ViPNet Удостоверяющий и ключевой центр 4

Руководство администратора по эксплуатации

infotecs

ФРКЕ.00109-07 32 03

Версия продукта 4.6.9

АО «ИнфоТеКС»

127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

Телефон: +7 (495) 737-6192, 8 (800) 250-0260 — бесплатный звонок из России (кроме Москвы)

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

Настоящий документ является подробным руководством по настройке и использованию программы ViPNet® Удостоверяющий и ключевой центр (далее — УКЦ). При его изучении рекомендуется дополнительно ознакомиться с остальной документацией из комплекта поставки (см. Комплект поставки на стр. 14). Это позволит получить общее представление об основных понятиях и структуре сети ViPNet.

Для кого предназначен документ

Данное руководство предназначено для администраторов сетей ViPNet®, отвечающих за организацию работы программы ViPNet Удостоверяющий и ключевой центр — администраторов УКЦ (см. глоссарий, стр. 209).

Предполагается, что читатель данного руководства предварительно прошел курс обучения в учебном центре ИнфоТеКС, знаком с технологией ViPNet и имеет представление о базовых понятиях в области криптографии (см. Основы криптографии на стр. 200), а также об инфраструктуре открытых ключей PKI (см. глоссарий, стр. 208).

Соглашения документа

Обозначение	Описание
	**Внимание!** Содержит критически важную информацию
	**Примечание.** Содержит рекомендательную информацию
	**Совет.** Содержит полезные приемы и хорошие практики
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская ее, нажмите вторую
Меню > Команда	Последовательность элементов или действий
`Код`	Имя файла, путь, фрагмент кода или команда в командной строке

О программе

Программа ViPNet Удостоверяющий и ключевой центр (далее — УКЦ) является составной частью программного обеспечения ViPNet Administrator®, которое используется для администрирования сетей ViPNet.

Программа ViPNet Удостоверяющий и ключевой центр предназначена для управления ключевой структурой сети ViPNet, а также для выполнения функций удостоверяющего центра — издания и обслуживания сертификатов ключа проверки электронной подписи (см. глоссарий, стр. 216).

Новые возможности версии 4.6.9

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Удостоверяющий и ключевой центр 4.6.9 по сравнению с версией 4.6.7.

- **Поддержка ViPNet CSP 4.4.2**
- **Поддержка Windows Server 2016 и Windows Server 2019**
- **Совместимость с Microsoft SQL Server 2017 и Windows SQL Server 2019**
- **Изменения в списке поддерживаемых операционных систем**

  В связи с тем, что компания Microsoft прекратила общую поддержку операционных систем Windows 7 (32/64-разрядная), Windows 8 (32/64-разрядная), Windows Server 2008 R2 (64-разрядная), Windows Server 2012 (64-разрядная), Windows 8.1 (32/64-разрядная), работа программы ViPNet Удостоверяющий и ключевой центр на компьютерах с этими операционными системами также более не поддерживается ИнфоТеКС.
- **Поддержка изменений приказа ФСБ России №795**

  В УКЦ поддержаны изменения приказа Федеральной службы безопасности Российской Федерации от 29.01.2021 № 31 «О внесении изменений в приказ ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»:

  - **Отображение типа владельца сертификата при издании сертификатов по входящим запросам**

    Теперь при издании сертификатов вручную по запросам внешних пользователей (из файлов *.p10 и *.cmc), так и при издании сертификата из входящего запроса отображается тип владельца сертификата.

    Если в запросе на сертификат указаны атрибуты, которые однозначно характеризуют владельца сертификата как индивидуального предпринимателя, физическое или юридическое лицо, то есть в запросе были заданы поля ОГРНИП, ИНН ФЛ или ИНН ЮЛ соответственно, то при издании сертификатов отображается тип владельца в заголовке первой страницы мастера издания сертификатов.

Если такие поля не были заданы в запросе, то при издании сертификатов необходимо выбрать тип владельца сертификата. В зависимости от выбранного типа будет предложено заполнить поля сертификата. Например, если выбрать **Индивидуальный предприниматель**, то будут доступны поля для ИП (**ОГРНИП** и другие). А при выборе **Юридическое лицо** появится новое поле — **ИНН ЮЛ** (расширение INNLE), в котором задается ИНН из 10 символов.

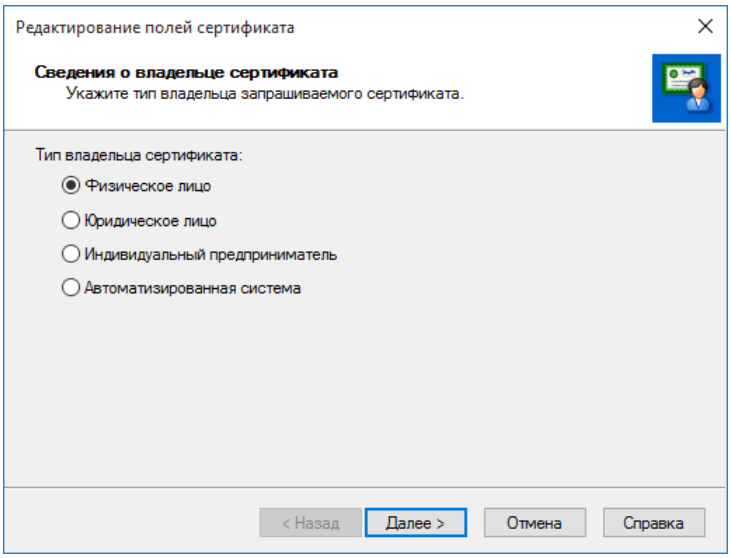

Рисунок 1. Выбор типа владельца сертификата при удовлетворении запроса на сертификат

- **Возможность указания типа идентификации владельца сертификата**

  Теперь при издании квалифицированных сертификатов необходимо добавлять расширение «Тип идентификации». Это нужно для того, чтобы определить, как идентифицировал себя пользователь при создании запроса на сертификат. Возможны следующие типы идентификации:

  - **Личное присутствие**.
  - **Действующий сертификат**.
  - **Заграничный паспорт**.
  - **ЕСИА/ЕБС** (Единая система идентификации и аутентификации/Единая биометрическая система).

  Указанное расширение должно добавляться в запросы на квалифицированные сертификаты или в издаваемые квалифицированные сертификаты, его наличие не является обязательным для неквалифицированных сертификатов.

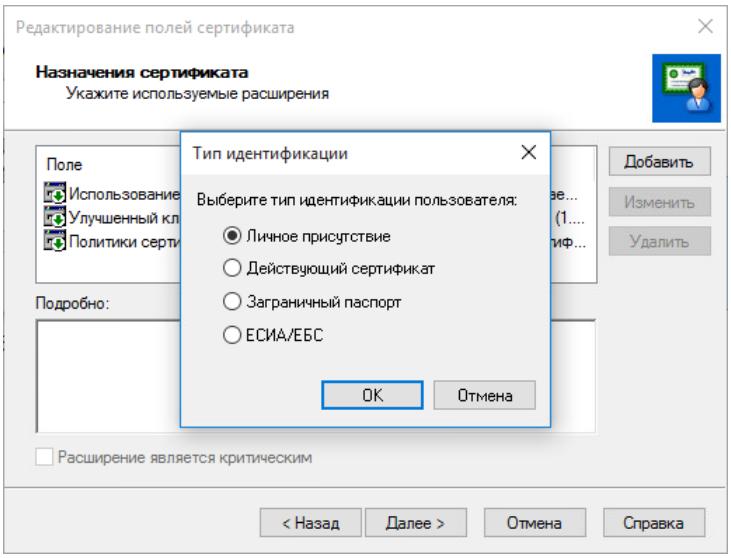

Рисунок 2. Указание типа идентификации владельца сертификата

- **Улучшение внутренней функциональности**

  Исправлены ошибки, выявленные в процессе эксплуатации программы ViPNet Удостоверяющий и ключевой центр версии 4.6.7.

Системные требования

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

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 1 Гбайт (при использовании 64-разрядных версий ОС Microsoft Windows — не менее 2 Гбайт).
- Свободное место на жестком диске — не менее 20 Гбайт.
- Операционная система — Windows Server 2012 R2 (64-разрядная), Windows 10 (32/64-разрядная), Windows Server 2016, Windows Server 2019.

  Для операционной системы должен быть установлен самый последний пакет обновлений.
- При использовании Internet Explorer — версия 11.

Дополнительные требования:

- Для возможности сохранения паролей пользователей в файлы на компьютере должен быть установлен виртуальный принтер Microsoft XPS Document Writer. Данный принтер по умолчанию присутствует в операционной системе Windows 10 (32/64-разрядная). Если используется операционная система Windows Server 2012 R2 SP1 или Windows Server 2016, виртуальный принтер следует устанавливать вручную (см. Не удается посмотреть пароль, сохраненный в файле на стр. 180).
- При печати паролей пользователей ViPNet на ПИН-конвертах рекомендуется использовать:
  - Специализированные принтеры для печати ПИН-конвертов или аналогичные матричные принтеры модели OKI ML5100FB.
  - Стандартные четырехслойные ПИН-конверты с расширенным полем для секретной информации.

Комплект поставки

Программа ViPNet Удостоверяющий и ключевой центр поставляется в составе программного обеспечения ViPNet Administrator.

В комплект поставки программного обеспечения ViPNet Administrator входит:

- Установочный файл программы ViPNet Удостоверяющий и ключевой центр.
- Документация в формате PDF:
  - Руководство администратора
  - «ViPNet Удостоверяющий и ключевой центр. Руководство администратора по эксплуатации».
  - «Печать сертификатов. Приложение к документации ViPNet».

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, частые вопросы и полезная информация на сайте ИнфоТеКС:

- Информация о продуктах ViPNet.
- Информация о решениях ViPNet.
- Часто задаваемые вопросы.
- Форум пользователей продуктов ViPNet.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ИнфоТеКС:

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба поддержки: hotline@infotecs.ru.

  Форма для обращения в службу поддержки через сайт.

  Канал поддержки в Telegram: t.me/vhd21

  Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов компании ИнфоТеКС регулируется политикой ответственного разглашения.

1

Общие сведения

Назначение программы ViPNet Удостоверяющий и ключевой центр

Программу ViPNet Удостоверяющий и ключевой центр условно можно разделить на два компонента: ключевой центр и удостоверяющий центр. Схематично данное деление представлено на рисунке ниже.

Рисунок 3. Условное деление УКЦ на компоненты

При работе УКЦ в роли ключевого центра осуществляется:

- Формирование мастер-ключей (см. глоссарий, стр. 214), в том числе межсетевых мастер-ключей (см. глоссарий, стр. 214), необходимых для установления взаимодействия с доверенными сетями.
- Создание ключей для объектов сети ViPNet. Данные ключи используются программным обеспечением ViPNet для организации безопасного обмена конфиденциальной информацией.

При работе УКЦ в роли удостоверяющего центра осуществляется:

- Издание сертификатов ключа проверки электронной подписи по запросам, поступающим от пользователей сети ViPNet либо из центров регистрации (узлов с программным обеспечением ViPNet Registration Point (см. глоссарий, стр. 209)).

Примечание. Издание сертификатов может осуществляться на базе алгоритма стандарта ГОСТ Р 34.10-2012. С описанием алгоритма можно ознакомиться в RFC 7836.

При необходимости сертификаты подписи могут быть изданы в формате квалифицированных (см. глоссарий, стр. 211).

- Аннулирование выпущенных сертификатов.
- Формирование сертификата администратора (см. глоссарий, стр. 213), списков аннулированных сертификатов (см. глоссарий, стр. 217) и их распространение в своей и доверенных сетях.
- Создание запросов на проведение кросс-сертификации (см. глоссарий, стр. 214) с другими удостоверяющими центрами либо издание кросс-сертификатов (см. Издание кросс-сертификата по запросу на стр. 133).
- Импорт корневых сертификатов и CRL из доверенных сетей ViPNet и других удостоверяющих центров.
- Другие стандартные операции, связанные с работой удостоверяющего центра.

Криптографические функции выполняются программой ViPNet CSP, которая устанавливается автоматически вместе с УКЦ. Программа ViPNet CSP позволяет создавать ключи электронной подписи, формировать и проверять электронную подпись. Подробнее о функциях программы ViPNet CSP см. в документе «ViPNet CSP. Руководство пользователя».

Взаимодействие с программой ViPNet Registration Point

Программа ViPNet Registration Point предназначена для выполнения функций центра регистрации пользователей. Администратор программы ViPNet Registration Point имеет возможность зарегистрировать нового пользователя и создать для пользователя запрос на получение сертификата электронной подписи или дистрибутива ключей ViPNet. Впоследствии администратор центра регистрации также может сформировать запрос на аннулирование сертификата.

Сформированные запросы из ViPNet Registration Point передаются на обработку в программу ViPNet Удостоверяющий и ключевой центр с помощью транспортного модуля ViPNet MFTP (см. глоссарий, стр. 218). Необходимая информация из запросов автоматически записывается в базу данных, после чего эти запросы передаются в программу ViPNet Удостоверяющий и ключевой центр. Администратор УКЦ может удовлетворить либо отклонить полученные запросы.

Взаимодействие с программой ViPNet Publication Service

Программа ViPNet Publication Service (см. глоссарий, стр. 209) предназначена для публикации (см. глоссарий, стр. 216) сертификатов пользователей, администраторов УКЦ, кросс-сертификатов и списков аннулированных сертификатов (CRL), которые издаются в программе ViPNet Удостоверяющий и ключевой центр, в общедоступных хранилищах данных (AD, FTP-сервер) или в различных точках распространения (см. глоссарий, стр. 217) с целью обеспечения доступа к ним пользователей инфраструктуры открытого ключа (PKI). Обычно это требуется в том случае, если сеть ViPNet используется для электронного документооборота.

Примечание. В точках распространения могут размещаться только CRL и сертификаты издателей.

Взаимодействие всех компонентов, участвующих в процессе публикации, представлено на схеме ниже.

Рисунок 4. Схема взаимодействия узлов, участвующих в документообороте

Также программа ViPNet Publication Service может производить автоматический опрос точек распространения сторонних удостоверяющих центров и скачивание сертификатов издателей и CRL из доверенных сетей, если требуется постоянная актуализация их сертификатов издателей и CRL на узлах вашей сети.

Подробную информацию о взаимодействии с сервисом публикации и настройке параметров публикации данных см. в разделе Публикация сертификатов и списков аннулированных сертификатов (на стр. 108).

Совместимость с программным обеспечением ViPNet

Если версии программы ViPNet Удостоверяющий и ключевой центр и ПО ViPNet на сетевых узлах, используемые в вашей сети, различаются, следует учитывать следующие особенности:

- Программа ViPNet Удостоверяющий и ключевой центр версии 4.x может быть несовместима с программами ViPNet Registration Point и ViPNet Publication Service версий ниже 4.x.
- Первый дистрибутив ключей, созданный в УКЦ версии 4.2.x или выше, невозможно установить на сетевые узлы с ПО ViPNet Client или ViPNet CryptoService версий ниже 3.2.9. На сетевые узлы с ПО ViPNet Client или ViPNet CryptoService версий 3.2.9 и выше установить первый дистрибутив ключей, созданный в УКЦ версии 4.2.x или выше, можно только дважды щелкнув файл дистрибутива ключей.
- На сетевых узлах с ПО ViPNet Client для Windows версии 3.2.x не поддерживается аутентификация по персональному ключу, сохраненному на внешних устройствах семейства eToken Aladdin. Поэтому при задании для пользователей таких узлов способа аутентификации **Устройство (персональный ключ)** следует сохранять персональный ключ на устройствах другого типа либо следует задавать другой способ аутентификации.
- Если на сетевых узлах с ПО ViPNet Client для Windows версии 3.1.x или 3.2.x, а также на узлах с ПО ViPNet CryptoService версии 3.1.x или 3.2.x. установлены ключи, созданные в УКЦ версии 3.2.x, то на них будут корректно приняты обновления ключей, созданные в УКЦ версии 4.2.x или выше.
- Ключи, созданные в УКЦ версии 4.2.x или выше, можно установить на координаторах с версией ПО ViPNet Coordinator Linux 3.7.x и на программно-аппаратных комплексах ViPNet Coordinator HW версии 3.2 или выше.

2

Начало работы с программой ViPNet Удостоверяющий и ключевой центр

Установка и первичная инициализация программы ViPNet Удостоверяющий и ключевой центр

Чтобы развернуть программное обеспечение ViPNet Удостоверяющий и ключевой центр, выполните следующие действия:

1. Перед установкой УКЦ убедитесь, что вы располагаете установочным файлом программы ViPNet Удостоверяющий и ключевой центр.
2. Установите программу ViPNet Удостоверяющий и ключевой центр.

   Будет запущен мастер первичной инициализации программ, следуйте его указаниям. Подробнее см. в документе «ViPNet Administrator. Руководство по установке», в разделе «Первичная инициализация программы ViPNet Удостоверяющий и ключевой центр».

   В результате будет создана учетная запись администратора УКЦ, созданы мастер-ключи (см. руководство администратора на УКЦ). В случае если ваша лицензия разрешает использование функций удостоверяющего центра, также будет издан сертификат проверки электронной подписи администратора УКЦ (см. Издание сертификата администратора на стр. 147).
3. Если ваш УКЦ выступает в роли подчиненного удостоверяющего центра, получите в вышестоящем удостоверяющем центре сертификат издателя, которым вы сможете подписывать издаваемые сертификаты пользователей (см. Установление доверительных отношений с вышестоящим или подчиненным удостоверяющим центром на стр. 120).

   Если необходимо установить с другим удостоверяющим центром доверительные отношения на основе распределенной модели, следуйте указаниям раздела Установление доверительных отношений с равнозначным удостоверяющим центром (на стр. 130).

Подробная информация об установке и первичной инициализации программы ViPNet Удостоверяющий и ключевой центр содержится в документе «ViPNet Administrator. Руководство по установке».

Запуск и завершение работы программы

Чтобы запустить программу ViPNet Удостоверяющий и ключевой центр:

1 На начальном экране откройте список приложений и выберите **ViPNet** > **Удостоверяющий и ключевой центр**.

Примечание. Во время установки положение программы в меню **Пуск** или в списке приложений могло быть изменено.

---

2 Чтобы начать работу с программой, в окне **Вход в Удостоверяющий и ключевой центр** выберите учетную запись администратора, под которой будет производиться вход в программу, и введите пароль (см. глоссарий, стр. 215).

Внимание! Если вы 3 раза ввели неправильный пароль, то дальнейший ввод пароля будет возможен по истечении 40 секунд.

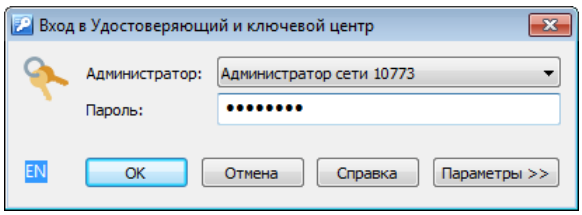

Рисунок 5. Окно входа в программу

3 Укажите место хранения ключей администратора (см. глоссарий, стр. 212) 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. Внешние устройства на стр. 183). 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.

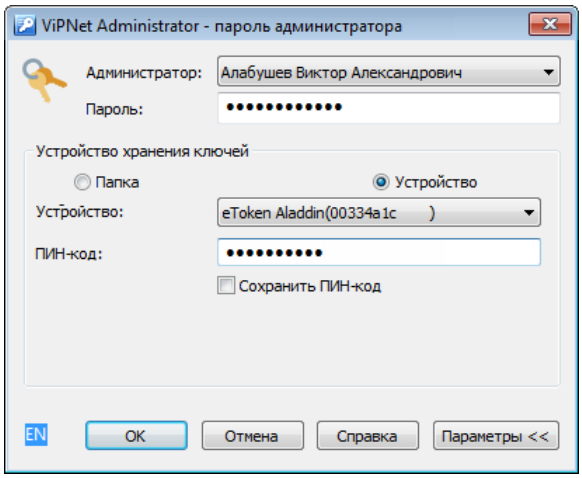

Рисунок 6. Окно входа в программу с указанием места хранения ключей

4 После ввода необходимых для аутентификации данных нажмите кнопку **OK**.

Будет выполнена проверка соединения с SQL-сервером. Если проверка пройдет успешно, произойдет вход в программу под выбранной учетной записью администратора и появится главное окно УКЦ (см. Интерфейс программы ViPNet Удостоверяющий и ключевой центр на стр. 27). 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. 25).

После появления главного окна программы можно приступать к работе с УКЦ.

Примечание. Если в настройках автоматического режима (см. Настройка автоматического режима на стр. 39) выбраны операции **Создавать ключи узлов** и **Удовлетворять запросы на дистрибутивы ключей,** появится электронная рулетка. Следуйте указаниям в окне **Электронная рулетка**.

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 в меню **УКЦ** выберите пункт **Выход**.
- Нажмите кнопку **Закрыть** в правом верхнем углу окна.

Подключение к SQL-серверу при запуске программы

При каждом запуске УКЦ после ввода пароля администратора производится проверка подключения к SQL-серверу (см. глоссарий, стр. 209), на котором размещена база данных программы. Первоначально параметры подключения к серверу задаются в процессе первичной

инициализации (см. документ «ViPNet Administrator. Руководство по установке»), но при необходимости они могут быть изменены.

При успешной проверке осуществляется вход в программу, в случае возникновения ошибок в ходе проверки появляется окно подключения к SQL-серверу (см. рисунок ниже).

При возникновении ошибок требуется установить их причину (см. Не удается войти в программу ViPNet Удостоверяющий и ключевой центр на стр. 179), проверить и, если требуется, изменить параметры в появившемся окне **Подключение к SQL Server**. Чтобы изменить параметры подключения:

1 В окне **Подключение к SQL Server** в поле **Сервер** укажите SQL-сервер, на котором была развернута база данных.

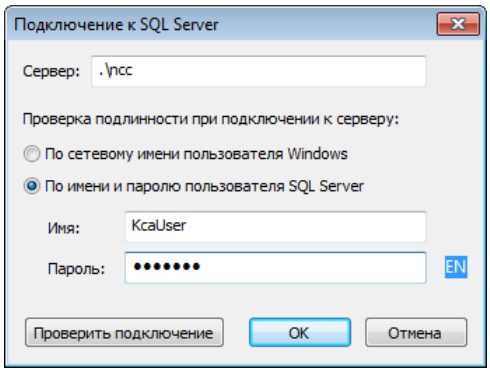

Рисунок 7. Подключение к SQL-серверу

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

При выборе типа **По имени и паролю пользователя SQL Server** укажите имя пользователя, под учетной записью которого необходимо подключиться к SQL-серверу, и пароль.

По умолчанию заданы имя пользователя `KcaUser` и пароль `Number1`.

3 Нажмите кнопку **Проверить подключение**. Если подключение к указанному SQL-серверу было проведено успешно, кнопка **OK** станет активной. В противном случае измените настройки подключения и нажмите кнопку **Проверить подключение** еще раз.

4 Нажмите кнопку **OK**.

Внимание! В случае возникновения проблем с подключением к SQL-серверу, не пытайтесь устранить их самостоятельно, обратитесь к администратору используемого SQL-сервера (подробнее см. документ «ViPNet Administrator. Руководство по установке», глава «Установка программного обеспечения ViPNet Administrator», раздел «Информация для администраторов SQL»).

Интерфейс программы ViPNet Удостоверяющий и ключевой центр

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

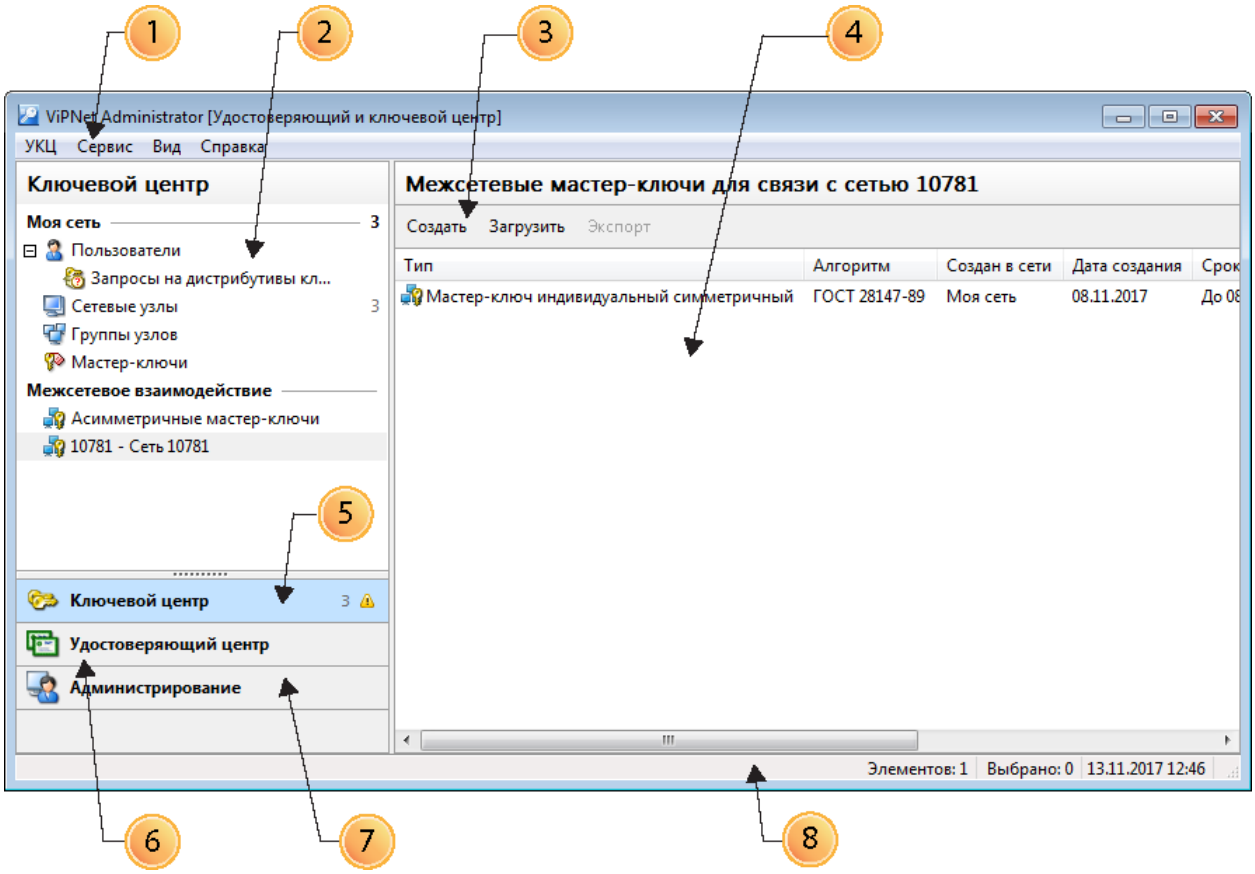

Рисунок 8. Интерфейс программы ViPNet Удостоверяющий и ключевой центр

Цифрами на рисунке обозначены:

1 Главное меню программы.

2 Панель навигации. Отображает элементы одного из трех выбранных представлений: **Ключевой центр** (5), **Удостоверяющий центр** (6) и **Администрирование** (7). Для перехода в нужное представление выберите его на панели навигации или щелкните в меню **Вид** соответствующий пункт.

3 Панель инструментов. Отображается при выборе определенных разделов на панели навигации.

4 Панель просмотра. Отображает раздел, выбранный на панели навигации (2).

5 Представление **Ключевой центр**. При выборе представления **Ключевой центр** на панели навигации отображаются объекты вашей сети ViPNet и ключи, созданные для этих объектов, а также информация о межсетевых мастер-ключах, созданных для организации взаимодействия вашей сети с доверенными сетями ViPNet (см. Представление «Ключевой центр» на стр. 29).

6 Представление **Удостоверяющий центр**. При выборе представления **Удостоверяющий центр** на панели навигации отображаются разделы для управления изданными сертификатами пользователей и различными запросами на сертификаты (см. Представление «Удостоверяющий центр» на стр. 30).

7 Представление **Администрирование**. При выборе представления **Администрирование** на панели навигации отображаются разделы для управления учетными записями администраторов и получателями списков аннулированных сертификатов (CRL), а также для работы с сертификатами, кросс-сертификатами и CRL (см. Представление «Администрирование» на стр. 31).

8 Строка состояния. Информирует о количестве объектов выбранного раздела, которое содержится в базе данных программы и отображается в текущий момент. Чтобы показать или скрыть строку состояния, в меню **Вид** выберите пункт **Строка состояния**.

9 Строка поиска (на рисунке не обозначено). Отображается в разделах, в которых на панели просмотра содержатся списки пользователей, сетевых узлов, сертификатов, запросов или иных объектов. Для поиска элементов в разделе укажите столбец поиска и сочетание букв для поиска. При поиске по дате укажите интервал времени.

Примечание. Следует учесть, что поиск может производиться только по информации в отображаемых столбцах раздела. То есть, например, для поиска сертификата по ИНН в списке сертификатов должен присутствовать столбец с ИНН для каждого сертификата.

В разделе со списками сертификатов поиск сертификатов возможен по множеству столбцов. Все возможные столбцы вы можете просмотреть в окне **Выбор столбцов в таблице** (меню **Вид** > **Выбрать столбцы**).

Если от вас требуется выполнить в программе некоторые важные операции, например, создать ключи для пользователя, обновить CRL или обработать поступивший запрос на сертификат, то на панели навигации главного окна программы появятся значки оповещений . Значок оповещения будет рядом с названием того представления, с объектами которого требуется выполнить нужные операции. Рядом со значком будет указано количество операций, которое нужно выполнить. Количество операций также будет указано напротив разделов данного представления.

Вы можете выделить сразу все объекты в рамках одного раздела, для которых требуется выполнить одну и ту же операцию. Для этого перейдите в нужный раздел и в меню **Вид** выберите пункт **Выделить требующие внимания** или нажмите сочетание клавиш **Ctrl+W**.

Представление «Ключевой центр»

Чтобы получить сведения об объектах вашей сети ViPNet и ключах, созданных в процессе работы программы в роли ключевого центра, выберите представление **Ключевой центр**.

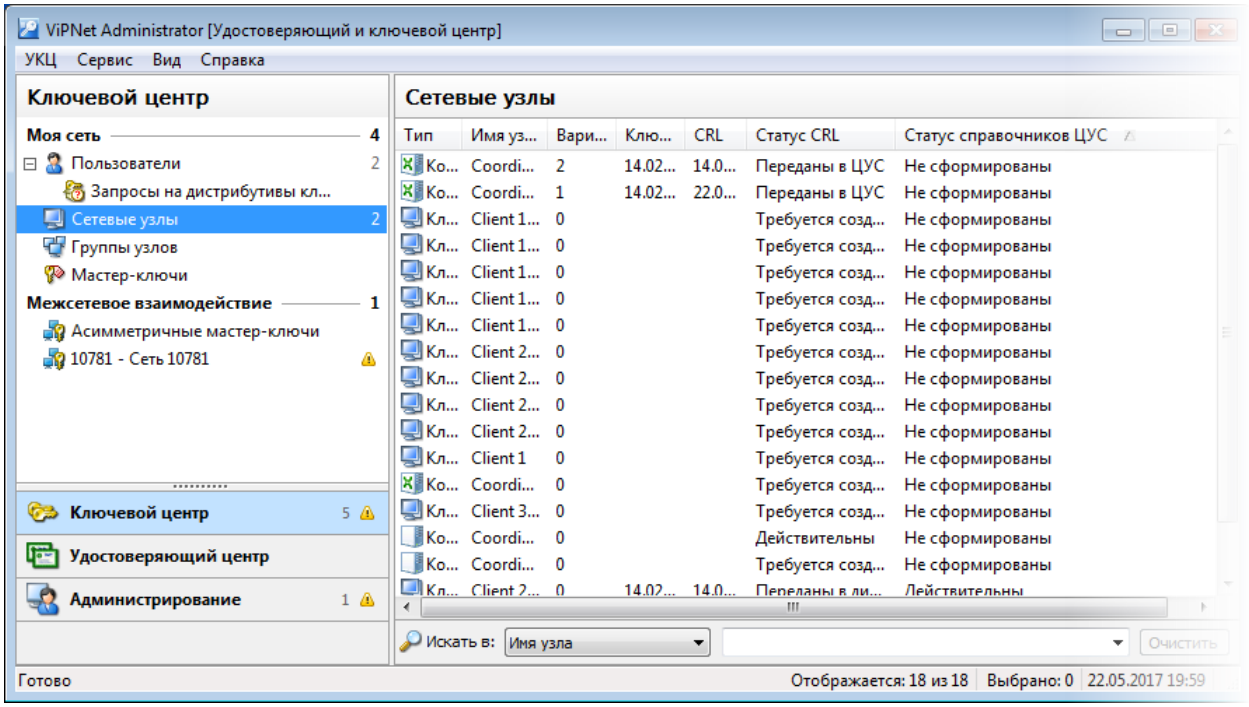

Рисунок 9. Информация об узлах своей сети ViPNet

На панели навигации будут отображены следующие разделы:

- **Моя сеть**. В этом разделе сведения об объектах вашей сети и их ключах распределены по соответствующим вложенным разделам следующим образом:
  - **Пользователи** — содержит список всех пользователей, зарегистрированных в вашей сети ViPNet. Вложенные разделы содержат информацию о резервных наборах персональных ключей, а также поступившие в УКЦ запросы на дистрибутивы ключей.
  - **Сетевые узлы** — содержит список всех сетевых узлов, имеющихся в вашей сети ViPNet.
  - **Группы узлов** — содержит список групп узлов, организованных в вашей сети ViPNet.
  - **Мастер-ключи** — содержит мастер-ключи, используемые в вашей сети ViPNet: мастер-ключ персональных ключей, мастер-ключ ключей защиты и мастер-ключ ключей обмена.
- **Межсетевое взаимодействие**. Во вложенном разделе **Асимметричные мастер-ключи** приводятся все созданные в процессе работы УКЦ асимметричные межсетевые мастер-ключи. Если установлено межсетевое взаимодействие с доверенной сетью ViPNet, то во вложенном разделе с номером данной сети содержатся:
  - созданные или импортированные индивидуальные межсетевые мастер-ключи для связи вашей сети с доверенной сетью;
  - импортированные из доверенной сети открытые части асимметричных мастер-ключей.

Представление «Удостоверяющий центр»

Чтобы получить сведения о сертификатах и запросах на сертификаты, созданных или используемых в процессе работы программы в роли удостоверяющего центра, выберите представление **Удостоверяющий центр**.

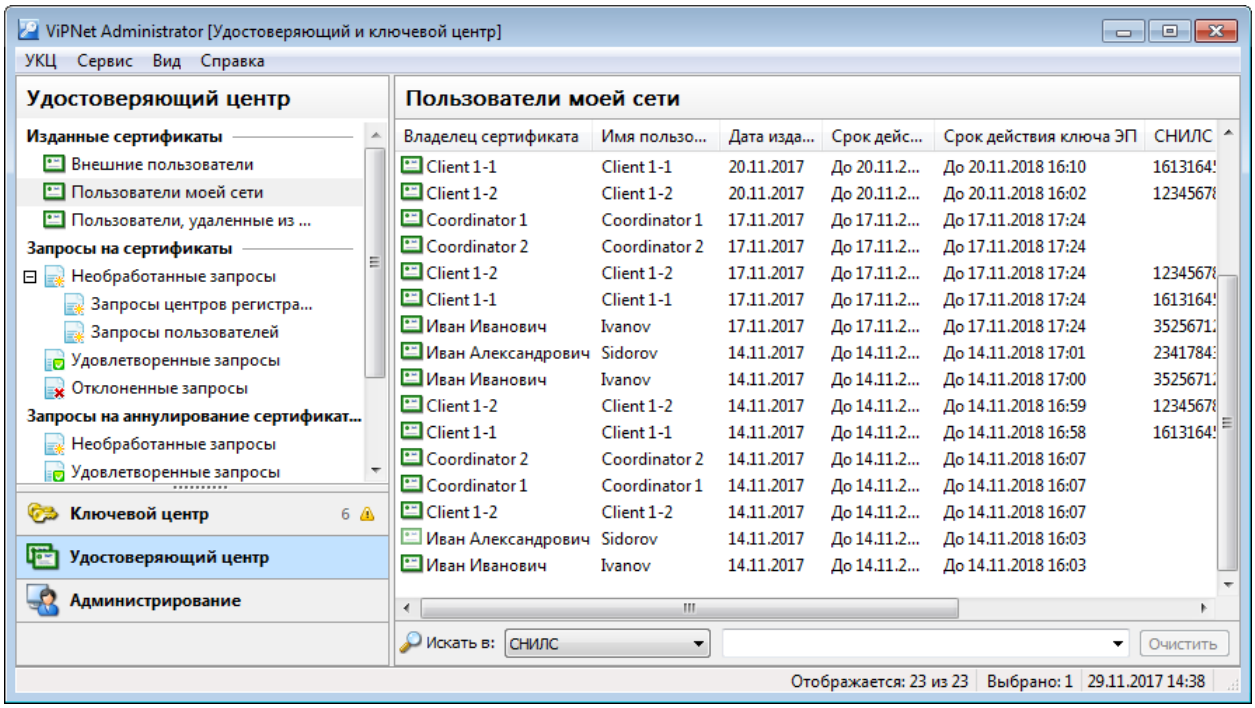

Рисунок 10. Информация об изданных сертификатах пользователей своей сети ViPNet

На панели навигации будут отображены следующие разделы:

- **Изданные сертификаты** — содержит информацию об изданных сертификатах подписи внешних пользователей (см. глоссарий, стр. 210) и пользователей сети ViPNet (см. глоссарий, стр. 216), включая тех, которые были удалены из сети ViPNet.

Совет. По умолчанию в подразделах раздела **Изданные сертификаты** отображается не более 100 сертификатов пользователей. О том, как увеличить количество отображаемых сертификатов, см. в разделе Настройка количества сертификатов, отображаемых в окне программы (на стр. 93).

- **Запросы на сертификаты** — содержит информацию о запросах на издание сертификатов пользователей, поступивших из центров регистрации и от пользователей вашей сети ViPNet. Обработанные запросы содержатся во вложенных разделах **Удовлетворенные запросы** и **Отклоненные запросы** в соответствии с тем, как они были обработаны — удовлетворены или отклонены.
- **Запросы на аннулирование сертификатов** — содержит информацию о поступивших из центров регистрации запросов на аннулирование сертификатов пользователей. Обработанные запросы содержатся во вложенных разделах **Удовлетворенные запросы** и **Отклоненные запросы** в соответствии с тем, как они были обработаны — удовлетворены или отклонены.

- **Запросы с ошибками** — содержит информацию о запросах, которые не могут быть обработаны по причине ошибок в них (например, если файл с запросом был поврежден).

Представление «Администрирование»

Для управления учетными записями администраторов и получателями списков аннулированных сертификатов (CRL), а также для работы с сертификатами, кросс-сертификатами и CRL выберите представление **Администрирование**.

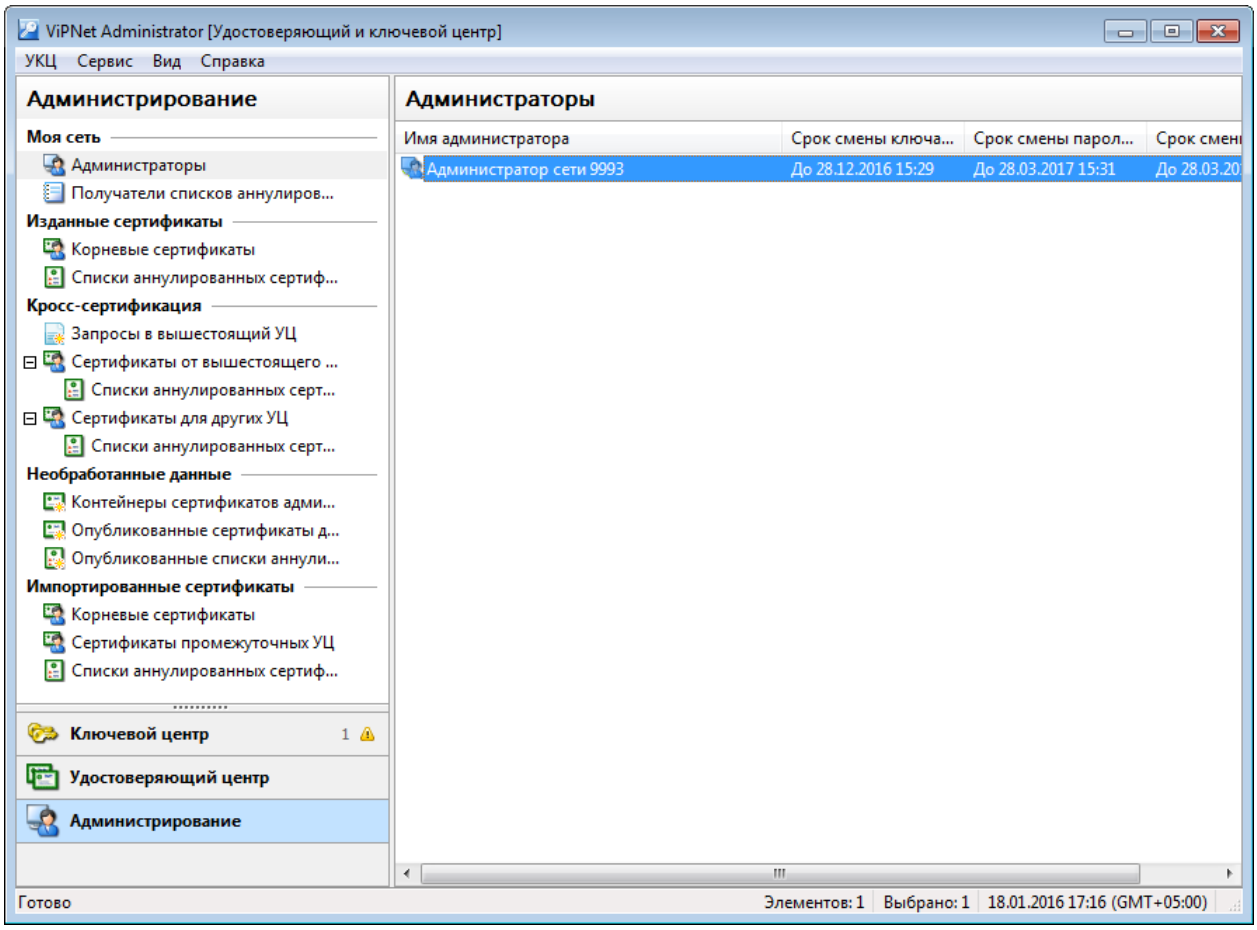

Рисунок 11. Управление учетными записями администраторов

На панели навигации будут отображены следующие разделы:

- **Моя сеть**. Этот раздел содержит два вложенных раздела:
  - **Администраторы** — в этом разделе вы можете просматривать сроки действия ключей электронной подписи администраторов, паролей администраторов, ключа защиты УКЦ, а также удалять учетные записи администраторов программы ViPNet Удостоверяющий и ключевой центр.
  - **Получатели списков аннулированных сертификатов** — в этом разделе вы можете формировать список получателей CRL в вашей сети ViPNet.

- **Изданные сертификаты** — содержит информацию об изданных корневых сертификатах администраторов и CRL.
- **Кросс-сертификация** — содержит информацию о сертификатах администраторов, полученных из вышестоящих удостоверяющих центров, запросах на сертификаты к вышестоящему удостоверяющему центру и сертификатах, изданных в УКЦ по запросам из других удостоверяющих центров.
- **Необработанные данные** — содержит информацию о сертификатах администраторов и CRL доверенных сетей, которые не были обработаны (в том числе о контейнерах с сертификатами и CRL).
- **Импортированные сертификаты** — содержит информацию об импортированных сертификатах администраторов и CRL доверенных сетей.

3

Режимы работы в программе ViPNet Удостоверяющий и ключевой центр

Режимы работы УКЦ

Работа в программе ViPNet Удостоверяющий и ключевой центр возможна в двух режимах: ручном и автоматическом.

В ручном режиме администратором выполняются, как правило, такие операции, как издание сертификатов администраторов, работа с кросс-сертификатами и другие, а также операции по работе с дистрибутивами ключей, ключами пользователей, резервными наборами ключей и мастер-ключами.

Автоматический режим работы УКЦ удобно использовать в следующих случаях:

- Во время отсутствия администратора на рабочем месте (например, в ночное время, если программа запущена круглосуточно).
- Для того чтобы освободить администратора от выполнения некоторых операций (если в УКЦ поступает большое количество запросов на сертификаты, которые требуется обрабатывать единовременно).

В ручном режиме администратором программы также могут выполняться операции автоматического режима. В автоматическом режиме выполняются те операции, которые определены в настройках программы. В окне автоматического режима администратор может только следить за ходом выполнения операций, а также за уведомлениями об операциях, которые потребуется выполнить в ручном режиме работы.

В таблице ниже приведены списки операций, которые могут быть выполнены автоматически и которые могут быть выполнены только вручную.

Таблица 1. Операции, выполняемые в разных режимах работы

Операции, которые могут быть выполнены в автоматическом и ручном режимах	Операции, которые могут быть выполнены только в ручном режиме
• Создание ключей узлов. • Удовлетворение запросов на сертификаты, подписанных пользователями сети ViPNet. • Удовлетворение запросов на сертификаты, подписанных в центрах регистрации. • Удовлетворение запросов на аннулирование сертификатов, подписанных в центрах регистрации. • Удовлетворение запросов на дистрибутивы ключей, подписанные в центрах регистрации. • Загрузка списков аннулированных сертификатов из доверенных сетей ViPNet и их передача на узлы. • Импорт списков аннулированных сертификатов других удостоверяющих центров с помощью программы ViPNet Publication Service. • Обновление списков аннулированных сертификатов и их отправка в доверенные сети ViPNet. • Отправка обновления списка аннулированных сертификатов на все узлы сети ViPNet. • Передача на публикацию списков аннулированных сертификатов с помощью программы ViPNet Publication Service. • Создание резервных копий конфигурации сети ViPNet (см. Настройка параметров создания резервных копий на стр. 167).	• Создание дистрибутивов ключей, ключей пользователей, резервных наборов персональных ключей. • Создание и обновление мастер-ключей (в том числе межсетевых). • Издание сертификатов издателей и кросс-сертификатов. • Создание запросов на кросс-сертификаты. • Передача на публикацию сертификатов издателей и сертификатов пользователей. • Импорт сертификатов издателей, полученных с помощью сервиса публикации из других удостоверяющих центров.

Операции, которые должны выполняться в автоматическом режиме, определяются на усмотрение администратора. Так, например, если в ходе эксплуатации сети ViPNet не используется инфраструктура PKI (см. глоссарий, стр. 208), но при этом довольно часто меняется структура сети (добавляются новые узлы, изменяются связи), то в автоматическом режиме целесообразно выполнять создание ключей узлов и их передачу пользователям. Остальные операции могут быть не выбраны для выполнения в автоматическом режиме.

Либо, наоборот, если пользователи сети ViPNet в своей работе используют электронную подпись, то постоянно требуется поддерживать списки аннулированных сертификатов (CRL) в актуальном состоянии. В этом случае УКЦ может переводиться в автоматический режим для обновления списков аннулированных сертификатов (см. Обновление списков аннулированных сертификатов на стр. 96).

Работа в автоматическом режиме

Переход в автоматический режим работы может производиться двумя способами:

- По команде администратора. В этом случае для перехода в автоматический режим в меню **УКЦ** выберите пункт **Перейти в автоматический режим**.

  Если для автоматического режима работы выбраны операции **Создавать ключи узлов** и **Удовлетворять запросы на дистрибутивы ключей**, при переходе в автоматический режим работы появится электронная рулетка, если в текущем сеансе работы она не запускалась. Следуйте указаниям в окне **Электронная рулетка**.

- При неактивности администратора, то есть когда в программе не производятся никакие действия в течение заданного в настройках времени (см. Настройка автоматического режима на стр. 39). В этом случае за 30 секунд до перехода в автоматический режим появится окно с сообщением. Если вы против перехода в автоматический режим, в окне с сообщением нажмите кнопку **Отмена**.

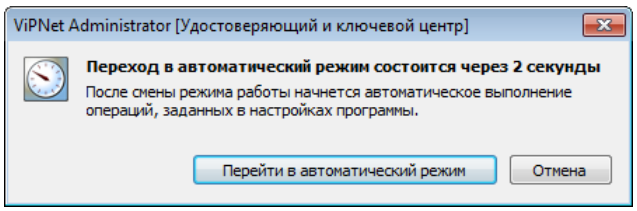

Рисунок 12. Сообщение о переходе в автоматический режим работы

Примечание. Если у вас открыты другие окна программы кроме главного (например, окно настроек), то переход в автоматический режим не будет выполнен даже по истечении заданного времени бездействия.

При переходе в автоматический режим работы появляется окно, в котором вы можете контролировать автоматическое выполнение операций (в окне отображается очередь операций, прогресс выполнения текущей операции и другое), а также следить за списком тех операций, которые требуется выполнить в ручном режиме.

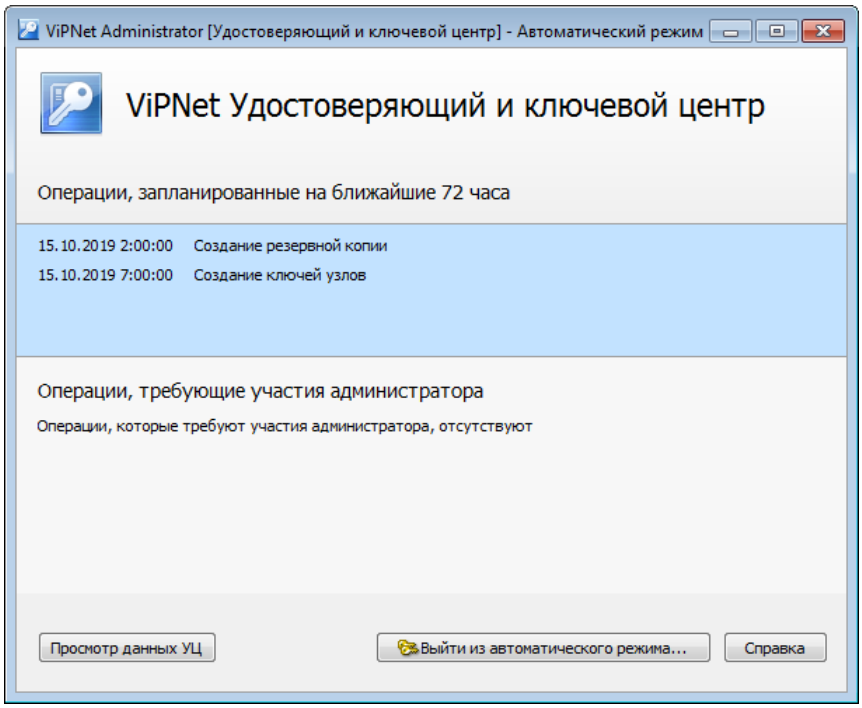

Рисунок 13. Работа программы в автоматическом режиме

При необходимости вы можете перейти из окна автоматического режима в окно просмотра данных удостоверяющего центра (изданных сертификатов и другой информации). Для этого нажмите кнопку **Просмотр данных УЦ**. Данные удостоверяющего центра в появившемся окне доступны только для чтения.

Примечание. Как правило, просмотр данных удостоверяющего центра может вам потребоваться в случае издания сертификатов по запросам в автоматическом режиме, когда нужно проанализировать количество изданных сертификатов или найти нужный сертификат, не переходя в ручной режим работы.

