ViPNet Registration Point 4.6

Руководство администратора

infotecs

ФРКЕ.00111-06 32 01

ОАО «ИнфоТеКС»

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

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

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

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

В данном документе описывается функциональное назначение и применение программы ViPNet Registration Point, принципы работы с программой и ее основные возможности, содержится информация, необходимая для настройки и использования ViPNet Registration Point, а также приводится описание пользовательского интерфейса.

Для кого предназначен документ

Настоящее руководство предназначено для администраторов сетей ViPNet, в которых используются центры регистрации (см. «Центр регистрации» на стр. 205) на базе программного обеспечения ViPNet Registration Point.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

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

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

О программе

Программное обеспечение ViPNet Registration Point позволяет развернуть центр регистрации в сети ViPNet, управляемой с помощью ПО ViPNet Administrator.

Назначение ViPNet Registration Point

Программное обеспечение ViPNet Registration Point предназначено для регистрации и обслуживания внешних пользователей (см. «Внешний пользователь» на стр. 201) и пользователей сети ViPNet (см. «Пользователь ViPNet» на стр. 203) и хранения их регистрационных данных.

В части инфраструктуры PKI (см. «PKI (инфраструктура открытых ключей)» на стр. 199) программа ViPNet Registration Point является связующим звеном между внешними пользователями и удостоверяющим центром (далее — программой ViPNet Удостоверяющий и ключевой центр, УКЦ) и обеспечивает взаимодействие между ними — формирует и обрабатывает запросы на выпуск сертификатов пользователей, аннулирование, приостановление и возобновление их действия.

Рисунок 1. Взаимодействие ViPNet Registration Point в части инфраструктуры PKI

С точки зрения VPN-технологии, ViPNet Registration Point выполняет функции обслуживания пользователей как клиентов защищенной сети ViPNet — формирует запросы на создание дистрибутивов ключей, производит выдачу готовых дистрибутивов ключей.

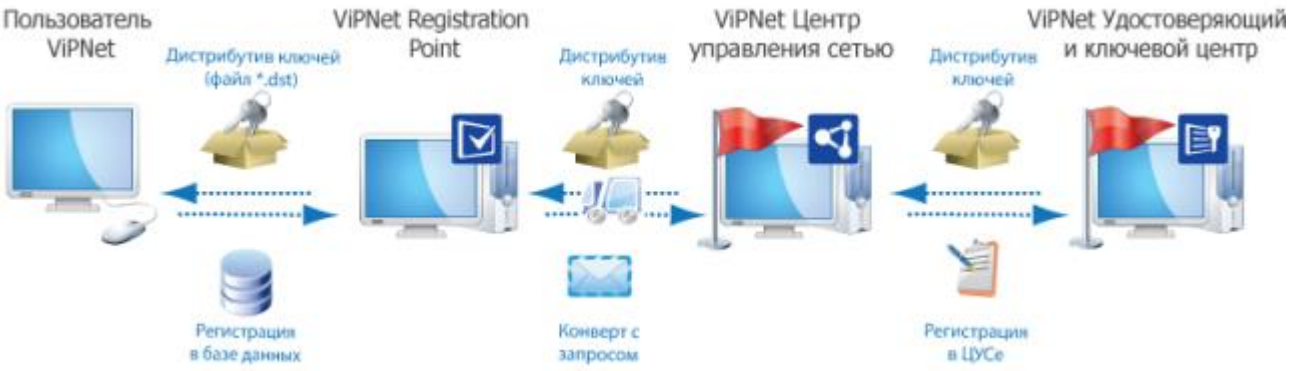


Рисунок 2. Взаимодействие ViPNet Registration Point при обслуживании клиентов сети ViPNet

Используемые компоненты

Программное обеспечение ViPNet Registration Point включает в себя исполняемый модуль.

В процессе своей работе ViPNet Registration Point использует следующие компоненты:

- Транспортный модуль ViPNet MFTP из состава ViPNet Client. Описание компонента см. в документации на ViPNet Client.
- Криптопровайдер ViPNet CSP. Описание компонента см. в документации на данный продукт.
- Систему обновления ViPNet из состава ViPNet Client. Описание компонента см. в документации на ViPNet Client.

Системные требования

Требования к компьютерам для установки ViPNet Registration Point:

- 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 ОС Windows — не менее 2 Гбайт).
- Свободное место на жестком диске — не менее 300 Мбайт.
- Операционная система — Microsoft Windows XP (32-разрядная), Server 2003 (32-разрядная), Vista (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная), Server 2008 R2 (64-разрядная), Windows 8 (32/64-разрядная), Server 2012 (64-разрядная), Windows 8.1 (32/64-разрядная), Server 2012 R2 (64-разрядная).

  Для операционной системы должен быть установлен самый последний пакет обновлений.
- При использовании Internet Explorer — версия 6.0 и выше.

Комплект поставки

В комплект поставки программного обеспечения ViPNet Registration Point входит:

- Установочный файл `setup.exe`.
- Документ«ViPNet Registration Point. Руководство администратора» (данный документ).

Новые возможности версии 4.6

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Registration Point версии 4.6 по сравнению с версией 4.5.

- **Изменена процедура создания запроса на дистрибутив ключей**

  В связи с тем, что был реализован новый способ аутентификации пользователей в ПО ViPNet на сетевых узлах по сертификату, при создании запроса на дистрибутив ключей с помощью мастера вы можете задать способ аутентификации пользователя. Отображение данной страницы мастера зависит от настроек программы ViPNet Registration Point.

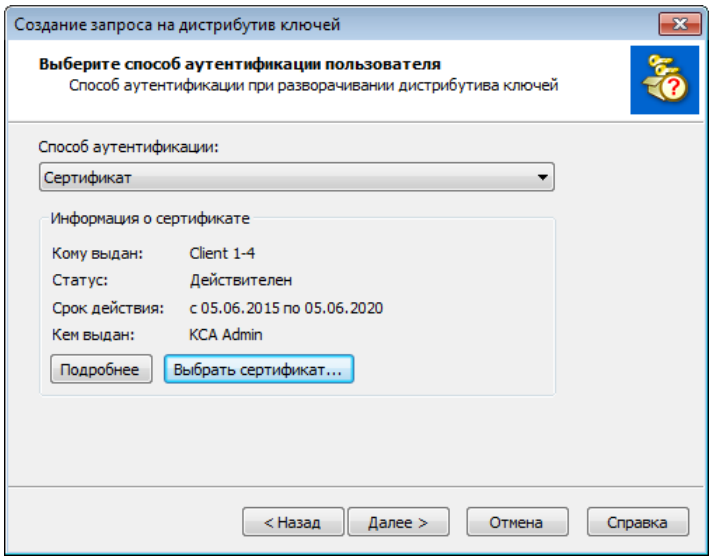


Рисунок 3. Настройка аутентификации по сертификату

- **Расширены возможности загрузки данных Active Directory**

  Теперь при регистрации пользователей вы можете искать в Active Directory данные не только о пользователях, но и о компьютерах, входящих в домен.

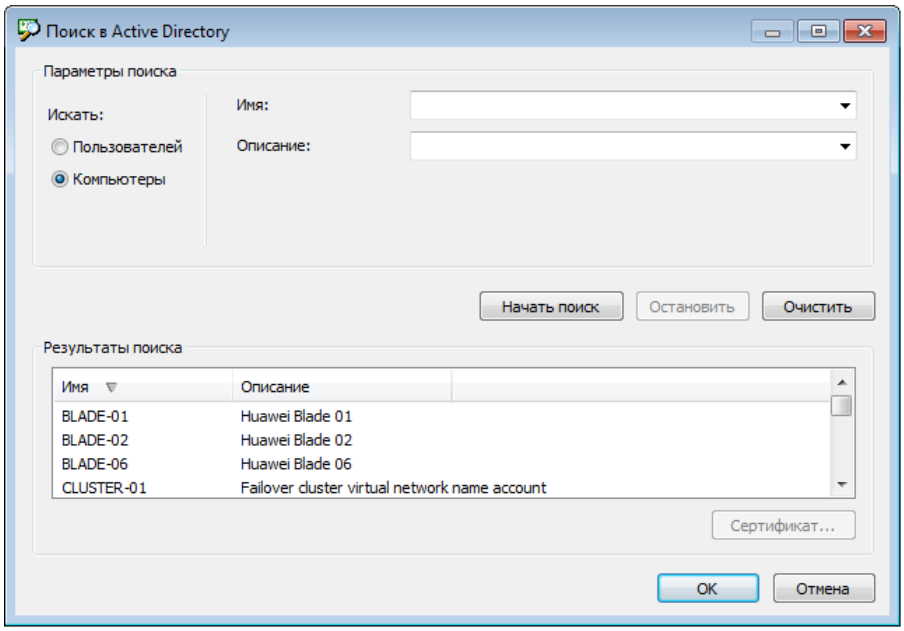


Рисунок 4. Поиск компьютеров в Active Directory

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС»:

- Веб-портал документации ViPNet http://docs.infotecs.ru.
- Описание продуктов ViPNet http://www.infotecs.ru/products/line/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/.
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet http://www.infotecs.ru/forum.
- Законодательная база в сфере защиты информации http://www.infotecs.ru/laws/.

Контактная информация

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

- Техническая поддержка для пользователей продуктов ViPNet: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки http://www.infotecs.ru/support/request/.
- Регистрация продуктов и консультации по телефону для клиентов, имеющих расширенный уровень технического сопровождения:

  8 (495) 737-6196,

  8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется политикой ответственного разглашения http://infotecs.ru/products/disclosure.php. Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru.

1

Общие сведения

Основные возможности программы ViPNet Registration Point

Основные возможности программы ViPNet Registration Point представлены в таблице ниже. Для удобства они распределены на три категории: общая функциональность, функциональность в части технологии PKI и функциональность с точки зрения технологии VPN.

Категория	Функциональная возможность	Ссылка
Общие	**Регистрация пользователей ViPNet**. Программа позволяет регистрировать пользователей ViPNet	Регистрация пользователей (на стр. 66)
	Возможность импорта данных из LDAP Active Directory. Регистрацию пользователей можно производить на основе данных из домена Active Directory	Регистрация через Active Directory (на стр. 69)
	Удаление учетных записей пользователей. Программа позволяет удалять учетные записи зарегистрированных пользователей: внешних пользователей — из базы данных ViPNet Registration Point, пользователей сети ViPNet — из программы ViPNet Центр управления сетью по соответствующему запросу	Удаление учетных записей пользователей (на стр. 80)
	Ведение журнала событий. Регистрация событий и учет действий администратора программы ViPNet Registration Point	Работа с журналом событий программы ViPNet Registration Point (на стр. 152)
	Использование резервных копий конфигураций программы ViPNet Registration Point. Возможность создания резервных копий конфигураций программы и восстановления конфигураций из резервных копий	Работа с резервными копиями конфигураций программы (на стр. 146)
В части технологии PKI	**Создание запросов на выдачу сертификатов ключа проверки электронной подписи**. Для зарегистрированных пользователей ViPNet можно формировать запросы на получение сертификата ключа проверки электронной подписи	Создание запроса на новый сертификат (на стр. 93)
	Добавление сертификата пользователя в контейнер ключей. При получении сертификата возможно его добавление в контейнер ключей	Добавление сертификата в контейнер ключей (на стр. 116)

Категория	Функциональная возможность	Ссылка
	Создание запросов на аннулирование сертификатов пользователей, приостановление и возобновление их действия. От имени администратора ViPNet Registration Point можно формировать запросы на аннулирование, приостановление и возобновление действия изданных сертификатов пользователей	Аннулирование сертификата (на стр. 111) Приостановление действия сертификата (на стр. 109) Возобновление действия сертификата (на стр. 110)
	Обработка запросов на сертификаты от внешних пользователей. Прием запросов на получение или обновление сертификатов от внешних пользователей в формате PKCS#10 или CMC и выдача готовых сертификатов по данным запросам	Обработка запросов на сертификаты от внешних пользователей (на стр. 102)
	Экспорт сертификатов пользователей. Возможен экспорт полученных сертификатов пользователей в различные форматы	Экспорт сертификата (на стр. 113)
	Просмотр контейнеров ключей. Возможен просмотр параметров контейнеров ключей ,созданных в программе или пользователями	Просмотр свойств контейнера ключей (на стр. 127)
В части технологии VPN	**Создание запросов на дистрибутивы ключей или их обновления.** Для зарегистрированных пользователей ViPNet можно формировать запросы на получение или обновление дистрибутивов ключей ViPNet	Создание запроса на дистрибутив ключей (на стр. 130) Создание запроса на обновление дистрибутива ключей (на стр. 131)
	Обработка дистрибутивов ключей. Перенос или распаковка созданных дистрибутивов ключей для передачи пользователям	Перенос дистрибутива в папку (на стр. 141) Распаковка дистрибутива ключей (на стр. 143)

Работа в ViPNet Registration Point без ключа электронной подписи и сертификата

Если в вашем дистрибутиве ключей отсутствует ключ электронной подписи (на стр. 202) и соответствующий сертификат ключа проверки электронной подписи (на стр. 204), работа в программе ViPNet Registration Point будет возможна со следующими ограничениями:

- Вы не сможете создавать запросы на сертификаты для пользователей (см. «Создание запроса на новый сертификат» на стр. 93). В интерфейсе программы будут отсутствовать все элементы, связанные с созданием и управлением запросов на сертификаты зарегистрированных пользователей, просмотром полученных сертификатов, списков аннулированных сертификатов (CRL).

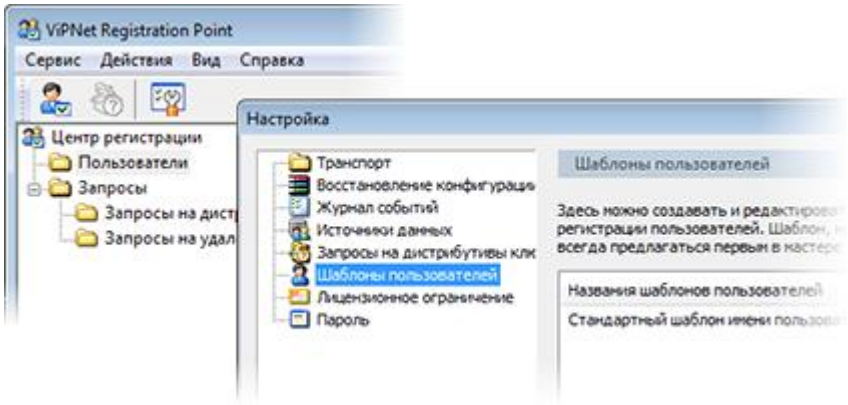


Рисунок 5. Ограничение интерфейса программы при работе без ключа электронной подписи

- Дистрибутивы ключей пользователей, поступающие из программы ViPNet Удостоверяющий и ключевой центр по вашим запросам, не будут содержать ключи электронной подписи и сертификаты ключей проверки электронной подписи (см. «Создание запроса на дистрибутив ключей» на стр. 130).
- В настройках параметров безопасности будут отсутствовать элементы, с помощью которых производится работа с сертификатами администратора центра регистрации (см. «Работа с сертификатами» на стр. 145) и работа с контейнерами ключей (см. «Работа с контейнером ключей» на стр. 145).

Для снятия перечисленных ограничений вам требуется запросить у администратора УКЦ сертификат ключа проверки электронной подписи. Ключ электронной подписи в данном случае вы можете сформировать сами с помощью программы ViPNet CSP (подробнее см. документ «ViPNet CSP. Руководство пользователя») либо получить в составе ключей из УКЦ вместе с сертификатом, а затем его обновить (см. «Обновление ключа электронной подписи и сертификата» на стр. 145).

Лицензионные ограничения

Использование ViPNet Registration Point осуществляется в соответствии с лицензионными ограничениями, которые задаются администратором сети в программе ViPNet Центр управления сетью при назначении узлу роли «Registration Point». Лицензия на ViPNet Registration Point определяет максимальное число запросов на дистрибутивы ключей и сертификаты пользователей, которые можно сформировать в программе.

Чтобы просмотреть параметры лицензии, выполните следующие действия:

1 В окне программы ViPNet Registration Point в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка** на панели инструментов.

2 В появившемся окне на панели навигации выберите раздел **Лицензионное ограничение**.

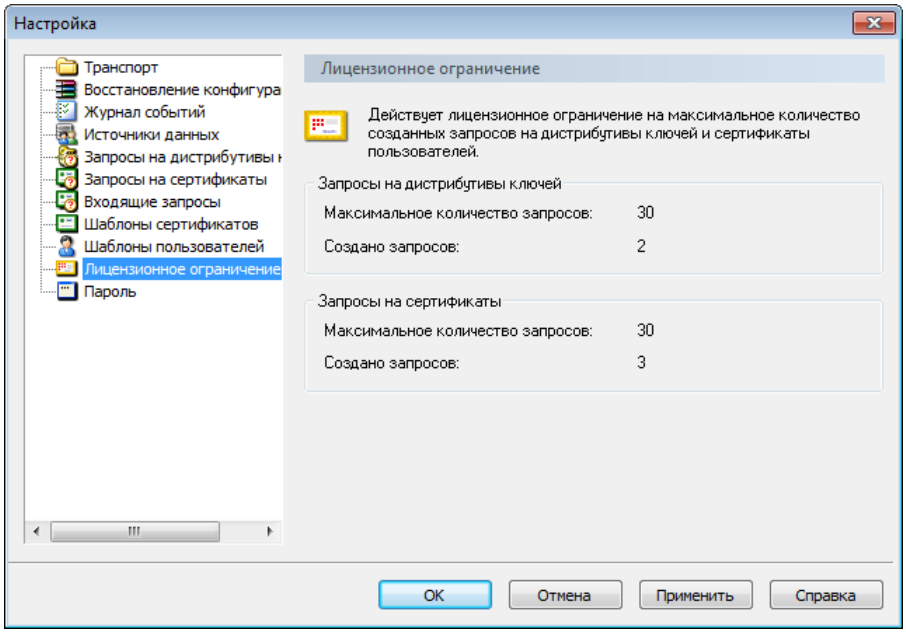


Рисунок 6. Просмотр лицензионных ограничений

В разделе **Лицензионное ограничение** можно получить следующие сведения:

- число запросов на дистрибутивы ключей и сертификаты, которые позволяет создать лицензия;
- число уже созданных запросов.

Примечание. Число запросов на создание дистрибутивов ключей зависит от числа клиентских узлов (см. «Клиент (ViPNet-клиент)» на стр. 202), указанного в лицензионном файле. Число запросов на сертификаты пользователей лицензией может не ограничиваться.

Если в процессе работы с программой число созданных запросов превысит или станет равным максимальному, создание нового запроса будет невозможно. В случае удаления учетных записей

пользователей из базы данных ViPNet Registration Point число созданных запросов уменьшается, поскольку вместе с регистрационными сведениями удаляются и сформированные для них запросы (см. раздел Удаление учетных записей пользователей (на стр. 80)).

Чтобы увеличить максимально допустимое число создаваемых запросов, обратитесь к администратору сети ViPNet и закажите новую лицензию. При удовлетворении запроса на расширение лицензии администратор вышлет вам обновление справочников и ключей (на стр. 39), после принятия которого вы будете использовать расширенную лицензию.

2

Установка, обновление и удаление программы ViPNet Registration Point

Порядок действий при типовом варианте развертывания программы ViPNet Registration Point

При развертывании на сетевом узле программы ViPNet Registration Point вместе с программой ViPNet Client выполните все задачи из приведенного ниже списка.

Таблица 3. Последовательность действий при типовом варианте установки ViPNet Registration Point

	Задача	Ссылка на раздел или документ для использования
☐	Установите программу ViPNet Registration Point.	Установка программы (на стр. 23).
☐	Установите программу ViPNet Client.	Документ «ViPNet Client Монитор. Руководство пользователя», раздел «Установка ПО ViPNet Client».
☐	Установите справочники и ключи с помощью дистрибутива ключей. При использовании нескольких программ ViPNet на одном сетевом узле справочники и ключи помещаются в папку установки одной из них. В связи с этим в процессе установки справочников и ключей укажите одну из программ: ViPNet Registration Point или ViPNet Client. В результате справочники и ключи будут помещены только в папку установки выбранной программы.	Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet (на стр. 35).
☐	При запуске второй программы, для которой не были установлены справочники и ключи, укажите папку ключей узла. В качестве папки ключей узла выберите папку установки программы, в которую были помещены справочники и ключи на предыдущем шаге.	Использование справочников и ключей, установленных ранее (на стр. 38).

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

Установка программы

Перед установкой ПО ViPNet Registration Point убедитесь, что на компьютере выполнены стандартные сетевые настройки, а также правильно заданы часовой пояс, дата и время.

Если ViPNet Registration Point устанавливается на компьютер с операционной системой Windows, локализация которой отличается от русской, для правильного отображения кириллицы в интерфейсе ViPNet Registration Point нужно изменить региональные настройки Windows (см. «Региональные настройки» на стр. 192).

Установку должен выполнять пользователь, обладающий правами администратора в ОС Windows.

Для установки ViPNet Registration Point требуются:

- Установочный EXE-файл программы.
- Дистрибутив ключей (на стр. 201) для сетевого узла (файл *.dst). Если на узле планируется работа нескольких пользователей, для каждого из них нужен отдельный дистрибутив ключей.

  Перед формированием dst-файла сетевому узлу, на котором будет установлена программа ViPNet Registration Point, требуется назначить роль «Registration Point» в программе ViPNet Центр управления сетью, причем при регистрации должно быть указано максимальное число запросов на дистрибутивы ключей и сертификаты, которые можно сформировать в ViPNet Registration Point на данном узле. Подробнее см. документ «ViPNet Центр управления сетью. Руководство администратора», раздел «Добавление ролей на сетевые узлы».
- Пароль пользователя сетевого узла или внешнее устройство аутентификации. Список доступных устройств хранения данных и полезная информация об использовании устройств приведена в документе «ViPNet CSP. Руководство пользователя».

  Дистрибутив ключей и пароль пользователя (либо внешнее устройство) нужно получить у администратора сети ViPNet.

Для установки ПО ViPNet Registration Point выполните следующие действия:

1 Запустите установочный файл. Начнется установка ViPNet CSP (на стр. 11). Дождитесь, пока завершится установка ViPNet CSP и подготовка к установке ViPNet Registration Point.

Примечание. После запуска программы установки может появиться предупреждение системы безопасности о невозможности проверить сертификат подписи файла установки. В этом случае см. указания раздела Невозможно проверить сертификат, которым подписан файл установки программы (на стр. 180).

---

2 Ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку **Продолжить**.

3 Если вы хотите настроить параметры установки, нажмите кнопку **Настроить** и укажите:

   - путь к папке установки программы ViPNet Registration Point на компьютере;

- имя пользователя и название организации;
- название папки для программы ViPNet Registration Point в меню **Пуск**.

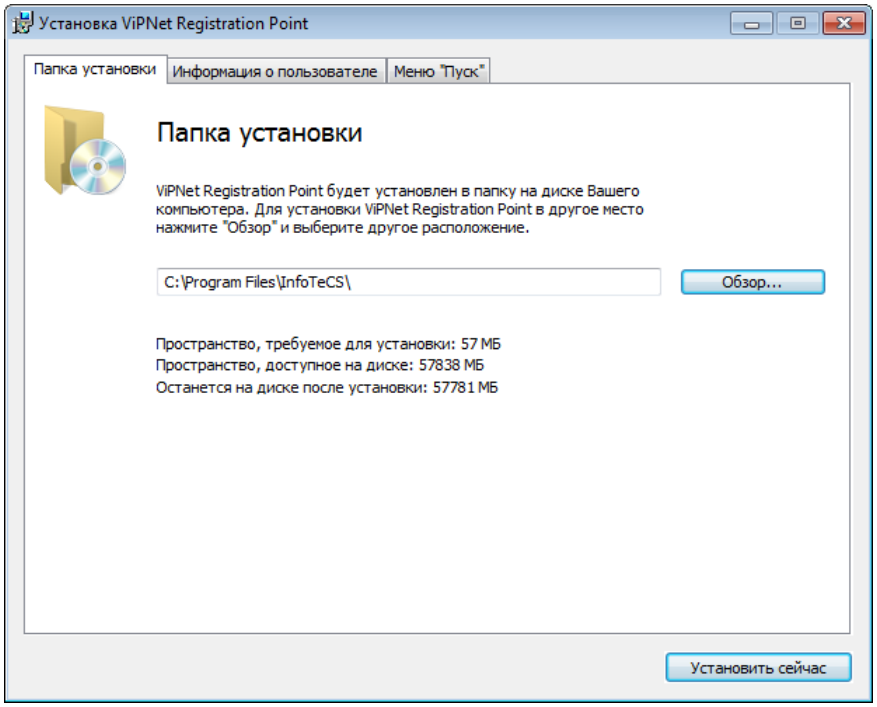


Рисунок 7. Настройка параметров установки ViPNet Registration Point

4 Чтобы начать установку ViPNet Registration Point, нажмите кнопку **Установить сейчас**.

5 Если после завершения установки появится сообщение о необходимости перезагрузить компьютер, выполните перезагрузку.

6 В зависимости от наличия на компьютере справочников и ключей, установленных ранее, выполните одно из действий:

- Если справочники и ключи еще не установлены на компьютере, выполните их установку (см. «Установка справочников и ключей» на стр. 30).
- Если на компьютере уже имеется программное обеспечение ViPNet, для которого ранее были установлены справочники и ключи, при запуске программы ViPNet Registration Point укажите путь к папке ключей сетевого узла (см. «Использование справочников и ключей, установленных ранее» на стр. 38).

Внимание! В данном случае получать новый файл дистрибутива ключей для ПО ViPNet Registration Point у администратора сети ViPNet и устанавливать ключи из этого файла крайне не рекомендуется, поскольку это может привести к сбоям в работе программного обеспечения ViPNet.

Обновление программы

Внимание. Допускается обновление только сертифицированной версии ПО ViPNet Registration Point.

Программу Registration Point вы можете обновить на сетевом узле только вручную с помощью установочного файла.

Для обновления программы ViPNet Registration Point получите установочный файл новой версии программного обеспечения. Затем выполните следующие действия:

1. Завершите работу программы ViPNet Registration Point.
2. Запустите установочный файл программы  . Дождитесь, пока завершится подготовка к установке ViPNet Registration Point.
3. В окне **Установка ViPNet Registration Point** нажмите кнопку **Начать обновление**.
4. По окончании процесса обновления нажмите кнопку **Закрыть**.
5. Если появится сообщение о необходимости перезагрузить компьютер, выполните перезагрузку.

Удаление программы

В случае необходимости вы можете удалить с компьютера программу ViPNet Registration Point. Перед удалением программы рекомендуется сделать резервную копию базы данных `rc.mdb`, в которой хранится информация о зарегистрированных пользователях, созданных запросах, полученных сертификатах и другое. При удалении программы ViPNet Registration Point вы можете сохранить пользовательские данные, необходимые для запуска и использования программы: справочники и ключи ViPNet, настройки параметров работы программы.

Чтобы удалить программу ViPNet Registration Point, выполните следующие действия:

1. Завершите работу программы ViPNet Registration Point.
2. Запустите установочный файл программы  . Дождитесь, пока завершится подготовка к удалению ViPNet Registration Point.
3. На странице изменения установленных компонентов выберите пункт **Удалить все компоненты**.
4. Нажмите кнопку **Продолжить**.
5. В зависимости от того, хотите ли вы сохранить пользовательские данные, установите или снимите флажок **Удалить пользовательские данные**.
6. Для продолжения нажмите кнопку **Удалить**.
7. Дождитесь завершения удаления программного обеспечения и нажмите кнопку **Закрыть**.
8. Если появится сообщение о необходимости перезагрузить компьютер, выполните перезагрузку.

Совет. Вы также можете полностью удалить ViPNet Registration Point, в меню **Пуск** выбрав **Все программы** > **ViPNet** > **ViPNet Registration Point** > **Установка ViPNet Registration Point**. При этом пользовательские данные не будут сохранены.

Перенос сетевого узла на другой компьютер

При необходимости вы можете перенести функционирующий сетевой узел с развернутым ПО ViPNet Registration Point с одного компьютера на другой (например, в случае замены устаревшего компьютера), сохранив при этом текущие настройки программы и все регистрационные сведения. Для этого вам нужно скопировать на новый компьютер справочники и ключи ViPNet, базу данных и другие данные из папки программы ViPNet Registration Point.

Путем переноса справочников и ключей можно восстановить сетевой узел после переустановки операционной системы или после изменения папки установки программы ViPNet Registration Point.

Внимание! Не следует использовать данный сценарий для переноса сетевого узла с 32-разрядной версии операционной системы Windows на 64-разрядную версию Windows и наоборот, поскольку в этом случае возможна некорректная работа программного обеспечения ViPNet.

После переноса справочников и ключей следует удалить их исходный экземпляр. Недопустима ситуация, когда одни и те же справочники и ключи используются на разных узлах.

Для переноса справочников и ключей выполните следующие действия:

1. Скопируйте на съемный носитель или в другое надежное место следующие вложенные папки и файлы, находящиеся в папке установки программы ViPNet Registration Point:
   - `\d_station`;
   - Папку ключей пользователя, обычно `\user_AAAA` (где `AAAA` — шестнадцатеричный идентификатор пользователя ViPNet без номера сети).

     В некоторых случаях папка ключей пользователя может совпадать с папкой установки программы, тогда следует скопировать папку `\key_disk`.
   - Файлы `APAXXXX.TXT`, `APCXXXX.TXT`, `APIXXXX.TXT`, `APLXXXX.TXT`, `APNXXXX.CRC`, `APNXXXX.CRG`, `APNXXXX.TXT`, `APSXXXX.TXT`, `APUXXXX.TXT` (где XXXX — шестнадцатеричный идентификатор сетевого узла без номера сети).
   - `infotecs.re`;
   - `nodeXXXX.tun`;
   - `mftp.ini`;
   - Базу данных `rc.mdb`;
   - Файл с настройками программы `regpoint.ini`.

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

2 Перед переносом справочников и ключей на новый компьютер установите на этот компьютер программу ViPNet Registration Point (см. «Установка программы» на стр. 23), но не выполняйте установку справочников и ключей.

3 При переносе справочников и ключей на компьютер, на котором уже установлена программа ViPNet Registration Point, убедитесь, что на этом компьютере не используются справочники и ключи ViPNet другого сетевого узла. Если такая информация присутствует, удалите следующие папки и файлы:

- папку ключей пользователя `\user_AAAA`;
- файлы `AP*.TXT`, `APNXXXX.CRC`, `APNXXXX.CRG`.

4 Файлы и папки, скопированные на шаге 1, поместите в новую папку установки программы ViPNet Registration Point.

5 В файле `mftp.ini` укажите путь к новой папке установки программы ViPNet Registration Point в значениях всех параметров, где он встречается.

6 Запустите программу ViPNet Registration Point. В окне ввода пароля щелкните значок  справа от кнопки **Настройка** и выберите пункт **Папка ключей пользователя**. Укажите путь к папке ключей пользователя.

7 Выполните вход в программу (см. «Способы аутентификации пользователя» на стр. 50).

8 Установите контейнер ключей (см. «Установка контейнера ключей» на стр. 145).

9 На компьютере, с которого вы осуществили перенос сетевого узла, удалите исходные экземпляры справочников и ключей.

После выполнения перечисленных действий программа ViPNet Registration Point готова к работе.

Для переноса только базы данных, созданной в процессе работы ViPNet Registration Point, достаточно скопировать в папку установки программы на другом компьютере файл базы данных (`rc.mdb`).

3

Установка и обновление справочников и ключей

Установка справочников и ключей

Установка справочников и ключей выполняется при развертывании ПО ViPNet на сетевом узле, при добавлении новых пользователей ViPNet на сетевой узел, а также в других случаях, когда справочники и ключи, установленные на узле, были повреждены или являются устаревшими.

Если вы хотите выполнить первоначальную установку справочников и ключей на сетевом узле с одним пользователем, выполните рекомендации раздела Установка справочников и ключей одного пользователя (на стр. 31).

В случаях, описанных ниже, перед установкой дополнительно ознакомьтесь с соответствующими разделами:

- Если вы хотите организовать работу нескольких пользователей на одном сетевом узле или добавить нового пользователя на сетевой узел, на котором уже работают другие пользователи, см. раздел Установка справочников и ключей нескольких пользователей на одном сетевом узле (на стр. 33).
- Если вы хотите самостоятельно задать папки, в которых будут храниться справочники и ключи, см. раздел Расширенный режим установки справочников и ключей (на стр. 33).
- Если на сетевом узле имеется несколько программ ViPNet, но ни для одной из них не установлены справочники и ключи, см. раздел Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet (на стр. 35).

Примечание. Если на узле уже установлены справочники и ключи для какой-либо программы ViPNet, выполните указания раздела Использование справочников и ключей, установленных ранее (на стр. 38).

- Если в результате программного или системного сбоя вы не можете войти в программу ViPNet Registration Point и необходимо выполнить повторную установку справочников и ключей, см. раздел Повторная установка справочников и ключей после сбоя программы (на стр. 36).

В сети ViPNet, управляемой с помощью ПО ViPNet Administrator, в составе первоначального дистрибутива ключей каждому пользователю передается резервный набор персональных ключей (РНПК) (на стр. 204). Файл, в котором содержится резервный набор ключей, имеет вид `AAAA.pk` (где `AAAA` — идентификатор пользователя в сети ViPNet). Во время установки справочников и ключей он помещается в папку ключей пользователя (см. «Папка ключей пользователя» на стр. 203).

Из соображений безопасности после первичной установки справочников и ключей рекомендуется переместить файл резервного набора из папки ключей пользователя на внешнее устройство для хранения в безопасном месте, не доступном для посторонних лиц (например, в сейфе). После получения резервного набора ключей пользователи сети ViPNet несут личную ответственность за его хранение.

Внимание! Если обнаружен факт доступа посторонних лиц к вашему резервному набору ключей либо если вы подозреваете, что такой факт имел место, следуйте рекомендациям раздела Действия при компрометации ключей (на стр. 46).

Установка справочников и ключей одного пользователя

Для установки справочников и ключей (см. «Справочники и ключи» на стр. 205) выполните следующие действия:

1. Получите дистрибутив ключей у администратора сети ViPNet.
2. Завершите работу всех компонентов программы ViPNet Registration Point (см. «Запуск и завершение работы с программой» на стр. 49).
3. Запустите программу установки ключей сети ViPNet одним из двух способов:
   - Дважды щелкните файл дистрибутива ключей.
   - Запустите программу ViPNet Registration Point (см. «Запуск и завершение работы с программой» на стр. 49). Затем в окне ввода пароля щелкните значок справа от кнопки **Настройка** и в меню выберите пункт **Установить ключи**.

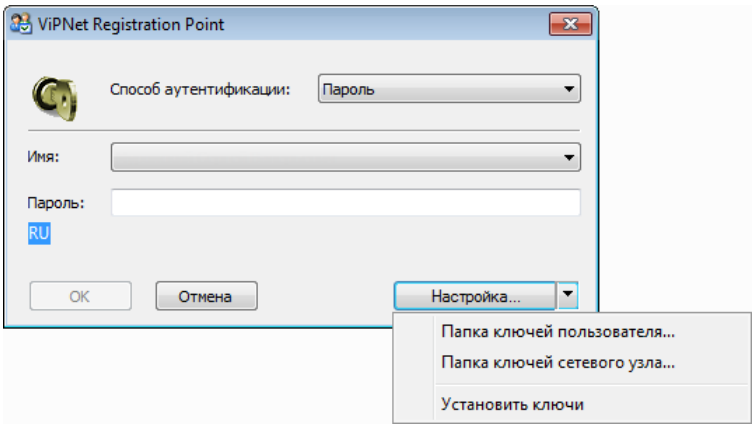


Рисунок 8. Запуск программы установки ключей

4. Если при запуске программы установки ключей будут обнаружены работающие приложения ViPNet, будет выведено сообщение о необходимости завершить их работу. Закройте указанные приложения и нажмите кнопку **Повтор**.
5. Если на странице **Укажите файл дистрибутива ключей** не указано местоположение файла дистрибутива, задайте его с помощью кнопки **Обзор**.
6. Убедитесь, что выбран дистрибутив ключей, предназначенный именно для текущего сетевого узла. Имя сетевого узла и имя пользователя отображаются ниже поля для указания пути к файлу дистрибутива. При необходимости укажите другой дистрибутив ключей.

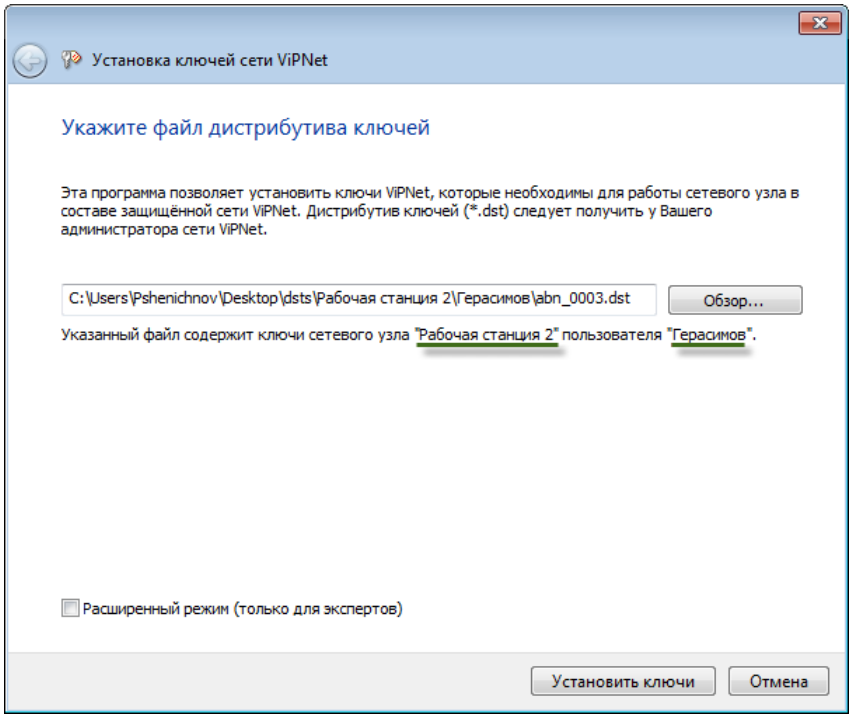


Рисунок 9. Выбор файла дистрибутива ключей

По умолчанию справочники и ключи устанавливаются в одну папку `C:\ProgramData\Infotecs\<папка с идентификатором узла>`.

При необходимости вы можете указать другую папку (или две папки) для их установки (см. «Расширенный режим установки справочников и ключей» на стр. 33).

7 Нажмите кнопку **Установить ключи**.

Примечание. Кнопка **Установить ключи** может быть скрыта в том случае, если на сетевом узле установлено несколько программ ViPNet (см. «Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet» на стр. 35).

8 Если установка ключей прошла успешно, появится соответствующее сообщение.

9 Для просмотра информации о выполненной установке ключей щелкните ссылку **Подробнее о произведенных действиях**. Для завершения установки ключей нажмите кнопку **Закрыть**.

Если выполнить установку ключей не удалось, внимательно ознакомьтесь с сообщением о возникших ошибках и обратитесь к администратору сети ViPNet для их устранения.

Примечание. Если при установке ключей будут найдены ранее установленные ключи для этого узла, новые ключи будут установлены в ту же папку поверх предыдущих.

После успешной установки ключей можно запустить ПО ViPNet Registration Point.

Установка справочников и ключей нескольких пользователей на одном сетевом узле

Если на сетевом узле планируется работа нескольких пользователей, установите ключи для каждого пользователя.

Если на сетевом узле уже работают пользователи, и вы хотите добавить на узел новых пользователей, для установки вам понадобятся только ключи новых пользователей.

Примечание. Справочники и ключи нескольких пользователей из разных сетей ViPNet не могут быть установлены на одном компьютере.

Для установки справочников и ключей нескольких пользователей на одном компьютере выполните следующие действия:

1. Для каждого нового пользователя получите дистрибутив ключей у администратора сети ViPNet.
2. Последовательно выполните установку справочников и ключей (см. «Установка справочников и ключей одного пользователя» на стр. 31) с использованием дистрибутива каждого нового пользователя.

В результате в окне входа в программу (см. «Запуск и завершение работы с программой» на стр. 49) в списке учетных записей будут отображаться пользователи, справочники и ключи которых вы установили.

Расширенный режим установки справочников и ключей

По умолчанию справочники и ключи устанавливаются в папку `C:\ProgramData\Infotecs\<папка с идентификатором узла>`. При необходимости вы можете использовать расширенный режим установки, который позволяет вам самостоятельно задать папки для установки справочников и ключей. Такая необходимость может возникнуть, если из соображений безопасности вы хотите хранить справочники и ключи на специальном съемном носителе.

Папки, в которые производится установка справочников и ключей в расширенном режиме установки, должны отвечать следующим требованиям:

- В папках не должны находиться справочники и ключи другой программы ViPNet.
- У вас должно быть право на изменение и запись файлов в данных папках.
- Информационная защита папок должна отвечать требованиям безопасности вашей организации.
- ПО ViPNet Registration Point должно иметь постоянный доступ к данным папкам.

Внимание! Неправильно заданные параметры установки могут привести к сбоям в работе программы. Не рекомендуется использовать данный режим без необходимости.

Для установки ключей в расширенном режиме выполните следующие действия:

1 Получите новый дистрибутив ключей у администратора сети ViPNet.

2 Следуйте указаниям раздела Установка справочников и ключей одного пользователя (на стр. 31).

На странице указания файла дистрибутива ключей установите флажок **Расширенный режим (только для экспертов)** и нажмите кнопку **Далее**.

3 На следующей странице мастера:

- В поле **Папка ключей сетевого узла** укажите папку для установки справочников и ключей сетевого узла.
- В поле **Папка ключей пользователя** (на стр. 203) укажите папку для установки ключей пользователя.

