой узел ViPNet \(СУ\)](#).

Администратор сети ViPNet

Лицо, отвечающее за конфигурирование сети ViPNet, создание и обновление справочно-ключевой информации для сетевых узлов ViPNet, настройку межсетевое взаимодействие с доверенными сетями и обладающее правом доступа к программе ViPNet Manager или ViPNet ЦУС и (или) ViPNet УКЦ.

См. также: [Доверенная сеть](#), [Межсетевое взаимодействие](#), [Обновление справочно-ключевой информации](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#), [Центр управления сетью \(ЦУС\)](#), [ViPNet Manager](#).

Администратор УКЦ

Лицо, обладающее правом доступа в Удостоверяющий и ключевой центр (УКЦ), отвечающее за создание и обновление справочно-ключевой информации сетевых узлов ViPNet, создание и отзыв сертификатов ViPNet, обеспечение взаимодействия с доверенными сетями ViPNet.

См. также: [Доверенная сеть](#), [Обновление справочно-ключевой информации](#), [Сетевой узел ViPNet \(СУ\)](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#).

Адресные справочники

Набор файлов, содержащих информацию об объектах сети ViPNet (узлах, пользователях, коллективах), в том числе об их именах, идентификаторах, адресах, связях. Эти файлы формируются управляющими приложениями ViPNet, предназначенными для создания структуры и конфигурирования сети ViPNet (ViPNet ЦУС, ViPNet Manager).

См. также: [Центр управления сетью \(ЦУС\)](#), [ViPNet Manager](#).

Аккредитованный Удостоверяющий центр

Удостоверяющий центр, прошедший аккредитацию федеральным органом исполнительной власти и получивший сертификат соответствия требованиям Федерального закона РФ № 63 «Об электронной подписи» от 6 апреля 2011 года.

См. также: [Удостоверяющий центр](#).

Асимметричный ключ

Один из двух ключей (закрытый или открытый), которые используются в инфраструктуре открытых ключей (Public Key Infrastructure (PKI)). При использовании PKI создаются два взаимосвязанных асимметричных ключа: закрытый ключ и открытый ключ. В зависимости от назначения различают асимметричные ключи подписи и асимметричные ключи шифрования.

См. также: [PKI \(инфраструктура открытых ключей\)](#).

Аутентификация

Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности). Аутентификация осуществляется на основании того или иного секретного элемента (аутентификатора), которым располагает субъект.

В

Внешний пользователь ViPNet

Пользователь, для которого в Удостоверяющем центре сети ViPNet издан сертификат открытого ключа подписи и который не является внутренним пользователем сети ViPNet.

См. также: [Внутренний пользователь сети ViPNet](#) (см. «[Внутренний пользователь ViPNet](#)»), [Сеть ViPNet](#), [Сертификат открытого ключа подписи пользователя](#).

Внутренний пользователь ViPNet

Пользователь, зарегистрированный в сети ViPNet. Администратор сети создает для пользователя дистрибутив ключей и пароль пользователя. Пользователь может быть зарегистрирован в составе одного или нескольких коллективов на одном или нескольких сетевых узлах одной и той же сети ViPNet.

Внутренний пользователь может выступать в роли внешнего, если у него есть право подписи и сертификат открытого ключа подписи.

См. также: [Администратор сети ViPNet](#), [Внешний пользователь ViPNet](#), [Дистрибутив ключей](#), [Коллектив](#), [Пароль пользователя](#), [Сертификат открытого ключа подписи пользователя](#), [Сеть ViPNet](#).

Выпуск (издание) сертификата

Заполнение необходимых полей сертификата и заверение его электронной подписью Удостоверяющего центра.

См. также: [Удостоверяющий и ключевой центр \(УКЦ\)](#), [Электронная подпись](#).

Вышестоящий удостоверяющий центр

Если удостоверяющий центр (А) является вышестоящим по отношению к удостоверяющему центру (Б), это значит, что он находится выше УЦ (Б) в иерархической системе доверительных отношений между удостоверяющими центрами. Может быть подчиненным по отношению к удостоверяющему центру (В), если не является головным.

См. также: [Головной удостоверяющий центр](#), [Подчиненный удостоверяющий центр](#), [Удостоверяющий центр](#).

Г

Головной удостоверяющий центр

Удостоверяющий центр, который находится на вершине иерархической системы доверительных отношений между удостоверяющими центрами.