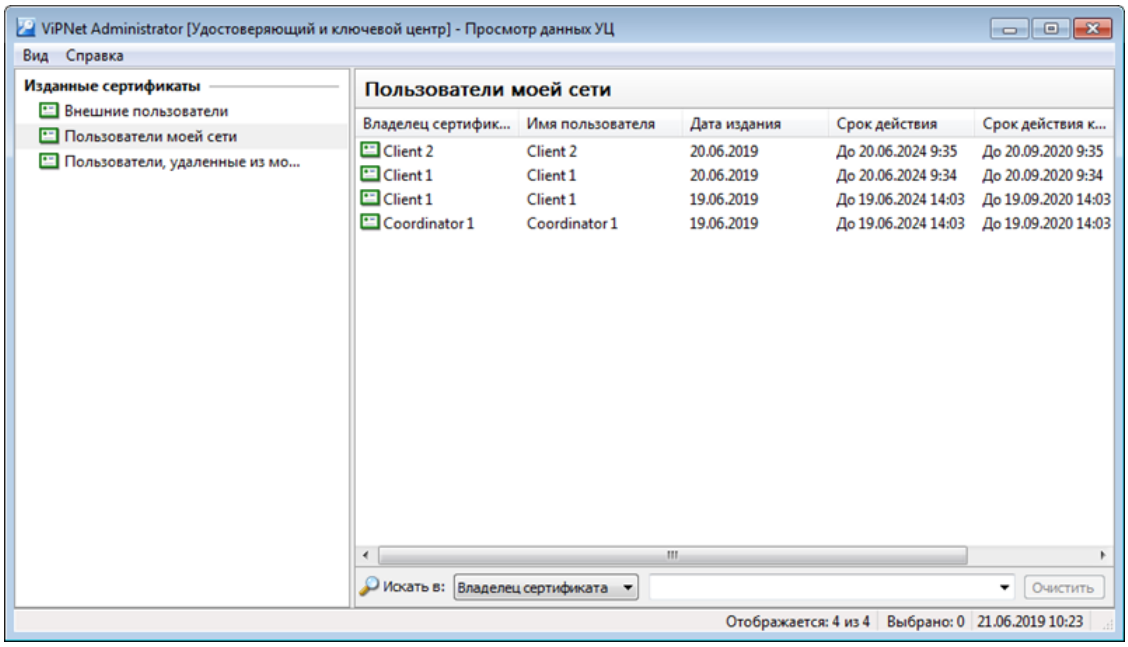

Рисунок 14. Просмотр изданных сертификатов при работе в автоматическом режиме

Чтобы перейти в ручной режим работы, в окне автоматического режима нажмите кнопку **Выйти из автоматического режима**, после чего в появившемся окне введите ваш пароль администратора. При подтверждении введенного пароля появится главное окно программы (см. Интерфейс программы ViPNet Удостоверяющий и ключевой центр на стр. 27).

Чтобы свернуть окно автоматического режима, выполните одно из действий:

- Нажмите кнопку **Закрыть** в правом верхнем углу окна.
- Нажмите сочетание клавиш **Alt+F4**.

Чтобы снова развернуть окно программы, щелкните значок в области уведомлений на панели задач.

Настройка автоматического режима

Параметры работы УКЦ в автоматическом режиме выбираются в процессе первичной инициализации программы (подробно см. в документе «ViPNet Administrator. Руководство по установке», в главе «Начало работы»). Чтобы изменить эти параметры:

1 В окне программы в меню **Сервис** выберите пункт **Настройка**.

2 В окне **Настройка** перейдите в раздел **Автоматический режим**.

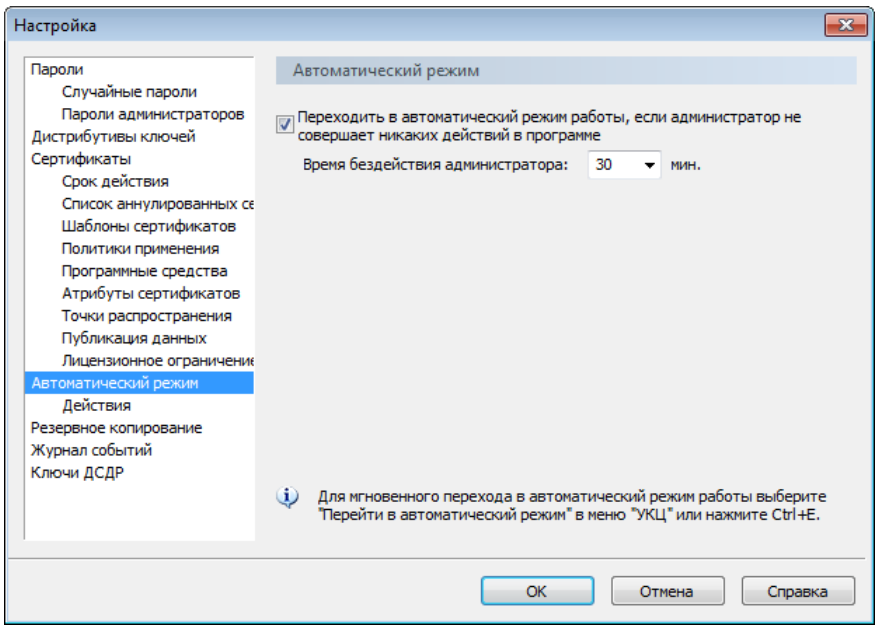

Рисунок 15. Настройка параметров перехода в автоматический режим работы в случае бездействия администратора

3 При необходимости перехода программы в автоматический режим работы, если администратор не совершает никаких действий, установите соответствующий флажок и укажите время неактивности администратора до перехода программы в автоматический режим работы в минутах.

4 Чтобы выбрать операции, которые должны выполняться в автоматическом режиме, в окне **Настройка** перейдите в раздел **Автоматический режим** > **Действия**. На панели просмотра отобразится список операций.

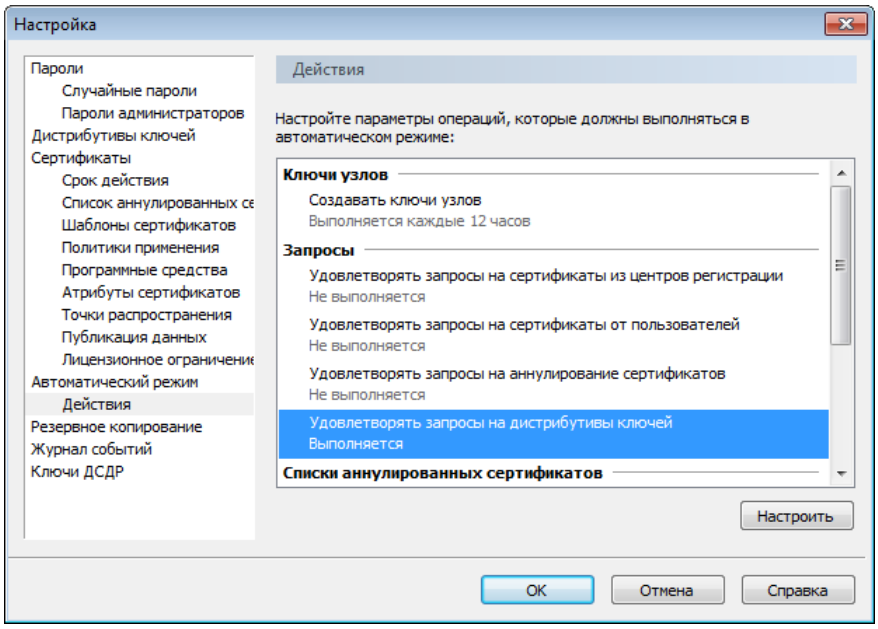

Рисунок 16. Выбор операций, которые должны выполняться в автоматическом режиме

Примечание. Если у вас отсутствует лицензия на работу УКЦ в роли удостоверяющего центра (см. Общие сведения на стр. 16), для выполнения в автоматическом режиме работы программы вы можете выбрать только операции создания ключей узлов и удовлетворения запросов на дистрибутивы ключей.

Чтобы операция выполнялась в автоматическом режиме работы УКЦ:

4.1 На панели просмотра выберите нужную операцию и нажмите кнопку **Настроить**.

4.2 В появившемся окне установите флажок и нажмите кнопку **OK**.

При выборе некоторых операций укажите, когда или с какой периодичностью они должны выполняться. Подробную информацию о таких операциях см. в следующих разделах:

- Настройка автоматического создания ключей узлов (на стр. 42).
- Настройка автоматического обновления CRL (на стр. 96).
- Настройка автоматической передачи CRL (на стр. 101).

5 Для сохранения настроек нажмите кнопку **OK**.

Примечание. Если для автоматического режима выбраны операции **Создавать ключи узлов** и **Удовлетворять запросы на дистрибутивы ключей** и установлен флажок **Переходить в автоматический режим работы, если администратор не совершает никаких действий в программе**, появится электронная рулетка (если в текущем сеансе работы она не запускалась). Следуйте указаниям в окне **Электронная рулетка**.

Особенности работы в автоматическом режиме

При работе в автоматическом режиме важно помнить о следующих особенностях:

- При переходе в автоматический режим составляется очередь операций, в соответствии с которой данные операции начинают выполняться. В очередь попадают операции, которые указаны в настройках УКЦ как автоматические (см. Настройка автоматического режима на стр. 39), а также автоматическое создание резервных копий конфигурации сети ViPNet (см. Настройка параметров создания резервных копий на стр. 167).
- Если операции создания ключей узлов или обновления списков аннулированных сертификатов (CRL) должны выполняться с определенной периодичностью, то при переходе в автоматический режим они попадут в очередь только в том случае, если истек заданный период времени с момента последнего автоматического создания ключей или обновления CRL.
- Если список аннулированных сертификатов обновляется в автоматическом режиме, то в случае наличия межсетевого взаимодействия с другими сетями ViPNet этот список сразу передается в доверенные сети вместе с корневым сертификатом администратора (сертификатом издателя).

4

Управление сертификатами

Издание сертификатов

В программе ViPNet Удостоверяющий и ключевой центр вы можете издавать сертификаты пользователей, если это разрешено вашей лицензией (см. руководство администратора на УКЦ). Сертификаты пользователей могут издаваться:

- по вашей собственной инициативе (при создании для пользователей своей сети ViPNet ключей или дистрибутивов ключей) (см. Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ на стр. 45);
- по запросам, сформированным пользователями сети ViPNet (см. Издание сертификатов по запросам от пользователей своей сети ViPNet на стр. 52);
- по запросам, поступающим из центров регистрации (см. Издание сертификатов по запросам, поступившим из центра регистрации на стр. 54);
- по запросам от внешних пользователей (см. Издание сертификатов по запросам от внешних пользователей на стр. 56).

Издание сертификатов невозможно в следующих случаях:

- Вы издали максимальное количество сертификатов, разрешенное вашей лицензией. Обратитесь за расширением лицензии к представителю компании ИнфоТеКС.
- Истек срок действия вашего текущего сертификата. Издайте новый сертификат (см. Издание сертификата администратора на стр. 147) либо получите новый сертификат по запросу в вышестоящем удостоверяющем центре, если ваш удостоверяющий центр (функции которого выполняет УКЦ) является подчиненным (см. Создание запроса на сертификат к вышестоящему удостоверяющему центру на стр. 122).
- Истек срок действия списка аннулированных сертификатов (CRL), соответствующего вашему текущему сертификату. Обновите данный CRL (см. Обновление CRL вручную на стр. 97).

Перед изданием сертификатов выполните следующие дополнительные настройки, если такие требуются:

- Чтобы при издании сертификатов появлялись мастер подготовки к изданию сертификата и мастер редактирования полей сертификата, с помощью которых вы сможете изменять параметры издаваемых сертификатов, в окне программы в меню **Сервис** выберите пункт **Настройка** и в разделе **Сертификаты** установите флажок **Редактировать поля сертификатов при издании**.
- Если при издании сертификатов будут использоваться шаблоны сертификатов, в настройках программы в разделе **Сертификаты** > **Шаблоны сертификатов** убедитесь, что присутствуют необходимые шаблоны, или создайте недостающие. Информацию по созданию и редактированию шаблонов сертификатов см. в разделе Создание и редактирование шаблонов сертификатов (см. Создание и изменение шаблонов сертификатов на стр. 58).
- Чтобы сертификаты пользователей издавались в формате квалифицированных (см. глоссарий, стр. 211), перед их изданием в настройках программы в разделе **Сертификаты** > **Программные средства** укажите ряд дополнительных параметров. Кроме этого, убедитесь, что ваш текущий

сертификат администратора имеет формат квалифицированного. Информацию по настройке см. в разделе Издание квалифицированных сертификатов (на стр. 70).

- Чтобы атрибуты в сертификатах специальным образом размещались в полях «Владелец» и «Дополнительный атрибут имени», то перед изданием сертификатов в настройках программы в разделе **Сертификаты** > **Атрибуты сертификатов** укажите, какие атрибуты в какие поля должны быть помещены. Информацию по настройке см. в разделе Настройка распределения атрибутов сертификатов (на стр. 67).

Особенности издания сертификатов

При издании сертификатов следует учитывать следующие особенности:

- При издании сертификатов в процессе создания ключей пользователей (см. руководство администратора на УКЦ), ключей электронной подписи (см. Руководство администратора) или дистрибутивов ключей (см. руководство администратора на УКЦ) создается пара ключей: ключ электронной подписи (см. глоссарий, стр. 212) и ключ проверки электронной подписи (см. глоссарий, стр. 212); ключ электронной подписи помещается в специальный контейнер . После издания сертификат с ключом проверки электронной подписи помещается также в этот контейнер и в составе ключей передается пользователю.
- При издании сертификатов по запросам ключ электронной подписи не создается, поскольку он был создан пользователем в процессе формирования запроса; издается только сертификат, который после этого отправляется пользователю вместе с ключом проверки электронной подписи. Сертификаты пользователей хранятся в базе данных ПО ViPNet Administrator.
- Издание сертификатов в процессе создания ключей пользователей (см. руководство администратора на УКЦ), ключей электронной подписи (см. руководство администратора на УКЦ) или дистрибутивов ключей (см. руководство администратора на УКЦ) производится только в том случае, если для пользователей разрешено создание ключей электронной подписи. При издании сертификатов используются параметры шаблона сертификата, установленного по умолчанию, или другого указанного вами шаблона.
- Если пользователь зарегистрирован на нескольких сетевых узлах и дистрибутивы ключей (см. руководство администратора на УКЦ) создаются для каждого узла по отдельности, количество изданных сертификатов пользователя будет совпадать с числом созданных дистрибутивов. Если дистрибутивы ключей создаются сразу для всей группы узлов, на которых зарегистрирован пользователь, то будет издан один сертификат для всех дистрибутивов этого пользователя.
- Издание сертификатов по запросам от пользователей сети и из центров регистрации может производиться в автоматическом режиме (см. Работа в автоматическом режиме на стр. 36) или вручную. Издание сертификатов по запросам от внешних пользователей выполняется только вручную. При издании сертификатов по запросам могут использоваться как параметры из шаблона сертификата, так и параметры из самого запроса.
- При издании сертификаты пользователей заверяются вашим текущим сертификатом. Поэтому они не могут быть изданы на срок, превышающий срок действия сертификата издателя.

- Если сертификат пользователя издается по запросу (в качестве источника параметров выбран именно запрос на сертификат) и в запросе присутствует политика применения, которая не зарегистрирована в УКЦ (см. Настройка списка политик применения сертификата на стр. 64), данная политика не будет добавлена в изданный сертификат.
- В сертификате пользователя не будет указан срок действия ключа электронной подписи (не будет расширения «Срок действия закрытого ключа» (PrivateKeyUsagePeriod)) в следующих случаях:
  - Сертификат издается на срок равный или менее 15 месяцев и для хранения ключа электронной подписи используется внешнее устройство без аппаратной поддержки российских криптографических алгоритмов.
  - Сертификат издается на срок равный или менее 36 месяцев и для хранения ключа электронной подписи используется устройство с аппаратной поддержкой российских криптографических алгоритмов.

  Срок действия ключа в данных случаях будет равен сроку действия сертификата.

Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ

В программе ViPNet Удостоверяющий и ключевой центр вы можете издавать сертификаты ключа проверки электронной подписи для пользователей сети ViPNet, если для них разрешено создание ключа электронной подписи и ключа проверки электронной подписи. В данном случае сертификаты можно издать при создании ключей пользователей либо дистрибутивов ключей.

Если в настройках программы в разделе **Сертификаты** установлен флажок **Редактировать поля сертификатов при издании**, то вы сможете изменить параметры издаваемого сертификата в появившемся мастере подготовки к изданию сертификата и мастере редактирования полей сертификата. Если указанный флажок не установлен, то все параметры сертификата будут полностью заимствованы из шаблона, выбранного по умолчанию. Поэтому во втором случае убедитесь, что по умолчанию выбран нужный шаблон.

Примечание. Из шаблона сертификата полностью заимствуются такие параметры, как криптопровайдер и параметры алгоритма подписи. Поэтому независимо от того, производится ли редактирование полей сертификата, данные параметры невозможно изменить при издании сертификата (они не отображаются в мастере подготовки к изданию сертификата). В связи с этим перед изданием сертификата убедитесь, что в шаблоне, который будет использоваться, правильно указаны эти параметры (см. раздел Создание и редактирование шаблонов сертификатов (см. Создание и изменение шаблонов сертификатов на стр. 58)).

Чтобы издать сертификат ключа проверки электронной подписи для пользователя:

1 В процессе создания ключей пользователя, ключей электронной подписи либо дистрибутивов ключей при соответствующих настройках программы будет запущен мастер подготовки к

созданию ключей либо мастер подготовки к выдаче новых дистрибутивов, следуйте его указаниям.

2 На странице **Выбор шаблона сертификата** выберите шаблон, из которого будут заимствованы параметры издаваемого сертификата. Затем нажмите кнопку **Далее**.

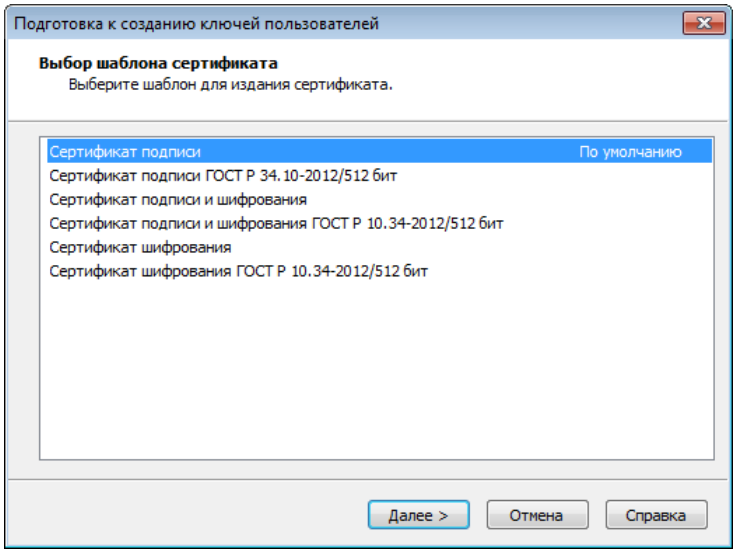

Рисунок 17. Выбор шаблона сертификата

3 На странице **Срок действия сертификата** при необходимости измените срок действия издаваемого сертификата любым удобным способом, после чего нажмите кнопку **Далее**.

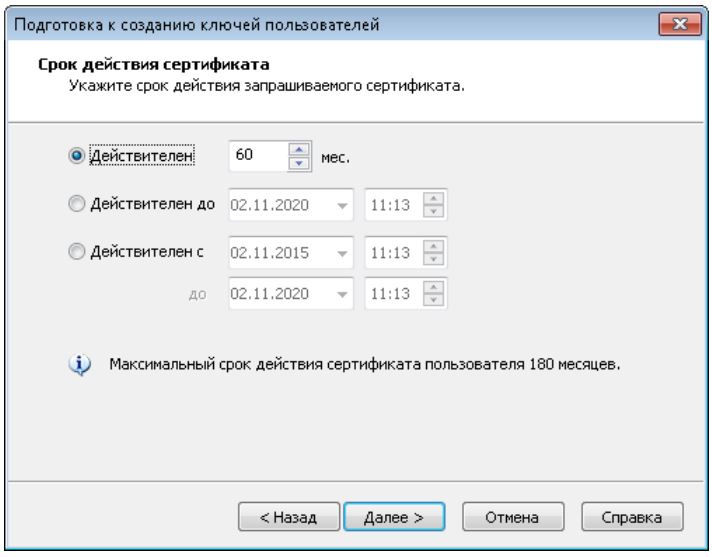

Рисунок 18. Указание срока действия сертификата

Примечание. Заданный срок действия сертификата определит срок действия ключа электронной подписи. Если срок действия сертификата не более 12 месяцев (1 года), то такой же срок действия будет у ключа электронной подписи. Если срок действия сертификата больше 12 месяцев (1 года), то срок действия ключа электронной подписи не будет превышать 15 месяцев (1 год и 3 месяца). Максимальный срок действия сертификата пользователя составляет 180 месяцев (15 лет).

4 На странице **Назначения сертификата** при необходимости измените расширения издаваемого сертификата или добавьте новые. Расширения сертификата позволяют регулировать возможности использования сертификата для выполнения определенных действий и работы с различными сервисами, например, OCSP-сервером (см. глоссарий, стр. 208), TSP-сервером (см. глоссарий, стр. 209), EFS (шифрованная файловая система) и другими.

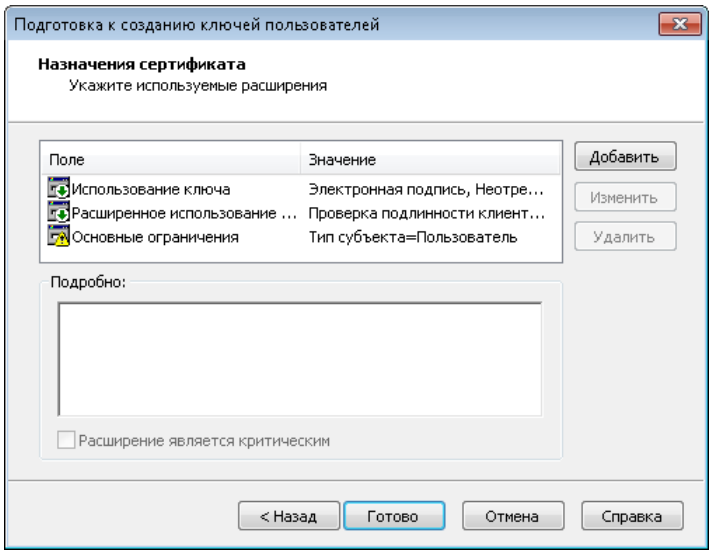

Рисунок 19. Формирование назначений сертификата

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 **OK**.

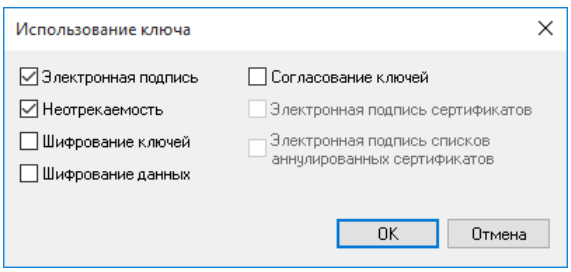

Рисунок 20. Настройка параметров использования ключа

- **Расширенное использование ключа**. В появившемся окне с помощью кнопок **Добавить** и **Удалить** сформируйте список назначений ключа и нажмите кнопку **OK**.

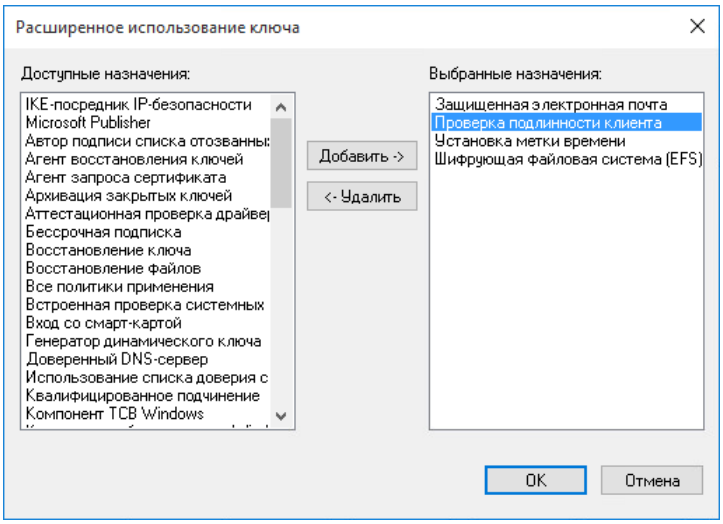

Рисунок 21. Выбор назначений расширенного использования ключа

- **Политики сертификата**. В появившемся окне с помощью кнопок **Добавить** и **Удалить** выберите политики применения сертификата, которые должны быть включены в сертификат, и нажмите кнопку **OK**. При необходимости предварительно выполните настройку списка политик применения сертификата (см. Настройка списка политик применения сертификата на стр. 64).

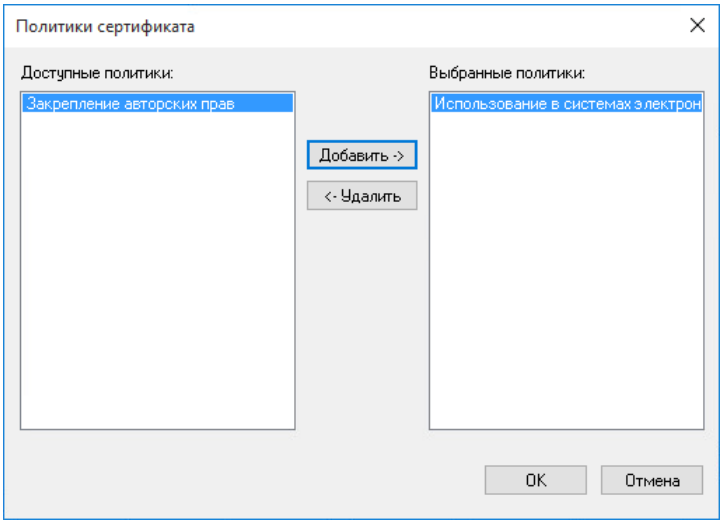

Рисунок 22. Добавление политики применения сертификата

- **Дополнительное имя субъекта**. Для указания дополнительного имени пользователя (например, DNS-имени компьютера или имени пользователя сервиса) нажмите кнопку **Добавить**, в появившемся окне задайте тип имени и его значение, затем нажмите кнопку **OK**.

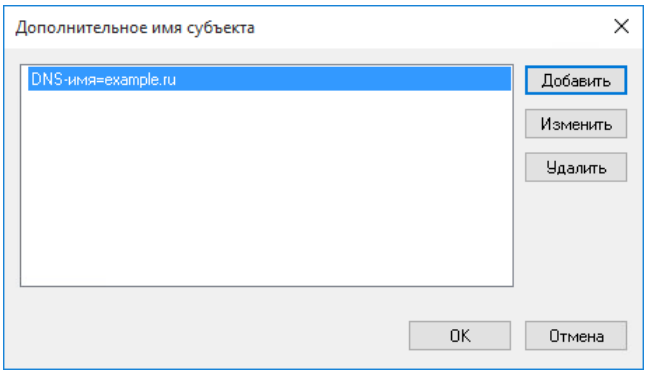

Рисунок 23. Задание альтернативного имени владельца сертификата ключа проверки электронной подписи

Для изменения параметров используемого расширения воспользуйтесь кнопкой **Изменить**, для удаления ненужного расширения — кнопкой **Удалить**.

Примечание. Расширение **Основные ограничения** нельзя изменить или удалить. С его помощью определяется, что сертификат издается для пользователя.

Если при издании сертификата вы добавили расширение **Использование ключа** или выбрали шаблон, содержащий это расширение, то данное расширение нельзя будет удалить. С его помощью определяется, в каких целях может быть использован сертификат.

При необходимости для выбранного расширения установите флажок **Расширение является критическим**. В этом случае расширение будет отмечено как критическое. Это означает, что если прикладное ПО не сможет обработать такое расширение, то сертификат будет признан недействительным.

5 Нажмите кнопку **Готово**. Появится электронная рулетка (см. глоссарий, стр. 218), если она еще не запускалась в рамках текущего сеанса работы программы. Следуйте указаниям в окне **Электронная рулетка**.

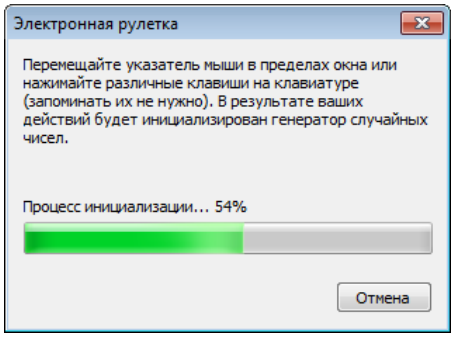

Рисунок 24. Запуск электронной рулетки

Внимание! При издании нескольких сертификатов заданные на предыдущих страницах настройки будут применены ко всем издаваемым сертификатам.

---

6 После запуска мастера **Редактирование полей сертификата** на первых трех страницах **Сведения о владельце сертификата** укажите основные данные о владельце сертификата и нажмите кнопку **Далее**.

Примечание. Если для пользователя ранее уже издавался в УКЦ сертификат, то на страницах со сведениями о владельце сертификата будут указаны данные о нем. Эти данные берутся автоматически из последнего сертификата, изданного для пользователя. При необходимости, вы можете их изменить.

Просмотреть список всех сертификатов, изданных для пользователя, и узнать, какой из них — последний, вы можете в окне просмотра свойств пользователя (см. Просмотр свойств пользователя на стр. 42).

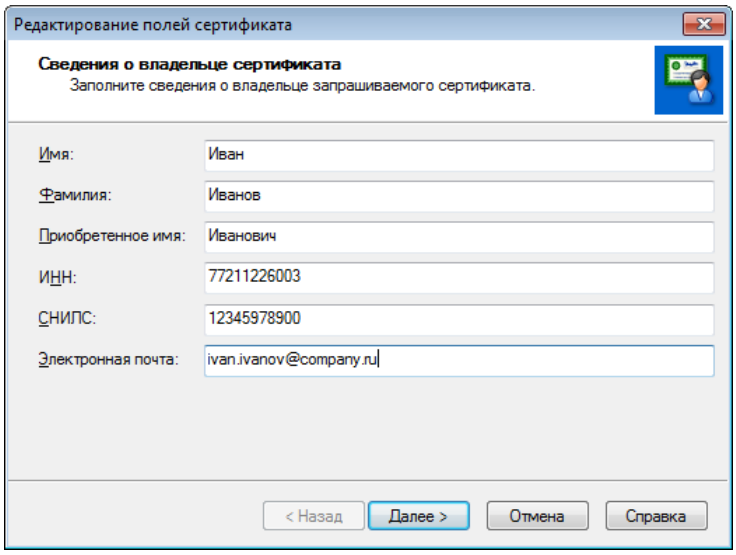

Рисунок 25. Заполнение основных сведений о владельце сертификата ключа проверки электронной подписи

7 На четвертой странице **Сведения о владельце сертификата** с помощью кнопки **Изменить** отредактируйте дополнительные данные о владельце и нажмите кнопку **Далее**.

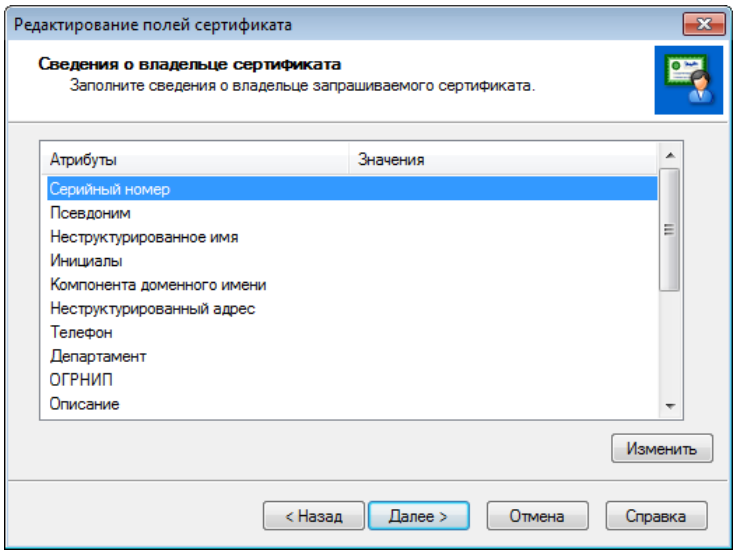

Рисунок 26. Заполнение дополнительных сведений о владельце сертификата ключа проверки электронной подписи

8 На странице **Состав сертификата** убедитесь в правильности параметров издаваемого сертификата, заданных на предыдущих страницах мастера, и нажмите кнопку **Готово**. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.

Внимание! При нажатии на кнопку **Отмена** на этой странице или на предыдущих страницах мастер прекратит свою работу, сертификат не будет издан, и дистрибутивы ключей не будут созданы.

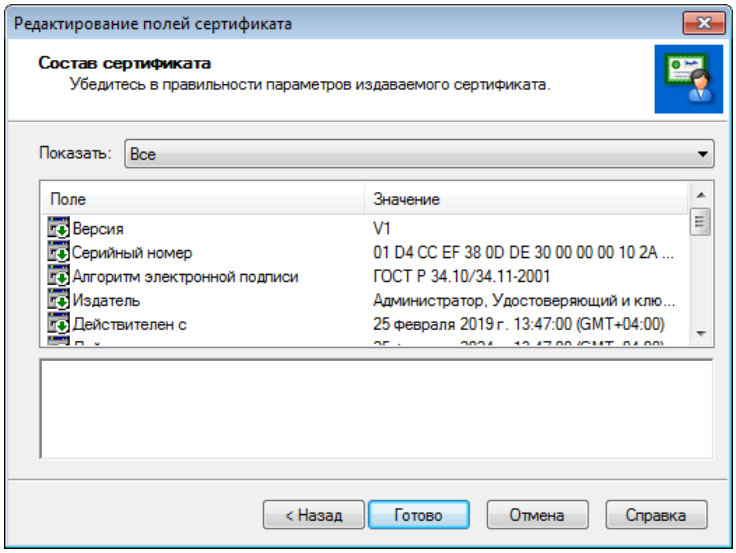

Рисунок 27. Просмотр параметров издаваемого сертификата

В результате по завершении создания ключей будет создан контейнер с ключом электронной подписи и издан сертификат ключа проверки электронной подписи пользователя. Пользователь получит изданный сертификат после того, как ключи будут переданы на узел пользователя.

Изданный сертификат появится в представлении **Удостоверяющий центр** в разделе **Изданные сертификаты** > **Пользователи моей сети**. При необходимости вы можете его там найти и просмотреть (см. Просмотр сертификатов на стр. 84).

Издание сертификатов по запросам от пользователей своей сети ViPNet

Если срок действия ключа электронной подписи и соответствующего сертификата ключа проверки электронной подписи заканчивается, либо пользователь по каким-либо причинам желает получить новый сертификат (например, сертификат с новым назначением или расширениями), он может создать запрос на новый сертификат (см. глоссарий, стр. 211) в ПО ViPNet, установленном на своем сетевом узле, и передать его в программу ViPNet Удостоверяющий и ключевой центр. Запрос будет содержаться в файле `*.sok`.

При поступлении запросы на сертификаты от пользователей помещаются в раздел **Запросы на сертификаты** > **Необработанные запросы** > **Запросы пользователей** представления **Удостоверяющий центр**. Все поступившие запросы требуется обработать: удовлетворить либо отклонить. Запросы на сертификаты могут обрабатываться в автоматическом режиме (см. Работа в автоматическом режиме на стр. 36) или вручную. При автоматической обработке запросы всегда удовлетворяются. Отклонить запрос можно только при обработке вручную.

Для обработки запросов на сертификаты от пользователей в автоматическом режиме должны быть выполнены соответствующие настройки (см. Настройка автоматического режима на стр. 39).
Чтобы обработать запросы на сертификаты вручную:

1. В окне программы на панели навигации выберите представление **Удостоверяющий центр** и перейдите в раздел **Запросы на сертификаты** > **Необработанные запросы** > **Запросы пользователей**.
2. На панели просмотра выберите один или несколько запросов и на панели инструментов нажмите кнопку **Удовлетворить** или кнопку **Отклонить**. При необходимости просмотрите параметры запроса (см. Просмотр запроса на сертификат на стр. 82).
3. При удовлетворении запроса начнется процесс издания сертификата. Если в настройках программы в разделе **Сертификаты** установлен флажок **Редактировать поля сертификатов при издании**, будет запущен мастер редактирования полей сертификата. Вы можете изменить параметры издаваемого сертификата, следуя указаниям мастера:
   - **3.1** На страницах **Сведения о владельце сертификата** выберите тип владельца сертификата и укажите необходимые данные о владельце сертификата.

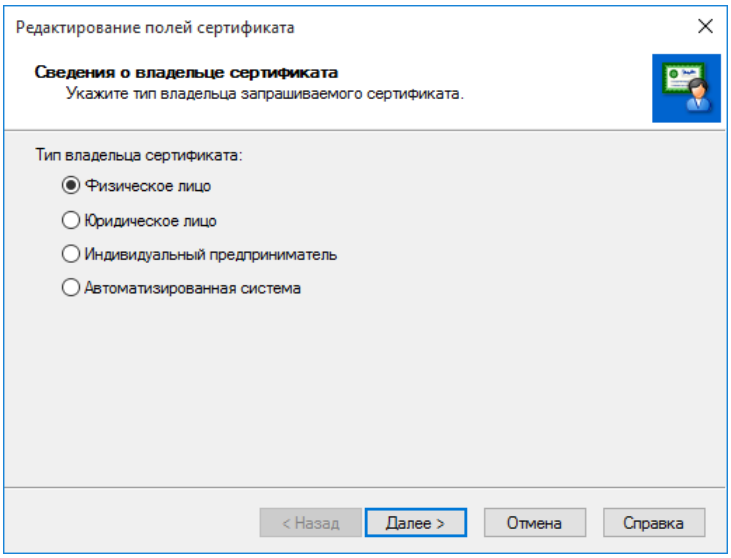

Рисунок 28. Выбор типа владельца сертификата при удовлетворении запроса на сертификат

3.2 На странице **Источник параметров сертификата** укажите источник, из которого будут заимствованы параметры издаваемого сертификата: запрос на сертификат либо шаблон сертификата. Во втором случае в списке также выберите нужный шаблон. Чтобы отказаться от просмотра параметров издаваемого сертификата снимите флажок **Показывать параметры сертификата.**

3.3 Если на странице **Источник параметров сертификата** был установлен флажок **Показывать параметры сертификата**, на остальных страницах мастера при необходимости измените параметры сертификата, установленные по умолчанию в соответствии с выбранным источником.

3.4 На странице **Состав сертификата** убедитесь в правильности параметров издаваемого сертификата, заданных на предыдущих страницах мастера, и нажмите кнопку **Готово**.

Примечание. При удовлетворении запроса с недействительной подписью появится сообщение с предложением отклонить запрос. Издать сертификат по такому запросу нельзя.

---

4 При отклонении запроса в появившемся окне с сообщением подтвердите операцию.

В результате удовлетворения запроса будет издан сертификат, после чего отправлен на сетевой узел пользователя. Изданный сертификат появится в разделе **Изданные сертификаты** > **Пользователи моей сети**, запрос будет перемещен в раздел **Запросы на сертификаты** > **Удовлетворенные запросы**.

В результате отклонения запроса на сетевой узел пользователя будет отправлен файл запроса в неизменном виде. Подобный ответ будет интерпретирован как отказ в издании сертификата. Запрос будет перемещен в раздел **Запросы на сертификаты** > **Отклоненные запросы**.

Издание сертификатов по запросам, поступившим из центра регистрации

Выдача сертификатов подписи пользователям своей сети ViPNet или зарегистрированным внешним пользователям может производиться по специальным запросам через центры регистрации. В данном случае в программе ViPNet Registration Point для пользователя формируется запрос на сертификат, который заверяется сертификатом администратора центра регистрации, после чего передается в программу ViPNet Удостоверяющий и ключевой центр (см. раздел Взаимодействие с программой ViPNet Registration Point (на стр. 19)).

При поступлении запроса на сертификаты из центра регистрации помещаются в раздел **Запросы на сертификаты** > **Необработанные запросы** > **Запросы центров регистрации** представления **Удостоверяющий центр**. Все поступившие запросы требуется обработать: удовлетворить либо отклонить. Запросы на сертификаты могут обрабатываться в автоматическом режиме (см. Работа в автоматическом режиме на стр. 36) или вручную. При автоматической обработке запросы всегда удовлетворяются. Отклонить запрос можно только при обработке вручную.

Совет. Если требуется, чтобы сертификаты, изданные по запросам из центров регистрации, содержали информацию об этих центрах — имя и серийный номер сертификата администратора центра регистрации — перед обработкой запросов выполните соответствующую настройку (см. Настройка добавления информации о центрах регистрации в сертификаты пользователей на стр. 66).

Для обработки запросов на сертификаты из центра регистрации в автоматическом режиме должны быть выполнены соответствующие настройки (см. Настройка автоматического режима на стр. 39). Чтобы обработать запросы на сертификаты вручную:

1. В окне программы на панели навигации выберите представление **Удостоверяющий центр** и перейдите в раздел **Запросы на сертификаты** > **Необработанные запросы** > **Запросы центров регистрации**.
2. На панели просмотра выберите один или несколько запросов и на панели инструментов нажмите кнопку **Удовлетворить** или кнопку **Отклонить**. При необходимости просмотрите параметры запроса (см. Просмотр запроса на сертификат на стр. 82).
3. При удовлетворении запроса начнется процесс издания сертификата. Если в настройках программы в разделе **Сертификаты** установлен флажок **Редактировать поля сертификатов при издании**, будет запущен мастер редактирования полей сертификата. Вы можете изменить параметры издаваемого сертификата, следуя указаниям мастера:
   3.1 На страницах **Сведения о владельце сертификата** выберите тип владельца сертификата и укажите необходимые данные о владельце сертификата.

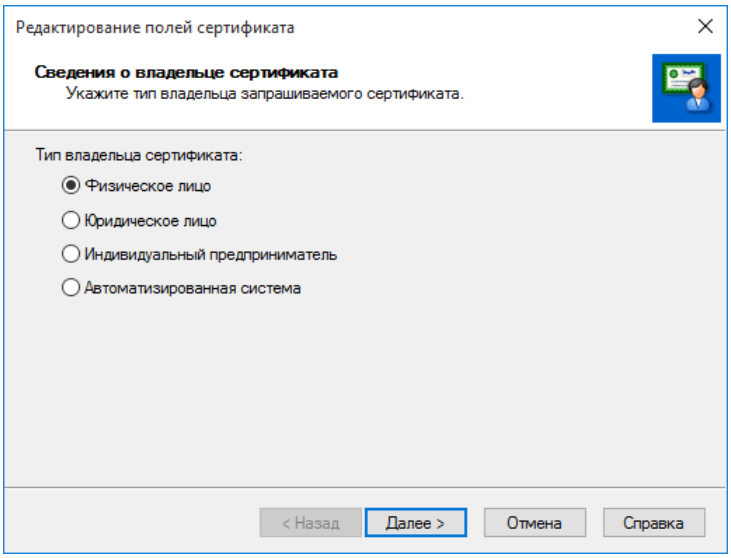

Рисунок 29. Выбор типа владельца сертификата при удовлетворении запроса на сертификат

3.2 На странице **Источник параметров сертификата** укажите источник, из которого будут заимствованы параметры издаваемого сертификата: запрос на сертификат либо шаблон сертификата. Во втором случае в списке также выберите нужный шаблон. Чтобы отказаться от просмотра параметров издаваемого сертификата снимите флажок **Показывать параметры сертификата.**

3.3 Если на странице **Источник параметров сертификата** был установлен флажок **Показывать параметры сертификата**, на остальных страницах мастера при необходимости измените параметры сертификата, установленные по умолчанию в соответствии с выбранным источником.

3.4 На странице **Состав сертификата** убедитесь в правильности параметров издаваемого сертификата, заданных на предыдущих страницах мастера, и нажмите кнопку **Готово**.

Примечание. При удовлетворении запроса с недействительной подписью появится сообщение с предложением отклонить запрос. Издать сертификат по такому запросу нельзя.

---

4 При отклонении запроса в появившемся окне с сообщением подтвердите операцию.

В результате удовлетворения запроса будет издан сертификат, после чего отправлен в центр регистрации. Изданный сертификат для пользователя своей сети ViPNet появится в разделе **Изданные сертификаты** > **Пользователи моей сети**. Изданный сертификат для внешнего пользователя появится в разделе **Изданные сертификаты** > **Внешние пользователи**. Запрос будет перемещен в раздел **Запросы на сертификаты** > **Удовлетворенные запросы**.

В результате отклонения запроса в центр регистрации будет отправлен файл с запросом в неизменном виде. Подобный ответ будет интерпретирован как отказ в издании сертификата. Запрос будет перемещен в раздел **Запросы на сертификаты** > **Отклоненные запросы**.

Издание сертификатов по запросам от внешних пользователей

Запросы на издание сертификатов могут поступать напрямую от внешних пользователей. Такие запросы передаются в виде файлов в одном из следующих форматов:

- PKCS #10 (файл `*.p10`) — широко распространенный формат запросов на сертификат, поддерживаемый большинством удостоверяющих центров. Подробнее см. RFC 2986).
- CMC (файл `*.cmc`) — менее распространенный формат запросов на сертификат. Подробнее см. RFC 5272.

Запросы на издание сертификатов от внешних пользователей вы можете обработать только вручную. Для этого выполните следующие действия:

1 В окне программы на панели навигации выберите представление **Удостоверяющий центр** и перейдите в раздел **Изданные сертификаты** > **Внешние пользователи**.

2 На панели просмотра нажмите кнопку **Загрузить и обработать запрос**.

3 В появившемся окне выберите файл `*.p10` или `*.cmc`, в котором содержится запрос.

Примечание. При необходимости можно выбрать сразу несколько файлов с запросами.

Запросы, размер которых превышает 10 Кбайт, загрузить нельзя.

---

4 В окне **Издание сертификатов пользователей** в списке ознакомьтесь с параметрами запроса: для кого запрошен сертификат и какой статус у запроса в текущий момент. При необходимости просмотрите параметры запроса с помощью кнопки **Свойства** (см. Просмотр запроса на сертификат (на стр. 82)).

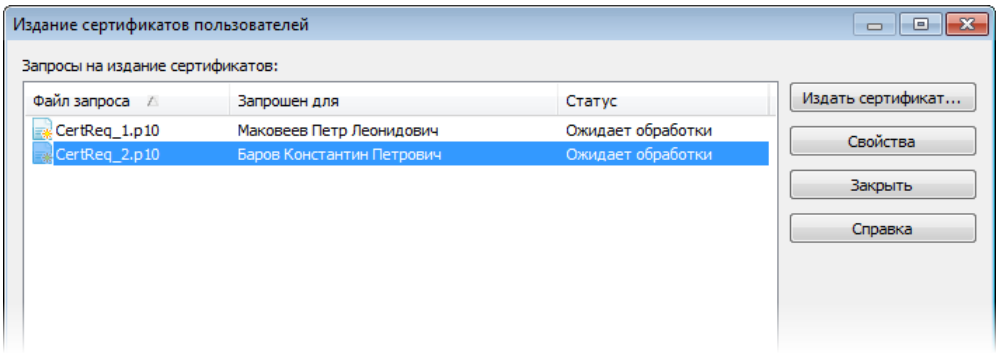

Рисунок 30. Выбор запроса для издания сертификата

5 Выберите запрос в списке, после чего нажмите кнопку **Издать сертификат**. Если в настройках программы в разделе **Сертификаты** установлен флажок **Редактировать поля сертификатов при издании**, будет запущен мастер редактирования полей сертификата. Вы можете изменить параметры издаваемого сертификата, следуя указаниям мастера.

6 На страницах **Сведения о владельце сертификата** выберите тип владельца сертификата и укажите необходимые данные о владельце сертификата.

7 На странице **Источник параметров сертификата** укажите источник, из которого будут заимствованы параметры издаваемого сертификата: запрос на сертификат либо шаблон сертификата. Во втором случае в списке также выберите нужный шаблон. Чтобы отказаться от просмотра параметров издаваемого сертификата снимите флажок **Показывать параметры сертификата**.

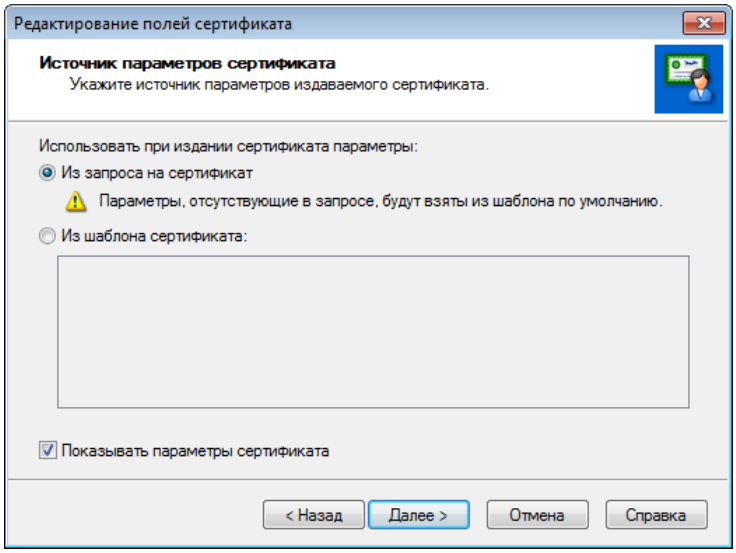

Рисунок 31. Выбор источника параметров издаваемого сертификата

8 Если на странице **Источник параметров сертификата** был установлен флажок **Показывать параметры сертификата**, на остальных страницах мастера при необходимости измените параметры сертификата, установленные по умолчанию в соответствии с выбранным источником.

9 На странице **Состав сертификата** убедитесь в правильности параметров издаваемого сертификата, заданных на предыдущих страницах мастера, после чего нажмите кнопку **Готово**.

10 В окне сообщения об успешном издании сертификата нажмите кнопку **OK**.

В результате будет издан сертификат, который появится в представлении **Удостоверяющий центр** в разделе **Изданные сертификаты** > **Внешние пользователи**. Выполните экспорт сертификата (см. Экспорт сертификатов на стр. 88) для его последующей передачи пользователю.

Настройка параметров издания сертификатов

Создание и изменение шаблонов сертификатов

В программе ViPNet Удостоверяющий и ключевой центр при издании сертификатов ключа проверки электронной подписи используются шаблоны сертификатов (см. глоссарий, стр. 218) в следующих случаях:

- всегда при издании сертификатов по инициативе администратора УКЦ;
- при издании сертификатов по запросам, если в качестве источника параметров сертификата выбран шаблон.

В зависимости от настроек программы во время издания сертификата его параметры могут либо заимствоваться из шаблона полностью без возможности изменения, либо дополняться и изменяться (за исключением криптопровайдера и параметров алгоритма подписи, которые всегда берутся из шаблона).

Примечание. Параметры всех шаблонов сертификатов хранятся в файле `cert_tem.ini` в папке `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\ini`. При обновлении программного обеспечения существующие шаблоны не изменяются и не удаляются.

В конфигурацию программы входит несколько стандартных шаблонов сертификатов подписи и шифрования с разными алгоритмами подписи:

- «Сертификат подписи» — пользователь может использовать ключ для электронной подписи и не может отказаться от совершенного действия.
- «Сертификат подписи и шифрования» — пользователь может использовать ключ для электронной подписи, шифрования ключей и данных, согласования ключей и не может отказаться от совершенного действия.
- «Сертификат шифрования» — пользователь может использовать ключ для шифрования ключей и данных, а также согласования ключей.

Примечание. По требованиям ФСБ России после 31 декабря 2019 года использование алгоритма ГОСТ Р 34.10-2001 для формирования электронной подписи недопустимо. Поэтому в качестве шаблона сертификата вы можете назначить только шаблон с алгоритмом ГОСТ Р 34.10-2012.

При необходимости администратор УКЦ может с помощью мастера создать другие шаблоны сертификатов или отредактировать существующие.

Для создания нового шаблона сертификата:

1 В окне программы в меню **Сервис** выберите пункт **Настройка**.

2 В появившемся окне на панели навигации выберите раздел **Сертификаты** > **Шаблоны сертификатов**.