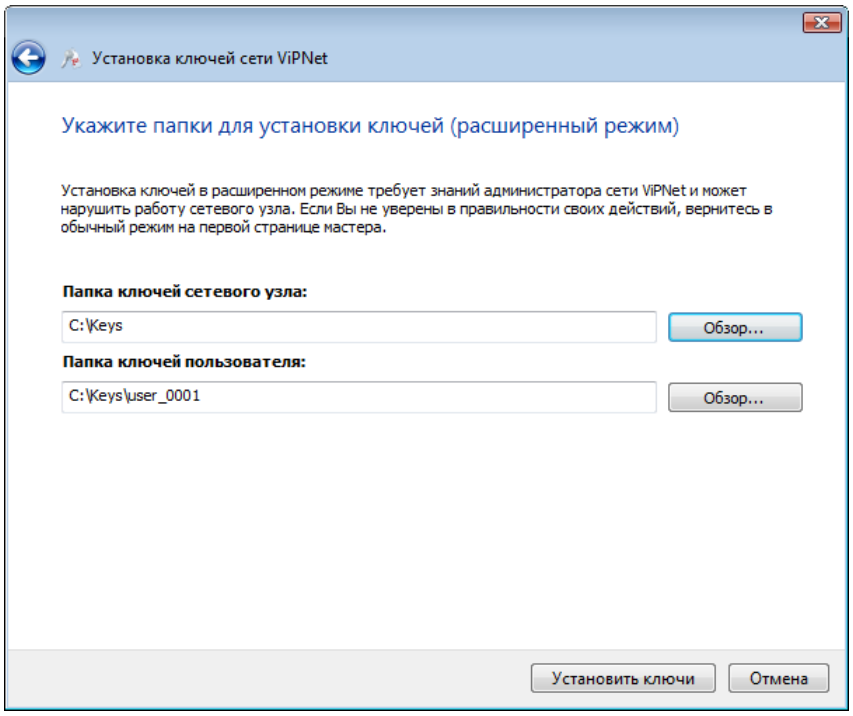


Рисунок 10. Указание папок для установки ключей узла и ключей пользователя в расширенном режиме

4 Для начала установки нажмите кнопку **Установить ключи**.

5 Если установка ключей прошла успешно, в завершающем окне будет выведено соответствующее сообщение. Для просмотра информации о выполненной установке ключей щелкните ссылку **Подробнее о произведенных действиях**. Для завершения установки ключей нажмите кнопку **Закрыть**.

Если выполнить установку ключей не удалось, внимательно ознакомьтесь с сообщением о возникших ошибках и обратитесь к администратору сети ViPNet для их устранения.

6 При первом запуске программы ViPNet Registration Point укажите папки, в которые были установлены ключи сетевого узла и пользователя:

- В окне ввода пароля щелкните значок  справа от кнопки **Настройка** и выберите пункт **Папка ключей сетевого узла**. В окне **Обзор папок** укажите путь к папке ключей узла.
- Снова щелкните значок  справа от кнопки **Настройка** и выберите пункт **Папка ключей пользователя**. Укажите путь к папке ключей пользователя.

Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet

Если на сетевом узле установлено несколько программ ViPNet, но при этом ни для одной из них не установлены справочники и ключи, то необходимо указать приложение, в папке установки которого будут храниться справочники и ключи.

Внимание! Если на узле уже имеются справочники и ключи для какой-либо из программ ViPNet, устанавливать новые справочники и ключи нельзя. В этом случае выполните указания раздела Использование справочников и ключей, установленных ранее (на стр. 38).

Для установки справочников и ключей выполните следующие действия:

1 Начните установку справочников и ключей (см. «Установка справочников и ключей одного пользователя» на стр. 31). После указания файла дистрибутива ключей нажмите кнопку **Далее**.

2 В окне выбора приложения ViPNet выберите **ViPNet Registration Point**. В результате для установки справочников и ключей будет использована папка установки ПО ViPNet Registration Point.

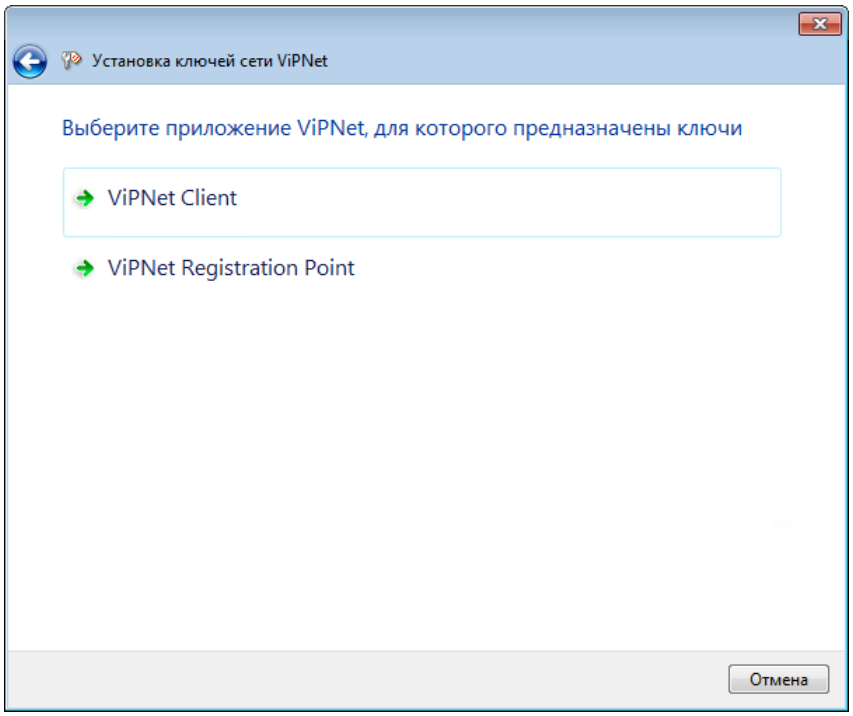


Рисунок 11. Выбор программы, для которой устанавливаются ключи

Примечание. В расширенном режиме установки ключей (см. «Расширенный режим установки справочников и ключей» на стр. 33) данное окно не отображается.

---

3 Если установка ключей прошла успешно, в завершающем окне будет выведено соответствующее сообщение. Для просмотра информации о выполненной установке ключей щелкните ссылку **Подробнее о произведенных действиях**. Для завершения установки ключей нажмите кнопку **Закрыть**.

   Если выполнить установку ключей не удалось, внимательно ознакомьтесь с сообщением о возникших ошибках и обратитесь к администратору сети ViPNet для их устранения.

4 При первом запуске других программ ViPNet, установленных на узле, в качестве папки ключей узла укажите папку установки программы ViPNet Registration Point.

После успешной установки ключей можно запустить ПО ViPNet Registration Point.

Повторная установка справочников и ключей после сбоя программы

Если в результате программного или системного сбоя вы не можете войти в программу ViPNet Registration Point, рекомендуется обратиться в службу поддержки для восстановления доступа к программе. В исключительных случаях вы можете получить у администратора сети ViPNet новый дистрибутив ключей и выполнить повторную установку справочников и ключей.

Внимание! Крайне не рекомендуется проводить повторную установку ключей без особой необходимости.

Для повторной установки справочников и ключей на сетевом узле выполните следующие действия:

1. Получите у администратора сети ViPNet новый дистрибутив ключей.
2. Установите справочники и ключи (см. «Установка справочников и ключей одного пользователя» на стр. 31), используя полученный дистрибутив.

Использование справочников и ключей, установленных ранее

В момент установки программы ViPNet Registration Point на сетевом узле уже могут иметься другие программы ViPNet, для работы которых установлены справочники, ключи сетевого узла и транспортный модуль MFTP. В этом случае задайте в программе ViPNet Registration Point папку ключей сетевого узла, которую используют установленные ранее программы ViPNet.

Примечание. Если на сетевом узле не установлены справочники и ключи ни для одной из программ ViPNet, выполните указания раздела Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet (на стр. 35).

Чтобы указать папку ключей сетевого узла, выполните следующие действия:

1. Запустите программу ViPNet Registration Point (см. «Запуск и завершение работы с программой» на стр. 49).
2. В окне ввода пароля щелкните значок  справа от кнопки **Настройка** и выберите пункт **Папка ключей сетевого узла**.
3. В окне **Обзор папок** укажите путь к нужной папке ключей узла.

Примечание. По умолчанию папкой ключей сетевого узла является папка `C:\ProgramData\Infotecs\<папка с идентификатором узла>`.

После задания папки ключей сетевого узла вы можете приступать к работе с программой ViPNet Registration Point.

Обновление справочников и ключей

Для поддержания работоспособности узла следует регулярно обновлять справочники и ключи. Обновления справочников и ключей могут быть отправлены администратором сети ViPNet из программы ViPNet Центр управления сетью (см. «Прием справочников и ключей из программы ViPNet Центр управления сетью» на стр. 39). Если по каким-либо причинам обновление справочников и ключей не может быть отправлено через сеть ViPNet, вы можете выполнить его вручную с помощью дистрибутива ключей (см. «Обновление справочников и ключей с помощью дистрибутива ключей» на стр. 43).

Прием справочников и ключей из программы ViPNet Центр управления сетью

Обновления справочников и ключей создаются администратором сети ViPNet в программе ViPNet Administrator и могут быть автоматически отправлены на сетевые узлы, которых коснулись изменения.

На сетевом узле полученные обновления справочников и ключей можно принять с помощью системы обновления ViPNet. Установка обновлений может осуществляться как в автоматическом режиме, так и вручную.

Если на узле настроена установка обновлений вручную, то при поступлении файлов обновления в области уведомлений отображается значок **ViPNet Система обновления** и соответствующая информация.

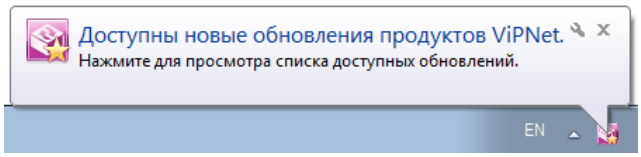


Рисунок 12. Отображение наличия обновлений в области уведомлений

Значок **ViPNet Система обновления** в области уведомлений может принимать следующий вид:

- — доступны новые обновления;
- — обновления успешно установлены;
- — обновления успешно установлены, необходима перезагрузка.

После установки обновлений, если не требуется перезагрузка, значок системы перестает отображаться в области уведомлений.

Если же на узле настроена автоматическая установка обновлений, то все операции ViPNet Система обновления будет производить в «тихом» режиме без каких-либо сообщений. В области уведомлений значок системы будет отображаться, только если требуется перезагрузка компьютера (значок будет иметь вид ⚠).

Автоматическая установка обновлений

Если вы хотите, чтобы обновления устанавливались на узле автоматически, выполните следующие действия:

1. Войдите в операционную систему с правами администратора.

   Без прав администратора вы не сможете изменить настройки программы ViPNet Система обновления.

2. Выполните одно из действий:

   - Если вы используете операционную систему Windows 7, Windows Server 2008 R2 или более ранней версии, в меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Система обновления**.
   - Если вы используете операционную систему Windows 8, Windows Server 2012 или более поздней версии, на начальном экране откройте список приложений и выберите **ViPNet** > **ViPNet Система обновления**.

3. В открывшемся окне на вкладке **Параметры** установите флажок **Устанавливать обновления автоматически**.

4. Если вы хотите, чтобы, когда это необходимо, после обновления перезагрузка выполнялась автоматически, установите соответствующий флажок.

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

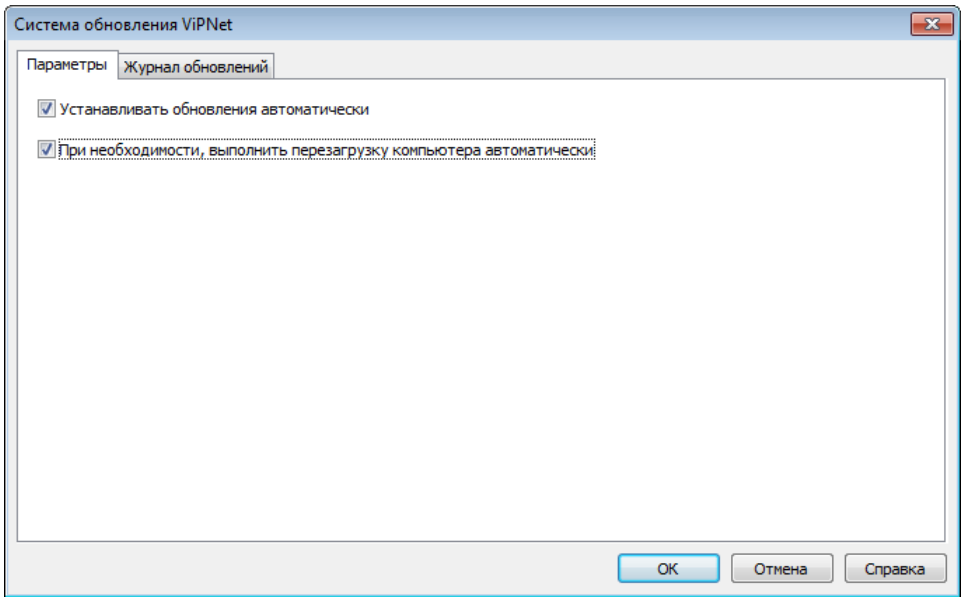


Рисунок 13. Настройка автоматической установки обновлений

Установка обновлений вручную

Если вы хотите самостоятельно контролировать установку обновлений на сетевом узле, отключите автоматическую установку обновлений. Для этого выполните следующие действия (см. Рисунок 16 на стр. 40):

1. Войдите в операционную систему с правами администратора.

   Без прав администратора вы не сможете изменить настройки программы ViPNet Система обновления.

2. Выполните одно из действий:

   - Если вы используете операционную систему Windows 7, Windows Server 2008 R2 или более ранней версии, в меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Система обновления**.
   - Если вы используете операционную систему Windows 8, Windows Server 2012 или более поздней версии, на начальном экране откройте список приложений и выберите **ViPNet** > **ViPNet Система обновления**.

3. В открывшемся окне на вкладке **Параметры** снимите флажок **Устанавливать обновления автоматически**.

4. Если вы хотите, чтобы, когда это необходимо, после обновления перезагрузка выполнялась автоматически, установите соответствующий флажок.

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

Если автоматическая установка обновлений отключена, то после получения обновлений выполните их установку вручную:

1. В области уведомлений щелкните значок **Система обновления ViPNet** правой кнопкой мыши и в контекстном меню выберите пункт **Доступные обновления**.

2. В открывшемся окне проверьте список устанавливаемых обновлений (они отмечены флажком). Если какое-либо обновление устанавливать не нужно, снимите соответствующий флажок.

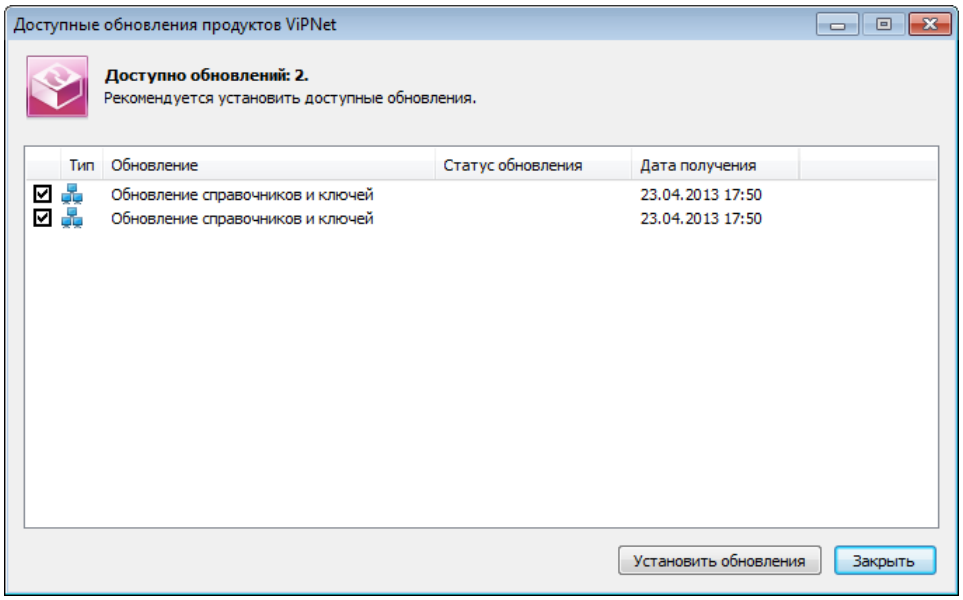


Рисунок 14. Список доступных обновлений

3 Нажмите кнопку **Установить обновления**.

Программа ViPNet Registration Point будет выгружена из памяти компьютера, и начнется процесс обновления. При этом в области уведомлений будет отображаться соответствующая информация.

Просмотр журнала установленных обновлений

Информация об установленных обновлениях отображается в журнале обновлений. Для просмотра журнала обновлений выполните следующее:

1 Выполните одно из действий:

- Если вы используете операционную систему Windows 7, Windows Server 2008 R2 или более ранней версии, в меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Система обновления.**
- Если вы используете операционную систему Windows 8 или Windows Server 2012, на начальном экране откройте список приложений и выберите **ViPNet** > **ViPNet Система обновления**.

2 Выберите вкладку **Журнал обновлений**.

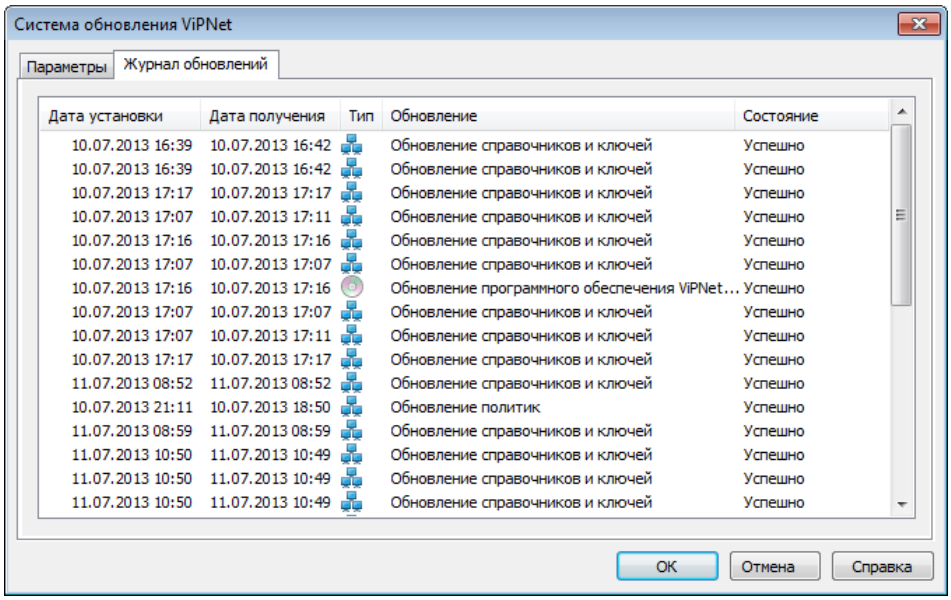


Рисунок 15. Журнал обновлений

Обновление справочников и ключей с помощью дистрибутива ключей

Если по каким-либо причинам обновление справочников и ключей не может быть принято по сети, вы можете выполнить обновление вручную с помощью дистрибутива ключей. Для этого:

1 Получите новый дистрибутив ключей у администратора сети ViPNet.

Следуйте указаниям раздела Установка справочников и ключей одного пользователя (на стр. 31) с использованием нового дистрибутива.

При указании дистрибутива ключей автоматически проверяется соответствие между установленными ранее ключами и новыми ключами, которые находятся в указанном файле дистрибутива ключей (например, предназначены ли данные ключи для одного и того же сетевого узла).

Внимание! При установке ключей в расширенном режиме (см. «Расширенный режим установки справочников и ключей» на стр. 33) данное сопоставление ключей производиться не будет.

2 Для установки справочников и ключей нажмите кнопку **Установить ключи**.

Примечание. Также при указании дистрибутива ключей автоматически проверяется соответствие между справочниками, содержащимися в нем, и справочниками, установленными на узле. Если на узле обнаружены более новые справочники, то вы можете выполнить установку только новых ключей и продолжать использовать актуальные справочники. Для этого убедитесь, что в окне программы установки ключей

ViPNet установлен флажок **Не устанавливать справочники**.

Если кнопка недоступна, это значит, что обнаружены несоответствия между новыми и установленными ранее ключами. Для получения информации о выявленных несоответствиях нажмите кнопку **Далее**. В зависимости от характера несоответствия появится сообщение одного из двух типов:

- Если выбранный дистрибутив содержит ключи другого сетевого узла, формат ключей в дистрибутиве отличается от формата текущих ключей, а также в ряде других случаев будет выведено предупреждение, содержащее описание выявленного несоответствия.

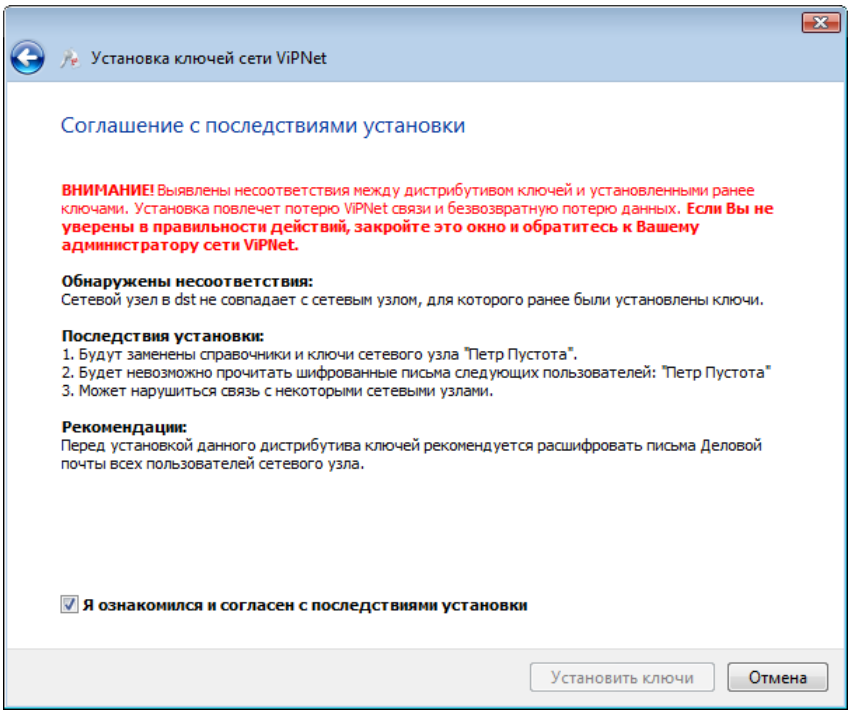


Рисунок 16. Обнаружено несоответствие между дистрибутивом и текущими ключами на узле

- Чтобы отказаться от установки ключей, нажмите кнопку **Отмена**, затем в окне подтверждения нажмите кнопку **Да**.

Внимание! Если вы хотите продолжить установку, ознакомьтесь с информацией о возможных последствиях и проконсультируйтесь у администратора вашей сети ViPNet.

- Для продолжения установите флажок **Я ознакомился и согласен с последствиями установки**, затем нажмите кнопку **Установить ключи**.

- Если выбранный дистрибутив не может быть установлен (например, он создан для другой программы ViPNet), будет выведено сообщение об ошибке, и дальнейшая установка будет невозможна. Ознакомьтесь с информацией о выявленном несоответствии и нажмите кнопку **Закрыть**.

В случае отказа от установки в результате несоответствий новых и установленных ранее ключей обратитесь за помощью к администратору сети ViPNet.

3 Завершите установку согласно указаниям раздела Установка справочников и ключей одного пользователя (на стр. 31).

После успешного обновления ключей можно запустить ПО ViPNet.

Действия при компрометации ключей

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

Различают явную и неявную компрометацию ключей:

- Явной называют компрометацию, факт которой становится известным в течение срока действия данного ключа.
- Неявной называют компрометацию ключа, факт которой остается неизвестным для лиц, являющихся законными пользователями данного ключа. Неявная компрометация представляет наибольшую опасность.

Основные события, при которых ключи можно считать скомпрометированными, перечислены ниже:

1. Посторонним лицам мог стать доступным файл дистрибутива ключей.
2. Посторонним лицам могло стать доступным внешнее устройство с ключами пользователя.
3. Посторонним лицам мог стать доступным пароль пользователя, и эти лица могли иметь доступ к компьютеру пользователя.
4. Посторонние лица могли получить неконтролируемый физический доступ к ключам пользователя, хранящимся на компьютере.
5. Был уволен сотрудник, имевший доступ к ключам.
6. Входящий документ подписан аннулированным сертификатом (см. «Аннулирование сертификата» на стр. 201), находящимся в списке аннулированных сертификатов (см. «Список аннулированных сертификатов (CRL)» на стр. 205).
7. Случаи, когда нельзя достоверно установить, что произошло с внешними устройствами (например, внешнее устройство вышло из строя, и существует возможность того, что это произошло в результате несанкционированных действий злоумышленника).

К событиям, требующим проведения расследования и принятия решения о факте компрометации, также относится возникновение подозрений в утечке информации или ее искажение в системе конфиденциальной связи.

При наступлении любого из перечисленных выше событий:

- Немедленно прекратите работу на сетевом узле и сообщите о факте компрометации (или предполагаемом факте компрометации) администратору сети ViPNet.
- Если скомпрометированы только ключи подписи, прекратите использование этих ключей для подписи документов и сообщите администратору сети ViPNet.

- Если есть подозрение, что посторонние лица могут знать пароль пользователя ViPNet, но эти посторонние лица не имеют доступа к компьютеру, смените пароль и продолжайте работу. Если доступ посторонних лиц к компьютеру пользователя возможен, то следует считать ключи скомпрометированными.

В сети ViPNet, управляемой с помощью ПО ViPNet Administrator, на случай компрометации ключей пользователя предусмотрена возможность дистанционного обновления ключей с помощью резервного набора персональных ключей (РНПК). Файл резервного набора (`AAAA.pk`, где AAAA — идентификатор пользователя в сети ViPNet) входит в состав первоначального дистрибутива ключей и при установке справочников и ключей помещается в папку ключей пользователя (см. «Установка справочников и ключей» на стр. 30).

Если текущий персональный ключ пользователя оказался скомпрометирован, администратор программы ViPNet Удостоверяющий и ключевой центр высылает пользователю новые ключи, защищенные с помощью очередного варианта персонального ключа, который не нужно передавать по сети, так как он уже содержится в резервном наборе. Если при обновлении файл резервного набора не найден, требуется указать путь к этому файлу. Если резервный набор персональных ключей отсутствует или не подходит пароль, откажитесь от ввода данных и обратитесь к администратору программы ViPNet Удостоверяющий и ключевой центр, чтобы получить его копию.

4

Начало работы с программой ViPNet Registration Point

Запуск и завершение работы с программой

Чтобы запустить программу ViPNet Registration Point:

1 Выполните одно из действий:

- В меню **Пуск** выберите **Все программы** > **ViPNet** > **Registration Point** > **ViPNet Registration Point**.

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

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

Откроется окно входа в программу.

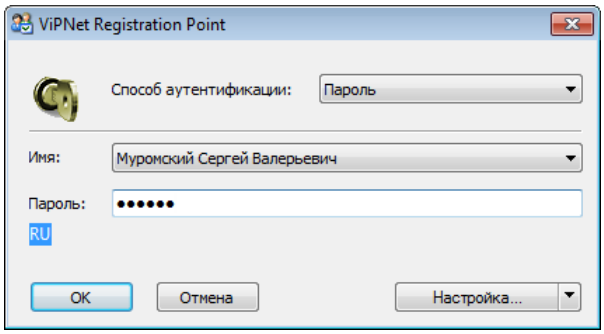


Рисунок 17. Окно входа в программу

2 Выберите способ аутентификации для входа в программу (см. «Способы аутентификации пользователя» на стр. 50) и в зависимости от выбранного способа введите пароль пользователя либо подключите внешнее устройство и введите ПИН-код.

Если на вашем компьютере работает несколько пользователей ViPNet Registration Point и для аутентификации вы используете пароль, в списке **Имя** выберите ваше имя пользователя.

3 После ввода необходимых для аутентификации данных нажмите кнопку **OK**. Откроется окно программы ViPNet Registration Point (см. «Интерфейс программы ViPNet Registration Point» на стр. 57).

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 **Сервис** выберите пункт **Выход**.

- Нажмите кнопку **Закрыть**  в правом верхнем углу окна.

Если в настройках программы установлена опция автоматического создания резервных копий, то перед выходом из программы будет создана резервная копия ее текущей конфигурации (см. «Работа с резервными копиями конфигураций программы» на стр. 146).

Смена пользователя

Если на сетевом узле зарегистрировано несколько пользователей, то при необходимости можно сменить пользователя. Для этого перезапустите ViPNet Registration Point и в окне входа в программу:

1 Выберите способ аутентификации для входа в программу (см. «Способы аутентификации пользователя» на стр. 50) и в зависимости от выбранного способа введите пароль пользователя либо подключите внешнее устройство и введите ПИН-код.

Если на вашем компьютере работает несколько пользователей ViPNet Registration Point и для аутентификации вы используете пароль, в списке **Имя** выберите ваше имя пользователя.

Примечание. На сетевом узле должны быть предварительно установлены ключи пользователя (см. «Установка справочников и ключей» на стр. 30), от имени которого выполняется вход в программу.

2 Нажмите кнопку **OK**.

Способы аутентификации пользователя

В программе ViPNet Registration Point предусмотрено три способа аутентификации:

- Пароль (на стр. 52). Для входа в программу вам следует ввести свой пароль. Каждый раз после ввода пароля вычисляется парольный ключ, который используется для доступа к вашему персональному ключу.
- Пароль на устройстве (на стр. 53). Для входа в программу вам следует подключить устройство и ввести ПИН-код.

Внимание! Способ аутентификации **Пароль на устройстве** не отвечает требованиям безопасности, и возможность его использования оставлена исключительно для совместимости с программным обеспечением ViPNet более ранних версий. В связи с этим, если программа ViPNet Registration Point была обновлена до версии 3.2.x и выше и в ней используется данный способ аутентификации, то настоятельно рекомендуется его изменить на **Пароль** или **Устройство**.

- Устройство (на стр. 54). Для входа в программу вам следует подключить устройство и ввести ПИН-код (и в некоторых случаях пароль).

По умолчанию установлен способ аутентификации **Пароль**. В режиме администратора можно изменить способ аутентификации.

При использовании способов **Пароль на устройстве** и **Устройство** аутентификация пользователя осуществляется с помощью внешних устройств. Список доступных устройств хранения данных и полезная информация об использовании устройств приведена в документе «ViPNet CSP. Руководство пользователя». Чтобы использовать какое-либо устройство для аутентификации пользователя, на компьютер необходимо установить драйверы этого устройства и затем записать ключи на это устройство. Записать ключи на внешнее устройство можно при изменении способа аутентификации пользователя или в программе ViPNet Удостоверяющий и ключевой центр при создании дистрибутива ключей.

На схеме ниже представлены факторы аутентификации, используемые при выборе каждого способа аутентификации в зависимости от типа внешнего устройства.

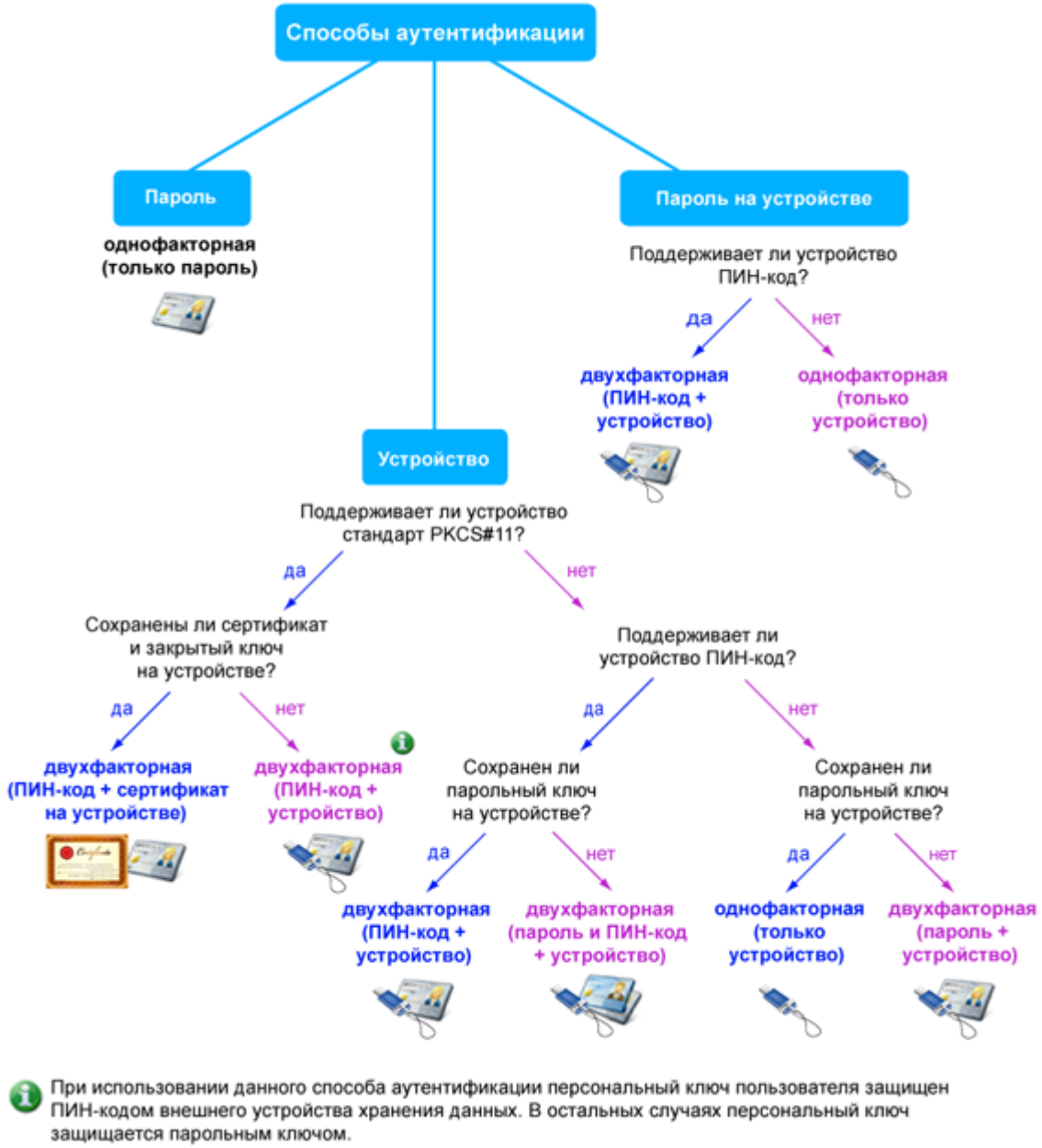


Рисунок 18. Схема соответствия между факторами и способами аутентификации

Пароль

Для входа в программу ViPNet Registration Point с помощью пароля в окне аутентификации выполните следующие действия:

1 В списке **Способ аутентификации** выберите **Пароль**.

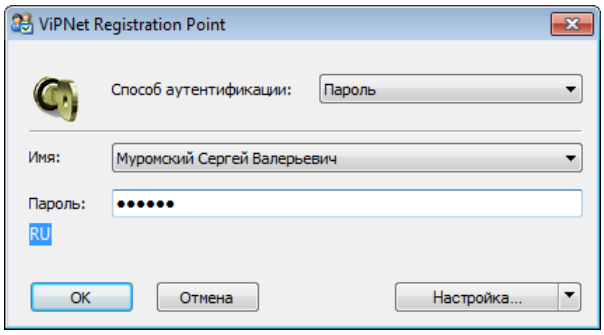


Рисунок 19. Способ аутентификации «Пароль»

2 При необходимости в списке **Имя** выберите ваше имя пользователя ViPNet.

Примечание. В данном списке отображаются имена всех пользователей, ключи которых были установлены на данном сетевом узле (см. «Установка справочников и ключей» на стр. 30). Если на узле не установлены ключи ни одного пользователя, список будет пуст.

3 В поле **Пароль** введите ваш пароль.

Если сохранение пароля в реестре разрешено настройками программы (см. «Дополнительные настройки параметров безопасности» на стр. 145), для сохранения пароля можно установить соответствующий флажок.

4 Нажмите кнопку **OK**.

Пароль на устройстве

Внимание! Во избежание неполадок в работе ПО ViPNet не следует использовать способ аутентификации **Пароль на устройстве**. При использовании данного способа аутентификации рекомендуется его изменить на **Пароль** или **Устройство**.

Для входа в программу ViPNet Registration Point с помощью пароля на устройстве в окне аутентификации выполните следующие действия:

1 В списке **Способ аутентификации** выберите **Пароль на устройстве**.

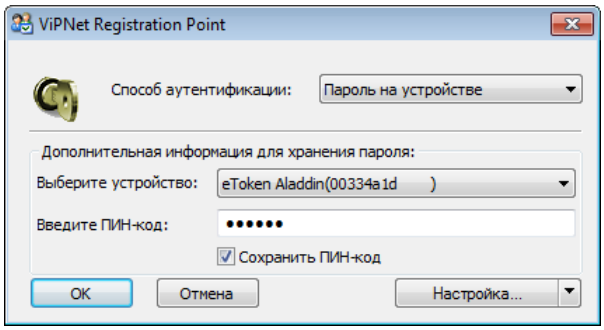


Рисунок 20. Способ аутентификации «Пароль на устройстве»

2 Подключите внешнее устройство, на котором находится ваш пароль.

3 В списке **Выберите устройство** выберите внешнее устройство.

4 Введите ПИН-код, если требуется. Необходимость ввода ПИН-кода зависит от типа используемого внешнего устройства (см. Рисунок 21 на стр. 52).

Чтобы сохранить ПИН-код и в дальнейшем не вводить его при аутентификации, установите соответствующий флажок.

5 Нажмите кнопку **OK**.

Как правило, использование способа аутентификации **Пароль на устройстве** предполагает, что ваш пароль хранится на устройстве и вам не известен. Однако если вы знаете пароль, то помимо аутентификации с помощью внешнего устройства для входа в программу можно использовать аутентификацию по паролю. Данная возможность обеспечивает вход в программу в случае неисправности внешнего устройства (для этого вам понадобится узнать свой пароль у администратора сети ViPNet).

Устройство

Для входа в программу ViPNet Registration Point с помощью устройства в окне аутентификации выполните следующие действия:

1 В списке **Способ аутентификации** выберите **Устройство**.

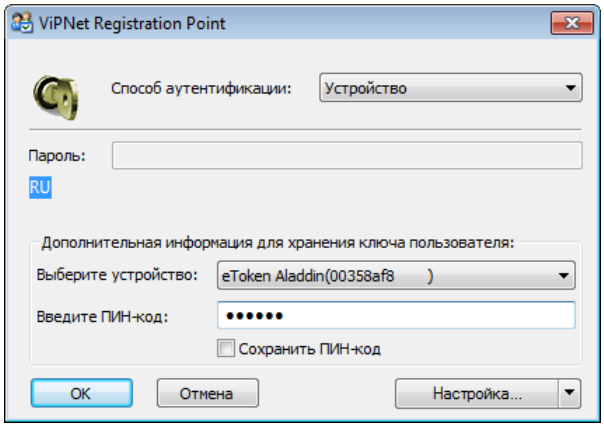


Рисунок 21. Способ аутентификации «Устройство»

2 Подключите внешнее устройство.

3 Если требуется, в списке ниже выберите ваше имя пользователя и в поле **Пароль** введите свой пароль. Необходимость ввода пароля зависит от типа используемого внешнего устройства (см. Рисунок 21 на стр. 52).

4 В списке **Устройство** выберите внешнее устройство, на котором находится ваш персональный ключ или сертификат.

5 Введите ПИН-код, если требуется. Необходимость ввода ПИН-кода зависит от типа используемого внешнего устройства. Чтобы сохранить ПИН-код и в дальнейшем не вводить его при аутентификации, установите соответствующий флажок.

6 В списке **Производить аутентификацию при помощи** установите переключатель в одно из следующих положений:

- **Сертификата** — чтобы выполнить аутентификацию с помощью сертификата, хранящегося на используемом устройстве. В списке сертификатов, обнаруженных на устройстве, выберите нужный сертификат. Подробнее о требованиях, предъявляемых к сертификату, используемому для аутентификации см. в разделе Особенности аутентификации с помощью сертификата (на стр. 55). В случае возникновения затруднений при аутентификации с помощью сертификата см. раздел Не удается выполнить аутентификацию с помощью сертификата (на стр. 181).
- **Персонального ключа** — чтобы выполнить аутентификацию с помощью персонального ключа (который входит в состав ключей пользователя и хранится на используемом устройстве).

7 Нажмите кнопку **OK**.

Особенности аутентификации с помощью сертификата

Для возможности аутентификации в программе ViPNet Монитор с помощью сертификата должны быть выполнены следующие условия:

- Внешнее устройство поддерживает стандарт PKCS#11.
- Аутентификация с помощью сертификата ГОСТ выполняется с помощью устройства, на котором реализована аппаратная поддержка алгоритмов ГОСТ.

Примечание. Информация о том, какие внешние устройства обеспечивают аппаратную поддержку алгоритмов ГОСТ и поддержку стандарта PKCS#11, содержится в документе «ViPNet CSP. Руководство пользователя».

- Сертификат имеет назначение «Проверка подлинности клиента». Это назначение отображается в окне **Сертификат**, на вкладке **Состав**, в поле **Расширенное использование ключа**.
- В контейнере на устройстве находится закрытый ключ, которому соответствует используемый сертификат.
- Сертификат действителен (срок действия сертификата не истек).
- Сертификат не аннулирован.

Чтобы получить сертификат ГОСТ, подходящий для аутентификации в ПО ViPNet Монитор, выполните следующие действия:

1 Создайте запрос на сертификат. При этом сохраните контейнер ключей на внешнее устройство (см. «Обновление ключа электронной подписи и сертификата» на стр. 145).

2 Предупредите администратора программы ViPNet Удостоверяющий и ключевой центр о том, что при издании сертификата в него необходимо добавить назначение «Проверка подлинности клиента». Если в УКЦ обработка запросов на сертификаты производится в

автоматическом режиме, администратору нужно будет отключить этот режим и обработать ваш запрос вручную.