См. также: [Вышестоящий удостоверяющий центр](#), [Иерархия удостоверяющих центров](#), [Подчиненный удостоверяющий центр](#), [Удостоверяющий центр](#).

Д

Дистрибутив ключей

Файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Manager для каждого пользователя сетевого узла ViPNet. В этом файле помещены адресные справочники, ключевая информация и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

См. также: [Адресные справочники](#), [Сетевой узел ViPNet \(СУ\)](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#), [Файл лицензии](#).

Доверенная сеть

Сеть ViPNet, с узлами которой своя сеть ViPNet осуществляет защищенное взаимодействие.

См. также: [Межсетевое взаимодействие](#), [Своя сеть](#).

З

Закрытый ключ

Сохраняемый в тайне элемент ключевой пары, используемый при асимметричном шифровании. Закрытый ключ применяется при формировании электронной подписи в процессе подписания исходящего сообщения, а также при расшифровании полученного сообщения.

См. также: [Асимметричный ключ](#), [Открытый ключ](#), [Электронная подпись](#).

Запрос на сертификат

Файл, содержащий имя пользователя в формате X.500, открытый ключ и его параметры, желаемый срок действия сертификата, предполагаемые назначения сертификата и другие параметры (полный набор параметров зависит от формата запроса и программного обеспечения, в котором он был сформирован).

Запрос может быть сформирован как на издание нового, так и на обновление уже имеющегося сертификата.

См. также: [Сертификат открытого ключа подписи пользователя, Открытый ключ, Закрытый ключ](#).

И

Идентификатор объекта (OID)

Каждый объект может быть описан несколькими классами с соответствующими этим классам атрибутами. Каждому классу или атрибуту может быть присвоен уникальный идентификатор OID (Object Identifier) и имя.

Формат сертификата X.509 версии 3, существующий и используемый на данный момент, предполагает наличие полей расширенного применения, политик сертификации и стандартных полей. Данные поля определяют области применения, ограничения на использования сертификата, криптографические алгоритмы и другие параметры. Применение OID позволяет однозначно определить данные в сертификате, заменив объемное текстовое описание.

См. также: [Сертификат открытого ключа подписи пользователя, Открытый ключ, Электронная подпись](#).

Иерархия удостоверяющих центров

Система распространения доверительных отношений между удостоверяющими центрами, в которой вышестоящие удостоверяющие центры выпускают сертификаты для подчиненных удостоверяющих центров.

См. также: [Вышестоящий удостоверяющий центр, Головной удостоверяющий центр, Подчиненный удостоверяющий центр, Удостоверяющий центр](#).

К

Квалифицированный сертификат

Сертификат открытого ключа подписи, выданный аккредитованным Удостоверяющим центром (или его доверенным лицом) либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

См. также: [Аккредитованный Удостоверяющий центр](#), [Сертификат открытого ключа подписи пользователя](#), [Электронная подпись](#).

Ключ защиты УКЦ

Ключ, на котором защищены список администраторов Удостоверяющего и ключевого центра, мастер-ключи, пароли пользователей ViPNet, ключи пользователя при хранении их в УКЦ.

См. также: [Администратор УКЦ](#), [Ключи пользователя ViPNet](#), [Пароль пользователя](#).

Ключи пользователя ViPNet

Совокупность файлов, необходимых пользователю для аутентификации в сети ViPNet, к которым имеет доступ только данный пользователь.

Ключи пользователя могут содержать:

- действующий персональный ключ пользователя;
- случайный ключ защиты пользователя;
- контейнер с ключом (ключами) подписи;
- файл хэша пароля пользователя.

Содержимое ключей пользователя формируется в зависимости от типа аутентификации пользователя.

См. также: [Аутентификация](#), [Персональный ключ пользователя](#).

Ключи узла ViPNet

Совокупность файлов, необходимых пользователям сетевых узлов ViPNet для защиты информации приложений ViPNet, хранимой локально на компьютере, и (или) трафика, а также для проверки электронной подписи.

См. также: [Сетевой узел ViPNet \(СУ\)](#), [Электронная подпись](#).

Компрометация ключей

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

После компрометации необходимо создать ключи пользователя и ключи узлов и выслать обновления на сетевые узлы ViPNet. Поскольку изменяются как общие ключи, так и личные, а также ключи обмена, необходимо выслать ключи узлов на все сетевые узлы ViPNet, связанные с данным сетевым узлом.