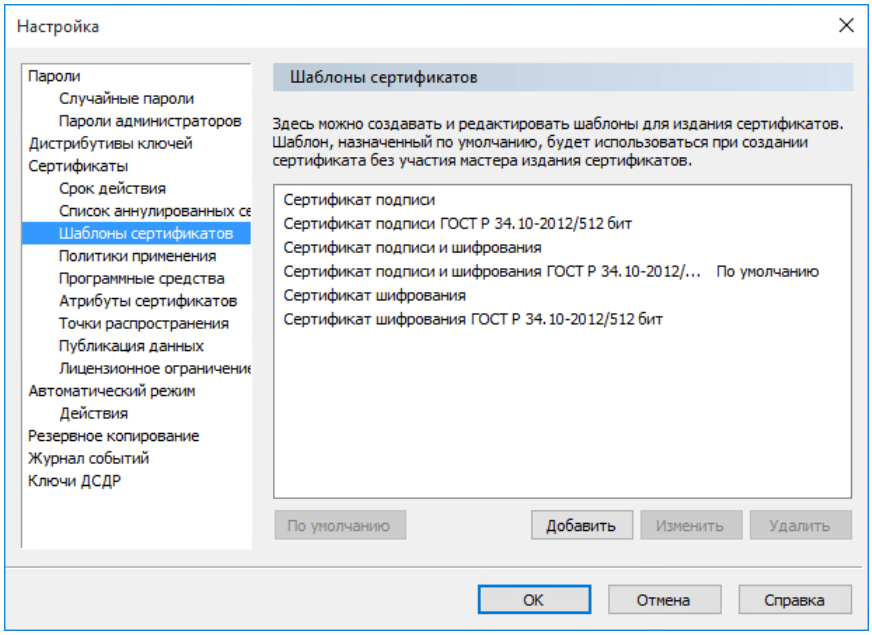

Рисунок 32. Управление шаблонами сертификатов

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** выберите криптопровайдер, установленный на компьютере. Выбранный криптопровайдер определит алгоритм электронной подписи, по которому будут создаваться ключ электронной подписи и ключ проверки электронной подписи.

Кроме этого, укажите параметры алгоритма электронной подписи. В соответствии с заданными параметрами будет автоматически определена длина ключа проверки электронной подписи. Характеристики ViPNet CSP и алгоритмов электронной подписи см. в документе «ViPNet CSP 4.4. Руководство пользователя».

Совет. Рекомендуется использовать параметры алгоритма, предлагаемые по умолчанию. Данные параметры характеризуются наибольшей скоростью вычисления и проверки электронной подписи.

После этого нажмите кнопку **Далее**.

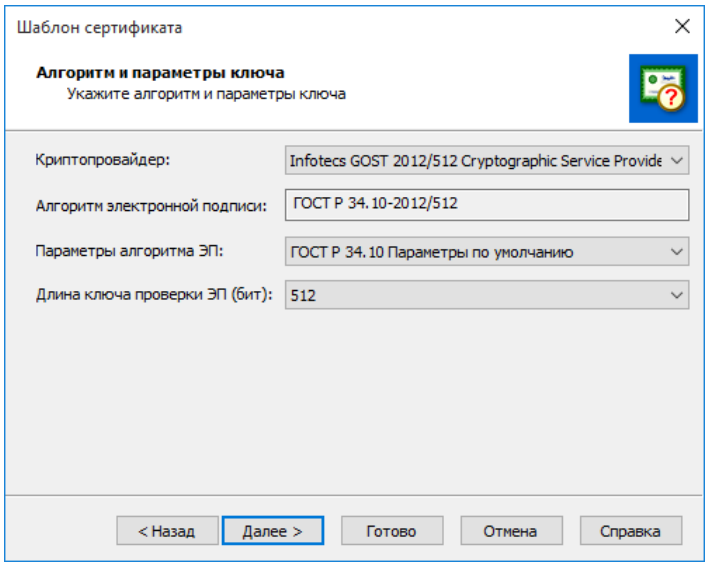

Рисунок 33. Настройка параметров ключа электронной подписи

6 На следующей странице задайте срок действия сертификата, после чего нажмите кнопку **Далее**.

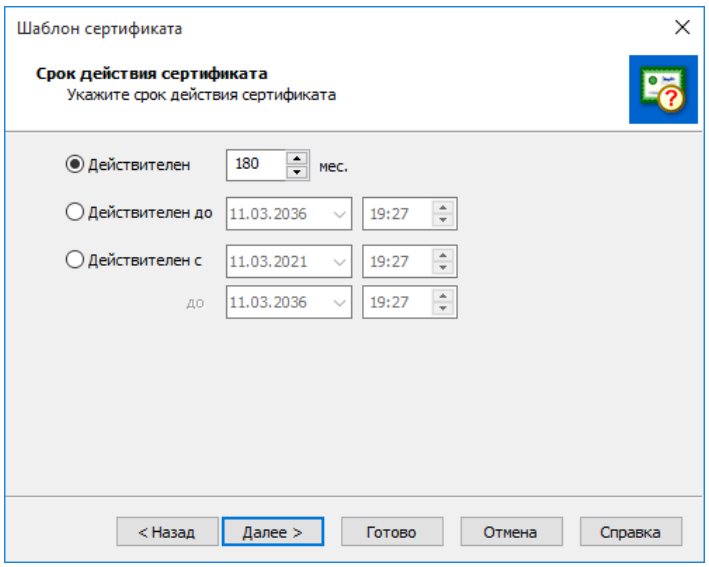

Рисунок 34. Указание срока действия сертификата

Примечание. Заданный срок действия сертификата определяет срок действия ключа электронной подписи. Если срок действия сертификата не более 12 месяцев (1 года), то такой же срок действия будет у ключа электронной подписи. Если срок действия сертификата больше 12 месяцев (1 года), то срок действия ключа электронной подписи не будет превышать 15 месяцев (1 год и 3 месяца). Максимальный срок действия сертификата пользователя составляет 180 месяцев (15 лет).

---

7 На странице **Расширения сертификата** укажите необходимые расширения, которые будут добавлены в новый шаблон. Расширения сертификата позволяют регулировать возможности использования сертификата для выполнения определенных действий и работы с различными

сервисами, например, OCSP-сервером (см. глоссарий, стр. 208), TSP-сервером (см. глоссарий, стр. 209), EFS (шифрованная файловая система) и другими.

По умолчанию в шаблон добавлено расширение **Основные ограничения**, с помощью которого определяется, что сертификат издается для пользователя. Удалить это расширение или изменить его нельзя.

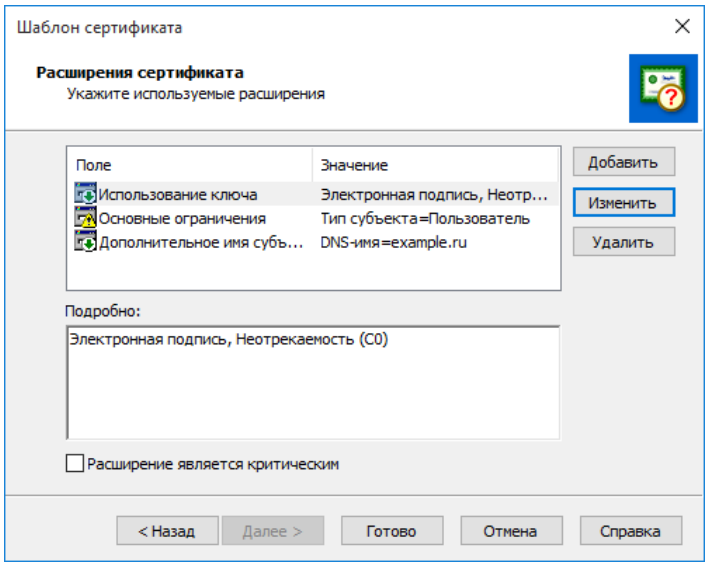

Рисунок 35. Формирование расширений сертификата

Для добавления расширения нажмите кнопку **Добавить** и в окне **Допустимые расширения** выберите одно из расширений:

- **Тип идентификации**. В появившемся окне укажите тип идентификации владельца сертификата.

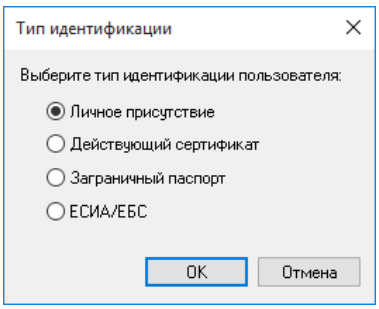

Рисунок 36. Выбор типа идентификации владельца сертификата

- **Использование ключа**. В появившемся окне укажите назначение ключа и сертификата, установив соответствующие флажки, и нажмите кнопку **OK**.

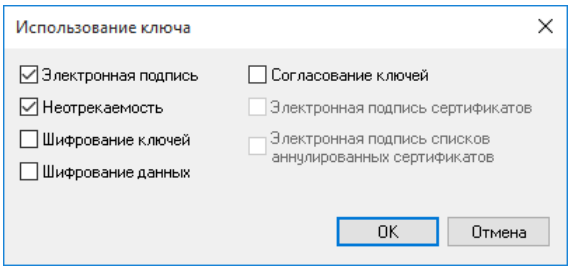

Рисунок 37. Настройка параметров использования ключа

- **Улучшенный ключ**. В окне **Расширенное использование ключа** с помощью кнопок **Добавить** и **Удалить** сформируйте список расширенного использования ключа и нажмите кнопку **OK**.

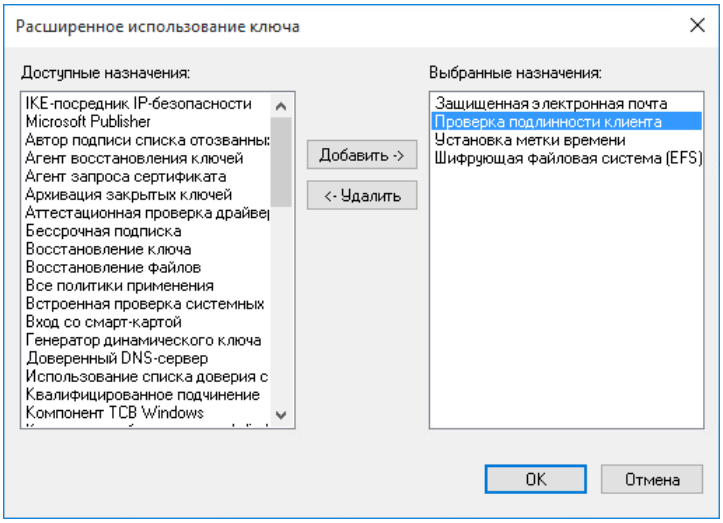

Рисунок 38. Выбор назначений расширенного использования ключа

- **Политики сертификата**. В появившемся окне с помощью кнопок **Добавить** и **Удалить** выберите политики применения сертификата и нажмите кнопку **OK**. При необходимости предварительно выполните настройку списка политик применения сертификата (см. Настройка списка политик применения сертификата на стр. 64).

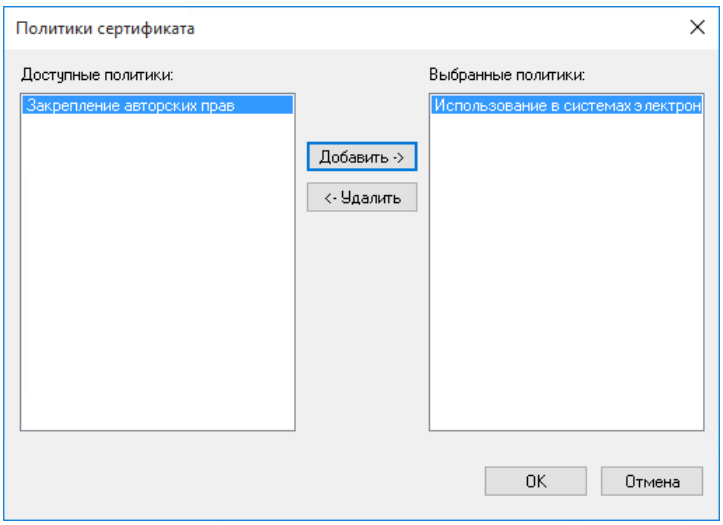

Рисунок 39. Добавление политики применения сертификата

Примечание. В настройках программы в списке используемых политик применения присутствуют политики, описывающие класс защиты средств удостоверяющего центра. В создаваемые шаблоны их добавить нельзя. В издаваемые сертификаты пользователей эти политики добавляются всегда по умолчанию при соответствующих настройках программы (см. Настройка параметров издания квалифицированных сертификатов на стр. 74).

- **Дополнительное имя субъекта**. Для указания дополнительного имени пользователя сертификата (например, DNS-имени компьютера или имени пользователя сервиса) нажмите кнопку **Добавить**, в появившемся окне задайте тип имени и его значение, затем нажмите кнопку **OK**.

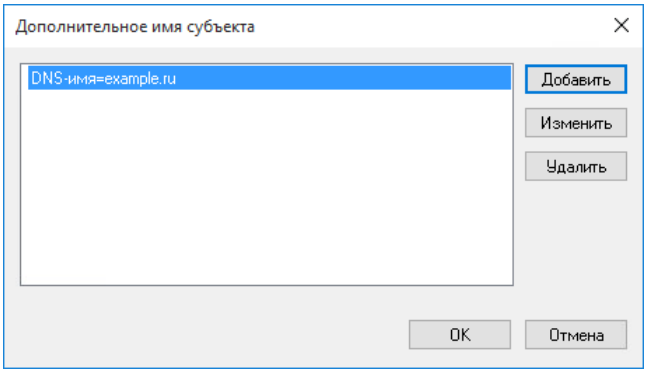

Рисунок 40. Задание альтернативного имени владельца сертификата ключа проверки электронной подписи

Для изменения параметров используемого расширения воспользуйтесь кнопкой **Изменить**, для удаления ненужного расширения — кнопкой **Удалить**.

При необходимости для выбранного расширения установите флажок **Расширение является критическим**. В этом случае расширение будет отмечено как критическое. Это означает, что если прикладное ПО не сможет обработать такое расширение, то сертификат будет признан недействительным.

8 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 **OK**.

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 **OK**.

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 (см. глоссарий, стр. 209)) после добавления, изменения или удаления шаблонов сертификатов сформируйте и отправьте на них ключи узлов (см. руководство администратора на УКЦ). Данная операция требуется для того, чтобы в центры регистрации поступила актуальная информация о шаблонах сертификатов, сформированных в УКЦ.

Чтобы назначить шаблон используемым по умолчанию, выберите его в списке и нажмите кнопку **По умолчанию**. В соответствии с параметрами данного шаблона будет производиться издание сертификатов ключа проверки электронной подписи при автоматическом создании ключей и дистрибутивов.

Настройка списка политик применения сертификата

Область использования сертификата ключа проверки электронной подписи можно определить путем добавления в него специального расширения — политики применения (см. глоссарий, стр. 216). 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).

С политикой применения изданного сертификата ключа проверки электронной подписи можно ознакомиться, нажав кнопку **Заявление издателя** в окне просмотра сертификата.

Примечание. Политика применения может быть представлена в виде текста или ссылки на веб-страницу.

В конфигурации программы имеются политики применения, описывающие классы защищенности средств электронной подписи, но они скрыты от администратора и в настройках программы не отображаются. Данные политики в обязательном порядке добавляются в издаваемые квалифицированные сертификаты при соответствующих настройках программы (см. Издание квалифицированных сертификатов на стр. 70).

Политики применения также можно добавлять в шаблоны сертификатов. Подробнее см. раздел Создание и редактирование шаблонов сертификатов (см. Создание и изменение шаблонов сертификатов на стр. 58).

Прежде чем добавить политику применения в издаваемый сертификат или шаблон сертификата, ее предварительно требуется создать. Чтобы создать политику применения:

1. В окне программы в меню **Сервис** выберите пункт **Настройка**.
2. В появившемся окне на панели навигации выберите раздел **Сертификаты** > **Политики применения**.

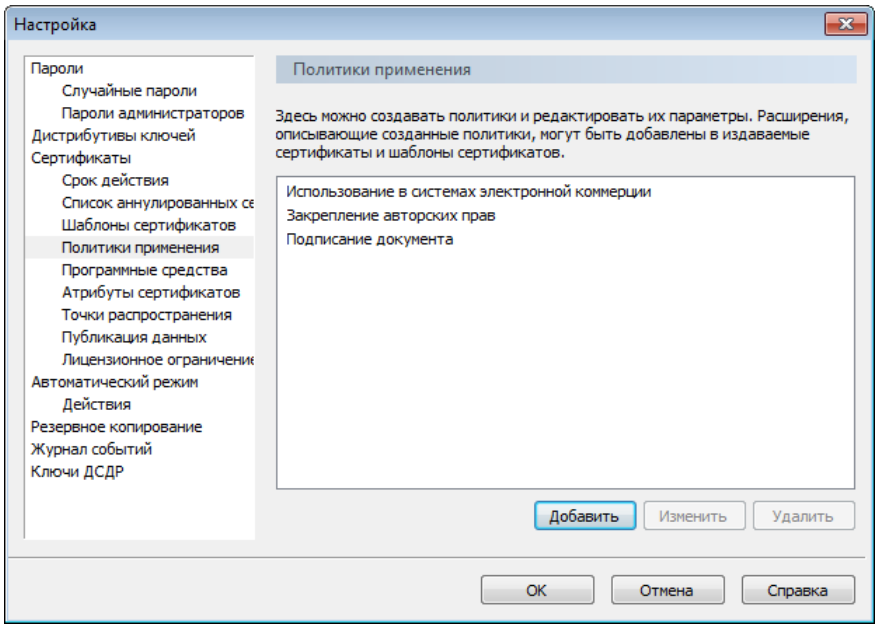

Рисунок 41. Управление политиками применения сертификатов

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 — OID (см. глоссарий, стр. 211). 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.

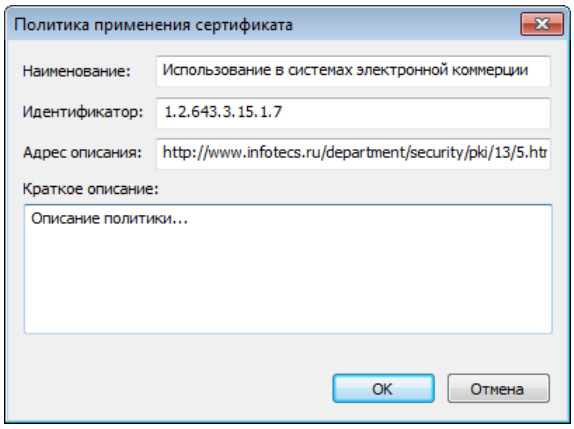

Рисунок 42. Добавление политики применения

5 По окончании ввода данных нажмите кнопку **OK**. Созданная политика появится в списке в разделе **Политики применения**.

6 Для сохранения новой политики применения нажмите кнопку **OK**.

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 **OK**.

Чтобы удалить политику, выберите ее в списке и нажмите кнопку **Удалить**.

Примечание. При взаимодействии с центрами регистрации (узлами с программным обеспечением ViPNet Registration Point (см. глоссарий, стр. 209)) после добавления, изменения или удаления политик применения сертификатов сформируйте и отправьте на них ключи узлов (см. руководство администратора на УКЦ). Данная операция требуется для того, чтобы в центры регистрации поступила актуальная информация о политиках применения, заданных в УКЦ.

Настройка добавления информации о центрах регистрации в сертификаты пользователей

В сертификаты пользователей, издаваемые по запросам из центров регистрации (см. Издание сертификатов по запросам, поступившим из центра регистрации на стр. 54), может добавляться информация об этих центрах — имя и серийный номер сертификата администратора центра регистрации.

Примечание. Информация о центре регистрации, по запросу из которого был издан сертификат, может потребоваться при возникновении конфликтных ситуаций, связанных с использованием сертификата, особенно в том случае, если в удостоверяющем центре функционирует большое количество центров регистрации и невозможно быстро установить, каким из них этот сертификат был выдан.

Чтобы информация о центрах регистрации добавлялась в издаваемые сертификаты пользователей:

1 В окне программы в меню **Сервис** выберите пункт **Настройка**.

2 В появившемся окне на панели навигации выберите раздел **Сертификаты** > **Атрибуты сертификатов**.

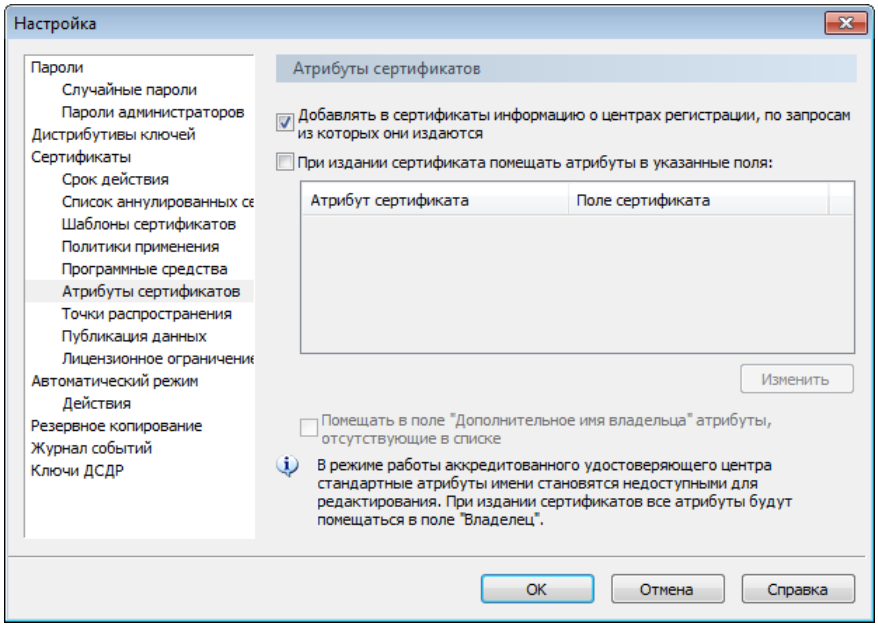

Рисунок 43. Настройка добавления информации о центрах регистрации в издаваемые сертификаты

3 Установите флажок **Добавлять в сертификаты информацию о центрах регистрации, по запросам из которых они издаются**.

4 Чтобы сохранить настройки, нажмите кнопку **OK**.

В результате информация о центрах регистрации будет добавляться в сертификаты, издаваемые по их запросам.

Настройка распределения атрибутов сертификатов

Для передачи идентификационных данных о владельце сертификата используются атрибуты имени. Например, такие как «ОГРН», «ОГРНИП», «ИНН физического лица», «ИНН юридического лица», «СНИЛС». В сертификатах атрибуты имени могут размещаться в полях типа «Владелец» или «Дополнительный атрибут имени». Если вы хотите, чтобы в соответствии с рекомендациями приказа ФСБ от 27.12.2011 № 795 в сертификатах часть атрибутов имени находилась в поле «Владелец», а часть — в поле «Дополнительный атрибут имени», то вы можете указать, в какое поле должны помещаться те или иные атрибуты при издании сертификатов.

Внимание! Заданное распределение атрибутов будет распространяться только на сертификаты пользователей.

В квалифицированных сертификатах все атрибуты автоматически помещаются в поле «Владелец». Если в запросе на сертификат для каких-то атрибутов было указано поле «Дополнительный атрибут имени», то в режиме работы аккредитованного удостоверяющего центра оно будет автоматически изменено на поле «Владелец». Возможность изменения полей в настройках УКЦ для стандартных атрибутов станет недоступна.

Чтобы указать, в каких полях должны располагаться атрибуты в издаваемых сертификатах, выполните следующие действия:

1 В окне программы в меню **Сервис** выберите пункт **Настройка**.

2 В появившемся окне на панели навигации выберите раздел **Сертификаты** > **Атрибуты сертификатов**.

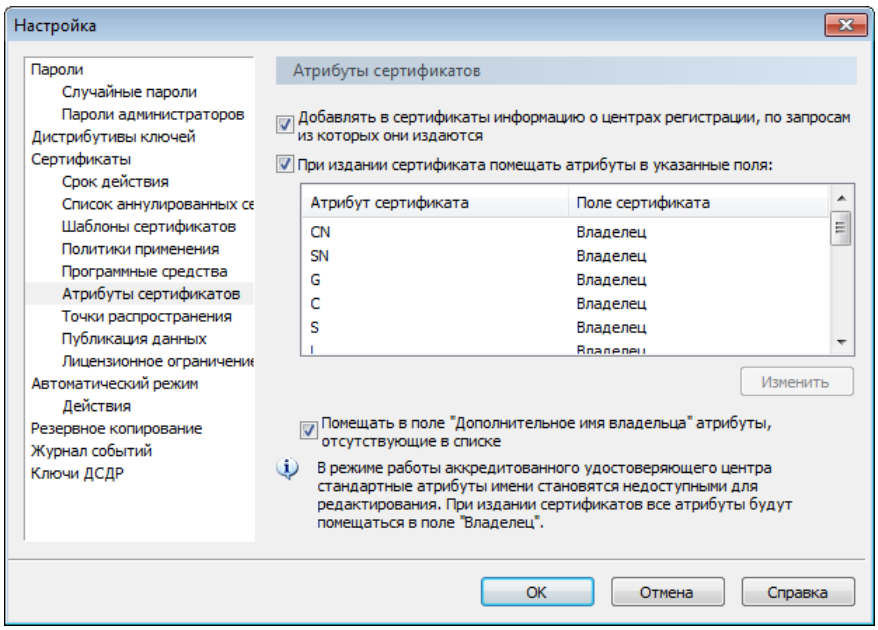

Рисунок 44. Распределение атрибутов сертификатов

3 В разделе **Атрибуты сертификатов** установите флажок **При издании сертификата помещать атрибуты в указанные поля** и для нужных атрибутов в списке с помощью кнопки **Изменить** укажите поле, в которое они должны помещаться при издании сертификатов.

Примечание. В списке представлены наиболее распространенные атрибуты сертификатов.

4 Если вы издаете сертификаты с атрибутами, которые не указаны в списке и которые по требованиям не должны попадать в поле «Владелец», установите флажок **Помещать в поле «Дополнительный атрибут имени» атрибуты, отсутствующие в списке.** При издании сертификатов такие атрибуты будут помещаться в поле «Дополнительный атрибут имени».

5 Для сохранения настроек нажмите кнопку **OK**.

Настройка оповещения об истечении срока действия сертификатов пользователей

Ключи подписи и сертификаты пользователей имеют ограниченный срок действия. В программе ViPNet Удостоверяющий и ключевой центр предусмотрена возможность оповещения об истечении срока действия изданных сертификатов пользователей своей сети. В зависимости от настроек программы оповещение может производиться как перед истечением срока действия, так и после него.

Чтобы настроить параметры оповещения об истечении срока действия сертификатов пользователей:

1 В окне программы в меню **Сервис** выберите пункт **Настройка**.

2 В появившемся окне на панели навигации выберите раздел **Сертификаты** > **Срок действия**.

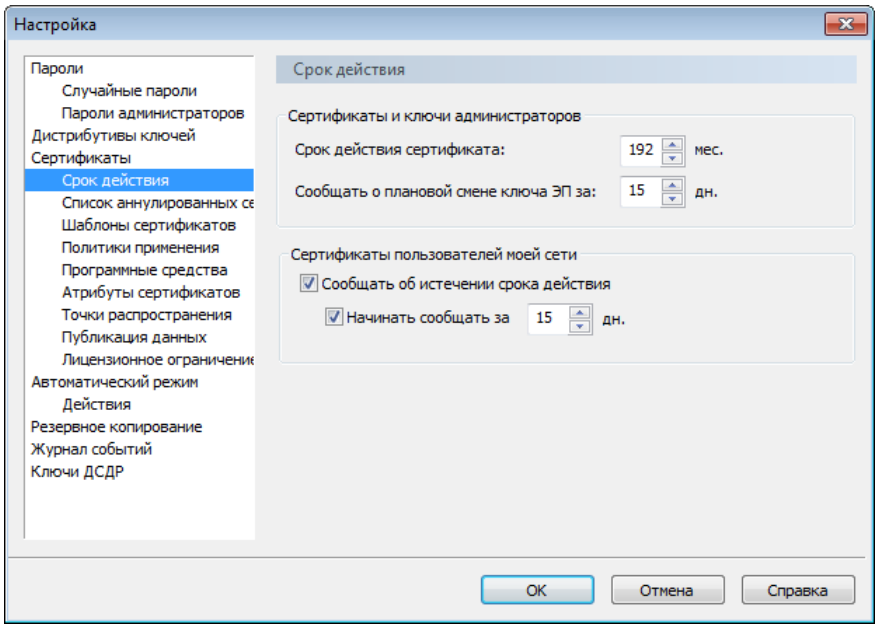

Рисунок 45. Настройка оповещения об окончании сроков действия изданных сертификатов пользователей своей сети

3 В разделе **Срок действия** в группе **Сертификаты пользователей моей сети** установите флажки **Сообщать об истечении срока действия** и **Начинать сообщать за** для предварительного оповещения об окончании срока действия изданных сертификатов пользователей своей сети.

В поле справа от флажка **Начинать сообщать за** введите количество дней до истечения срока действия (не более 30), когда следует производить оповещение.

Если будет установлен только флажок **Сообщать об истечении срока действия**, то оповещение будет производиться уже после окончания срока действия изданных сертификатов пользователей своей сети.

4 Для сохранения указанных настроек нажмите кнопку **OK**.

Издание квалифицированных сертификатов

Требования к изданию квалифицированных сертификатов

Если удостоверяющий центр, функции которого осуществляет программа ViPNet Удостоверяющий и ключевой центр, выступает в качестве аккредитованного (см. глоссарий, стр. 209), то все издаваемые сертификаты пользователей и сертификаты администраторов, которыми они заверяются, должны быть в формате, соответствующем требованиям приказа ФСБ от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи». Кроме того, чтобы издавать квалифицированные сертификаты, в качестве текущего сертификата администратора УКЦ (см. Выбор текущего сертификата администратора на стр. 153) должен быть выбран квалифицированный сертификат, полученный от удостоверяющего центра Минцифры России (см. Установление доверительных отношений с удостоверяющим центром Минцифры России на стр. 139).

Примечание. Издаваемые сертификаты в этом случае будут являться квалифицированными (см. глоссарий, стр. 211).

Для соответствия требованиям приказа № 795 в издаваемых сертификатах (в том числе, и в сертификатах администраторов) в обязательном порядке должны присутствовать:

- Дополнительные атрибуты имени владельца сертификата.

  Наборы атрибутов, которые должны содержаться в квалифицированных сертификатах, выдаваемых разным видам субъектов, приведены в разделе ниже (см. Дополнительные атрибуты имени в квалифицированных сертификатах разных видов субъектов на стр. 72).

- Расширения, содержащие:
  - Наименование средств удостоверяющего центра.
  - Наименование средства электронной подписи, используемого в удостоверяющем центре.
  - Номера сертификатов соответствия средств удостоверяющего центра и средств электронной подписи удостоверяющего центра требованиям контролирующих органов (требованиям, установленным в соответствии с Федеральным законом 06.04.2011 № 63-ФЗ «Об электронной подписи» (текст закона)).
  - Политики сертификата, в соответствии с которыми должен использоваться квалифицированный сертификат и которые описывают класс защищенности средств электронной подписи. Указываются в расширении «Политики сертификата» путем включения идентификаторов, описанных в таблице ниже:

Таблица 2. Идентификаторы политик классов защищенности

Класс защищенности	Идентификатор политики (OID)
Класс средств КС1	1.2.643.100.113.1
Класс средств КС2	1.2.643.100.113.1 1.2.643.100.113.2
Класс средств КС3	1.2.643.100.113.1 1.2.643.100.113.2 1.2.643.100.113.3
Класс средств КВ1	1.2.643.100.113.1 1.2.643.100.113.2 1.2.643.100.113.3 1.2.643.100.113.4
Класс средств КВ2	1.2.643.100.113.1 1.2.643.100.113.2 1.2.643.100.113.3 1.2.643.100.113.4 1.2.643.100.113.5
Класс средств КА1	1.2.643.100.113.1 1.2.643.100.113.2 1.2.643.100.113.3 1.2.643.100.113.4 1.2.643.100.113.5 1.2.643.100.113.6

Совет. Для средств электронной подписи, класс которых отличается от класса средств удостоверяющего центра, где они используются, следует указывать идентификаторы класса средств удостоверяющего центра.

При необходимости дополнительно можно указать информацию о средстве электронной подписи владельцев сертификатов (в сертификатах пользователей).

- Тип идентификации при выдаче сертификата:
  - **Личное присутствие**.
  - **Действующий сертификат**.
  - **Заграничный паспорт**.
  - **ЕСИА/ЕБС** (Единая система идентификации и аутентификации/Единая биометрическая система).

Дополнительные атрибуты имени владельца сертификата требуется добавлять вручную в каждый издаваемый сертификат, поэтому в процессе издания параметры сертификатов должны отображаться для редактирования. В большей степени это относится к сертификатам пользователей, поскольку их можно издавать без мастера редактирования полей сертификатов. Подробнее см. раздел Издание сертификатов (на стр. 43).

Остальные расширения из перечисленных в издаваемые сертификаты добавляются автоматически, в том случае, если в УКЦ заданы дополнительные настройки. Данные настройки вы можете задать либо при первичной инициализации (см. Установка и первичная инициализация программы ViPNet Удостоверяющий и ключевой центр на стр. 23), либо непосредственно при работе с программой (см. Настройка параметров издания квалифицированных сертификатов на стр. 74). Разница состоит в следующем:

- В первом случае изданный в процессе инициализации сертификат администратора УКЦ, а также сертификаты пользователей, изданные сразу после развертывания УКЦ, будут в формате квалифицированных (поскольку в них будут все необходимые расширения).
- Во втором случае имеющийся сертификат администратора и сертификаты пользователей придется переиздавать, чтобы они получили формат квалифицированных сертификатов.

Дополнительные атрибуты имени в квалифицированных сертификатах разных видов субъектов

Набор дополнительных атрибутов имени, которые должны присутствовать в квалифицированном сертификате, зависит от того, для какого субъекта издается данный сертификат. Наборы дополнительных атрибутов имени в сертификатах разных видов субъектов с указанием соответствующих расширений приведены в таблице ниже.

Таблица 3. Списки атрибутов имени в квалифицированных сертификатах разных видов субъектов

Атрибут имени владельца сертификата	Расширение сертификата
Сертификат для физического лица:	
Фамилия, имя, отчество владельца сертификата	Common Name
ИНН (индивидуальный номер налогоплательщика) владельца сертификата	INN
СНИЛС (страховой номер индивидуального лицевого счета) владельца сертификата	SNILS
Страна (RU)	Country
Фамилия владельца сертификата	Surname
Имя и отчество владельца сертификата	Given Name

Атрибут имени владельца сертификата	Расширение сертификата
Сертификат для субъекта, являющегося физическим лицом и представляющего юридическое лицо:	
Наименование организации, которую представляет владелец сертификата	Common Name
СНИЛС владельца сертификата (представителя организации)	SNILS
Фамилия владельца сертификата	Surname
Имя и отчество владельца сертификата	Given Name
Наименование организации, которую представляет владелец сертификата	Organization
Наименование подразделения организации, сотрудником которого является владелец сертификата	Organization Unit
Должность владельца сертификата	Title
ИНН (индивидуальный номер налогоплательщика) физического лица	INN
ИНН (индивидуальный номер налогоплательщика) организации — Российского юридического лица	INNLE
ОГРН (основной государственный регистрационный номер) организации — юридического лица	OGRN
Страна (RU)	Country
Субъект Российской Федерации, в котором зарегистрирована организация	State
Сертификат для Российского юридического лица:	
Наименование организации (юридического лица), которая является владельцем сертификата	Common Name
Наименование организации	Organization
ИНН (индивидуальный номер налогоплательщика) организации — Российского юридического лица	INNLE
ОГРН организации	OGRN
Страна (RU)	Country
Субъект Российской Федерации, в котором зарегистрирована организация	State
Сертификат для индивидуального предпринимателя:	
Фамилия, имя, отчество владельца сертификата	Common Name
Наименование предприятия индивидуального предпринимателя, которого представляет владелец сертификата	Organization
Фамилия владельца сертификата	Surname
Имя и отчество владельца сертификата	Given Name

Атрибут имени владельца сертификата	Расширение сертификата
ИНН индивидуального предпринимателя	INN
ОГРНИП (основной государственный регистрационный номер индивидуального предпринимателя)	OGRNIP
Страна (RU)	Country
Субъект Российской Федерации, в котором зарегистрирован индивидуальный предприниматель	State

Настройка параметров издания квалифицированных сертификатов

Расширения, содержащие сведения о средствах удостоверяющего центра, средстве его электронной подписи, их сертификатах соответствия, а также политиках применения, описывающих класс данных средств, по умолчанию добавляются в издаваемые сертификаты, если в программе ViPNet Удостоверяющий и ключевой центр заданы дополнительные настройки. Поэтому если данные настройки не были заданы в процессе первичной инициализации, то прежде чем начать издание сертификатов в формате квалифицированных, выполните следующие действия:

1 В окне программы в меню **Сервис** выберите пункт **Настройка**.

2 Выберите раздел **Сертификаты** > **Программные средства**.

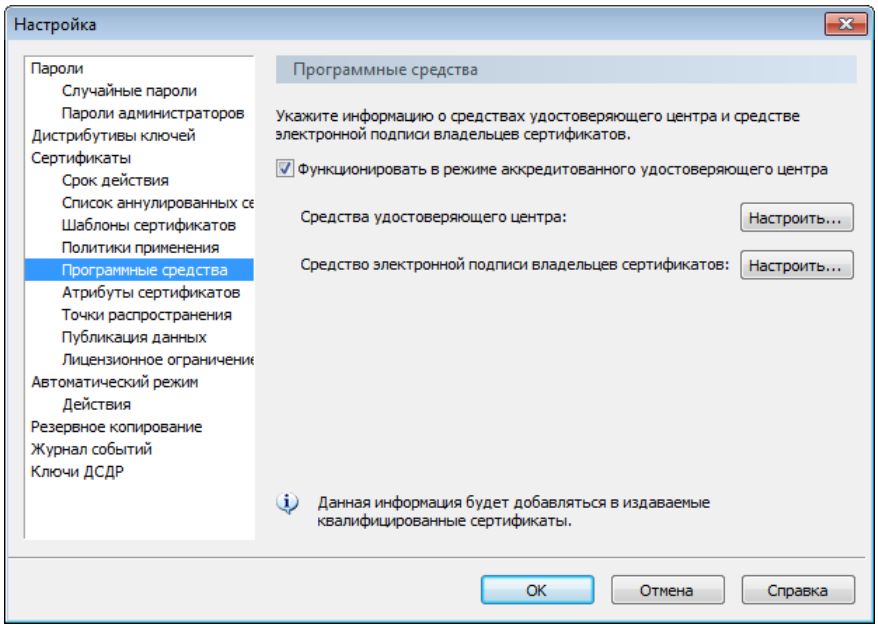

Рисунок 46. Настройка параметров работы УКЦ в режиме аккредитованного удостоверяющего центра

3 В разделе **Программные средства** установите флажок **Функционировать в режиме аккредитованного удостоверяющего центра**. Если флажок не будет установлен, дальнейшие настройки будут невозможны.

4 Укажите сведения о средствах вашего удостоверяющего центра. Для этого нажмите кнопку **Настроить** напротив названия **Средства удостоверяющего центра**, после чего в появившемся окне укажите следующую информацию:

- На вкладке **Программные средства** в соответствующих полях введите:
  - полное наименование криптографического средства, которое используется для создания электронной подписи издателя (администратора УКЦ);
  - полное наименование программного средства, которое используется для реализации функций удостоверяющего центра.

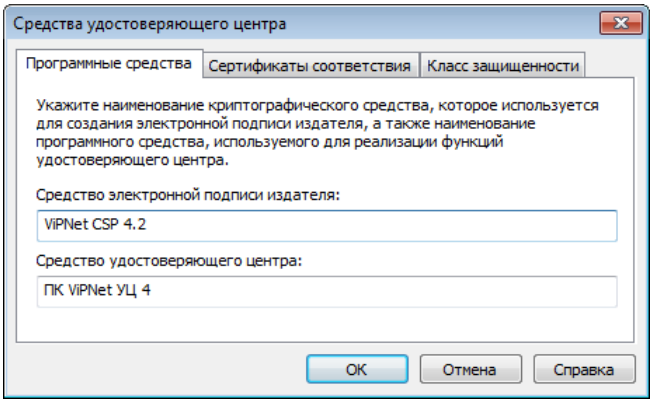

Рисунок 47. Указание сведений о средствах удостоверяющего центра

- На вкладке **Сертификаты соответствия** в нужных полях введите номера сертификатов соответствия средства электронной подписи и средства удостоверяющего центра требованиям Федерального закона № 63.

Примечание. Копии сертификатов соответствия предоставляются вашим поставщиком программного обеспечения.

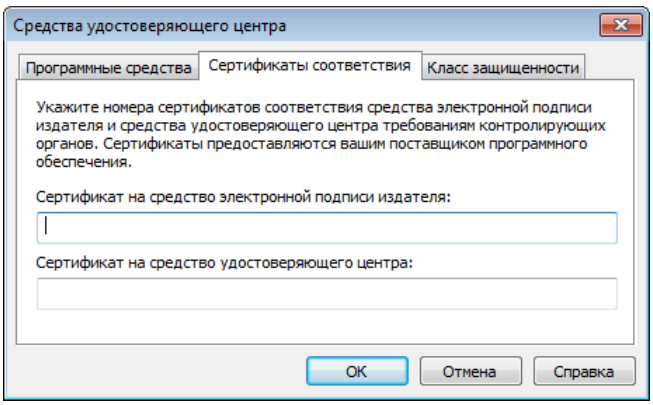

Рисунок 48. Указание сертификатов соответствия средств удостоверяющего центра требованиям Федерального закона

- На вкладке **Класс защищенности** выберите класс защищенности, которому соответствуют указанные программные средства. Согласно выбранному классу в издаваемые сертификаты будут добавляться расширения с нужными политиками применения.

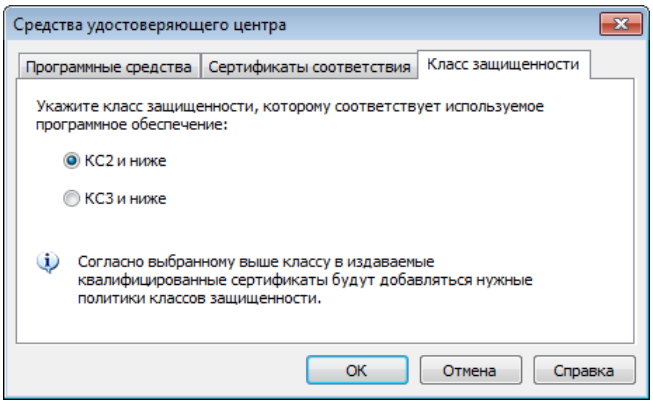

Рисунок 49. Указание класса защищенности средств удостоверяющего центра

Нажмите кнопку **OK**.

5 Если вы хотите, чтобы в издаваемые сертификаты добавлялась информация о криптографическом средстве, которое используется для создания электронной подписи их владельцев, то нажмите кнопку **Настроить** напротив названия **Средство электронной подписи владельцев сертификатов**, после чего в появившемся окне укажите наименование данного средства и нажмите кнопку **OK**.

Стоит учесть, что данная информация будет добавляться только в сертификаты, издаваемые для пользователей по запросам, в которых не содержится информация о средстве электронной подписи владельца. Если информация о средстве электронной подписи владельца содержится в запросе, то именно она помещается в издаваемый сертификат.

В сертификаты администраторов и сертификаты пользователей, издаваемые по инициативе администратора УКЦ, в качестве наименования средства создания электронной подписи владельца всегда добавляется наименование средства создания электронной подписи издателя. Для вашего сведения оно отображается в нередактируемом поле.

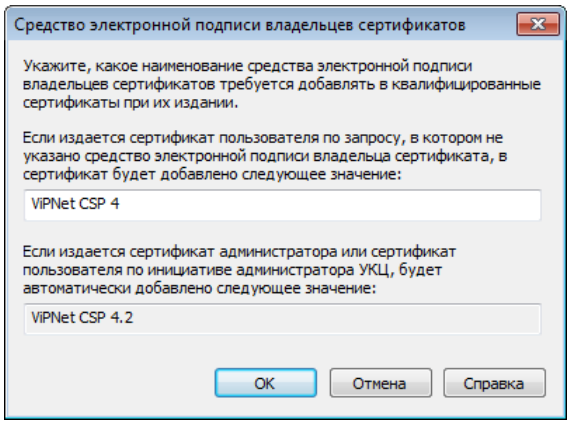

Рисунок 50. Указание сведений о средстве создания электронной подписи владельца сертификата ключа проверки электронной подписи

6 Для сохранения настроек нажмите кнопку **OK**.

В результате во все издаваемые сертификаты будут добавляться расширения, содержащие указанные выше сведения.

Аннулирование сертификатов

В некоторых случаях может возникнуть необходимость аннулирования сертификата пользователя, например:

- Компрометация ключей пользователя (см. Действия в случае компрометации ключа электронной подписи пользователя на стр. 42).
- Смена места работы владельца сертификата.
- Издание нового сертификата с другими параметрами вместо действующего сертификата.

Аннулирование сертификата пользователя может происходить:

- По запросу из центра регистрации (на стр. 78).
- По инициативе администратора УКЦ (на стр. 79).

Иногда также может возникнуть необходимость аннулирования кросс-сертификатов, изданных при установлении доверительных отношений (см. Установление доверительных отношений с другими удостоверяющими центрами на стр. 117).

Аннулированный сертификат попадает в ваш список аннулированных сертификатов (CRL), который находится в разделе **Изданные сертификаты** > **Списки аннулированных сертификатов** представления **Администрирование**.

После каждой операции аннулирования сертификата вам требуется рассылать обновленный CRL на узлы вашей сети. Подробнее о способах передачи CRL см. в разделе Работа со списками аннулированных сертификатов (на стр. 94).

По запросу из центра регистрации

Администратор центра регистрации может инициировать аннулирование сертификатов, выдача которых производилась через центр регистрации. Для этого он формирует соответствующие запросы в программе ViPNet Registration Point и передает их в ViPNet Удостоверяющий и ключевой центр (см. раздел Взаимодействие с программой ViPNet Registration Point (на стр. 19)).

Запросы на аннулирование сертификатов пользователей при поступлении в УКЦ помещаются в раздел **Запросы на аннулирование сертификатов** > **Необработанные запросы** представления **Удостоверяющий центр**. Все поступившие запросы требуется обработать: удовлетворить либо отклонить. Запросы могут обрабатываться в автоматическом режиме (см. Работа в автоматическом режиме на стр. 36) или вручную. При автоматической обработке запросы могут быть только удовлетворены. Отклонить запрос можно только при обработке вручную.

Для обработки запросов в автоматическом режиме должны быть выполнены соответствующие настройки (см. Настройка автоматического режима на стр. 39). Чтобы обработать запросы вручную:

1 В окне программы на панели навигации выберите представление **Удостоверяющий центр** и перейдите в раздел **Запросы на аннулирование сертификатов** > **Необработанные запросы**.

2 На панели просмотра выберите один или несколько запросов и на панели инструментов нажмите кнопку **Удовлетворить** или кнопку **Отклонить**.

3 В появившемся окне с сообщением подтвердите операцию, которая будет выполнена.

В результате удовлетворения запроса статус сертификата будет изменен, запрос будет перемещен в раздел **Запросы на аннулирование сертификатов** > **Удовлетворенные запросы**. При аннулировании сертификат попадет в ваш список аннулированных сертификатов (CRL), который вы можете найти в разделе **Изданные сертификаты** > **Списки аннулированных сертификатов** представления **Администрирование**. Для аннулированного сертификата будет указана причина аннулирования, содержащаяся в запросе. Измененный CRL передайте на узлы вашей сети (см. Распространение списков аннулированных сертификатов на стр. 99).

В результате отказа в обработке запроса администратору центра регистрации будет отправлен файл запроса в неизменном виде. Такой запрос будет перемещен в раздел **Запросы на аннулирование сертификатов** > **Отклоненные запросы**.

По инициативе администратора УКЦ

Чтобы аннулировать сертификата:

1 В окне программы на панели навигации выберите:

- Представление **Удостоверяющий центр** и перейдите в раздел:
  - **Изданные сертификаты** > **Пользователи моей сети** для работы с сертификатами пользователей сети ViPNet.
  - **Изданные сертификаты** > **Пользователи, удаленные из моей сети** для работы с сертификатами пользователей, которые были удалены из сети ViPNet.
  - **Изданные сертификаты** > **Внешние пользователи** для работы с сертификатами внешних пользователей.
- Представление **Администрирование** и перейдите в раздел **Кросс-сертификация** > **Сертификаты для других УЦ** для работы с изданными кросс-сертификатами администраторов других удостоверяющих центров.

2 На панели просмотра щелкните правой кнопкой мыши по нужному сертификату и в контекстном меню выберите **Аннулировать** для аннулирования сертификата пользователя или кросс-сертификата.

3 В случае аннулирования сертификата в появившемся окне **Аннулирование сертификата** выполните следующие действия:

3.1 В списке укажите одну из причин аннулирования:

- **Прекращение действия** — если сертификат пользователя не предполагает дальнейшего использования.

- **Компрометация ключа** — если произошла компрометация ключей пользователя (например, вследствие утери им контейнера ключей).
- **Изменение принадлежности** — при изменении удостоверяющего центра.
- **Сертификат заменен** — если данные, указанные в сертификате пользователя, стали неактуальными.

3.2 Нажмите кнопку **Аннулировать**.

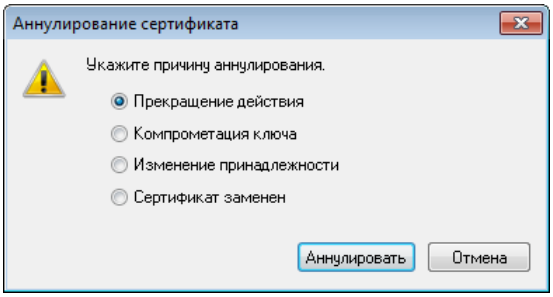

Рисунок 51. Аннулирование сертификата

4 После аннулирования сертификата в колонке **Статус** для данного сертификата появится соответствующее значение. В окне **Сертификат** на вкладке **Общие** (см. Просмотр сертификатов на стр. 84) также появится соответствующая информация.

Чтобы аннулировать сертификаты, изданные для конкретного пользователя:

1 В окне программы на панели навигации выберите представление **Ключевой центр**.

2 Перейдите в раздел **Моя сеть** > **Пользователи.**

3 На панели просмотра дважды щелкните кнопкой мыши нужного пользователя.

4 В появившемся окне **Свойства пользователя** перейдите на вкладку **Сертификаты**.

5 В списке **Изданные сертификаты** выберите сертификат и нажмите кнопку **Аннулировать**.

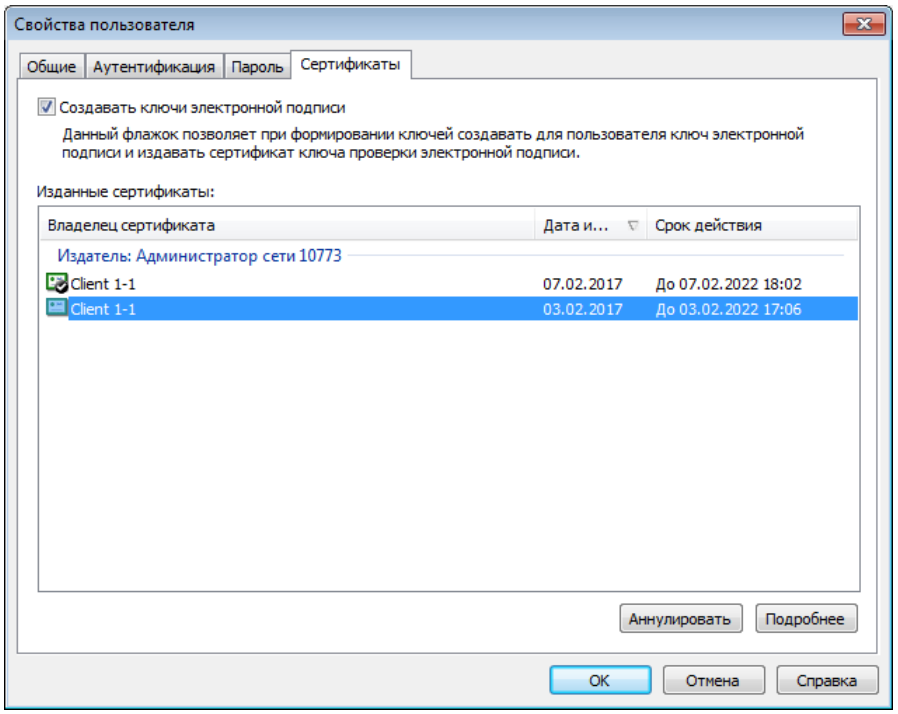

Рисунок 52. Аннулирование сертификата пользователя в окне Свойства пользователя

6 В появившемся окне **Аннулирование сертификата** выберите причину аннулирования и нажмите кнопку **Аннулировать**.

Просмотр запросов и сертификатов

Просмотр запроса на сертификат

Прежде чем обработать запрос на издание сертификата, вы можете просмотреть его параметры.

При необходимости также можно просмотреть параметры уже обработанных запросов.