3 Установите изданный сертификат в контейнер ключей, сохраненный на устройстве (см. «Установка сертификатов в хранилище операционной системы» на стр. 145).

Интерфейс программы ViPNet Registration Point

Внешний вид окна программы ViPNet Registration Point представлен на рисунке ниже. При работе в программе без ключа электронной подписи и сертификата ключа проверки электронной подписи в интерфейсе программы будут отсутствовать элементы, связанные с созданием и управлением запросов на сертификаты, просмотром полученных по запросам сертификатов, списков аннулированных сертификатов (CRL) (см. «Работа в ViPNet Registration Point без ключа электронной подписи и сертификата» на стр. 18).

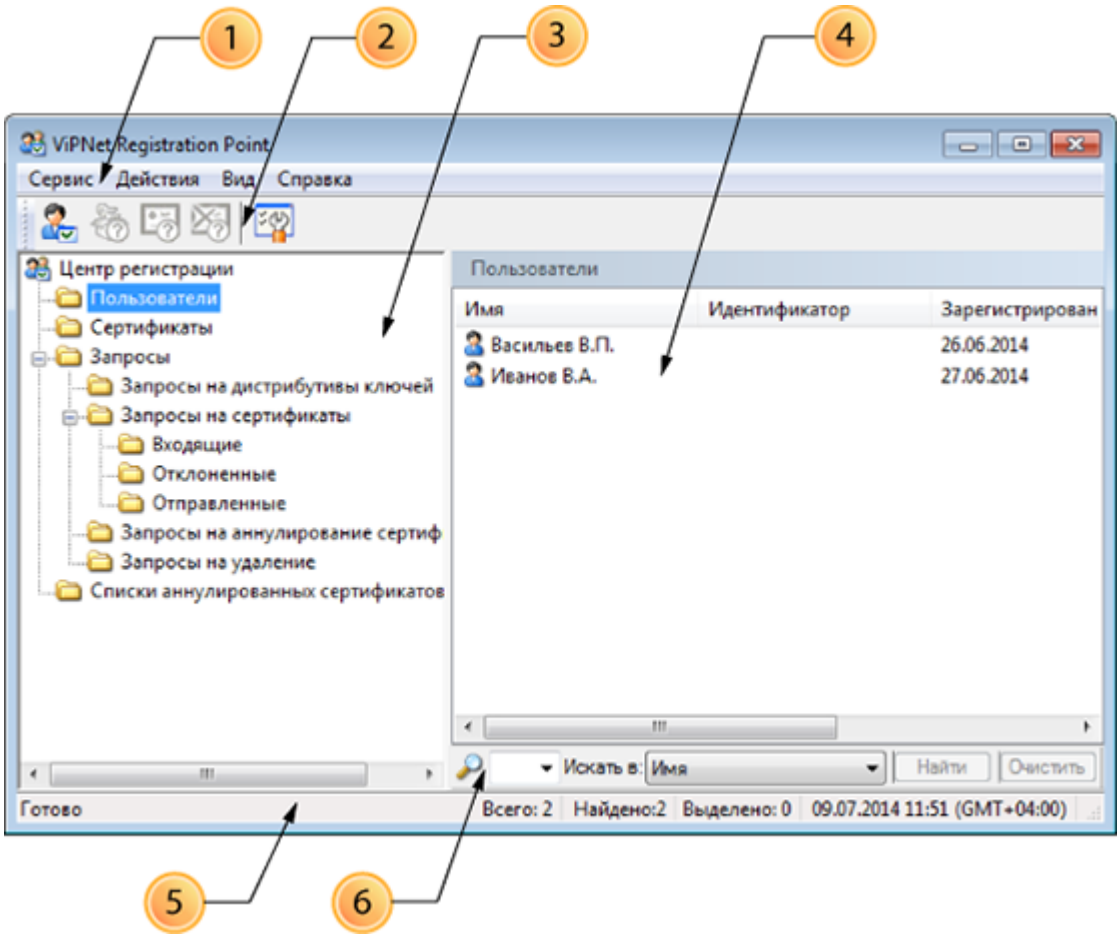


Рисунок 22. Окно программы ViPNet Registration Point

Цифрами на рисунке обозначены:

1. Главное меню программы.
2. Панель инструментов. Чтобы удалить или добавить кнопки на панель инструментов, в меню **Вид** выберите пункт **Панель инструментов**.
3. Панель навигации. Содержит перечень следующих разделов:
   - **Пользователи** — содержит список пользователей, зарегистрированных в программе.

- **Сертификаты** — содержит список сертификатов, полученных пользователями в соответствии с удовлетворенными запросами.
- **Запросы** — включает в себя вложенные подразделы, в которых содержится информация о запросах на дистрибутивы ключей, издание сертификатов и их обслуживание.
- **Списки аннулированных сертификатов** — содержит списки аннулированных сертификатов, полученных из программы ViPNet Удостоверяющий и ключевой центр.

4 Панель просмотра. Предназначена для отображения раздела, выбранного на панели навигации (3).

5 Строка состояния. Чтобы отобразить или скрыть строку состояния, в меню **Вид** выберите пункт **Строка состояния**.

6 Строка поиска. Отображается в разделах, в которых на панели просмотра содержатся списки (пользователей, сертификатов, запросов и других объектов). В каждом из таких разделов вы можете осуществлять поиск по разным параметрам.

5

Быстрый старт

Перед началом работы

Данная глава содержит краткие указания по использованию основных возможностей программы ViPNet Registration Point (см. «Основные возможности программы ViPNet Registration Point» на стр. 16). Эта информация поможет приступить к работе без подробного изучения данного руководства.

Прежде чем начать работу, запустите программу (см. «Запуск и завершение работы с программой» на стр. 49). Об основных действиях, которые можно выполнить в ViPNet Registration Point, можно узнать далее в данной главе.

Подробная информация о регистрации и удалении пользователей, а также экспорте и изменении их регистрационных данных приводится в главе Работа с пользователями (на стр. 65). Создание запросов на издание, отзыв, приостановление и возобновление действия сертификатов пользователей описано в главе Действия с сертификатами пользователей (на стр. 92). Формирование запросов на дистрибутивы и обновления дистрибутивов ключей описано в главе Работа с дистрибутивами ключей (на стр. 129). В случае каких-либо затруднений обратитесь к этим главам.

Как вручную зарегистрировать пользователя

Чтобы вручную зарегистрировать пользователя, выполните следующие действия:

1. В окне программы ViPNet Registration Point на панели инструментов нажмите кнопку **Зарегистрировать пользователя**  .
2. На странице **Регистрация пользователя** установите переключатель в положение **Зарегистрировать пользователя самостоятельно** и в списке выберите шаблон пользователя (на стр. 206).
3. На последующих страницах мастера регистрации введите все необходимые сведения о пользователе.
4. На странице **Завершение регистрации** нажмите кнопку **Готово**.

   В результате новый пользователь появится в списке в разделе **Пользователи**.

Пользователей ViPNet также можно регистрировать через внешние источники данных. Подробнее см. раздел Регистрация пользователей (на стр. 66).

Как создать запрос на новый сертификат

Чтобы создать запрос на новый сертификат для зарегистрированного пользователя (см. «Сертификат ключа проверки электронной подписи» на стр. 204), выполните следующие действия:

1. В окне программы ViPNet Registration Point в разделе **Пользователи** выберите нужного пользователя и на панели инструментов нажмите кнопку **Создать запрос на сертификат**  , будет запущен мастер создания запроса на сертификат.
2. На первой странице мастера в списке выберите шаблон сертификата (на стр. 206), который будет использоваться при создании запроса.
3. На каждой последующей странице мастера укажите требуемые параметры сертификата.
4. При необходимости создайте пароль к контейнеру ключей (пароль пользователя).

   Если в качестве типа пароля вы выберите тип **Собственный пароль**, на странице **Пароль защиты ключа электронной подписи** задайте пароль и его подтверждение.

   Если вы выберите тип одного из случайных паролей, запомните новый пароль (или парольную фразу), отображенный на странице **Пароль защиты ключа электронной подписи**.

   Внимание! Длина пароля должна быть не меньше 8 символов и не должна превышать 31 символ. Пароли с длиной более 31 символа не могут использоваться в текущих версиях приложений ViPNet. Данное ограничение связано с существующим алгоритмом передачи пароля в криптопровайдер.

   ---

5. На странице готовности к созданию запроса на сертификат убедитесь в правильности параметров, заданных на предыдущих страницах мастера.
6. На странице **Завершение создания запроса на сертификат** нажмите кнопку **Готово**.

   Созданный запрос появится в разделе **Запросы на сертификаты** > **Отправленные запросы на сертификаты** и будет отправлен в программу ViPNet Удостоверяющий и ключевой центр.

Подробнее см. раздел Создание запроса на новый сертификат (на стр. 93).

После издания и получения сертификата пользователя можно приостанавливать и возобновлять его действие, отзывать, экспортировать сертификат в файл и сохранять в контейнере ключей. Подробнее см. соответствующие разделы в главе Действия с сертификатами пользователей (на стр. 92).

Как обработать запрос на сертификат от внешнего пользователя

Чтобы обработать запрос на издание сертификата от внешнего пользователя:

1. Поместите полученный от пользователя запрос в папку `Import`, которая находится в папке обработки входящих запросов (см. «Настройка параметров обработки запросов от внешних пользователей» на стр. 105). По умолчанию это папка `C:\Program Files\InfoTeCS\ViPNet Registration Point\PKCS10`.
2. Если в настройках установлена соответствующая опция, то поступивший запрос будет обработан и отправлен в программу ViPNet Удостоверяющий и ключевой центр автоматически, после чего помещен в раздел **Запросы на сертификаты** > **Отправленные**.
3. Если опция не установлена, запрос появится в разделе **Запросы на сертификаты** > **Входящие**. В этом случае чтобы обработать запрос, щелкните его правой кнопкой мыши и в контекстном меню выберите пункт:
   - **Принять**, чтобы принять и отправить запрос на сертификат в УКЦ.
   - **Отклонить**, чтобы его отклонить.

Подробнее см. раздел Обработка запросов на сертификаты от внешних пользователей (на стр. 102).

Как создать запрос на дистрибутив ключей

Чтобы создать запрос на дистрибутив ключей (на стр. 201), выполните следующие действия:

1. В окне программы ViPNet Registration Point в разделе **Пользователи** выберите нужного пользователя и на панели инструментов нажмите кнопку **Создать запрос на дистрибутив ключей**  .

   Если для выбранного пользователя запрос на дистрибутив ключей ранее не создавался, то будет запущен мастер создания запроса на дистрибутив ключей. Следуйте указаниям мастера (см. ниже).

   Если для данного пользователя ранее был создан дистрибутив ключей, будет запущен мастер, позволяющий создать запрос на обновление дистрибутива ключей (см. «Создание запроса на обновление дистрибутива ключей» на стр. 131).

   Если для пользователя уже был создан запрос на дистрибутив или обновление дистрибутива ключей, но он еще не был удовлетворен, появится сообщение с предложением повторно отправить созданный запрос или создать новый. Выполните необходимое действие.

2. На странице **Параметры сетевого узла пользователя** укажите сетевой узел, на котором следует зарегистрировать пользователя.

   При регистрации пользователя на новом узле выберите координатор, который будет являться для данного узла сервером-маршрутизатором (см. «Сервер-маршрутизатор» на стр. 204).

3. На странице **Связи с сетевыми узлами** задайте связи узла пользователя со всеми узлами сети или с определенными узлами согласно списку.

4. На странице **Добавить роли на сетевой узел** укажите способ назначения ролей сетевому узлу пользователя.

5. При необходимости задайте пароль к дистрибутиву ключей (пароль пользователя), если он не задавался для пользователя ранее. Это возможно только в том случае, если в настройках программы в разделе **Запросы на дистрибутивы ключей** установлен флажок **Создавать пароль пользователя в мастере создания запросов на дистрибутив ключей** (см. «Настройка параметров создания запросов на дистрибутивы» на стр. 139).

6. На странице **Завершение создания запроса на дистрибутив ключей** нажмите кнопку **Готово**.

   Созданный запрос появится в разделе **Запросы на дистрибутивы** и будет отправлен в программу ViPNet Центр управления сетью.

Подробнее см. раздел Создание запроса на дистрибутив ключей (на стр. 130).

6

Работа с пользователями

Регистрация пользователей

В программе ViPNet Registration Point зарегистрировать пользователя вы можете несколькими способами:

- Вручную путем самостоятельного заполнения сведений о пользователе (см. Регистрация вручную (на стр. 66)). Такой способ обычно используется для регистрации единичных пользователей.
- При использовании внешнего источника данных Active Directory (см. Регистрация через Active Directory (на стр. 69)). Этот способ удобен в том случае, если пользователи сети зарегистрированы в единой централизованной базе данных под управлением Active Directory (AD) (на стр. 199).
- С помощью текстового файла (см. Регистрация с помощью текстового файла (на стр. 72)). Такой способ используется для регистрации пользователей, информация о которых была экспортирована в текстовый файл из другого центра регистрации либо из стороннего приложения.

Примечание. Способы регистрации пользователей через Active Directory и текстовый файл считаются дополнительными. Они предоставляют возможность групповой регистрации пользователей на основе уже имеющейся информации, за счет чего позволяют значительно упростить процесс регистрации и тем самым сэкономить время.

Регистрация вручную

Чтобы вручную зарегистрировать пользователя, выполните следующие действия:

1 В окне программы ViPNet Registration Point на панели инструментов нажмите кнопку **Зарегистрировать пользователя**  . Будет запущен мастер регистрации пользователя.

2 На странице **Регистрация пользователя**:

2.1 Щелкните **Зарегистрировать пользователя самостоятельно**.

2.2 В списке выберите шаблон пользователя (на стр. 206), по которому будет осуществляться регистрация, иначе будет использоваться шаблон, указанный по умолчанию.

При необходимости создайте другой шаблон регистрации пользователя (см. «Создание и редактирование шаблонов пользователей» на стр. 82). По умолчанию в состав программы ViPNet Registration Point входит встроенный шаблон пользователя (**Стандартный шаблон имени пользователя**), состоящий из стандартного набора атрибутов. Данный шаблон нельзя изменить или удалить.

2.3 Чтобы выбранный шаблон использовался при следующей регистрации пользователя, установите флажок **Использовать по умолчанию**.

2.4 Нажмите кнопку **Далее**.

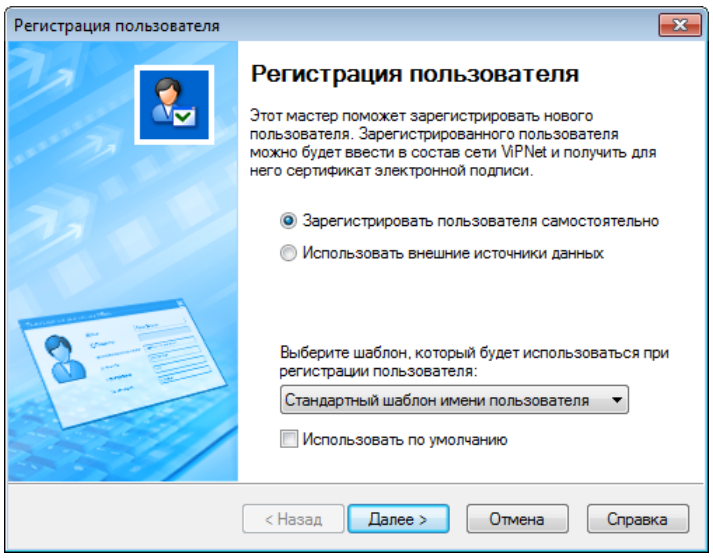


Рисунок 23. Мастер регистрации пользователя

3 На странице **Сведения о пользователе** укажите имя и другие необходимые данные о пользователе и нажмите кнопку **Далее**.

Если в программе уже зарегистрирован пользователь с данным именем, появится соответствующее сообщение.

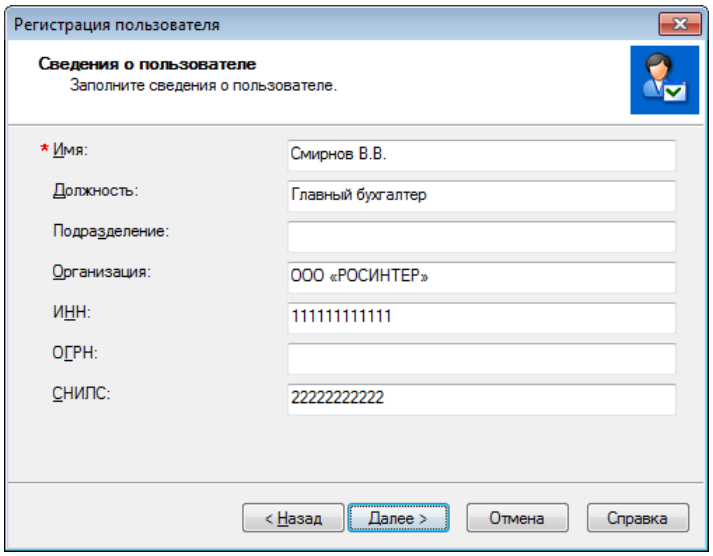


Рисунок 24. Заполнение основных сведений о пользователе

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

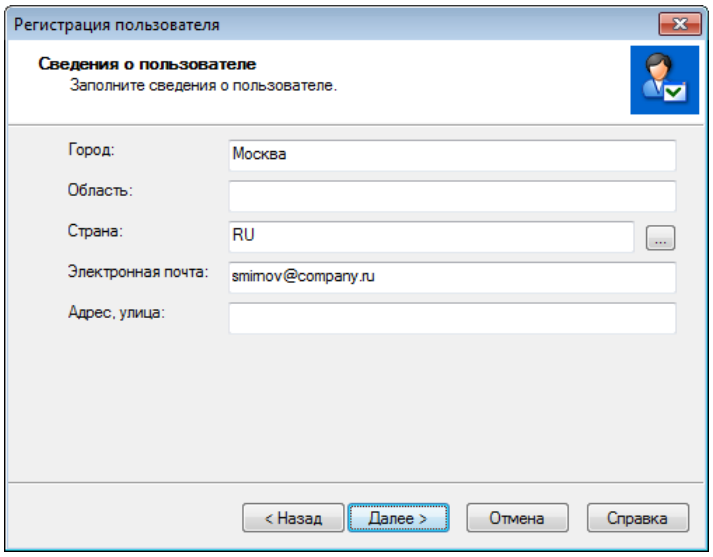


Рисунок 25. Заполнение сведений об адресе пользователя

Примечание. Поля, отмеченные красной звездочкой, являются обязательными для заполнения. В зависимости от выбранного шаблона поля, доступные для заполнения, могут быть различными.

Имя пользователя не должно включать следующие символы: * ? : & \ | / < > «».

5 На странице **Система готова к регистрации пользователя** убедитесь в правильности данных, заданных на предыдущих страницах мастера, и нажмите кнопку **Далее**. При необходимости вернитесь на нужную страницу с помощью кнопки **Назад**.

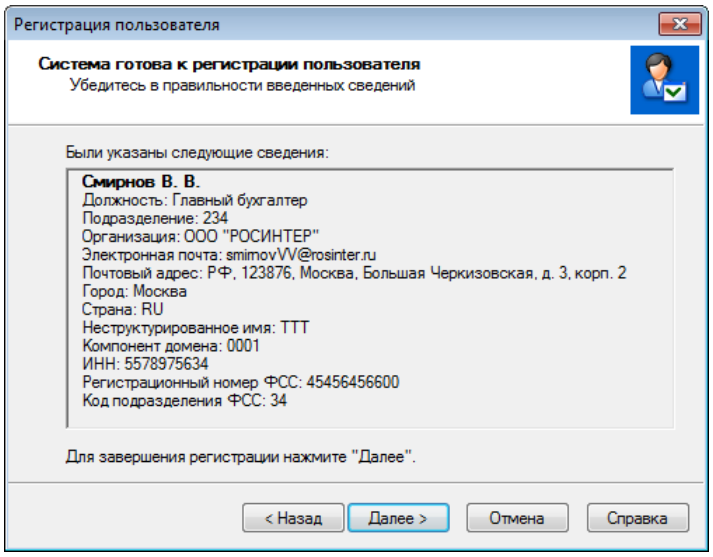


Рисунок 26. Проверка правильности введенных данных

В результате начнется обработка введенных сведений о пользователе.

При успешной регистрации на странице **Завершение регистрации** появится соответствующее сообщение и напротив имени пользователя будет значок ✔.

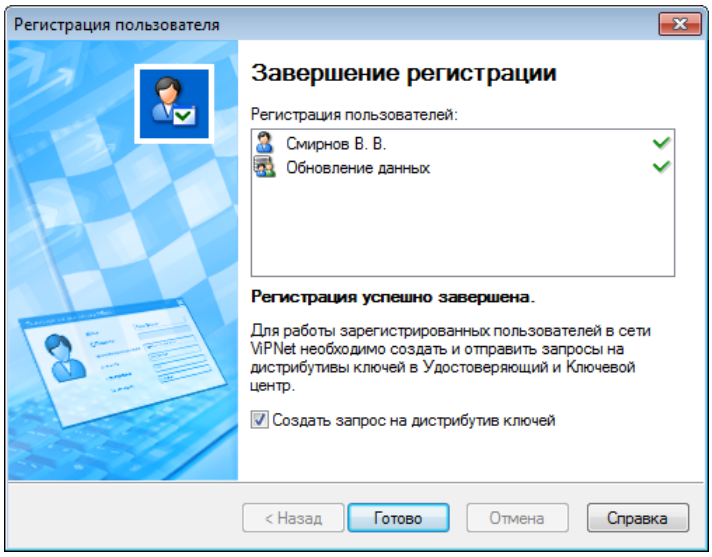


Рисунок 27. Окончание регистрации пользователя

Если в ходе регистрации в программе будет найден пользователь с таким же именем (или псевдонимом), но с другими регистрационными данными, появится сообщение с предложением зарегистрировать пользователя как нового или изменить данные существующего пользователя (подробнее см. раздел Действия при совпадении имен пользователей (на стр. 75)).

В случае полного совпадения данных регистрируемого пользователя с другим пользователем регистрация не произойдет. На странице **Завершение регистрации** появится сообщение о том, что не удалось зарегистрировать пользователя, и напротив его имени будет значок .

6 Для формирования запроса на дистрибутив ключей сразу по завершении регистрации пользователя установите флажок **Создать запрос на дистрибутив ключей** (см. Создание запроса на дистрибутив ключей (на стр. 130)).

7 Нажмите кнопку **Готово**.

При успешной регистрации учетная запись нового пользователя появится в списке в разделе **Пользователи**.

Регистрация через Active Directory

Для регистрации пользователей через Active Directory выполните следующие действия:

1 В окне программы ViPNet Registration Point на панели инструментов нажмите кнопку **Зарегистрировать пользователя** . Будет запущен мастер регистрации пользователя.

2 На странице **Регистрация пользователя** выберите режим **Использовать внешние источники данных** (см. Рисунок 26 на стр. 67).

3 На странице **Выбор внешнего источника** в списке выберите **AD Connector** и нажмите кнопку **Далее**.

При необходимости нажмите кнопку **Настройка** и выполните настройку подключения к домену Active Directory (см. «Настройка подключения к Active Directory» на стр. 85).

Примечание. Настройку подключения к Active Directory также можно выполнить перед началом регистрации.

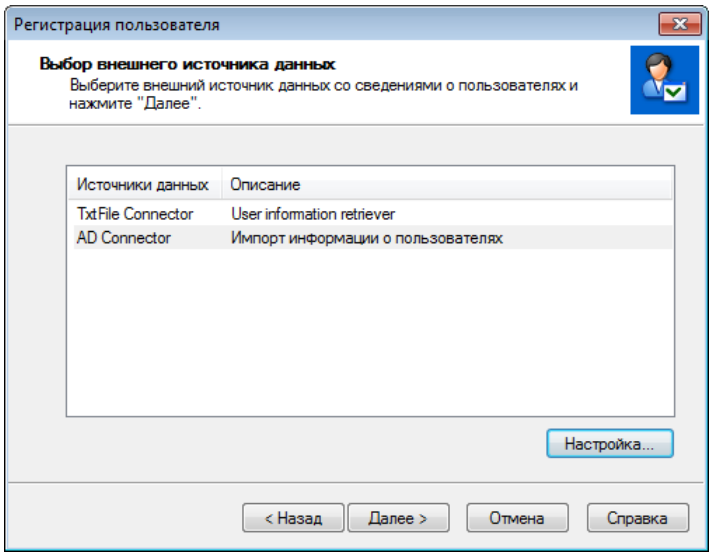


Рисунок 28. Выбор внешнего источника данных

4 На странице **Выбор пользователей** нажмите кнопку **Найти пользователей**.

Будет выполнено подключение к Active Directory. При неудачной попытке подключения появится соответствующее сообщение, в этом случае проверьте правильность настройки параметров подключения к домену (см. п. 3).

5 В случае успешного подключения к источнику данных в окне **Поиск в Active Directory** выполните поиск пользователей или компьютеров домена:

- В группе **Параметры поиска** с помощью переключателя **Искать** укажите, требуется ли вам найти пользователей или компьютеры.
- При необходимости уточнить поиск укажите параметры пользователей или компьютеров, которые вы хотите найти.
- Нажмите кнопку **Начать поиск**. В группе **Результаты поиска** будут отображены найденные по запросу объекты.

Если вы выполняете поиск по пользователям, вы можете просмотреть сертификаты ключа проверки электронной подписи найденных пользователей. Для этого выберите пользователя в списке и нажмите кнопку **Сертификат**.

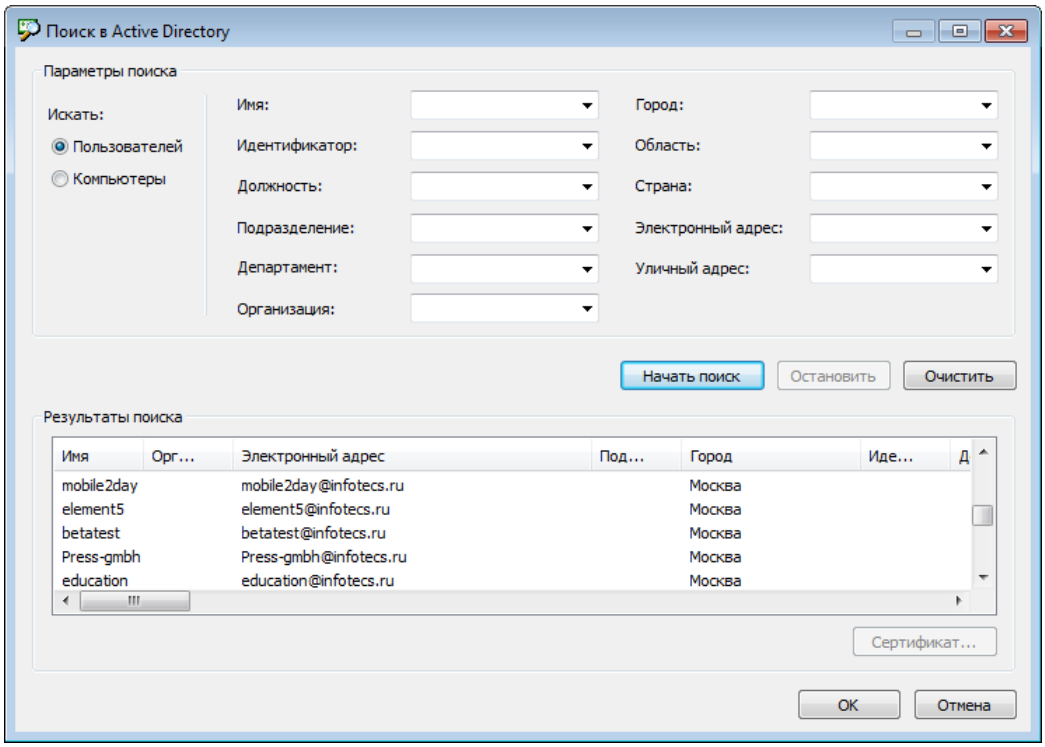


Рисунок 29. Поиск пользователей из домена Active Directory

6 В окне **Поиск в Active Directory** в списке **Результаты поиска** выберите тех пользователей, которых следует зарегистрировать, и нажмите кнопку **OK**.

7 На странице **Выбор пользователей** проверьте список пользователей и нажмите кнопку **Далее**. Если список неполный, повторите поиск (см. п. 4).

Примечание. При повторном поиске список пользователей, выбранных при предыдущем поиске, не сохранится.

При необходимости удалите лишних пользователей.

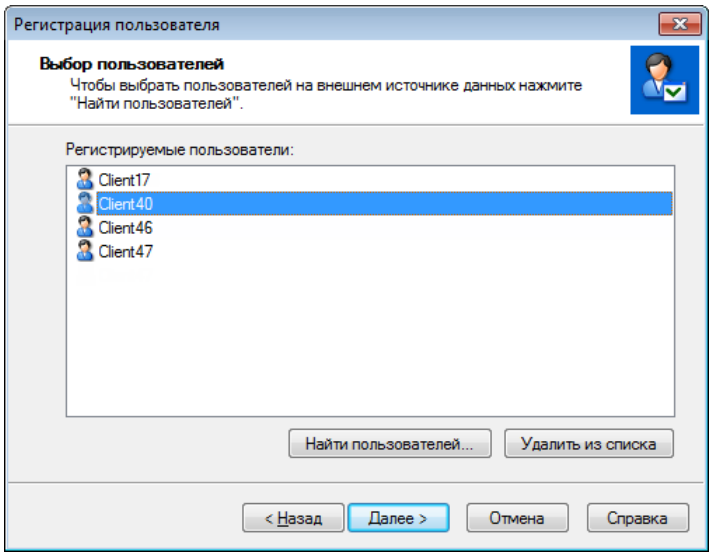


Рисунок 30. Результат выбора пользователей домена Active Directory

8 На странице **Система готова к регистрации пользователя** убедитесь в правильности данных, указанных на предыдущих страницах мастера, и нажмите кнопку **Далее**. При необходимости вернитесь на нужную страницу с помощью кнопки **Назад**.

Начнется проверка на совпадение имен выбранных пользователей с именами уже зарегистрированных.

При успешной регистрации на странице **Завершение регистрации** появится соответствующее сообщение и напротив имени каждого пользователя будет значок .

Если в ходе регистрации в программе будет найден пользователь с таким же именем (или псевдонимом), но с другими регистрационными данными, появится сообщение с предложением зарегистрировать пользователя как нового или изменить данные существующего пользователя (подробнее см. раздел Действия при совпадении имен пользователей (на стр. 75)).

В случае полного совпадения данных регистрируемого пользователя с другим пользователем, регистрация не произойдет. На странице **Завершение регистрации** появится сообщение о том, что не удалось зарегистрировать пользователя, и напротив его имени будет значок .

9 По окончании регистрации нажмите кнопку **Готово**.

В результате учетные записи зарегистрированных пользователей отобразятся в списке в разделе **Пользователи**.

Регистрация с помощью текстового файла

Для регистрации пользователей с помощью текстового файла выполните следующие действия:

1 В окне программы ViPNet Registration Point на панели инструментов нажмите кнопку **Зарегистрировать пользователя** . Будет запущен мастер регистрации пользователя.

2 На странице **Регистрация пользователя** выберите режим **Использовать внешние источники данных** (см. Рисунок 26 на стр. 67).

3 На странице **Выбор внешнего источника** в списке выберите **TxtFile Connector** и нажмите кнопку **Далее** (см. Рисунок 31 на стр. 70).

При необходимости нажмите кнопку **Настройка** и укажите путь к файлу с данными пользователей.

Примечание. Задать путь к файлу `*.txt` можно предварительно при настройке внешних источников данных (см. «Настройка подключения к внешним источникам данных» на стр. 85).

Если для регистрации используется файл, сформированный каким-либо сторонним приложением, то он должен соответствовать требованиям, указанным в разделе Требования к текстовому файлу (на стр. 74).

---

4 На странице **Выбор пользователей** нажмите кнопку **Найти пользователей**.

При неудачной попытке подключения к источнику данных появится соответствующее сообщение. В данном случае проверьте правильность указанного пути к файлу `*.txt` (см. п. 3).

5 При обнаружении текстового файла на странице **Выбор пользователей** появится список пользователей для регистрации. При необходимости удалите из данного списка всех лишних пользователей с помощью кнопки **Удалить из списка**.

6 По завершении нажмите кнопку **Далее**.

7 На странице **Система готова к регистрации пользователя** убедитесь в правильности данных, заданных на предыдущих страницах мастера, и нажмите кнопку **Далее**. При необходимости вернитесь на нужную страницу с помощью кнопки **Назад**.

Начнется проверка на совпадение имен выбранных пользователей с именами уже зарегистрированных.

При успешной регистрации на странице **Завершение регистрации** появится соответствующее сообщение и напротив имени каждого пользователя будет значок ✔.

Если в ходе регистрации в программе будет найден пользователь с таким же именем (или псевдонимом), но с другими регистрационными данными, появится сообщение с предложением зарегистрировать пользователя как нового или изменить данные существующего пользователя (подробнее см. раздел Действия при совпадении имен пользователей (на стр. 75)).

В случае полного совпадения данных регистрируемого пользователя с другим пользователем, регистрация не произойдет. На странице **Завершение регистрации** появится сообщение о том, что не удалось зарегистрировать пользователя, и напротив его имени будет значок ✖.

8 Нажмите кнопку **Готово**.

В результате учетные записи всех зарегистрированных пользователей отобразятся в списке в разделе **Пользователи**.

Требования к текстовому файлу

Файл, который может использоваться для регистрации пользователей в программе ViPNet Registration Point, должен соответствовать следующим требованиям:

1. Формат файла — текстовый (`*.txt`).
2. Кодировка файла — UCS-2 Little Endian.
3. В структуре файла одна запись (строка) — уникальное имя пользователя в формате X.500. Например: `CN=Андрей, O=Ростелеком`.
4. Запись может состоять только из следующих атрибутов X.500: `O; C; L; OU; CN; SerialNumber; E, Email; S, ST; STREET; T, Title; Pseudonym; Department; UnstructuredName; INN; OGRN; OGRNIP; SNILS`.

Примечание. Максимальную длину значения и допустимые символы для атрибутов: `O; C; L; OU; CN; SerialNumber; E, Email; S, ST; STREET; T, Title; Department` можно узнать на сайте MSDN http://msdn.microsoft.com/ru-ru/.

Максимальная длина значения и допустимые символы для атрибутов `Pseudonym` и `UnstructuredName` эквивалентны атрибуту `CN`.

В соответствии с приказом ФСБ №795 от 27.12.2011 максимальная длина значения атрибута `INN=12; OGRN=13; OGRNIP=15; SNILS=11` символам.

5. Каждый из атрибутов может встречаться в записи только один раз.
6. Значение атрибута должно заключаться в кавычки, если оно содержит служебные символы: # ; , «» \ = \n \r.

   Например: `STREET="ул. Гоголя, д. 8, корп.3"`.
7. Для перехода на новую строку следует использовать последовательность `"\r\n"` — `00 0D 00 0A`.

   Перейти на новую строку также следует после последней строки в текстовом файле.

В разделе Пример текстового файла (на стр. 74) вы можете ознакомиться с примером текстового файла для регистрации пользователей.

Пример текстового файла

Ниже приведен пример того, как может быть составлен текстовый файл для регистрации пользователей:

```
STREET="ул. Карла Маркса, д. 87",E=babt@mail.ru,C=RU,S=Московская
обл.,L=г.Москва,SNILS=34232323122,INN=564342345434,Phone=8 (495)-100-66-
78,UnstructuredName=001-00-306900,O="ОАО "Ветка"",OU=Исполнительная
дирекция,T=Экспедитор,CN=Бабушкина Татьяна Петровна

STREET="ул. Боголюбова, д. 103, корп. 3",E=dorofeevap@roskompred.ru,C=RU,S=Московская
обл.,L=г.Москва,SNILS=56563443423,INN=645454345345,Phone=8 903-562-69-
```

```
71,UnstructuredName=00-00-789,O=Роскомпред,OU=Исполнительная дирекция,T=Старший
менеджер,CN=Дорофеев Антон Петрович
```

Действия при совпадении имен пользователей

Если в процессе регистрации будет найден пользователь с именем или псевдонимом, который уже был зарегистрирован в ViPNet Registration Point (например, при регистрации однофамильца), но при этом у пользователей есть отличия в других данных, программа выдаст следующее сообщение.

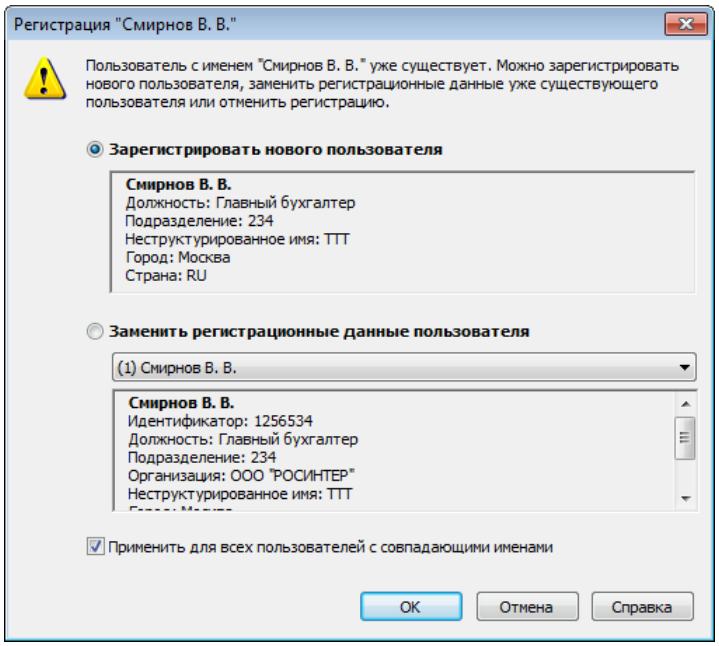


Рисунок 31. Сообщение о совпадение имен пользователей

В данном окне выполните следующие действия:

- Чтобы зарегистрировать пользователя как нового, но с тем же именем, в окне с сообщением выберите режим **Зарегистрировать нового пользователя** и нажмите кнопку **OK**. Установите флажок **Применить для всех пользователей с совпадающими именами** (при наличии) для автоматической регистрации всех новых пользователей с одинаковыми именами.

Примечание. Флажок **Применить для всех пользователей с совпадающими именами** появляется в случае, если в процессе регистрации программа обнаружит несколько пользователей, у которых будут совпадать имена с ранее зарегистрированными пользователями.

- Чтобы заменить данные ранее зарегистрированного пользователя на данные, которые были указаны в процессе регистрации нового пользователя:
  - Выберите режим **Заменить регистрационные данные пользователя**.
  - В списке выберите того пользователя, данные которого следует заменить.

В списке перечислены все пользователи, зарегистрированные ранее и имеющие одинаковые имена, но отличающиеся другими регистрационными данными. Пользователи с одинаковыми именами перечисляются в списке с добавлением порядкового номера в скобках (от 1 до N) перед именем. При выборе пользователя из списка ниже отображаются его регистрационные данные. По умолчанию в списке выбран самый первый пользователь.

- Установите флажок **Применить для всех пользователей с совпадающими именами** (при наличии) для автоматической замены регистрационных данных существующих пользователей.

Примечание. В данном случае опция будет работать следующим образом:

- Если имеется только один зарегистрированный пользователь, имя которого совпадает с именем нового пользователя, то замена данных для такого пользователя выполнится автоматически.
- Если имеется несколько зарегистрированных пользователей, имена которых совпадают с именем нового пользователя, то замена данных для таких пользователей будет проводиться индивидуально, то есть каждый раз будет появляться окно с сообщением о совпадении имен (см. Рисунок 34 на стр. 75).

- Нажмите кнопку **OK**.

В результате этой операции пользователь не будет удален, изменятся только его регистрационные данные. На странице **Завершение регистрации** к имени пользователя добавится слово «замена» и напротив появится значок  .

Совет. Если данные пользователя изменились, рекомендуется создать запрос на новый сертификат (см. «Создание запроса на новый сертификат» на стр. 93) и запрос на обновление дистрибутива ключей (см. «Создание запроса на обновление дистрибутива ключей» на стр. 131).

- Чтобы отменить регистрацию, нажмите кнопку **Отмена**. В этом случае новый пользователь не будет зарегистрирован, а данные ранее зарегистрированного пользователя, выбранного в списке, не изменятся.

Экспорт данных пользователей

В программе ViPNet Registration Point вы можете выполнить экспорт данных зарегистрированных пользователей в текстовый файл. Такой файл впоследствии можно использовать, например, для регистрации этих же пользователей в другом центре регистрации (см. раздел Регистрация с помощью текстового файла (на стр. 72)).

Для экспорта данных о пользователях выполните следующие действия:

1. В окне программы ViPNet Registration Point в разделе **Пользователи** выберите одного или нескольких пользователей, данные о которых требуется экспортировать.
2. В контекстном меню для данных пользователей выберите пункт **Экспортировать в файл**.
3. Укажите имя и путь к файлу экспорта.
4. По завершении всех действий нажмите кнопку **OK**.

Просмотр и редактирование данных пользователя

В программе ViPNet Registration Point вы можете просмотреть данные зарегистрированных пользователей. Для этого:

1. В окне программы в разделе **Пользователи** дважды щелкните учетную запись пользователя, сведения о котором вы хотите просмотреть, или в его контекстном меню выберите пункт **Свойства**.
2. В окне просмотра свойств пользователя ознакомьтесь с информацией на следующих вкладках:
   - **Общие** — содержит основные данные, указанные при регистрации пользователя, а также дату его регистрации в программе ViPNet Registration Point и идентификатор в программе ViPNet Центр управления сетью (создается при формировании дистрибутива ключей и не редактируется).

     Вы можете распечатать информацию о выбранном пользователе с помощью кнопки **Печать**.
   - **Местоположение** — содержит информацию о местонахождении пользователя и адрес его электронной почты.
   - **Дополнительно** — содержит дополнительные сведения о пользователе.
   - **Пароль** — содержит информацию о заданном пароле пользователя. Пароль задается либо при формировании запроса на сертификат ключа проверки электронной подписи (см. «Создание запроса на новый сертификат» на стр. 93), либо при формировании запроса на дистрибутив ключей (см. «Создание запроса на дистрибутив ключей» на стр. 130). Если пароль не задан, то указана информация о том, что его нет.