См. также: [Ключ обмена](#), [Ключи пользователя ViPNet](#), [Ключи узла ViPNet](#), [Сетевой узел ViPNet \(СУ\)](#).

Контейнер ключей

Файл, в котором хранятся закрытый ключ и соответствующий ему сертификат открытого ключа.

При формировании запроса на обновление сертификата имя контейнера, в котором будет храниться новая пара ключей подписи (закрытый и сертификат), задается автоматически и имеет вид `sgn-
<случайное число 16-ричного формата>`.

См. также: [Сертификат открытого ключа подписи пользователя](#).

Контрольная сумма

Значение, используемое для проверки целостности файла.

Корневой сертификат

Самоподписанный сертификат администратора удостоверяющего центра, являющийся последним сертификатом в цепочке доверия, то есть для корневого сертификата нет сертификата, на котором его можно было бы проверить. С помощью корневого сертификата проверяется достоверность сертификатов пользователей сети.

См. также: [Сертификат открытого ключа подписи пользователя](#).

Кросс-сертификат

Сертификат уполномоченного лица одного удостоверяющего центра, изданный уполномоченным лицом другого удостоверяющего центра.

См. также: [Кросс-сертификация](#), [Уполномоченное лицо \(администратор\) удостоверяющего центра](#).

Кросс-сертификация

Механизм установления доверительных отношений между удостоверяющими центрами.

См. также: [Удостоверяющий центр](#).

М

Мастер-ключ

Ключ для формирования симметричных ключей в результате шифрования на нем пары идентификаторов соответствующих коллективов или сетевых узлов ViPNet. В сети ViPNet формируется три вида мастер-ключей:

- мастер-ключ ключей обмена коллективов,
- мастер-ключ ключей защиты ключей обмена,
- мастер-ключ персональных ключей пользователей.

Мастер-ключ формируется с помощью датчика случайных чисел. Мастер-ключ хранится в программе ViPNet Удостоверяющий и ключевой центр в полной секретности, поскольку компрометация мастер-ключа приводит к компрометации всех ключей, сформированных на его основе.

При установлении взаимодействия с другой виртуальной сетью в качестве мастер-ключа для генерации межсетевых ключей обмена используются так называемый межсетевой мастер-ключ.

См. также: [Ключ обмена](#), [Коллектив](#), [Компрометация ключей](#), [Межсетевой мастер-ключ](#), [Персональный ключ пользователя](#), [Сетевой узел ViPNet \(СУ\)](#), [Сеть ViPNet](#), [Симметричный ключ](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#).

Межсетевое взаимодействие

Между своей сетью и другими сетями ViPNet может быть организовано межсетевое взаимодействие. Межсетевое взаимодействие позволяет сетевым узлам различных сетей ViPNet обмениваться информацией по защищенным каналам. Для организации взаимодействия между сетевыми узлами различных сетей ViPNet администраторы этих сетей обмениваются межсетевой информацией.

См. также: [Администратор сети ViPNet](#), [Межсетевая информация](#), [Своя сеть](#).

Межсетевой мастер-ключ

Ключ, служащий для формирования ключей обмена между сетевыми узлами разных сетей ViPNet.

См. также: [Ключ обмена](#), [Сетевой узел ViPNet \(СУ\)](#), [Сеть ViPNet](#).

О

Обновление ключей узла

Совокупность файлов, к которым относятся справочники сертификатов администраторов УКЦ, списки отозванных сертификатов (как своей сети, так и доверенных), контрольные суммы паролей администраторов, корневые сертификаты администраторов доверенных сетей и служебная информация о пользователе данного узла (право подписи).

Фактически, обновление ключей узла является урезанным вариантом ключей узла ViPNet.

При внесении каких-либо изменений в структуру сети ViPNet администратором сети ViPNet адресные справочники и ключи узлов, которых коснулись эти изменения, тоже изменяются. В этом случае администратор должен разослать обновления ключей узлов на эти узлы сети ViPNet.

Обновление ключей узла формируется в УКЦ, рассылается из ЦУСа. После обновления ключей узла изменяется справочно-ключевая информация для сетевых узлов ViPNet.

См. также: [Адресные справочники](#), [Доверенная сеть](#), [Ключи узла ViPNet](#), [Контрольная сумма](#), [Корневой сертификат](#), [Своя сеть](#), [Список отозванных сертификатов \(СОС\)](#), [Справочно-ключевая информация](#).