Примечание. Просмотреть параметры запросов, поступающих от пользователей сети ViPNet или из центров регистрации, можно в том случае, если они не были обработаны в автоматическом режиме (см. Работа в автоматическом режиме на стр. 36).

Чтобы посмотреть подробную информацию о запросе на сертификат (см. глоссарий, стр. 211) от пользователя сети ViPNet или из центра регистрации:

1. В окне программы на панели навигации перейдите в представление **Удостоверяющий центр** и выберите раздел, соответствующий состоянию запроса (необработанный, удовлетворенный или отклоненный).
2. Дважды щелкните нужный запрос либо в контекстном меню запроса выберите пункт **Открыть запрос**.

Посмотреть подробную информацию о запросе на сертификат от внешнего пользователя можно при его обработке в окне **Издание сертификатов пользователей** с помощью кнопки **Свойства**.

В зависимости от того, в каком приложении ViPNet был сформирован запрос на сертификат, внешний вид окна просмотра параметров запроса будет выглядеть по-разному. В окне просмотра параметров запроса от пользователя сети ViPNet или из центра регистрации содержится ряд вкладок, на которых отображается следующая информация:

- **Общие** — основная информация о запросе: номер запроса; имя администратора, подписавшего запрос; имя владельца ключа проверки электронной подписи; желательный срок действия сертификата; статус запроса и электронной подписи.
- **Владелец ключа** — сведения о пользователе ViPNet, для которого создан запрос на сертификат.
- **Срок действия** — срок действия сертификата, заявленный в запросе.
- **Ключ проверки электронной подписи** — параметры ключа проверки электронной подписи.
- **Состав** — список расширений, определяющих назначение сертификата.
- **Информация о запросе** — дополнительные сведения о владельце ключа проверки электронной подписи.

- **Статус** — текущий статус запроса и история запроса (дата и время создания, отправки, доставки и других статусов запроса).
- **Электронная подпись** — информация об электронной подписи, заверившей запрос, и контрольной сумме запроса. На вкладке также с помощью кнопки **Просмотр сертификата** можно просмотреть сведения о сертификате, которым был подписан запрос.

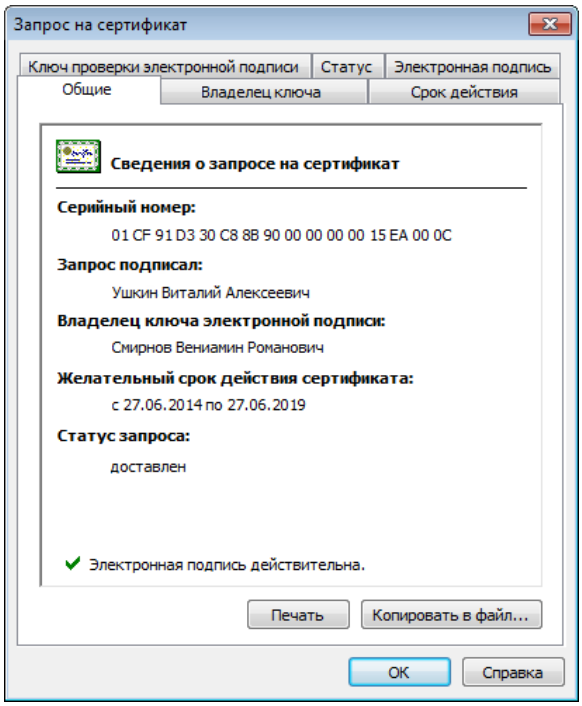

Рисунок 53. Просмотр общей информации о запросе

В окне просмотра параметров запроса на сертификат от внешнего пользователя вся информация о содержимом запроса представлена рядом расширений на вкладке **Состав запроса**. К данной информации относится:

- сведения о пользователе, для которого создан запрос на сертификат;
- параметры ключа проверки электронной подписи — алгоритм, который использовался при создании этого ключа;
- список назначений и политик применения, которые должны быть включены в сертификат.

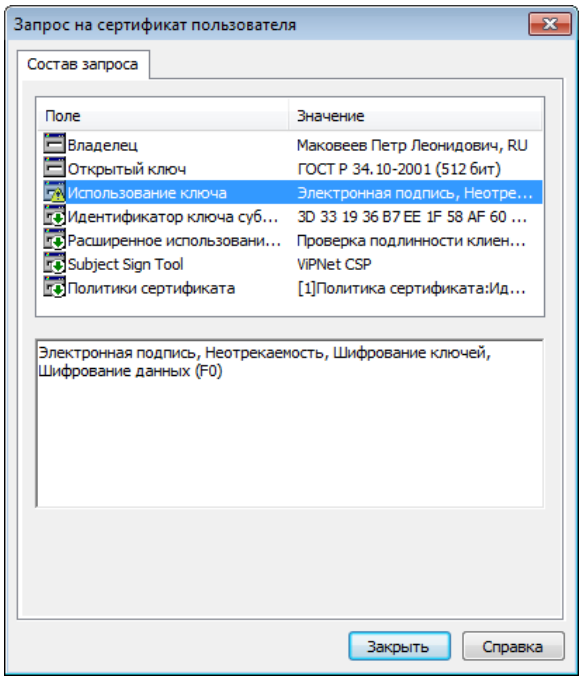

Рисунок 54. Просмотр информации о запросе на сертификат от внешнего пользователя

Просмотр сертификатов

Все сертификаты, изданные в программе ViPNet Удостоверяющий и ключевой центр, — сертификаты пользователей, администраторов, кросс-сертификаты, а также сертификаты, импортированные из сторонних удостоверяющих центров или доверенных сетей, вы можете просмотреть (в том числе аннулированные).

Просмотр сертификата может понадобиться для получения информации о его назначении, издателе, составе полей, причине недействительности сертификата и так далее.

Чтобы просмотреть сведения, содержащиеся в сертификате:

1. Перейдите в представление **Удостоверяющий центр** для просмотра сертификата пользователя или в представление **Администрирование** для просмотра сертификата другого типа.
2. Выберите раздел, соответствующий типу сертификата.
3. Дважды щелкните нужный сертификат или в контекстном меню выберите пункт **Открыть.**

Примечание. Сертификаты пользователей сети ViPNet также можно просмотреть на вкладке **Сертификаты** в окне **Свойства пользователя**, сертификаты администраторов УКЦ — на вкладке **Сертификаты** в окне **Свойства администратора**.

В появившемся окне **Сертификат** сведения представлены на нескольких вкладках.

На вкладке **Общие** содержится основная информация о выбранном сертификате:

- назначение сертификата или (для недействительных сертификатов) причина недействительности сертификата;
- имя владельца ключа проверки электронной подписи, которому выдан сертификат;
- имя издателя сертификата;
- срок действия сертификата;
- срок действия ключа электронной подписи, соответствующего данному сертификату (только для сертификатов пользователей);
- информация о политиках применения сертификата, отображаемая при нажатии кнопки **Заявление издателя**.

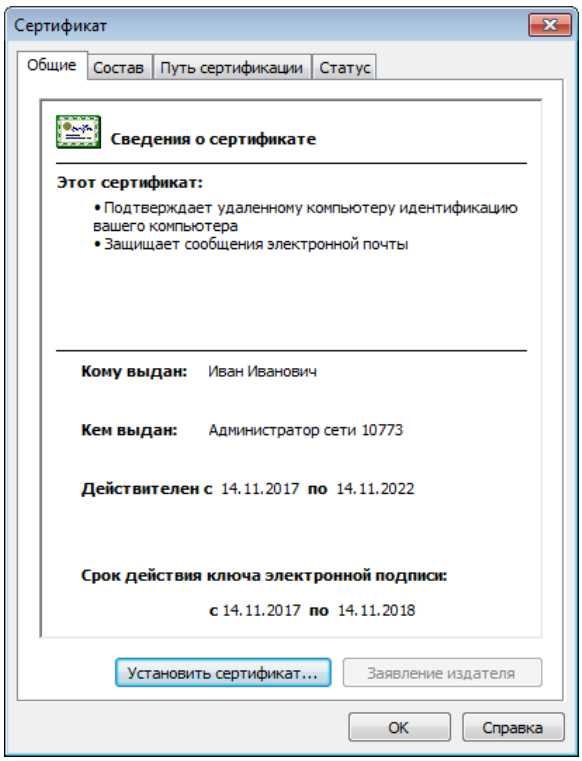

Рисунок 55. Просмотр сведений о сертификате

Вкладка **Состав** включает в себя список всех полей сертификата. Чтобы просмотреть содержимое интересующего поля, выберите его в списке. Для удобства вы можете ограничить количество просматриваемых полей, выбрав нужную группу полей в выпадающем списке **Показать**:

- **Только поля V1** — все поля, кроме расширений;
- **Только расширения** — дополнительные поля сертификата, соответствующего стандарту X.509 версии 3;

Примечание. Расширение **Срок действия ключа электронной подписи** отображается в том случае, если срок действия сертификата превышает 12 месяцев (1 год). Срок действия ключа электронной подписи в этом случае не может превышать 15 месяцев (1 год и 3 месяца).

- **Только критические расширения** — только те расширения, которые признаны издателем критическими;
- **Только свойства** — параметры, которые не являются полями сертификата, но присваиваются сертификату при хранении его в системном хранилище компьютера.

Кроме этого вы можете экспортировать сертификат в файл различных форматов с помощью кнопки **Копировать в файл** (см. раздел Экспорт сертификатов (на стр. 88)) или отправить его на принтер, нажав кнопку **Печать**. Сертификат будет распечатан (см. Печать сертификатов на стр. 92).

На вкладке **Путь сертификации** отображаются сертификаты, образующие иерархию издателей выбранного сертификата, — цепочка сертификации, а также информация об их статусе. При необходимости вы можете просмотреть более подробную информацию о каждом сертификате издателя из цепочки с помощью кнопки **Просмотр сертификата**.

На вкладке **Статус** содержатся сведения о текущем статусе сертификата, а также список операций, которые производились с сертификатом с момента его издания. Данная вкладка присутствует только в окне просмотра сертификатов пользователей, поскольку учет производимых операций ведется только для этих сертификатов.

Просмотр истории сертификатов

Операции, которые производятся с сертификатами пользователей в программе с момента их издания, фиксируются в истории сертификатов. Историю каждого изданного сертификата пользователя при необходимости впоследствии вы можете просмотреть.

Чтобы просмотреть историю сертификата внешнего пользователя или пользователя сети ViPNet:

1. В окне программы на панели навигации перейдите в представление **Удостоверяющий центр** и в разделе **Изданные сертификаты** выберите нужный подраздел.
2. На панели просмотра дважды щелкните сертификат или в контекстном меню сертификата выберите пункт **Открыть.**
3. В окне просмотра сертификата перейдите на вкладку **Статус** и ознакомьтесь с операциями, которые производились с сертификатом, а также датами их проведения.

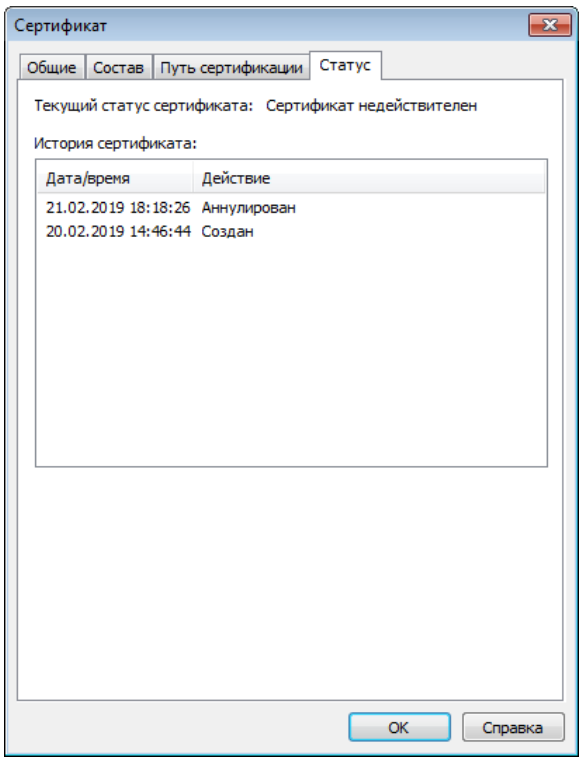

Рисунок 56. Просмотр истории сертификата

Экспорт сертификатов

Изданные сертификаты пользователей ViPNet, кросс-сертификаты, а также сертификаты администраторов вы можете экспортировать в различные форматы. Экспорт сертификатов может потребоваться в разных случаях, например, при архивировании сертификатов либо при выдаче сертификатов непосредственно внешним пользователям (без участия центра регистрации).

Примечание. Подробнее об экспорте кросс-сертификатов см. раздел Экспорт кросс-сертификата (на стр. 136).

Чтобы экспортировать сертификат:

1. В окне программы на панели навигации перейдите в представление **Удостоверяющий центр** для экспорта сертификата пользователя или в представление **Администрирование** для экспорта сертификата другого типа.
2. Выберите раздел, соответствующий типу сертификата.
3. На панели просмотра выберите в списке нужный сертификат.
4. Выполните одно из действий:
   - Щелкните сертификат правой кнопкой мыши и в контекстном меню выберите пункт **Экспорт**.
   - Дважды щелкните сертификат и в окне **Сертификат** на вкладке **Состав** нажмите кнопку **Копировать в файл**.

   Будет запущен мастер экспорта сертификатов.
5. На начальной странице мастера экспорта сертификатов нажмите кнопку **Далее**.

Совет. Если при последующих запусках мастера желательно пропускать первую страницу, установите на ней флажок **Не отображать в дальнейшем эту страницу**.

---

6. На странице **Формат экспортируемого файла** выберите один из предлагаемых форматов (см. Форматы экспорта сертификатов на стр. 89), после чего нажмите кнопку **Далее**.

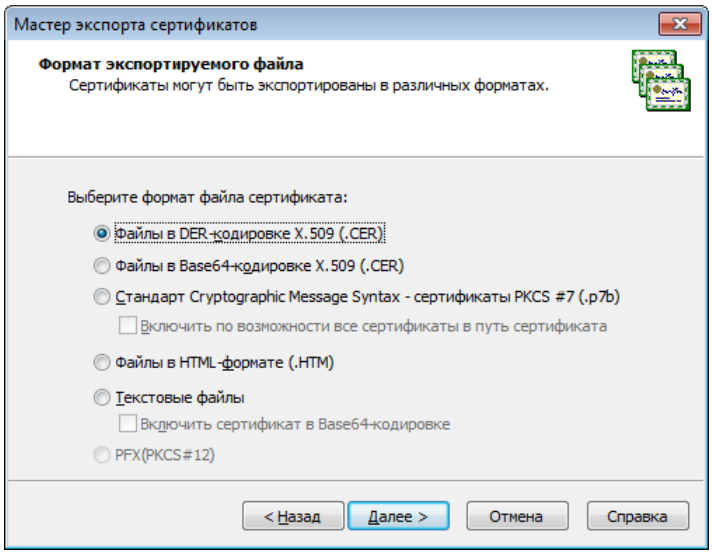

Рисунок 57. Выбор формата файла

7 На странице **Имя файла экспорта** укажите полный путь к создаваемому файлу, после чего нажмите кнопку **Далее**.

8 На странице **Завершение работы мастера экспорта сертификатов** убедитесь в правильности параметров экспорта, заданных на предыдущих страницах мастера, после чего нажмите кнопку **Готово**.

9 В окне с сообщением об успешном экспорте нажмите кнопку **ОК**.

В результате экспорта сертификат будет сохранен в файле заданного формата по указанному пути.

Форматы экспорта сертификатов

При выборе формата экспорта сертификата следует руководствоваться перечисленными положениями.

- При экспорте сертификатов для импорта на компьютер с ОС Windows предпочтительный формат экспорта — PKCS #7, поскольку этот формат обеспечивает сохранение цепочки центров сертификации (пути сертификации). 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 приведена подробная информация о каждом из форматов экспорта сертификатов, поддерживаемых 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 веб-сайте RSA Laboratories.

- **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).

- **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, что обеспечивает целостность информации при ее передаче по сети. 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, спецификация RFC 1341 и последующие) 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).

- **Файлы в HTML-формате**

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

- **Текстовые файлы**

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

- **Файлы в формате PFX (PKCS #12)**

  Формат PFX (PKCS#12) поддерживает безопасное хранение сертификата и закрытого ключа, соответствующего сертификату пользователя, может содержать все сертификаты в цепочке доверия от сертификата пользователя до корневого сертификата удостоверяющего центра и CRL.

Проверка сертификатов

В процессе электронного взаимодействия у пользователей могут возникать вопросы, можно ли доверять тем или иным сертификатам (как правило, изданным в сторонних удостоверяющих центрах). В этом случае они вправе обратиться в свой удостоверяющий центр для проверки таких сертификатов.

В программе ViPNet Удостоверяющий и ключевой центр может быть выполнена процедура проверки сертификата ключа проверки электронной подписи по запросу пользователя. Для проведения процедуры проверки сертификата пользователь должен обратиться с заявлением в письменном либо электронном виде. Заявление в электронном виде должно быть подписано действующим сертификатом пользователя. Вместе с заявлением должен быть предоставлен файл сертификата подписи `*.cer`, который требуется проверить.

Чтобы проверить полученный сертификат пользователя:

1. В окне программы в меню **Сервис** выберите пункт **Открыть сертификат из файла**.
2. В появившемся окне выберите файл сертификата, который был вам предоставлен пользователем, и нажмите кнопку **Открыть**.
3. В появившемся окне **Сертификат** ознакомьтесь с информацией, которая содержится в проверяемом сертификате. Если на вкладке **Общие** указано, что срок действия сертификата или ключа электронной подписи истек, то сертификат является недействительным и ему не следует доверять. Если указано, что недостаточно информации для проверки сертификата, то в этом случае ему также не следует доверять. Если никакой из перечисленной информации в сертификате не содержится и на вкладке **Путь сертификации** окна **Сертификат** указано, что сертификат действителен, то сертификату можно доверять.
4. Сообщите пользователю о результатах проверки сертификата.

Печать сертификатов

Сертификаты, используемые либо изданные в программе ViPNet Удостоверяющий и ключевой центр, вы можете распечатать. Для вывода на печать любого сертификата в окне просмотра данного сертификата на вкладке **Состав** нажмите кнопку **Печать** (см. Просмотр сертификатов на стр. 84). Если вам требуется распечатать сразу несколько сертификатов пользователей, то укажите нужные сертификаты и в их контекстном меню выберите пункт **Печать**.

В результате сертификаты будут отправлены на принтер, используемый по умолчанию на вашем компьютере. Они будут распечатаны в соответствии с форматом, заданным в специальных шаблонах. Подробнее о том, как задать формат в шаблонах, см. документ «Печать сертификатов. Приложение к документации ViPNet» из комплекта поставки (см. Комплект поставки на стр. 14).

Настройка количества сертификатов, отображаемых в окне программы

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

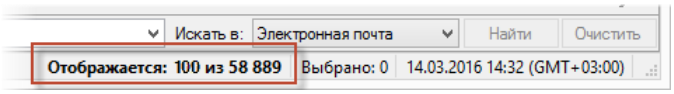

Рисунок 58: Количество сертификатов, отображаемых в программе по умолчанию

Чтобы в списках сертификатов этих разделов отображалось большее количество сертификатов:

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

   Например:

   ```
   [Certification]
   Certificates cache capacity=200
   ```

Примечание. Стоит учитывать, что при увеличении количества сертификатов будет снижаться скорость отображения списка сертификатов в программе.

5

Работа со списками аннулированных сертификатов

Общие сведения о списках аннулированных сертификатов

В списках аннулированных сертификатов (см. глоссарий, стр. 217) содержится информация о том, какие сертификаты пользователей были аннулированы. Эта информация используется для проверки действительности сертификата.

Примечание. В CRL содержится информация только о сертификатах, срок действия которых не истек. Подробнее см. RFC 5280, раздел 5.

Списки аннулированных сертификатов создаются в процессе издания корневых сертификатов (см. Издание сертификата администратора на стр. 147) либо в процессе импорта сертификатов администраторов, изданных вышестоящим удостоверяющим центром при установлении доверительных отношений (см. Импорт сертификата, выданного вышестоящим удостоверяющим центром на стр. 127). Они отображаются в разделах представления **Администрирование**: в первом случае — в разделе **Изданные сертификаты** > **Списки аннулированных сертификатов**, во втором — в разделе **Кросс-сертификация** > **Списки аннулированных сертификатов**.

Списки аннулированных сертификатов, импортированные из доверенных сетей ViPNet или других удостоверяющих центров, содержатся в разделе **Импортированные сертификаты** > **Списки аннулированных сертификатов** представления **Администрирование**.

Обновление списков аннулированных сертификатов

Списки аннулированных сертификатов (CRL) имеют ограниченный срок действия и должны регулярно обновляться. При наличии CRL с истекшим сроком действия будет запрещено издание сертификатов (на стр. 43).

Обновление CRL может производиться несколькими способами:

- В автоматическом режиме по расписанию (см. Настройка автоматического обновления CRL на стр. 96). В данном случае обновляются сразу все CRL, которые соответствуют действительному ключу электронной подписи администратора, при работе программы в автоматическом режиме.
- Вручную по команде администратора (см. Обновление CRL вручную на стр. 97). В ручном режиме могут быть обновлены все CRL либо только выбранные CRL.

Кроме того, автоматическое обновление CRL выполняется при аннулировании сертификатов пользователей (см. Аннулирование сертификатов на стр. 78).

CRL после обновления действуют в течение срока, который задан в настройках программы. Поэтому перед обновлением CRL любым из указанных способов убедитесь, что в настройках задан нужный срок (см. Настройка срока действия CRL на стр. 98).

CRL, срок действия которых истек, автоматически удаляются во время проверки текущих данных (см. Проверка текущих данных на стр. 175) и перед созданием резервной копии по расписанию (см. Настройка параметров создания резервных копий на стр. 167). Также CRL удаляются при их обновлении, если срок действия ключа электронной подписи истек.

Настройка автоматического обновления CRL

Списки аннулированных сертификатов (CRL) могут обновляться в автоматическом режиме работы программы (см. Работа в автоматическом режиме на стр. 36) со следующей периодичностью:

- Раз в несколько минут, часов, дней или месяцев.
- Каждый день в конкретное время.

Поэтому, если вы выбрали операцию обновления CRL для выполнения в автоматическом режиме работы программы (см. Настройка автоматического режима на стр. 39), в окне **Параметры действия в автоматическом режиме** укажите периодичность обновления CRL, установив переключатель в нужное положение.

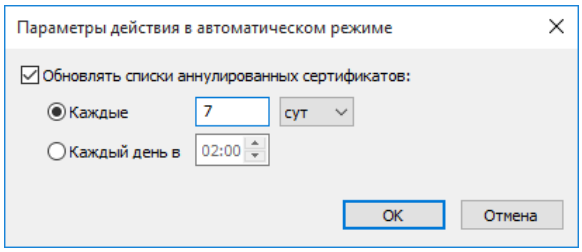

Рисунок 59. Настройка автоматического обновления CRL

В случае наличия межсетевого взаимодействия с другими сетями ViPNet при обновлении CRL в автоматическом режиме список аннулированных сертификатов сразу передается в доверенные сети вместе с корневым сертификатом администратора (сертификатом издателя).

При наличии доверительных отношений со сторонними удостоверяющими центрами обновите CRL вручную (см. Обновление CRL вручную на стр. 97), выполните экспорт обновленного CRL в файл (см. Экспорт одного CRL в файл на стр. 106), после чего передайте файл с CRL в данные удостоверяющие центры.

Обновление CRL вручную

Обновление списков аннулированных сертификатов (CRL) в программе ViPNet Удостоверяющий и ключевой центр вы можете производить вручную. Как правило, это может потребоваться при необходимости срочного обновления CRL, чтобы не переходить в автоматический режим работы и не ожидать обновления CRL по расписанию (см. Настройка автоматического обновления CRL на стр. 96).

Чтобы обновить CRL:

1. В окне программы на панели навигации перейдите в представление **Администрирование**.
2. Выберите раздел **Изданные сертификаты** > **Списки аннулированных сертификатов** (или **Кросс-сертификация** > **Сертификаты от вышестоящего УЦ** > **Списки аннулированных сертификатов**).
3. На панели просмотра выберите CRL и нажмите кнопку **Обновить**.

   В результате выбранный CRL будет обновлен и будет действовать в течение срока, указанного в настройках программы (см. Настройка срока действия CRL на стр. 98).
4. Распространите обновленный CRL любым возможным способом (см. Распространение списков аннулированных сертификатов на стр. 99).
5. При наличии межсетевого взаимодействия с другими сетями ViPNet выполните экспорт служебных данных (см. Экспорт межсетевой информации на стр. 42) для передачи обновленного CRL в доверенные сети.
6. При наличии доверительных отношений со сторонними удостоверяющими центрами выполните экспорт обновленного CRL в файл (см. Экспорт одного CRL в файл на стр. 106), после чего передайте файл с CRL в данные удостоверяющие центры.

Настройка срока действия CRL

Списки аннулированных сертификатов (CRL) после обновления действуют в течение срока, указанного в настройках программы. Поэтому для обновления CRL в настройках задайте нужный срок в соответствии с регламентом работы вашей организации. Кроме этого, в настройках УКЦ вы также можете изменить количество дней или часов, за которое должно производиться оповещение об истечении срока действия CRL.

Чтобы настроить данные параметры:

1 В окне программы в меню **Сервис** выберите пункт **Настройка**.

2 В окне **Настройка** на панели навигации выберите раздел **Сертификаты** > **Список аннулированных сертификатов**.

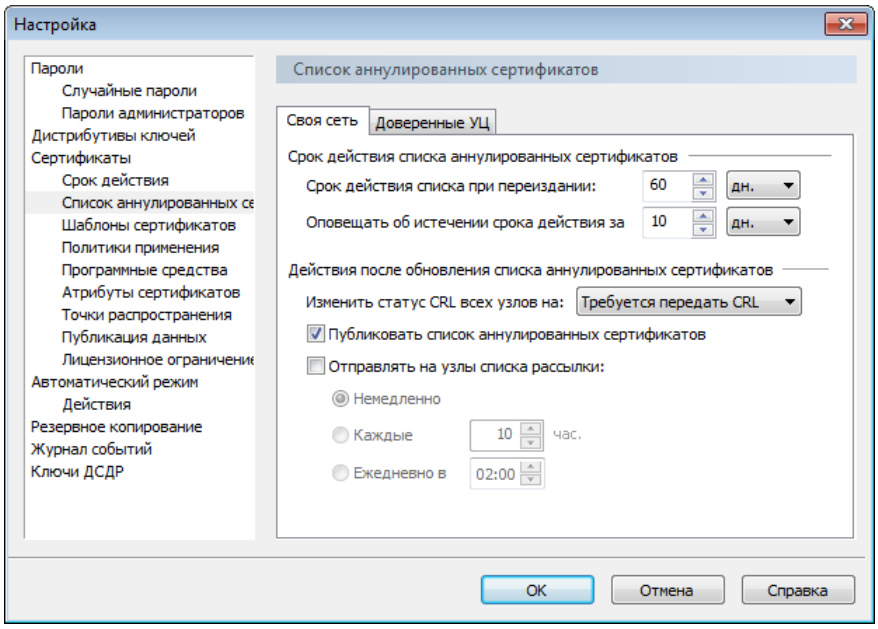

Рисунок 60. Настройка срока действия списков аннулированных сертификатов

3 На вкладке **Своя сеть** в группе **Срок действия списка аннулированных сертификатов**:

- Задайте срок действия CRL. Для этого в списке рядом с полем **Срок действия списка при переиздании** выберите единицу измерения (дни или часы), затем в самом поле введите срок, в течение которого CRL будет действителен после своего обновления. По умолчанию установлено 60 дней.
- Задайте время оповещения об истечении срока действия CRL. Для этого в списке рядом с полем **Сообщать об истечении срока действия за** выберите единицу измерения (дни или часы), затем в самом поле укажите количество дней или часов, за которое должно выдаваться предупреждение об истечении срока действия CRL с рекомендацией его обновить. По умолчанию установлено 10 дней.

4 Для сохранения указанных настроек нажмите кнопку **OK**.

Распространение списков аннулированных сертификатов

На узлах пользователей сети ViPNet, которые работают с электронной подписью, должны присутствовать актуальные списки аннулированных сертификатов (CRL). Поэтому в перечисленных ниже случаях CRL следует своевременно передавать на все узлы сети:

- Обновление CRL вашей сети, если истек срок его действия либо был аннулирован сертификат пользователя в сети (см. Обновление списков аннулированных сертификатов на стр. 96).
- Издание нового корневого сертификата администратора (сертификата издателя) (см. Издание сертификата администратора на стр. 147).

Примечание. После издания корневого сертификата на сетевые узлы автоматически передается комплект CRL, в составе которого присутствует новый сертификат издателя и CRL для него.

- Получение сертификата администратора (сертификата издателя) в вышестоящем удостоверяющем центре (см. Импорт сертификата, выданного вышестоящим удостоверяющим центром на стр. 127), издание кросс-сертификата (см. Издание кросс-сертификата по запросу на стр. 133).
- Получение сертификатов администраторов либо CRL из доверенной сети ViPNet или сторонних удостоверяющих центров.

Распространять CRL вы можете несколькими способами:

- Через список рассылки (см. Передача CRL через список рассылки на стр. 100). Этим способом распространяется обновленный CRL, соответствующий текущему сертификату издателя. Распространяется данный CRL только на узлы, заданные в списке рассылки. Может передаваться автоматически.
- В автоматическом режиме УКЦ (см. Настройка автоматической передачи CRL на стр. 101). Этим способом распространяются все CRL, которые присутствуют в программе, включая CRL из доверенных сетей ViPNet или других удостоверяющих центров.
- Вручную по команде администратора (см. руководство администратора на УКЦ). Этим способом распространяются все CRL, которые присутствуют в программе, включая CRL из доверенных сетей ViPNet или других удостоверяющих центров.
- Путем публикации в хранилищах данных (см. Публикация сертификатов и списков аннулированных сертификатов на стр. 108). Данный способ, как правило, используется, когда в сети организации развернута PKI-инфраструктура и передача данных по сети (в том числе CRL) не производится.

Передача CRL через список рассылки

Если в вашей сети есть узлы, на которых требуется гарантированное оперативное получение CRL (например, на узлах центров регистрации), организуйте распространение CRL через список рассылки. Для этого выполните следующие действия:

1 Сформируйте список рассылки CRL (список получателей CRL).

2 Настройте параметры передачи CRL на узлы списка рассылки.

Внимание! Через список рассылки может распространяться только текущий CRL после обновления (см. Обновление списков аннулированных сертификатов на стр. 96).

Чтобы сформировать список получателей CRL:

1 В окне программы в представлении **Администрирование** выберите раздел **Моя сеть** > **Получатели списков аннулированных сертификатов**.

2 Для добавления узла в перечень получателей CRL:

2.1 Щелкните панель просмотра правой кнопкой мыши и в контекстном меню выберите **Добавить сетевой узел**.

2.2 В окне **Добавление получателей списков аннулированных сертификатов** выберите один или несколько сетевых узлов. При необходимости воспользуйтесь строкой быстрого поиска.

2.3 Нажмите кнопку **OK**.

3 Для удаления узла из перечня получателей CRL в контекстном меню данного узла выберите пункт **Удалить**.

Совет. Добавляйте в список получателей только те сетевые узлы, на которых действительно требуется оперативное обновление CRL, чтобы не перегружать сеть постоянной рассылкой CRL.

Вы также можете добавить сетевые узлы в список получателей CRL следующим способом:

1 В окне программы в представлении **Ключевой центр** выберите раздел **Сетевые узлы**.

2 На панели просмотра выберите один или несколько сетевых узлов и в контекстном меню выберите пункт **Получать текущий CRL**. В результате напротив этого пункта появится флажок, а выбранные узлы будут добавлены в список получателей CRL.

3 Таким же способом вы можете удалить сетевые узлы из списка получателей CRL. Отсутствие флажка напротив пункта **Получать текущий CRL** означает отсутствие сетевого узла в списке получателей CRL.

Чтобы настроить параметры передачи CRL на узлы списка рассылки:

1 В окне программы в меню **Сервис** выберите пункт **Настройка**.

2 В появившемся окне на панели навигации выберите раздел **Сертификаты** > **Список аннулированных сертификатов**.

3 На вкладке **Своя сеть** установите флажок **Отправлять на узлы списка рассылки** и укажите условие отправки CRL, установив переключатель в одно из трех положений:

   - Для отправки изменений CRL сразу после их возникновения выберите **Немедленно**.
   - Для регулярной проверки наличия изменений в CRL выберите **Каждые** и в поле справа введите соответствующий временной интервал (в часах, в диапазоне от 1 до 999). При обнаружении изменений соответствующая информация будет отправлена получателям CRL.
   - Для ежедневной однократной проверки изменений в CRL выберите **Ежедневно в** и в поле справа введите желаемое время проверки. При обнаружении изменений соответствующая информация будет отправлена получателям CRL.

4 Для сохранения настроек нажмите кнопку **OK**.

Настройка автоматической передачи CRL

После обновления CRL всем узлам присваивается статус CRL. Вы можете настроить значение статуса CRL, которое присваивается узлам. В зависимости от присвоенного узлам статуса будет происходить отправка CRL в автоматическом режиме УКЦ. Вы можете выбрать один из следующих статусов CRL для узлов:

- **Требуется передать CRL**. На узлы с таким статусом передается CRL в автоматическом режиме УКЦ по расписанию.
- **Неактуальные**. На узлы с таким статусом передается CRL только вручную, передача в автоматическом режиме УКЦ недоступна.

Периодичность отправки обновления CRL определяется настройками автоматического режима УКЦ. Вы можете автоматически передавать CRL на все узлы вашей сети ViPNet со следующей периодичностью:

- Каждые несколько часов.
- Каждый день в конкретное время.
- Сразу после изменения статуса CRL на **Требуется передать CRL**.

Чтобы в автоматическом режиме УКЦ передавать CRL по расписанию на все сетевые узлы вашей сети ViPNet:

1 В окне программы в меню **Сервис** выберите пункт **Настройка**.

2 В окне **Настройка** на панели навигации выберите раздел **Сертификаты** > **Список аннулированных сертификатов**.

3 На вкладке **Своя сеть** в группе **Действия после обновления списка аннулированных сертификатов** в списке **Изменить статус CRL всех узлов на** выберите **Требуется передать CRL.**

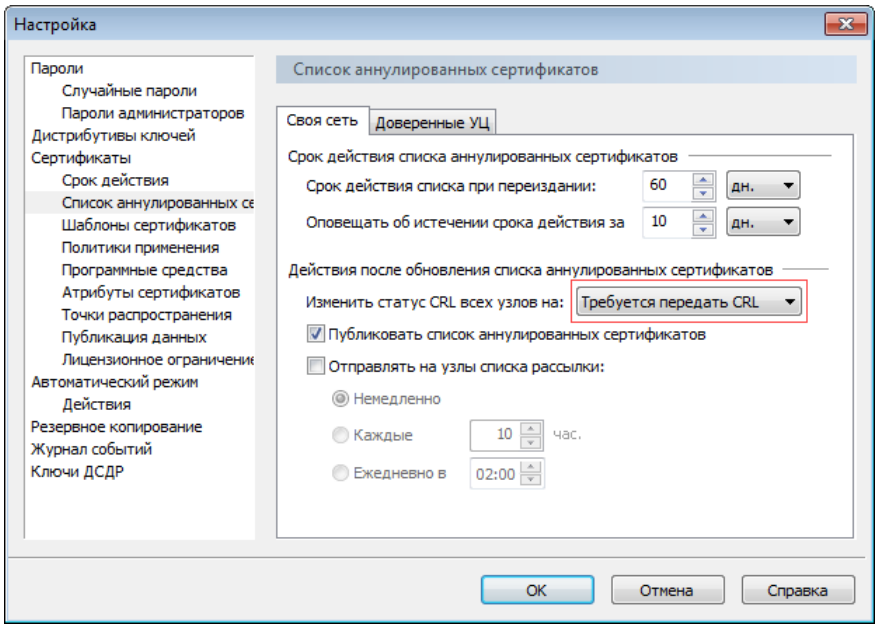

Рисунок 61. Настройка передачи обновления CRL для всех сетевых узлов

4 Чтобы после обновления CRL доверенной сети ViPNet автоматически передавать CRL на все узлы, связанные с доверенной сетью, на вкладке **Доверенные УЦ** в группе **Действия после обновления списка аннулированных сертификатов доверенной сети ViPNet** в соответствующем списке выберите **Требуется передать CRL**. При обновлении CRL доверенной сети статус CRL для сетевых узлов вашей сети, связанных с доверенной сетью, будет изменен на выбранный.

5 Чтобы после обновления CRL другого УЦ, с которым установлены доверительные отношения, автоматически передавать CRL на все узлы вашей сети, на вкладке **Доверенные УЦ** в группе **Действия после обновления списка аннулированных сертификатов стороннего УЦ** в соответствующем списке выберите **Требуется передать CRL**.

При обновлении CRL стороннего УЦ статус CRL для всех сетевых узлов вашей сети будет изменен на выбранный.

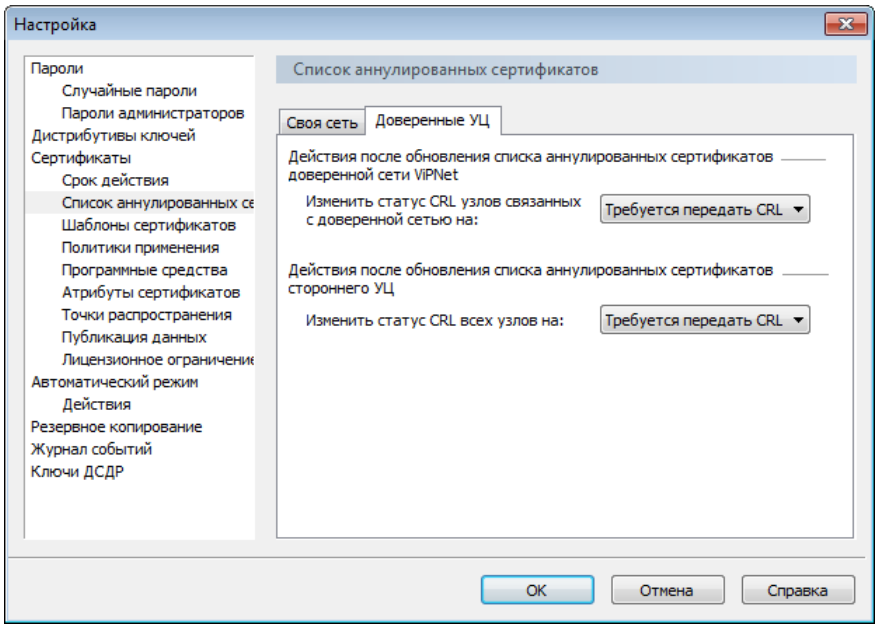

Рисунок 62. Передача CRL доверенных УЦ

6 В настройках автоматического режима УКЦ выберите операцию передачи всех CRL (см. Настройка автоматического режима на стр. 39).

7 В открывшемся окне **Параметры действия в автоматическом режиме** укажите периодичность обновления CRL, установив переключатель в нужное положение.

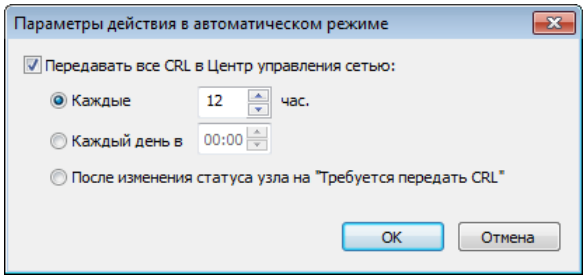

Рисунок 63. Настройка автоматической отправки CRL на все узлы

Если потребуется отключить передачу обновления CRL для всех узлов вашей сети в автоматическом режиме программы, в соответствующем списке выберите статус CRL **Неактуальные**. После обновления CRL статус CRL для узлов изменится на **Неактуальные**. В автоматическом режиме УКЦ CRL не будет отправлен. В этом случае обновленный CRL может быть отправлен только вручную (см. руководство администратора на УКЦ).

Просмотр списков аннулированных сертификатов

В программе ViPNet Удостоверяющий и ключевой центр вы можете просмотреть списки аннулированных сертификатов (CRL) вашей сети, а также импортированные CRL доверенных сетей ViPNet или других удостоверяющих центров.

Чтобы просмотреть CRL:

1. В окне программы на панели навигации перейдите в представление **Администрирование**.
2. Выберите раздел **Изданные сертификаты (Кросс-сертификация)** > **Списки аннулированных сертификатов** для просмотра CRL вашей сети или раздел **Импортированные сертификаты** > **Списки аннулированных сертификатов** для просмотра CRL доверенных сетей и сторонних УЦ.
3. На панели просмотра дважды щелкните CRL, который вы хотите просмотреть.
4. В окне **Список аннулированных сертификатов** ознакомьтесь с информацией на следующих вкладках:
   - **Общие** — содержит ряд полей, описывающих свойства списка аннулированных сертификатов: издатель списка (администратор УКЦ, для сертификата которого был издан список), дата ввода в действие и дата следующего обновления, алгоритм шифрования и другие.
   - **Список аннулированных сертификатов** — содержит серийные номера сертификатов, входящих в данный список, и дату окончания действия каждого из сертификатов. Вы можете просмотреть любой сертификат из списка с помощью кнопки **Просмотр сертификата** (см. Просмотр сертификатов на стр. 84).

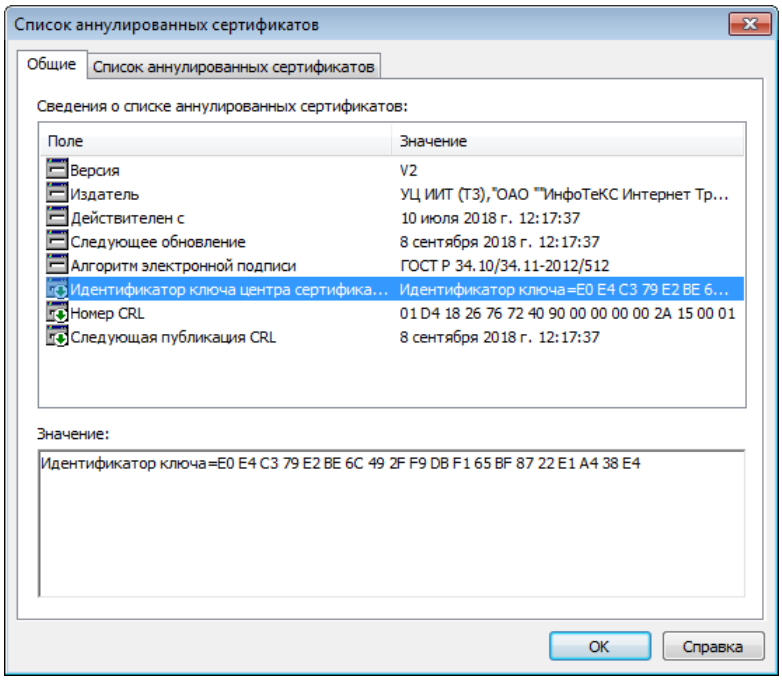

Рисунок 64. Просмотр общей информации о списке аннулированных сертификатов

Экспорт списков аннулированных сертификатов в файл

Вы можете экспортировать содержимое списков аннулированных сертификатов (CRL) в файлы. При этом несколько CRL могут экспортироваться несколькими способами:

- по отдельности в разные файлы (см. Экспорт одного CRL в файл на стр. 106);
- сразу все в один файл (см. Экспорт всех CRL в файл на стр. 107).

Экспорт одного CRL в файл

Вы можете экспортировать отдельные списки аннулированных сертификатов (CRL), за исключением импортированных CRL доверенных сетей ViPNet или других удостоверяющих центров, в файлы `*.crl`.

Файлы с отдельными CRL, как правило, требуются в следующих случаях:

- Для передачи CRL в доверенные удостоверяющий центры.
- Для публикации CRL в сетевых хранилищах или точках распространения, например, без использования сервиса публикации.
- Для передачи CRL внешнему пользователю вместе с изданным сертификатом пользователя и сертификатом администратора.

Чтобы экспортировать конкретный CRL в файл:

1. В окне программы на панели навигации перейдите в представление **Администрирование**.
2. Выберите раздел **Изданные сертификаты** (или **Кросс-сертификация**) > **Списки аннулированных сертификатов**.
3. На панели просмотра щелкните нужный CRL правой кнопкой мыши и в контекстном меню выберите пункт **Экспорт в файл**.
4. В появившемся окне укажите путь сохранения файла с CRL.

   В результате выбранный CRL будет сохранен в файле `*.crl` по указанному пути.

Экспорт всех CRL в файл

Вы можете экспортировать в файл сразу все списки отозванных сертификатов (CRL), которые присутствуют в программе, в том числе CRL из доверенных сетей ViPNet или других удостоверяющих центров. Это может потребоваться в том случае, если вам нужно отправить весь комплект CRL на узел, но по сети он не может быть доставлен, например, из-за отсутствия связи с этим узлом. В таком случае вы можете передать CRL на узел в файле `*.ke`.

Экспортировать таким образом CRL можно только для конкретного узла. Поэтому для экспорта в данном случае выполните следующие действия:

1. В окне программы на панели навигации выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть** > **Сетевые узлы**.
2. В списке на панели просмотра выберите нужный узел. При необходимости выберите несколько узлов.
3. В контекстном меню узла выберите **Сохранить все CRL в файл**.
4. В появившемся окне выберите папку на жестком или съемном диске.

   В результате CRL для выбранного узла будут сохранены в файл `apn_XXXX.ke` (где `XXXX` — шестнадцатеричный идентификатор узла в сети) в указанную папку. Передайте файл с CRL пользователю узла, ему необходимо поместить этот файл в папку установки программы ViPNet Client в подпапку `\CCC\key\` и затем перезапустить программу ViPNet Монитор.

Примечание. Вместе с полным комплектом CRL в файле `apn_XXXX.ke` также будет присутствовать справочник сертификатов администраторов.

6

Публикация сертификатов и списков аннулированных сертификатов

Взаимодействие с сервисом публикации

Поскольку компьютер с УКЦ исходя из требований безопасности не имеет выхода во внешние сети и доступа к общедоступным хранилищам, для размещения в них сертификатов и списков аннулированных сертификатов (CRL) используется сервис публикации — программа ViPNet Publication Service (см. глоссарий, стр. 209).

Взаимодействие УКЦ с сервисом публикации осуществляется следующим образом:

- Программа ViPNet Удостоверяющий и ключевой центр помещает данные для публикации в заданную папку обмена (см. Настройка папок обмена с программой ViPNet Publication Service на стр. 112), откуда эти данные поступают в программу ViPNet Publication Service. Передача данных для публикации из УКЦ может производиться автоматически (см. Режимы работы УКЦ на стр. 34) и вручную. Автоматически могут передаваться на публикацию только CRL. Для этого должны быть выполнены соответствующие настройки (см. Настройка автоматического режима на стр. 39). Остальные данные (сертификаты пользователей и администраторов, кросс-сертификаты) на публикацию требуется передавать вручную.
- После этого сервис публикации размещает эти данные в соответствии со своими настройками в заданных хранилищах или точках распространения. Точки распространения, в которых будет размещать данные сервис публикации, могут быть также заданы в УКЦ для того, чтобы информация об этих точках автоматически добавлялась в издаваемые сертификаты пользователей. Подробнее см. раздел Настройка списка точек распространения (на стр. 113).

  По завершении каждой публикации сервис формирует и отправляет в УКЦ отчет о результатах публикации в виде специального файла:

  - Полностью успешная публикация означает, что данные опубликованы на всех выбранных в программе ViPNet Publication Service серверах доступа.
  - Частично успешная публикация означает, что данные опубликованы не на всех выбранных серверах, но хотя бы на одном из них.
  - Неудачная публикация означает, что данные не удалось опубликовать.

  Файлы, которые не удалось опубликовать, вместе с отчетом помещаются в папку, заданную в УКЦ для приема неопубликованных данных.
- Если в сервисе публикации указаны точки распространения внешних удостоверяющих центров или доверенных сетей, то он производит их опрос с заданной периодичностью и скачивает из них новые сертификаты издателей и CRL.
- Данные, полученные из точек распространения, сервис публикации передает в УКЦ через папку, заданную для приема входящих файлов.
- УКЦ принимает полученные данные и импортирует их. Импорт CRL может производиться как автоматически, так и вручную, импорт сертификатов издателей — только вручную (см. Импорт данных, опубликованных сторонними удостоверяющими центрами на стр. 111). Для

автоматического импорта CRL должны быть выполнены соответствующие настройки (см. Настройка автоматического режима на стр. 39).

Затем импортированные данные могут быть отправлены на сетевые узлы в составе комплектов CRL или ключей узлов.

Подробнее о работе сервиса публикации см. документ «ViPNet Publication Service. Руководство администратора».

О том, как организовать взаимодействие между УКЦ и сервисом публикации, см. в разделе ниже.

Организация взаимодействия с сервисом публикации

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

1 Задайте папки для обмена данными с программой ViPNet Publication Service (см. Настройка папок обмена с программой ViPNet Publication Service на стр. 112).

Примечание. Если в соответствии с разделом «Типовые схемы размещения компонент ПК ViPNet УЦ» документа «ViPNet Удостоверяющий центр. Правила пользования» в вашей организации используется схема с внешним носителем, для переноса используйте внешний отчуждаемый носитель.

2 Если программы ViPNet Удостоверяющий и ключевой центр и ViPNet Publication Service установлены на разных компьютерах, то на компьютере с УКЦ средствами операционной системы откройте сетевой доступ к заданным папкам обмена для компьютера, на котором установлена программа ViPNet Publication Service.

3 Если вы хотите, чтобы списки аннулированных сертификатов (CRL) передавались на публикацию в автоматическом режиме, выполните дополнительные настройки УКЦ (см. Настройка автоматического режима на стр. 39).

4 Если сертификаты издателей и CRL будут публиковаться в точках распространения и вы хотите, чтобы в сертификаты пользователей добавлялась информация об этих точках, в настройках программы создайте эти точки распространения (см. Настройка списка точек распространения на стр. 113).

Передача данных для публикации вручную

Списки аннулированных сертификатов (CRL) для публикации могут передаваться в программу ViPNet Publication Service автоматически и вручную. Автоматическая передача CRL производится в том случае, если выполнены соответствующие настройки и программа работает в автоматическом режиме (см. Настройка автоматического режима на стр. 39). Сертификаты пользователей,

сертификаты издателей (администраторов УКЦ), кросс-сертификаты для публикации требуется передавать вручную.

Чтобы вручную передать данные для публикации:

1 В окне программы выберите объекты, которые требуется передать для публикации.

2 В контекстном меню объектов выберите пункт **Опубликовать**.

   В результате файлы с выбранными объектами будут помещены в папку, которая используется для обмена данными с программой ViPNet Publication Service.

Импорт данных, опубликованных сторонними удостоверяющими центрами

Сертификаты издателей и CRL, опубликованные сторонними удостоверяющими центрами и полученные сервисом публикации из точек распространения, передаются в УКЦ через папку обмена (см. Настройка папок обмена с программой ViPNet Publication Service на стр. 112). В УКЦ эти данные могут быть импортированы для дальнейшей рассылки на узлы своей сети. Сертификаты издателей могут быть импортированы только вручную, CRL — как вручную, так и автоматически (см. Настройка автоматического режима на стр. 39).

Примечание. Опубликованный CRL можно импортировать только после того, как будет импортирован сертификат его издателя. При этом сертификаты издателей можно импортировать только по одному.

Чтобы импортировать опубликованные данные вручную:

1 В окне программы на панели навигации выберите представление **Администрирование** и перейдите в раздел **Необработанные данные** > **Опубликованные сертификаты других УЦ**.

2 На панели просмотра выберите сертификат, который требуется импортировать, и на панели инструментов нажмите кнопку **Загрузить**. Импортированный сертификат будет перемещен в раздел **Импортированные сертификаты** в подраздел, соответствующий его типу.

Внимание! Прежде чем импортировать сертификат, рекомендуется проверить его параметры. Для просмотра параметров дважды щелкните сертификат (см. Просмотр сертификатов на стр. 84).

   Таким же образом импортируйте все необходимые сертификаты издателей.

3 Перейдите в раздел **Необработанные данные** > **Опубликованные списки аннулированных сертификатов других УЦ** и аналогичным образом импортируйте необходимые CRL.

   В результате выбранные CRL будут импортированы в УКЦ и перемещены в раздел **Импортированные сертификаты** > **Списки аннулированных сертификатов**.