     Вы можете сохранить пароль в файл (`*.psw`) с помощью кнопки **Сохранить в файле**.

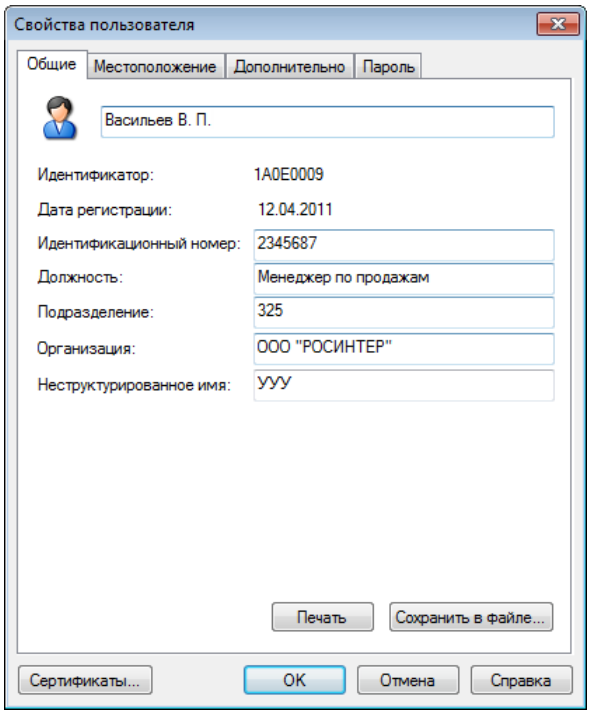


Рисунок 32. Просмотр общей информации о пользователе

3 Для просмотра списка сертификатов пользователя нажмите кнопку **Сертификаты**.

Вы также можете при необходимости отредактировать общую информацию о пользователе и изменить его дополнительные регистрационные данные. Для этого на вкладке **Общие**, **Местоположение** или **Дополнительно** внесите необходимые изменения и нажмите кнопку **OK**.

Удаление учетных записей пользователей

В программе ViPNet Registration Point вы можете удалять учетные записи зарегистрированных пользователей. При этом возможно несколько вариантов удаления:

- Вы можете удалить регистрационные данные пользователя, его сертификат и запросы, которые создавались для пользователя, из базы данных ViPNet Registration Point. При этом если удаляется учетная запись пользователя сети ViPNet, то информация о нем будет сохранена в программе ViPNet Центр управления сетью. Подробнее см. Удаление из базы данных ViPNet Registration Point (на стр. 80).
- С помощью соответствующего запроса вы можете удалить регистрационные данные пользователя сети ViPNet из базы данных ViPNet Центр управления сетью. В программе ViPNet Registration Point при этом все данные пользователя, сертификаты и запросы сохранятся. После удаления данных в ЦУСе пользователь становится внешним (см. «Внешний пользователь» на стр. 201). Подробнее см. Удаление из базы данных ViPNet Центр управления сетью (на стр. 81).

Удаление из базы данных ViPNet Registration Point

Примечание. Данным способом вы можете удалить одновременно несколько учетных записей пользователей.

Чтобы удалить учетную запись пользователя из базы данных ViPNet Registration Point, выполните следующие действия:

1. В окне программы ViPNet Registration Point в разделе **Пользователи** выберите пользователя, учетную запись которого требуется удалить.
2. В контекстном меню пользователя выберите пункт **Удалить в центре регистрации**.
3. В появившемся окне установите флажок **Я осознаю, что информацию невозможно будет восстановить** и нажмите кнопку **Удалить пользователя**.

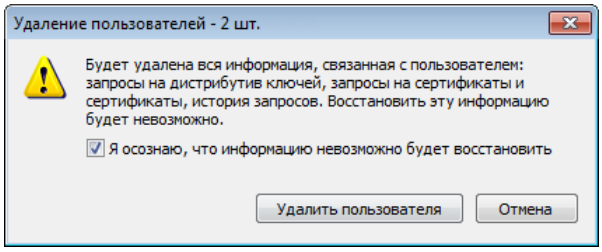


Рисунок 33. Сообщение об удалении сведений о пользователе

В результате учетная запись выбранного пользователя и вся связанная с ним информация будет удалена из базы данных ViPNet Registration Point.

Если пользователь являлся пользователем сети ViPNet, то информация о нем будет сохранена в программе ViPNet Центр управления сетью. Восстановить информацию о пользователе в программе ViPNet Registration Point можно будет только путем повторной регистрации.

Удаление из базы данных ViPNet Центр управления сетью

Удаление учетной записи пользователя из программы ViPNet Центр управления сетью осуществляется через формирование специального запроса в ViPNet Registration Point.

Чтобы удалить учетную запись пользователя из ЦУСа, выполните следующие действия:

1. В окне программы ViPNet Registration Point в разделе **Пользователи** выберите пользователя, учетную запись которого нужно удалить в ЦУСе. Для данного варианта удаления вы можете выбрать только учетную запись пользователя сети ViPNet, то есть пользователя, который получал через ViPNet Registration Point хотя бы один раз дистрибутив ключей.
2. В контекстном меню учетной записи пользователя выберите пункт **Запрос на удаление в ЦУСе**.

   В результате будет создан запрос на удаление учетной записи этого пользователя. Он появится в разделе **Запросы** > **Запросы на удаление** и с помощью транспортного модуля будет отправлен в ЦУС (см. раздел Запуск транспортного модуля (на стр. 20)). Если администратор ЦУСа (на стр. 200) примет решение об удовлетворении этого запроса, то вся информация о пользователе будет удалена из базы данных ЦУСа. В программе ViPNet Registration Point запросу на удаление будет присвоен статус **Удовлетворен**. При этом регистрационные сведения о данном пользователе в программе ViPNet Registration Point останутся.

Создание и редактирование шаблонов пользователей

При регистрации пользователей вручную используются специальные шаблоны пользователей (см. «Шаблон пользователя» на стр. 206). В состав ViPNet Registration Point по умолчанию входит встроенный стандартный шаблон пользователя, который нельзя изменить или удалить. В процессе работы вы можете создавать другие шаблоны пользователей и впоследствии редактировать их и удалять. При создании нового шаблона или редактировании уже созданного шаблона добавляются необходимые атрибуты пользователя, устанавливается порядок их следования, назначаются обязательные для заполнения атрибуты, а также задаются значения атрибутов по умолчанию. При отсутствии других шаблонов регистрация пользователя производится на основе стандартного шаблона.

Для создания нового шаблона пользователя выполните следующие действия:

1 В окне программы ViPNet Registration Point в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка** на панели инструментов.

2 В появившемся окне на панели навигации выберите раздел **Шаблоны пользователей**.

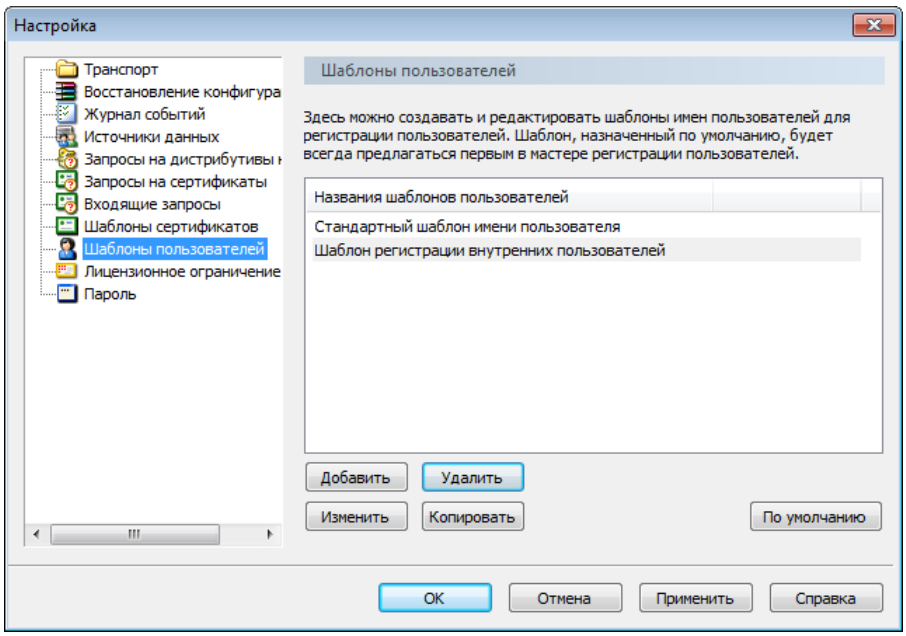


Рисунок 34. Управление шаблонами пользователей

3 В разделе **Шаблоны пользователей** нажмите кнопку **Добавить** и следуйте указаниям мастера создания шаблона пользователя.

4 На первой странице мастера введите имя шаблона и нажмите кнопку **Далее**.

5 На странице **Сведения о пользователе** укажите атрибуты имени пользователя, которые будут заполняться при регистрации. Для добавления атрибутов воспользуйтесь кнопкой

Добавление атрибутов, для удаления ненужных атрибутов — кнопкой **Удалить**. С помощью кнопок **Вверх** и **Вниз** определите порядок следования атрибутов.

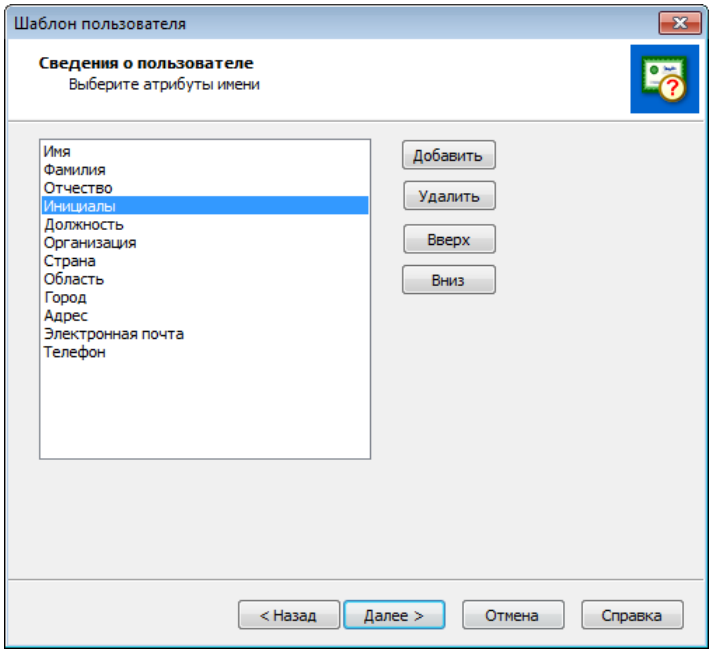


Рисунок 35. Выбор атрибутов имени пользователя

Нажмите кнопку **Далее**.

6 При необходимости на следующей странице задайте параметры атрибутов. Для этого:

6.1 В списке выберите нужный атрибут и нажмите кнопку **Изменить**.

6.2 В окне **Значения атрибутов** укажите значение атрибута по умолчанию.

Чтобы при регистрации пользователя поле атрибута было обязательным для заполнения, установите флажок **Поле обязательно для заполнения**.

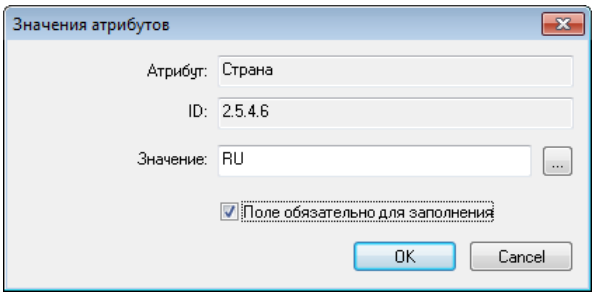


Рисунок 36. Задание параметров атрибута

7 По завершении всех действий нажмите кнопку **Готово**. При необходимости изменения параметров шаблона вернитесь на нужную страницу с помощью кнопки **Назад**.

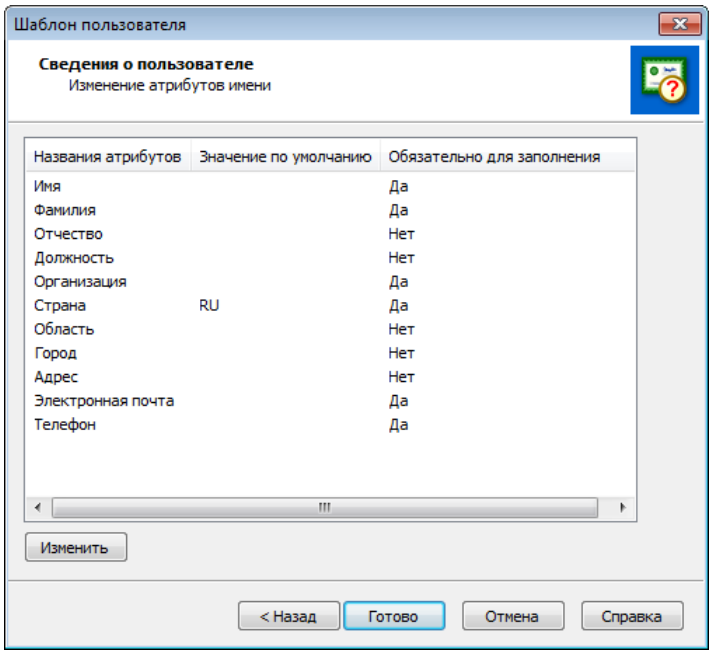


Рисунок 37. Настройка используемых в шаблоне атрибутов и их значений

8 В результате в списке шаблонов пользователей появится новый шаблон. Для сохранения созданного шаблона нажмите кнопку **Применить**.

Вы также можете создать новый шаблон на основе существующего. Для этого:

1 В списке шаблонов раздела **Шаблоны пользователей** выберите нужный шаблон и нажмите кнопку **Копировать**.

2 В появившемся окне укажите название нового шаблона.

3 Нажмите кнопку **ОК**.

В результате параметры нового шаблона будут полностью соответствовать тому шаблону, на основе которого он был создан.

Для изменения параметров шаблона пользователя воспользуйтесь кнопкой **Изменить**, для удаления ненужного шаблона — кнопкой **Удалить**. Чтобы при регистрации пользователя использовался нужный шаблон по умолчанию, выберите его в списке и нажмите кнопку **По умолчанию**.

Настройка подключения к внешним источникам данных

Настройка подключения к внешним источникам данных требуется в том случае, если при регистрации пользователей будет использоваться информация из домена Active Directory (AD) (на стр. 199) или текстового файла.

Настройка подключения к Active Directory

Чтобы настроить параметры подключения к Active Directory, выполните следующие действия:

1 В окне программы в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка** на панели инструментов.

2 В появившемся окне на панели навигации выберите раздел **Источники данных**.

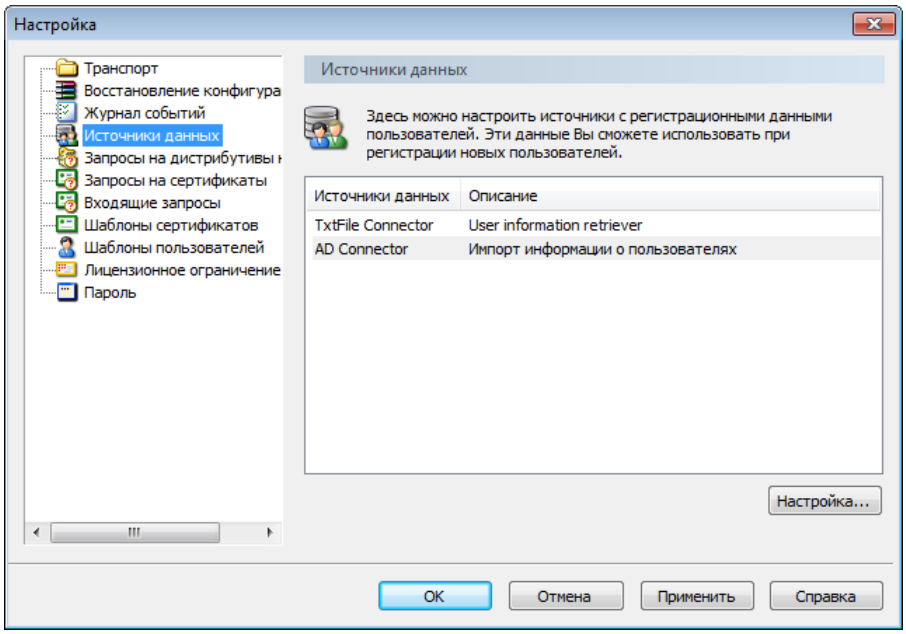


Рисунок 38. Настройка подключения к внешним источникам данных

Примечание. Настройку параметров подключения к Active Directory вы также можете выполнить в процессе регистрации при выборе внешнего источника данных (см. Регистрация через Active Directory (на стр. 69)).

---

3 В разделе **Источники данных** в списке источников выберите **AD Connector** и нажмите кнопку **Настройка**.

4 В окне **Настройка работы с Active Directory** на вкладке **Подключение** выполните следующие действия:

- Установите переключатель **Контроллер домена** в положение:
  - **По умолчанию** для подключения к контроллеру домена вашей организации, если он в ней развернут. Подключение к контроллеру произойдет только в том случае, если вы являетесь пользователем корпоративного домена.
  - **Другой контроллер домена** для подключения к конкретному контроллеру домена. При этом в поле введите IP-адрес домена либо его DNS-имя.
- Укажите учетные данные пользователя для подключения к домену:
  - Чтобы по умолчанию использовались учетные данные пользователя ОС, щелкните **Учетные данные текущего пользователя Windows**.
  - Чтобы использовались учетные данные конкретного пользователя, щелкните **Другие учетные данные** и задайте имя пользователя и пароль.
- Задайте область поиска данных:
  - Для поиска по всему каталогу Active Directory щелкните **Поиск по всему каталогу**.
  - Для поиска по конкретному каталогу щелкните **Ограничить область поиска** и укажите отличительное имя контейнера.
- В поле **Порт подключения** введите номер порта подключения к домену. Номер должен состоять не более чем из 5 знаков в диапазоне от 1 до 65000.
- Чтобы установить параметры подключения к домену по умолчанию, нажмите кнопку **По умолчанию**.

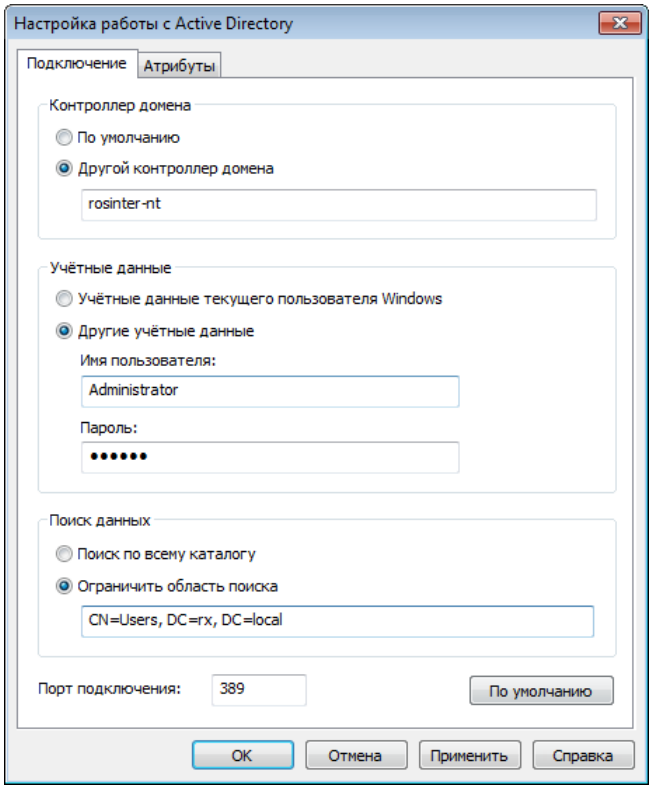


Рисунок 39. Настройка параметров подключения к Active Directory

5 В окне **Настройка работы с Active Directory** на вкладке **Атрибуты** настройте соответствие между атрибутами имени пользователя в формате X.500 и атрибутами каталога Active Directory http://msdn.microsoft.com/en-us/library/ms677979%28v=vs.85%29.aspx , а также при необходимости измените параметры обработки атрибутов.

Для того, чтобы установить все значения и параметры обработки атрибутов по умолчанию, нажмите кнопку **По умолчанию**. Все атрибуты, заданные по умолчанию, обрабатываются.

Вы можете изменить значение атрибута с помощью кнопки **Изменить атрибут Active Directory**. Значение должно быть непустым и уникальным. При изменении значения атрибута выполняется его проверка. В случае успешной проверки введенное значение присваивается атрибуту.

Для изменения параметра обработки атрибута установите или снимите флажок напротив его названия.

Внимание! Снятие флажка напротив атрибута означает, что:

- Сертификаты, имеющие в имени владельца данный атрибут, обрабатываться не будут.
- Не будет выполняться проверка наличия поддержки атрибута на стороне сервера.

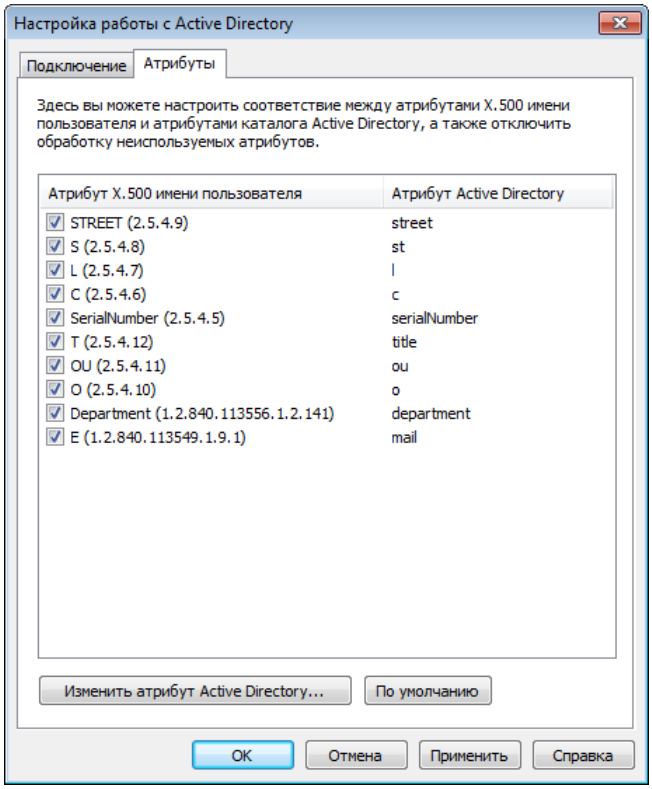


Рисунок 40. Настройка соответствия атрибутов имени X.500 с атрибутами Active Directory

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

7 В окне **Настройка** нажмите кнопку **OK**.

В результате указанные параметры будут использоваться при подключении к домену во время регистрации пользователя.

Выбор текстового файла для регистрации

Чтобы предварительно указать текстовый файл, который будет использоваться для регистрации пользователей, выполните следующие действия:

1 В окне программы в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка** на панели инструментов.

2 В появившемся окне (см. Рисунок 41 на стр. 85) перейдите в раздел **Источники данных**.

3 В списке источников данных выберите **TxtFile Connector** и нажмите кнопку **Настройка**.

4 В появившемся окне с помощью кнопки **Обзор** задайте путь к файлу, который будет использоваться для регистрации пользователей.

5 Нажмите кнопку **OK**.

Примечание. Задать путь к файлу с именами пользователей вы также можете в процессе регистрации при выборе внешнего источника данных (см. Регистрация с помощью текстового файла (на стр. 72)).

Настройка параметров паролей пользователей

В процессе формирования запроса на сертификат или запроса на дистрибутив ключей задается пароль пользователя, который является и паролем к контейнеру ключей, и паролем к дистрибутиву ключей. Прежде чем задать пароль, требуется определить его тип. Для экономии времени тип задаваемых паролей по умолчанию вы можете задать в настройках программы ViPNet Registration Point и не указывать его в мастере создания запроса на сертификат. Для случайных паролей в настройках вы также можете указать параметры их создания.

Для настройки параметров создаваемых паролей выполните следующие действия:

1 В окне программы ViPNet Registration Point в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка** на панели инструментов.

2 В появившемся окне на панели навигации выберите раздел **Пароли**.

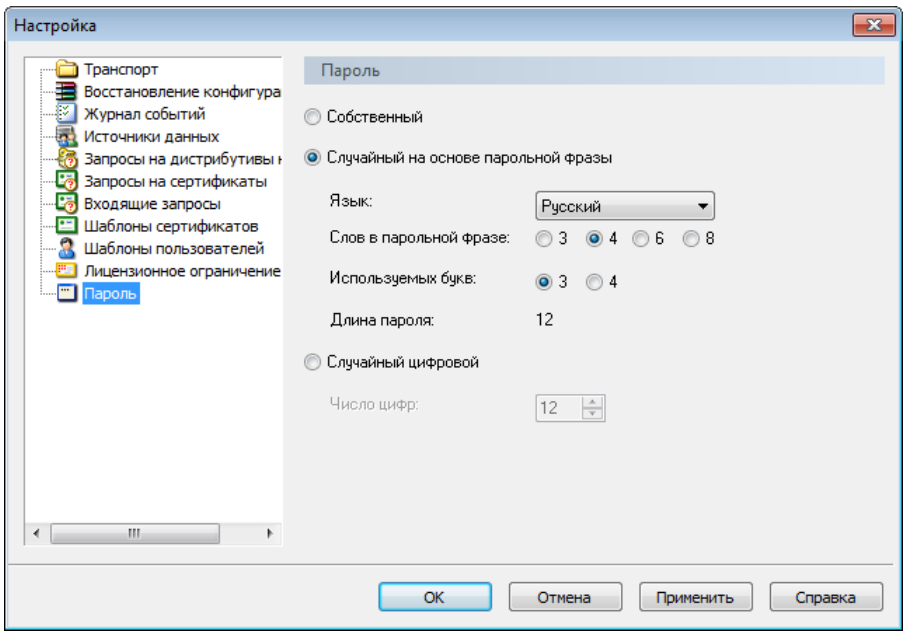


Рисунок 41. Настройка параметров создаваемых паролей

3 В разделе **Пароли** выберите тип пароля:

- **Собственный пароль** — для создания паролей вручную. Длина таких паролей должна быть не менее 8 символов и не более 31.
- **Случайный пароль** — для создания паролей, формируемых автоматически на основе парольных фраз (см. «Парольная фраза» на стр. 203) по заданным параметрам.
- **Случайный цифровой пароль** — для создания паролей, формируемых автоматически из заданного числа цифр.

Внимание! Длина пароля должна быть не меньше 8 символов и не должна превышать 31 символ. Пароли с длиной более 31 символа не могут использоваться в текущих версиях приложений ViPNet. Данное ограничение связано с существующим алгоритмом передачи пароля в криптопровайдер. В соответствии с этим алгоритмом длина пароля не должна превышать 31 символ.

4 При выборе типа **Случайный пароль** дополнительно укажите параметры случайных паролей на основе парольных фраз:

- В списке **Язык** выберите язык парольной фразы (русский, английский, немецкий, испанский или французский).
- В списке **Слов в парольной фразе** выберите число слов (3, 4, 6 или 8), из которых будет состоять парольная фраза. Чем больше число слов, тем длиннее и, соответственно, надежнее будет пароль.
- В списке **Используемых букв** выберите число начальных букв каждого слова (3 или 4), которые войдут в пароль.

В строке **Длина пароля** отобразится количество букв в пароле, который будет сформирован с учетом указанных параметров. Формируемый пароль имеет длину не менее 9 символов.

5 При выборе типа **Случайный цифровой пароль** дополнительно укажите длину случайных цифровых паролей (от 8 до 32 цифр). Для обеспечения стойкости, эквивалентной случаю использования символьного пароля длины 8 при мощности алфавита 36 следует выбирать размерность пароля не менее 14 цифр.

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

В результате в мастере создания запроса на сертификат или дистрибутив ключей по умолчанию будет выбран тип пароля, которые вы указали. Параметры случайных паролей, если вы их задавали, в мастере также будут указаны.

7

Действия с сертификатами пользователей

Создание запроса на новый сертификат

В программе ViPNet Registration Point для любого зарегистрированного пользователя вы можете сформировать запрос на получение сертификата подписи.

Внимание! Создание запроса на сертификат будет невозможно в следующих случаях:

- У вас нет ключа электронной подписи и сертификата ключа проверки электронной подписи. Получите их у администратора ViPNet Удостоверяющий и ключевой центр (см. раздел Работа в ViPNet Registration Point без ключа электронной подписи и сертификата (на стр. 18)).
- Текущий сертификат администратора ViPNet Registration Point стал недействительным, требуется его обновить (см. раздел Процедура обновления ключа электронной подписи и сертификата (на стр. 145)).
- Число запросов на сертификаты достигло числа, указанного в лицензии. Требуется расширить лицензию (см. раздел Лицензионные ограничения (на стр. 19)).

Внимание! Администратор центра регистрации несет ответственность за проверку данных создаваемых и обрабатываемых входящих запросов и последующее издание сертификата по этим запросам.

При создании запроса на сертификат формируется пара ключей, при этом ключ электронной подписи (на стр. 202) помещается в отдельный контейнер на диске или внешнем устройстве (см. «Контейнер ключей» на стр. 202), а ключ проверки электронной подписи (на стр. 202) — непосредственно в запрос на сертификат.

Чтобы при создании запроса в него добавлялось расширение с информацией о криптографическом средстве, используемом для электронной подписи, предварительно выполните дополнительную настройку (см. «Настройка параметров создания запросов на сертификаты» на стр. 100). Чтобы при создании запроса пароль к контейнеру ключей создавался нужного типа и с заданными параметрами (если пароль случайный), выполните настройку параметров создаваемых паролей (см. «Настройка параметров паролей пользователей» на стр. 90).

Чтобы создать запрос на новый сертификат для зарегистрированного пользователя, выполните следующие действия:

1. В окне программы ViPNet Registration Point в разделе **Пользователи** выберите нужного пользователя и выполните одно из действий:
   - В контекстном меню для данного пользователя выберите пункт **Сертификаты**, затем щелкните **Создать запрос**.

- На панели инструментов нажмите кнопку **Создать запрос на сертификат**  .

Следуйте указаниям мастера создания запроса на сертификат.

Внимание! В зависимости от настроек программы некоторые страницы мастера могут быть пропущены (подробнее см. раздел Настройка параметров создания запросов на сертификаты (на стр. 100)).

---

2 На первой странице мастера в списке выберите шаблон сертификата, который будет использоваться при создании запроса, и нажмите кнопку **Далее**.

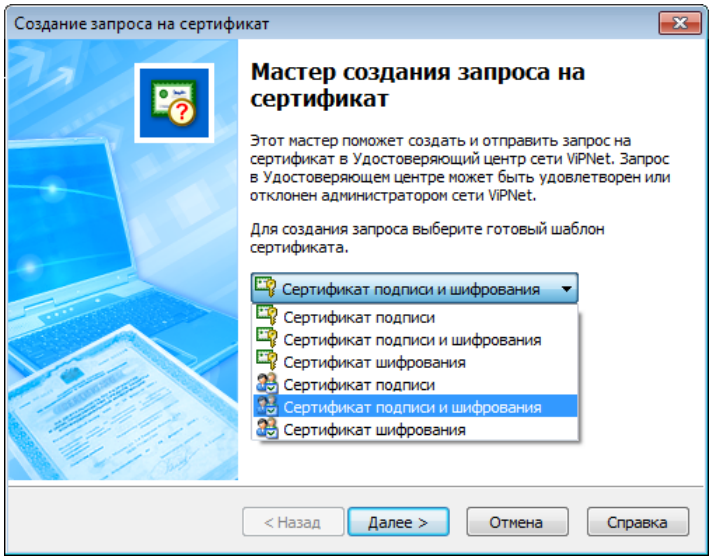


Рисунок 42. Выбор шаблона сертификата

В списке присутствуют шаблоны сертификатов двух типов:

- Шаблоны, заданные в программе ViPNet Удостоверяющий и ключевой центр (отмечены значком ). Список этих шаблонов доставляется на сетевой узел с программой ViPNet Registration Point в составе списков аннулированных сертификатов (см. «Список аннулированных сертификатов (CRL)» на стр. 205). Параметры шаблонов сертификатов этого типа вы не можете изменять в программе ViPNet Registration Point.
- Шаблоны, заданные в программе ViPNet Registration Point (отмечены значком ). При необходимости вы можете изменить параметры существующих шаблонов сертификатов этого типа или создать новые (см. «Создание и редактирование шаблонов сертификатов» на стр. 118).

  В конфигурацию программы ViPNet Registration Point входит несколько стандартных шаблонов сертификатов: **Сертификат подписи**, **Сертификат подписи и шифрования**, **Сертификат шифрования**. Данные шаблоны отличаются только набором используемых расширений, определяющих назначение сертификата.

Внимание! Если требуется, чтобы в списке стандартных шаблонов сертификатов присутствовали шаблоны сертификатов подписи и шифрования с алгоритмом ГОСТ Р 34.11-2012/512, то запросите у администратора УКЦ

обновление ключей узлов или списков аннулированных сертификатов, в составе которых на узел с ViPNet Registration Point поступят указанные шаблоны сертификатов.

3 На странице **Ключ электронной подписи** выберите криптопровайдер в соответствии с приведенной ниже таблицей. Выбранный криптопровайдер определит алгоритм электронной подписи, по которому будут создаваться ключ электронной подписи и ключ проверки электронной подписи.

Внимание! В запросе на сертификат пользователя алгоритм электронной подписи должен быть таким же, как и в сертификате администратора центра регистрации. Поэтому вы не можете создать запрос на сертификат пользователя с алгоритмом, отличным от алгоритма в вашем сертификате.

Кроме этого, укажите параметры алгоритма электронной подписи. В соответствии с заданными параметрами будет автоматически определена длина ключа проверки электронной подписи.

Внимание! По требованиям ФСБ России с 1 января 2019 года использование алгоритма ГОСТ Р 34.10-2001 будет недопустимо. В связи с этим уже сейчас рекомендуется выдавать сертификаты по новому алгоритму ГОСТ Р 34.10-2012.

Таблица 4. Характеристика криптопровайдеров и алгоритмов электронной подписи

Криптопровайдер и соответствующий ему алгоритм электронной подписи	**Параметры алгоритма подписи**	**Длина ключа проверки электронной подписи и алгоритм хэширования**
Infotecs Cryptographic Service Provider ГОСТ Р 34.10-2001 См. RFC 4357 http://www.ietf.org/rfc/rfc4357.txt Стандарт электронной подписи, основанный на арифметике эллиптических кривых OID «1.2.643.2.2.19»	ГОСТ Р 34.10 - 2001. Параметры по умолчанию OID «1.2.643.2.2. 35.1» ГОСТ Р 34.10 - 2001 Параметры подписи B OID «1.2.643.2.2. 35.2» ГОСТ Р 34.10 - 2001. Параметры подписи C OID «1.2.643.2.2. 35.3»	512 бит ГОСТ Р 34.11-94
Infotecs GOST 2012/512 Cryptographic Service Provider ГОСТ Р 34.10-2012/512 Новый стандарт электронной подписи от 2012 года с	ГОСТ Р 34.10 - 2001. Параметры по умолчанию OID «1.2.643.2.2. 35.1» ГОСТ Р 34.10 - 2001 Параметры подписи B	512 бит ГОСТ Р 34.11-2012/256

Криптопровайдер и соответствующий ему алгоритм электронной подписи	Параметры алгоритма подписи	Длина ключа проверки электронной подписи и алгоритм хэширования
длиной ключа электронной подписи 256 бит OID «1.2.643.7.1.1.1.1»	OID «1.2.643.2.2. 35.2» ГОСТ Р 34.10 - 2001. Параметры подписи С OID «1.2.643.2.2. 35.3»	
Infotecs GOST 2012/1024 Cryptographic Service Provider ГОСТ Р 34.10-2012/1024 Новый стандарт электронной подписи от 2012 года с длиной ключа электронной подписи 512 бит OID «1.2.643.7.1.1.1.2»	ГОСТ Р 34.10 - 2012/1024. Набор параметров А ГОСТ Р 34.10 - 2012/1024. Набор параметров В	1024 бит ГОСТ Р 34.11-2012/512

Чтобы при последующих запусках мастера пропускать данную страницу, установите флажок **Не показывать больше эту страницу**. Включить опцию отображения этой страницы можно будет только в настройках программы.

После этого нажмите кнопку **Далее**.

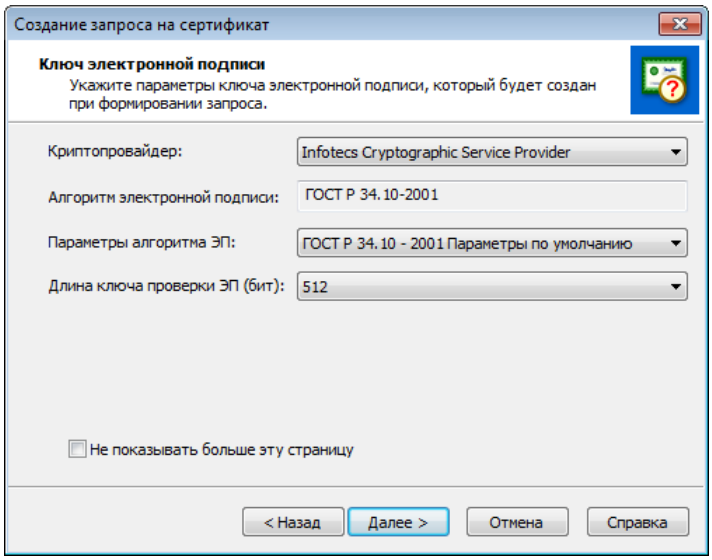


Рисунок 43. Выбор параметров ключа электронной подписи

4 На странице **Срок действия сертификата** задайте желаемый срок действия запрашиваемого сертификата любым удобным способом, после чего нажмите кнопку **Далее**.

Чтобы при последующих запусках мастера пропускать данную страницу, установите флажок **Не показывать больше эту страницу**. После этого включить опцию отображения этой страницы можно будет только в настройках программы.

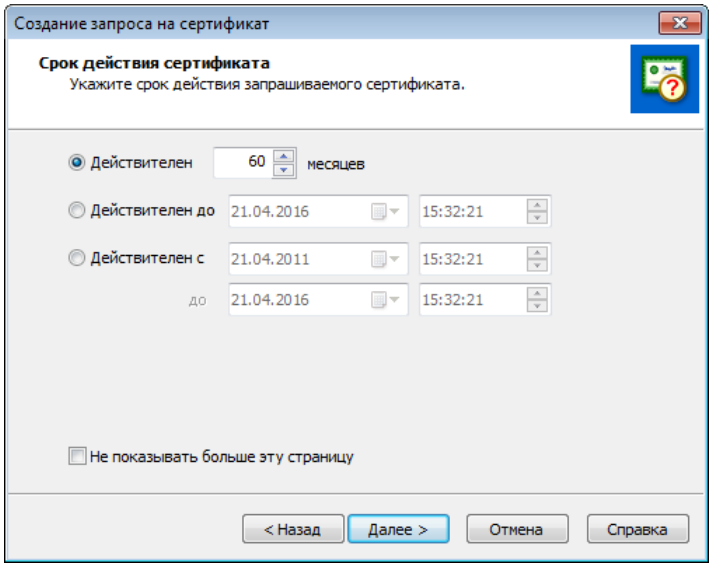


Рисунок 44. Указание желаемого срока действия сертификата

5 На странице **Создание контейнера ключей** укажите место сохранения контейнера ключей:

- папку на жестком или съемном диске;
- устройство с указанием его параметров и ПИН-кода.

Примечание. Для использования какого-либо внешнего устройства необходимо подключить и установить драйверы этого устройства. Перечень доступных устройств хранения данных и полезная информация об использовании устройств содержится в документе «ViPNet CSP. Руководство пользователя».

После этого нажмите кнопку **Далее**.

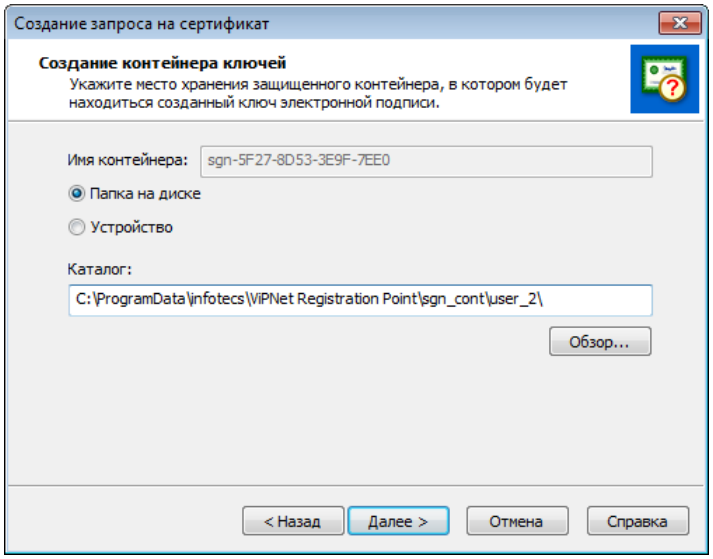


Рисунок 45. Указание места сохранения контейнера ключей

6 На странице **Тип пароля защиты ключа электронной подписи** укажите тип пароля к контейнеру ключей, если он не был задан предварительно в настройках программы:

- **Собственный пароль** — пароль, задаваемый вами вручную.
- **Случайный пароль на основе парольной фразы** — пароль, формируемый автоматически на основе парольной фразы (см. «Парольная фраза» на стр. 203).
- **Случайный цифровой пароль** — пароль, формируемый автоматически из заданного числа цифр.