Отзыв сертификата

Признание сертификата недействительным в период его действия (например, в случае компрометации соответствующего закрытого ключа).

См. также: [Компрометация ключей](#).

П

Пароль администратора УКЦ

Пароль для входа в программу ViPNet Administrator УКЦ.

Пароль пользователя

Индивидуальный пароль пользователя для работы в приложениях ViPNet на сетевом узле ViPNet. Первоначально создается администратором сети ViPNet в УКЦ или ViPNet Manager. Этот пароль может быть изменен пользователем на сетевом узле ViPNet.

См. также: [Администратор сети ViPNet](#), [Пользователь ViPNet](#), [Сетевой узел ViPNet \(СУ\)](#), [ViPNet Manager](#).

Пароль пользователя на основе парольной фразы

Пароль пользователя необходим для входа в любую программу ViPNet. Случайный пароль создается на основе парольной фразы, которую можно использовать для запоминания пароля. Парольные фразы могут быть созданы на русском, английском и немецком языках. Фразы представляют собой грамматически корректные конструкции, однако слова, составляющие фразу, выбираются случайным образом из большого по объему словаря (русского, немецкого или английского). Парольная фраза может содержать 3 или 4 слова, при желании пароль может быть создан из двух парольных фраз.

Чтобы получить пароль из парольной фразы, достаточно набрать без пробелов в английской раскладке первые X букв из каждого слова парольной фразы, содержащей Y слов. Пользователь сам задает параметры X и Y, а также язык парольной фразы.

Например, при использовании трех первых букв из каждого слова парольной фразы «Затейливый ювелир утащил сдобу» получим пароль «pfm.dtenfclj».

См. также: [Пароль пользователя](#), [Парольная фраза](#).

Парольная фраза

Набор грамматически согласованных между собой слов, выбираемых случайным образом из специальных словарей. Парольная фраза формируется при создании паролей и служит для их запоминания. Пароль из парольной фразы получается по следующему правилу: в латинской раскладке клавиатуры набираются по N первых букв от каждого из M слов парольной фразы без пробелов, где N определяется длиной пароля.

Например, парольной фразе «**служ**ащий **лата**ет **рель**с» соответствует пароль «ske;kfnfhktm». В данном случае, при вводе пароля необходимо набирать по 4 первых буквы каждого слова парольной фразы.

См. также: [Пароль пользователя на основе парольной фразы](#).

Персональный ключ пользователя

Главный ключ защиты ключей, к которым имеет доступ пользователь. Персональный ключ используется для защиты ключей пользователя. Действующий персональный ключ входит в состав ключей пользователя, поэтому его необходимо хранить в безопасном месте, так как компрометация этого ключа означает компрометацию всех других ключей пользователя и ключей защиты коллективов, в которых пользователь зарегистрирован. При компрометации ключей пользователя в УКЦ изменяется вариант персонального ключа пользователя (его порядковый номер в РНПК), при этом для него устанавливается следующий ключ из резервного набора персональных ключей (РНПК).

См. также: [Ключи пользователя ViPNet](#), [Коллектив](#), [Компрометация ключей](#), [Пользователь ViPNet](#), [Резервный набор персональных ключей \(РНПК\)](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#).

Подчиненный удостоверяющий центр

Удостоверяющий центр, которому в иерархической системе распространения доверительных отношений доверяет вышестоящий удостоверяющий центр.

См. также: [Вышестоящий удостоверяющий центр](#), [Головной удостоверяющий центр](#), [Иерархия удостоверяющих центров](#), [Удостоверяющий центр](#).

Политика применения сертификата

Расширение сертификата открытого ключа подписи, определяющее, в каких случаях допустимо или следует использовать данный сертификат в соответствии с требованиями безопасности.

Содержит сведения об авторских правах, политиках выдачи сертификатов, ограничениях ответственности и другие. В сертификате представлена идентификатором объекта (также называемым OID) в формате X.509.

См. также: [Идентификатор объекта \(OID\)](#), [Сертификат открытого ключа подписи пользователя](#).

Пользователь ViPNet

Лицо, которое использует программное обеспечение ViPNet или которое может иметь ключи электронной подписи.

Условно пользователей ViPNet можно разделить на внутренних и внешних.