Настройка параметров публикации данных

Сертификаты пользователей, сертификаты администраторов и списки аннулированных сертификатов (CRL), изданные в программе ViPNet Удостоверяющий и ключевой центр, могут быть опубликованы в общедоступных хранилищах или точках распространения с помощью программы ViPNet Publication Service (см. Взаимодействие с сервисом публикации на стр. 109). Ниже описана настройка параметров публикации данных в программе ViPNet Удостоверяющий и ключевой центр. Описание настройки программы ViPNet Publication Service приведено в документе «ViPNet Publication Service. Руководство администратора».

Настройка папок обмена с программой ViPNet Publication Service

Обмен данными между программами ViPNet Удостоверяющий и ключевой центр и ViPNet Publication Service осуществляется через папки, местоположение которых вы можете настраивать.

Примечание. Если в соответствии с разделом «Типовые схемы размещения компонент ПК ViPNet УЦ» документа «ViPNet Удостоверяющий центр. Правила пользования» в вашей организации используется схема с внешним носителем, для переноса используйте внешний отчуждаемый носитель.

Для настройки папок обмена с программой ViPNet Publication Service:

1. В окне программы в меню **Сервис** выберите пункт **Настройка**.
2. В появившемся окне на панели навигации выберите раздел **Публикация данных**.

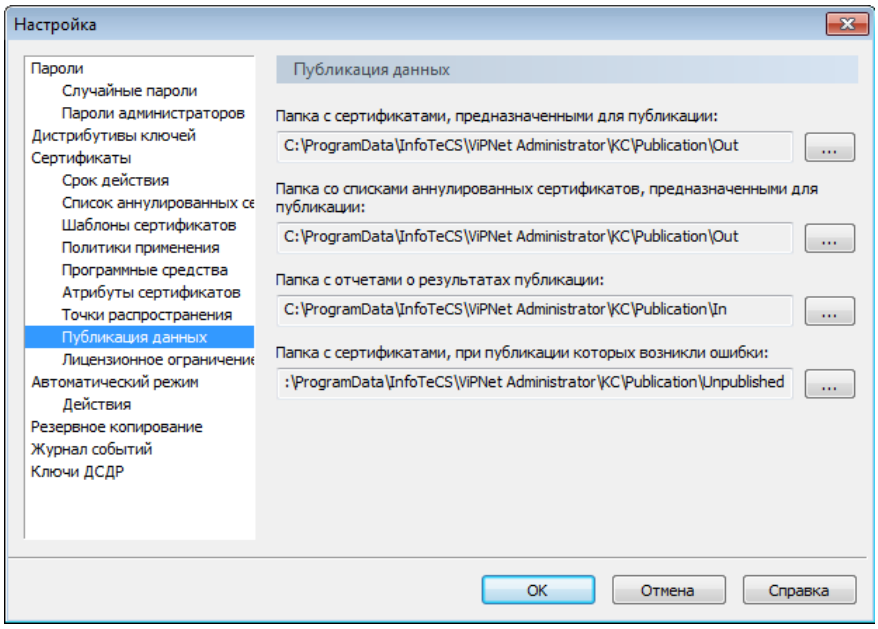

Рисунок 65. Настройка папок обмена данных

3 В соответствующих полях укажите с помощью кнопки ... папки для обмена данными с программой ViPNet Publication Service. По умолчанию заданы следующие папки обмена:

- Папка данных, предназначенных для публикации: `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Publication\Out`.
- Папка для списков аннулированных сертификатов: `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Publication\Out`.

  Для публикации обновленных CRL в указанную папку убедитесь, что в разделе **Список аннулированных сертификатов** на вкладке **Своя сеть** установлен флажок **Публиковать список аннулированных сертификатов**.
- Папка для приема данных и отчетов из сервиса публикации: `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Publication\In`.
- Папка для файлов, при публикации которых возникли ошибки: `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Publication\Unpublished`.

В программе ViPNet Publication Service необходимо настроить обмен данными с УКЦ через папки, заданные в программе ViPNet Удостоверяющий и ключевой центр. Подробнее см. документ «ViPNet Publication Service. Руководство администратора», глава «Настройка взаимодействия УКЦ и Сервиса публикации», раздел «Настройка папок обмена».

Настройка списка точек распространения

Списки аннулированных сертификатов (CRL) и сертификаты издателей (администраторов) с помощью программы ViPNet Publication Service могут публиковаться в точках распространения данных (см. глоссарий, стр. 217). Через точки распространения пользователи могут получать доступ к нужным им сертификатам издателей и CRL. Точкой распространения данных может быть,

например, FTP- или HTTP-сервер. Также точкой распространения может выступать сервер онлайн-проверки статуса сертификатов — OCSP-сервер (см. глоссарий, стр. 208).

Если в соответствии с инфраструктурой PKI (см. глоссарий, стр. 208), развернутой в вашей организации, сертификаты администраторов и CRL размещаются в точках распространения, то информация об этих точках должна помещаться в издаваемые сертификаты пользователей. Для этого в программе ViPNet Удостоверяющий и ключевой центр должен быть сформирован список этих точек распространения. Если сертификаты и CRL публикуются на OCSP-сервер, то в программе должен быть задан адрес доступа к нему.

Точки распространения и адрес доступа к OCSP-серверу задаются в настройках программы. Точки распространения также могут задаваться при издании сертификата администратора (см. Издание сертификата администратора на стр. 147). В этом случае задается точка распространения для издаваемого сертификата или для его CRL. Точки распространения, заданные при издании сертификатов администраторов, сохраняются в настройках программы.

Чтобы в настройках УКЦ создать точку распространения или задать адрес доступа к OCSP-серверу:

1 В окне программы в меню **Сервис** выберите пункт **Настройка**.

2 В появившемся окне на панели навигации выберите раздел **Точки распространения**.

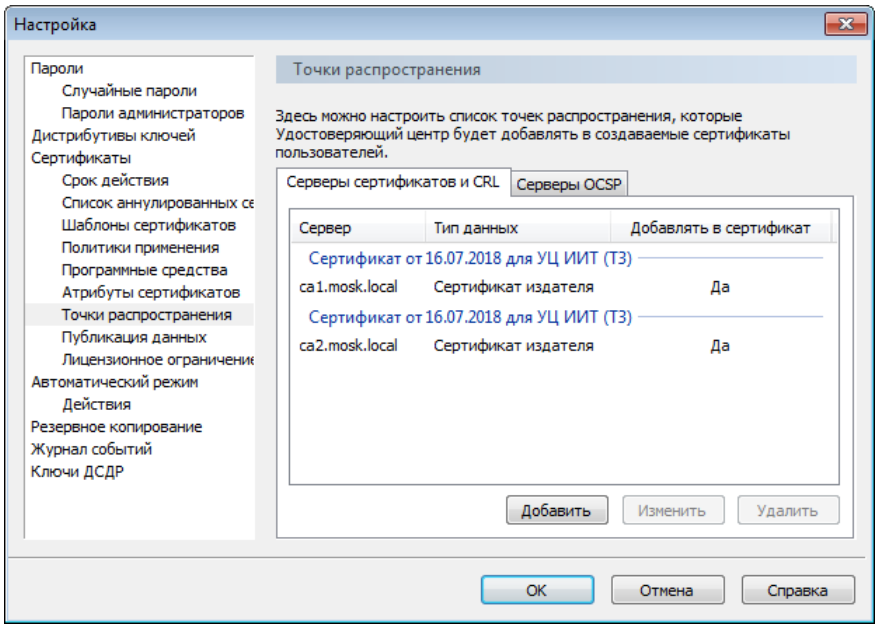

Рисунок 66. Настройка списка точек распространения

3 Чтобы создать точку распространения сертификата администратора или точку распространения CRL:

3.1 На вкладке **Серверы сертификатов и CRL** нажмите кнопку **Добавить**.

3.2 В появившемся окне укажите следующие параметры:

- **Сертификат издателя** — сертификат администратора. В зависимости от того, какой тип точки распространения вы укажете (см. параметр ниже), в созданной точке будет опубликован этот сертификат или соответствующий ему CRL.
- **Имя сервера** — имя точки распространения.

- **Сетевой путь** — URL-адрес сетевого ресурса, на котором будет размещаться данная точка распространения. В качестве URL-адреса может быть указан один из следующих адресов:

  HTTP-адрес, например: `http://www.infotecs.ca.ru/10A1_rem.crl`.

  FTP-адрес, например: `ftp://192.168.12.158/crl/5606-kid939/10A1_rem.crl`.

  LDAP-адрес, например: `ldap://192.168.45.144:389/CN=CDP,DC=kd,DC=local`.

- **Тип точки распространения**. Для публикации в точке распространения выбранного сертификата администратора укажите тип **Сертификат издателя**. Для публикации CRL, который соответствует выбранному сертификату, укажите **Список аннулированных сертификатов**.
- Для добавления информации о точке распространения в издаваемые сертификаты пользователей установите флажок **Добавлять в сертификаты пользователей**.

Примечание. В некоторых случаях может потребоваться не добавлять в сертификаты пользователей адрес точки распространения, в которой опубликован сертификат их издателя или CRL. Например, если точка распространения в будущем будет заменена OCSP-сервером и не будет использоваться. В этих случаях вам следует снять флажок в параметрах точки.

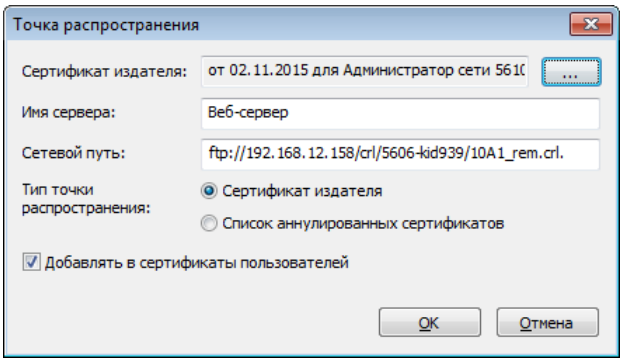

Рисунок 67. Добавление точки распространения

3.3 Нажмите кнопку **OK**. В списке появится новая точка распространения.

4 Чтобы задать адрес доступа к OCSP-серверу:

4.1 На вкладке **Серверы OCSP** нажмите кнопку **Добавить**.

4.2 В появившемся окне укажите следующие параметры:

- **Имя сервера** — имя OCSP-сервера.
- **Сетевой путь** — URL-адрес OCSP-сервера, например, `http://infotecs.ru/ocsp/ocsp.srf`.
- Для добавления информации об OCSP-сервере в издаваемые сертификаты пользователей установите флажок **Добавлять в сертификаты пользователей**.

Примечание. В некоторых случаях может потребоваться не добавлять в сертификаты пользователей адрес доступа к OCSP-серверу, на котором размещается сертификат их издателя или CRL. Например, если OCSP-сервер используется в тестовом режиме или на какое-то время прекращена его эксплуатация. В этих случаях вам следует снять флажок в параметрах доступа к OCSP-серверу.

4.3 Нажмите кнопку **OK**. В списке появится новый адрес доступа к OCSP-серверу.

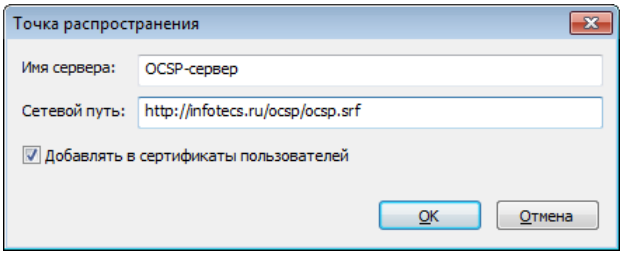

Рисунок 68. Добавление адреса доступа к OCSP-серверу

5 Для сохранения созданных точек распространения или адресов доступа к OCSP-серверу нажмите кнопку **OK**.

Чтобы изменить параметры точки распространения (или адреса доступа к OCSP-серверу), выберите ее в списке и нажмите кнопку **Изменить**, затем в окне **Точка распространения** внесите необходимые коррективы (см. выше) и нажмите кнопку **OK**. Чтобы удалить точку распространения (или адрес доступа), выберите ее в списке и нажмите кнопку **Удалить**.

7

Установление доверительных отношений с другими удостоверяющими центрами

Общая информация

Примечание. Представленные ниже описания относятся к неаккредитованным удостоверяющим центрам.

Между несколькими удостоверяющими центрами могут быть установлены доверительные отношения. Удостоверяющие центры, функционирующие на базе программного обеспечения ViPNet Удостоверяющий и ключевой центр, могут устанавливать отношения не только между собой, но и с удостоверяющими центрами, использующими программное обеспечение других производителей.

Установление доверительных отношений осуществляется путем кросс-сертификации (см. глоссарий, стр. 214). Кросс-сертификация, как правило, проводится на основе иерархической либо распределенной модели.

- В иерархической модели доверительных отношений удостоверяющие центры объединяются в древовидную структуру, в основании которой находится головной удостоверяющий центр (см. глоссарий, стр. 210). Головной удостоверяющий центр выдает кросс-сертификаты подчиненным ему центрам, тем самым обеспечивая доверие к ключам проверки электронной подписи этих центров. Каждый удостоверяющий центр вышестоящего уровня аналогичным образом делегирует право выпуска сертификатов подчиненным ему центрам. В результате доверие к сертификату каждого удостоверяющего центра основано на заверении его ключом вышестоящего центра. Сертификат головного удостоверяющего центра (корневой сертификат (см. глоссарий, стр. 213)) является самоподписанным. В остальных удостоверяющих центрах администраторы не имеют собственных корневых сертификатов и для установления доверительных отношений формируют запросы на кросс-сертификат к своим вышестоящим удостоверяющим центрам.

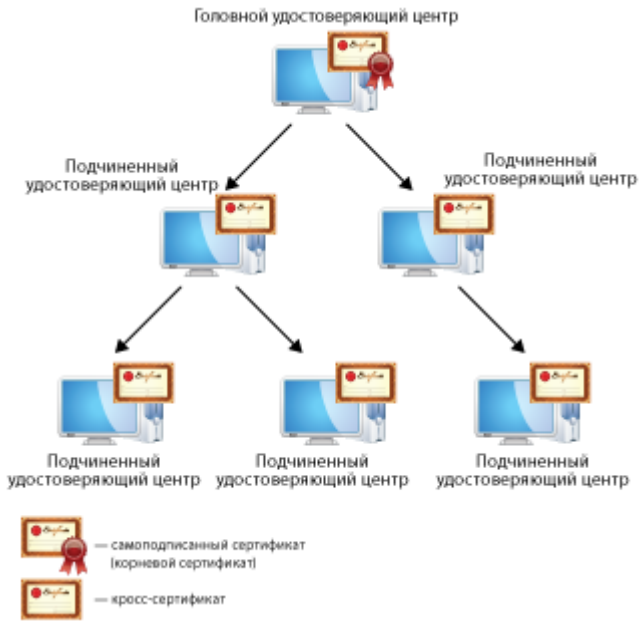

Рисунок 69. Иерархическая модель доверительных отношений

- В распределенной модели доверительных отношений все удостоверяющие центры равнозначны: в каждом удостоверяющем центре администратор имеет свой корневой (самоподписанный) сертификат. Доверительные отношения между удостоверяющими центрами в этой модели устанавливаются обычно путем двусторонней кросс-сертификации, когда два удостоверяющих центра издают кросс-сертификаты друг для друга. Взаимная кросс-сертификация проводится попарно между всеми удостоверяющими центрами. В результате в каждом удостоверяющем центре в дополнение к корневому сертификату имеются кросс-сертификаты, изданные для администраторов в других удостоверяющих центрах.

  Для подписания сертификатов пользователей каждый удостоверяющий центр продолжает пользоваться своим корневым сертификатом, а кросс-сертификат, изданный для другого удостоверяющего центра, использует для проверки сертификатов пользователей другой сети. Это возможно в силу того, кросс-сертификат для доверенного удостоверяющего центра издается на базе его корневого сертификата и содержит сведения о его ключе проверки электронной подписи. Поэтому в сети, отправившей запрос, нет необходимости переиздавать сертификаты пользователей.

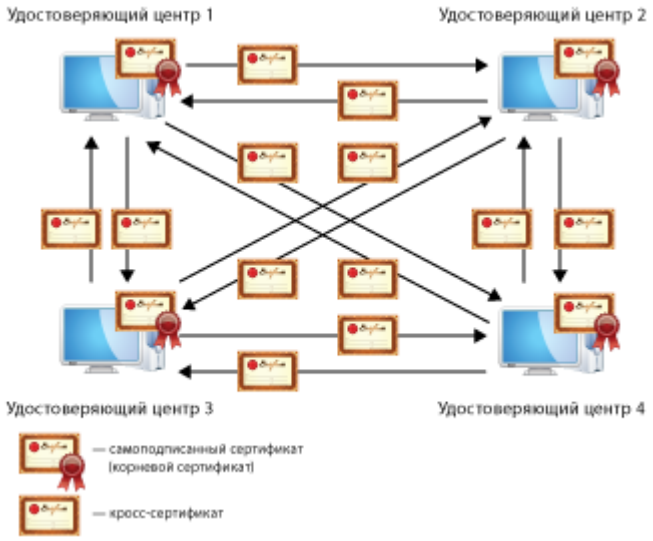

Рисунок 70. Распределенная модель доверительных отношений

О том, как установить доверительные отношения на основе данных моделей, см. в разделах ниже.

Установление доверительных отношений с вышестоящим или подчиненным удостоверяющим центром

Если вам требуется установить доверительные отношения с удостоверяющим центром (назовем его удостоверяющий центр А) на основе иерархической модели и ваш удостоверяющий центр является подчиненным по отношению к нему (см. глоссарий, стр. 216), выполните следующие действия:

1 Сформируйте запрос на сертификат к вышестоящему удостоверяющему центру для администратора программы ViPNet Удостоверяющий и ключевой центр. Подробнее см. раздел Создание запроса на сертификат к вышестоящему удостоверяющему центру (на стр. 122). Если администраторов в программе несколько, сформируйте запрос для каждого из них.

2 Сформированный запрос (или запросы, если их было создано несколько) передайте администратору удостоверяющего центра А лично либо любым защищенным способом.

   Администратор удостоверяющего центра А должен издать в соответствии с полученным от вас запросом кросс-сертификат (см. глоссарий, стр. 213) — сертификат администратора подчиненного удостоверяющего центра, после чего экспортировать его и передать вам вместе с сертификатом издателя, которым он был заверен, и соответствующим списком аннулированных сертификатов (CRL) (см. глоссарий, стр. 217).

Внимание! Если удостоверяющий центр А не является головным (см. глоссарий, стр. 210), то вам также должны быть переданы сертификаты и CRL вышестоящих удостоверяющих центров по отношению к удостоверяющему центру А, включая корневой сертификат и соответствующий ему CRL головного удостоверяющего центра. В противном случае изданный сертификат не сможет быть импортирован (см. пункт ниже) по причине отсутствия информации для его проверки.

---

3 Импортируйте полученные от администратора удостоверяющего центра А данные в следующей последовательности:

   3.1 Импортируйте сертификат издателя (см. Импорт сертификатов администраторов, полученных из вышестоящего удостоверяющего центра на стр. 124). Если соответствующий CRL содержится в одном файле с сертификатом, он также будет автоматически импортирован.

3.2 Если CRL, соответствующий сертификату издателя, был передан в отдельном файле, импортируйте его (см. Импорт списков аннулированных сертификатов, полученных из вышестоящего удостоверяющего центра на стр. 126).

3.3 Импортируйте изданный для вас сертификат (см. Импорт сертификата, выданного вышестоящим удостоверяющим центром на стр. 127).

4 Импортированный сертификат администратора сделайте текущим (см. Выбор текущего сертификата администратора на стр. 153). В процессе данной операции для сертификата будет сформирован соответствующий CRL.

В результате доверительные отношения между вашим и вышестоящим удостоверяющим центром будут установлены. Сертификатом администратора начнут подписываться все сертификаты, издаваемые в вашем удостоверяющем центре.

Если ваш удостоверяющий центр является по отношению к другому удостоверяющему центру (назовем его удостоверяющий центр B) вышестоящим (см. глоссарий, стр. 210), и удостоверяющий центр B хочет установить с вами доверительные отношения, то в этом случае выполните следующие действия:

1 В соответствии с полученным из удостоверяющего центра B запросом (или запросами) издайте сертификат (или сертификаты). При издании сертификат будет заверен вашим текущим сертификатом. Подробнее см. раздел Издание кросс-сертификата по запросу (на стр. 133).

2 Экспортируйте изданный сертификат. Подробнее см. раздел Экспорт кросс-сертификата (на стр. 136). Кроме этого, аналогичным образом экспортируйте тот сертификат, которым был заверен изданный сертификат, и соответствующий этому сертификату CRL.

Внимание! Если ваш удостоверяющий центр не является головным, то вы также должны экспортировать и передать сертификаты издателей и CRL вышестоящих по отношению к вам удостоверяющих центров, включая корневой сертификат и соответствующий ему CRL головного удостоверяющего центра. В противном случае администратор удостоверяющего центра B не сможет импортировать изданный сертификат по причине отсутствия информации для его проверки.

---

3 Экспортированные сертификаты и CRL передайте администратору удостоверяющего центра B лично либо любым защищенным способом.

Администратор удостоверяющего центра B должен импортировать все полученные от вас данные.

На этом установка доверительных отношений между вашим удостоверяющим центром и удостоверяющим центром B будет считаться завершенной.

Создание запроса на сертификат к вышестоящему удостоверяющему центру

Для получения сертификата (кросс-сертификата) в вышестоящем удостоверяющем центре требуется сформировать запрос. Сформировать запрос может администратор, учетная запись которого является текущей (см. Смена текущей учетной записи администратора на стр. 142).

Примечание. При создании запроса на сертификат к вышестоящему удостоверяющему центру формируется контейнер ключей, в который помещается ключ электронной подписи. Сертификат, изданный по запросу, в процессе импорта сопоставляется с данным ключом электронной подписи (см. Импорт сертификата, выданного вышестоящим удостоверяющим центром на стр. 127).

Чтобы создать запрос на сертификат к вышестоящему удостоверяющему центру:

1 В окне программы на панели навигации выберите представление **Администрирование** и перейдите в раздел **Кросс-сертификация** > **Запросы в вышестоящий УЦ**.

2 На панели просмотра нажмите кнопку **Создать**.

Будет запущен мастер создания запроса на сертификат в вышестоящий удостоверяющий центр, следуйте его указаниям.

3 На начальных страницах мастера укажите необходимую информацию, криптопровайдер и параметры алгоритма подписи, место хранения ключа электронной подписи, ограничения и расширения сертификата, на который создается запрос. Данные сведения указываются таким же способом, как и при издании обычного сертификата администратора (см. Издание сертификата администратора на стр. 147).

Примечание. В запросе вы также можете задать основные ограничения сертификата. Это может быть ограничение на длину цепочки. Длина цепочки определяет количество издателей — других удостоверяющих центров, которые могут следовать за вашим удостоверяющим центром. Этим издателям будет доверять удостоверяющий центр, в который вы отправите запрос. Если длина будет равна 0, то удостоверяющий центр, в который вы отправите запрос, будет доверять только вашему удостоверяющему центру.

---

4 На странице **Место хранения контейнера ключей** укажите место хранения контейнера ключей: **На внешнем устройстве**. Нажмите кнопку **Далее**.

Подключите внешнее устройство к компьютеру и выберите его на странице **Место хранения контейнеров ключа электронной подписи и ключа защиты УКЦ**. Если требуется, введите ПИН-код. После этого нажмите кнопку **Далее**.

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 Внешние устройства (на стр. 183).

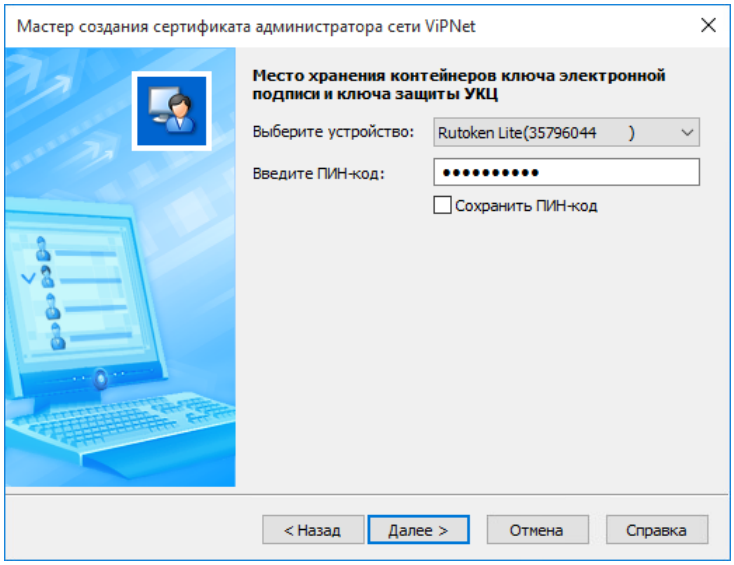

Рисунок 71. Выбор внешнего устройства

5 На странице готовности к созданию запроса на сертификат убедитесь в правильности параметров, заданных на предыдущих страницах мастера, и нажмите кнопку **Далее**. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.

6 Появится электронная рулетка (см. глоссарий, стр. 218), если она еще не запускалась в текущем сеансе работы. Следуйте указаниям в окне **Электронная рулетка**. После этого будет запущен процесс создания запроса на сертификат.

7 На последней странице мастера при успешном создании и сохранении запроса появится соответствующее сообщение и значок напротив каждой операции. Нажмите кнопку **Закрыть**.

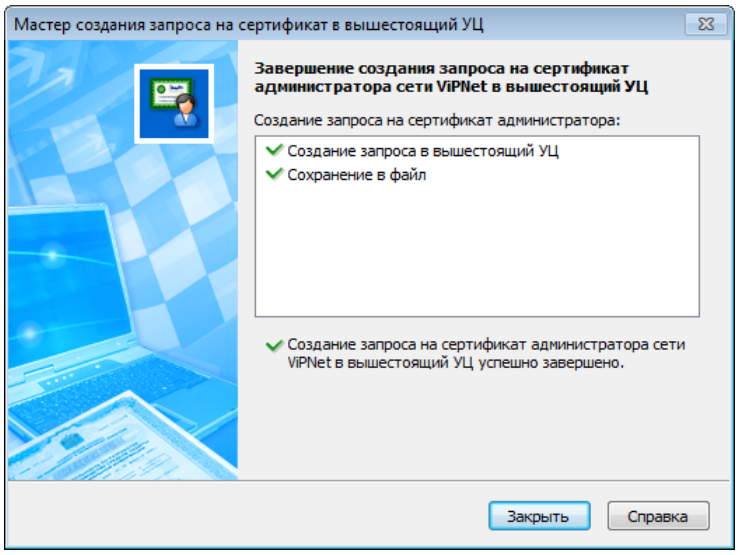

Рисунок 72. Результат создания запроса на сертификат к вышестоящему удостоверяющему центру

В результате для вас будет сформирован запрос на сертификат к вышестоящему удостоверяющему центру в формате PKCS#10 (файл `*.p10`). Передайте его администратору вышестоящего удостоверяющего центра для издания сертификата (кросс-сертификата).

Созданный запрос будет добавлен в список запросов к вышестоящему удостоверяющему центру и появится в разделе **Кросс-сертификация** > **Запросы в вышестоящий УЦ**. При необходимости вы можете его там найти и просмотреть (см. Просмотр запроса на сертификат к вышестоящему удостоверяющему центру на стр. 128).

Импорт сертификатов администраторов, полученных из вышестоящего удостоверяющего центра

Прежде чем импортировать сертификат, изданный в вышестоящем удостоверяющем центре, требуется импортировать сертификат издателя — сертификат администратора вышестоящего удостоверяющего центра, которым заверен ваш сертификат. Также необходимо импортировать соответствующий сертификату издателя список аннулированных сертификатов (CRL). Сертификат издателя и соответствующий CRL требуются для проверки сертификата, изданного вышестоящим удостоверяющим центром.

Примечание. Если удостоверяющий центр, который выдал вам сертификат, не является головным (см. глоссарий, стр. 210), то вам также должны быть переданы сертификаты и CRL вышестоящих по отношению к нему удостоверяющих центров, включая корневой сертификат и соответствующий ему CRL головного удостоверяющего центра. Данные сертификаты и CRL также должны быть импортированы.

Сертификат и соответствующий ему CRL передаются в отдельных файлах, поэтому импортируются отдельно друг от друга. О том, как импортировать CRL, см. в разделе Импорт списков аннулированных сертификатов, полученных из вышестоящего удостоверяющего центра (на стр. 126). Чтобы импортировать сертификат администратора вышестоящего удостоверяющего центра:

1 В окне программы на панели навигации выберите представление **Администрирование** и перейдите в раздел:

- **Импортированные сертификаты** > **Корневые сертификаты** — для импорта корневого сертификата головного удостоверяющего центра.
- **Импортированные сертификаты** > **Сертификаты промежуточных УЦ** — для импорта сертификата промежуточного удостоверяющего центра.

После этого на панели просмотра нажмите кнопку **Загрузить из файла**.

2 В появившемся окне выберите один или несколько файлов сертификатов, которые требуется импортировать. Выбранные сертификаты будут отображены в окне **Загрузка корневых сертификатов** или **Загрузка кросс-сертификатов**.

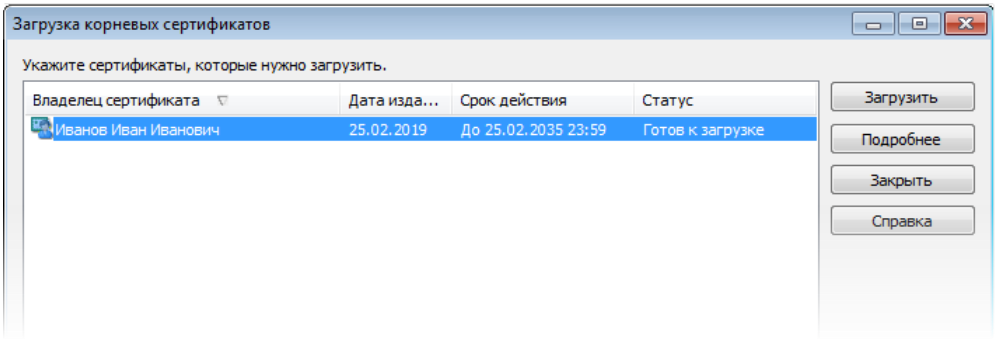

Рисунок 73. Импорт корневых сертификатов

Примечание. В окне **Загрузка корневых сертификатов** невозможно импортировать сертификаты, не являющиеся корневыми. В окне **Загрузка кросс-сертификатов** невозможно импортировать корневые сертификаты.

Кроме этого, невозможно импортировать сертификаты, которые уже были импортированы ранее.

3 Прежде чем импортировать сертификаты, вы можете просмотреть их содержимое. Для этого выберите нужный сертификат в списке и нажмите кнопку **Подробнее**. Откроется окно просмотра сертификата (см. Просмотр сертификатов на стр. 84).

Примечание. Сертификаты, которые еще не были импортированы, не являются действительными. В связи с этим при просмотре и проверке этих сертификатов на вкладке **Путь сертификации** отображается информация о том, что нет доверия к корневому сертификату центра сертификации. Данное сообщение не является препятствием для импорта сертификата. При отсутствии других ошибок и совпадении содержимого полей сертификата с содержимым в бумажной копии, сертификат может быть импортирован. После импорта он станет действительным.

4 Чтобы импортировать сертификаты, выберите их в списке и нажмите кнопку **Загрузить**. Будет выполнен импорт выбранных сертификатов.

5 После импорта сертификатов издателей передайте CRL на узлы вашей сети (см. руководство администратора на УКЦ). В составе CRL на узлы будут доставлены сертификаты издателей.

Импорт списков аннулированных сертификатов, полученных из вышестоящего удостоверяющего центра

Список аннулированных сертификатов, соответствующий сертификату администратора вышестоящего удостоверяющего центра, требуется для проверки вашего сертификата, который был издан в этом удостоверяющем центре.

Если списки аннулированных сертификатов поступили вместе с сертификатами администраторов в одном наборе формата PKCS #7, то они будут импортированы автоматически вместе с сертификатами (см. Импорт сертификатов администраторов, полученных из вышестоящего удостоверяющего центра на стр. 124). Если список аннулированных сертификатов поступил в виде файла `*.crl`, то для его импорта выполните следующие действия:

1 В окне программы на панели навигации выберите представление **Администрирование** и перейдите в раздел **Импортированные сертификаты** > **Списки аннулированных сертификатов**, затем нажмите кнопку **Загрузить из файла**.

2 В появившемся окне выберите один или несколько файлов, содержащих списки аннулированных сертификатов. Выбранные списки будут отображены в окне **Загрузка списков аннулированных сертификатов**.

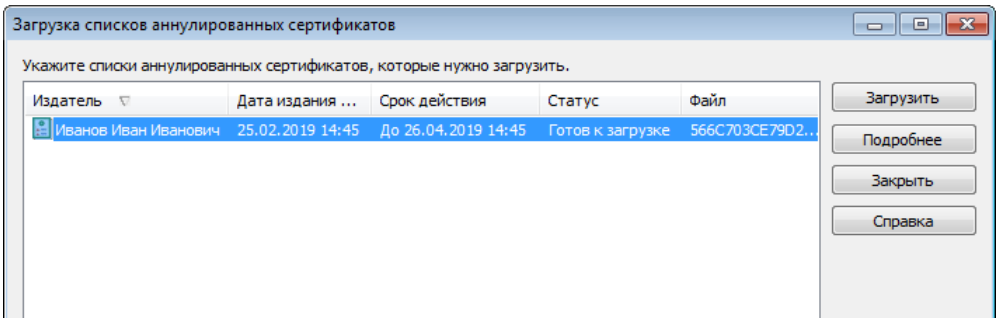

Рисунок 74. Импорт списков аннулированных сертификатов

3 Прежде чем импортировать списки аннулированных сертификатов, вы можете просмотреть их содержимое. Для этого выберите нужный список и нажмите кнопку **Подробнее**. Откроется окно просмотра CRL.

4 Чтобы импортировать списки аннулированных сертификатов, выберите их и нажмите кнопку **Загрузить**. Будет выполнен импорт выбранных списков.

Примечание. Невозможно импортировать списки аннулированных сертификатов, если ранее не были импортированы соответствующие им сертификаты администраторов. Также невозможно импортировать списки аннулированных сертификатов, срок действия которых истек.

---

5 После импорта списков аннулированных сертификатов передайте их на узлы вашей сети (см. руководство администратора на УКЦ).

Импорт сертификата, выданного вышестоящим удостоверяющим центром

Чтобы использовать сертификат (кросс-сертификат), полученный из вышестоящего удостоверяющего центра, в своем удостоверяющем центре, вам его требуется импортировать. Импортировать сертификат может администратор, учетная запись которого является текущей (см. Смена текущей учетной записи администратора на стр. 142).

Внимание! Импорт сертификата вы сможете выполнить только после того, как были импортированы сертификат его издателя — сертификат, которым он был подписан при издании, и соответствующий ему список аннулированных сертификатов (CRL).

В процессе импорта сертификат (а точнее ключ проверки электронной подписи, который содержится в сертификате) сопоставляется с ключом электронной подписи, который был создан при формировании запроса на данный сертификат (см. Создание запроса на сертификат к вышестоящему удостоверяющему центру на стр. 122).

Для импорта сертификата, изданного в вышестоящем удостоверяющем центре:

1 В окне программы на панели навигации выберите представление **Администрирование** и перейдите в раздел **Кросс-сертификация** > **Сертификаты от вышестоящего УЦ**, затем нажмите кнопку **Загрузить из файла**.

2 В появившемся окне выберите файл с изданным сертификатом, предварительно указав тип его расширения. Выбранный сертификат появится в окне **Загрузка сертификатов изданных в вышестоящем УЦ**.

Примечание. Изданный сертификат может быть передан в файле `*.p7b`, `*.cer` или `*.crt`.

3 Прежде чем импортировать загруженный сертификат, вы можете просмотреть его содержимое. Для этого выберите сертификат в списке и нажмите кнопку **Подробнее**. Откроется окно просмотра сертификата (см. Просмотр сертификатов на стр. 84).

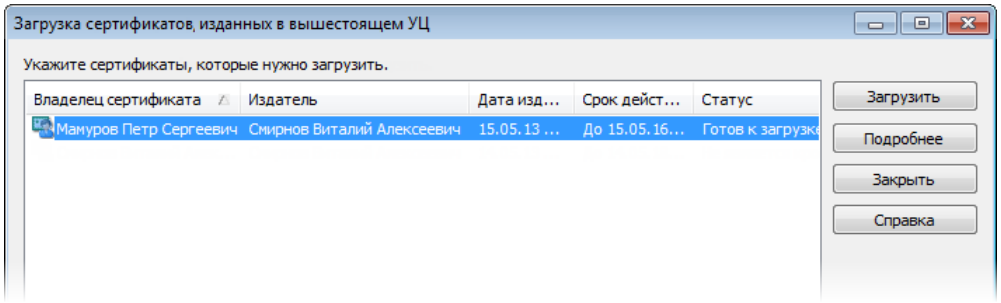

Рисунок 75. Импорт сертификата, изданного вышестоящим удостоверяющим центром

4 Для импорта сертификата нажмите кнопку **Загрузить**.

В результате сертификат, полученный из вышестоящего удостоверяющего центра, будет импортирован (появится в списке сертификатов в разделе **Кросс-сертификация** > **Сертификаты от вышестоящего УЦ**). Запрос, в соответствии с которым был издан данный сертификат, будет считаться удовлетворенным, его статус изменится на **Удовлетворен вышестоящим УЦ**. Кроме этого, будет создан список аннулированных сертификатов, соответствующий импортированному сертификату. Данный список появится в разделе **Кросс-сертификация** > **Список аннулированных сертификатов.**

5 Импортированный сертификат, полученный из вышестоящего удостоверяющего центра, назначьте текущим сертификатом администратора (см. Выбор текущего сертификата администратора на стр. 153). Появится окно о необходимости отправить CRL на узлы своей сети, нажмите **ОК**.

6 Передайте CRL на узлы своей сети (см. руководство администратора на УКЦ).

При наличии межсетевого взаимодействия выполните экспорт служебных данных (см. руководство администратора на УКЦ). В составе CRL ваш новый сертификат, а также сертификат его издателя и список аннулированных сертификатов, будут доставлены на сетевые узлы, в составе экспорта — в доверенные сети.

Просмотр запроса на сертификат к вышестоящему удостоверяющему центру

Чтобы просмотреть параметры сформированных запросов на сертификаты к вышестоящему удостоверяющему центру:

1 В окне программы на панели навигации перейдите в представление **Администрирование** и выберите раздел **Кросс-сертификация** > **Запросы в вышестоящий УЦ**.

2 Дважды щелкните нужный запрос либо в контекстном меню запроса выберите пункт **Открыть запрос**.

3 В окне просмотра параметров запроса ознакомьтесь с информацией на следующих вкладках:

- **Состав запроса** — содержит список расширений запроса, в которых указаны:
  - сведения об администраторе, для которого создан запрос;
  - параметры ключа проверки электронной подписи — алгоритм, который использовался при создании ключа, заявленный срок действия;
  - список назначений, ограничений и политик применения, которые должны быть включены в сертификат.
- **Изданный сертификат** — содержит информацию о сертификате, изданном по данному запросу: серийный номер, срок действия и статус (**Действителен**, **Недействителен**). С помощью кнопки **Открыть сертификат** можно просмотреть параметры сертификата. Если по запросу не издавался сертификат либо был получен, но не импортировался, то данная вкладка отображаться не будет.

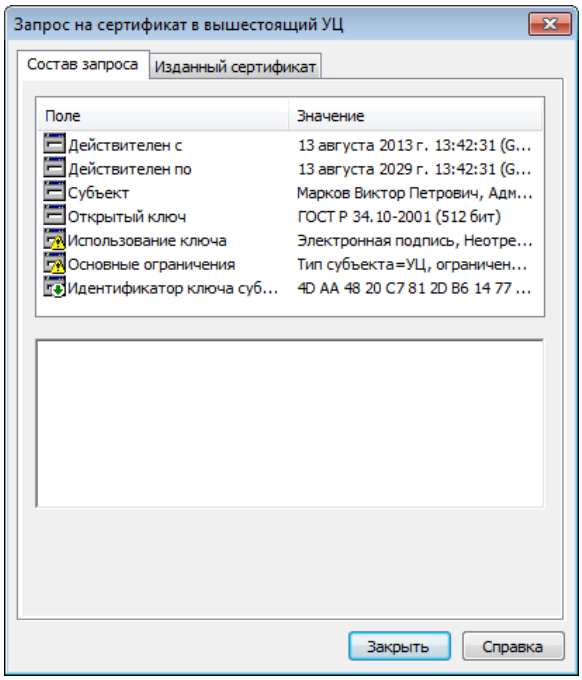

Рисунок 76. Просмотр параметров запроса на сертификат к вышестоящему удостоверяющему центру

Установление доверительных отношений с равнозначным удостоверяющим центром

Если вы хотите, чтобы между вашим и другим удостоверяющим центром (назовем его удостоверяющий центр С) были установлены доверительные отношения по распределенной модели, и администратор удостоверяющего центра С согласен с этим, выполните следующие действия:

1. Для каждого действительного сертификата администратора программы ViPNet Удостоверяющий и ключевой центр сформируйте запрос на кросс-сертификат. Подробнее см. в раздел Создание запроса на кросс-сертификат (на стр. 131). Если администраторов в программе несколько, то запрос на кросс-сертификат необходимо создать для сертификатов каждого администратора.
2. Сформированные запросы передайте администратору удостоверяющего центра С лично либо любым защищенным способом.

   Администратор удостоверяющего центра С должен издать в соответствии с полученными от вас запросами кросс-сертификаты, после чего распространить их среди своих пользователей.

   В результате удостоверяющий центр С будет доверять вашему удостоверяющему центру, то есть все издаваемые в вашем удостоверяющем центре сертификаты в удостоверяющем центре С будут считаться действительными.

Если администратор удостоверяющего центра С хочет, чтобы ваш удостоверяющий центр также ему доверял, и вы с этим согласны, то в этом случае выполните следующие действия:

1. В соответствии с полученными из удостоверяющего центра С запросами издайте кросс-сертификаты. Подробнее см. раздел Издание кросс-сертификата по запросу (на стр. 133).
2. Распространите изданные кросс-сертификаты между вашими пользователями путем передачи на их узлы CRL (см. руководство администратора на УКЦ).

   В результате ваш удостоверяющий центр будет доверять удостоверяющему центру С, то есть все сертификаты, издаваемые в удостоверяющем центре С, в вашем удостоверяющем центре будут проверяться и считаться действительными.

Таким образом, будет проведена двусторонняя кросс-сертификация между вашим и удостоверяющим центром С.

Примечание. При установлении доверительных отношений с несколькими удостоверяющими центрами описанную выше процедуру двусторонней кросс-сертификации потребуется провести с каждым из них.

Создание запроса на кросс-сертификат

Чтобы администратор удостоверяющего центра, с которым вы хотите установить доверительные отношения, смог издать кросс-сертификат, вам требуется создать и передать ему запрос на кросс-сертификат. Сформировать запрос на кросс-сертификат может администратор, учетная запись которого является текущей (см. Смена текущей учетной записи администратора на стр. 142).

Примечание. При создании запроса на кросс-сертификат, в отличие от создания запроса к вышестоящему удостоверяющему центру, ключ электронной подписи не формируется. Запрос на кросс-сертификат подписывается ключом электронной подписи, соответствующим сертификату, на основе которого данный запрос создается.

Чтобы создать запрос на кросс-сертификат:

1. В окне программы выберите представление **Администрирование** и перейдите в раздел **Моя сеть** > **Администраторы**.
2. В списке на панели просмотра щелкните вашу учетную запись правой кнопкой мыши и в контекстном меню выберите пункт **Создать запрос на кросс-сертификат**. Будет запущен мастер создания запроса на кросс-сертификат, следуйте его указаниям.
3. На странице **Сертификат администратора** выберите сертификат, на основе которого будет создан запрос на кросс-сертификат.

   При необходимости просмотрите параметры сертификата с помощью кнопки **Посмотреть сертификат**. Создаваемый запрос впоследствии будет подписан ключом электронной подписи, который соответствует выбранному сертификату.

   Нажмите кнопку **Далее**.

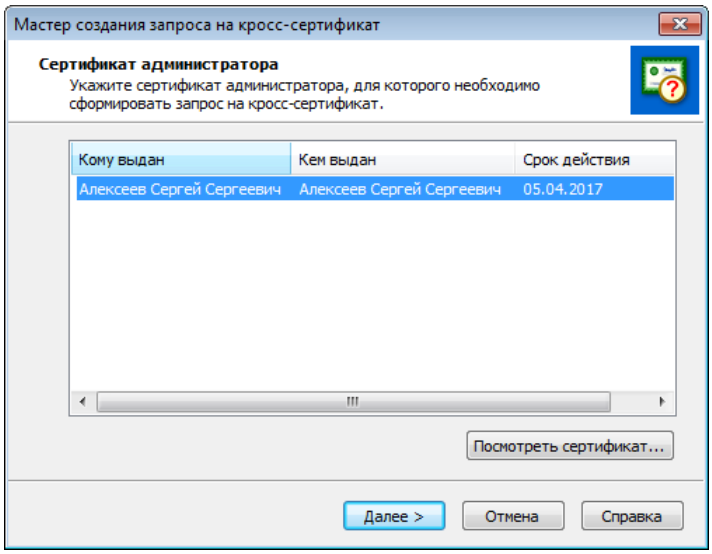

Рисунок 77. Выбор сертификата администратора для создания запроса на кросс-сертификат

4 На странице **Назначение кросс-сертификата**, если требуется, добавьте или измените ограничения и расширения, которые будет содержать запрос на кросс-сертификат, а после издания и сам кросс-сертификат. Формирование ограничений и расширений для кросс-сертификата осуществляется так же, как и при издании обычного сертификата администратора (см. Издание сертификата администратора на стр. 147).

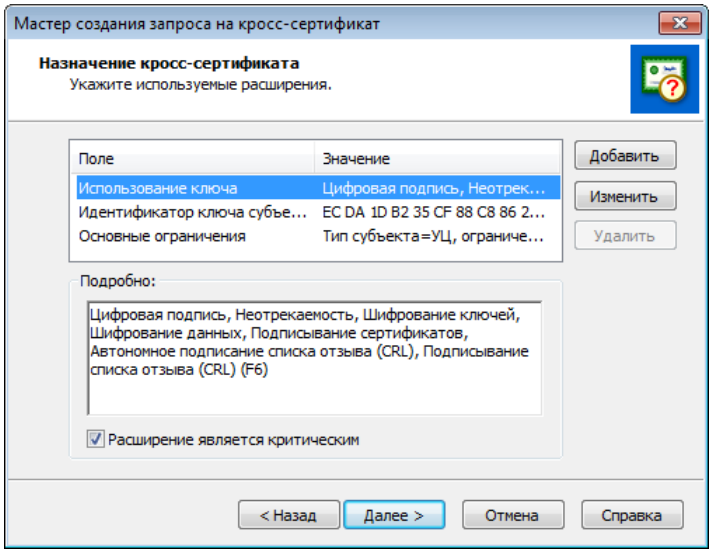

Рисунок 78. Указание расширений кросс-сертификата

Примечание. В запросе вы также можете задать основные ограничения сертификата. Это может быть ограничение на длину цепочки. Длина цепочки определяет количество издателей — других удостоверяющих центров, которые могут следовать за вашим удостоверяющим центром. Этим издателям будет доверять удостоверяющий центр, в который вы отправите запрос. Если длина будет равна 0, то удостоверяющий центр, в который вы отправите запрос, будет доверять только вашему удостоверяющему центру. Длина не может превышать длину, указанную в сертификате администратора, для которого создается запрос.

---

5 После задания параметров кросс-сертификата нажмите кнопку **Далее**.

6 На последней странице **Файл запроса** задайте путь и имя файла, в котором будет сохранен запрос, затем нажмите кнопку **Готово**.

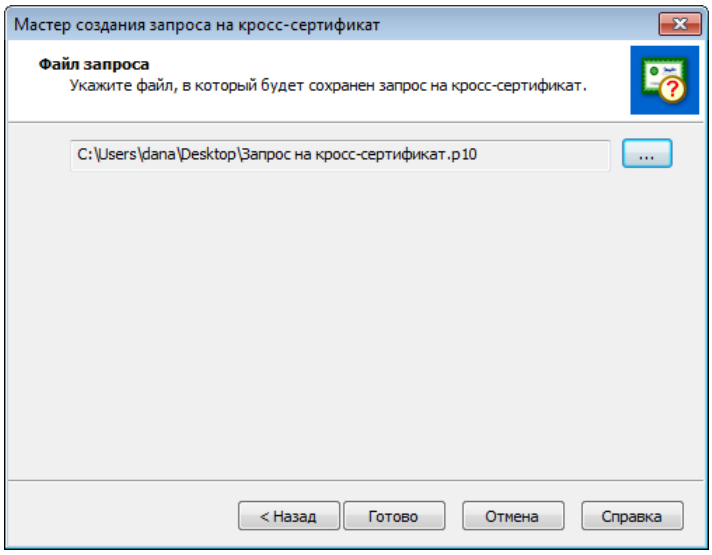

Рисунок 79. Указание места хранения файла с запросом на кросс-сертификат

В результате будет сформирован запрос на кросс-сертификат в формате PKCS#10 (файл `*.p10`). Передайте запрос администратору удостоверяющего центра, с которым устанавливаются доверительные отношения, для издания кросс-сертификата.

Издание кросс-сертификата по запросу

Если вам поступил запрос на кросс-сертификат, то его требуется обработать — издать по нему кросс-сертификат.

Кроме этого, если по запросу уже когда-то был издан кросс-сертификат, то вы можете издать по нему еще один повторно (например, если срок действия имеющегося кросс-сертификата истекает или если требуется добавить в него дополнительные расширения).

Примечание. Издание кросс-сертификатов производится одинаково как по запросам от подчиненных удостоверяющих центров, так и по запросам от равнозначных удостоверяющих центров.

Чтобы издать кросс-сертификат в соответствии с запросом, полученным из другого удостоверяющего центра:

1. В окне программы на панели навигации выберите представление **Администрирование** и перейдите в раздел **Кросс-сертификация** > **Сертификаты для других УЦ**, затем нажмите кнопку **Загрузить и обработать запрос**.
2. В появившемся окне выберите файл `*.p10`, в котором содержится запрос на кросс-сертификат, и нажмите кнопку **Открыть**. При необходимости вы можете выбрать сразу несколько файлов с запросами.
3. В окне **Издание кросс-сертификатов** в списке ознакомьтесь с параметрами запроса, который содержится в файле.

Для запроса указывается следующая информация:

- Кем запрос создан.
- Статус запроса: **Ожидает обработки**, **Действителен**, **Искажен** или **Неверный набор атрибутов**.
- Присутствуют ли в запросе сведения о сертификате, для которого он создавался (только для запросов, поступивших из равнозначных удостоверяющих центров).

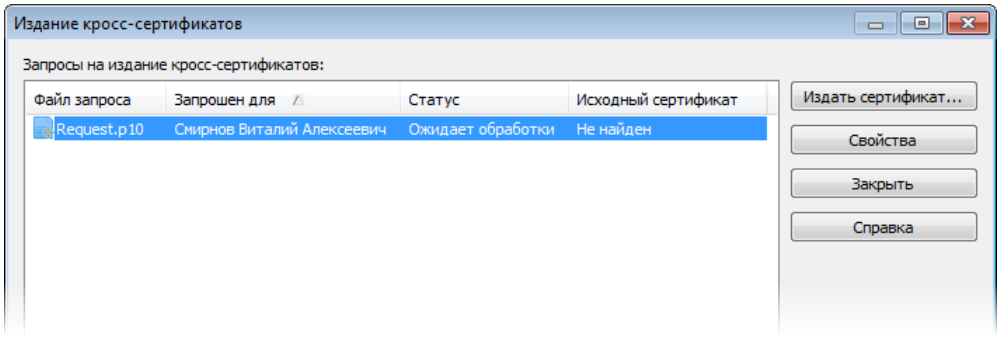

Рисунок 80. Выбор запроса для издания кросс-сертификата

4 При необходимости просмотрите параметры запроса с помощью кнопки **Свойства** (см. Просмотр запроса на кросс-сертификат (на стр. 137)).