Данный пароль станет паролем пользователя. Если для пользователя уже создавался пароль (например, при создании запроса на дистрибутив ключей), то на странице мастера будет установлен флажок **Использовать текущий пароль пользователя**. Для просмотра текущего пароля нажмите кнопку **Пароль пользователя**. Если вы хотите, чтобы для пользователя был создан новый пароль, снимите указанный флажок и при необходимости измените тип пароля.

Нажмите кнопку **Далее**.

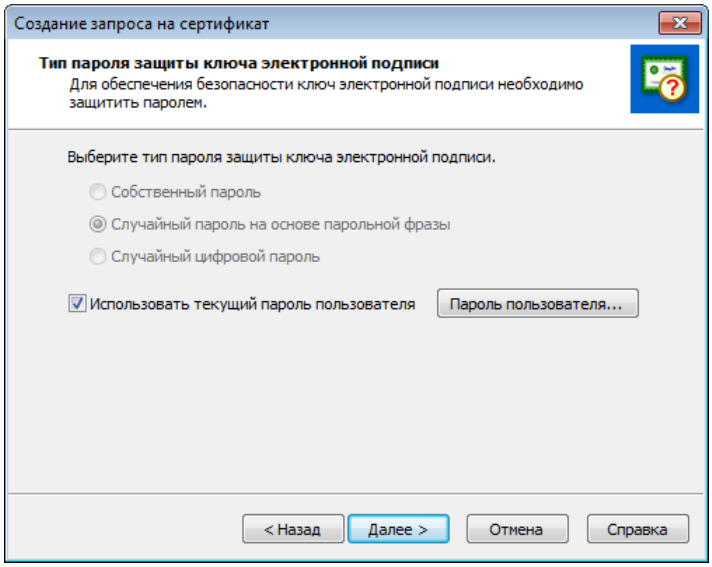


Рисунок 46. Выбор типа пароля доступа к контейнеру ключей

7 Если сохраняется текущий пароль пользователя, появится страница готовности к созданию запроса на сертификат (см. п. 8).

Если должен быть создан новый пароль и был выбран тип **Собственный пароль**, то на появившейся странице задайте пароль и его подтверждение и нажмите кнопку **Далее**.

Если был выбран тип одного из случайных паролей, то появится электронная рулетка, если она еще не запускалась в рамках текущего сеанса работы программы. Поводите указателем в пределах окна **Электронная рулетка**, после чего запомните новый пароль (или парольную фразу) на странице **Пароль защиты ключа электронной подписи**. При необходимости измените параметры случайного пароля и создайте другой.

Внимание! Длина пароля должна быть не меньше 8 символов и не должна превышать 31 символ. Пароли с длиной более 31 символа не могут использоваться в текущих версиях приложений ViPNet. Данное ограничение связано с существующим алгоритмом передачи пароля в криптопровайдер. В соответствии с этим алгоритмом длина пароля не должна превышать 31 символ.

Нажмите кнопку **Далее**.

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

9 На странице **Завершение создания запроса на сертификат** нажмите кнопку **Готово**.

Чтобы дождаться ответа по данному запросу из УКЦ, установите флажок **Ожидать сертификат из Удостоверяющего центра**.

Чтобы добавить изданный сертификат в контейнер ключей сразу после его получения, установите флажок **Автоматически сохранять пришедший сертификат в контейнер ключей** (доступен только при включении опции ожидания сертификата).

В результате будет сформирован запрос, который появится в разделе **Запросы на сертификаты** > **Отправленные**. Запрос будет подписан текущим сертификатом администратора ViPNet Registration Point и с помощью модуля ViPNet MFTP отправлен в УКЦ (см. раздел Запуск транспортного модуля (на стр. 20)).

Если администратор УКЦ примет решение об удовлетворении запроса, то будет издан сертификат ключа проверки электронной подписи, после чего отправлен в форме ответа на запрос на узел с ViPNet Registration Point. В программе ViPNet Registration Point полученный сертификат появится в разделе **Сертификаты**, а запросу на данный сертификат будет присвоен статус **Удовлетворен**. Если сертификат был получен, но по каким-то причинам не отобразился в программе в разделе **Сертификаты**, см. указания раздела Получены не все сертификаты, изданные в УКЦ по запросам (на стр. 182).

Изданный сертификат будет автоматически добавлен в контейнере ключей, если при создании запроса на сертификат была установлена соответствующая опция (см. п. 9 списка). В противном случае его следует добавить в контейнер ключей вручную (см. «Добавление сертификата в контейнер ключей» на стр. 116).

При отклонении запроса на сертификат администратором УКЦ появится соответствующее сообщение, запросу будет присвоен статус **Отклонен**.

Настройка параметров создания запросов на сертификаты

В программе ViPNet Registration Point вы можете настроить некоторые параметры создания запросов на сертификаты для пользователей.

Если при создании запроса на сертификат значения параметров ключа проверки электронной подписи и его срока действия остаются по умолчанию (то есть не изменяются), то вы можете упростить процедуру создания запроса на сертификат, исключив из мастера страницы с данными параметрами.

Кроме этого, если требуется, чтобы создаваемые запросы на сертификаты содержали расширение с информацией о криптографическом средстве, которое используется для создания электронной подписи, то вы можете настроить опцию добавления такого расширения. Впоследствии данное расширение попадет в сертификаты, изданные по таким запросам.

Примечание. Указанное расширение может добавляться в запросы на сертификаты и соответственно в издаваемые сертификаты подписи по требованиям приказа ФСБ РФ 27.12.2011 №795 «Об утверждении Требований к форме квалифицированного сертификата (см. „Квалифицированный сертификат“ на стр. 202) ключа проверки электронной подписи», его наличие не является обязательным.

Чтобы настроить указанные параметры, выполните следующие действия:

1. В окне программы ViPNet Registration Point в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
2. В появившемся окне на панели навигации выберите раздел **Запросы на сертификаты**.

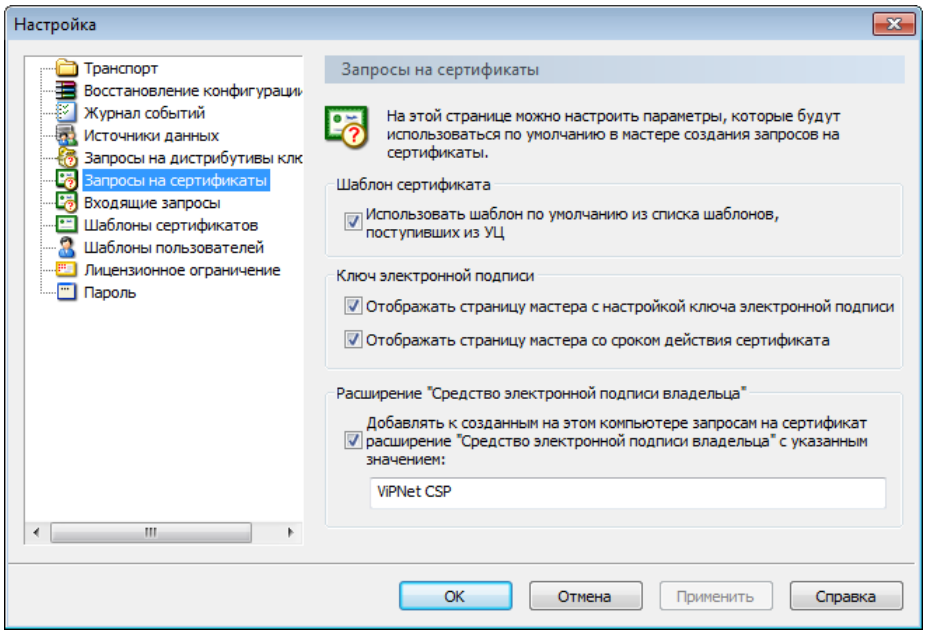


Рисунок 47. Настройки параметров создания запроса на сертификат

3 Чтобы при создании запроса использовать шаблон сертификата, заданный по умолчанию в программе ViPNet Удостоверяющий и ключевой центр, установите флажок **Использовать шаблон по умолчанию из списка шаблонов, поступивших из УЦ**. Если вы хотите использовать свой шаблон по умолчанию (то есть заданный в программе ViPNet Registration Point), снимите этот флажок.

4 Чтобы не показывать в мастере страницу **Ключ электронной подписи**, снимите флажок **Отображать страницу мастера с настройкой ключа электронной подписи**.

5 Чтобы не показывать в мастере страницу **Срок действия сертификата**, снимите флажок **Отображать страницу мастера со сроком действия сертификата**.

6 Чтобы в создаваемые запросы на сертификаты автоматически добавлялось расширение с информацией о средстве создания электронной подписи, в группе **Расширение «Средство электронной подписи владельца»** установите соответствующий флажок и в поле ниже введите наименование данного средства.

7 Для сохранения настроек нажмите кнопку **Применить**.

Обработка запросов на сертификаты от внешних пользователей

Программа ViPNet Registration Point позволяет принимать и обрабатывать запросы на сертификаты от внешних пользователей (см. «Внешний пользователь» на стр. 201). Такие запросы формируются в сторонних приложениях (например, в ViPNet CSP) и могут быть двух видов:

- Запрос на издание нового сертификата в формате PKCS#10 http://www.rsa.com/rsalabs/node.asp?id=2132. См. раздел Обработка запроса на издание сертификата (на стр. 102).
- Запрос на обновление сертификата, подписанный предыдущим сертификатом зарегистрированного пользователя в формате CMC http://en.wikipedia.org/wiki/Certificate_Management_over_CMS. См. раздел Обработка запроса на обновление сертификата (на стр. 105).

Примечание. При обработке перечисленных запросов используется шаблон сертификата по умолчанию. В соответствии с этим шаблоном в запросы добавляется желаемый срок действия сертификата, поскольку данный параметр первоначально в них отсутствует (не задается при создании).

Обработка запроса на издание сертификата

При обработке запроса на издание сертификата в формате PKCS#10 сначала производится регистрация пользователя. Затем сформированный запрос на сертификат подписывается текущим сертификатом администратора ViPNet Registration Point и с помощью модуля ViPNet MFTP отправляется в ViPNet Удостоверяющий и ключевой центр.

Чтобы обработать запрос на издание сертификата, выполните следующие действия:

1 Поместите полученный от пользователя запрос в папку `Import`, которая находится в папке обработки входящих запросов. Вы можете задать папку обработки входящих запросов в настройках программы (см. «Настройка параметров обработки запросов от внешних пользователей» на стр. 105). По умолчанию это папка `C:\Program Files\InfoTeCS\ViPNet Registration Point\PKCS10`.

Появится сообщение о поступлении новых запросов на сертификаты и запрос будет помещен в раздел **Запросы на сертификаты** > **Входящие**.

Выполните обработку запроса. Для этого щелкните данный запрос правой кнопкой мыши и в контекстном меню выберите пункт:

- **Принять**, чтобы принять, подписать и отправить запрос на сертификат в УКЦ. Запрос будет перемещен в раздел отправленных запросов.

  Если в настройках программы установлена опция редактирования полей, запустится мастер регистрации пользователя на основе входящего запроса. Выполните регистрацию пользователя (см. «Регистрация вручную» на стр. 66).

- **Отклонить**, чтобы отклонить запрос. Запрос будет перемещен в раздел отклоненных запросов.

Внимание! Если поступивший запрос на сертификат идентичен одному из уже обработанных запросов, то он будет проигнорирован и помещен в подпапку `Bad` папки установки программы.

Если поступивший запрос на издание сертификата имеет данные уже зарегистрированного пользователя и при этом включает другой ключ проверки электронной подписи, то в зависимости от настроек он будет автоматически обработан как запрос на обновление сертификата либо помещен в раздел **Запросы на сертификаты** > **Входящие** для обработки вручную (подробнее см. раздел Обработка запроса на издание сертификата при совпадении имен пользователей (на стр. 104)).

Если в запросе указаны политики применения сертификата, не зарегистрированные в программе ViPNet Registration Point (и соответственно в УКЦ), появится сообщение, содержащее предупреждение и предложение продолжить работу с запросом. Чтобы удалить политики и обработать запрос, в окне предупреждения нажмите кнопку **Да**. Чтобы отклонить запрос, нажмите кнопку **Нет**.

Если вы отправили запрос на сертификат в УКЦ и администратор примет решение о его удовлетворении, то будет издан сертификат ключа проверки электронной подписи, после чего отправлен в форме ответа на запрос на узел с ViPNet Registration Point. В программе ViPNet Registration Point полученный сертификат появится в разделе **Сертификаты**, а запросу на данный сертификат будет присвоен статус **Удовлетворен**. Если сертификат был получен, но по каким-то причинам не отобразился в программе в разделе **Сертификаты**, см. указания раздела Получены не все сертификаты, изданные в УКЦ по запросам (на стр. 182).

Если в настройках программы установлена опция автоматического переноса сертификата в папку, изданный сертификат будет автоматически экспортирован в нужную папку. По умолчанию папка экспорта: `C:\Program Files\InfoTeCS\ViPNet Registration Point\PKCS10\Export`. В противном случае при необходимости выполните экспорт сертификата в папку вручную (см. «Экспорт сертификата» на стр. 113).

Обработка запроса на издание сертификата при совпадении имен пользователей

В программу ViPNet Registration Point может поступить запрос на издание сертификата, в котором данные пользователя будут совпадать с данными уже зарегистрированного пользователя и при этом будет содержаться другой ключ проверки электронной подписи.

Такой запрос будет помещен в раздел **Запросы на сертификаты** > **Входящие**.

Чтобы обработать запрос подобного типа, выполните следующие действия:

1 Щелкните данный запрос правой кнопкой мыши и в контекстном меню выберите пункт:

- **Принять**, чтобы принять и отправить запрос на сертификат в программу ViPNet Удостоверяющий и ключевой центр.
- **Отклонить**, чтобы отклонить запрос. Запрос будет перемещен в раздел отклоненных запросов.

2 В случае принятия запроса появится окно **Пользователь уже существует в ViPNet Registration Point**. Установите в данном окне переключатель в положение:

- **Редактировать данные пользователя** для регистрации нового пользователя на основе выбранного запроса на обновление.
- **Отклонить запрос**, чтобы отклонить запрос. Запрос будет перемещен в раздел отклоненных запросов.

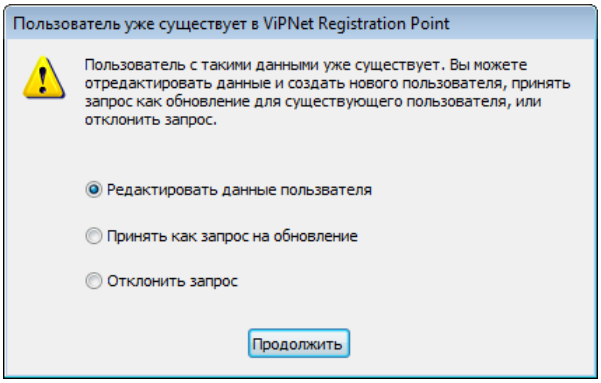


Рисунок 48. Сообщение об обнаружении уже зарегистрированного пользователя

3 Нажмите кнопку **Продолжить**.

Если вы выбрали опцию редактирования данных, запустится мастер регистрации пользователя на основе входящего запроса. Выполните регистрацию пользователя (см. «Регистрация вручную» на стр. 66), после чего сформируйте для него запрос на сертификат (см. «Создание запроса на новый сертификат» на стр. 93).

Обработка запроса на обновление сертификата

Чтобы обработать запрос на обновление существующего сертификата пользователя, поместите его в папку `Import`, которая находится в папке обработки входящих запросов (см. «Настройка параметров обработки запросов от внешних пользователей» на стр. 105). По умолчанию это папка `C:\Program Files\InfoTeCS\ViPNet Registration Point\PKCS10`.

Внимание! Если поступивший запрос идентичен одному из уже обработанных запросов, то он будет проигнорирован и помещен в подпапку `Bad` папки установки программы.

Данный запрос будет автоматически отправлен в программу ViPNet Удостоверяющий и ключевой центр. Если администратор УКЦ примет решение о его удовлетворении, то будет издан новый сертификат ключа проверки электронной подписи, после чего отправлен в форме ответа на запрос на узел с ViPNet Registration Point. В программе ViPNet Registration Point полученный сертификат появится в разделе **Сертификаты**, а запросу на данный сертификат будет присвоен статус **Удовлетворен**. Если сертификат был получен, но по каким-то причинам не отобразился в программе в разделе **Сертификаты**, см. указания раздела Получены не все сертификаты, изданные в УКЦ по запросам (на стр. 182).

Если в настройках программы установлена опция автоматического переноса сертификата в папку, изданный сертификат будет автоматически экспортирован в нужную папку. По умолчанию папка экспорта: `C:\Program Files\InfoTeCS\ViPNet Registration Point\PKCS10\Export`. В противном случае при необходимости выполните экспорт сертификата в папку вручную (см. «Экспорт сертификата» на стр. 113).

Настройка параметров обработки запросов от внешних пользователей

Для настройки параметров обработки запросов на сертификаты от внешних пользователей (см. «Внешний пользователь» на стр. 201) выполните следующие действия:

1. В окне программы ViPNet Registration Point в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.
2. В появившемся окне на панели навигации выберите раздел **Входящие запросы**.

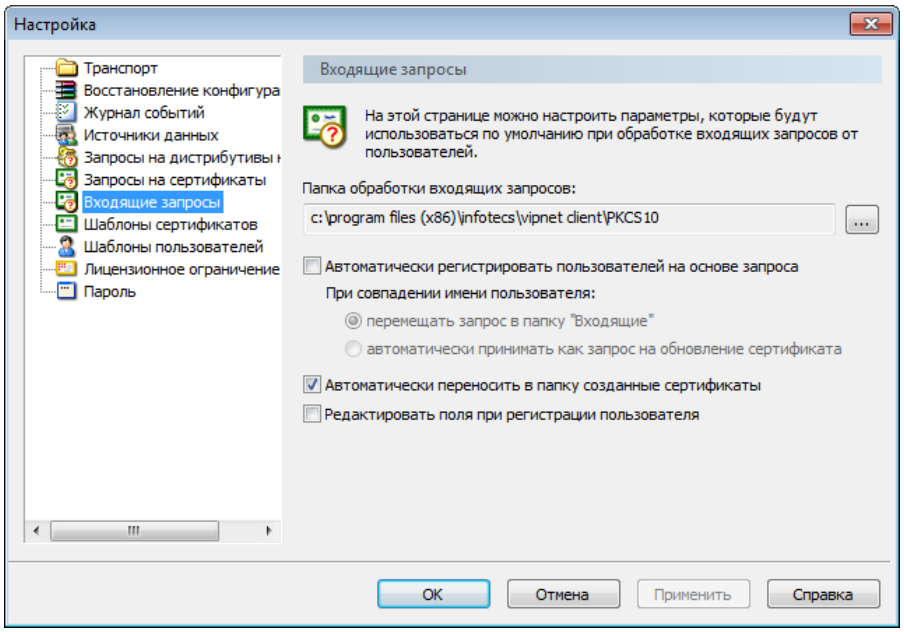


Рисунок 49. Настройка параметров обработки внешних запросов

3 В разделе **Входящие запросы** укажите следующие параметры:

- Чтобы изменить папку обработки входящих запросов на сертификаты, нажмите кнопку ... и в появившемся окне укажите папку импорта входящих запросов (по умолчанию: `C:\Program Files\InfoTeCS\ViPNet Registration Point\PKCS10`).

Совет. Не рекомендуется изменять папку обработки входящих запросов на сертификаты.

- Чтобы переносить сертификаты, изданные в УКЦ по запросам от внешних пользователей, в папку экспорта (по умолчанию: `C:\Program Files\InfoTeCS\ViPNet Registration Point\PKCS10\Export`), установите флажок **Автоматически переносить в папку созданные сертификаты**.
- Для редактирования информации о пользователе при его регистрации в ходе обработки поступившего запроса установите флажок **Редактировать поля при регистрации пользователя**.

Внимание! Флажок Автоматически регистрировать пользователей на основе запросов и параметры под ним по требованиям безопасности настраивать запрещено. Все поступающие запросы должны обрабатываться вручную администратором.

---

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

Просмотр запроса на сертификат

Вы можете посмотреть подробную информацию о любом созданном или обработанном запросе на сертификат (см. «Запрос на сертификат» на стр. 201). Для этого в окне программы в разделе **Запросы** > **Запросы на сертификаты** дважды щелкните нужный запрос.

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

- **Общие** — основная информация о запросе:
  - для запросов, сформированных в программах ViPNet Client и ViPNet Registration Point — номер запроса; имя администратора, заверившего запрос; имя владельца ключа электронной подписи; желательный срок действия сертификата; статус запроса и электронной подписи;
  -

> **Примечание.** ViPNet Client, имеющий сертификат соответствия требованиям к электронной подписи, может являться клиентом центра регистрации.

  - для запросов, сформированных в СКЗИ ViPNet CSP — имя файла запроса; назначение сертификата; имя пользователя, для которого запрошен сертификат; идентификатор ключа 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 о подписи, заверившей запрос, и контрольной сумме запроса. На вкладке также с помощью кнопки **Просмотр сертификата** можно просмотреть сведения о сертификате, которым был подписан запрос.

> **Примечание.** В зависимости от того, где был сформирован запрос на сертификат (в программе ViPNet Client, в программе ViPNet Registration Point или в ViPNet CSP), набор вкладок может быть различным.На рисунке ниже набор вкладок в окне просмотра параметров запроса применим для запроса, сформированного в программе ViPNet Client или ViPNet Registration Point.

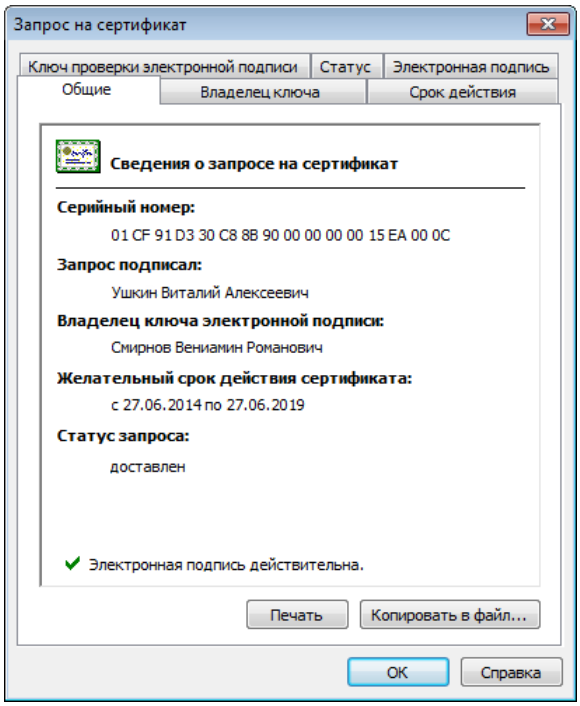


Рисунок 50. Просмотр общей информации о запросе

Приостановление действия сертификата

Приостановление действия сертификата ключа проверки электронной подписи (см. «Приостановление действия сертификата» на стр. 203) может выполняться по требованию его владельца или по решению администратора УКЦ в случае утраты доверия к сертификату, например, при наличии оснований полагать, что тайна ключа электронной подписи нарушена.

Чтобы приостановить действие сертификата пользователя, выполните следующие действия:

1. В окне программы ViPNet Registration Point в разделе **Сертификаты** выберите сертификат, действие которого требуется приостановить.
2. Щелкните сертификат правой кнопкой мыши и в контекстном меню выберите **Приостановить**.
3. Для подтверждения приостановки действия сертификата в появившемся окне с сообщением нажмите кнопку **Да**.

При подтверждении приостановления действия сертификата будет автоматически сформирован запрос, подписанный текущим сертификатом администратора ViPNet Registration Point, и с помощью модуля ViPNet MFTP отправлен в программу ViPNet Удостоверяющий и ключевой центр (см. раздел Запуск транспортного модуля (на стр. 20)).

Запрос появится в разделе **Запросы** > **Запросы на аннулирование сертификатов**. При удовлетворении запроса сертификату будет присвоен статус **Приостановлен**. Сертификат попадет в список аннулированных сертификатов (CRL) администратора УКЦ (его издателя). Данный CRL поступит в программу ViPNet Registration Point из УКЦ вместе с ответом на запрос о приостановлении действия сертификата и появится в разделе **Списки аннулированных сертификатов**. При необходимости вы можете найти там этот список и просмотреть (см. «Просмотр списков аннулированных сертификатов» на стр. 125).

В дальнейшем действие приостановленного сертификата можно возобновить (см. «Возобновление действия сертификата» на стр. 110).

Возобновление действия сертификата

Если действие сертификата по какой-либо причине было приостановлено (см. «Приостановление действия сертификата» на стр. 109), то его можно возобновить.

Чтобы возобновить действие приостановленного сертификата пользователя, выполните следующие действия:

1. В окне программы ViPNet Registration Point в разделе **Сертификаты** выберите сертификат, действие которого требуется возобновить.
2. Щелкните сертификат правой кнопкой мыши и в контекстном меню выберите **Возобновить**.
3. Для подтверждения возобновления действия сертификата в появившемся окне с сообщением нажмите кнопку **Да**.

При подтверждении восстановления действия сертификата автоматически будет сформирован запрос, подписанный текущим сертификатом администратора ViPNet Registration Point, и с помощью модуля ViPNet MFTP отправлен в программу ViPNet Удостоверяющий и ключевой центр (см. раздел Запуск транспортного модуля (на стр. 20)).

Данный запрос появится в разделе **Запросы** > **Запросы на аннулирование сертификатов**. При удовлетворении запроса сертификату будет присвоен статус **Действителен**. Сертификат будет удален из списка аннулированных сертификатов администратора УКЦ (его издателя). Обновленный CRL поступит в программу ViPNet Registration Point из УКЦ вместе с ответом на запрос о возобновлении действия сертификата и появится в разделе **Списки аннулированных сертификатов**. При необходимости вы можете найти там этот список и просмотреть (см. «Просмотр списков аннулированных сертификатов» на стр. 125).

Аннулирование сертификата

Аннулирование сертификата ключа проверки электронной подписи пользователя означает признание сертификата недействительным до истечения срока его действия (см. Аннулирование сертификата (на стр. 201)). Необходимость в аннулировании сертификата может возникнуть по разным причинам:

- смена места работы владельца сертификата;
- утрата пользователем устройства с контейнером ключей;
- издание нового сертификата с другими параметрами вместо действующего сертификата и так далее.

Для аннулирования сертификата пользователя выполните следующие действия:

1. В окне программы ViPNet Registration Point в разделе **Сертификаты** выберите сертификат, который требуется аннулировать.
2. Щелкните сертификат правой кнопкой мыши и в контекстном меню выберите пункт **Аннулировать**.
3. В появившемся окне укажите причину аннулирования сертификата, выбрав в списке:
   - **Прекращение действия** — если сертификат пользователя не предполагает дальнейшего использования.
   - **Компрометация** — если произошла компрометация ключей пользователя (например, вследствие утери им контейнера ключей).
   - **Изменение подчиненности** — при изменении удостоверяющего центра.
   - **Устаревание информации** — если данные, указанные в сертификате пользователя, стали неактуальными.

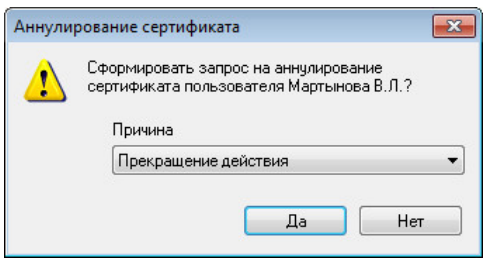


Рисунок 51. Создание запроса на аннулирование сертификата пользователя

Нажмите кнопку **Да** для подтверждения аннулирования сертификата.

При подтверждении аннулирования сертификата будет автоматически сформирован запрос, подписанный текущим сертификатом администратора ViPNet Registration Point, и с помощью модуля ViPNet MFTP отправлен в программу ViPNet Удостоверяющий и ключевой центр ViPNet (см. раздел Запуск транспортного модуля (на стр. 20)).

Запрос появится в разделе **Запросы** > **Запросы на аннулирование сертификатов** с указанной причиной аннулирования. При удовлетворении запроса сертификат попадет в список

аннулированных сертификатов администратора УКЦ (издателя сертификата) и будет иметь статус **Аннулирован**. Данный CRL поступит в программу ViPNet Registration Point из УКЦ вместе с ответом на запрос об аннулировании сертификата и появится в разделе **Списки аннулированных сертификатов**. При необходимости вы можете найти там этот список и просмотреть (см. «Просмотр списков аннулированных сертификатов» на стр. 125). С момента получения остальными пользователями обновленного CRL аннулированный сертификат станет недействительным.

Экспорт сертификата

В программе ViPNet Registration Point вы можете экспортировать полученные из программы ViPNet Удостоверяющий и ключевой центр сертификаты пользователей в различные форматы. Выбор формата экспорта зависит от целей, для которых проводится данный экспорт.

Экспорт сертификата может понадобиться для выполнения следующих задач:

- архивирование сертификата;
- копирование сертификата для использования на другом компьютере;
- отправка сертификата другому пользователю для организации обмена зашифрованными сообщениями;
- просмотр сертификата в удобной форме.

Для экспорта сертификата пользователя выполните следующие действия:

1 В окне программы ViPNet Registration Point в разделе **Сертификаты** выберите сертификат для экспорта.

2 Щелкните сертификат правой кнопкой мыши и в контекстном меню выберите **Экспорт** либо в окне свойств сертификата на вкладке **Состав** нажмите кнопку **Копировать в файл**. Следуйте указаниям мастера экспорта сертификатов.

3 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**.

---

4 На странице **Формат экспортируемого файла** выберите один из предлагаемых форматов (см. «Форматы экспорта сертификатов» на стр. 114), после чего нажмите кнопку **Далее**.

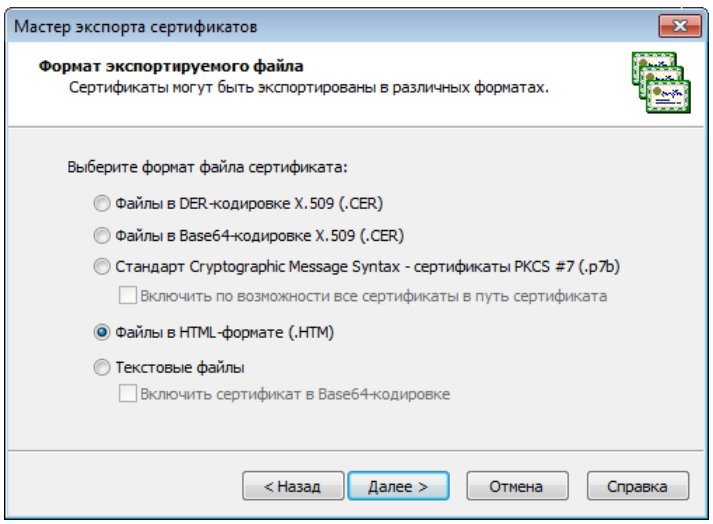


Рисунок 52. Выбор формата файла

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

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

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

Ниже 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 странице PKCS #7 веб-узла RSA Labs http://www.rsa.com/rsalabs/node.asp?id=2129.

- **Файлы в DER-кодировке X.509**

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

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

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

- **Файлы в Base64-кодировке X.509**

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

  MIME (Multipurpose Internet Mail Extensions, 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) http://www.ietf.org/rfc/rfc2633.txt?number=2633.

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

Добавление сертификата в контейнер ключей

Чтобы пользователь мог использовать изданный сертификат и соответствующий ключ электронной подписи, сертификат нужно добавить в контейнер ключей (на стр. 202), который был создан при формировании запроса на сертификат (см. «Создание запроса на новый сертификат» на стр. 93). Это требуется в том случае, если сертификат был получен из программы ViPNet Удостоверяющий и ключевой центр не сразу после отправки запроса на его издание.

Чтобы вручную добавить сертификат пользователя в контейнер ключей, выполните следующие действия:

1. В окне программы ViPNet Registration Point в разделе **Сертификаты** выберите сертификат, который требуется добавить.
2. Щелкните сертификат правой кнопкой мыши и в контекстном меню выберите **Сохранить в контейнер**.

   Будет произведена проверка доступа к контейнеру ключей. При наличии доступа сертификат будет автоматически добавлен в контейнер ключей. При отсутствии доступа к контейнеру ключей, если требуется, укажите место и пароль к контейнеру, как описано ниже.
3. В появившемся окне **ViPNet CSP - инициализация контейнера ключа** укажите место хранения контейнера ключей:
   - папку на жестком или съемном диске;

     Внимание! На съемном флэш-диске контейнер обязательно должен находиться в папке `Infotecs\Containers`.
   - устройство с указанием его параметров и ПИН-кода.

   После этого нажмите кнопку **OK**.

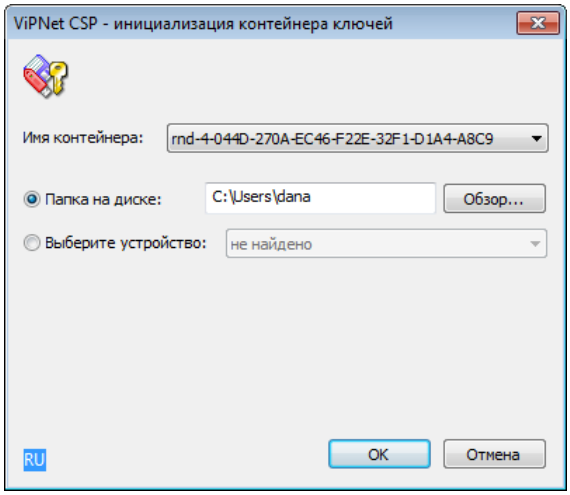


Рисунок 53. Указание места хранения контейнера ключей

4 При появлении окна ввода пароля укажите пароль к выбранному контейнеру, после чего нажмите кнопку **OK**.

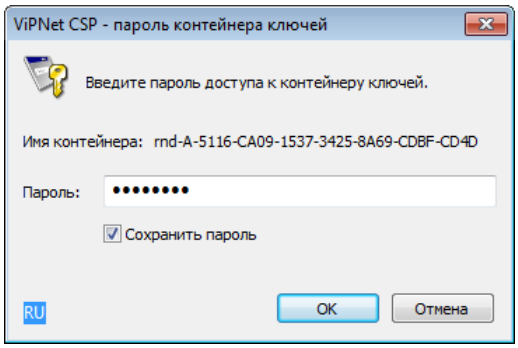


Рисунок 54. Ввод пароля доступа к контейнеру ключей

Если пароль к контейнеру ключей указан верно, и в контейнере найден соответствующий ключ электронной подписи, то сертификат будет успешно добавлен в него.

Создание и редактирование шаблонов сертификатов

При создании запросов на сертификаты используются специальные шаблоны сертификатов (см. «Шаблон сертификата» на стр. 206). В конфигурацию программы ViPNet Registration Point входит несколько стандартных шаблонов сертификатов подписи и шифрования, которые вы можете при необходимости изменить. Параметры этих шаблонов и всех новых, которые будут созданы впоследствии, сохраняются в файле `cert_tem.ini` в папке установки программы ViPNet Registration Point.

Также шаблоны сертификатов могут поступать из программы ViPNet Удостоверяющий и ключевой центр в составе обновлений ключей узлов. Эти шаблоны сертификатов не могут быть изменены, и они не отображаются в настройках программы. Их можно просмотреть только при создании запроса на сертификат (см. раздел Создание запроса на новый сертификат (на стр. 93)).

Примечание. Если требуется, чтобы в списке стандартных шаблонов сертификатов в настройках ViPNet Registration Point присутствовали шаблоны сертификатов подписи и шифрования с алгоритмом ГОСТ Р 34.11-2012/512, то запросите у администратора УКЦ обновление ключей узлов или списков аннулированных сертификатов, в составе которых на узел с ViPNet Registration Point поступят указанные шаблоны сертификатов.

Шаблоны, созданные в программе ViPNet Registration Point, могут быть использованы также при создании запросов на сертификаты с помощью программы ViPNet CSP. О том, как перенести шаблоны в данную программу, см. раздел Перенос шаблонов сертификатов в программу ViPNet CSP (на стр. 176).

При необходимости вы можете создать другие шаблоны сертификатов или отредактировать существующие. Для создания нового шаблона сертификата выполните следующие действия:

1. В окне программы ViPNet Registration Point в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка** на панели инструментов.
2. В окне **Настройка** на панели навигации выберите раздел **Шаблоны сертификатов**.

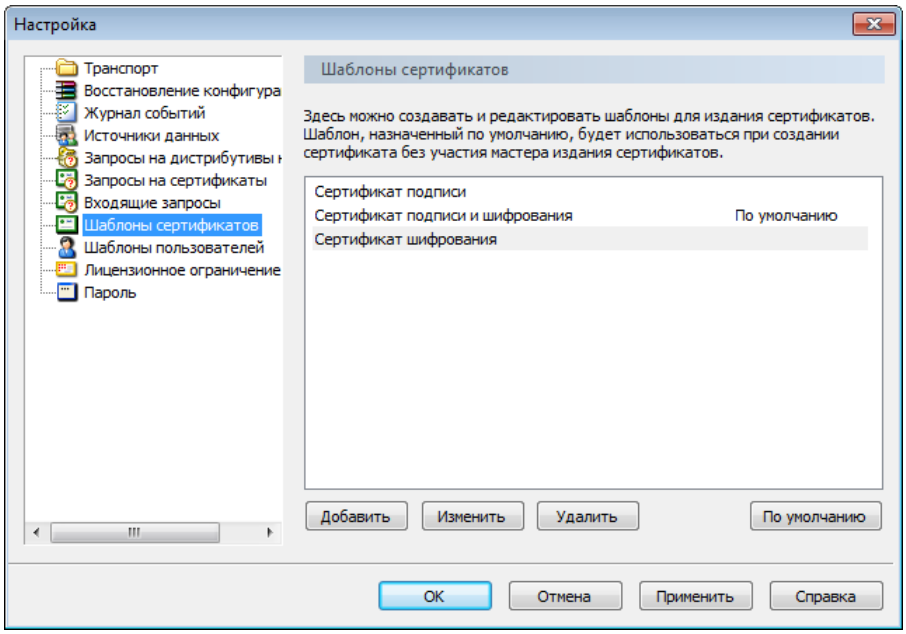


Рисунок 55. Управление шаблонами сертификатов

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 в соответствии с приведенной ниже таблицей. 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.

Внимание! По требованиям ФСБ России с 1 января 2019 года использование алгоритма ГОСТ Р 34.10-2001 будет недопустимо. В связи с этим уже сейчас рекомендуется выдавать сертификаты по новому алгоритму ГОСТ Р 34.10-2012.

Таблица 5. Характеристика криптопровайдеров и алгоритмов подписи

Криптопровайдер и соответствующий ему алгоритм электронной подписи	Параметры алгоритма электронной подписи	Длина ключа проверки электронной подписи
Infotecs Cryptographic Service Provider ГОСТ Р 34.10-2001	ГОСТ Р 34.10 - 2001. Параметры по умолчанию OID «1.2.643.2.2. 35.1»	512 бит

Криптопровайдер и соответствующий ему алгоритм электронной подписи	Параметры алгоритма электронной подписи	Длина ключа проверки электронной подписи
См. RFC 4357 http://www.ietf.org/rfc/rfc4357.txt Стандарт электронной подписи, основанный на арифметике эллиптических кривых OID «1.2.643.2.2.19»	ГОСТ Р 34.10 - 2001 Параметры подписи B OID «1.2.643.2.2. 35.2» ГОСТ Р 34.10 - 2001. Параметры подписи C OID «1.2.643.2.2. 35.3»	
Infotecs GOST 2012/512 Cryptographic Service Provider ГОСТ Р 34.10-2012/512 Новый стандарт электронной подписи от 2012 года с длиной ключа электронной подписи 256 бит OID «1.2.643.7.1.1.1.1»	ГОСТ Р 34.10 - 2001. Параметры по умолчанию OID «1.2.643.2.2. 35.1» ГОСТ Р 34.10 - 2001 Параметры подписи B OID «1.2.643.2.2. 35.2» ГОСТ Р 34.10 - 2001. Параметры подписи C OID «1.2.643.2.2. 35.3»	512 бит
Infotecs GOST 2012/1024 Cryptographic Service Provider ГОСТ Р 34.10-2012/1024 Новый стандарт электронной подписи от 2012 года с длиной ключа электронной подписи 512 бит OID «1.2.643.7.1.1.1.2»	ГОСТ Р 34.10 - 2012/1024. Набор параметров A ГОСТ Р 34.10 - 2012/1024. Набор параметров B	1024 бит

После этого нажмите кнопку **Далее**.

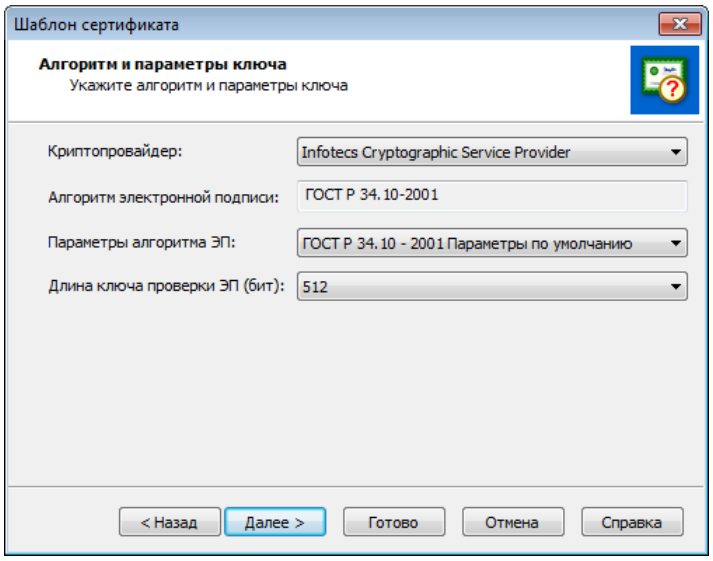


Рисунок 56. Выбор алгоритма и настройка параметров ключа

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

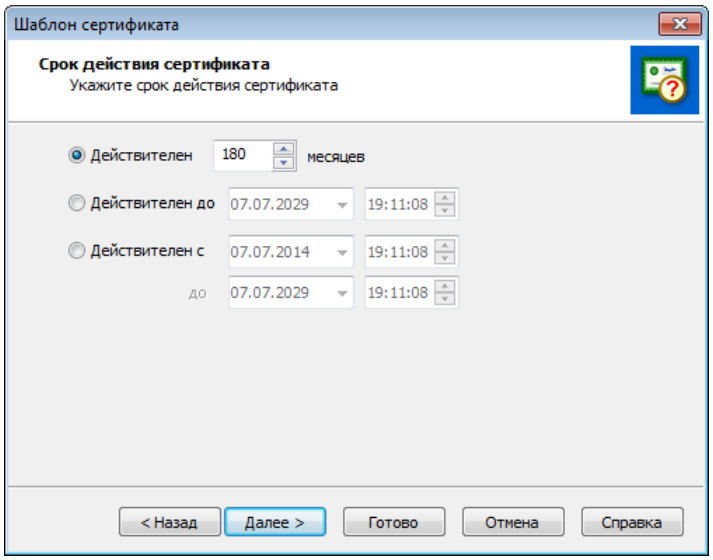


Рисунок 57. Указание срока действия сертификата

Примечание. При задании срока действия сертификата автоматически определяется срок действия ключа электронной подписи. Если срок действия сертификата задается меньше или равным 12 месяцам (1 году), то срок действия ключа электронной подписи будет равен заданному сроку действия сертификата. Если заданный срок действия сертификата больше 1 года, то срок действия ключа электронной подписи не будет превышать 15 месяцев (1 год и 3 месяца). Максимальный срок действия сертификата пользователя составляет 5 лет.