См. также: [Внешний пользователь ViPNet](#), [Внутренний пользователь ViPNet](#), [Электронная подпись](#).

Приостановление действия сертификата

Однократное временное ограничение действия сертификата в период его действия.

Публикация

Размещение сформированной в УКЦ информации на источниках данных, доступных по общеизвестным протоколам (например, FTP, LDAP).

См. также: [Удостоверяющий и ключевой центр \(УКЦ\)](#).

Р

Резервный набор персональных ключей (РНПК)

Администратор УКЦ создает для пользователя несколько запасных персональных ключей (в виде файла AAAA.pk, где AAAA – идентификатор пользователя в рамках своей сети). Резервный набор персональных ключей (РНПК) пользователя предназначен для удаленного обновления ключей пользователя при их компрометации и при смене мастер-ключа персональных ключей. Файл РНПК входит в состав дистрибутива ключей и передается пользователю вместе с ним или отдельно. Пользователи должны хранить РНПК в безопасном месте отдельно от ключей пользователя ViPNet.

См. также: [Администратор УКЦ](#), [Дистрибутив ключей](#), [Ключи пользователя ViPNet](#), [Компрометация ключей](#), [Персональный ключ пользователя](#).

С

Сертификат издателя

Сертификат, с помощью закрытого ключа которого подписывается другой сертификат.

Сертификат открытого ключа подписи пользователя

Электронный документ заранее определенного формата, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Сертификат содержит информацию о владельце ключа, открытый ключ, сведения о его назначении и области применения, информацию о выпустившем сертификат Удостоверяющем центре, период действия сертификата, а также некоторые дополнительные параметры. В сети ViPNet сертификат создается программой УКЦ и заверяется электронной подписью администратора УКЦ.

Электронная подпись Удостоверяющего центра (администратора УКЦ), заверяющая содержимое каждого сертификата, обеспечивает подлинность и целостность указанной в нем информации, включая описание владельца и его открытый ключ. Спецификация

содержимого и формат сертификата в сети ViPNet соответствует стандарту X.509 версии 3 и Федеральному закону РФ № 63 «Об электронной подписи» от 6 апреля 2011 года.

См. также: [Администратор УКЦ](#), [Открытый ключ](#), [Электронная подпись](#).

Сетевая группа

Именованное множество сетевых узлов ViPNet. Объединяет сетевые узлы ViPNet для удобства администрирования. Например, позволяет объединять пользователей в один тип коллектива, зарегистрированный более чем на одном сетевом узле ViPNet, а также для задания одного и того же пароля администратора сетевого узла ViPNet.

См. также: [Пароль администратора сетевого узла ViPNet](#), [Пользователь ViPNet](#), [Сетевой узел ViPNet \(СУ\)](#).

Сетевой узел ViPNet (СУ)

Узел с установленным ПО ViPNet, с помощью которого защищают информацию приложений ViPNet, хранимую локально на компьютере, и (или) трафик посредством шифрования, имитозащиты и электронной подписи.

См. также: [Сеть ViPNet](#), [Электронная подпись](#).

Сеть ViPNet

Логическая сеть, организованная с помощью ПО ViPNet и представляющая собой совокупность сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

См. также: [Сетевой узел ViPNet \(СУ\)](#).

Симметричный ключ

Последовательность бит заданной длины (для алгоритма ГОСТ 28147-89 — 256 бит), используемая как для зашифрования, так и для расшифрования информации.

В ПО ViPNet симметричные ключи используются для зашифрования и расшифрования IP-трафика, информации приложений (в том числе, почтовой), служебных и прикладных конвертов.

См. также: [Прикладной конверт](#), [Служебный конверт](#).

Список отозванных сертификатов (СОС)

Список сертификатов, которые были отозваны администратором Удостоверяющего центра и на данный момент недействительны.

См. также: [Уполномоченное лицо \(администратор\) Удостоверяющего центра](#).

Справочно-ключевая информация

Включает в себя адресные справочники, ключи узла и ключи пользователя. Изменяется при обновлении из Центра управления сетью или ViPNet Manager.

См. также: [Адресные справочники](#), [Ключи пользователя ViPNet](#), [Ключи узла ViPNet](#), [Обновление справочно-ключевой информации](#).