5 Выберите запрос в списке, после чего нажмите кнопку **Издать сертификат**.

Примечание. Кнопка **Издать сертификат** будет неактивна в следующих случаях:

- Запрос поврежден (имеет статус **Искажен**).
- В запросе отсутствуют критические расширения (имеет статус **Неверный набор атрибутов**).
- Запрос принадлежит администратору вашего удостоверяющего центра (имеет статус **Не является запросом от другого УЦ**).

---

6 В появившемся мастере на странице **Срок действия кросс-сертификата** задайте срок действия издаваемого кросс-сертификата.

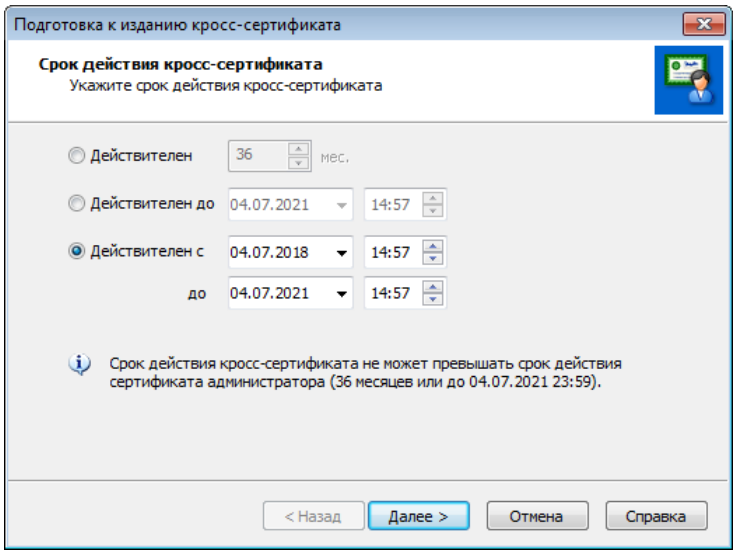

Рисунок 81. Задание срока действия издаваемого кросс-сертификата

7 На странице **Назначение кросс-сертификата** добавьте или измените основные ограничения и расширения издаваемого сертификата и нажмите кнопку **Далее**. Данные сведения формируются так же, как и при издании обычного сертификата пользователя (см. Издание сертификатов на стр. 43).

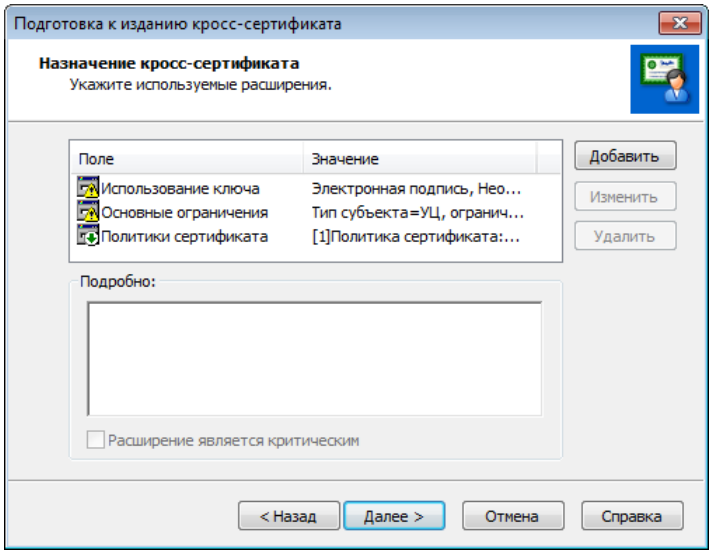

Рисунок 82. Формирование назначений кросс-сертификата

Если сертификат администратора удостоверяющего центра, на основе которого был создан запрос и для которого соответственно издается кросс-сертификат, включает политики применения, можно добавить расширение **Политики сертификата**. Это расширение позволит установить соответствие между политиками применения, содержащимися в запросе, и политиками применения вашего удостоверяющего центра (см. Настройка списка политик применения сертификата на стр. 64). Для этого:

7.1 На странице **Назначение кросс-сертификата** нажмите кнопку **Добавить**.

7.2 В окне **Допустимые расширения** выберите **Политики сертификата** и нажмите кнопку **OK**.

7.3 В окне **Политики сертификата** на левой панели выберите собственную политику, затем нажмите кнопку **Добавить**. Из списка политик запроса укажите ту политику, которую требуется поставить в соответствие выбранной собственной политике, затем нажмите кнопку **OK**.

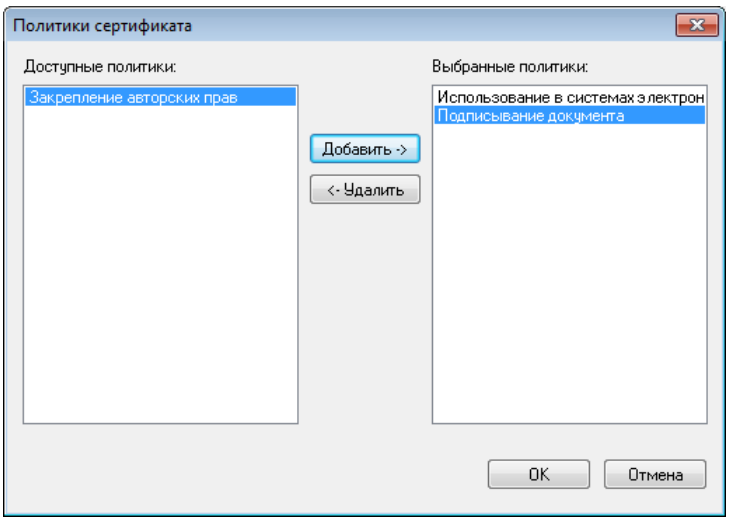

Рисунок 83. Сопоставление политик применения при издании кросс-сертификата

8 На странице **Состав кросс-сертификата** убедитесь в правильности параметров издаваемого сертификата, заданных на предыдущих страницах мастера, и нажмите кнопку **Готово**. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.

9 В окне сообщения об успешном издании кросс-сертификата нажмите кнопку **OK**.

После издания кросс-сертификата передайте CRL на узлы вашей сети (см. руководство администратора на УКЦ). В составе CRL на узлы будет доставлен изданный кросс-сертификат.

Изданный кросс-сертификат будет сохранен в контейнере кросс-сертификатов, который содержится в файле `issued_cross_cert_issuers_trl.p7s` в папке `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Key management\Certificates Issuers`, и появится в разделе **Кросс-сертификация** > **Сертификаты для других УЦ**. При необходимости вы можете его там найти и просмотреть (см. Просмотр сертификатов на стр. 84).

Если кросс-сертификат издавался для администратора подчиненного удостоверяющего центра, то его требуется экспортировать в файл для передачи данному администратору (см. Экспорт кросс-сертификата на стр. 136).

Экспорт кросс-сертификата

Кросс-сертификаты, изданные в процессе установления доверительных отношений с другими удостоверяющими центрами, также как и обычные сертификаты, можно экспортировать в файл (см. Экспорт сертификатов (на стр. 88)). Чаще всего экспортировать требуется сертификаты, изданные при установлении отношений по иерархической модели, потому что их необходимо передавать администраторам подчиненных удостоверяющих центров. Сертификаты, изданные при

установлении отношений на основе распределенной модели, как правило, после издания распространяются только среди своих пользователей с помощью отправки файлов CRL на узлы этих пользователей. При необходимости они также могут быть экспортированы.

Чтобы экспортировать изданный кросс-сертификат:

1 В окне программы перейдите в представление **Администрирование** и выберите раздел **Кросс-сертификация** > **Сертификаты для других УЦ**.

2 В списке на панели просмотра выберите нужный сертификат.

3 Щелкните по сертификату правой кнопкой мыши и в контекстном меню выберите пункт **Экспортировать**.

4 В появившемся мастере задайте параметры экспорта сертификата таким же образом, как и при экспорте обычного сертификата.

   В результате выбранный сертификат будет экспортирован в файл с указанным расширением и будет готов к передаче.

Просмотр запроса на кросс-сертификат

Прежде чем обработать поступивший запрос на кросс-сертификат, просмотрите его параметры:

1 В окне **Издание кросс-сертификатов** в списке выберите запрос и нажмите кнопку **Свойства**.

2 В окне просмотра параметров запроса ознакомьтесь с информацией на следующих вкладках:

- **Общие** — содержит список расширений запроса, в которых указаны параметры ключа проверки электронной подписи; сведения об администраторе, для которого запрошен кросс-сертификат; назначение и использование ключа; основные ограничения и другое.
- **Сертификат автора запроса** — содержит сведения о сертификате, для которого создавался запрос и которым он был подписан: серийный номер, срок действия и статус (**Действителен**, **Недействителен**). При необходимости можно просмотреть параметры данного сертификата с помощью кнопки **Открыть сертификат из файла** (см. раздел Просмотр сертификатов (на стр. 84)).

  Примечание. Данные сведения отображаются только для запросов на кросс-сертификаты от равнозначных удостоверяющих центров и только в том случае, если сертификаты, для которых создавались запросы, были предварительно импортированы. Во всех остальных случаях на данной вкладке указано, что сертификат не найден.

- **Изданные сертификаты** — содержит список кросс-сертификатов, которые уже были изданы по данному запросу ранее (в том случае, если по запросу повторно издается кросс-сертификат). Для каждого сертификата отображается имя владельца, срок действия и статус (**Действителен**, **Недействителен**). С помощью кнопки **Подробнее** можно просмотреть параметры каждого сертификата из списка.

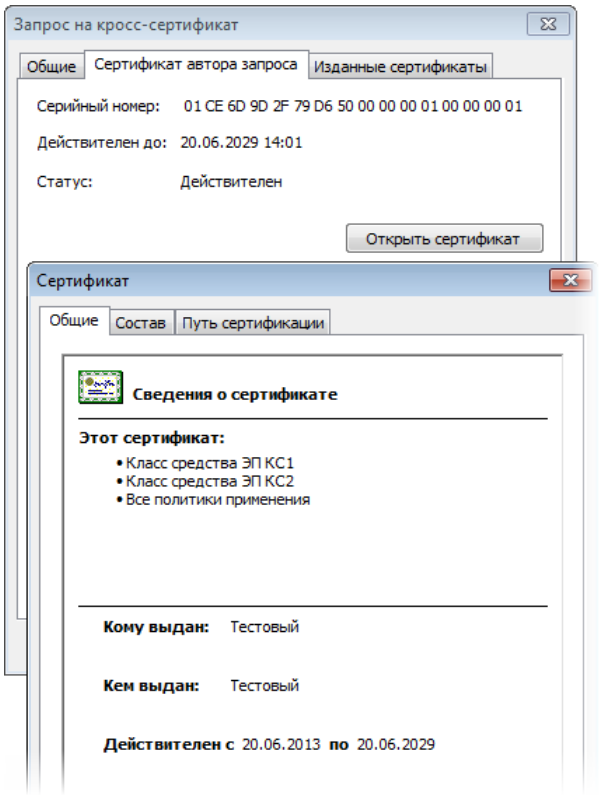

Рисунок 84. Просмотр параметров запроса на кросс-сертификат

Установление доверительных отношений с удостоверяющим центром Минцифры России

Если удостоверяющий центр, функции которого выполняет программа ViPNet Удостоверяющий и ключевой центр, на территории РФ планирует работать в качестве аккредитованного удостоверяющего центра (см. глоссарий, стр. 209), в процессе его аккредитации требуется установить доверительные отношения между ним и головным аккредитованным удостоверяющим центром, функции которого выполняет уполномоченный федеральный орган. Аккредитованный удостоверяющий центр для подписания от своего имени квалифицированных сертификатов обязан использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром. Аккредитованному удостоверяющему центру запрещается использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, для подписания сертификатов, не являющихся квалифицированными сертификатами.

Чтобы установить доверительные отношения с головным аккредитованным УЦ:

1. Для администратора программы ViPNet Удостоверяющий и ключевой центр сформируйте запрос на сертификат к вышестоящему УЦ (см. Создание запроса на сертификат к вышестоящему удостоверяющему центру на стр. 122).
2. Передайте сформированный запрос администратору головного аккредитованного УЦ.
3. Получите от администратора головного аккредитованного УЦ подчиненный сертификат, который он издал по вашему запросу, а также сертификат издателя, которым заверен ваш подчиненный сертификат, и соответствующий список аннулированных сертификатов (CRL). Сертификат издателя и соответствующий список аннулированных сертификатов при аккредитации и при смене сертификата издателя должны передаваться доверенным образом.
4. Импортируйте в УКЦ сертификат издателя и CRL, полученные от администратора головного аккредитованного УЦ. Подробнее см. разделы Импорт сертификатов администраторов, полученных из вышестоящего удостоверяющего центра (на стр. 124) и Импорт списков аннулированных сертификатов, полученных из вышестоящего удостоверяющего центра (на стр. 126).
5. Импортируйте в УКЦ подчиненный сертификат, изданный для вас в головном аккредитованном УЦ (см. Импорт сертификата, выданного вышестоящим удостоверяющим центром на стр. 127). Этот сертификат автоматически будет назначен вашим текущим сертификатом.

   После этого вы можете издавать для пользователей квалифицированные сертификаты.

8

Работа с данными администратора программы ViPNet Удостоверяющий и ключевой центр

Управление учетной записью администратора

Отказ от использования нескольких учетных записей администратора

Начиная с версии 4.0, в программе ViPNet Удостоверяющий и ключевой центр можно использовать только одну учетную запись администратора, создание дополнительных учетных записей невозможно. Если в вашей сети ранее были созданы несколько учетных записей администраторов УКЦ, то при переходе на версию 4.0 и выше они продолжат нормально функционировать. Однако мы настоятельно рекомендуем оставить среди них только одну учетную запись для администрирования УКЦ, а остальные учетные записи — удалить (см. Удаление учетной записи администратора на стр. 141). Использование нескольких учетных записей администраторов программы ViPNet Удостоверяющий и ключевой центр не рекомендуется по следующим соображениям:

- С увеличением количества администраторов повышается сложность надежного хранения сертификатов и ключей электронной подписи этих администраторов. В случае утери ключа электронной подписи одного из администраторов или удаления его учетной записи будет потеряно доверие ко всей цепочке сертификатов, изданных с использованием сертификата этого администратора. Аннулирование, проверка, обновление сертификатов пользователей будут невозможны.
- Организационно усложняется процедура обновления списков аннулированных сертификатов (CRL). Для обновления CRL необходимо физическое присутствие администратора, сертификату которого соответствует данный CRL. Если администратор по тем или иным причинам недоступен (отпуск, болезнь), другой администратор с его ведома должен войти в УКЦ с использованием пароля отсутствующего администратора и обновить CRL. Однако передача собственной конфиденциальной информации крайне нежелательна из соображений безопасности.
- При наличии нескольких учетных записей администратора УКЦ и, соответственно, нескольких CRL у каждого CRL после его публикации на внешней точке доступа будет собственный адрес. Собственный адрес необходим, поскольку для проверки разных сертификатов пользователей нужно скачивать разные CRL.

Удаление учетной записи администратора

Если в вашей сети есть несколько учетных записей администраторов, которые были созданы в УКЦ еще до перехода на версию 4.0 и выше, то настоятельно рекомендуется оставить только одну учетную запись, остальные записи следует удалить.

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

В процессе удаления учетной записи администратора требуется перевыпустить сертификаты пользователей, которые были изданы этим администратором (если срок действия сертификатов этого администратора еще не истек). Потому что после удаления учетной записи будет невозможно обновить списки аннулированных сертификатов (CRL) (см. глоссарий, стр. 217), соответствующих действующим сертификатам подписи этого администратора. Отсутствие актуальных CRL, в свою очередь, приведет к тому, что на узлах сети будет невозможно проверить сертификаты пользователей, выданные этим администратором.

Чтобы удалить учетную запись администратора:

1. В окне программы выберите представление **Администрирование** и перейдите в раздел **Моя сеть** > **Администраторы**.
2. Щелкните учетную 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**.
5. Издайте новые сертификаты пользователей на смену сертификатам, которые были изданы администратором с удаленной учетной записью. Изданные сертификаты должны быть заверены вашим действующим сертификатом подписи (см. Издание сертификатов на стр. 43).
6. 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. 159).

Смена текущей учетной записи администратора

Под текущей учетной записью администратора понимается учетная запись администратора, сертификатом которого подписываются издаваемые в данный момент сертификаты пользователей. Учетная запись, которая используется для входа в программу ViPNet Удостоверяющий и ключевой центр, становится текущей (см. Запуск и завершение работы программы на стр. 24). Если в вашей сети есть несколько учетных записей администраторов, которые были созданы в УКЦ еще до перехода на версию 4.0 и выше, вы можете сменить текущую учетную запись непосредственно в самом сеансе работы с программой (см. ниже).

Внимание! В силу сложности организационных мер по поддержанию работоспособности системы доверительных отношений не рекомендуется использовать в программе ViPNet Удостоверяющий и ключевой центр более одной учетной записи администратора программы (см. Отказ от использования нескольких учетных записей администратора на стр. 141).

Только одна учетная запись из имеющихся может являться текущей. Список зарегистрированных учетных записей администраторов содержится в представлении **Администрирование** в разделе **Моя сеть** > **Администраторы**. Текущая учетная запись администратора в списке обозначена значком , остальные учетные записи — значком .

Если в УКЦ зарегистрировано несколько учетных записей администраторов, вы можете сменить текущую учетную запись (текущего администратора), не выходя из программы. Для этого:

1 В окне программы в меню **УКЦ** выберите пункт **Сменить администратора**.

2 В окне с сообщением о необходимости завершить текущий сеанс работы нажмите кнопку **Да**.

3 В появившемся окне выберите учетную запись администратора, под которой будет производиться вход в программу, и введите пароль (см. глоссарий, стр. 215).

Внимание! Если вы 3 раза ввели неправильный пароль, то дальнейший ввод пароля будет возможен по истечении 40 секунд.

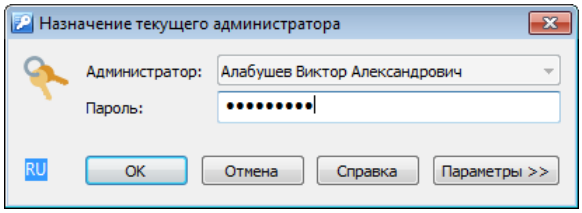

Рисунок 85. Смена текущей учетной записи

4 Укажите место хранения ключей администратора (см. глоссарий, стр. 212) 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. Внешние устройства на стр. 183). 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.

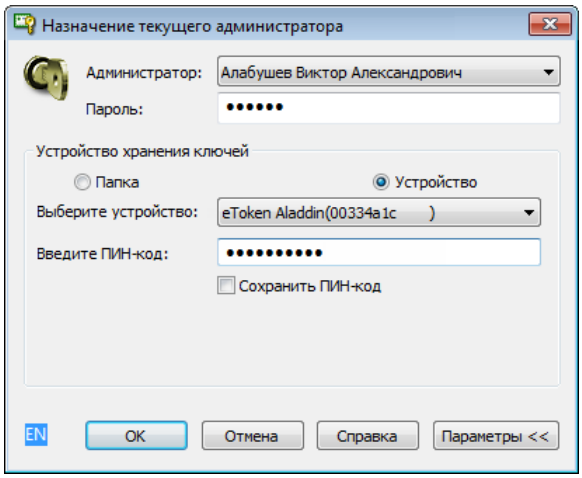

Рисунок 86. Смена текущей учетной записи с указанием места хранения ключей

5 После ввода необходимых для аутентификации данных нажмите кнопку **OK**.

В результате произойдет смена текущей учетной записи администратора, и все операции в программе будут осуществляться от имени администратора с текущей учетной записью.

Просмотр и изменение данных об администраторе

Для просмотра или изменения информации об администраторах программы ViPNet Удостоверяющий и ключевой центр:

1. В окне программы выберите представление **Администрирование** и перейдите в раздел **Моя сеть** > **Администраторы**.
2. В списке на панели просмотра дважды щелкните учетную запись администратора либо в контекстном меню учетной записи выберите пункт **Открыть**.
3. В окне просмотра свойств администратора ознакомьтесь с информацией на следующих вкладках:
   - **Общие** — указано имя администратора. На вкладке также имеется кнопка смены пароля (см. Смена пароля администратора на стр. 157) и кнопка смены ключа защиты УКЦ (см. Смена ключа защиты УКЦ на стр. 159).
   - **Текущий сертификат** — содержатся сведения о текущем сертификате администратора (сертификате, которым заверяются издаваемые сертификаты пользователей), сроке плановой смены ключа электронной подписи, размещении контейнера ключей (см. глоссарий, стр. 213).

     С помощью кнопок **Подробнее** вы можете узнать подробную информацию о текущем сертификате администратора (см. Просмотр сертификатов на стр. 84) и просмотреть свойства контейнера ключей (см. Просмотр контейнера ключей подписи администратора на стр. 156).

Примечание. Если в программе зарегистрировано несколько администраторов, то вкладка **Текущий сертификат** отображается только в том случае, если открыты свойства администратора, учетная запись которого является текущей (см. Смена текущей учетной записи администратора на стр. 142).

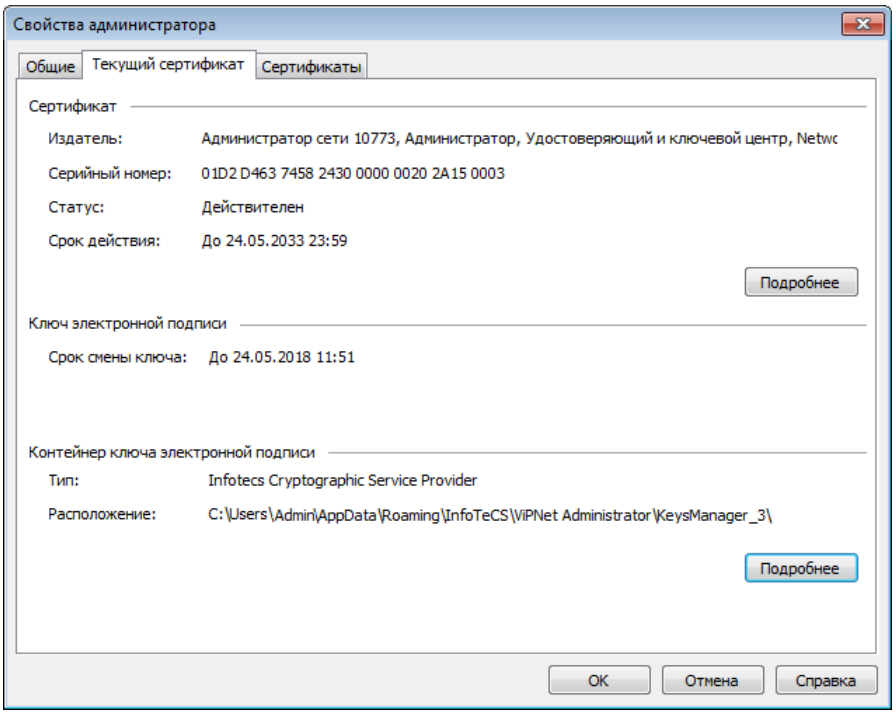

Рисунок 87. Просмотр сведений о текущем сертификате администратора

4 Чтобы изменить имя учетной записи администратора, на вкладке **Общие** в поле **Имя** введите новое имя, которое будет использоваться для входа в программу УКЦ, и нажмите кнопку **OK**.

Для отображения списка всех сертификатов и выбора текущего сертификата администратора перейдите на вкладку **Сертификаты** (см. Выбор текущего сертификата администратора (на стр. 153)).

Управление ключами электронной подписи и сертификатом администратора

Издание сертификата администратора

Издание сертификата администратора производится автоматически при первичной инициализации (см. Установка и первичная инициализация программы ViPNet Удостоверяющий и ключевой центр на стр. 23). Вы также можете вручную издать новый сертификат администратора УКЦ, например, при плановой смене ключа электронной подписи текущего сертификата администратора. Вручную издавать сертификаты администраторов целесообразно в том случае, если ваш удостоверяющий центр не является подчиненным. В противном случае изданные сертификаты нельзя будет использовать для подписи сертификатов пользователей.

Внимание! Как правило, издание сертификатов администраторов должно определяться регламентом работы удостоверяющего центра вашей организации.

В процессе издания сертификата формируется ключ электронной подписи. По истечении срока плановой смены ключ электронной подписи не сможет быть использован для подписи издаваемых сертификатов пользователей. Подпись списка аннулированных сертификатов (CRL) данным ключом электронной подписи при этом будет возможна в течение срока действия ключа электронной подписи. Срок действия ключа электронной подписи зависит от места его хранения.

В сертификате администратора отсутствует расширение «**Срок действия закрытого ключа**», если он издается на срок меньше, чем допустимый срок действия ключа электронной подписи (см. Плановая смена ключа электронной подписи и сертификата администратора на стр. 154) — 3 года при хранении на устройстве с аппаратной поддержкой российских криптографических алгоритмов. Срок действия ключа в данном случае будет равен сроку действия сертификата. CRL обновляется в течение всего срока действия сертификата. После того, как срок действия сертификата администратора истек, CRL будет удален.

В сертификате администратора будет расширение «Срок действия закрытого ключа», если он издается на срок равный или больше допустимого срока действия ключа электронной подписи. В данном случае CRL обновляется в течение срока действия ключа электронной подписи. После того, как истечет срок действия ключа электронной подписи, статус CRL будет отображен как **Действителен (текущий, финальный)**. При этом в УКЦ будет запрещено отзывать сертификаты пользователей. После истечения срока действия сертификата CRL будет удален. Таким образом, CRL своевременно удаляются из УКЦ по истечении допустимого срока действия ключа электронной подписи.

Издать сертификат можно только для администратора, учетная запись которого является текущей (см. Смена текущей учетной записи администратора на стр. 142).

Совет. Если требуется, чтобы сертификат администратора имел формат квалифицированного сертификата, то перед его изданием необходимо выполнить ряд дополнительных настроек программы (см. Издание квалифицированных сертификатов на стр. 70).

Кроме этого, в настройках программы вы можете предварительно задать срок, на который должен быть издан сертификат администратора. Как правило, данная настройка полезна в том случае, если при издании сертификата администратора вы не планируете редактирование параметров на страницах мастера. Чтобы задать срок действия сертификата администратора, в настройках программы перейдите в раздел **Срок действия**, в котором в группе **Сертификаты и ключи администраторов** в поле **Срок действия сертификата** укажите срок (в месяцах). Срок не может превышать 192 месяца (16 лет).

Для издания сертификата администратора:

1 В окне программы выберите представление **Администрирование** и перейдите в раздел **Моя сеть** > **Администраторы**.

2 Щелкните имя своей учетной записи правой кнопкой мыши и в контекстном меню выберите **Создать корневой сертификат**.

Появится электронная рулетка, если она еще не запускалась в рамках текущего сеанса работы программы. Поводите указателем в пределах окна **Электронная рулетка**.

3 На первых страницах мастера **Сведения о владельце сертификата** укажите имя администратора и другие необходимые данные, которые впоследствии будут добавлены в его сертификат, и нажмите кнопку **Далее**.

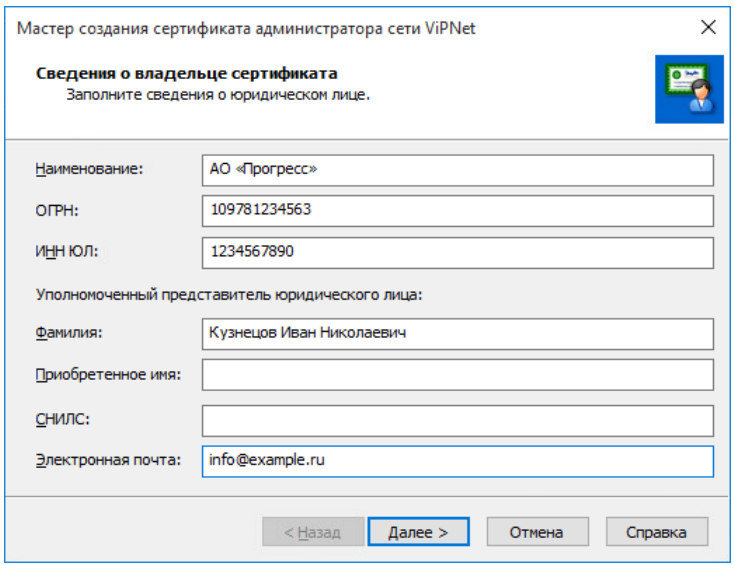

Рисунок 88. Указание сведений об администраторе, для которого создается сертификат

4 На странице **Дополнительные сведения о владельце сертификата** при необходимости отредактируйте дополнительные сведения о владельце. Для этого в списке выберите

соответствующие атрибуты, нажмите кнопку **Изменить** и внесите необходимую информацию. Затем нажмите кнопку **Далее**.

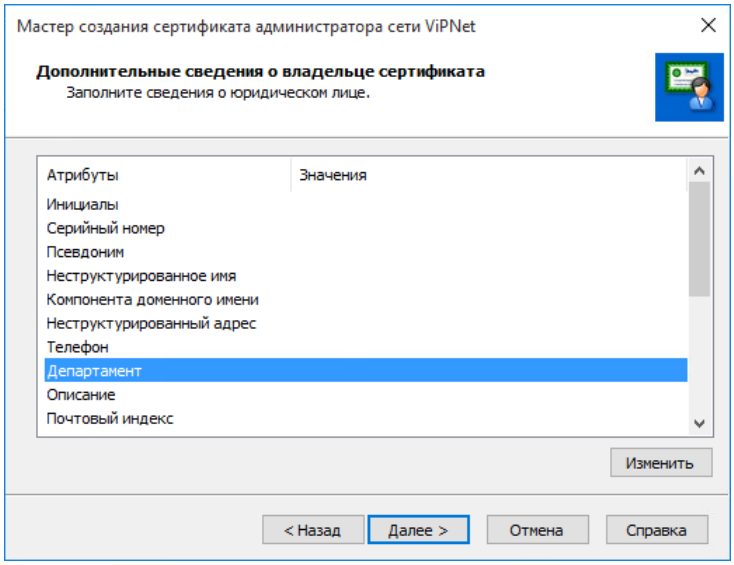

Рисунок 89. Указание дополнительных сведений об администраторе, для которого создается сертификат

5 На странице **Параметры ключа электронной подписи** выберите криптопровайдер, установленный на компьютере. Выбранный криптопровайдер определит алгоритм подписи, по которому будет создаваться ключ электронной подписи и ключ проверки электронной подписи и вычисляться хэш-функция.

Кроме этого, укажите параметры алгоритма подписи. В соответствии с заданными параметрами будет автоматически определена длина ключа проверки электронной подписи и алгоритм хэширования.
Характеристики ViPNet CSP и алгоритмов электронной подписи см. в документе «ViPNet CSP 4.4. Руководство пользователя».

Совет. Рекомендуется использовать параметры алгоритма, предлагаемые по умолчанию. Данные параметры характеризуются наибольшей скоростью вычисления и проверки электронной подписи.

Нажмите кнопку **Далее**.

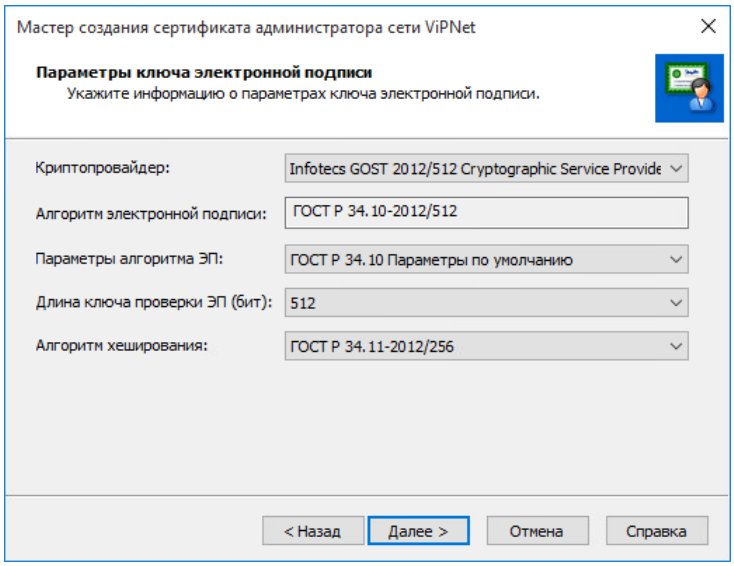

Рисунок 90. Настройка параметров ключа электронной подписи

6 На странице **Место хранения контейнера ключей** укажите место хранения контейнера ключей: **На внешнем устройстве**. Нажмите кнопку **Далее**.

Подключите внешнее устройство к компьютеру и выберите его на странице **Место хранения контейнеров ключа электронной подписи и ключа защиты УКЦ**. Если требуется, введите ПИН-код. После этого нажмите кнопку **Далее**.

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 Внешние устройства (на стр. 183).

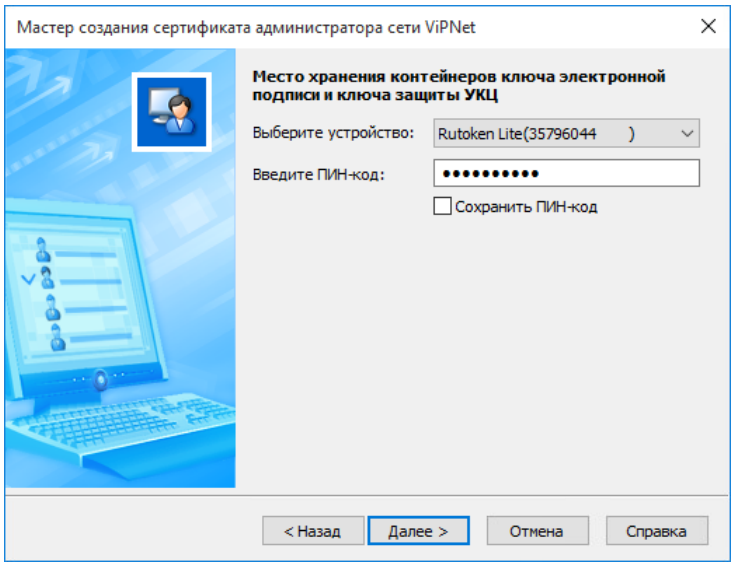

Рисунок 91. Выбор внешнего устройства

При хранении ключа электронной подписи на устройстве с аппаратной поддержкой ГОСТ Р 34.10-2012 (был непосредственно сформирован на нем) смена ключа должна производиться каждые 3 года, период действия ключа электронной подписи для обновления CRL составляет 36 месяцев.

Место хранения и срок плановой смены ключа электронной подписи должны быть зафиксированы в регламенте работы удостоверяющего центра.

7 На странице **Срок действия сертификата** задайте срок действия сертификата администратора, после чего нажмите кнопку **Далее**. Если вы предварительно задавали срок действия сертификата администратора в настройках программы, то редактирование параметров на данной странице мастера вы можете пропустить.

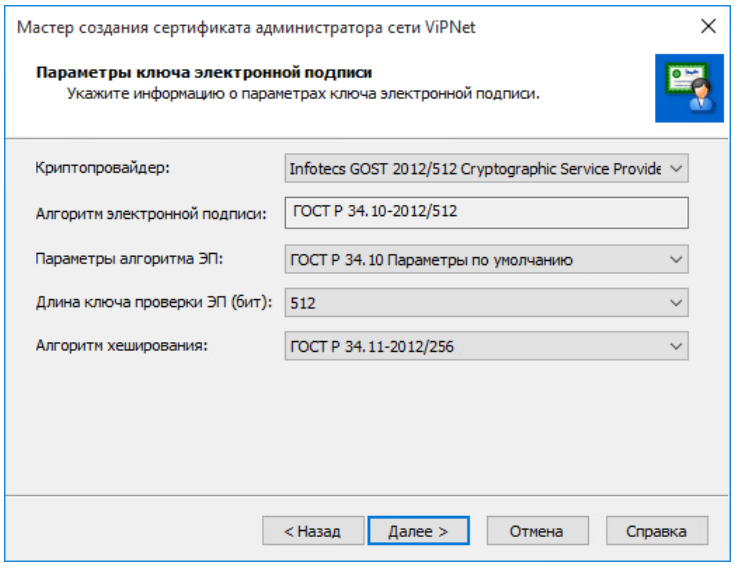

Рисунок 92. Задание срока действия сертификата администратора

8 На странице **Назначение сертификата** укажите ограничения, расширения и политики применения издаваемого сертификата и нажмите кнопку **Далее**. Данные сведения формируются так же, как и при издании обычного сертификата пользователя (см. Издание сертификатов пользователей сети ViPNet по инициативе администратора УКЦ на стр. 45).

Примечание. При издании сертификата администратора вы не можете редактировать расширение «Использование ключа».

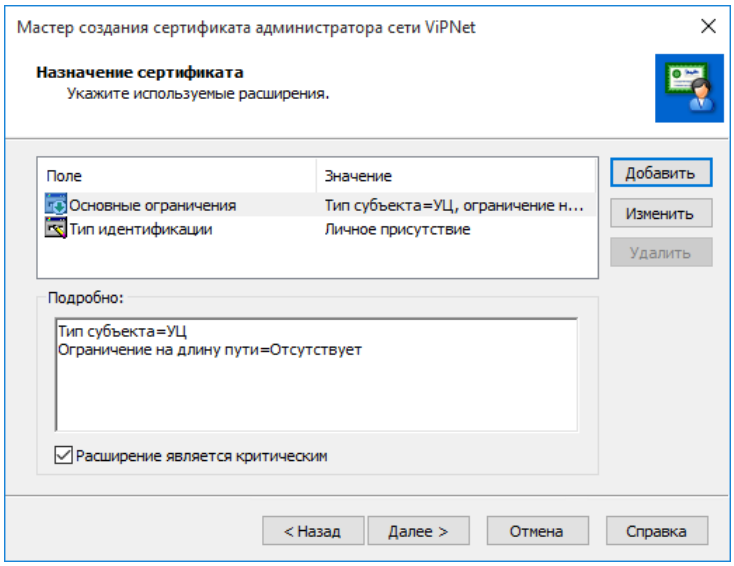

Рисунок 93. Указание расширений издаваемого сертификата администратора

9 Если требуется, на странице **Сведения о точках распространения** создайте точку распространения (см. глоссарий, стр. 217) для издаваемого сертификата или для списка аннулированных сертификатов (CRL), который будет сформирован после издания сертификата. Информация о созданных точках будет помещаться в сертификаты пользователей, заверенные данным сертификатом администратора. Кроме этого, заданные точки будут перенесены в настройки программы. Задать или изменить их вы можете в настройках программы (см. Настройка списка точек распространения на стр. 113).

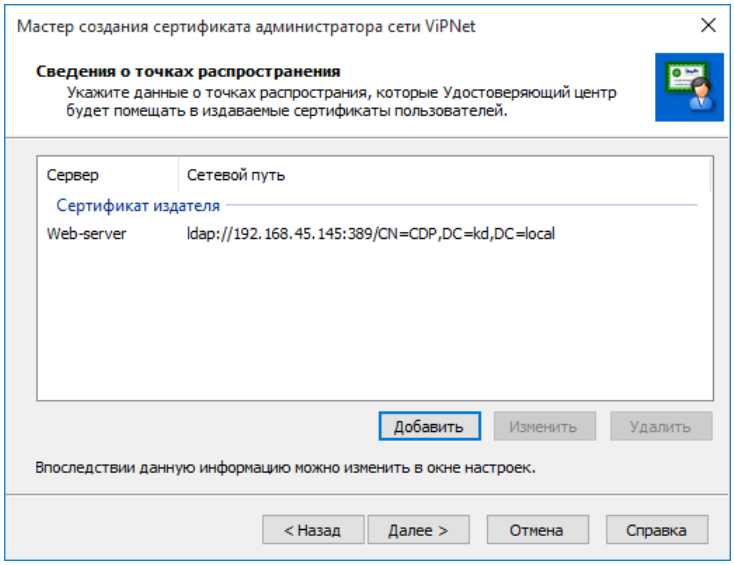

Рисунок 94. Указание точек распространения

На странице готовности к изданию сертификата убедитесь в правильности параметров, заданных на предыдущих страницах мастера, и нажмите кнопку **Далее**. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.

10 На последней странице мастера ознакомьтесь с результатом издания сертификата, после чего нажмите кнопку **Готово**. После издания сертификата будет автоматически произведены

экспорт межсетевой информации (см. руководство администратора на УКЦ) и передача CRL на узлы вашей сети (см. руководство администратора на УКЦ).

При успешном издании сертификата 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  .

Если в УКЦ установлены доверительные отношения с каким-либо другим удостоверяющим центром на основе распределенной модели, то после издания сертификата администратора УКЦ необходимо, чтобы в удостоверяющем центре, с которым установлены доверительные отношения, был издан новый сертификат, выданный вышестоящим УЦ (подробнее см. раздел Создание запроса на кросс-сертификат (на стр. 131)).

Выбор текущего сертификата администратора

Если у вас имеется несколько ключей электронной подписи и соответственно несколько сертификатов ключа проверки электронной подписи, то в каждый момент времени только один из имеющихся ключей и сертификатов может являться текущим и использоваться для подписи издаваемых сертификатов пользователей. В программе ViPNet Удостоверяющий и ключевой центр можно просмотреть список всех сертификатов (см. ниже) и изменить текущий сертификат. При назначении сертификата текущим ключ электронной подписи, которому он соответствует, также назначается текущим.

Выбирать текущий сертификат может только администратор, учетная запись которого является текущей (см. Смена текущей учетной записи администратора на стр. 142).

Для смены текущего сертификата:

1. В окне программы выберите представление **Администрирование** и перейдите в раздел **Изданные сертификаты** > **Корневые сертификаты** или **Кросс-сертификация** > **Сертификаты от вышестоящего УЦ**.
2. Щелкните нужный сертификат правой кнопкой мыши и в контекстном меню выберите пункт **Назначить текущим**.

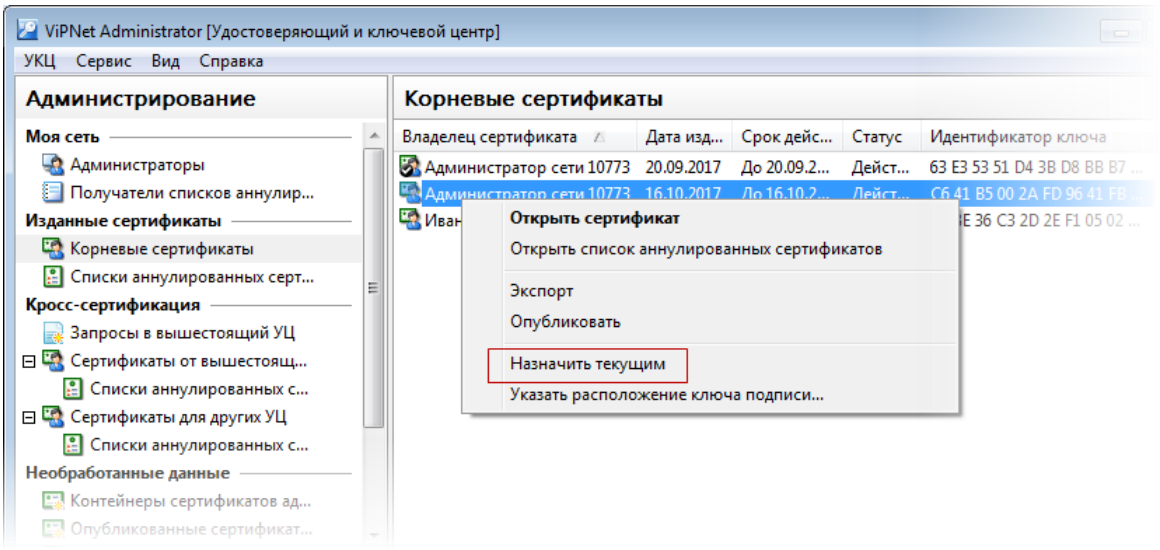

Рисунок 95. Выбор текущего сертификата администратора

Сертификат, назначенный текущим, будет использоваться для подписания сертификатов пользователей, издаваемых данным администратором. В разделе главного окна, в котором отображается данный сертификат, у него будет статус **Действителен (текущий)**.

Плановая смена ключа электронной подписи и сертификата администратора

Из соображений безопасности в процессе работы удостоверяющего центра проводится плановая смена ключа электронной подписи администратора. Срок плановой смены ключа электронной подписи при хранении ключа электронной подписи на устройстве с аппаратной поддержкой российских криптографических алгоритмов (был непосредственно сформирован на нем) составляет 18 месяцев.

По истечении срока плановой смены электронной подписи ключ электронной подписи администратора не сможет быть использован для подписи издаваемых сертификатов пользователей. Подписание списка аннулированных сертификатов (CRL) данным ключом электронной подписи при этом остается возможным до истечения срока действия ключа электронной подписи, а именно в течение следующих периодов:

- 36 месяцев, если корневой сертификат был издан на срок больше срока плановой смены ключа электронной подписи;
- срока действия сертификата администратора, если корневой сертификат был издан на срок равный или менее срока плановой смены ключа электронной подписи. Срок действия ключа электронной подписи в данном случае будет равен сроку действия сертификата.

Таблица 4. Срок плановой смены ключа электронной подписи администратора

Место хранения ключа электронной подписи	Срок плановой смены ключа электронной подписи	Срок действия ключа электронной подписи для обновления CRL
Устройство с аппаратной поддержкой российских криптографических алгоритмов	18 месяцев	36 месяцев

Узнать, в какие устройства встроена аппаратная поддержка криптографических алгоритмов, вы можете в разделе Список поддерживаемых внешних устройств.

Внимание! Место хранения ключа электронной подписи и срок его плановой смены должны быть зафиксированы в регламенте работы удостоверяющего центра вашей организации.

По истечении срока плановой смены ключа электронной подписи появится оповещение о необходимости проведения смены ключа электронной подписи. Количество дней, за которое будет произведено оповещение, задается в настройках программы. Требуется незамедлительно провести плановую смену ключа электронной подписи. Если смена ключа электронной подписи не будет своевременно проведена, издание сертификатов пользователей в программе будет невозможно.

Во время плановой смены требуется создать новый ключ электронной подписи и получить новый сертификат администратора одним из следующих способов:

- издать новый сертификат, если ваш удостоверяющий центр, в роли которого выступает УКЦ, является головным (см. глоссарий, стр. 210);
- получить новый сертификат по соответствующему запросу в вышестоящем удостоверяющем центре, если ваш удостоверяющий центр является подчиненным (см. глоссарий, стр. 216).

Настройка оповещений о плановой смене ключа электронной подписи и сертификата администратора

Для настройки оповещений о плановой смене ключа электронной подписи и сертификата администратора:

1. В окне программы в меню **Сервис** выберите пункт **Настройка**.
2. В появившемся окне на панели навигации выберите раздел **Сертификаты** > **Срок действия**.
3. В разделе **Срок действия** в группе **Сертификаты и ключи администраторов** в поле **Сообщать о плановой смене ключа ЭП за** введите количество дней (не более 30), за которое следует производить оповещение об истечении срока плановой смены ключа электронной подписи и сертификата администратора.

Примечание. Оповещение об истечении срока плановой смены ключа электронной подписи должно производиться за 15 дней.

4 Для сохранения указанных настроек нажмите кнопку **OK**.

Просмотр контейнера ключей подписи администратора

В процессе первичной инициализации, а также при каждом издании сертификата администратора или создании запроса на сертификат к вышестоящему удостоверяющему центру создается ключ электронной подписи, который помещается вместе с сертификатом в специальный контейнер ключей (см. глоссарий, стр. 213). В свою очередь, контейнер ключей сохраняется либо локально на компьютере (в заданной папке на диске), либо на внешнем устройстве хранения данных и является составной частью ключей администратора (см. глоссарий, стр. 212).

В программе ViPNet Удостоверяющий и ключевой центр вы можете просмотреть подробную информацию о контейнере ключей администратора: имя, место хранения (название внешнего устройства) и содержимое (сведения о ключе электронной подписи и сертификате ключа проверки электронной подписи). При наличии нескольких контейнеров ключей можно просмотреть информацию только о контейнере, в котором находится ключ электронной подписи, соответствующий его текущему сертификату (см. Выбор текущего сертификата администратора на стр. 153).

Для просмотра контейнера ключей текущего администратора:

1 В окне программы перейдите в представление **Администрирование** и выберите раздел **Моя сеть** > **Администраторы** и дважды щелкните свою учетную запись.

2 В окне **Свойства администратора** перейдите на вкладку **Текущий сертификат** и в группе **Контейнер ключа электронной подписи** нажмите кнопку **Подробнее**.

3 В появившемся окне **Свойства контейнера ключей** ознакомьтесь с содержимым контейнера ключей.

Внимание! Кроме просмотра содержимого, не производите никаких действий в данном окне.

Смена пароля администратора

В целях обеспечения безопасности рекомендуется менять пароль администратора программы ViPNet Удостоверяющий и ключевой центр каждые 6 месяцев. По истечении 6 месяцев после создания пароля администратора появится оповещение о необходимости смены пароля. Сменить пароль может только администратор, учетная запись которого является текущей (см. Смена текущей учетной записи администратора на стр. 142).

Чтобы сменить пароль администратора:

1. В окне программы выберите представление **Администрирование** и перейдите в раздел **Моя сеть** > **Администраторы**.
2. Выполните одно из действий:
   - В контекстном меню вашей учетной записи выберите пункт **Сменить пароль администратора**.
   - В контекстном меню вашей учетной записи выберите пункт **Открыть** и в окне просмотра свойств администратора на вкладке **Общие** нажмите кнопку **Сменить пароль**.
3. В окне **Смена пароля и ключа защиты администратора** укажите свой текущий пароль.
4. В группе **Новый пароль** задайте тип нового пароля:
   - **Собственный** — пароль, задаваемый вами вручную. Пароль данного типа должен включать в себя не менее 8 символов.
   - **На основе парольной фразы** — пароль, формируемый автоматически на основе парольных фраз (см. глоссарий, стр. 215) согласно параметрам, заданным в настройках программы (см. Настройка параметров случайных паролей на стр. 42).

   После этого в зависимости от выбранного типа пароля, выполните соответствующие действия:
   - Если вы выбрали тип пароля **Собственный**, задайте и подтвердите пароль.
   - Если вы выбрали тип пароля **На основе парольной фразы**, появится электронная рулетка, если она еще не запускалась в рамках текущего сеанса работы программы. Поводите указателем в пределах окна **Электронная рулетка**.

     Если вы выбрали тип пароля **На основе парольной фразы**, то появится автоматически сформированный пароль с парольной фразой, помогающей запомнить пароль.

     При необходимости измените параметры или длину случайного пароля на основе парольной фразы с помощью кнопки **Свойства**, после чего создайте другой пароль, нажав кнопку **Другой**.

Совет. Рекомендуется задавать сложные пароли, в состав которых входят буквы в разных регистрах, цифры и специальные символы.

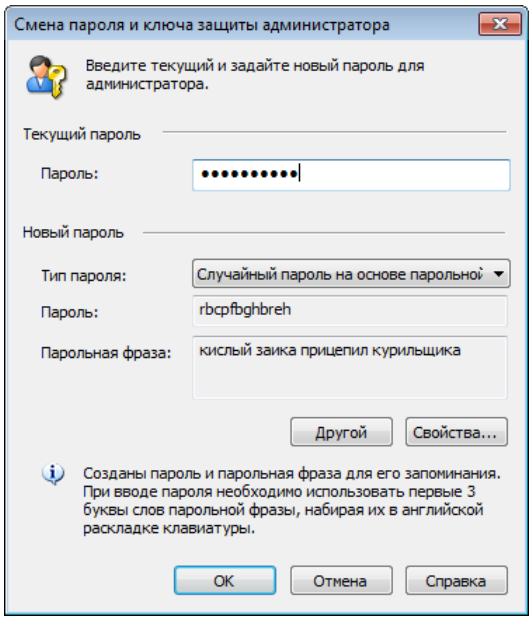

Рисунок 96. Смена пароля администратора

5 Для завершения смены пароля нажмите кнопку **OK**.

В результате ваш пароль будет изменен.

Внимание! Запомните новый пароль (парольную фразу). При утере данный пароль невозможно будет восстановить.

При следующей аутентификации используйте новый пароль.

Смена ключа защиты УКЦ

Вся информация, хранящаяся в программе ViPNet Удостоверяющий и ключевой центр, зашифрована на ключе защиты УКЦ (см. глоссарий, стр. 212). Данный ключ входит в состав ключей каждого администратора УКЦ, которые могут находиться в локальной папке или на внешнем устройстве. Ключ защиты УКЦ зашифрован на ключе защиты администратора.