---

7 На странице **Назначения сертификата** укажите необходимые расширения, которые будут добавлены в новый шаблон.

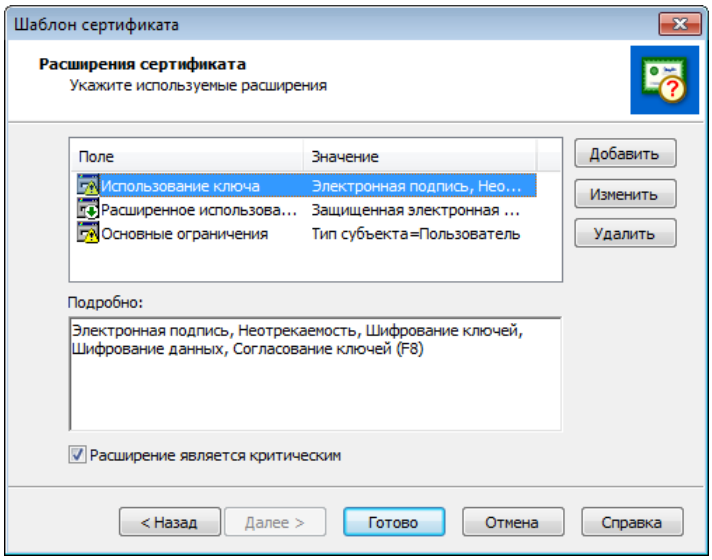


Рисунок 58. Формирование назначений сертификата

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

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

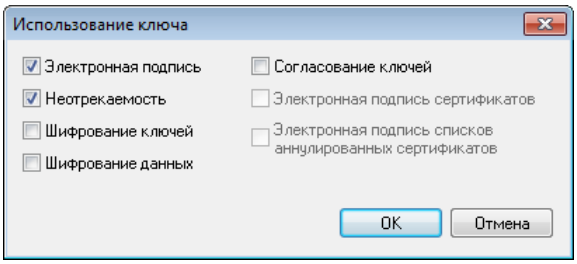


Рисунок 59. Настройка параметров использования ключа

Примечание. Если в качестве назначения ключа и сертификата вы укажете шифрование, то параметры алгоритма подписи, заданного на предыдущем шаге, будут автоматически изменены на следующие: ГОСТ 34.10-2001. EDH Параметры по умолчанию (OID «1.2.643.2.2.36.0»).

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

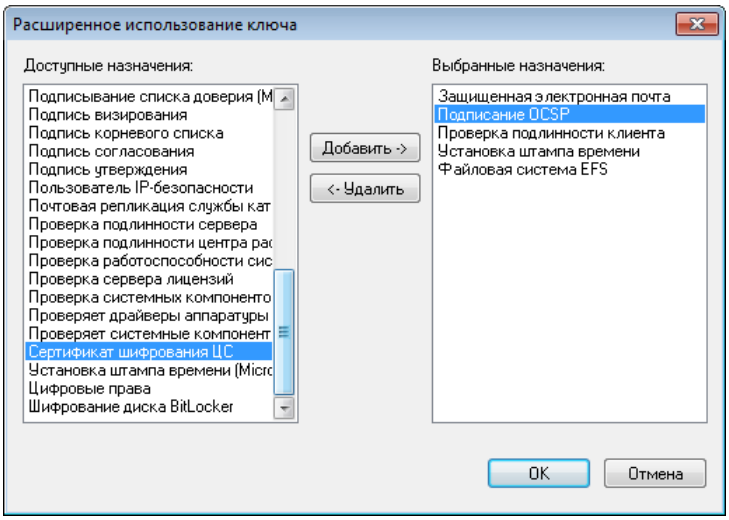


Рисунок 60. Выбор назначений расширенного использования ключа

- **Политики сертификата**. В появившемся окне с помощью кнопок **Добавить** и **Удалить** выберите политики применения сертификата и нажмите кнопку **OK**.

Примечание. Список политик применения сертификатов формируется на основе информации, поступающей из УКЦ в составе списков аннулированных сертификатов (см. «Список аннулированных сертификатов (CRL)» на стр. 205).

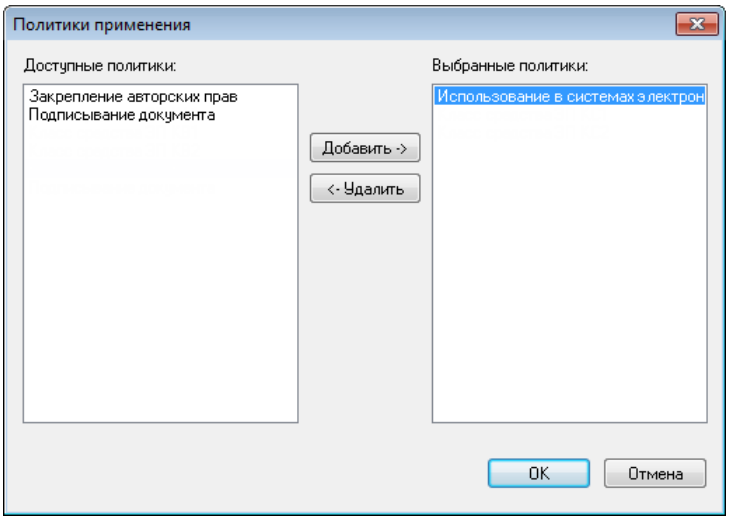


Рисунок 61. Добавление политики применения сертификата

- **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**.

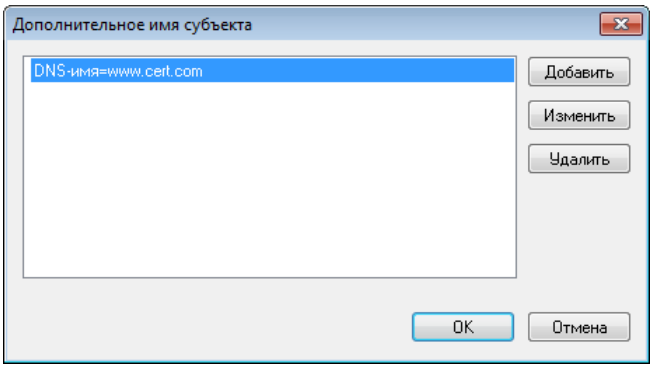


Рисунок 62. Задание альтернативного имени владельца сертификата ключа проверки электронной подписи

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 **Применить**.

Чтобы изменить параметры шаблона сертификата, выберите его в списке и нажмите кнопку **Изменить**, затем на страницах мастера внесите необходимые коррективы (см. выше) и нажмите кнопку **ОК**.

Чтобы удалить ненужный шаблон, выберите его в списке и нажмите кнопку **Удалить**. Чтобы при создании запроса на сертификат использовался нужный шаблон по умолчанию, выберите его в списке и нажмите кнопку **По умолчанию**.

Просмотр списков аннулированных сертификатов

В программе ViPNet Registration Point вы можете просмотреть списки аннулированных сертификатов (см. «Список аннулированных сертификатов (CRL)» на стр. 205), которые поступили из программы ViPNet Удостоверяющий и ключевой центр. Данные списки поступают каждый раз вместе с ответами на запросы об аннулировании, приостановлении или возобновлении действия сертификатов, а также с определенной периодичностью, если узел с ViPNet Registration Point присутствует в списке получателей CRL в УКЦ.

Чтобы просмотреть списки аннулированных сертификатов, выполните следующие действия:

1. В окне программы в разделе **Списки аннулированных сертификатов** дважды щелкните список, который вы хотите просмотреть, или в его контекстном меню выберите пункт **Свойства**.
2. 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**.

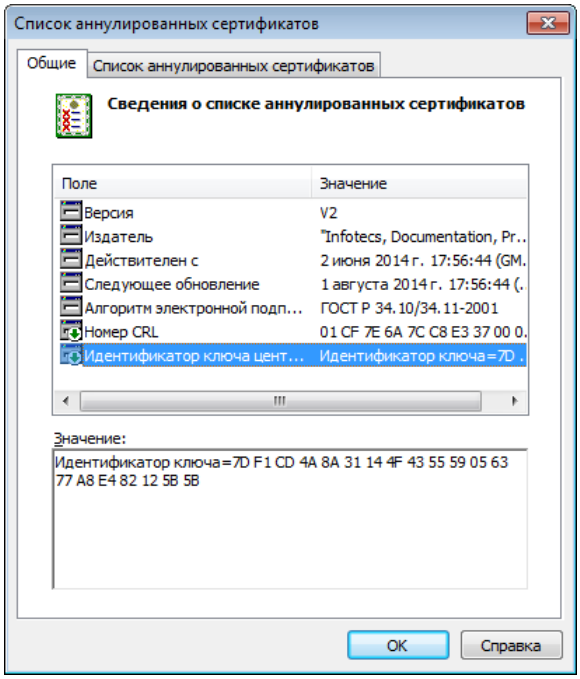


Рисунок 63. Просмотр общей информации о списке аннулированных сертификатов

Просмотр свойств контейнера ключей

В процессе работы с программой ViPNet Registration Point вам может потребоваться просмотреть свойства контейнера ключей, созданного в программе либо пользователем. В процессе просмотра свойств контейнера ключей вы можете узнать, присутствует ли в контейнере ключей сертификат, и при необходимости проверить действительность сертификата.

Чтобы просмотреть свойства контейнера ключей, выполните следующие действия:

1. В окне программы ViPNet Registration Point в меню **Сервис** выберите пункт **Контейнер ключей**.
2. В окне **ViPNet CSP - инициализация контейнера ключа** укажите место хранения контейнера ключей:
   - папку на жестком или съемном диске;

     Внимание! На съемном флэш-диске контейнер обязательно должен находиться в папке `Infotecs\Containers`.

   - устройство с указанием его параметров и ПИН-кода.

   После этого нажмите кнопку **OK**.

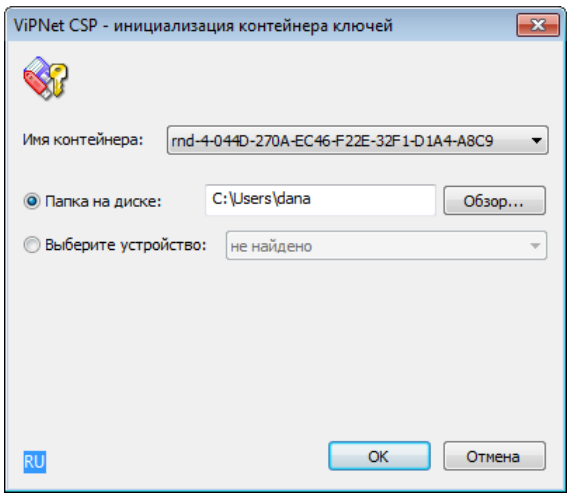


Рисунок 64. Указание места хранения контейнера ключей

3. В появившемся окне ознакомьтесь с параметрами указанного контейнера: для кого создавался контейнер, содержит ли он в себе сертификат. Параметры сертификата при его наличии вы можете просмотреть с помощью кнопки **Сертификат**.

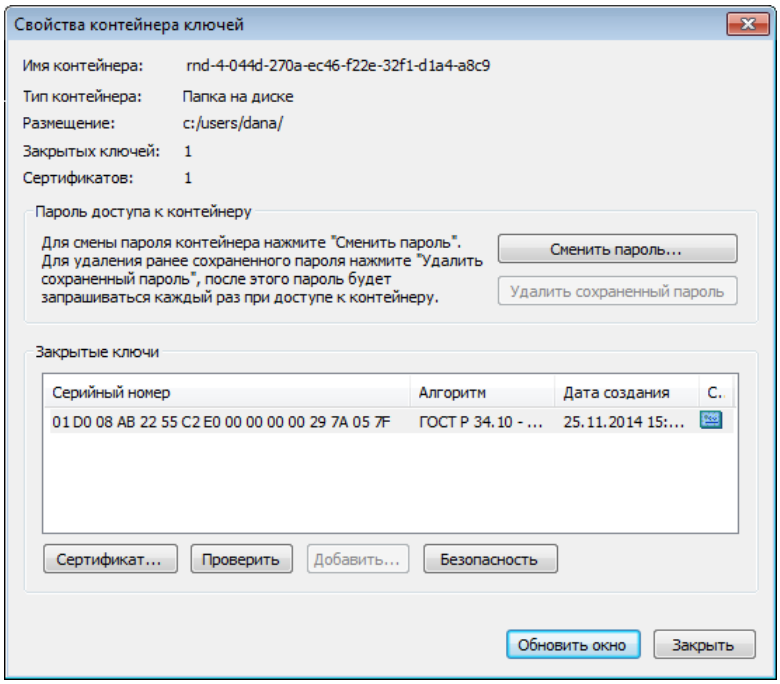


Рисунок 65. Просмотр свойств контейнера ключей

4 Если вам известен пароль к контейнеру, то в окне свойств контейнера вы можете:

- проверить действительность сертификата, находящегося в контейнере с помощью кнопки **Проверить**;
- сменить пароль к контейнеру с помощью кнопки **Сменить пароль**.

8

Работа с дистрибутивами ключей

Создание запроса на дистрибутив ключей

В программе ViPNet Registration Point для любого зарегистрированного пользователя можно создать запрос на получение дистрибутива ключей (см. «Дистрибутив ключей» на стр. 201). Запрос на дистрибутив ключей вы можете создать сразу по окончании регистрации пользователя вручную (см. «Регистрация вручную» на стр. 66) либо в любой момент в процессе работы с программой. При необходимости вы можете сформировать запросы на дистрибутивы ключей сразу для группы пользователей.

Внимание! Если число запросов на дистрибутивы ключей достигло числа, указанного в лицензии, создание запроса на дистрибутив ключей пользователя будет невозможно (см. раздел Лицензионные ограничения (на стр. 19)).

Если у вас отсутствует ключ электронной подписи и сертификат проверки электронной подписи либо они стали недействительными, то дистрибутивы ключей пользователей, полученные по запросам из программы ViPNet Удостоверяющий и ключевой центр, не будут содержать ключа электронной подписи и сертификата. В этом случае для получения дистрибутивов ключей с ключом электронной подписи и сертификатом вам требуется запросить у администратора УКЦ для себя ключ и сертификат или обновить текущий сертификат (см. «Процедура обновления ключа электронной подписи и сертификата» на стр. 145).

Чтобы создать запрос на дистрибутив ключей пользователя, выполните следующие действия:

1. В окне программы ViPNet Registration Point в разделе **Пользователи** выберите одного или несколько пользователей.
2. Выполните одно из действий:
   - В контекстном меню для данного пользователя выберите пункт **Дистрибутивы ключей** > **Создать запрос**.
   - В меню **Действие** выберите пункт **Дистрибутивы ключей**, затем щелкните **Создать запрос**.
   - На панели инструментов нажмите кнопку **Создать запрос на дистрибутив ключей**  .

   Если для выбранного пользователя запрос на дистрибутив ключей ранее не создавался, то будет запущен мастер создания запроса на дистрибутив. Далее следуйте указаниям мастера (см. «Формирование запроса на дистрибутив ключей с помощью мастера» на стр. 132).

Если для выбранного пользователя ранее был создан дистрибутив ключей, то будет запущен мастер, позволяющий создать запрос на обновление дистрибутива (см. «Создание запроса на обновление дистрибутива ключей» на стр. 131).

Если для выбранного пользователя был создан запрос на дистрибутив или обновление дистрибутива ключей, который еще не был удовлетворен, появится сообщение с предложением

повторно отправить созданный запрос или создать новый. В данном окне следует выбрать необходимое действие.

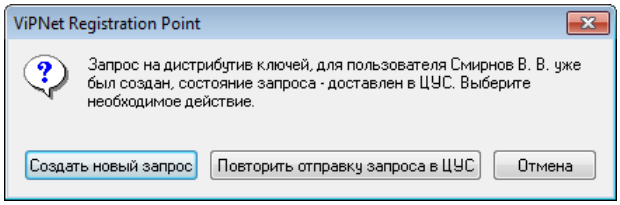


Рисунок 66. Сообщение с предложением повторной отправки запроса или создания нового

Если было выбрано несколько пользователей, для каждого из них по очереди будет запущен мастер создания запроса на дистрибутив или выполнено другое действие.

Внимание! В зависимости от настроек программы мастер создания запроса может не запускаться (см. раздел Настройка параметров создания запросов на дистрибутивы (на стр. 139)). Запрос на дистрибутив в этом случае будет создан согласно параметрам, указанным по умолчанию.

Создание запроса на обновление дистрибутива ключей

Если по каким-либо причинам произошло изменение учетных данных пользователя, которому ранее был выдан дистрибутив ключей, то в этом случае следует сформировать запрос на обновление данного дистрибутива.

Чтобы создать запрос на обновление дистрибутива ключей:

1. В окне программы ViPNet Registration Point в разделе **Пользователи** выберите пользователя, для которого требуется обновить дистрибутив, и выполните одно из действий:
   - В контекстном меню для данного пользователя выберите пункт **Дистрибутивы ключей** > **Создать запрос**.
   - В меню **Действие** выберите пункт **Дистрибутивы ключей**, затем щелкните **Создать запрос**.
   - На панели инструментов нажмите кнопку **Создать запрос на дистрибутив ключей**  .
2. Следуйте указаниям мастера создания запроса на дистрибутив (см. «Формирование запроса на дистрибутив ключей с помощью мастера» на стр. 132).

Примечание. Запросы на обновление дистрибутивов ключей можно сформировать одновременно для группы пользователей. Если было выбрано несколько пользователей, для каждого из них по очереди будет запущен указанный мастер.

В результате созданный запрос на обновление дистрибутива ключей появится в разделе **Запросы** > **Запросы на дистрибутивы ключей** со значком  . Аналогично запросу на создание дистрибутива он будет передан в программу ViPNet Центр управления сетью, а затем в ViPNet Удостоверяющий и ключевой центр (подробнее см. Создание запроса на дистрибутив ключей (на стр. 130)). При его удовлетворении будет создан новый дистрибутив ключей.

Для использования обновленный дистрибутив ключей следует перенести в папку (см. «Перенос дистрибутива в папку» на стр. 141), при необходимости его можно распаковать (см. «Распаковка дистрибутива ключей» на стр. 143).

Формирование запроса на дистрибутив ключей с помощью мастера

При создании запроса на дистрибутив ключей с помощью мастера вы можете указать сетевой узел, на котором следует зарегистрировать пользователя, и параметры этого узла.

При создании запроса на дистрибутив ключей выполнение некоторых действий и появление соответствующих страниц мастера зависит от параметров, заданных в окне настройки программы ViPNet Registration Point в разделе **Запросы на дистрибутив ключей** (см. «Настройка параметров создания запросов на дистрибутивы» на стр. 139):

- Чтобы при создании запроса задать пароль пользователя, установите флажок **Создавать пароль пользователя в мастере создания запросов на дистрибутив ключей**.

  Чтобы настроить тип создаваемого пароля и параметры случайных паролей, также выполните настройку параметров создаваемых паролей (см. «Настройка параметров паролей пользователей» на стр. 90).

- Чтобы при создании запроса задать способ аутентификации пользователя на сетевом узле, установите флажок **Выбирать способ аутентификации пользователя в мастере создания запросов на дистрибутивы ключей**.

Чтобы сформировать запрос на дистрибутив ключей с помощью мастера, выполните следующие действия:

1. На первой странице мастера нажмите кнопку **Далее**.
2. На странице **Параметры сетевого узла пользователя** выполните следующие действия:
   - Чтобы зарегистрировать пользователя на новом сетевом узле:
     - Установите переключатель в положение **Создать новый сетевой узел для пользователя**.
     - В списке **Создать сетевой узел за координатором** выберите координатор, который будет являться для нового узла сервером-маршрутизатором (см. «Сервер-маршрутизатор» на стр. 204). По умолчанию выбран координатор, указанный в настройках программы.

- В поле **Имя сетевого узла** укажите название нового узла. По умолчанию задано имя пользователя.

Внимание! Имя сетевого узла не должно включать следующие символы: * ? : & \ | / < > «».

Если в имени узла будут содержаться недопустимые символы, то при переходе на следующую страницу мастера появится предупреждение с предложением их исправить.

- Чтобы зарегистрировать пользователя на сетевом узле, который был создан ранее, установите переключатель в положение **Зарегистрировать пользователя на существующем сетевом узле** и в списке выберите нужный сетевой узел.

Примечание. Вы можете выбрать для регистрации пользователя только те сетевые узлы, которые были созданы по запросу на дистрибутив ключей, отправленному из программы ViPNet Registration Point.

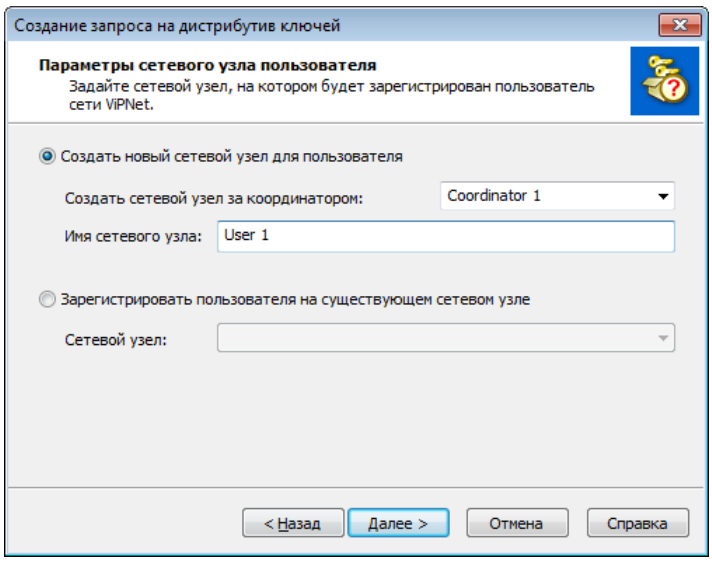


Рисунок 67. Выбор узла, на котором будет зарегистрирован пользователь

Указав все необходимые параметры, нажмите кнопку **Далее**.

3 На следующей странице мастера задайте связи узла пользователя с другими узлами сети.

- Чтобы связать узел пользователя со всеми возможными узлами сети ViPNet, в списке выберите пункт **Со всеми сетевыми узлами**.
- Чтобы связать узел пользователя с определенными узлами сети, в списке выберите пункт **Согласно списку** и с помощью кнопок **Добавить связь** и **Удалить связь** сформируйте список узлов для связи.

Примечание. В запросе на дистрибутив ключей вы не можете задать связи сетевого узла пользователя с узлами, с которыми не связан узел с ПО ViPNet Registration Point.

После этого нажмите кнопку **Далее**.

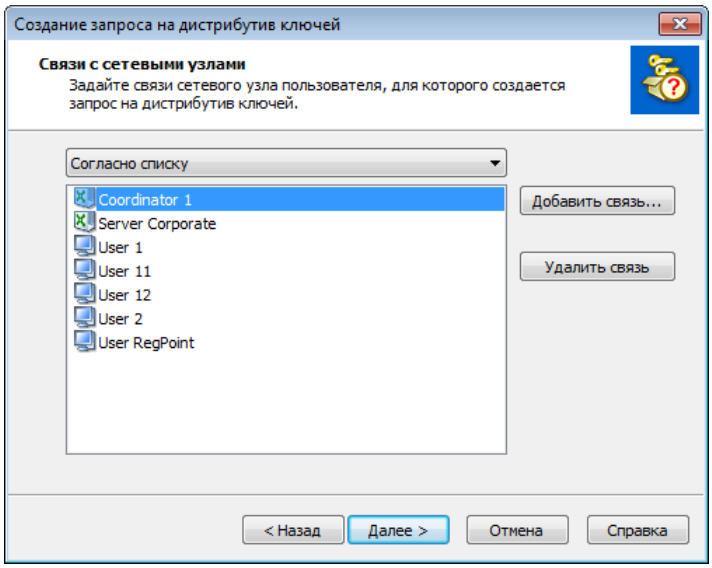


Рисунок 68. Настройка связи узла пользователя с другими узлами сети

4 На странице **Добавить роли на сетевой узел** укажите способ назначения ролей сетевому узлу пользователя.

- Для назначения узлу ролей, указанных по умолчанию в настройках программы ViPNet Центр управления сетью, в списке выберите пункт **В соответствии с настройками ЦУС**. Информацию о настройках программы можно узнать у администратора ЦУСа (см. «Администратор ЦУСа» на стр. 200).
- Чтобы назначить узлу конкретные роли, в списке выберите **Только выбранные роли** с помощью кнопки **Добавить** укажите нужные роли. Список возможных ролей ограничивается лицензией ЦУСа. Максимально широкий список включает роли «Деловая почта», «VPN-клиент», CryptoService и SDK. Удалить ненужную роль можно с помощью кнопки **Удалить**.

После этого нажмите кнопку **Далее**.

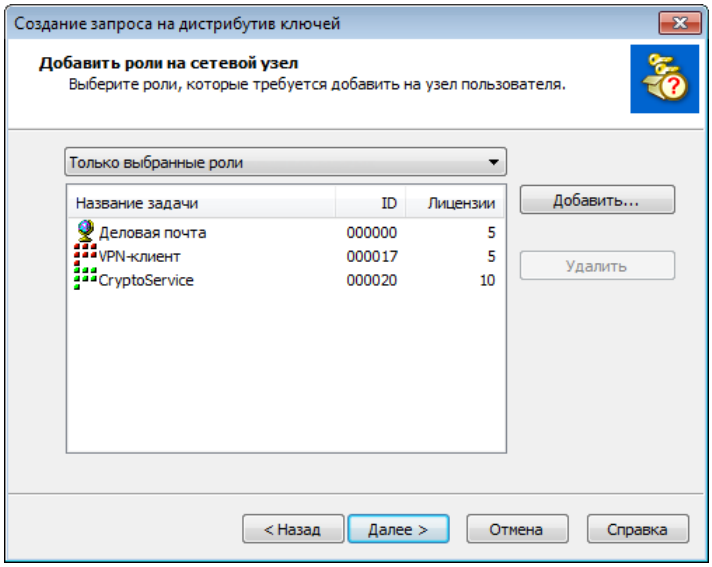


Рисунок 69. Выбор способа назначения ролей сетевому узлу пользователя

5 На странице **Тип пароля пользователя** при необходимости измените тип пароля к дистрибутиву ключей:

- **Собственный пароль** — пароль, задаваемый вами вручную.
- **Случайный пароль на основе парольной фразы** — пароль, формируемый автоматически на основе парольной фразы (см. «Парольная фраза» на стр. 203).
- **Случайный цифровой пароль** — пароль, формируемый автоматически из заданного числа цифр.

Данный пароль станет паролем пользователя. Если для пользователя уже создавался пароль (например, при создании запроса на сертификат), то на странице мастера будет установлен флажок **Использовать текущий пароль пользователя**. Для просмотра текущего пароля нажмите кнопку **Пароль пользователя**. Если вы хотите, чтобы для пользователя был создан новый пароль, снимите указанный флажок и задайте тип пароля.

Нажмите кнопку **Далее**.

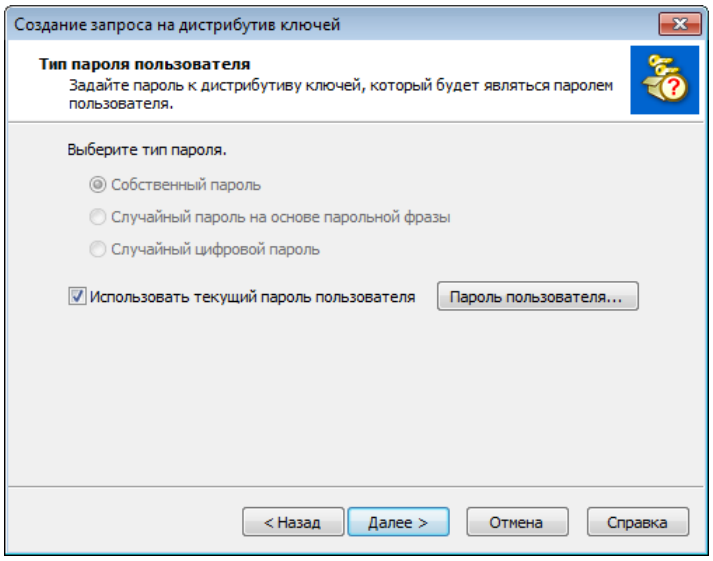


Рисунок 70. Выбор типа пароля к дистрибутиву ключей пользователя

6 Если сохраняется текущий пароль пользователя, появится страница завершения создания запроса на дистрибутив ключей (см. п. 8).

Если должен быть создан новый пароль и был выбран тип **Собственный пароль**, то на появившейся странице задайте пароль и его подтверждение и нажмите кнопку **Далее**.

Если был выбран тип одного из случайных паролей, то появится электронная рулетка, если она еще не запускалась в рамках текущего сеанса работы программы. Поводите указателем в пределах окна **Электронная рулетка**, после чего запомните новый пароль (или парольную фразу) на странице **Пароль пользователя**. При необходимости измените параметры случайного пароля и создайте другой.

Внимание! Длина пароля должна быть не меньше 8 символов и не должна превышать 31 символ. Пароли с длиной более 31 символа не могут использоваться в текущих версиях приложений ViPNet. Данное ограничение связано с существующим алгоритмом передачи пароля в криптопровайдер. В соответствии с этим алгоритмом длина пароля не должна превышать 31 символ.

Нажмите кнопку **Далее**.

7 На странице **Выберите способ аутентификации пользователя** при необходимости измените способ аутентификации. Для этого в соответствующем списке выберите один из пунктов:

- **Пароль.** Для входа в программу будет использоваться пароль, заданный на предыдущем шаге. Этот способ аутентификации установлен по умолчанию.

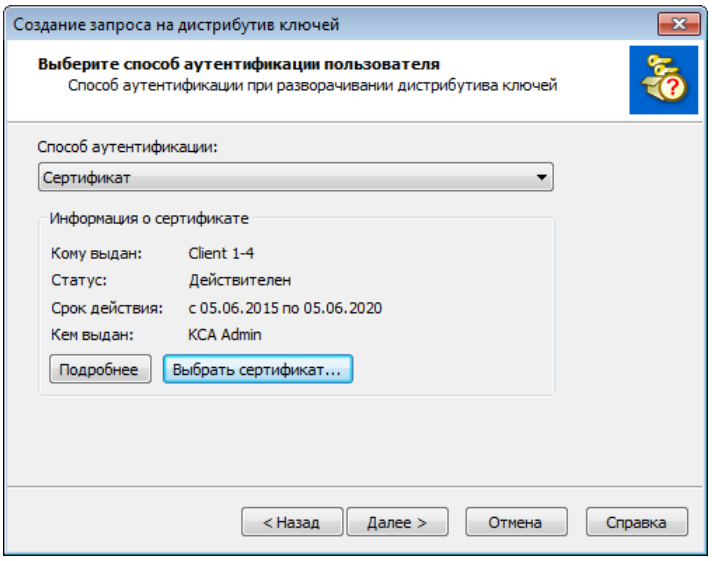


Рисунок 71. Выбор способа аутентификации пользователя

- **Сертификат.** Для входа в программу пользователю требуется контейнер ключей и сертификат ключа проверки электронной подписи. Данный способ аутентификации используется, если у пользователей организации уже имеются сертификаты, изданные сторонним удостоверяющим центром. При настройке данного способа аутентификации администратору ViPNet Registration Point не требуется контейнер ключей электронной подписи пользователя, за счет этого обеспечивается защита ключей от доступа третьих лиц.

  Для аутентификации может использоваться сертификат, изданный своим или сторонним удостоверяющим центром, при этом должны выполняться следующие условия:

  - Сертификат должен быть действительным.
  - Для сертификата в расширении «Использование ключа» должен быть указан параметр «Шифрование ключей», в расширении «Расширенное использование ключа» — параметр «Проверка подлинности клиента».

Выбрав способ аутентификации, нажмите кнопку **Далее**.

8 На последней странице мастера нажмите кнопку **Готово**. Чтобы в дальнейшем не показывать окно мастера создания запросов на дистрибутивы ключей, установите соответствующий флажок. После этого включить опцию запуска мастера можно будет только в настройках программы (см. «Настройка параметров создания запросов на дистрибутивы» на стр. 139).

В результате созданный запрос появится в разделе **Запросы** > **Запросы на дистрибутивы ключей** и с помощью модуля ViPNet MFTP будет отправлен в ЦУС (см. раздел Запуск транспортного модуля (на стр. 20)).

На основе данных, указанных в запросе, произойдет регистрация пользователя в ЦУСе. При удовлетворении запроса в УКЦ будет создан дистрибутив ключей. В этом случае запросу на создание дистрибутива будет присвоен статус **Удовлетворен**, в списке пользователей в столбце **Дистрибутивы** напротив данного пользователя появится значок .

Внимание! В запросе на дистрибутив ключей указывается имя пользователя. При формировании запроса имя пользователя, содержащее запрещенные знаки (* ? : & \ | / < > «»), автоматически изменяется. Вследствие этого возможны ошибки при обработке запроса, поскольку разные имена будут содержать одинаковые знаки.

Для передачи пользователю созданный дистрибутив ключей следует перенести в папку (см. «Перенос дистрибутива в папку» на стр. 141), при необходимости его можно распаковать (см. «Распаковка дистрибутива ключей» на стр. 143).

Настройка параметров создания запросов на дистрибутивы

При необходимости в настройках программы ViPNet Registration Point вы можете запретить появление мастера при создании запросов на дистрибутивы ключей. Это может быть удобно в том случае, если для всех пользователей вы создаете запросы на дистрибутивы ключей с параметрами по умолчанию, заданными в этих же настройках.

Для настройки параметров создания запросов на дистрибутивы ключей выполните следующие действия:

1 В окне программы ViPNet Registration Point в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка** на панели инструментов.

2 В появившемся окне на панели навигации выберите раздел **Запросы на дистрибутивы ключей**.

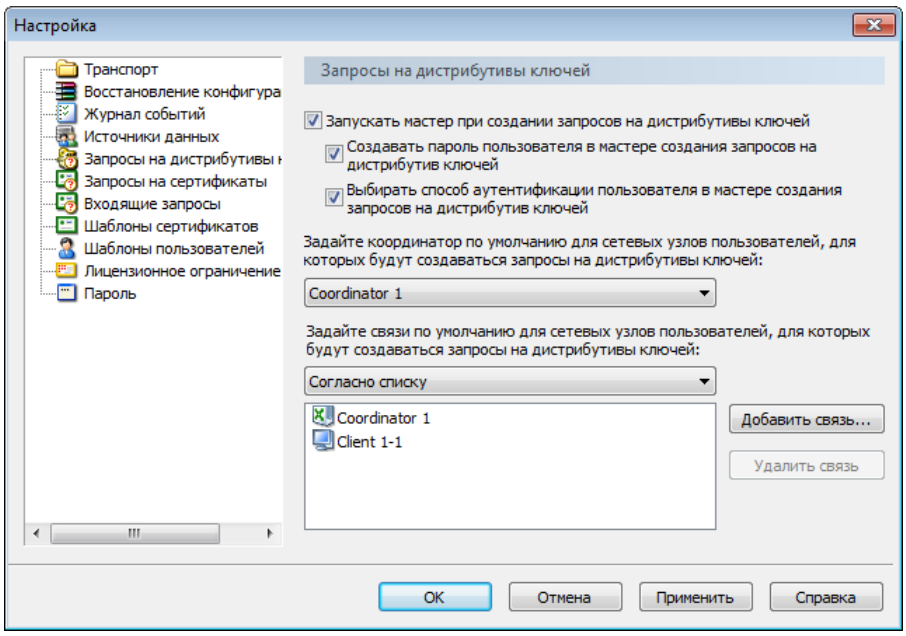


Рисунок 72. Настройка параметров создания запросов на дистрибутивы ключей

3 Чтобы формирование запросов на дистрибутивы ключей осуществлялось без запуска мастера и согласно настройкам, выполненным в этом окне и настройкам, заданным по умолчанию для страниц мастера, снимите флажок **Запускать мастер при создании запросов на дистрибутивы ключей**.

4 Для возможности задать пароль к дистрибутиву ключей (пароль пользователя) в мастере создания запросов на дистрибутивы ключей, в том случае если ранее он не создавался, установите флажок **Создавать пароль пользователя в мастере создания запросов на дистрибутивы ключей**.

5 Для возможности выбора и настройки способа аутентификации пользователя в ПО ViPNet в мастере создания запросов на дистрибутивы ключей установите флажок **Выбирать способ аутентификации пользователя в мастере создания запросов на дистрибутив ключей**.

6 Выберите координатор, который в мастере будет указан по умолчанию в качестве сервера-маршрутизатора для новых узлов пользователей (см. «Сервер-маршрутизатор» на стр. 204).

7 Укажите как по умолчанию задавать связи сетевых узлов пользователей, для которых будут создаваться дистрибутивы ключей:

- Чтобы по умолчанию связывать узлы пользователей со всеми возможными узлами сети ViPNet, в списке выберите пункт **Со всеми сетевыми узлами**.
- Чтобы связывать узлы пользователей с определенными узлами сети, в списке выберите пункт **Согласно списку** и с помощью кнопок **Добавить связь** и **Удалить связь** сформируйте список узлов для связи.

Примечание. С сетевыми узлами, с которыми не связан узел с ViPNet Registration Point, не могут быть связаны и сетевые узлы пользователей, для которых создаются дистрибутивы ключей.

8 Для сохранения настроек нажмите кнопку **Применить**.

Перенос дистрибутива в папку

Для передачи сформированного дистрибутива ключей пользователю ViPNet сначала требуется перенести его в папку на диске. В зависимости от параметров, заданных при переносе дистрибутива ключей, будет задан способ аутентификации пользователя на сетевом узле и место хранения его контейнера ключей и сертификата.

Чтобы перенести дистрибутив ключей в папку, выполните следующие действия:

1. В окне программы ViPNet Registration Point в разделе **Пользователи** выберите пользователя с созданным дистрибутивом ключей и в меню **Действие** либо в контекстном меню выберите **Дистрибутивы ключей**, затем щелкните **Перенести в папку на диске**.
2. В окне **Перенос дистрибутивов ключей** укажите следующие параметры:
   - В списке **Считывание ключей защиты** выберите место, откуда будет считываться ключ защиты (персональный ключ (см. «Персональный ключ пользователя» на стр. 203)) при аутентификации пользователя. Если персональный ключ будет считываться из папки, то у пользователя будет способ аутентификации — «Пароль», если с внешнего устройства — «Устройство».
   - В группе **Папка и внешнее устройство для переноса дистрибутивов ключей** с учетом заданных параметров аутентификации укажите:
     - папку на жестком или съемном диске для сохранения файла дистрибутива ключей;
     - доступное устройство с указанием его параметров и ПИН-кода для переноса ключа защиты.

Примечание. Для использования какого-либо внешнего устройства необходимо подключить и установить драйверы этого устройства. Перечень доступных устройств хранения данных и полезная информация об использовании устройств содержится в документе «ViPNet CSP. Руководство пользователя».

   - Чтобы сохранить ключи подписи на внешнее устройство, установите флажок **Перенести ключи электронной подписи на внешнее устройство**.

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

3. По завершении всех действий нажмите кнопку **OK**.

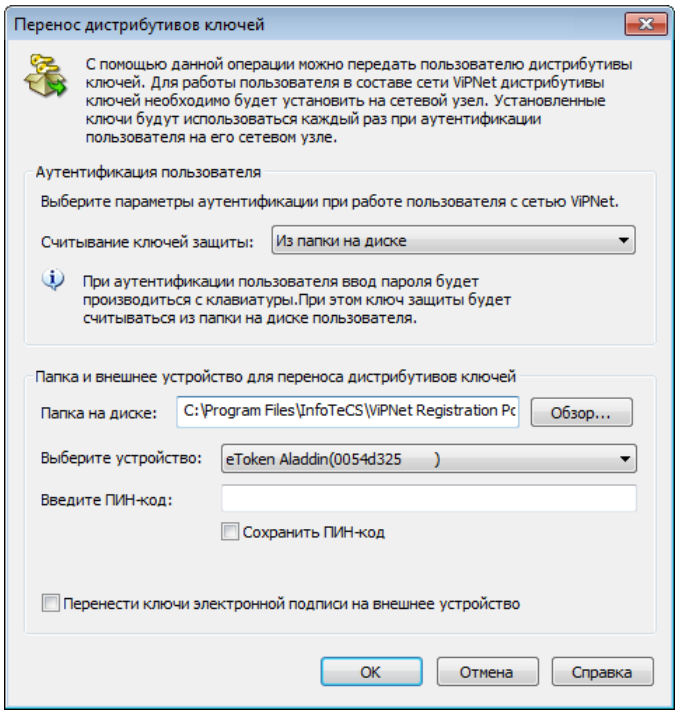


Рисунок 73. Настройка параметров переноса (распаковки) дистрибутива ключей

В результате дистрибутив ключей будет перенесен в папку с именем пользователя по указанному пути в виде файла `*.dst` и будет готов для передачи пользователю.