Структура сети ViPNet

Для обеспечения безопасности корпоративной сети необходима установка программного обеспечения ViPNet, которое позволяет защитить весь сетевой трафик, а также информацию, хранящуюся на компьютерах. При этом доступ к защищенному компьютеру с открытых или других защищенных компьютеров может быть в той или иной степени ограничен.

Для организации такой защиты необходимо развернуть сеть ViPNet, базовыми компонентами которой являются:

- рабочее место администратора сети ViPNet с установленным ПО ViPNet Administrator и ViPNet Client или ViPNet CryptoService (для сети ViPNet CUSTOM) или ViPNet Manager и ViPNet Client (для сети ViPNet OFFICE) для организации обмена служебной информацией с другими узлами сети ViPNet;
- координаторы — серверы с установленным ПО ViPNet Coordinator, размещенные на границах сетей или сегментов сети;
- компьютеры пользователей с установленным клиентским ПО ViPNet Client (для сетей ViPNet CUSTOM и ViPNet OFFICE) или ViPNet CryptoService (только для сетей ViPNet CUSTOM).

Каждый клиентский узел должен быть зарегистрирован на координаторе. Каналы связи между координаторами и рабочим местом администратора, а также между координатором и его клиентами обязательны. Остальные связи создаются в соответствии с корпоративной политикой безопасности.

См. также: [«ViPNet Administrator»](#), [«Сеть ViPNet»](#).

Т

Точка распространения данных

Источник, доступный по общеизвестным протоколам (например, FTP или LDAP), используемый для размещения сформированной в Удостоверяющем центре информации (сертификатов издателей и списков отозванных сертификатов).

См. также: [FTP \(File Transfer Protocol\)](#), [LDAP \(Lightweight Directory Access Protocol\)](#), [Сертификат издателя](#), [Список отозванных сертификатов \(СОС\)](#), [Удостоверяющий центр](#).

У

Удостоверяющий центр

Удостоверяющий центр (англ. Certificate authority, CA) — сервис, осуществляющий выпуск сертификатов ключей электронной подписи, а также сертификатов другого назначения. В сетях ViPNet сертификаты выпускает Удостоверяющий и ключевой центр (УКЦ).

См. также: [Сертификат открытого ключа подписи пользователя](#), [Сеть ViPNet](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#).

Уполномоченное лицо (администратор) Удостоверяющего центра

Лицо, обладающее правом заверять сертификаты от имени удостоверяющего центра.

См. также: [Удостоверяющий центр](#).

Ц

Центр управления сетью (ЦУС)

Программа, входящая в ПО ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение конфигурации виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка защищенных адресных справочников;
- формирование информации о связях пользователей для УКЦ;
- определений полномочий пользователей сетевых узлов ViPNet.

См. также: [Адресные справочники](#), [Полномочия пользователя](#), [Сетевой объект, Удостоверяющий и ключевой центр \(УКЦ\)](#), [ViPNet Administrator](#).

Ш

Шаблон сертификата

Частично заполненная структура, содержащая набор расширений, которые определяют назначение сертификата.

Используется в программах ViPNet Удостоверяющий и ключевой центр и ViPNet Registration Point и по умолчанию содержится в отдельном файле `cert_tem.ini`.

См. также: [ViPNet Registration Point](#), [Сертификат открытого ключа подписи пользователя, Удостоверяющий и ключевой центр \(УКЦ\)](#).

Э

Электронная подпись

Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.



Указатель

С

Сохранение паролей пользователей и администраторов сетевых узлов - 103

О

ODBC (Open Database Connectivity) - 50

Р

PKI (инфраструктура открытых ключей) - 308

В

ViPNet Administrator - 320, 322

ViPNet Publication Service - 271

ViPNet Registration Point - 12, 322

А

Абонентский пункт (АП) - 77

Администратор сети ViPNet - 309, 314, 316

Администратор УКЦ - 11, 199, 312, 318, 319

Адресные справочники - 89, 310, 315, 320, 322

Аккредитованный Удостоверяющий центр - 312

Асимметричный ключ - 310

Аутентификация - 312

В

Варианты развертывания - 46, 48

Ввод в действие кросс-сертификата, изданного в вышестоящем УЦ - 87, 220, 224, 229