Рекомендуется проводить плановую смену ключа защиты УКЦ не реже одного раза в 15 месяцев. По истечении 15 месяцев после создания ключа защиты УКЦ появится оповещение о необходимости его смены. Также рекомендуется менять ключ защиты УКЦ после удаления учетной записи администратора УКЦ (см. Удаление учетной записи администратора на стр. 141).

Перед сменой ключа защиты УКЦ автоматически создается резервная копия текущей конфигурации программы (см. Работа с резервными копиями конфигураций сети на стр. 162). С ее помощью можно будет восстановить работу УКЦ в случае, если смена ключа защиты будет проведена некорректно.

Внимание! Если база данных SQL и программа ViPNet Удостоверяющий и ключевой центр установлены на разных компьютерах, то резервная копия может быть создана только при соответствующей настройке программы (см. Настройка параметров создания резервных копий на стр. 167). В противном случае она не сможет быть создана. При этом если резервная копия не будет создана, смена ключа защиты УКЦ не будет выполнена.

Для смены ключа защиты УКЦ:

1 Выполните одно из действий:

- В окне программы в меню **УКЦ** выберите пункт **Сменить ключ защиты УКЦ**.
- В окне программы выберите представление **Администрирование** и перейдите в раздел **Моя сеть** > **Администраторы**. Затем в контекстном меню вашей учетной записи выберите пункт **Открыть** и в окне просмотра свойств администратора на вкладке **Общие** нажмите кнопку **Сменить ключ защиты УКЦ**.

2 В окне с сообщением о том, что будет создан новый ключ защиты УКЦ, нажмите кнопку **Продолжить**.

В результате будет запущен процесс смены ключа защиты. Дождитесь его завершения. Смена ключа защиты может занимать продолжительное время, поскольку в процессе смены производится перешифрование всей хранимой в УКЦ информации. Поэтому чем больше размер базы данных программы, тем больше времени займет смена ключа защиты УКЦ.

При успешной смене ключа защиты появится соответствующее сообщение.

Внимание! Если процесс смены ключа защиты не был завершен успешно, не выходите из программы и сразу выполните восстановление конфигурации из резервной копии, которая была автоматически сделана до смены ключа защиты (см. Восстановление конфигурации на стр. 165). В случае выхода из программы возобновить работу с ней будет невозможно.

Если с УКЦ работают несколько администраторов, сразу после смены ключа защиты УКЦ поочередно назначьте учетную запись каждого из них текущей (см. Смена текущей учетной записи администратора на стр. 142). При вводе пароля администратора в момент назначения учетной записи текущей новый ключ защиты УКЦ будет включен в состав ключей данного администратора и зашифрован на его ключе защиты, после чего станет для администратора доступным. Администраторы, для которых данное перешифрование не будет произведено, не смогут войти в программу.

9

Административные функции

Работа с резервными копиями конфигураций сети

В программе ViPNet Удостоверяющий и ключевой центр существует возможность создания резервных копий конфигурации сети, позволяющая при необходимости осуществлять возврат к более ранним конфигурациям.

В состав резервной копии конфигурации сети (файл `*.zip` или `*.rp`) входят следующие данные:

- Резервная копия базы данных ViPNet Administrator, в которой содержится информация о структуре сети ViPNet, сведения о лицензии, сертификатах и списках аннулированных сертификатов, изданных в УКЦ, и другие данные.
- Копия папки, в которой хранится служебная информация УКЦ: `C:\ProgramData\Infotecs\ViPNet Administrator\KC`.

Примечание. По требованиям безопасности в резервную копию конфигурации сети не включаются копии контейнеров ключей администраторов УКЦ. Резервные копии контейнеров ключей требуется создавать отдельно.

Также в резервную копию не включаются справочники и ключи узлов, при необходимости они могут быть созданы после восстановления конфигурации сети.

Резервные копии создаются на компьютере, на котором установлена база данных, но хранятся на компьютере с УКЦ. Если база данных и программа ViPNet Удостоверяющий и ключевой центр установлены на разных компьютерах, то созданная резервная копия автоматически перемещается на компьютер с УКЦ в папку по умолчанию `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore`. При необходимости вы можете изменить путь к этой папке (см. Изменение места хранения резервных копий, используемого по умолчанию на стр. 169). Чтобы обеспечить перенос резервных копий с одного компьютера на другой, необходимо в УКЦ настроить доступ к папке, в которую помещаются резервные копии на компьютере с базой данных (см. Настройка параметров создания резервных копий на стр. 167). В случае, если база данных установлена на одном компьютере с УКЦ, такая настройка не требуется.

Резервные копии могут создаваться двумя способами:

- Автоматически с определенной периодичностью согласно настройкам (см. Настройка параметров создания резервных копий на стр. 167). В этом случае при работе УКЦ в автоматическом режиме создание резервной копии конфигурации сети попадает в очередь автоматически выполняемых операций. Если администратор производит в программе какие-либо действия, за 30 секунд до создания резервной копии появится окно с сообщением, с помощью которого администратор при необходимости может отменить создание резервной копии, нажав кнопку **Отмена**.

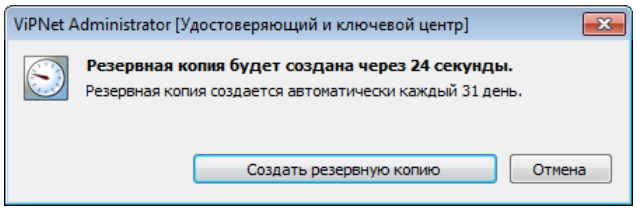

Рисунок 97. Сообщение о создании резервной копии конфигурации сети по расписанию

При смене ключа защиты УКЦ (см. Смена ключа защиты УКЦ на стр. 159) резервная копия всегда создается автоматически независимо от настроек программы.

- Вручную с использованием мастера восстановления конфигурации (см. Создание резервной копии текущей конфигурации на стр. 163). Таким способом рекомендуется создавать резервную копию каждый раз перед обновлением программного обеспечения ViPNet Administrator. Данную резервную копию можно будет использовать для восстановления конфигурации сети в случае нарушения ее работоспособности после обновления.

Внимание! Следует иметь в виду, что:

- Если резервная копия была создана в более поздней версии УКЦ по сравнению с установленной, эту резервную копию невозможно использовать для восстановления конфигурации сети.
- При удалении одной из учетных записей администратора рекомендуется сменить ключ защиты УКЦ и удалить те резервные копии, которые были созданы данным администратором.

Создание резервной копии текущей конфигурации

Резервная копия конфигурации создается для того, чтобы в случае необходимости можно было восстановить определенную конфигурацию сети.

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 Administrator в меню **Сервис** выберите пункт **Резервное копирование и восстановление**. Будет запущен мастер **Резервное копирование и восстановление конфигурации ViPNet Administrator**.
2. На странице **Резервное копирование и восстановление конфигурации ViPNet Administrator** выберите **Создать резервную копию текущей конфигурации**, затем нажмите кнопку **Далее**.

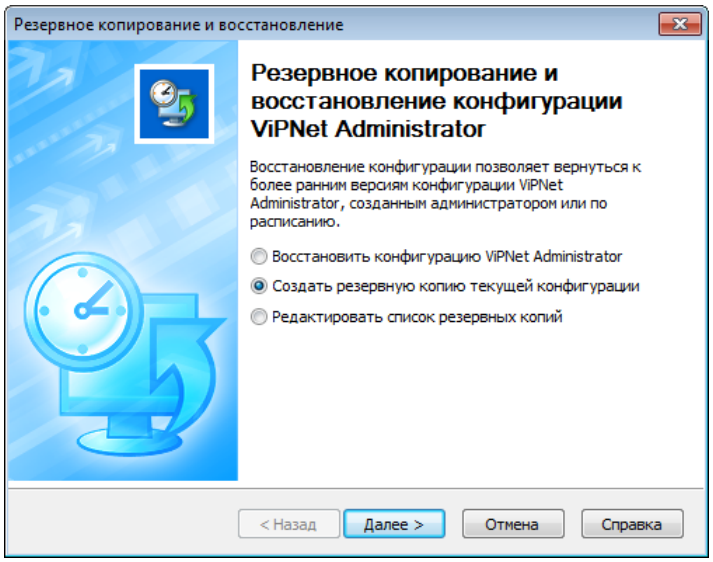

Рисунок 98. Запуск мастера создания и восстановления конфигурации

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.

4 Нажмите кнопку **Далее**. Будет создана резервная копия конфигурации.

Созданная резервная копия конфигурации будет сохранена на компьютере, на котором установлена программа ViPNet Удостоверяющий и ключевой центр, в папке по умолчанию `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore`.

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**.

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 Administrator в меню **Сервис** выберите пункт **Резервное копирование и восстановление**. Будет запущен мастер **Резервное копирование и восстановление конфигурации ViPNet Administrator**.

2 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 **Изменить 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**.

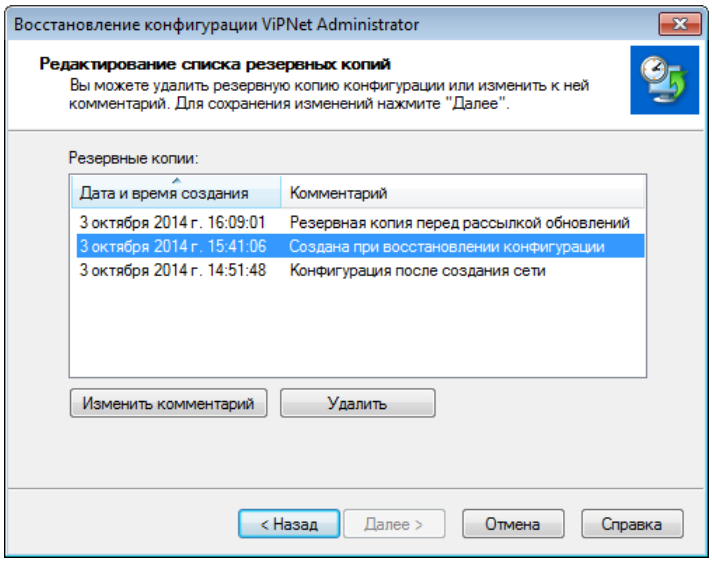

Рисунок 99. Редактирование списка резервных копий

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**.

Восстановление конфигурации

С помощью восстановления конфигурации вы можете вернуться к определенному состоянию сети ViPNet или восстановить работоспособность сети после сбоя. При восстановлении конфигурации сети выполняется также восстановление конфигурации программы ViPNet Удостоверяющий и ключевой центр.

В результате восстановления конфигурации структура сети ViPNet, параметры сетевых объектов, данные о ключах и сертификатах, настройки программы ViPNet Удостоверяющий и ключевой центр будут возвращены к состоянию, которое было актуально в момент создания резервной копии.

Чтобы восстановить конфигурацию из ранее созданной резервной копии:

1 В окне программы ViPNet Administrator в меню **Сервис** выберите пункт **Резервное копирование и восстановление**. Будет запущен мастер **Резервное копирование и восстановление конфигурации ViPNet Administrator**.

2 На странице **Резервное копирование и восстановление конфигурации ViPNet Administrator** выберите **Восстановить конфигурацию ViPNet Administrator**, затем нажмите кнопку **Далее**.

3 На странице **Выбор резервной копии** представлен список резервных копий конфигураций.

Резервные копии, созданные автоматически, могут иметь следующие комментарии:

- Создана при восстановлении конфигурации.
- Создана автоматически по расписанию.

Выберите резервную копию конфигурации, которую требуется восстановить, и нажмите кнопку **Далее**. Начнется процесс восстановления выбранной конфигурации сети.

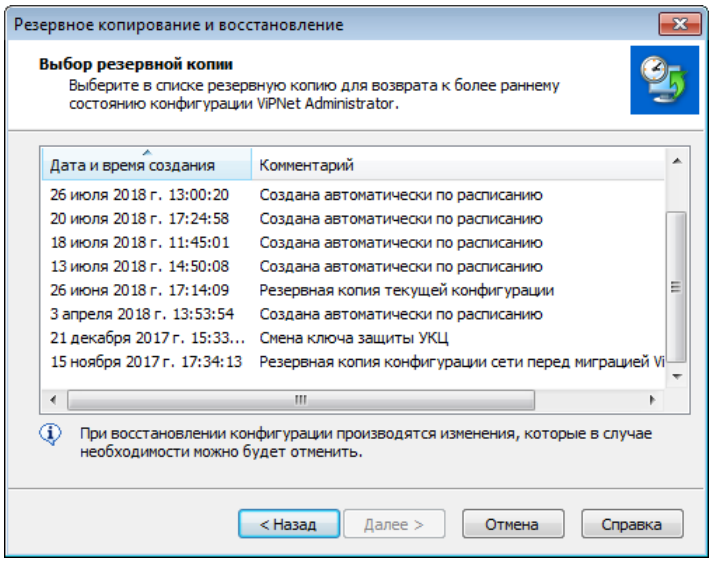

Рисунок 100. Восстановление конфигурации из резервной копии

4 Если база данных и УКЦ установлены на разных компьютерах, потребуется авторизация администратора SQL-сервера (подробнее см. в документе «ViPNet Administrator. Руководство по установке», в главе «Установка программного обеспечения ViPNet Administrator», в разделе «Информация для администратора SQL»). В появившемся окне укажите имя учетной записи и пароль администратора SQL-сервера. Иначе будет отказано в доступе к данным SQL-сервера и, следовательно, в доступе к базе данных ViPNet Administrator, и конфигурация не сможет быть восстановлена.

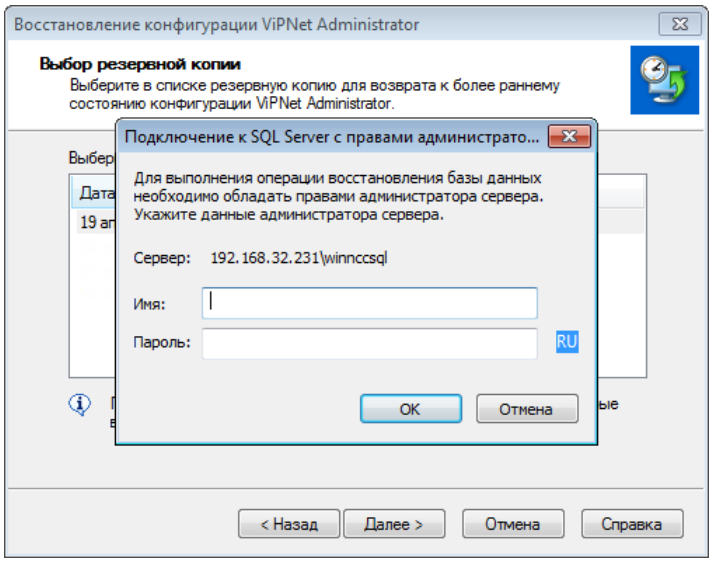

Рисунок 101. Ввод данных администратора SQL-сервера для получения доступа к базе данных ViPNet Administrator

5 Если база данных и УКЦ установлены на разных компьютерах и отсутствует доступ к данным SQL-сервера:

5.1 Для экземпляра SQL-сервера создайте учетную запись администратора с проверкой подлинности SQL Server и правами суперадминистратора sysadmin. Для работы с SQL-сервером вы можете использовать Microsoft SQL Server Management Studio.

5.2 Повторите подключение к базе данных с учетными данными созданного администратора SQL-сервера.

6 Чтобы закончить работу мастера, на странице **Завершение восстановления конфигурации ViPNet Administrator** нажмите кнопку **Закрыть**.

7 После восстановления конфигурации войдите в программу и убедитесь, что восстановленная конфигурация работоспособна. В случае необходимости вы можете отменить восстановление конфигурации.

8 После успешного восстановления конфигурации сети из резервной копии отправьте на сетевые узлы ключи узлов (см. глоссарий, стр. 213) и пользователей (см. глоссарий, стр. 212).

В том случае если в процессе работы с программой изменялось местоположение или имя папок обмена с программой ViPNet Publication Service, после восстановления конфигурации следует проверить, правильно ли заданы параметры взаимодействия с программой ViPNet Publication Service (см. Настройка параметров публикации данных на стр. 112).

Настройка параметров создания резервных копий

Вы можете настроить автоматическое создание резервных копий конфигурации с определенной периодичностью в заданное время. При переходе УКЦ в автоматический режим создание

резервных копий конфигурации будет включено в список выполняемых операций в этом режиме. При выходе из программы УКЦ автоматическое создание резервных копий конфигурации не будет выполняться.

Кроме того, если база данных и программа ViPNet Удостоверяющий и ключевой центр установлены на разных компьютерах, для возможности получения резервных копий конфигурации вам необходимо настроить доступ к папке на компьютере с базой данных, в которой будет размещаться резервная копия базы данных. Эта папка используется программой УКЦ для переноса резервных копий с компьютера с базой данных на компьютер с УКЦ при создании и восстановлении резервных копий конфигурации.

Чтобы настроить указанные параметры создания резервных копий конфигурации:

1 В окне программы в меню **Сервис** выберите пункт **Настройка**.

2 В появившемся окне на панели навигации выберите раздел **Резервное копирование**.

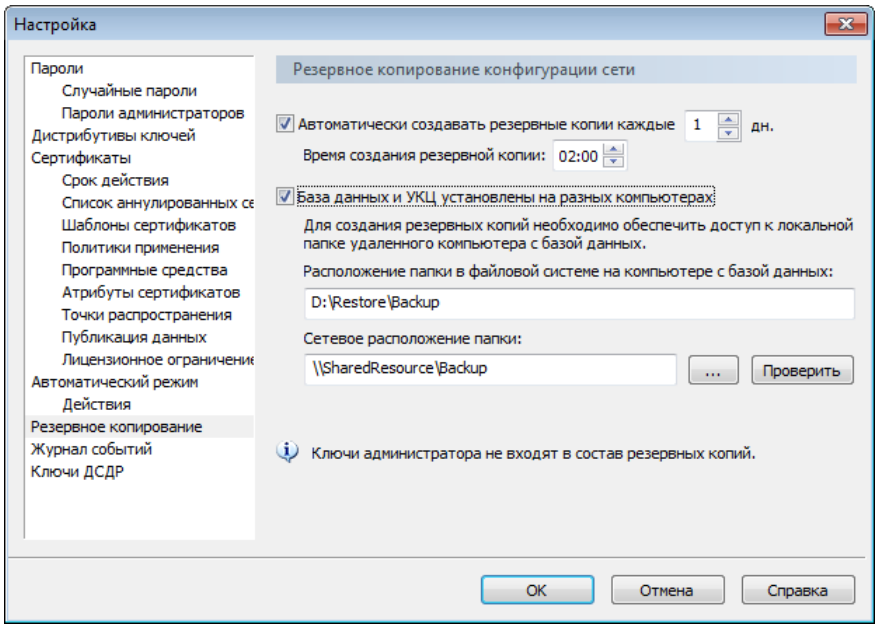

Рисунок 102. Настройка параметров восстановления конфигурации

3 Чтобы создание резервных копий выполнялось с определенной периодичностью в заданное время, укажите соответствующие значения в полях **Автоматически создавать резервные копии каждые** и **Время создания резервной копии**. По умолчанию резервные копии создаются ежедневно в 2 часа ночи.

Чтобы отключить автоматическое создание резервных копий, снимите соответствующий флажок.

4 Если база данных расположена на отдельном компьютере, установите флажок **База данных и УКЦ установлены на разных компьютерах** и укажите:

4.1 В поле **Расположение папки в файловой системе на компьютере с базой данных** укажите полный путь к общей папке на компьютере с базой данных ПО ViPNet Administrator. Например, `D:\Restore\Backup`.

4.2 В поле **Сетевое расположение папки** обеспечьте сетевой доступ к общей папке на компьютере с базой данных ПО ViPNet Administrator одним из двух способов:

- укажите сетевой путь в следующем формате: `\\<Имя сервера>\<Имя общей папки>`, где

  `<Имя сервера>` — имя в WINS или DNS-имя (предпочтительнее), или IP-адрес компьютера с базой данных ПО ViPNet Administrator;

  `<Имя общей папки>` — название общей папки на компьютере с базой данных ПО ViPNet Administrator.

  Например, `\\SharedResource\Backup`. Имя общей папки (например, Backup) может отличаться от полного пути на компьютере (например, `D:\Restore\Backup`).

- укажите букву сетевого диска, по которому подключена к компьютеру с УКЦ общая папка компьютера с базой данных ПО ViPNet Administrator, например, `Z:\`. Вы можете указать сетевой диск с помощью кнопки  .

Чтобы убедиться, что папка задана верно, нажмите кнопку **Проверить**.

Примечание. Общая папка задана верно, только если она существует и у вас есть права на чтение и запись данных в эту папку.

---

5 Для сохранения настроек нажмите кнопку **ОК**.

Если база данных и УКЦ расположены на одном компьютере, флажок **База данных и УКЦ установлены на разных компьютерах** должен быть снят, в этом случае резервные копии конфигурации сети сохраняются в папку по умолчанию `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore`. При необходимости вы можете изменить папку сохранения резервных копий на компьютере (см. Изменение места хранения резервных копий, используемого по умолчанию на стр. 169).

Изменение места хранения резервных копий, используемого по умолчанию

Резервные копии конфигурации сети могут занимать большой объем на диске `C:`, особенно если копии создаются автоматически с большой периодичностью. В этом случае вы можете изменить место хранения резервных копий конфигурации сети по умолчанию `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore`.

Чтобы изменить место хранения файлов резервных копий конфигурации сети, используемого по умолчанию:

1 Откройте для редактирования файл конфигурации УКЦ `KC.ini`, который находится в папке `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\ini`.

2 В секции `[Archive]` добавьте следующую строку:

```
Configuration backup folder=<Локальный путь к папке сохранения резервных копий>.
```

3 Чтобы все текущие резервные копии конфигурации сети были доступны для восстановления по новому пути, перенесите все содержимое папки автоматического сохранения резервных копий конфигурации сети `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore` в папку сохранения резервных копий по новому пути.

4 Чтобы применить изменения, перезапустите программу ViPNet Удостоверяющий и ключевой центр.

Работа с журналом событий

Информация о событиях, возникающих при работе программы ViPNet Удостоверяющий и ключевой центр, фиксируется в журнале событий, который находится в системном журнале Windows. Настройка журнала событий описана в разделе Настройка параметров журнала событий (на стр. 172).

Просмотр событий в журнале событий

Для мониторинга работы ViPNet Удостоверяющий и ключевой центр:

1 На **Панели управления** в категории **Администрирование** дважды щелкните значок **Просмотр событий**.

2 В окне **Просмотр событий** на панели навигации выберите **Журналы приложений и служб** > **ViPNet Administrator KCA**.

В результате на панели просмотра отобразится список зарегистрированных событий.

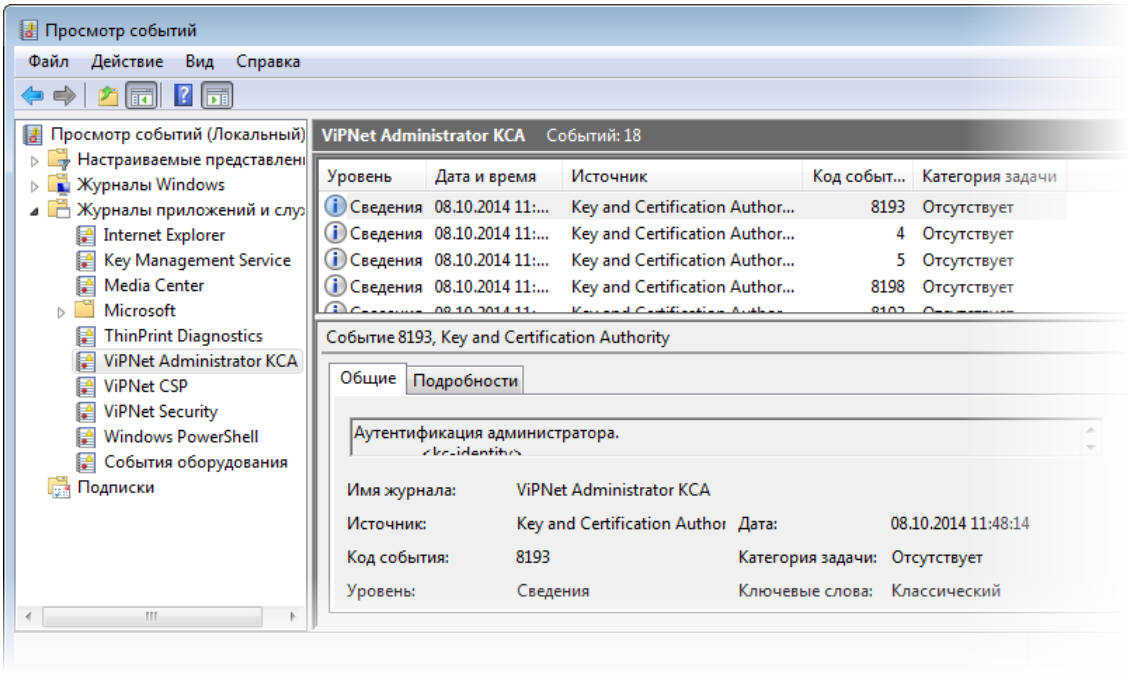

Рисунок 103. Просмотр событий в системном журнале событий УКЦ

Настройка параметров журнала событий

По умолчанию в журнале событий фиксируется наиболее важная информация о работе программы ViPNet Удостоверяющий и ключевой центр (издание сертификата подписи, издание списка аннулированных сертификатов, удовлетворение либо отклонение запроса на сертификат или его аннулирование и другое). В программе ViPNet Удостоверяющий и ключевой центр вы можете изменить степень детализации записей журнала либо отключить ведение журнала, если нет необходимости в мониторинге работы программы. Параметры хранения файла журнала событий настраиваются с помощью компонента Microsoft Windows Панель управления.

Для настройки параметров хранения файла журнала событий:

1. Нажмите кнопку **Пуск** и выберите пункт **Панель управления**.
2. На панели управления в категории **Администрирование** дважды щелкните значок **Просмотр событий**.
3. В окне **Просмотр событий** на панели навигации выберите **Журналы приложений и служб** > **ViPNet Administrator KCA**, щелкните **ViPNet Administrator KCA** правой кнопкой мыши и в меню выберите пункт **Свойства**.
4. В окне свойств журнала при необходимости измените:
   - Путь к папке для хранения и имя файла журнала.
   - Максимальный размер файла журнала (по умолчанию — 300 Мбайт).
   - Действие при достижении максимального размера файла журнала:
     - **Переписывать события при необходимости (сначала старые события)** — новые записи заносятся в журнал, при этом каждая новая запись заменяет в журнале наиболее старую.
     - **Архивировать журнал при заполнении; не перезаписывать события** (выбран по умолчанию) — файл журнала автоматически архивируется и сохраняется в папку, выбранную для хранения журнала.
     - **Не перезаписывать события (очистить журнал вручную)** — журнал очищается вручную.

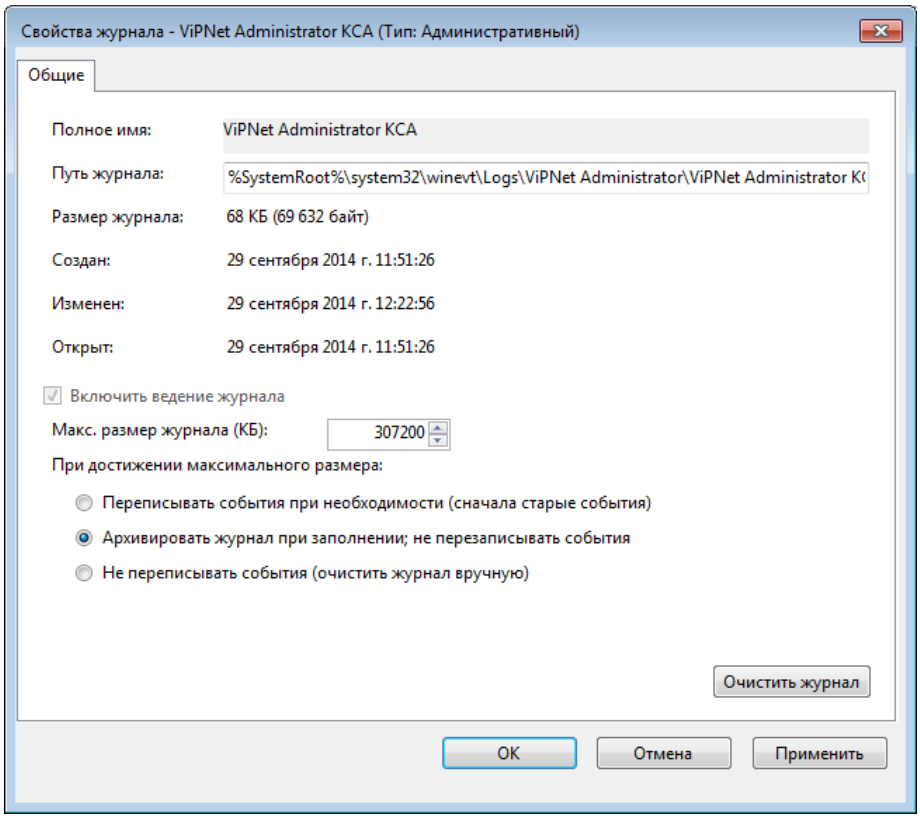

Рисунок 104. Настройка параметров сохранения журнала событий

Чтобы изменить степень детализации записей журнала событий или отключить ведение журнала в программе ViPNet Удостоверяющий и ключевой центр:

1 В окне программы в меню **Сервис** выберите пункт **Настройка**.

2 В появившемся окне на панели навигации выберите раздел **Журнал событий**.

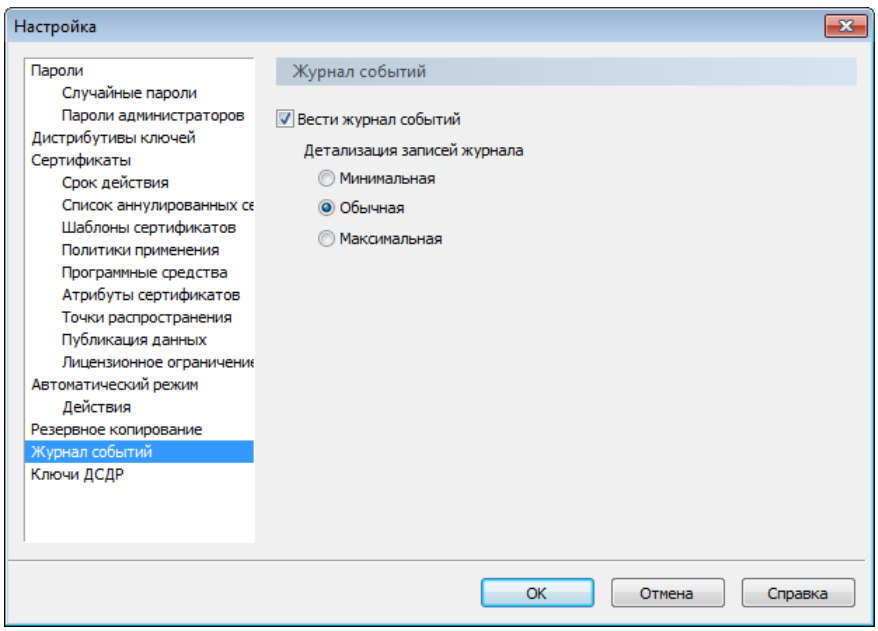

Рисунок 105. Настройка параметров журнала событий

3 Если требуется отключить ведение журнала событий, снимите флажок **Вести журнал событий**. Если данный флажок снят, настройка детализации записей журнала недоступна.

Примечание. Если в программе ViPNet Удостоверяющий и ключевой центр отключено ведение журнала, то в журнал событий **ViPNet Administrator KCA** записываются только события запуска и завершения работы программы.

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 аннулированных сертификатов, удовлетворение либо отклонение запроса на сертификат или его аннулирование.

- **Максимальная** — фиксируется вся информация.

Полный список событий УКЦ представлен в приложении Перечень событий УКЦ, регистрируемых в журнале событий (см. Перечень событий УКЦ, регистрируемых в журнале событий Windows на стр. 195).

5 Чтобы сохранить настройки, нажмите кнопку **OK**.

Проверка текущих данных

При запуске и в процессе работы программы ViPNet Удостоверяющий и ключевой центр автоматически производится проверка текущих данных на наличие следующих ошибок:

- **Критические** — ошибки, при которых программа не может продолжать свою работу и закрывается.
- **Аномальные** — ошибки, при которых некоторые функции программы либо недоступны, либо неуспешны. Например, могут быть недоступны операции с сертификатами (издание, аннулирование, импорт и прочее) вследствие истечения срока действия списка аннулированных сертификатов администратора или невозможны операции по созданию ключей для узлов, пароли администраторов которых искажены или недействительны.

  Примечание. Проверку данных на наличие аномальных ошибок также можно выполнить вручную (см. Проверка текущих данных вручную на стр. 178).

- **Рабочие** — ошибки, возникающие в рабочем порядке и не влияющие на функциональность программы.

Если в ходе проверки данных будет установлен факт возникновения какой-либо ошибки, будет выдано соответствующее сообщение с его описанием.

Перечень возможных критических, аномальных и рабочих ошибок, а также описание действий администратора при возникновении данных ошибок приведены ниже в таблице.

Таблица 5. Описание ошибок, которые могут возникнуть при проверке текущих данных

Описание ошибки и форма оповещения	Рекомендуемые действия администратора программы
Критические	
Нарушение целостности или повреждение исполняемых модулей программы. Контроль целостности осуществляется путем вычисления имитозащитной вставки. При обнаружении повреждений появляется сообщение о найденном несоответствии, и программа завершает свою работу.	Поставьте в известность должностное лицо, ответственное за безопасность эксплуатации сети ViPNet, и выявите причины появления данной ошибки. Особое внимание рекомендуется уделить исключению возможностей несанкционированного доступа к компьютеру и умышленного искажения файлов. Восстановление работоспособности программы в данном случае возможно только путем ее переустановки.

Описание ошибки и форма оповещения	Рекомендуемые действия администратора программы
Нарушение целостности ключей ViPNet (ключа защиты УКЦ, ключа электронной подписи текущего администратора). При обнаружении нарушения целостности появляется сообщение об ошибке инициализации администратора.	Выявите причины возникновения подобной ошибки. В зависимости от того, какой ключ был поврежден, устранение ошибки возможно будет либо путем восстановления конфигурации программы из резервной копии (см. Восстановление конфигурации на стр. 165), либо путем переиздания сертификата администратора (см. Плановая смена ключа электронной подписи и сертификата администратора на стр. 154).
Аномальные	
Истечение срока действия списка аннулированных сертификатов. 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 аннулированных сертификатов.	Обновите список аннулированных сертификатов (см. Обновление CRL вручную на стр. 97).
Истечение срока плановой смены ключа электронной подписи администратора. За определенное количество дней до истечения срока плановой смены ключа электронной подписи появляется сообщение о том, что необходимо обновить ключ электронной подписи и сертификат администратора. В противном случае издание сертификатов пользователей станет невозможным.	Выполните плановую смену ключа электронной подписи администратора (см. Плановая смена ключа электронной подписи и сертификата администратора на стр. 154).
Искажение паролей администраторов сетевых узлов. При обнаружении искаженных паролей администраторов сетевых узлов появляется соответствующее сообщение. Создание ключей для узлов с такими паролями невозможно.	Смените (см. Создание и смена пароля администратора сетевого узла или группы узлов на стр. 42) или сбросьте такие пароли администраторов (см. Сброс пароля администратора сетевого узла на стр. 42).
Истечение срока действия паролей администраторов сетевых узлов или групп узлов. За определенное количество дней до истечения срока действия (если установлена опция в настройках программы) либо при истечении срока действия паролей появляется соответствующее сообщение. Создание ключей для узлов с такими паролями невозможно.	Смените (см. Создание и смена пароля администратора сетевого узла или группы узлов на стр. 42) или сбросьте такие пароли администраторов (см. Сброс пароля администратора сетевого узла на стр. 42).

Описание ошибки и форма оповещения	Рекомендуемые действия администратора программы
Найдены искаженные межсетевые мастер-ключи или ключи, срок действия которых истек. Сообщение появляется, если обнаружены действующие межсетевые мастер-ключи, которые используются более 1 года. Рекомендуется выполнить смену указанных межсетевых мастер-ключей.	Выполните смену межсетевых мастер-ключей, указанных в сообщении (см. Смена межсетевого мастер-ключа на стр. 42).
Рабочие	
Истечение срока действия сертификата пользователя своей сети. 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 сертификата для следующего пользователя (списка пользователей).	Для пользователя, указанного в сообщении, сформируйте новые ключи (см. руководство администратора на УКЦ).
Наличие искажений в межсетевой информации (сертификатах администраторов доверенных сетей ViPNet, информации о пользователях и сетевых узлах, межсетевых мастер-ключах и прочем). При обнаружении искажений в процессе обращения к поврежденной информации появляется соответствующее сообщение об ошибке. До устранения неполадок выполнение ряда операций в программе будет невозможно.	Получите у администратора этой доверенной сети ViPNet обновленную межсетевую информацию и импортируйте ее.
Закончились лицензии на издание сертификатов пользователей в соответствии с лицензионным файлом. 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.	Обратитесь к представителю компании ИнфоТеКС с запросом на расширение текущей лицензии.
В программе появились необработанные контейнеры сертификатов, полученные от администраторов доверенных сетей ViPNet. Выдается сообщение с предложением обработать контейнеры сертификатов.	Выполните обработку контейнеров сертификатов. Поступившие контейнеры сертификатов находятся в представлении **Администрирование** в разделе **Необработанные данные** > **Контейнеры сертификатов администраторов сетей ViPNet**.

Описание ошибки и форма оповещения	Рекомендуемые действия администратора программы
Получены файлы с запросами на издание сертификатов от пользователей либо из центра регистрации или файлы с запросами на аннулирование сертификатов. Выдается сообщение с предложением обработать поступившие запросы.	Обработайте поступившие запросы. Запросы отображаются в представлении **Удостоверяющий центр**. Подробнее см. соответствующие разделы в главе Управление сертификатами (на стр. 42).

Проверка текущих данных вручную

В программе ViPNet Удостоверяющий и ключевой центр вы можете вручную выполнить проверку текущих данных на наличие аномальных ошибок. Описание возможных аномальных ошибок приведено в разделе Проверка текущих данных (на стр. 175).

Чтобы вручную выполнить проверку данных, в окне программы в меню **Сервис** выберите пункт **Проверка текущих данных**. Если аномальные ошибки отсутствуют, появится соответствующее сообщение.

A

Возможные неполадки и способы их устранения

Не удается войти в программу ViPNet Удостоверяющий и ключевой центр

Если вам не удается войти в программу ViPNet Удостоверяющий и ключевой центр, проблема может иметь следующие причины:

- **Изменились параметры подключения к SQL-серверу**

  При запуске УКЦ могут возникнуть следующие ошибки подключения к SQL-серверу:

  - выбранный SQL-сервер недоступен;
  - на SQL-сервере изменились учетные данные пользователя, имеющего доступ к базе данных;
  - изменились настройки подключения или настройки проверки подлинности SQL-сервера;
  - изменился IP-адрес или имя SQL-сервера и прочее.

  В случае возникновения указанных ошибок появится окно подключения к SQL-серверу. Укажите параметры подключения, как описано в разделе Подключение к SQL-серверу при запуске программы (на стр. 25).

- **Учетная запись Windows, которую вы используете, не имеет прав доступа к SQL-серверу**

  Например, эта проблема может возникнуть в том случае, если компьютер с УКЦ ввели в домен Active Directory.

Для решения проблемы:

- Удалите файл `C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\ini\sqlloginfo.dat`.
- Перезапустите программу ViPNet Удостоверяющий и ключевой центр. Появится окно **Подключение к SQL Server**.
- Укажите параметры подключения по имени и паролю пользователя SQL-сервера (см. Подключение к SQL-серверу при запуске программы на стр. 25).

- **Не найден контейнер ключей администратора УКЦ**

  По умолчанию контейнер ключей администратора УКЦ находится в папке: `C:\Users\<имя учетной записи Windows, от имени которой установлен УКЦ>\AppData\Roaming\Infotecs\ViPNet Administrator\KeysManager_1`.

  Причина проблемы может быть в том, что контейнер ключей администратора УКЦ перемещен или учетная запись Windows, которую вы используете, не имеет прав доступа к контейнеру. В случае перемещения контейнера ключей администратора УКЦ укажите место его хранения.

Не удается посмотреть пароль, сохраненный в файле

Пароли пользователей сохраняются в графическом виде в файлы формата `XPS`. Просмотреть файлы `*.xps` вы можете в том случае, если на компьютере установлена программа Средство просмотра XPS.

Программа Средство просмотра XPS по умолчанию не установлена на компьютерах с операционными системами Windows Server 2012 R2 или Windows Server 2016. Поэтому если на вашем компьютере используется одна из указанных ОС, установите Средство просмотра XPS вручную. Ниже описан сценарий установки компонента Средство просмотра XPS на Windows Server 2012. Установка компонента на других ОС включает в себя аналогичные действия, но мастер установки может иметь другой внешний вид.

Чтобы установить компонент Средство просмотра XPS вручную:

1. Запустите консоль **Диспетчер серверов** (**Server Manager**).
2. В окне консоли в меню **Управление** (**Manage**) выберите пункт **Добавить роли и компоненты** (**Add roles and Features**). Будет запущен мастер добавления ролей и компонентов, следуйте его указаниям.
3. На странице **Тип установки** (**Select installation type**) выберите **Установка ролей или компонентов** (**Role-based or feature-based installation**).
4. На странице **Компоненты** (**Select features**) в списке компонентов установите флажок напротив **Средство просмотра XPS** (**XPS Viewer**).

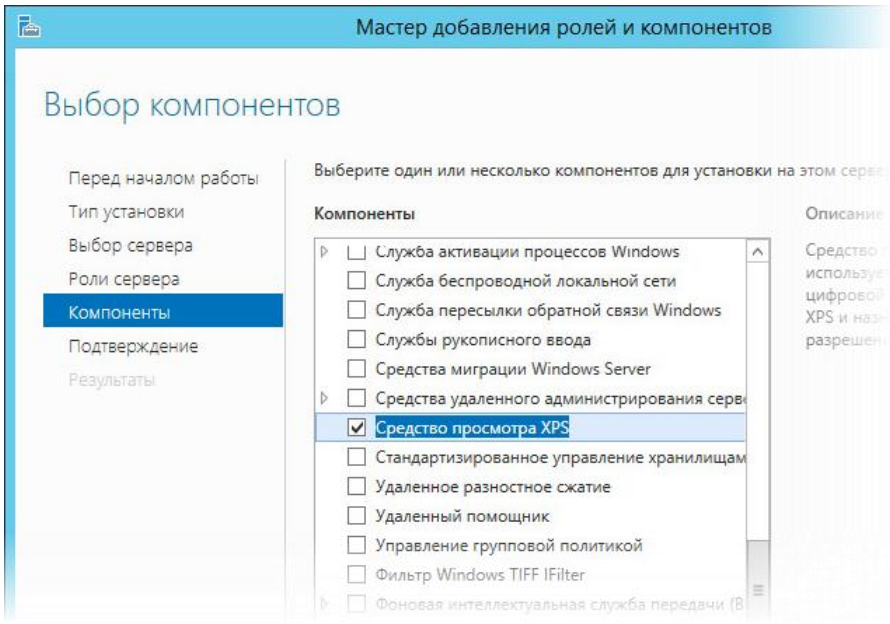

Рисунок 106. Добавление компонента Средство просмотра XPS

5 На странице **Подтверждение** (**Confirmation**) нажмите кнопку **Установить** (**Install**).

6 На последней странице мастера ознакомьтесь с результатом установки компонента и убедитесь, что в процессе установки не возникло ошибок. После этого завершите работу с мастером.

Теперь вы можете просматривать файлы с паролями пользователей.

Не удается выполнить обновление списка анулированных сертификатов

Проблема с обновлением списка аннулированных сертификатов может возникнуть, если было изменено место размещения контейнера с ключом электронной подписи, соответствующим этому списку аннулированных сертификатов. Например, путь к папке с контейнерами ключей мог измениться при миграции ПО ViPNet Administrator с одного компьютера на другой.

Чтобы указать корректный путь к папке с контейнером ключей:

1 В окне программы ViPNet Удостоверяющий и ключевой центр на панели навигации выберите представление **Администрирование**, и затем выберите раздел **Изданные сертификаты** > **Корневые сертификаты**.

2 Выберите корневой сертификат, соответствующий обновляемому списку аннулированных сертификатов, вызовите контекстное меню и выберите команду **Указать расположение ключа подписи**.

3 В открывшемся окне программы ViPNet CSP установите переключатель в положение **Папка на диске** и укажите путь к папке с контейнером ключей.

4 В списке **Имя контейнера** выберите контейнер, содержащий нужный ключ электронной подписи, и нажмите кнопку **OK**.

B

Внешние устройства

Общие сведения

Внешние устройства предназначены для хранения контейнеров ключей (см. глоссарий, стр. 213), которые вы можете использовать для аутентификации, формирования электронной подписи (см. глоссарий, стр. 218) или для других целей.

На внешнем устройстве могут храниться ключи, созданные по различным алгоритмам в программном обеспечении ViPNet или в сторонних программах. Максимальное количество контейнеров ключей, которое может храниться на одном внешнем устройстве, зависит от объема памяти устройства.

Все операции с контейнерами ключей и внешними устройствами вы можете выполнить в программе ViPNet CSP. Чтобы использовать какое-либо внешнее устройство, на компьютер необходимо установить драйверы этого устройства. Перед записью ключей на устройство убедитесь, что оно отформатировано.

Список поддерживаемых внешних устройств

Список внешних устройства, которые могут быть использованы в ViPNet Administrator, а также условия и особенности работы с устройствами см. в документе «ViPNet CSP. Руководство пользователя».

Примечание. Список поддерживаемых операционных систем для каждого из приведенных устройств вы найдете на официальном веб-сайте производителя этого устройства.

Получение CRL из локальных точек распространения

В процессе электронного документооборота для проверки подписи требуется наличие актуальных списков аннулированных сертификатов (CRL). В зависимости от того, каким образом устроен электронный документооборот в сети, получение CRL может производиться по-разному, например:

- путем скачивания из внешних точек распространения, указанных в сертификатах, при проверке электронной подписи;
- с помощью периодического опроса точек распространения, заданных администратором сети или локально на узле;
- с помощью сетевых хранилищ CRL.

Первый способ является стандартным способом для сетей с инфраструктурой PKI. Второй и третий способы используются, когда первый способ получения CRL неприменим: точки распространения в сертификатах не указаны или отсутствует доступ к ним, либо сеть ViPNet достаточно велика для рассылки CRL.

Если во взаимодействующих организациях используется различное ПО для документооборота, то может использоваться комбинация нескольких способов получения CRL. Если документооборот осуществляется между организациями, в которых развернуты защищенные сети ViPNet, то они могут обмениваться CRL с помощью передаваемой межсетевой информации, и затем распространять обновления CRL на сетевые узлы.

Рассмотрим подробнее использование второго и третьего способов получения CRL на следующем примере.

Имеются две организации A и B, между которыми осуществляется электронный документооборот. Из организации B в организацию A с определенной периодичностью поступают почтовые

сообщения, заверенные электронной подписью. В организации А развернута защищенная сеть ViPNet с большим количеством узлов. В организации В развернута только PKI-инфраструктура, при этом ПО ViPNet не используется.

Передача актуальных CRL из организации В в организацию А с помощью межсетевой информации невозможна — в организации В нет развернутой сети ViPNet, которая могла бы стать доверенной для сети в организации А. Поэтому получить CRL, выпущенные удостоверяющим центром организации В, можно в специальной внешней точке распространения. Но при этом узлы сети ViPNet, на которые поступают почтовые сообщения, доступа к внешней точке распространения не имеют. Импорт списков из внешней точки распространения в сеть ViPNet организовать возможно, но их распространение по узлам сети будет трудоемким. Как в данном случае можно обеспечить получение CRL узлами сети ViPNet организации А из внешней точки распространения?

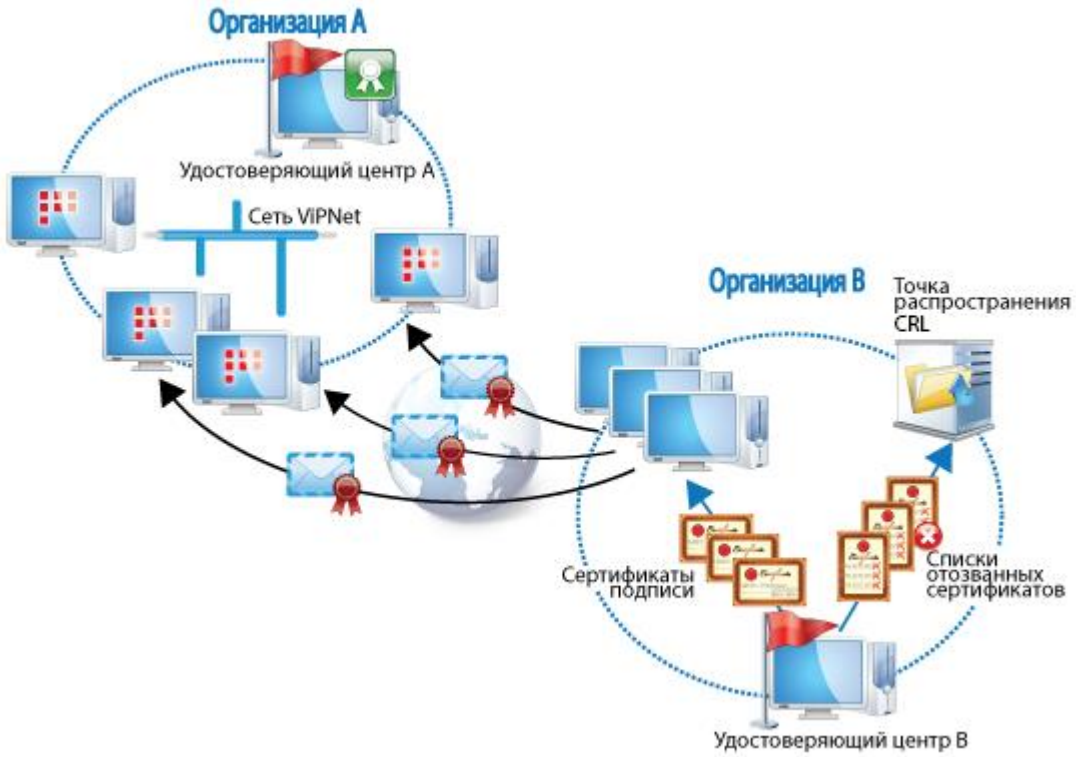

Рисунок 107. Пример организации электронного документооборота между несколькими организациями

С помощью технологии ViPNet данную задачу можно решить вторым способом, а именно: создать в сети организации А точку распространения или сетевое хранилище — место размещения CRL, к которому будут иметь доступ остальные узлы, и с помощью сервиса публикации публиковать в него CRL, скачанные из внешней точки. При этом информирование узлов сети о том, что при проверке подписи следует обращаться к данному месту хранения для получения CRL (если внешняя точка распространения недоступна), будет производиться с помощью файла `crl-update-setting.ini`.