Распаковка дистрибутива ключей

При необходимости можно распаковать дистрибутив ключей в указанную папку. Как правило, это может потребоваться в том случае, если нужно просмотреть состав дистрибутива ключей (например, какие файлы в нем есть, а каких нет). В процессе распаковки, как и при переносе дистрибутива ключей (см. «Перенос дистрибутива в папку» на стр. 141), определяется способ аутентификации пользователя на сетевом узле и место хранения его контейнера ключей и сертификата.

Чтобы распаковать дистрибутив ключей, выполните следующие действия:

1. В окне программы ViPNet Registration Point в разделе **Пользователи** выберите пользователя с созданным дистрибутивом ключей и в меню **Действие** либо в контекстном меню выберите **Дистрибутивы ключей**, затем щелкните **Распаковать**.
2. В окне **Перенос дистрибутивов ключей** (см. Рисунок 76 на стр. 142) укажите параметры:

   В списке **Считывание ключей защиты** выберите место, откуда будет считываться ключ защиты (персональный ключ (см. «Персональный ключ пользователя» на стр. 203)) при аутентификации пользователя. Если персональный ключ будет считываться из папки, то у пользователя будет способ аутентификации — «Пароль», если с внешнего устройства — «Устройство».

   - В группе **Папка и внешнее устройство для переноса дистрибутивов ключей** с учетом заданных параметров аутентификации укажите:
     - папку на жестком или съемном диске для распаковки дистрибутива ключей;
     - доступное устройство с указанием его параметров и ПИН-кода для переноса ключа защиты.

     Примечание. Для использования какого-либо внешнего устройства необходимо подключить и установить драйверы этого устройства. Перечень доступных устройств хранения данных и полезная информация об использовании устройств содержится в документе «ViPNet CSP. Руководство пользователя».

   - Чтобы сохранить ключи подписи на внешнее устройство, установите флажок **Перенести ключи электронной подписи на внешнее устройство**.

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

3. По завершении всех действий нажмите кнопку **OK**.

   В результате дистрибутив ключей будет распакован в папку с именем пользователя по указанному пути и представлен в виде набора файлов (справочников и ключей).

9

Административные функции

Настройка параметров безопасности

Описанные в настоящем разделе настройки выполняются в окне **Настройка параметров безопасности**. Чтобы вызвать данное окно, в меню **Сервис** выберите пункт **Настройка параметров безопасности**. Описание настроек, которые можно выполнить в данном окне, см. в аналогичном разделе в документе «ViPNet Client. Руководство пользователя»,

Работа с резервными копиями конфигураций программы

В программе ViPNet Registration Point существует возможность возврата к предыдущим конфигурациям. Для восстановления конфигурации используются резервные копии, которые автоматически создаются программой или вручную администратором. Каждая резервная копия конфигурации включает в себя базу данных и настройки программы.

Автоматическое создание резервных копии текущей конфигурации (без участия администратора) осуществляется в том случае, если в настройках программы установлена соответствующая опция (см. «Настройка параметров создания резервных копий конфигурации» на стр. 150). При создании резервных копий вручную используется мастер восстановления конфигурации.

Создание резервной копии текущей конфигурации

Резервная копия конфигурации создается для того, чтобы можно было восстановить определенную конфигурацию программы.

Примечание. Если для создания резервной копии конфигурации недостаточно свободного пространства на диске, программа выдаст сообщение об этом. Для создания резервной копии необходимо освободить больше пространства на диске.

Чтобы создать резервную копию текущей конфигурации:

1. В окне программы ViPNet Registration Point в меню **Сервис** выберите пункт **Восстановление конфигурации**. Будет запущен мастер **Восстановление конфигурации ViPNet Registration Point**.
2. На странице **Восстановление конфигурации ViPNet Registration Point** выберите **Создать резервную копию текущей конфигурации**, затем нажмите кнопку **Далее**.

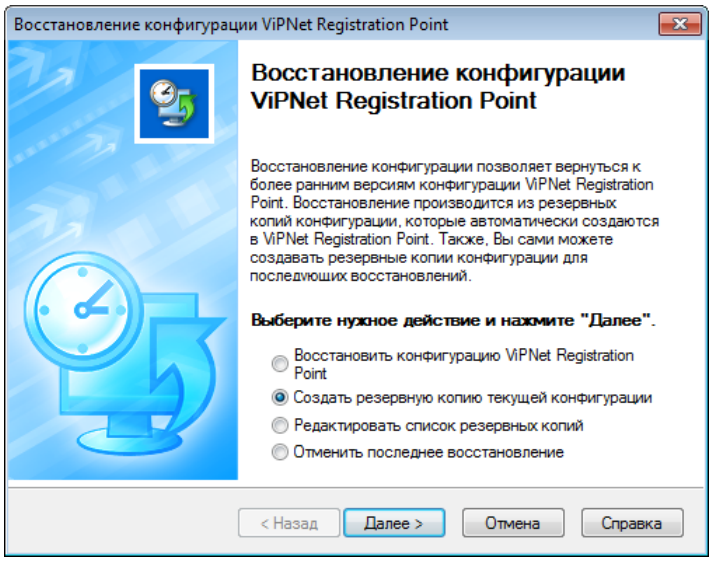


Рисунок 74. Запуск мастера создания и восстановления конфигурации

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.

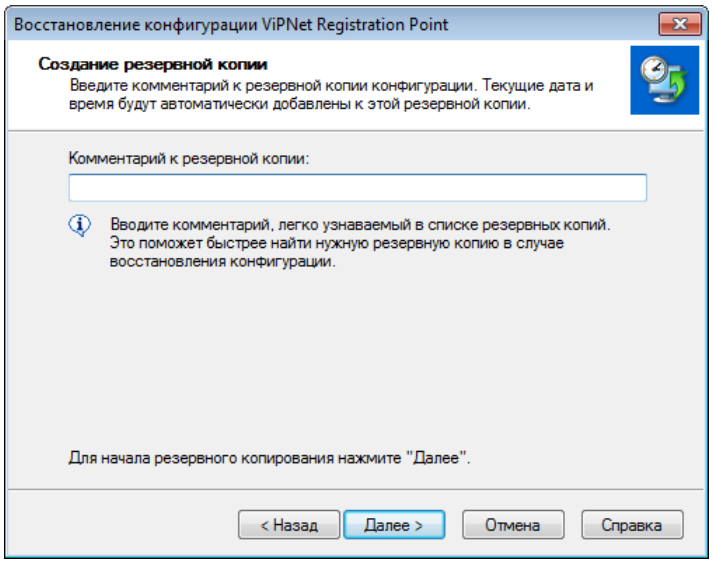


Рисунок 75. Создание резервной копии

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

Созданная резервная копия конфигурации будет сохранена в подпапке `\Restore` папки установки программы.

5 Чтобы закончить работу мастера, на странице **Завершение создания резервной копии конфигурации** нажмите кнопку **Готово**.

Чтобы выполнить новую операцию с резервными копиями, нажмите кнопку **В начало**.

Восстановление конфигурации

Чтобы восстановить конфигурацию из ранее созданной резервной копии:

1 В окне программы ViPNet Registration Point в меню **Сервис** выберите пункт **Восстановление конфигурации**. Будет запущен мастер **Восстановление конфигурации ViPNet Registration Point**.

2 На странице **Восстановление конфигурации ViPNet Registration Point** выберите **Восстановить конфигурацию ViPNet Registration Point**, затем нажмите кнопку **Далее**.

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

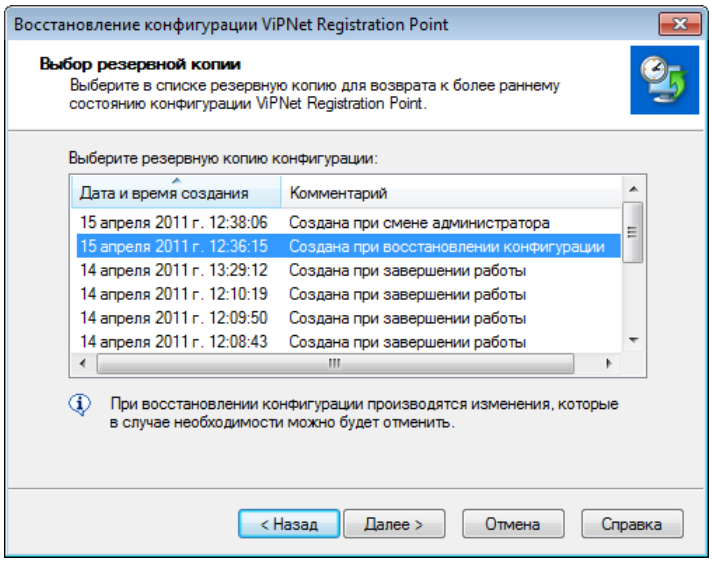


Рисунок 76. Восстановление резервной копии

Резервные копии, созданные автоматически, могут иметь следующие комментарии:

- Создана при восстановлении конфигурации.
- Создана при завершении работы.

Резервные копии конфигураций автоматически сортируются по дате и времени создания. Чтобы изменить порядок сортировки, щелкните заголовок столбца **Дата и время создания** или **Комментарий**.

Выберите резервную копию, из которой требуется восстановить конфигурацию, и нажмите кнопку **Далее**. Начнется процесс восстановления выбранной конфигурации. При восстановлении конфигурации текущий пароль администратора для входа в ViPNet Registration Point не изменится.

4 Чтобы закончить работу мастера, на странице **Завершение восстановления конфигурации ViPNet Registration Point** нажмите кнопку **Готово**.

Чтобы выполнить другую операцию с резервными копиями, нажмите кнопку **В начало**.

Примечание. Всегда можно отменить последнее восстановление или восстановить конфигурацию из другой резервной копии, вернувшись на первую страницу мастера. Если мастер уже закрыт, заново запустите его.

В том случае если в процессе работы с программой изменялась папка ее установки (например, содержимое папки установки было перенесено в другую папку либо папка установки была переименована), после восстановления конфигурации следует проверить правильность настройки параметров транспортного модуля (см. «Настройка транспортного модуля» на стр. 20).

Редактирование списка резервных копий

Список резервных копий конфигурации можно редактировать: удалять резервные копии или изменять комментарии.

Для редактирования списка резервных копий конфигурации выполните следующие действия:

1. В окне программы ViPNet Registration Point в меню **Сервис** выберите пункт **Восстановление конфигурации**. Будет запущен мастер **Восстановление конфигурации ViPNet Registration Point**.
2. На странице **Восстановление конфигурации ViPNet Registration Point** выберите **Редактировать список резервных копий** и нажмите кнопку **Далее**.
3. На странице **Редактирование списка резервных копий** выберите резервную копию, которую необходимо изменить. Чтобы изменить комментарий, нажмите кнопку **Редактировать комментарий**. Для удаления резервной копии нажмите кнопку **Удалить**.

   Резервные копии конфигурации автоматически сортируются по дате и времени создания. Чтобы изменить порядок сортировки, щелкните заголовок столбца **Дата и время создания** или **Комментарий**.

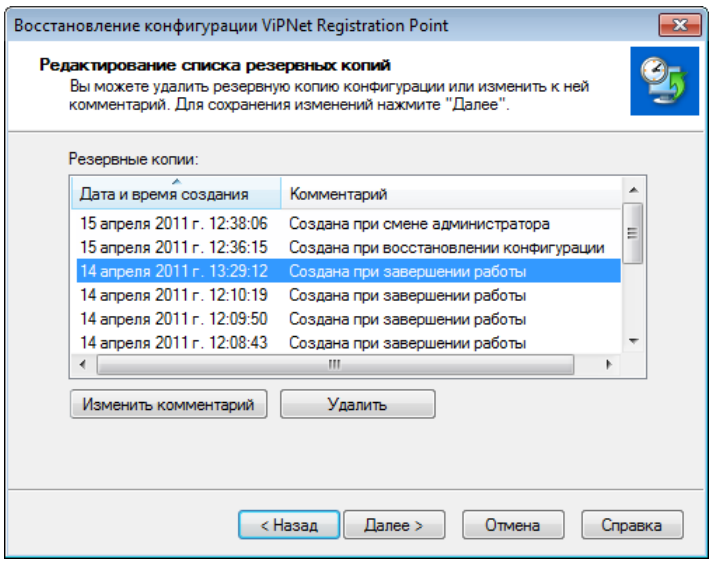


Рисунок 77. Редактирование списка резервных копий

4 Чтобы завершить редактирование, нажмите кнопку **Далее**.

5 Чтобы закончить работу мастера, на странице **Завершение создания резервной копии конфигурации** нажмите кнопку **Готово**.

Чтобы выполнить новую операцию с резервными копиями, нажмите кнопку **В начало**.

Отмена последнего восстановления конфигурации

Примечание. Это действие возможно только после восстановления конфигурации из резервной копии, если после этого не были созданы новые резервные копии конфигурации.

Чтобы отменить последнее восстановление конфигурации:

1 В окне программы ViPNet Registration Point в меню **Сервис** выберите пункт **Резервные копии конфигурации**. Будет запущен мастер **Восстановление конфигурации ViPNet Registration Point**.

2 На странице **Восстановление конфигурации ViPNet Registration Point** выберите **Отменить последнее восстановление**, затем нажмите кнопку **Далее**.

Начнется процесс отмены последнего восстановления конфигурации.

Чтобы закончить работу мастера, на странице **Завершение отмены последнего восстановления конфигурации** нажмите кнопку **Закрыть**.

Настройка параметров создания резервных копий конфигурации

В зависимости от настроек, резервные копии конфигураций программы ViPNet Registration Point могут создаваться автоматически без участия администратора.

Для настройки автоматического создания резервных копий конфигураций выполните следующие действия:

1 В окне программы в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка**  на панели инструментов.

2 В появившемся окне на панели навигации выберите раздел **Восстановление конфигурации**.

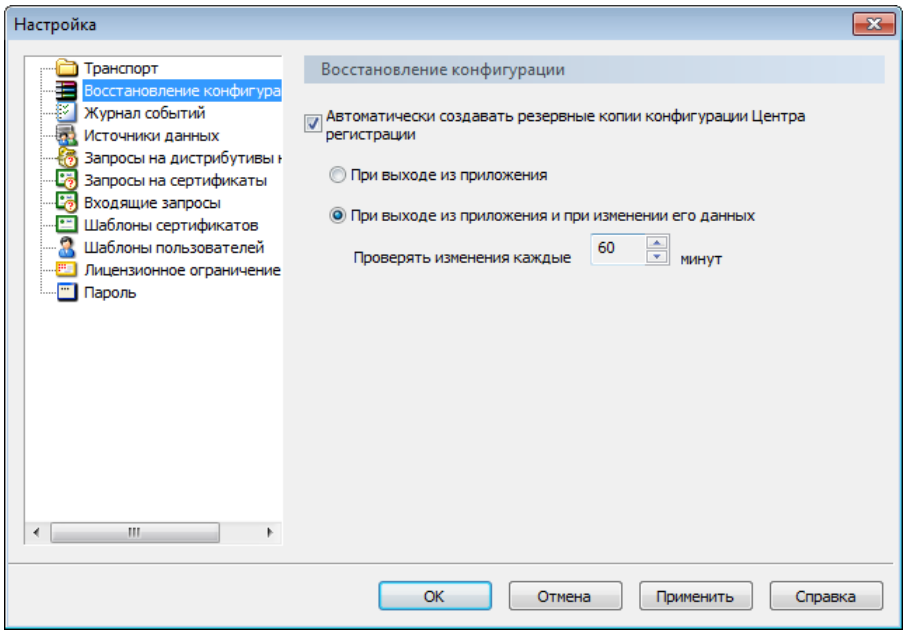


Рисунок 78. Настройка параметров создания резервных копий

3 Установите флажок **Автоматически создавать резервные копии конфигурации Центра регистрации** и выберите один из следующих режимов:

- Для создания резервной копии при каждом выходе из программы ViPNet Registration Point выберите режим **При выходе из приложения**.
- Для создания резервной копии не только при завершении работы с программой, но и с учетом вносимых изменений, выберите режим **При выходе из приложения и при изменении его данных** и в поле **Проверять изменения каждые** укажите интервал проверки изменений (в минутах).

Совет. Рекомендуется использовать данный режим при длительных сеансах работы с программой, в ходе которых она не закрывается.

---

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

Работа с журналом событий программы ViPNet Registration Point

Информация о событиях, возникающих при работе программы ViPNet Registration Point, фиксируется в журнале событий. Настройка журнала событий описана в разделе Настройка параметров журнала событий (на стр. 154).

Просмотр журнала событий

Совет. Для корректного отображения записей журнала событий рекомендуется использоваться Internet Explorer версии 6.0 и выше.

Для просмотра журнала событий выполните следующие действия:

1 В окне программы в меню **Сервис** выберите пункт **Журнал событий**. Откроется окно **Просмотр журналов**.

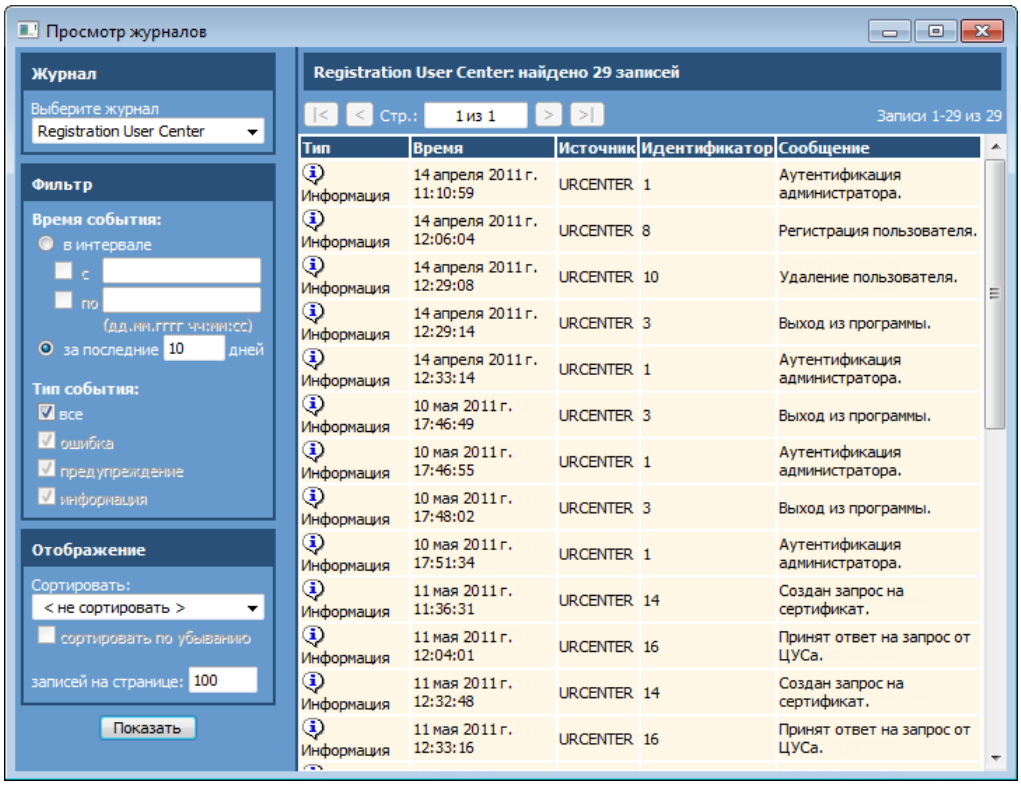


Рисунок 79. Просмотр журнала событий

2 В левой части окна **Просмотр журналов** на панели **Фильтр** задайте параметры поиска событий в журнале:

- Задайте время события одним из двух способов:
  - Для поиска событий, произошедших в определенном интервале времени, выберите пункт **в интервале**. Чтобы указать начало и конец интервала, установите соответствующие флажки (**с** и **по**) и в поле справа введите дату и время в формате `дд.мм.гггг чч:мм:сс`.
  - Для поиска событий, произошедших за последние несколько дней, выберите пункт **за последние** и в поле справа введите количество дней.

  По умолчанию задан поиск событий за последние 10 дней.
- Задайте тип события, установив или сняв флажки **все**, **ошибка**, **предупреждение**, **информация**. По умолчанию задан поиск всех событий.

3 На панели **Отображение**:

- Из списка **Сортировать** выберите порядок сортировки. По умолчанию выбран пункт **< не сортировать >**.
- Если требуется изменить порядок сортировки событий, установите флажок **сортировать по убыванию** (этот флажок недоступен, если в списке **Сортировать** выбран пункт **< не сортировать >**).
- В поле **Записей на странице** укажите число событий, отображаемых на одной странице (по умолчанию 100).

4 Задав параметры поиска, нажмите кнопку **Показать**. На правой панели окна **Просмотр журналов** отобразится список найденных событий (см. Рисунок 104 на стр. 153).

Примечание. В столбце **Источник** списка событий указывается название модуля, в котором произошло данное событие. Событие может произойти не только в программе ViPNet Registration Point, но и, например, в модуле сервиса безопасности.

5 Если результаты поиска отображаются на нескольких страницах, для переключения между страницами используйте кнопки, расположенные над списком событий.

6 Чтобы просмотреть подробную информацию о каком-либо событии, щелкните строку этого события. Откроется окно **Информация о событии**.

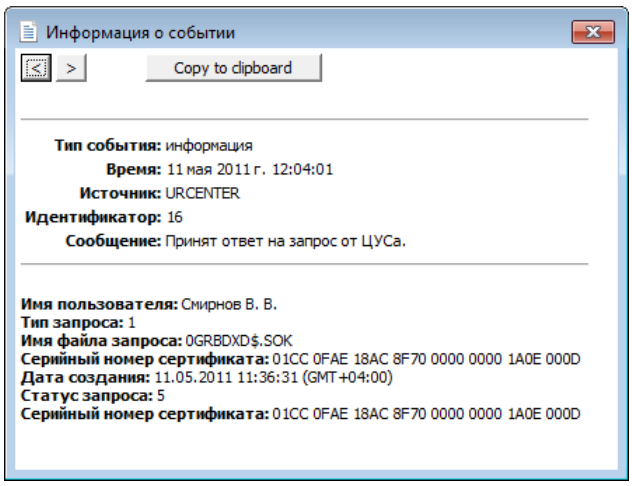


Рисунок 80. Подробная информация о событии

Чтобы перейти к предыдущему событию в списке, нажмите кнопку < в верхней части окна **Информация о событии**. Чтобы перейти к следующему событию, нажмите кнопку >.

Описание возможных событий представлено в приложении (см. «События, регистрируемые в программе ViPNet Registration Point» на стр. 173).

Настройка параметров журнала событий

С помощью настройки параметров журнала событий можно включить или отключить опцию ведения журнала событий, определить его максимальный размер и срок хранения архива журнала.

Для настройки параметров журнала событий выполните следующие действия:

1 В окне программы в меню **Сервис** выберите пункт **Настройка** либо нажмите кнопку **Настройка** на панели инструментов.

2 В появившемся окне на панели навигации выберите раздел **Журнал событий**.

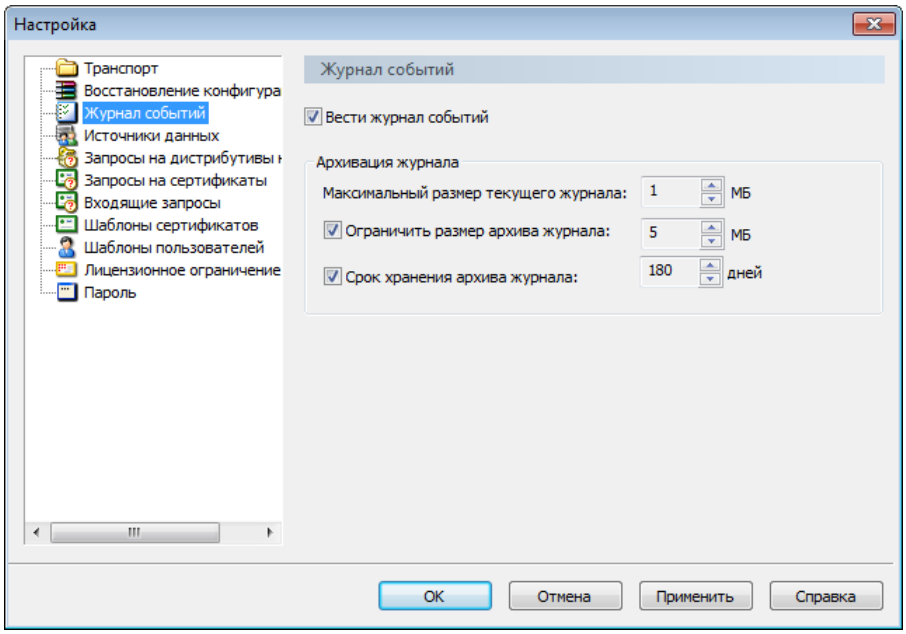


Рисунок 81. Настройка журнала событий

3 Если требуется отключить ведение журнала событий, снимите флажок **Вести журнал событий**.

Если данный флажок снят, настройка остальных параметров журнала событий недоступна.

4 В группе **Архивация журнала** задайте следующие параметры:

- В поле **Максимальный размер текущего журнала** введите размер журнала в мегабайтах (по умолчанию 1).

  Если размер текущего файла журнала превышает заданное значение, файлу присваивается статус архивного и создается новый текущий файл журнала.

- Чтобы задать ограничение по размеру архива журнала, установите флажок **Ограничить размер архива журнала** и в поле справа введите размер архива в мегабайтах (по умолчанию 5).

  Если суммарный размер архивных файлов журнала превысил заданное значение, последовательно удаляются самые старые архивные файлы до тех пор, пока суммарный размер архивов не станет меньше или равен заданному значению.

- Чтобы задать ограничение по времени хранения архива, установите флажок **Срок хранения архива журнала** и в поле справа введите максимальное время хранения архива в днях (по умолчанию 180).

  Если время хранения архивного файла журнала (разница между текущим временем и временем перевода файла в архив) превышает заданное значение, такой файл удаляется.

Примечание. Если установлен флажок **Срок хранения архива журнала**, не рекомендуется изменять системное время, так как это может иметь негативные последствия.

---

5 Чтобы сохранить настройки, нажмите кнопку **Применить**.

A

Общие сведения о сертификатах ключей проверки электронной подписи

Определение и назначение

Сертификат ключа проверки электронной подписи является одним из объектов криптографии с ключом проверки электронной подписи, в которой для прямого и обратного преобразований используются разные ключи:

- Ключ электронной подписи — для формирования электронной подписи (см. «Электронная подпись» на стр. 206) и расшифрования сообщения. Ключ электронной подписи хранится в тайне и не подлежит распространению.
- Ключ проверки электронной подписи — для проверки электронной подписи и зашифрования сообщения. Ключ проверки электронной подписи известен всем участникам информационного обмена и может передаваться по незащищенным каналам связи.

Таким образом, криптография с ключом проверки электронной подписи позволяет выполнять следующие операции:

- Подписание сообщения — формирование электронной подписи, прикрепление ее к сообщению и проверка электронной подписи на стороне получателя;
- Шифрование — зашифрование документа с возможностью расшифрования на стороне получателя.

Ключи электронной подписи и проверки электронной подписи являются комплементарными по отношению друг к другу — только владелец ключа электронной подписи может подписать данные, а также расшифровать данные, которые были зашифрованы ключом проверки электронной подписи, соответствующим ключу электронной подписи владельца. Простой аналогией может служить почтовый ящик: любой может кинуть письмо в почтовый ящик («зашифровать»), но только владелец секретного ключа (ключа электронной подписи) может извлечь письма из ящика («расшифровать»).

Поскольку ключ проверки электронной подписи распространяется публично, существует опасность того, что злоумышленник, подменив ключ проверки электронной подписи одного из пользователей, может выступать от его имени. Для обеспечения доверия к ключам проверки электронной подписи создаются удостоверяющие центры (согласно Федеральному закону РФ № 63 «Об электронной подписи» от 6 апреля 2011 года), которые играют роль доверенной третьей стороны и заверяют ключи проверки электронной подписи каждого из пользователей своими электронными подписями — иначе говоря, сертифицируют эти ключи.

Сертификат ключа проверки электронной подписи (далее — сертификат) представляет собой цифровой документ, заверенный электронной подписью удостоверяющего центра и призванный подтверждать принадлежность ключа проверки электронной подписи определенному пользователю.

Примечание. Несмотря на то, что защита сообщений выполняется фактически с помощью ключа проверки электронной подписи, в профессиональной речи используются выражения «подписать сертификатом (с помощью сертификата)», «зашифровать на сертификате (с помощью сертификата)».

Сертификат включает ключ проверки электронной подписи и список дополнительных атрибутов, принадлежащих пользователю (владельцу сертификата). К таким атрибутам относятся: имена владельца и издателя сертификата, номер сертификата, время действия сертификата, предназначение ключа проверки электронной подписи (электронная подпись, шифрование) и так далее. Структура и протоколы использования сертификатов определяются международными стандартами (см. «Структура» на стр. 160).

Различаются следующие виды сертификатов:

- Сертификат пользователя — для зашифрования исходящих сообщений и для проверки электронной подписи на стороне получателя.
- Сертификат издателя — сертификат, с помощью которого был издан текущий сертификат пользователя. Помимо основных возможностей, которые предоставляет сертификат пользователя, сертификат издателя позволяет также проверить все сертификаты, подписанные с помощью ключа электронной подписи, соответствующего этому сертификату.
- Корневой сертификат — самоподписанный сертификат издателя, являющийся главным из вышестоящих сертификатов. Корневой сертификат не может быть проверен с помощью другого сертификата, поэтому пользователь должен безусловно доверять источнику, из которого получен данный сертификат.
- Кросс-сертификат — это сертификат администратора удостоверяющего центра, изданный администратором другого удостоверяющего центра. Таким образом, для кросс-сертификата значения полей «Издатель» и «Субъект» различны и определяют разные удостоверяющие центры. С помощью кросс-сертификатов устанавливаются доверительные отношения между различными удостоверяющими центрами. В зависимости от модели доверительных отношений, установленной между удостоверяющими центрами (см. «PKI и асимметричная криптография» на стр. 163), может использоваться либо как сертификат издателя (в иерархической модели), либо для проверки сертификатов пользователей другой сети (в распределенной модели).

Рисунок 82. Типы сертификатов

Используя корневой сертификат, каждый пользователь может проверить достоверность сертификата, выпущенного удостоверяющим центром, и воспользоваться его содержимым. Если проверка сертификата по цепочке сертификатов, начиная с корневого, показала, что он является законным, действующим, не был просрочен или аннулирован, то сертификат считается действительным. Документы, подписанные действительным сертификатом и не изменявшиеся с момента их подписания, также считаются действительными.

Таким образом, криптография с ключом проверки электронной подписи и инфраструктура обмена сертификатами ключей проверки электронной подписи (см. «PKI и асимметричная криптография» на стр. 163) позволяют выполнять шифрование сообщений, а также предоставляют возможность подписывать сообщения с помощью электронной подписи.

Посредством шифрования конфиденциальная информация может быть передана по незащищенным каналам связи. В свою очередь, электронная подпись позволяет обеспечить:

- Подлинность (аутентификация) — возможность однозначно идентифицировать отправителя. Если сравнивать с бумажным документооборотом, то это аналогично собственноручной подписи отправителя.
- Целостность — защиту информации от несанкционированной модификации как при хранении, так и при передаче.
- Неотрекаемость — невозможность для отправителя отказаться от совершенного действия. Если сравнивать с бумажным документооборотом, то это аналогично предъявлению отправителем паспорта перед выполнением действия.

Структура

Чтобы сертификат можно было использовать, он должен обладать доступной универсальной структурой, позволяющей извлечь из него нужную информацию и легко ее понять. Например, благодаря тому, что паспорта имеют простую однотипную структуру, можно легко понять информацию, изложенную в паспорте любого государства, даже если вы никогда не видели раньше таких паспортов. Так же дело обстоит и с сертификатами: стандартизация форматов сертификатов позволяет читать и понимать их независимо от того, кем они были изданы.

Один из форматов сертификата определен в рекомендациях Международного Союза по телекоммуникациям (International Telecommuncations Union, ITU) X.509 | ISO/IEC 9594–8 и документе RFC 3280 Certificate & CRL Profile Организации инженерной поддержки Интернета (Internet Engineering Task Force, IETF). В настоящее время наиболее распространенной версией X.509 является версия 3, позволяющая задать для сертификата расширения, с помощью которых можно разместить в сертификате дополнительную информацию (о политиках безопасности, использовании ключа, совместимости и так далее).

Сертификат содержит элементы данных, сопровождаемые электронной подписью издателя сертификата. В сертификате имеются обязательные и дополнительные поля.

К обязательным полям относятся:

- номер версии стандарта X.509,
- серийный номер сертификата,
- идентификатор алгоритма подписи издателя,
- идентификатор алгоритма подписи владельца,
- имя издателя,
- период действия,
- ключ проверки электронной подписи владельца,
- имя владельца сертификата.

Примечание. Под владельцем понимается сторона, контролирующая ключ электронной подписи, соответствующий данному ключу проверки электронной подписи. Владельцем сертификата может быть конечный пользователь или удостоверяющий центр.

К необязательным полям относятся:

- уникальный идентификатор издателя,
- уникальный идентификатор владельца,
- расширения сертификата.

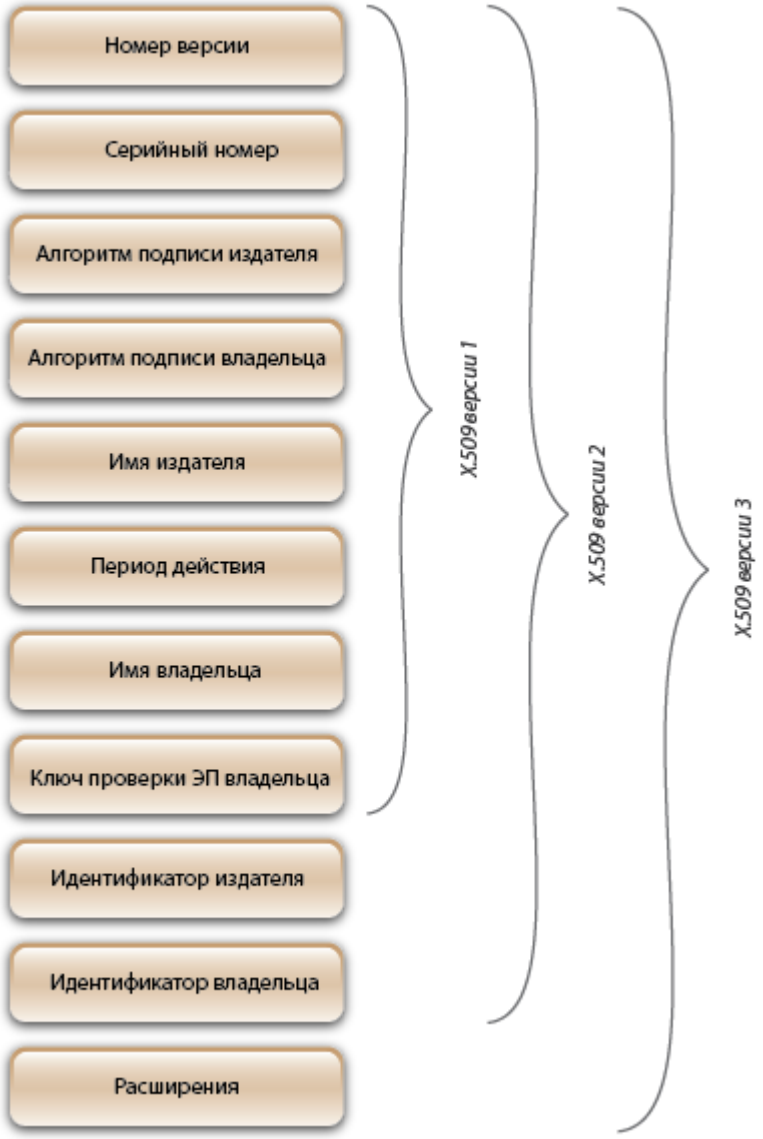
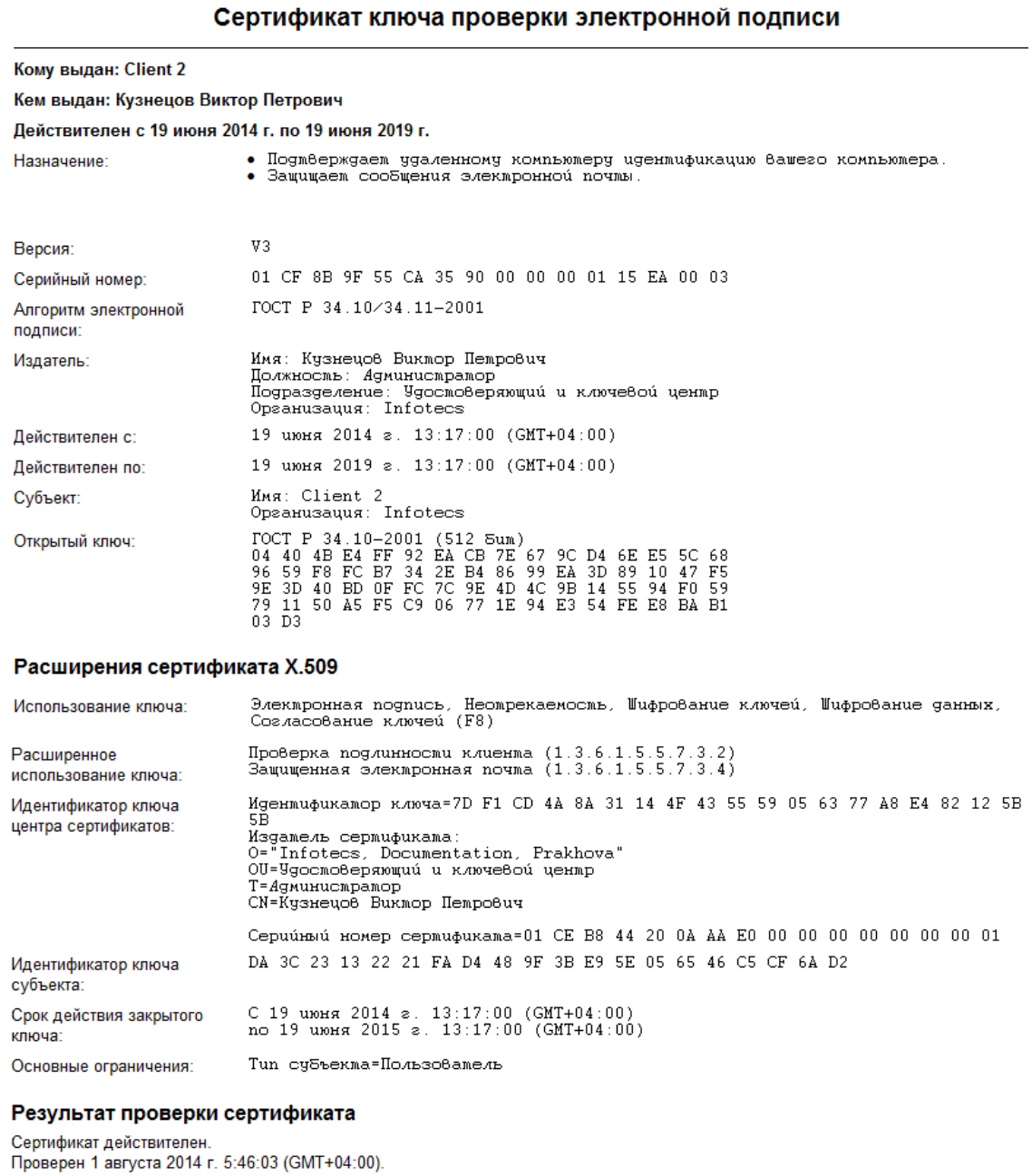


Рисунок 83. Структура сертификата, соответствующего стандарту X.509 версий 1, 2 и 3



Сертификат ключа проверки электронной подписи

Кому выдан: Client 2

Кем выдан: Кузнецов Виктор Петрович

Действителен с 19 июня 2014 г. по 19 июня 2019 г.

Назначение:	• Подтверждает удаленному компьютеру идентификацию вашего компьютера. • Защищает сообщения электронной почты.
Версия:	V3
Серийный номер:	01 CF 8B 9F 55 CA 35 90 00 00 00 01 15 EA 00 03
Алгоритм электронной подписи:	ГОСТ Р 34.10/34.11-2001
Издатель:	Имя: Кузнецов Виктор Петрович Должность: Администратор Подразделение: Удостоверяющий и ключевой центр Организация: Infotecs
Действителен с:	19 июня 2014 г. 13:17:00 (GMT+04:00)
Действителен по:	19 июня 2019 г. 13:17:00 (GMT+04:00)
Субъект:	Имя: Client 2 Организация: Infotecs
Открытый ключ:	ГОСТ Р 34.10-2001 (512 Бит) 04 40 4B E4 FF 92 EA CB 7E 67 9C D4 6E E5 5C 68 96 59 F8 FC B7 34 2E B4 86 99 EA 3D 89 10 47 F5 9E 3D 40 BD 0F FC 7C 9E 4D 4C 9B 14 55 94 F0 59 79 11 50 A5 F5 C9 06 77 1E 94 E3 54 FE E8 BA B1 03 D3

Расширения сертификата X.509

Использование ключа:	Электронная подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (F8)
Расширенное использование ключа:	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
Идентификатор ключа центра сертификатов:	Идентификатор ключа=7D F1 CD 4A 8A 31 14 4F 43 55 59 05 63 77 A8 E4 82 12 5B 5B Издатель сертификата: O="Infotecs, Documentation, Prakhova" OU=Удостоверяющий и ключевой центр T=Администратор CN=Кузнецов Виктор Петрович Серийный номер сертификата=01 CE B8 44 20 0A AA E0 00 00 00 00 00 00 00 01
Идентификатор ключа субъекта:	DA 3C 23 13 22 21 FA D4 48 9F 3B E9 5E 05 65 46 C5 CF 6A D2
Срок действия закрытого ключа:	С 19 июня 2014 г. 13:17:00 (GMT+04:00) по 19 июня 2015 г. 13:17:00 (GMT+04:00)
Основные ограничения:	Тип субъекта=Пользователь

Результат проверки сертификата

Сертификат действителен.
Проверен 1 августа 2014 г. 5:46:03 (GMT+04:00).