Внешний пользователь ViPNet - 14, 29, 65, 309, 317

Внутренний пользователь ViPNet - 14, 65, 309, 317

Возможные причины некорректной инициализации - 56

Выбор текущего сертификата администратора - 207

Вышестоящий удостоверяющий центр - 84, 310, 311, 317

Г

Головной удостоверяющий центр - 199, 309, 311, 317

Д

Действия при компрометациях ключей - 72, 90, 105

Действия с ключами пользователей - 72, 102, 105, 107

Действия с ключами узлов и обновлениями ключей для СУ - 70, 97, 99, 107, 164, 166

Действия с резервными персональными ключами - 68, 104, 108, 132

Действия с созданной ключевой информацией - 106

Действия с созданными дистрибутивами ключей - 68, 71, 105, 108

Дистрибутив ключей - 12, 71, 307, 309, 318

Доверенная сеть - 73, 307, 308, 315

З

Закрытый ключ - 204, 311

Запрос на сертификат - 180

Запуск и завершение работы с программой - 51, 62, 201, 203, 300

И

Идентификатор объекта (OID) - 317

Иерархия удостоверяющих центров - 310, 317

Издание (отклонение) сертификатов по запросам, поступившим из ViPNet Registration Point - 143

Издание (отклонение) сертификатов по запросам, поступившим с СУ пользователей сети ViPNet - 143

Издание кросс-сертификатов - 169, 174

Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ - 143

Изменение статуса межсетевого мастер-ключа - 78, 121, 123, 125, 127

Импорт межсетевых мастер-ключей - 123, 126

Импорт сертификатов администраторов вышестоящего УЦ - 220, 224, 235

Импорт сертификатов администраторов доверенных сетей ViPNet - 73, 74, 75, 98, 226

Импорт списков отозванных сертификатов доверенных сетей ViPNet - 74, 75, 98

Интерфейс программы ViPNet Удостоверяющий и ключевой центр - 56, 60

Информация о внешних устройствах хранения данных - 60, 110, 116, 219, 222

К

Квалифицированный сертификат - 22, 144, 256

Ключ защиты УКЦ - 62, 218, 277

Ключи пользователя ViPNet - 12, 72, 312, 313, 317, 318, 320

Ключи узла ViPNet - 12, 70, 313, 315, 320

Комплект поставки - 10, 32, 50

Компрометация ключей - 72, 314, 315, 317, 318

Контейнер ключей - 204

Контрольная сумма - 315

Корневой сертификат - 13, 315

Кросс-сертификат - 28

Кросс-сертификация - 313

Л

Лицензионное ограничение - 16, 250, 293

Логика выбора межсетевого мастер-ключа - 121, 128

М

Мастер редактирования полей сертификата - 31, 101, 143, 150, 153

Мастер-ключ - 12

Межсетевое взаимодействие - 307, 310

Межсетевой мастер-ключ - 12, 54, 73, 314

Н

Настройка оповещения об окончании лицензии - 14

Настройка папок обмена - 46, 53, 97, 100, 102, 107, 194, 281, 300

Настройка параметров журнала событий - 285

Настройка параметров издания сертификатов и обработки запросов - 95, 102, 143, 144, 150, 151, 152, 157, 180, 256

Настройка параметров публикации данных - 194

Настройка параметров работы с сертификатами - 170, 208

Настройка параметров работы со списками отозванных сертификатов - 159, 161, 167

Настройка параметров случайных паролей - 54, 92, 243

Настройка параметров создания резервных копий - 277

Настройка параметров создания резервных наборов персональных ключей - 103

Настройка списка политик применения сертификата - 261

Настройка списка точек распространения - 194, 265, 271
Настройка типа создаваемых паролей - 92, 106

О

Обновление ключей узла - 71
Обновление сертификата и закрытого ключа администратора - 200, 204
Обновление списка отозванных сертификатов своей сети - 264
Обработка запросов на кросс-сертификаты (в том числе запросов на сертификаты из подчиненных УЦ) - 86, 87, 235
Обратная связь - 300
Описание окна Запрос на кросс-сертификат - 170
Описание окна Издание кросс-сертификатов - 170
Организация иерархической системы доверительных отношений между УЦ - 30
Основные действия администратора УКЦ - 74
Отзыв сертификатов, приостановление действия сертификатов, возобновление действия сертификатов - 152, 154
Отсутствие функциональности программы в части Удостоверяющего центра ViPNet - 14, 31