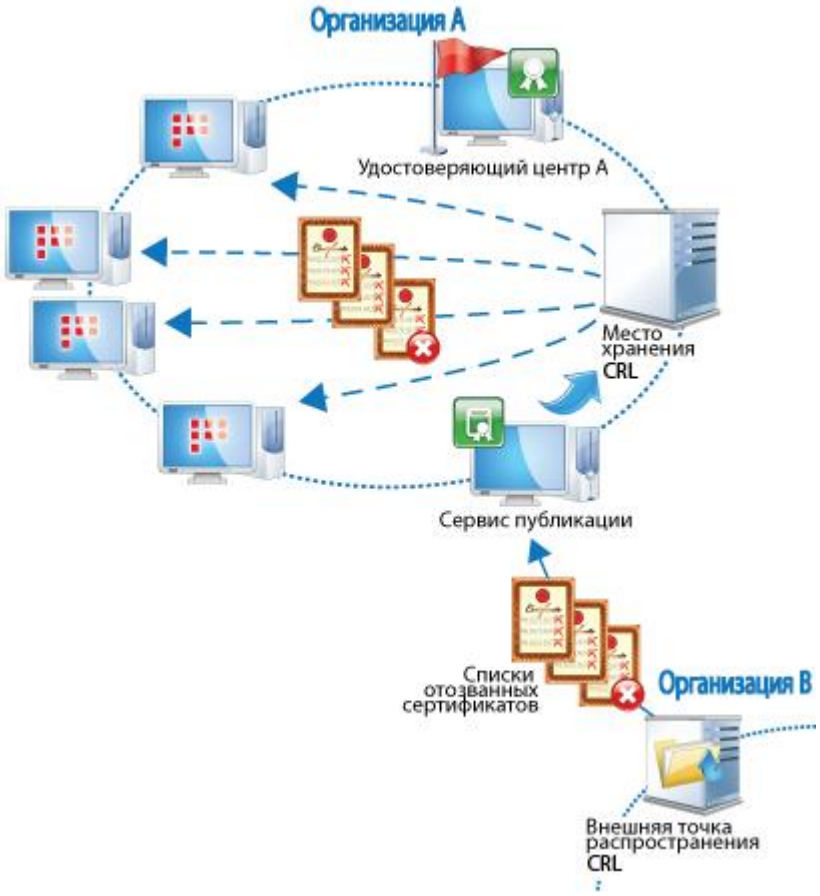

Рисунок 108. Пример реализации скачивания СОС из внешних точек распространения

Файл `crl-update-setting.ini` формируется на узле администратора сети (в процессе первичной инициализации программы ViPNet Удостоверяющий и ключевой центр) и на остальные узлы передается при рассылке CRL. В нем указываются точки распространения и сетевые хранилища, к которым могут обращаться узлы сети для получения списков отозванных сертификатов, а также задаются параметры поиска CRL в них.

Таким образом, для реализации описанной выше схемы получения CRL требуется выполнить следующие действия:

1. Организовать место хранения списков отозванных сертификатов в сети ViPNet.
2. С помощью сервиса публикации организовать регулярное скачивание CRL сторонних удостоверяющих центров из внешней точки распространения в место хранения CRL, доступное внутри организации. См. указания в документе «ViPNet Publication Service. Руководство администратора».
3. Подготовить файл `crl-update-setting.ini`. См. указания в разделах ниже.
4. На все узлы сети разослать CRL. См. указания в руководстве администратора на УКЦ.

Подготовка файла crl-update-settings.ini

В файле `crl-update-setting.ini` вы можете указать информацию о местах размещения списков аннулированных сертификатов и настроить параметры поиска CRL в них следующим образом:

1 Откройте файл `crl-update-settings.ini` в текстовом редакторе. Файл расположен в папке установки ViPNet Удостоверяющий и ключевой центр в подпапке `\ViPNet Administrator\KC\ini`.

2 Чтобы добавить информацию о месте хранения CRL, выполните следующие действия:

Если в качестве места хранения выступает сетевое хранилище:

- Создайте секцию с названием `[NetworkCrlStore-n]`, где `n` в названии секции — номер хранилища. Нумерация секций (хранилищ) должна начинаться с нуля: `[NetworkCrlStore-0]`, `[NetworkCrlStore-1]`. В противном случае не все секции будут учитываться при обработке.
- В созданной секции в виде параметра `URL` укажите сетевой путь, по которому доступно хранилище. Количество вводимых символов не должно быть меньше 6 и больше 2083. Например, сетевой путь может быть таким:
  `URL=ldap://192.168.45.144:389/CN=CDP,DC=kd,DC=local`

Если в качестве места хранения выступает точка распространения:

- Создайте секцию с названием `[CDP-n]`, где `n` в названии секции — номер точки. Нумерация секций (точек) должна начинаться с нуля: `[CDP-0]`, `[CDP-1]`. В противном случае не все секции будут учитываться при обработке.
- В созданной секции в виде параметра `URL` укажите сетевой путь, по которому доступна точка распространения. Количество вводимых символов не должно быть меньше 6 и больше 2083. Например, сетевой путь может быть таким:
  `URL=ftp://192.168.12.158/crl/5606-kid939FB75998C4D8044A4E341C024C4D73650C0AD6/revokedCerts.crl`.
- При необходимости для указанной точки распространения задайте следующие дополнительные параметры:
  - `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.
  - `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 CRL в формате X.500. Фактически данный параметр не используется и может содержать любое имя в формате X.500, которое может и не

соответствовать реальному издателю. Для простоты можно указать в качестве значения «cn=x». Пустое значение данного параметра недопустимо.

3 В секции [CrlUpdateAtSigVerification] задайте параметры поиска CRL при проверке электронной подписи:

- Укажите значение параметра AllowCrlUpdate равным 1, чтобы расширить поиск CRL в заданных местах хранения. Если значение параметра будет равно 0, то поиск CRL производиться не будет.
- Укажите значение параметра ForceCrlUpdate равным 1, чтобы форсировать поиск CRL (то есть производить поиск CRL даже при его наличии на узле с неистекшим сроком действия). Рекомендуется указывать такое значение в том случае, если производится частое обновление CRL (в основном это зависит от политики безопасности, применяемой в компании).
- Укажите значение параметра AllowUsingCDP равным 1 для возможности опроса точек распространения, заданных в сертификатах. Если установить значение 0, то опрос точек распространения производиться не будет.
- Укажите значение параметра AllowUsingNetworkCRLStores равным 1 для возможности опроса сетевых хранилищ, заданных в данном файле. Если установить значение 0, то опрос хранилищ данных производиться не будет.

4 В секции [PeriodicallyCrlUpdate] задайте параметры периодического обновления CRL, не в момент проверки электронной подписи:

- Укажите значение параметра AllowCrlUpdate равным 1 для выполнения периодического обновления CRL на узле. В этом случае будет производиться опрос точек распространения, заданных в данном файле.
- Укажите значение параметра CollectLocallyDetectedCdp равным 1 для автоматического добавления найденных при проверке электронной подписи точек распространения в список опроса, который хранится в специальном отдельном файле locally-detected-cdp.ini. То есть если при проверке электронной подписи была найдена новая точка распространения, то в этом случае она будет добавлена в список для дальнейшего периодического опроса.

5 Сохраните внесенные изменения и закройте файл.

С примером составления файла crl-update-settings.ini вы можете ознакомиться в разделе ниже.

Пример составления файла crl-update-settings.ini

Ниже приведен пример того, как может быть составлен файл `crl_update_settings.ini`:

```
[CrlUpdateAtSigVerification]
AllowCrlUpdate=1
ForceCrlUpdate=0
AllowUsingCDP=1
AllowUsingNetworkCRLStores=1

[PeriodicallyCrlUpdate]
AllowCrlUpdate=1
CollectLocallyDetectedCdp=0

[NetworkCrlStore-0]
URL=ldap://192.168.45.144:389/CN=CDP,DC=kd,DC=local

[CDP-0]
URL=ftp://192.168.12.158/crl/5606-
kid939FB75998C4D8044A4E341C024C4D73650C0AD6/revokedCerts.crl
IssuerName=O="ООО Ветка",OU=Удостоверяющий и ключевой
центр,T=Администратор,CN=Беляев Виталий Петрович
Enabled=1
NextUpdate=1344591938
IntervalInMinutes=1

[CDP-1]
URL=ldap://192.168.45.144/CN=kidF7CBBC571746304F0709C8C5EC7FF0B73AC9AF95,CN=9996,CN
=CDP,DC=kd,DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint
IssuerName=O="ООО Ветка",OU=Удостоверяющий и ключевой
центр,T=Администратор,CN=Беляев Виталий Петрович
Enabled=1
NextUpdate=1344591879
IntervalInMinutes=1
```

D

Региональные настройки

Для корректного отображения русской локализации интерфейса программ ViPNet в русифицированных ОС Microsoft Windows английской локализации необходимо установить поддержку кириллицы для программ, не поддерживающих Юникод. Эти настройки рекомендуется производить до установки самой программы.

Данные настройки также понадобится сделать, если установлен русскоязычный MUI (Multilanguage User Interface). Это значит, что ядро операционной системы английское, а русский язык для интерфейса и файлов справки был установлен позже. В этом случае региональные настройки по умолчанию английские и требуют изменения.

Внимание! Для изменения региональных настроек вы должны обладать правами администратора операционной системы.

Региональные настройки в Windows

Чтобы установить поддержку кириллицы:

1 Откройте панель управления (Control Panel) и в категории **Часы, язык и регион** (**Clock, Language, and Region**) выберите параметр **Изменение форматов даты, времени и чисел** (**Change date, time, or number formats**).

2 В окне **Регион** (**Region**) перейдите на вкладку **Дополнительно** (**Administrative**).

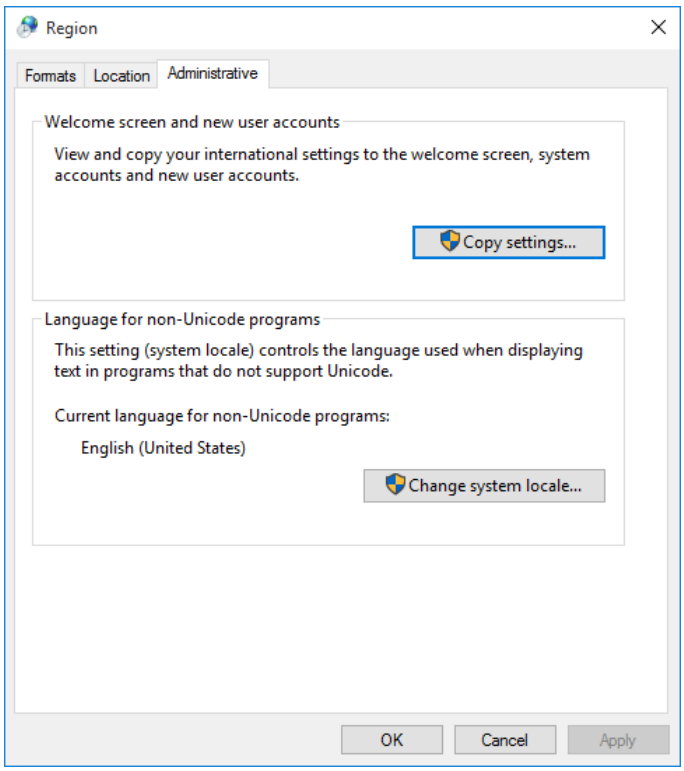

Рисунок 109. Дополнительные языковые параметры

3 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Изменить язык системы** (**Change system locale**).

4 В появившемся окне в списке выберите **Русский (Россия)** (**Russian (Russia)**).

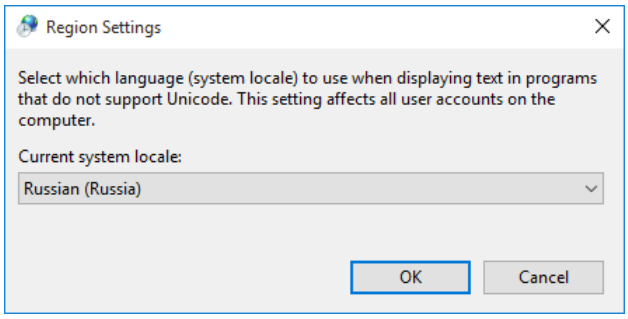

Рисунок 110. Выбор языка системы

5 Нажмите кнопку **OK**. Перезагрузите компьютер.

6 Дождитесь завершения перезагрузки компьютера, откройте панель управления (Control Panel) и в категории **Часы, язык и регион** (**Clock, Language, and Region**) выберите параметр **Изменение форматов даты, времени и чисел** (**Change date, time, or number formats**).

7 В окне **Регион** (**Region**) перейдите на вкладку **Дополнительно** (**Administrative**).

8 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Копировать параметры** (**Copy settings**).

9 В открывшемся окне в списке **Копировать текущие параметры в** (**Copy your current settings to**) установите флажок **Экран приветствия и системные учетные записи** (**Welcome screen and system accounts**) и нажмите кнопку **OK**.

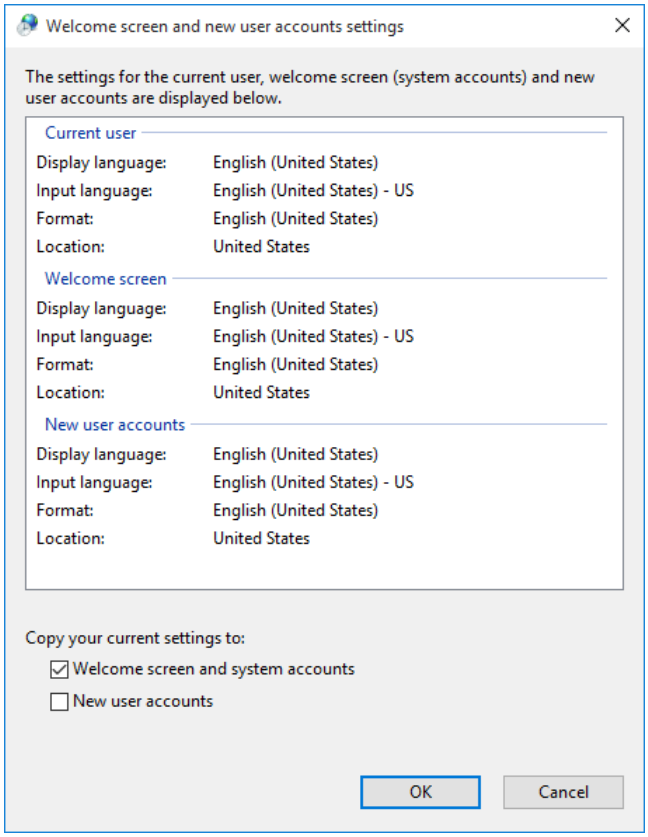

Рисунок 111. Копирование параметров

Также для исключения проблем с кодировкой в некоторых системах мы рекомендуем выполнить следующие действия:

1 В окне **Регион** (**Region**) на вкладке **Форматы** (**Formats**) в списке **Формат** (**Format**) выберите **Русский (Россия)** (**Russian (Russia)**).

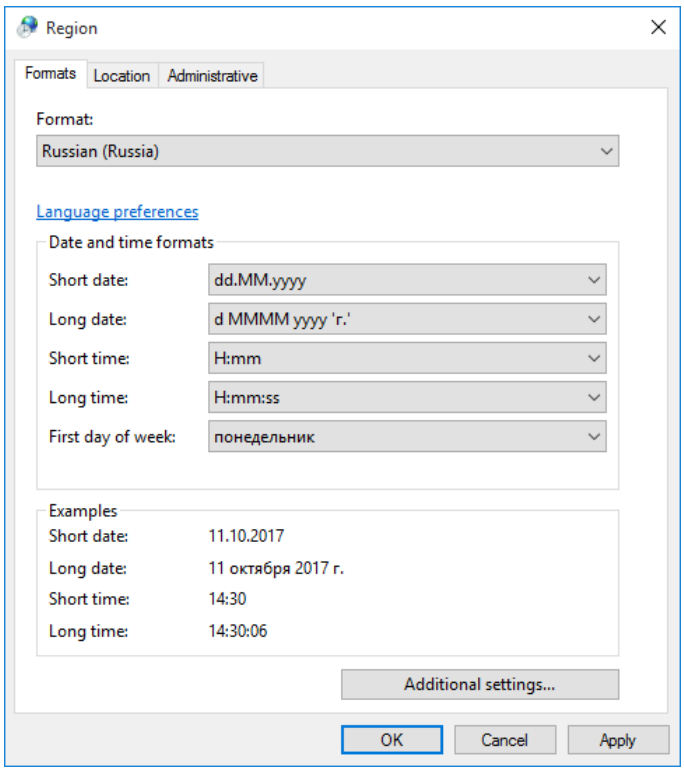

Рисунок 112. Настройка форматов

2 В окне **Регион** (**Region**) на вкладке **Местоположение** (**Location**) в списке **Основное расположение** (**Home location**) выберите **Россия** (**Russia**).

Примечание. В Windows 10 версии 1809 и выше нет вкладки **Location**, поэтому указанный параметр настраивать не нужно.

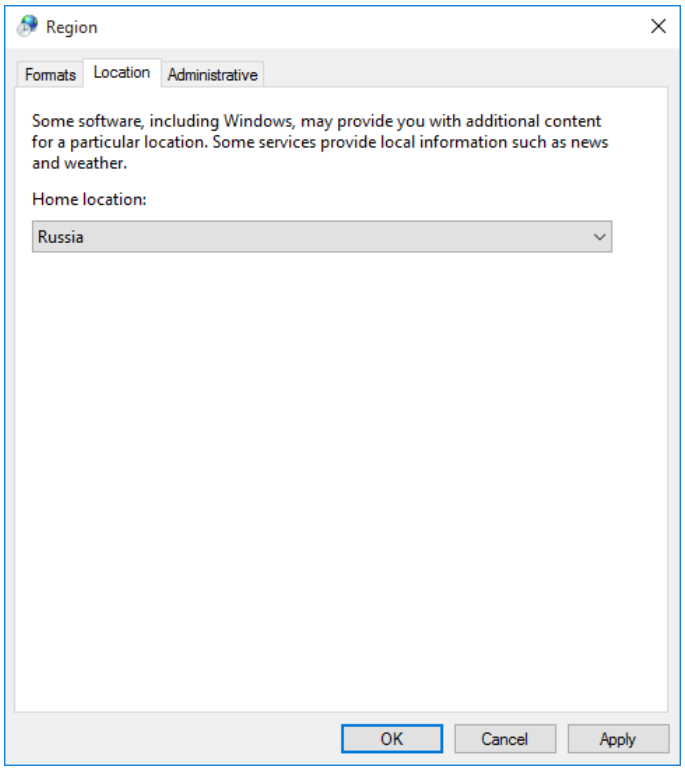

Рисунок 113. Выбор текущего расположения

E

Перечень событий УКЦ, регистрируемых в журнале событий Windows

В этом приложении представлен перечень всех событий программы ViPNet Удостоверяющий и ключевой центр, регистрируемых в журнале событий, для разной степени детализации записей. Настройка журнала событий описана в разделе Настройка параметров журнала событий (на стр. 172).

Таблица 6. События УКЦ для различных уровней детализации записей журнала событий

Название события	Минимальная	Обычная	Максимальная
Запущен процесс аудита событий	•	•	•
Завершен процесс аудита событий	•	•	•
Введен неверный пароль при аутентификации	•	•	•
Вход в систему	•	•	•
Выход из системы	•	•	•
Вход в режим администратора	•	•	•
Выход из режима администратора	•	•	•
Введен неверный пароль администратора	•	•	•
Проведено обновление ключей узла	•	•	•
Проведено обновление ключей пользователя	•	•	•

Название события	Минимальная	Обычная	Максимальная
Ошибка при обновлении ключей узла	•	•	•
Ошибка при обновлении ключей пользователя	•	•	•
Автоматический перезапуск приложения для применения обновления ключей	•	•	•
Автоматический вход в систему для применения обновления ключей	•	•	•
Изменен текущий сертификат ключа проверки электронной подписи пользователя	•	•	•
Ошибка при смене текущего сертификата ключа проверки электронной подписи пользователя	•	•	•
Сертификат введен в действие	•	•	•
Ошибка при вводе в действие сертификата	•	•	•
Смена места хранения ключа электронной подписи пользователя	•	•	•
Ошибка при смене места хранения ключа электронной подписи пользователя	•	•	•
Изменены настройки параметров безопасности	•	•	•
Ошибка при изменении настроек параметров безопасности	•	•	•
Изменен способ аутентификации	•	•	•
Ошибка при изменении способа аутентификации	•	•	•
Аутентификация администратора	•	•	•
Неудачная аутентификация администратора	•	•	•
Создание администратора	•	•	•
Ошибка создания администратора	•	•	•
Удаление администратора	•	•	•
Нормальное завершение работы УКЦ	•	•	•
Повторный запуск УКЦ	•	•	•
Создание мастер-ключа своей сети	•	•	•
Ошибка создания мастер-ключа своей сети	•	•	•
Создание сертификата администратора	•	•	•
Ошибка создания сертификата администратора	•	•	•
Смена ключевого носителя администратора	•	•	•

Название события	Минимальная	Обычная	Максимальная
Ошибка смены ключевого носителя администратора	•	•	•
Создание запроса на кросс-сертификат	•	•	•
Ошибка создания запроса на кросс-сертификат	•	•	•
Создание для сертификата администратора запроса к вышестоящему УЦ	•	•	•
Ошибка создания для сертификата администратора запроса к вышестоящему УЦ	•	•	•
Смена пароля администратора	•	•	•
Ошибка смены пароля администратора	•	•	•
Смена ключа защиты УКЦ	•	•	•
Ошибка смены ключа защиты УКЦ	•	•	•
Смена пароля администратора группы сетевых узлов	•	•	•
Ошибка смены пароля администратора группы сетевых узлов	•	•	•
Смена варианта персонального ключа пользователя	•	•	•
Смена варианта ключей сетевого узла	•	•	•
Компрометация ключей пользователя	•	•	•
Конфигурация восстановлена из резервной копии	•	•	•
Ошибка восстановления конфигурации из резервной копии	•	•	•
Инициализация приложения успешно пройдена	•	•	•
Неуспешная инициализация приложения	•	•	•
Смена имени администратора	•	•	•
Выдача нового дистрибутива ключей сетевого узла	•	•	•
Ошибка при выдаче нового дистрибутива ключей сетевого узла	•	•	•
Издан сертификат пользователя		•	•
Ошибка издания сертификата пользователя		•	•
Принят запрос на сертификат пользователя		•	•
Ошибка принятия запроса на издание сертификата		•	•
Дубликат запроса на сертификат пользователя		•	•
Отклонен запрос на издание сертификата		•	•
Принят запрос на аннулирование сертификата		•	•

Название события	Минимальная	Обычная	Максимальная
Ошибка принятия запроса на аннулирование сертификата		•	•
Дубликат запроса на аннулирование сертификата		•	•
Отклонен запрос на аннулирование сертификата		•	•
Издан CRL		•	•
Удовлетворен запрос на аннулирование сертификата		•	•
Ошибка создания ключевого набора сетевого узла		•	•
Созданы ключи узла		•	•
Ошибка создания обновления информации CRL для сетевого узла		•	•
Создано обновление информации CRL для сетевого узла		•	•
Сертификат аннулирован		•	•
Удовлетворен запрос на сертификат		•	•
Создана резервная копия		•	•
Ошибка создания резервной копии		•	•
Смена пароля администратора сетевого узла		•	•
Ошибка смены пароля администратора сетевого узла		•	•
Переключение в автоматический режим		•	•
Переключение в ручной режим		•	•
Смена пароля пользователя		•	•
Изменение прав пользователей			•
Создан межсетевой мастер-ключ			•
Импортирован межсетевой мастер-ключ			•
Импортирован сертификат администратора доверенной сети			•
Импортирован CRL доверенной сети			•
Ключи узла сохранены в файл			•
Ошибка создания ключевого диска пользователя			•
Ошибка создания ключевого набора сетевого узла			•
Ошибка создания межсетевого мастер-ключа			•
Ошибка импортирования межсетевого мастер-ключа			•

Название события	Минимальная	Обычная	Максимальная
Ошибка импортирования сертификата администратора доверенной сети			•
Ошибка импортирования CRL доверенной сети			•
Ошибка экспортирования ключевого носителя			•
Печать пароля пользователя			•
Ошибка при печати пароля пользователя			•
Смена способа аутентификации пользователя			•
Смена сертификата аутентификации пользователя			•
Удаление межсетевого мастер-ключа			•
Ошибка удаления межсетевого мастер-ключа			•

F

Основы криптографии

Криптография используется для решения трех основных задач:

- обеспечение конфиденциальности данных;
- контроль целостности данных;
- обеспечение подлинности авторства данных.

Первая задача решается с помощью симметричных алгоритмов шифрования. Для решения второй и третьей задач требуется использование асимметричных алгоритмов и электронной подписи.

В данном разделе содержится упрощенное описание алгоритмов с симметричным ключом, с асимметричным ключом, электронной подписи, а также приводятся примеры использования этих алгоритмов в информационных системах (приведенные примеры не относятся к технологии ViPNet).

Симметричное шифрование

В симметричных алгоритмах для зашифрования и расшифрования применяется один и тот же криптографический ключ. Для того чтобы и отправитель, и получатель могли прочитать исходный текст (или другие данные, не обязательно текстовые), обе стороны должны знать ключ алгоритма.

На схеме ниже изображен процесс симметричного зашифрования и расшифрования.

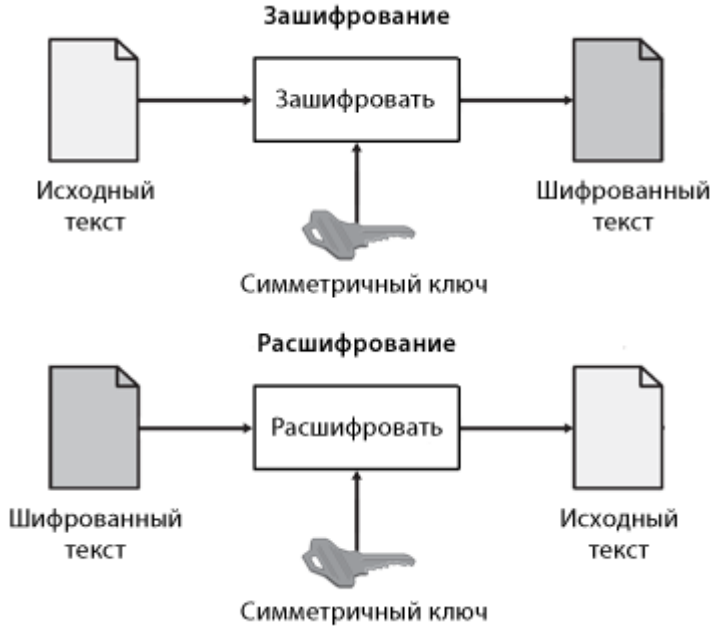

Рисунок 114. Зашифрование и расшифрование на симметричном ключе

Симметричные алгоритмы шифрования способны обрабатывать большое количество данных за короткое время благодаря использованию для зашифрования и расшифрования одного и того же ключа, а также благодаря простоте симметричных алгоритмов по сравнению с асимметричными. Поэтому симметричные алгоритмы часто используют для шифрования больших массивов данных.

Для шифрования данных с помощью симметричного алгоритма криптографическая система использует симметричный ключ. Длина ключа (обычно выражаемая в битах) зависит от алгоритма шифрования и программы, которая использует этот алгоритм.

С помощью симметричного ключа исходный (открытый) текст преобразуется в шифрованный (закрытый) текст. Затем шифрованный текст отправляется получателю. Если получателю известен симметричный ключ, на котором зашифрован текст, получатель может преобразовать шифрованный текст в исходный вид.

Примечание. На практике симметричный ключ нужно передать получателю каким-либо надежным способом. Обычно создается симметричный ключ парной связи, который передается получателю лично. Затем для шифрования используются случайные (сессионные) симметричные ключи, которые зашифровываются на ключе парной связи и в таком виде передаются по различным каналам вместе с шифрованным текстом.

Наибольшую угрозу безопасности информации при симметричном шифровании представляет перехват симметричного ключа парной связи. Если он будет перехвачен, злоумышленники смогут расшифровать все данные, зашифрованные на этом ключе.

Асимметричное шифрование

Асимметричные алгоритмы шифрования используют два математически связанных ключа: открытый ключ и закрытый ключ. Для зашифрования применяется открытый ключ, для расшифрования — закрытый ключ.

Открытый ключ распространяется свободно. Закрытым ключом владеет только пользователь, который создает пару асимметричных ключей. Закрытый ключ следует хранить в секрете, чтобы исключить возможность его перехвата.

Использование двух различных ключей для зашифрования и расшифрования, а также более сложный алгоритм делают процесс шифрования с помощью асимметричных ключей гораздо более медленным, чем шифрование с помощью симметричных ключей.

Открытый ключ может быть использован любыми лицами для отправки зашифрованных данных владельцу закрытого ключа. При этом парой ключей владеет только получатель зашифрованных данных. Таким образом, только получатель может расшифровать эти данные с помощью имеющегося у него закрытого ключа.

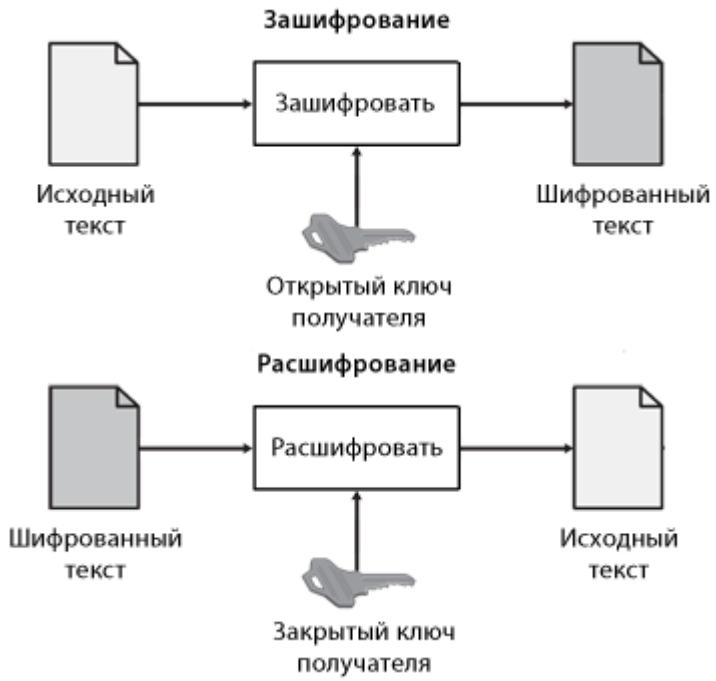

Рисунок 115. Зашифрование и расшифрование на асимметричном ключе

Примечание. На практике асимметричные алгоритмы в чистом виде используются очень редко. Обычно данные зашифровываются с помощью симметричного алгоритма, а затем с помощью асимметричного алгоритма зашифровывается только симметричный ключ. Комбинированные (гибридные) криптографические алгоритмы рассматриваются ниже (см. Сочетание симметричного и асимметричного шифрования на стр. 204).

Сочетание симметричного и асимметричного шифрования

В большинстве приложений симметричные и асимметричные алгоритмы применяются совместно, что позволяет использовать преимущества обоих алгоритмов.

В случае совместного использования симметричного и асимметричного алгоритмов:

- Исходный текст преобразуется в шифрованный с помощью симметричного алгоритма шифрования. Преимущество этого алгоритма заключается в высокой скорости шифрования.
- Для передачи получателю симметричный ключ, на котором был зашифрован текст, зашифровывается с помощью асимметричного алгоритма. Преимущество асимметричного алгоритма заключается в том, что только владелец закрытого ключа сможет расшифровать симметричный ключ.

На следующем рисунке изображен процесс шифрования с помощью комбинированного алгоритма.

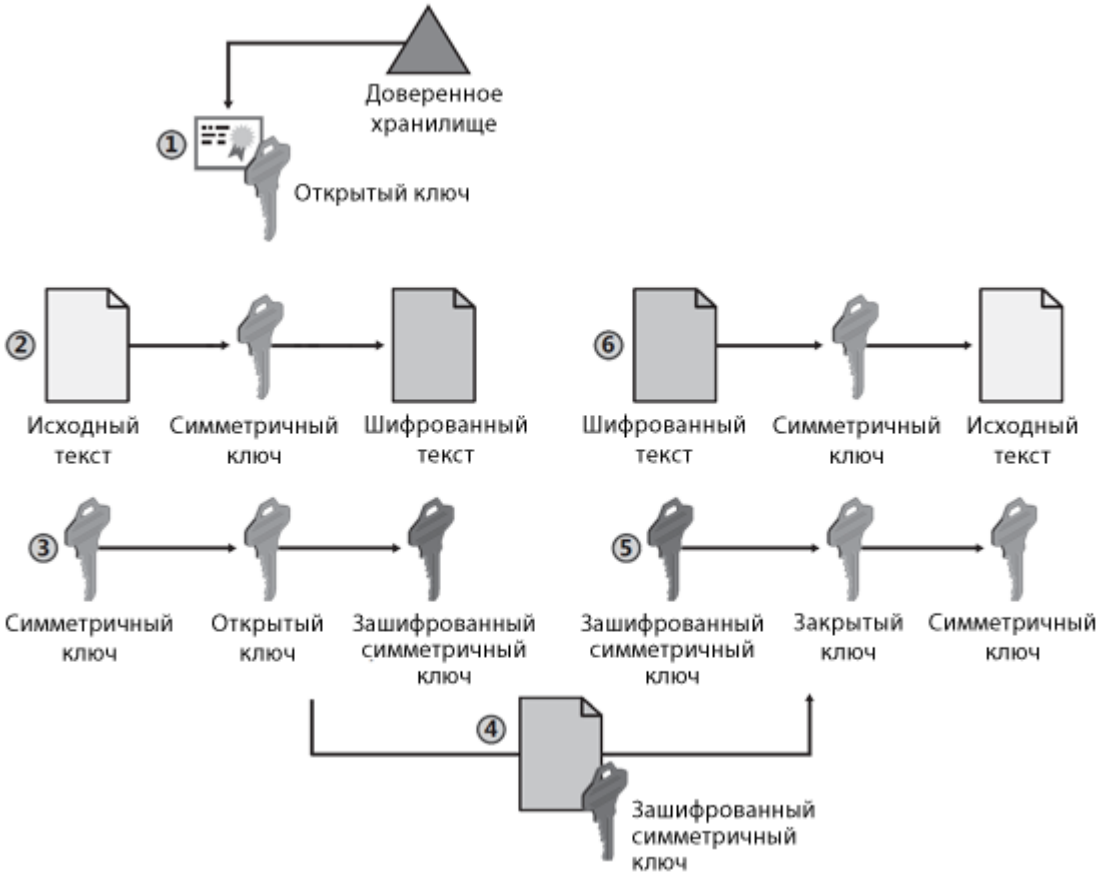

Рисунок 116. Шифрование с помощью комбинированного алгоритма

1 Отправитель запрашивает открытый ключ получателя из доверенного хранилища.

2 Отправитель создает симметричный ключ и зашифровывает с его помощью исходный текст.

3 Симметричный ключ зашифровывается на открытом ключе получателя, чтобы предотвратить перехват ключа во время передачи.

4 Зашифрованный симметричный ключ и шифрованный текст передаются получателю.

5 С помощью своего закрытого ключа получатель расшифровывает симметричный ключ.

6 С помощью симметричного ключа получатель расшифровывает шифрованный текст, в результате он получает исходный текст.

Сочетание хэш-функции и асимметричного алгоритма электронной подписи

Электронная подпись защищает данные следующим образом:

- Для подписания данных используется хэш-функция, с помощью которой определяется хэш-сумма исходных данных. По хэш-сумме можно определить, имеют ли место какие-либо изменения в этих данных.
- Полученная хэш-сумма подписывается электронной подписью, позволяя подтвердить личность подписавшего. Кроме того, электронная подпись не позволяет подписавшему лицу отказаться от авторства, так как только оно владеет ключом электронной подписи, использованным для подписания. Невозможность отказаться от авторства называется неотрекаемостью.

Большинство приложений, осуществляющих электронную подпись, используют сочетание хэш-функции и асимметричного алгоритма подписи. Хэш-функция позволяет проверить целостность исходного сообщения, а электронная подпись защищает полученную хэш-функцию от изменения и позволяет определить личность автора сообщения.

Приведенная ниже схема иллюстрирует применение хэш-функции и асимметричного алгоритма в электронной подписи.

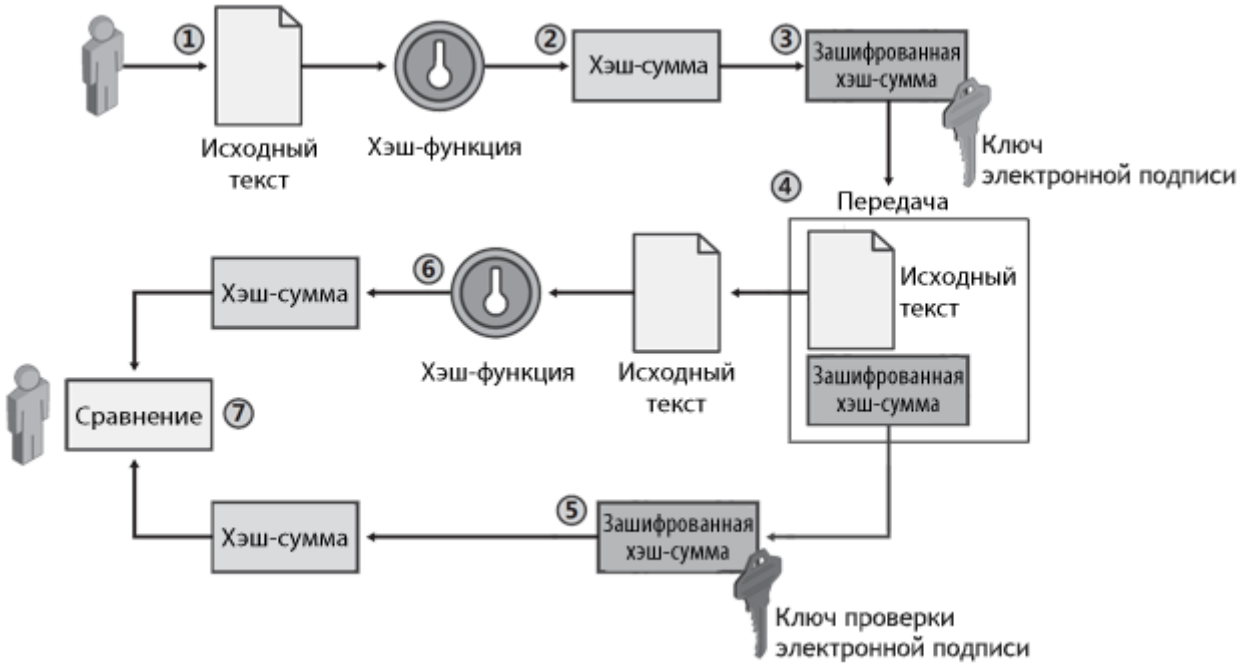

Рисунок 117. Применение хэш-функции и асимметричного криптографического алгоритма в электронной подписи

1 Отправитель создает файл с исходным сообщением.

2 Программное обеспечение отправителя вычисляет хэш-сумму исходного сообщения.

3 Полученная хэш-сумма зашифровывается с помощью ключа электронной подписи отправителя.

4 Исходное сообщение и зашифрованная хэш-функция передаются получателю.

Примечание. При использовании электронной подписи исходное сообщение не зашифровывается. Само сообщение может быть изменено, но любые изменения сделают хэш-сумму, передаваемую вместе с сообщением, недействительной.

5 Получатель расшифровывает хэш-сумму сообщения с помощью ключа проверки электронной подписи отправителя. Ключ проверки электронной подписи может быть передан вместе с сообщением или получен из доверенного хранилища.

6 Получатель использует ту же хэш-функцию, что и отправитель, чтобы вычислить хэш-сумму полученного сообщения.

7 Вычисленная хэш-сумма сравнивается с хэш-суммой, полученной от отправителя. Если эти хэш-суммы различаются между собой, то сообщение или хэш-сумма были изменены при передаче.

Глоссарий

Microsoft Access

Система управления реляционными базами данных, разработанная компанией Microsoft. Входит в состав пакета Microsoft Office.

Microsoft SQL Server

Система управления реляционными базами данных, разработанная компанией Microsoft. Используется для работы с базами данных размером от персональных до крупных баз данных масштаба предприятия.

OCSP-сервер (сервис проверки статуса сертификатов)

Доверенный субъект инфраструктуры открытых ключей, предоставляющий информацию о статусах сертификатов по соответствующим запросам в режиме реального времени.

ODBC (Open Database Connectivity)

Стандартный программный интерфейс (Application Programming Interface, API) доступа к различным источникам данных (базам данных), разработанный компанией Microsoft.

PKI (Public Key Infrastructure)

Инфраструктура открытых ключей — комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам (в том числе ключам проверки электронной подписи) в распределенных системах через создание сертификатов ключей проверки электронной подписи и поддержание их жизненного цикла.

SQL-сервер

Сервер базы данных, который работает под управлением программного обеспечения Microsoft SQL Server.

TSP-сервер (служба штампов времени)

Доверенный субъект инфраструктуры открытых ключей, обладающий точным и надежным источником времени и оказывающий услуги по созданию штампов времени.

ViPNet Administrator

Набор программного обеспечения для администрирования сети ViPNet, включающий в себя программу ViPNet Удостоверяющий и ключевой центр.

ViPNet Publication Service

Программное обеспечение для публикации сертификатов пользователей, издателей (администраторов) и списков отозванных сертификатов в общедоступных хранилищах данных.

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.

Администратор сети ViPNet

Лицо, отвечающее за управление сетью ViPNet, создание и обновление справочников и ключей для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями и обладающее правом доступа к программе ViPNet Удостоверяющий и ключевой центр.

Администратор УКЦ

Лицо, обладающее правом доступа к программе ViPNet Удостоверяющий и ключевой центр (УКЦ), отвечающее за создание ключей для сетевых узлов ViPNet, создание и обслуживание сертификатов ViPNet, обеспечение взаимодействия с доверенными сетями ViPNet.

Аккредитованный удостоверяющий центр

Удостоверяющий центр, прошедший аккредитацию в уполномоченном федеральном органе исполнительной власти в соответствии с требованиями Федерального закона от 6 апреля 2011г. № 63-ФЗ «Об электронной подписи».

Аннулирование сертификата

Признание сертификата недействительным до истечения его срока действия (например, в случае компрометации соответствующего ключа электронной подписи).

Аутентификация

Процесс идентификации пользователя, как правило, на основании его учетной записи. Аутентификация служит для подтверждения того, что входящий в систему пользователь является тем, за кого себя выдает, но процесс аутентификации не затрагивает права доступа пользователя (в отличие от авторизации).

Вариант персонального ключа пользователя

Номер персонального ключа пользователя из резервного набора персональных ключей (РНПК). Изменение варианта персонального ключа пользователя означает, что номер персонального ключа был увеличен на единицу и для создания новых ключей пользователя будет использоваться следующий персональный ключ из РНПК.

Внешний пользователь

Лицо, которое не является пользователем сетевого узла ViPNet и для которого в программе ViPNet Удостоверяющий и ключевой центр издан сертификат ключа проверки электронной подписи.

Вышестоящий удостоверяющий центр

Удостоверяющий центр, который является вышестоящим по отношению к другому удостоверяющему центру в иерархической системе доверительных отношений между удостоверяющими центрами. При этом может быть подчиненным по отношению к третьему удостоверяющему центру, если не является головным.

Головной удостоверяющий центр

Удостоверяющий центр, который находится на вершине иерархической системы доверительных отношений между удостоверяющими центрами.

Группа узлов

Множество сетевых узлов ViPNet, объединенное под общим именем для удобства администрирования. Например, позволяет задать единый пароль администратора для всех сетевых узлов ViPNet, входящих в данную группу.

Дистрибутив ключей

Файл с расширением *.dst, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи 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.

Доверенное лицо (администратор) удостоверяющего центра

Лицо, обладающее правом издавать сертификаты от имени удостоверяющего центра.

Запрос на сертификат

Защищенное электронной подписью сообщение, содержащее имя пользователя, ключ проверки электронной подписи 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).

Идентификатор ключа субъекта

Идентификатор (уникальный номер) ключа электронной подписи владельца сертификата.

Идентификатор объекта (OID)

От англ. «object identifier». Уникальная числовая последовательность, позволяющая однозначно идентифицировать класс или атрибут объекта.

Частным случаем использования OID является обозначение видов атрибутов и классов объектов в стандартах серии X.500.

Иерархия удостоверяющих центров

Система доверительных отношений между удостоверяющими центрами, в которой вышестоящие удостоверяющие центры выпускают сертификаты для подчиненных удостоверяющих центров.

Квалифицированный сертификат

Сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключ защиты

Ключ, на котором шифруется другой ключ.

Ключ защиты УКЦ

Ключ, на котором зашифрована вся информация, хранящаяся в программе ViPNet Удостоверяющий и ключевой центр (список администраторов УКЦ, мастер-ключи, пароли пользователей ViPNet, ключи пользователей, узлов и прочее).

Ключ защиты УКЦ входит в состав ключей администратора УКЦ и зашифрован на ключе защиты данного администратора.

Ключ обмена

Симметричный ключ, известный отправителю и получателю зашифрованной информации, которой обмениваются сетевые узлы ViPNet. Используется для зашифрования и расшифрования передаваемых данных.

Ключ проверки электронной подписи (ключ проверки ЭП)

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом проверки электронной подписи называется открытый ключ, который является несекретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, однозначно связанную с закрытым ключом и предназначенную для проверки подлинности электронной подписи.

Ключ электронной подписи (ключ ЭП)

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом электронной подписи называется закрытый ключ, который является секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Ключевой блокнот ДСДР

CD-диск, содержащий последовательность случайных чисел. Формируется в Федеральной службе безопасности России.

Ключи администратора УКЦ

Формируются при создании учетной записи администратора УКЦ и включают в себя:

- ключ защиты администратора, зашифрованный на пароле администратора;
- ключ защиты УКЦ, зашифрованный на ключе защиты администратора;
- контейнеры с ключами подписи.

Ключи пользователя ViPNet

Совокупность ключей, которые необходимы пользователю для аутентификации в сети ViPNet и шифрования других ключей, и к которым имеет доступ только данный пользователь.

Ключи пользователя могут содержать:

- действующий персональный ключ пользователя;
- ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи;
- хэш пароля пользователя.

Содержимое ключей пользователя формируется в зависимости от типа аутентификации пользователя.

Ключи узла ViPNet

Совокупность ключей, с использованием которых производится шифрование трафика, служебной информации и писем программы ViPNet Деловая почта.

Компрометация ключей

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

Контейнер сертификатов администраторов

Файл формата PKCS #7, который может содержать списки сертификатов издателей (администраторов удостоверяющего центра) и соответствующие им списки отозванных сертификатов. В программе ViPNet Удостоверяющий и ключевой центр используется для установки межсетевого взаимодействия.

Контрольная сумма

Значение, используемое для проверки целостности информации.

Корневой сертификат

Сертификат администратора удостоверяющего центра, являющийся последним сертификатом в цепочке доверия. Другими словами, для корневого сертификата нет сертификата, с помощью которого можно было бы проверить его достоверность. С помощью корневого сертификата проверяется достоверность сертификатов (пользователей и издателей), заверенных этим сертификатом.

Кросс-сертификат

Сертификат уполномоченного лица одного удостоверяющего центра, изданный уполномоченным лицом другого удостоверяющего центра.

Кросс-сертификация

Механизм установления доверительных отношений между удостоверяющими центрами, осуществляемый через выпуск кросс-сертификатов одним УЦ для другого УЦ.

Лицензия на сеть

Разрешение на пользование определенным набором функций продуктовой линейки ViPNet. В частности, лицензия на сеть ViPNet определяет следующее: номер сети, максимальное количество координаторов и клиентов, максимальное суммарное количество адресов, туннелируемых координаторами сети, максимальное количество узлов, на которые можно добавить ту или иную роль, максимальную разрешенную версию программного обеспечения ViPNet, срок действия лицензии и другие параметры.

Мастер-ключ

Ключ, который администратор сети ViPNet использует для формирования симметричных ключей пользователей и узлов. В сети ViPNet формируется три вида мастер-ключей:

- мастер-ключ ключей обмена;
- мастер-ключ ключей защиты ключей обмена;
- мастер-ключ персональных ключей пользователей.

Мастер-ключ формируется с помощью датчика случайных чисел. Он хранится в программе ViPNet Удостоверяющий и ключевой центр в полной секретности, поскольку компрометация мастер-ключа приводит к компрометации всех ключей, сформированных на его основе.

Межсетевое взаимодействие

Информационное взаимодействие, организованное между сетями ViPNet. Позволяет узлам различных сетей ViPNet обмениваться информацией по защищенным каналам. Для организации взаимодействия между узлами различных сетей ViPNet администраторы этих сетей обмениваются межсетевой информацией.

Межсетевой мастер-ключ

Ключ, служащий для формирования ключей обмена между сетевыми узлами разных сетей ViPNet.

Основной узел пользователя

Первый узел, на котором зарегистрирован пользователь.

Пароль администратора сетевого узла ViPNet

Пароль для входа на сетевом узле ViPNet в режим администратора, в рамках которого становятся доступны дополнительные возможности настройки приложений ViPNet. Пароль администратора сетевого узла ViPNet может быть создан администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр.

Пароль администратора УКЦ

Пароль для входа в программу ViPNet Удостоверяющий и ключевой центр.

Пароль пользователя

Индивидуальный пароль пользователя для работы в приложениях ViPNet на сетевом узле ViPNet. Первоначально создается администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager. Этот пароль может быть изменен пользователем на сетевом узле ViPNet.

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 нескольких языках. Фразы представляют собой грамматически корректные конструкции, однако слова, составляющие фразу, выбираются случайным образом из большого по объему словаря. 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 раскладке латиницей 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 «pfn.dtenfclj».

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 «cke;kfnfhtkm». В данном случае, при вводе пароля необходимо набирать по 4 первых буквы каждого слова парольной фразы.

Персональный ключ пользователя

Главный ключ защиты ключей, к которым имеет доступ пользователь. Действующий персональный ключ необходимо хранить в безопасном месте, так как компрометация этого ключа означает компрометацию всех других ключей пользователя, а также ключей защиты, на которых зашифрованы ключи обмена.

См. также: Ключи пользователя ViPNet (см. глоссарий, стр. 212), Компрометация ключей (см. глоссарий, стр. 213), Пользователь ViPNet (см. глоссарий, стр. 216), Резервный набор

персональных ключей (РНПК) (см. глоссарий, стр. 216), ViPNet Удостоверяющий и ключевой центр (УКЦ).

Подчиненный удостоверяющий центр

Удостоверяющий центр, сертификат администратора которого заверен вышестоящим удостоверяющим центром.

Политика применения сертификата

Совокупность правил применения сертификата ключа проверки электронной подписи, определяющих, в каких случаях допустимо или следует использовать данный сертификат в соответствии с требованиями безопасности.

Полномочия пользователя

Разрешения на определенные действия пользователей на сетевом узле ViPNet по изменению настроек некоторых программ ViPNet.

Администратор задает полномочия для всех пользователей сетевого узла ViPNet в свойствах ролей.

Пользователь ViPNet

Лицо, которое использует программное обеспечение ViPNet и имеет ключи для работы с ним.

Публикация

Размещение сформированной в удостоверяющем центре информации на источниках данных, доступных по общеизвестным протоколам (например, FTP, LDAP).

Резервный набор персональных ключей (РНПК)

Набор из нескольких запасных персональных ключей, которые администратор УКЦ создает для пользователя. Имя этого файла имеет маску `AAAA.pk`, где `AAAA` — идентификатор пользователя ViPNet в рамках своей сети. Используется для удаленного обновления ключей пользователя при их компрометации и при смене мастер-ключа персональных ключей.

Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet.

Симметричный ключ

Последовательность битов заданной длины (для алгоритма ГОСТ 28147-89 — 256 бит), используемая как для зашифрования, так и для расшифрования информации.

В программном обеспечении ViPNet симметричные ключи используются для зашифрования и расшифрования IP-трафика, информации приложений (в том числе почтовой), служебных и прикладных конвертов.

Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы администратором удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Справочники

Набор файлов, содержащих информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях.

Справочники и ключи

Справочники, ключи узла (см. глоссарий, стр. 213) и ключи пользователя.

Структура сети ViPNet

Упорядоченная совокупность связей между компонентами сети ViPNet, такими как:

- рабочее место администратора сети ViPNet;
- координаторы;
- клиенты.

Каждый клиент должен быть зарегистрирован на координаторе. Связи между координаторами и рабочим местом администратора, а также между координатором и его клиентами обязательны. Остальные связи создаются в соответствии с корпоративной политикой безопасности.

Точка распространения данных

Источник, доступный по общеизвестным протоколам (например, HTTP или LDAP), используемый для размещения сформированной в удостоверяющем центре информации (сертификатов издателей и списков аннулированных сертификатов).

Транспортный модуль (MFTP)

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

Удостоверяющий центр

Организация, осуществляющая выпуск сертификатов ключей проверки электронной подписи, а также сертификатов другого назначения.

Шаблон сертификата

Частично заполненная структура, содержащая набор расширений, которые определяют назначение сертификата.

Используется при создании запросов на сертификаты и издании сертификатов.

Электронная подпись (ЭП)

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронная рулетка

Встроенный компонент программного обеспечения ViPNet, позволяющий инициализировать датчик случайных чисел по действиям пользователя. Полученная последовательность используется при формировании криптографических ключей.