П

Пароль администратора сетевых узлов - 68, 75, 90, 97
Пароль администратора УКЦ - 59
Пароль пользователя - 309, 312, 316
Пароль пользователя на основе парольной фразы - 316
Парольная фраза - 316
Перенос базы данных УКЦ на SQL-сервер - 62
Персональный ключ пользователя - 312, 314, 318
Плановая смена мастер-ключей - 76, 120
Плановая смена межсетевых мастер-ключа - 76, 123
По запросу из ViPNet Registration Point - 157

По инициативе администратора УКЦ - 157
Подключение к SQL-серверу при запуске программы - 60, 300
Подчиненный удостоверяющий центр - 84, 309, 310, 311
Политика применения сертификата - 27, 268
Пользователь ViPNet - 307, 316, 317, 319
Проведение первичной инициализации программы - 47, 49, 62, 68, 119, 199, 239, 243, 300
Проверка сертификатов - 184
Проверка текущих данных - 94, 294
Просмотр запросов на сертификаты пользователей - 152, 154
Просмотр и изменение данных об администраторе - 203, 216
Просмотр лицензионного ограничения - 14, 17
Просмотр свойств запроса (окно Запрос на издание сертификата) - 228
Просмотр свойств пользователя - 69, 72, 111, 131
Просмотр свойств сетевого узла - 114, 129
Просмотр свойств сетевой группы - 129
Просмотр сертификатов - 103, 152, 154, 159, 160, 164, 188, 224
Просмотр списков отзыва сертификатов - 158, 161, 166, 167
Процесс создания - 68, 252
Публикация и прием опубликованных данных - 272

Р

Резервный набор персональных ключей (РНПК) - 92, 247, 317
Ручная проверка текущих данных - 290
Ручной экспорт данных - 295

С

Сертификат издателя - 199, 321
Сертификат открытого ключа подписи пользователя - 12, 307, 309, 311, 312, 313, 317, 321, 322
Сетевой узел ViPNet (СУ) - 89, 307, 308, 310, 312, 313, 314, 315, 316, 319

Сеть ViPNet - 307, 309, 314, 315, 319, 320, 321
Симметричный ключ - 314
Смена ключа защиты УКЦ - 202
Смена мастер-ключей своей сети - 76, 119
Смена текущей учетной записи администратора - 201, 204, 218, 225
Создание дистрибутивов ключей - 47, 71, 76, 81, 143
Создание запроса на кросс-сертификат и отправка его в другой УЦ - 86, 172
Создание запроса на кросс-сертификат к вышестоящему удостоверяющему центру - 87, 215
Создание запроса на кросс-сертификат к вышестоящему УЦ и установка изданного сертификата в иерархической системе доверительных отношений - 201, 220
Создание и восстановление резервных копий конфигурации программы - 61
Создание и редактирование шаблонов сертификатов - 95, 143, 144, 147, 252, 268
Создание ключевой информации при первоначальном развертывании сети - 82
Создание ключей пользователей - 72, 76, 132, 143, 149, 252
Создание ключей при изменениях в структуре своей сети - 70
Создание ключей при компрометациях - 81
Создание ключей при установлении взаимодействия с доверенной сетью ViPNet, а также при внесении изменений в это взаимодействие - 70
Создание ключей узлов - 70, 76, 78, 159
Создание межсетевых мастер-ключей - 54, 73, 77, 119
Создание обновлений ключей узлов - 72, 75, 130, 161, 164, 166, 168, 215
Создание учетной записи администратора - 54, 202
Список отозванных сертификатов (СОС) - 13, 28, 65, 264, 307, 315, 321
Справочно-ключевая информация - 315
Структура сети ViPNet - 70

Т

Точка распространения данных - 271, 273
Требования к SQL-серверу для развертывания базы данных УКЦ - 50, 299

У

Удостоверяющий центр - 83, 308, 309, 310, 311, 314, 317, 321
Уполномоченное лицо (администратор) Удостоверяющего центра - 313, 320
Управление ключевой структурой ViPNet - 74
Установка программы - 14, 46, 239, 300

Ц

Центр управления сетью (ЦУС) - 10, 307, 308

Ш

Шаблон сертификата - 256

Э

Экспорт и импорт межсетевых мастер-ключей - 73, 78, 121
Экспорт кросс-сертификатов - 169, 173
Экспорт межсетевых мастер-ключей - 122
Экспорт сертификатов - 179, 183
Экспорт служебных данных - 173, 200
Электронная подпись - 89, 309, 310, 311, 312, 317, 319