Рисунок 84. Пример сертификата ViPNet, соответствующего стандарту X.509 версии 3

PKI и асимметричная криптография

Одной из реализаций инфраструктуры, позволяющей управлять сертификатами ключей проверки электронной подписи, является технология PKI (инфраструктура открытых ключей) (на стр. 199). PKI обслуживает жизненный цикл сертификата: издание сертификатов, хранение, резервное копирование, печать, взаимную сертификацию, ведение списков аннулированных сертификатов (CRL), автоматическое обновление сертификатов после истечения срока их действия.

Основой технологии PKI являются отношения доверия, а главным управляющим компонентом — удостоверяющий центр. Удостоверяющий центр предназначен для регистрации пользователей, выпуска сертификатов, их хранения, выпуска CRL и поддержания его в актуальном состоянии. В сетях ViPNet удостоверяющий центр издает сертификаты как по запросам от пользователей, сформированным в специальной программе (например, ViPNet CSP или ViPNet Client), так и без запросов (в процессе создания пользователей ViPNet).

Для сетей с большим количеством пользователей создается несколько удостоверяющих центров. Доверительные отношения между этими удостоверяющими центрами могут выстраиваться по распределенной или иерархической модели.

- В иерархической модели доверительных отношений удостоверяющие центры объединяются в древовидную структуру, в основании которой находится головной удостоверяющий центр. 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 (на стр. 203)) 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.

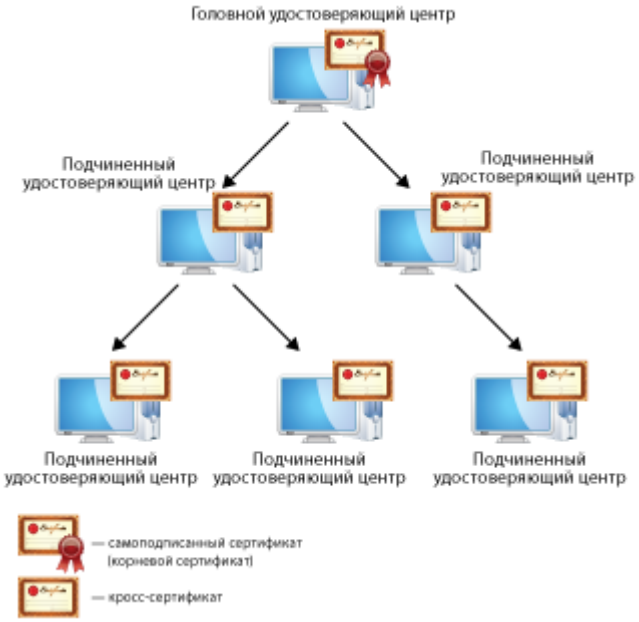


Рисунок 85. Иерархическая модель доверительных отношений

- 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.

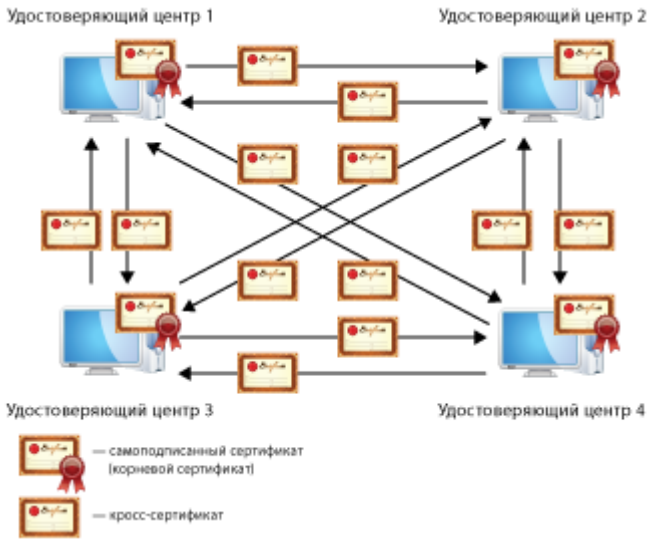


Рисунок 86. Распределенная модель доверительных отношений

Зная иерархию и подчиненность удостоверяющих центров друг другу, можно всегда точно установить, является ли тот или иной пользователь владельцем данного ключа проверки электронной подписи.

Использование сертификатов для шифрования электронных документов

Отправитель может зашифровать документ с помощью открытого ключа получателя, при этом расшифровать документ сможет только сам получатель. В данном случае для зашифрования применяется сертификат получателя сообщения.

Зашифрование

1. Пользователь создает электронный документ.
2. Открытый ключ получателя извлекается из сертификата.
3. Формируется симметричный сеансовый ключ, для однократного использования в рамках данного сеанса.
4. Подписанный документ зашифровывается с использованием сеансового ключа (в соответствии с алгоритмом ГОСТ 28147–89).
5. Сеансовый ключ зашифровывается на ключе, который вырабатывается по протоколу Диффи — Хеллмана с использованием открытого ключа получателя.
6. Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.
7. Документ отправляется.

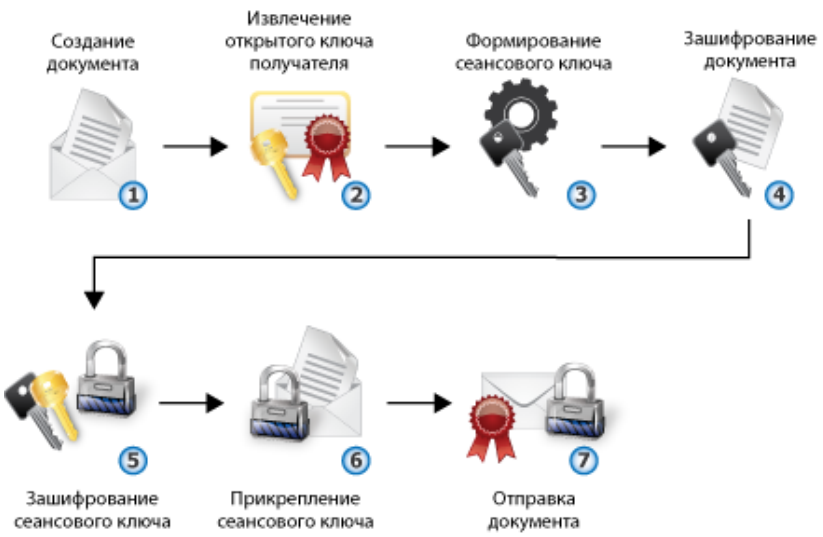


Рисунок 87. Процесс зашифрования электронных документов

Расшифрование

1. Пользователь получает электронный документ.
2. Зашифрованное содержимое документа и зашифрованный сеансовый ключ извлекаются из документа.
3. Закрытый ключ получателя документа извлекается из контейнера ключей.
4. Сеансовый ключ расшифровывается с использованием закрытого ключа получателя.
5. Документ расшифровывается с использованием расшифрованного сеансового ключа.
6. Расшифрованный документ доступен получателю.

Рисунок 88. Процесс расшифрования электронных документов

Использование сертификатов для подписания электронных документов

Когда отправитель подписывает документ, он использует ключ электронной подписи, соответствующий ключу проверки электронной подписи, который хранится в сертификате. Когда получатель проверяет электронную подпись (см. «Электронная подпись» на стр. 206) сообщения, он извлекает ключ проверки электронной подписи из сертификата отправителя.

Подписание

1. Пользователь создает электронный документ.
2. Вычисляется значение хэш-функции документа.

   Хэш-функция документа используется при формировании электронной подписи на стороне отправителя, а также при дальнейшей проверке электронной подписи на стороне получателя.
3. Ключ электронной подписи отправителя извлекается из контейнера ключей.
4. С использованием ключа электронной подписи отправителя на основе значения хэш-функции формируется электронная подпись.
5. Электронная подпись прикрепляется к документу.
6. Зашифрованный документ отправляется.

Рисунок 89. Процесс подписания электронного документа

Проверка подписи

1. Пользователь получает электронный документ.
2. Электронная подпись (зашифрованное значение хэш-функции) извлекается из документа.
3. Вычисляется значение хэш-функции документа.
4. Ключ проверки электронной подписи отправителя извлекается из сертификата отправителя.
5. Электронная подпись расшифровывается с использованием ключа проверки электронной подписи отправителя.
6. Значение хэш-функции электронной подписи сравнивается с полученным значением хэш-функции документа.
7. Если значения хэш-функций совпадают, электронная подпись документа считается действительной.

   Если значения хэш-функций не совпадают (то есть полученный документ был изменен с момента подписания), электронная подпись документа считается недействительной. Электронная подпись считается недействительной также в том случае, если сертификат отправителя просрочен, аннулирован, искажен или подписан удостоверяющим центром, с которым не установлены доверительные отношения.

Рисунок 90. Процесс проверки электронной подписи

Использование сертификатов для подписания и шифрования электронных документов

Подписание и зашифрование

1. Пользователь создает электронный документ.
2. Вычисляется значение хэш-функции документа.
3. Ключ электронной подписи отправителя извлекается из контейнера ключей.
4. Открытый ключ получателя извлекается из сертификата получателя.
5. С использованием ключа электронной подписи отправителя на основе значения хэш-функции формируется электронная подпись.
6. Электронная подпись прикрепляется к документу.
7. Формируется симметричный сеансовый ключ, для однократного использования в рамках данного сеанса.
8. Подписанный документ зашифровывается с использованием сеансового ключа (в соответствии с алгоритмом ГОСТ 28147–89).
9. Сеансовый ключ зашифровывается на ключе, который вырабатывается по протоколу Диффи — Хеллмана с открытого ключа получателя.
10. Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.
11. Документ отправляется.

Рисунок 91. Процесс подписания и зашифрования электронных документов

Расшифрование и проверка

1 Пользователь получает электронный документ.

2 Зашифрованное содержимое документа и зашифрованный сеансовый ключ извлекаются из сообщения.

3 Закрытый ключ получателя документа извлекается из контейнера ключей.

4 Сеансовый ключ расшифровывается с помощью закрытого ключа получателя.

5 Документ расшифровывается с использованием расшифрованного сеансового ключа.

6 Электронная подпись (зашифрованное значение хэш-функции) извлекается из документа.

7 Вычисляется значение хэш-функции документа.

8 Ключ проверки электронной подписи отправителя извлекается из сертификата отправителя.

9 Электронная подпись расшифровывается с использованием ключа проверки электронной подписи отправителя.

10 Значение хэш-функции электронной подписи сравнивается с полученным значением хэш-функции документа.

11 Если значения хэш-функций совпадают, электронная подпись документа считается действительной.

Если значения хэш-функций не совпадают (то есть полученный документ был изменен с момента подписания), электронная подпись документа считается недействительной. Подпись считается недействительной также в том случае, если сертификат отправителя просрочен, аннулирован, искажен или подписан удостоверяющим центром, с которым не установлены доверительные отношения.

12 Расшифрованный документ доступен получателю.

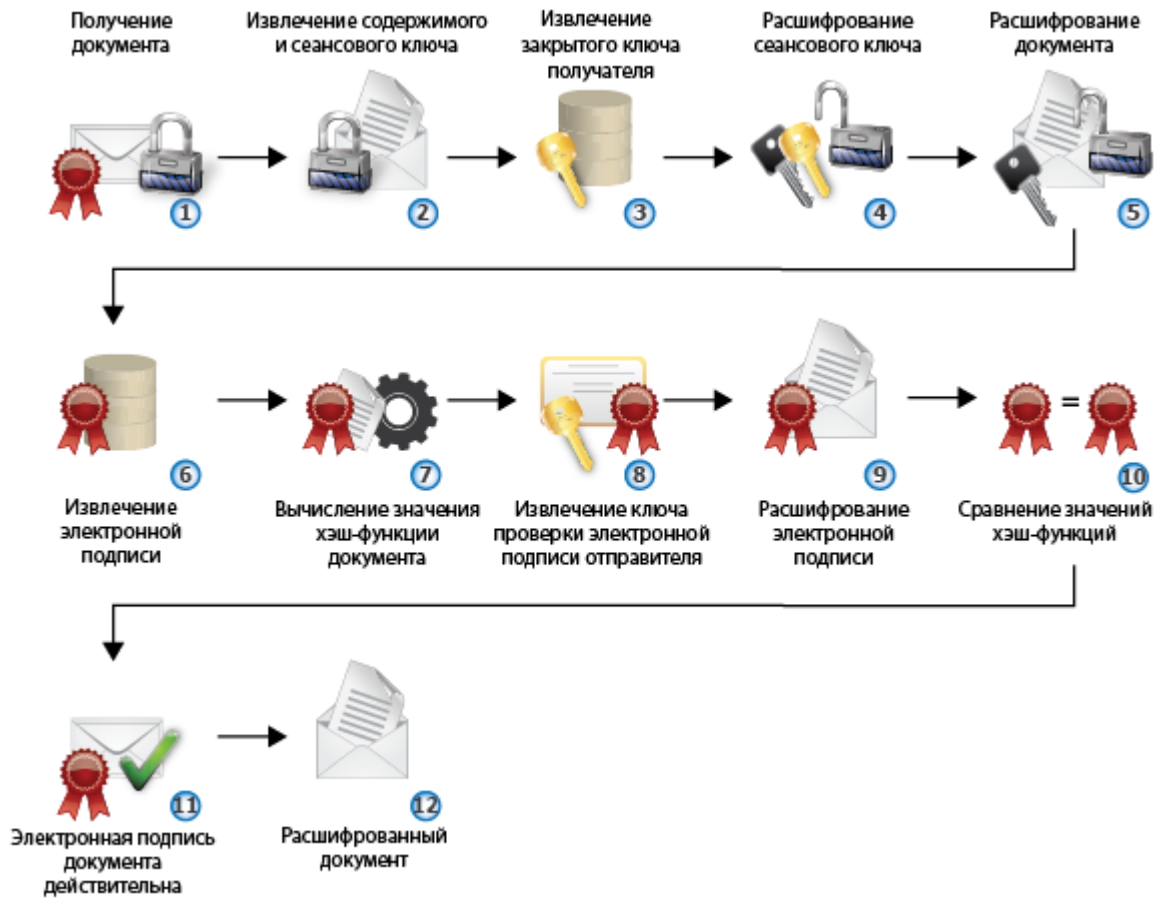


Рисунок 92. Процесс расшифрования и проверки электронной подписи документа

B

События, регистрируемые в программе ViPNet Registration Point

Таблица 6. События, фиксируемые в журнале ViPNet Registration Point

Тип события	Название события	Причины наступления события
	Аутентификация администратора	Успешный запуск программы
	Выход из программы	Завершена работа с программой
	Изменены настройки программы	Настройки ViPNet Registration Point изменены и вступили в действие
	Создана резервная копия	По команде администратора или автоматически в соответствии с настройками создана резервная копия программы
	Регистрация пользователя	По команде администратора зарегистрированы новые пользователи
	Изменение регистрационных данных пользователя	Отредактированы данные пользователя в окне свойств или в процессе создания запроса на сертификат

Тип события	Название события	Причины наступления события
Информация	Создан запрос на дистрибутив	По команде администратора либо автоматически после регистрации пользователя при наличии соответствующей настройки создан запрос на дистрибутив ключей для пользователя
	Создан запрос на обновление ключей	По команде администратора создан запрос на обновление дистрибутива ключей
	Создан запрос на сертификат	По команде администратора создан запрос на сертификат
	Принят ответ на запрос от ЦУСа	Из программы ViPNet Центр управления сетью получен ответ на запрос (любого вида). При этом запрос может быть как удовлетворен, так и отклонен
	Дистрибутив передан пользователю	По команде администратора распакован или перенесен в папку на диске дистрибутив ключей
	Сертификат передан пользователю	Автоматически или вручную по команде администратора добавлен сертификат в контейнер ключей
	Удаление пользователя	По команде администратора удалена информация о пользователе из базы данных ViPNet Registration Point
	Создан запрос на удаление пользователя в ЦУСе	По команде администратора создан и отправлен в программу ViPNet Центр управления сетью запрос на удаление регистрационных данных пользователя
Ошибка	Неудачная аутентификация администратора	Введен неправильный пароль или не найдены ключи при запуске программы
	Ошибка при изменении настроек программы	Произведена некорректная настройка программы
	Ошибка создания резервной копии	Произошел сбой при создании резервной копии
	Ошибка регистрации пользователя	Произошел сбой во время работы мастера регистрации пользователя
	Ошибка изменения регистрационных данных	Произошел сбой в процессе изменения регистрационных данных пользователя в окне свойств или в процессе создания запроса на сертификат
	Ошибка создания запроса на дистрибутив	Произошел сбой в процессе создания запроса на дистрибутив ключей для пользователя

Тип события	Название события	Причины наступления события
	Ошибка создания запроса на обновление ключей	Произошел сбой в процессе создания запроса на обновление дистрибутива ключей
	Ошибка создания запроса на сертификат	Произошел сбой в процессе создания запроса на сертификат
	Ошибка создания запроса на удаление пользователя в ЦУСе	Произошел сбой в процессе создания или отправки запроса на удаление регистрационных данных пользователя в ЦУСе

C

Перенос шаблонов сертификатов в программу ViPNet CSP

Шаблоны сертификатов, созданные в программе ViPNet Registration Point, могут быть использованы при создании запросов на сертификаты с помощью программы ViPNet CSP (например, если требуется создать запрос на сертификат, шаблон для которого отсутствует в списке стандартных шаблонов ViPNet CSP). Для этого необходимо перенести нужные шаблоны в программу ViPNet CSP с помощью утилиты `TemplateConverter.exe`. Данная утилита входит в комплект поставки ViPNet Registration Point и помещается в папку установки программы при ее развертывании.

При переносе также используется шаблон пользователя, на основе которого будет указываться информация о владельце сертификата при создании запроса в ViPNet CSP. Вы можете использовать стандартный шаблон «Стандартный шаблон имени пользователя» или создать другой шаблон (см. «Создание и редактирование шаблонов пользователей» на стр. 82).

Совет. Должен использоваться сертифицированный ViPNet CSP версии 4.2.

Чтобы перенести шаблон сертификата из программы ViPNet Registration Point в программу ViPNet CSP, выполните следующие действия:

1 В программе ViPNet Registration Point создайте шаблон сертификата с необходимыми расширениями (см. «Создание и редактирование шаблонов сертификатов» на стр. 118).

2 Запустите командную строку ОС Windows. Для этого выполните следующие действия:

2.1 Нажмите сочетание клавиш **Win+R**.

2.2 В появившемся окне введите команду `cmd` и нажмите клавишу **Enter**.

3 В командной строке с помощью команды `cd` перейдите в папку установки ViPNet Registration Point. По умолчанию `C:\Program Files\InfoTeCS\ViPNet Registration Point` (для 64-разрядных операционных систем — `C:\Program Files (x86)\InfoTeCS\ViPNet Registration Point`).

Например:

```
cd C:\Program Files (x86)\InfoTeCS\ViPNet Registration Point
```

4 Убедитесь, что шаблон пользователя (файл `names.ini`), который будет использован в ViPNet CSP для заполнения информации о владельце сертификата, и шаблон сертификата, который вы хотите перенести, находятся в папке установки ViPNet Registration Point (откуда запускается утилита `TemplateConverter.exe`). Если это не так, скопируйте нужный шаблон в папку установки ViPNet Registration Point.

5 Запустите исполняемый файл `TemplateConverter.exe` со следующими параметрами:

```
-d "<Путь к папке установки ViPNet Registration Point>" -tn "<Имя 1>" -tc "<Имя 2>" -o "<Путь к файлу *.p10tmp, в который будет сохранен шаблон>",
```

где:

- Имя 1 — название шаблона пользователя, который будет использован в ViPNet CSP для заполнения информации о владельце сертификата.
- Имя 2 — название шаблона сертификата, который вы хотите перенести.

Например:

```
TemplateConverter.exe -d "C:\Program Files (x86)\InfoTeCS\ViPNet Registration Point" -tn "Стандартный шаблон имени пользователя" -tc "Специализированный сертификат" -o "C:\Certificate Templates\Специализированный сертификат.p10tmp"
```

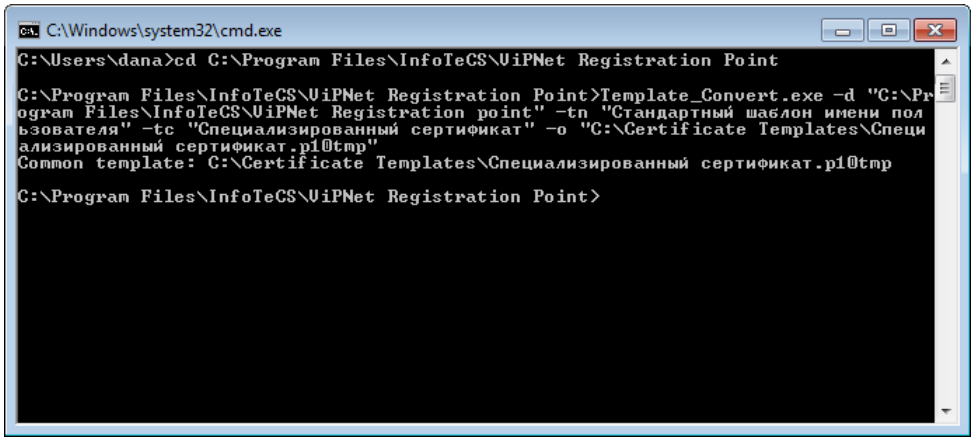


Рисунок 93. Перенос шаблона сертификата в программу ViPNet CSP

В результате шаблон сертификата будет перенесен в указанную папку. Теперь вы можете передать данный шаблон пользователям программы ViPNet CSP. Пользователям необходимо будет поместить шаблон в папку `C:\ProgramData\InfoTeCS\Certificate Templates` (для ОС Windows XP — `C:\Documents and Settings\All Users\Application Data\Infotecs\Certificate`

`Templates`) на своих компьютерах. После этого данный шаблон будет отображаться при создании запросов на сертификаты в программе «Создание запроса на сертификат», которая входит в комплект поставки ViPNet CSP, в списке **Шаблон сертификата**.

D

Возможные неполадки и способы их устранения

Возможные неполадки

Невозможно проверить сертификат, которым подписан файл установки программы

На компьютере с операционной системой Windows Vista при установке программы может появиться предупреждение системы безопасности о невозможности проверить сертификат, которым подписан данный файл установки.

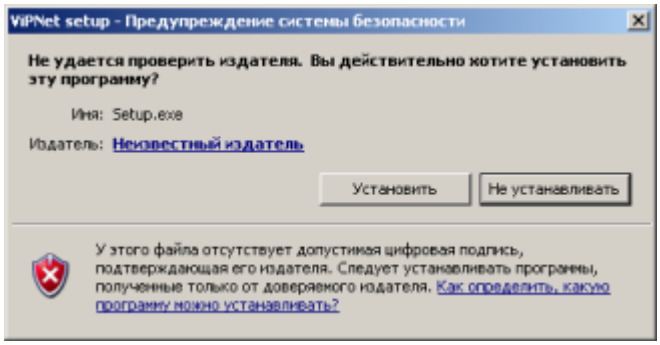


Рисунок 94. Невозможно проверить сертификат

Это может произойти, если отсутствует или недействителен корневой сертификат или какой-либо сертификат из цепочки сертификации.

Возможные варианты решения проблемы:

- С помощью кнопки **Не устанавливать** прервите установку программы, затем установите обновление операционной системы KB931125 (либо просто установите все обновления текущей версии вашей операционной системы). В результате цепочка сертификации будет обновлена, и сертификат, которым подписан файл установки, можно будет проверить.

  После обновления заново начните установку ViPNet Registration Point.

- При необходимости вы можете установить программу без обновления операционной системы. В этом случае в окне предупреждения системы безопасности нажмите кнопку **Установить**.

Невозможно запустить программу

Вероятно, программа ViPNet Registration Point была удалена с компьютера либо были удалены файлы, необходимые для ее работы. Убедитесь в том, что программа ViPNet Registration Point установлена, и в случае необходимости переустановите ее либо обратитесь за помощью к администратору сети ViPNet.

Нет ключей пользователя или неверный пароль

В этом случае программа выдает следующее сообщение:

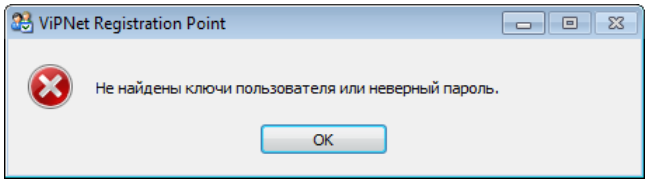


Рисунок 95. Сообщение о неверном пароле

Возможные варианты решения проблемы:

- Проверьте состояние клавиши **Caps Lock**.
- Проверьте раскладку клавиатуры, используя соответствующий индикатор в окне ввода пароля. Если используется случайный пароль, его следует набирать в английской раскладке клавиатуры.
- Проверьте правильность пароля и еще раз внимательно наберите пароль.
- Возможно, ключи пользователя установлены в папку, которая отличается от папки ключей пользователя по умолчанию.

  В этом случае в окне ввода пароля щелкните значок справа от кнопки **Настройка**, в меню выберите пункт **Папка ключей пользователя** и укажите путь к папке ключей пользователя.

Не удается выполнить аутентификацию с помощью сертификата

Если вам не удается войти в программу ViPNet Registration Point, используя для аутентификации сертификат и соответствующий ему ключ электронной подписи, которые хранятся на внешнем устройстве, это может быть вызвано одной из следующих причин:

- Вы используете сертификат ГОСТ совместно с внешним устройством, которое не обеспечивает аппаратную поддержку алгоритмов ГОСТ.
- Внешнее устройство хранения данных не поддерживает стандарт PKCS#11. Проверить, поддерживает ли ваше устройство этот стандарт, можно по информации об устройствах в документе «ViPNet CSP. Руководство пользователя».
- Срок действия выбранного сертификата истек. При выборе недействительного сертификата появится соответствующее сообщение. В этом случае следует передать сертификат администратору вашего удостоверяющего центра для обновления.
- Выбранный сертификат присутствует в списке аннулированных сертификатов, который установлен в хранилище данного узла. При выборе аннулированного сертификата появится

соответствующее сообщение. В этом случае следует обратиться к администратору вашего удостоверяющего центра.

- Выбранный сертификат не имеет расширения «Проверка подлинности клиента». Это расширение должно отображаться в окне **Сертификат**, на вкладке **Состав**, в поле **Расширенное использование ключа**. В этом случае следует обратиться к администратору вашего удостоверяющего центра для переиздания сертификата.

Невозможно сохранить пароль

Сохранения пароля можно разрешить только в режиме администратора (см. «Работа в программе с правами администратора» на стр. 145). Для этого вам требуется войти в программу ViPNet Registration Point с правами администратора и в окне настройки параметров безопасности на вкладке **Администратор** установить соответствующий флажок.

Получены не все сертификаты, изданные в УКЦ по запросам

Описание проблемы

Сформированные или обработанные запросы на сертификаты были отправлены в программу ViPNet Удостоверяющий и ключевой центр. Администратором УКЦ данные запросы были удовлетворены (по запросам были изданы сертификаты подписи). На узле, на котором установлена программа ViPNet Registration Point, ответы на запросы из УКЦ не были получены (изданные сертификаты в программе не появились). При этом по журналу событий ViPNet Registration Point можно установить, что управляющие конверты из УКЦ на узел поступили.

Решение

Данная проблема может быть вызвана тем, что в момент получения сертификатов из УКЦ было открыто окно настроек параметров безопасности в программе ViPNet Registration Point или в другом приложении ViPNet, если такое установлено на вашем узле. Вследствие этого поступившие ответы из УКЦ не смогли быть обработаны из-за занятой базы данных запросов на сертификаты. В таком случае файлы с ответами на запросы были перемещены в папку `ViPNet Registration Point\ccc\from_kc_s`.

Проверьте наличие файлов с ответами на запросы в указанной папке. При наличии в папке файлов, переместите их в папку `ViPNet Registration Point\ccc\from_kc`, предварительно закрыв окно настроек параметров безопасности. После выполнения описанных действий убедитесь, что в программе ViPNet Registration Point:

- Статус запросов, на которые не было получено ответов, изменился на **Удовлетворен**.
- Сертификаты, изданные по данным запросам, появились в разделе **Сертификаты** и стали доступны для установки в контейнеры ключей.

Невозможно добавить сертификат в контейнер ключей

Данная проблема может возникнуть в следующих случаях:

- Сертификат, который вы добавляете в контейнер ключей, не соответствует ключу электронной подписи, находящемуся в контейнере. Убедитесь, что вы добавляете правильный сертификат в контейнер ключей, и повторите попытку еще раз.
- Вы вводите неверный пароль к контейнеру ключей. Повторите попытку с вводом правильного пароля.

Предупреждения сервиса безопасности

Предупреждения сервиса безопасности предназначены для своевременного информирования пользователя о таких событиях, как истечение сроков действия пароля, текущего сертификата, ключа электронной подписи и списка аннулированных сертификатов, а также ввод в действие сертификата, изданного по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр.

Проверка статуса пароля, текущего сертификата и ключа электронной подписи выполняется каждые 5 минут.

Срок действия пароля истек

Окно с сообщением об истечении срока действия пароля пользователя появляется в следующих случаях:

- Если в окне **Настройка параметров безопасности** на вкладке **Пароль** установлен флажок **Ограничить срок действия пароля** и задан срок действия пароля.

  Появление окна свидетельствует о том, что указанный срок подошел к концу.

- Если от программы ViPNet Удостоверяющий и ключевой центр получены ключи пользователя с новым паролем пользователя.

  При этом автоматической смены пароля не происходит, поэтому пароль необходимо сменить вручную (см. «Смена пароля пользователя» на стр. 145).

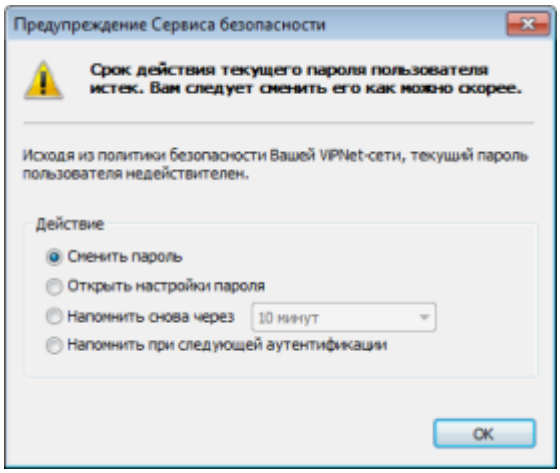


Рисунок 96. Предупреждение об истечении срока действия пароля пользователя

При появлении окна с таким предупреждением:

1. Выберите одно из предложенных действий:
   - **Сменить пароль** — для указания нового пароля в соответствии с настройками, заданными в окне **Настройка параметров безопасности** на вкладке **Пароль**;
   - **Открыть настройки пароля** — для вызова окна **Настройка параметров безопасности** на вкладке **Пароль**, с помощью которой можно сначала задать параметры пароля, а затем сменить его;
   - **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя);
   - **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Registration Point.
2. Нажмите кнопку **OK**.

Текущий сертификат не найден или недействителен

Окно с сообщением о том, что текущий сертификат не найден либо недействителен, появляется в следующих случаях:

- Если текущий сертификат не найден либо недействителен, однако найдены другие действительные личные сертификаты.

  В этом случае вы можете назначить один из них текущим, выбрав **Выбрать другой сертификат в качестве текущего**.

- Если не найден ни один действительный личный сертификат.

  В этом случае обратитесь к администратору вашей сети ViPNet для получения нового сертификата.

Внимание! Пока не получен и не введен в действие новый сертификат, подписание электронных документов невозможно.

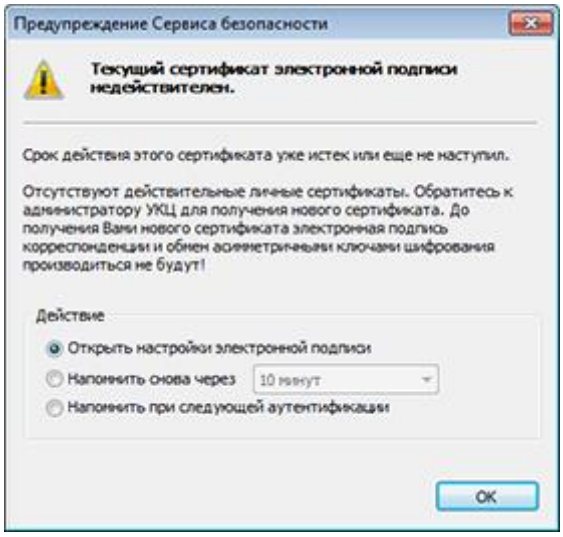


Рисунок 97. Предупреждение о том, что текущий сертификат недействителен

При появлении окна с таким предупреждением:

1 Выберите одно из предложенных действий:

- **Выбрать другой сертификат в качестве текущего** — для назначения другого действительного личного сертификата текущим с помощью окна **Назначение сертификата текущим**.

Примечание. Данное положение переключателя отображается в окне предупреждения в случае, если в хранилище пользователя найдены другие действительные личные сертификаты.

- **Открыть настройки электронной подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Электронная подпись**, с помощью которой можно управлять сертификатами.
- **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя).
- **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Registration Point.

2 Нажмите кнопку **OK**.

Срок действия текущего ключа электронной подписи или соответствующего сертификата близок к концу

Предупреждение о скором истечении срока действия ключа электронной подписи или соответствующего ему сертификата появляется в следующих случаях:

- Если срок действия ключа электронной подписи или сертификата близок к концу, при этом не найдено запросов на обновление текущего сертификата (или последний запрос на обновление удовлетворен, однако соответствующий сертификат не может быть назначен текущим).

  В этом случае Вы можете сформировать запрос на обновление сертификата (см. «Процедура обновления ключа электронной подписи и сертификата» на стр. 145). Для этого:

  - если истекает срок действия сертификата, выберите **Отправить запрос на обновление сертификата**;
  - если истекает срок действия ключа электронной подписи, выберите **Открыть настройки подписи**, затем в окне **Настройка параметров безопасности** на вкладке **Электронная подпись** нажмите кнопку **Обновить сертификат**.

- Если срок действия ключа электронной подписи или сертификата близок к концу, при этом последний запрос на обновление текущего сертификата либо отклонен, либо находится в состоянии обработки в программе ViPNet Удостоверяющий и ключевой центр.

  В этом случае обратитесь к администратору вашей сети ViPNet и, при необходимости, создайте еще один запрос на обновление текущего сертификата.

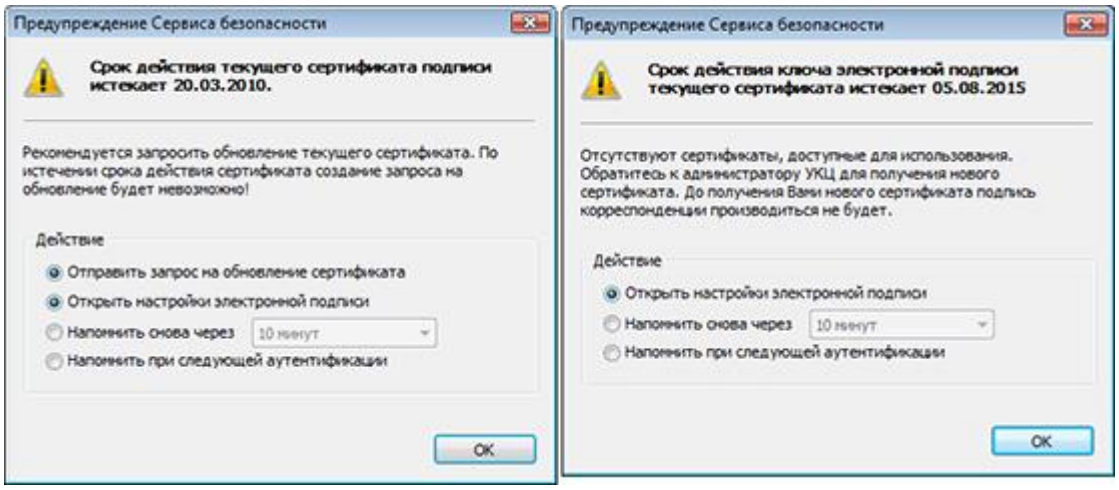


Рисунок 98. Предупреждения о скором истечении срока действия сертификата и ключа электронной подписи

При появлении окна с таким предупреждением:

1 В зависимости от вида предупреждения выберите одно из предложенных действий:

- **Выбрать другой сертификат в качестве текущего** — для назначения другого действительного личного сертификата текущим с помощью окна Н**азначение сертификата текущим**.
- **Отправить запрос на обновление сертификата** — для формирования запроса на обновление текущего сертификата с помощью мастера обновления сертификатов (см. «Процедура обновления ключа электронной подписи и сертификата» на стр. 145).
- **Открыть настройки электронной подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Электронная подпись**, с помощью которой можно управлять сертификатами.
- **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя).
- **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Registration Point.

2 Нажмите кнопку **OK**.

Срок действия текущего ключа электронной подписи уже истек

Предупреждение об истечении срока действия ключа электронной подписи появляется в следующих случаях:

- Если срок действия ключа электронной подписи подошел к концу, при этом не найдено запросов на обновление текущего сертификата (или последний запрос на обновление удовлетворен, однако соответствующий сертификат не может быть назначен текущим).

  В этом случае вы можете открыть вкладку **Электронная подпись** окна **Настройка параметров безопасности**, выбрав **Открыть настройки подписи**. С помощью соответствующей кнопки на вкладке **Электронная подпись** вы можете обновить текущий сертификат (см. «Процедура обновления ключа электронной подписи и сертификата» на стр. 145). Однако в программе ViPNet Удостоверяющий и ключевой центр такой запрос не будет обработан автоматически, а будет ожидать решения администратора.

  Внимание! Созданный запрос подписывается с использованием ключа электронной подписи, соответствующего текущему сертификату. Однако эта подпись используется не для подтверждения авторства, а только для проверки целостности запроса. Такие запросы имеют статус **Не подписан** (см. «Просмотр запроса на сертификат» на стр. 145).

- Если срок действия ключа электронной подписи подошел к концу, при этом последний запрос на обновление текущего сертификата либо отклонен, либо находится в состоянии обработки в программе ViPNet Удостоверяющий и ключевой центр.

В этом случае обратитесь к администратору вашей сети ViPNet и, при необходимости, создайте еще один запрос на обновление текущего сертификата.

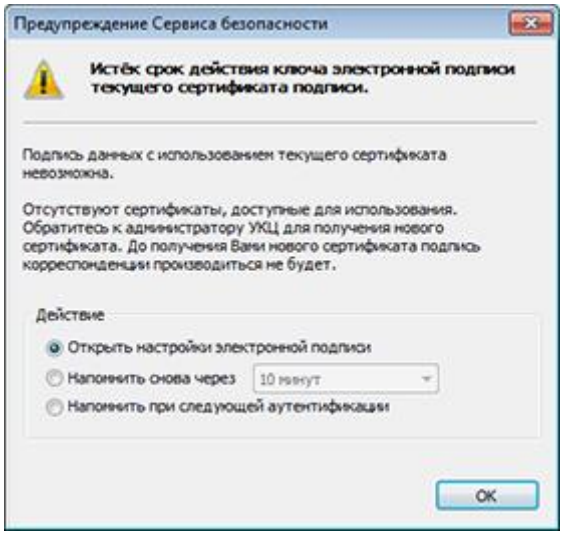


Рисунок 99. Предупреждение о том, что истек срок действия ключа электронной подписи

При появлении окна с таким предупреждением:

1 Выберите одно из предложенных действий:

- **Открыть настройки электронной подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Электронная подпись**, с помощью которой можно управлять сертификатами.
- **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя).
- **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Registration Point.

2 Нажмите кнопку **OK**.

Действительный список аннулированных сертификатов не найден

Предупреждение о том, что действительный список аннулированных сертификатов не найден, появляется при выполнении следующих условий:

- если список аннулированных сертификатов не обнаружен в хранилище пользователя или срок его действия истек;
- если в окне **Настройка параметров безопасности** на вкладке **Администратор** снят флажок **Игнорировать отсутствие списков аннулированных сертификатов** (см. «Дополнительные настройки параметров безопасности» на стр. 145).

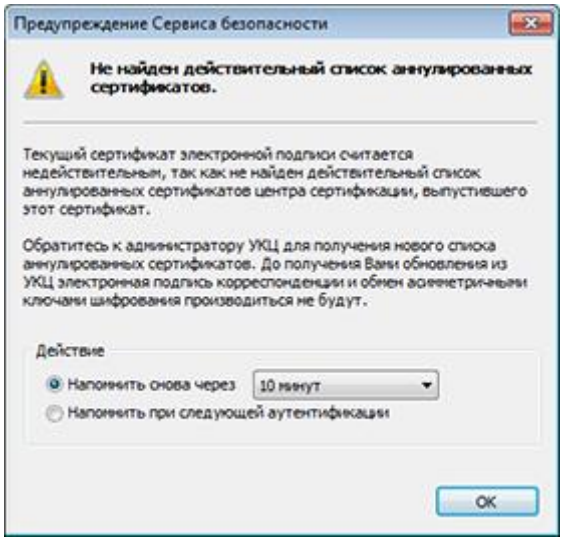


Рисунок 100. Предупреждение о том, что действительный список аннулированных сертификатов не найден

При появлении окна с таким предупреждением:

- Обратитесь к администратору вашей сети ViPNet для получения нового списка аннулированных сертификатов.
- Выберите одно из предложенных действий:
  - **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя).
  - **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Registration Point.

  После этого нажмите кнопку **OK**.

Сертификат, изданный по инициативе администратора, введен в действие

Предупреждение о том, что введен в действие сертификат, изданный по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр, появляется при выполнении следующих условий:

- В окне **Настройка параметров безопасности** на вкладке **Электронная подпись** установлен флажок **Автоматически вводить в действие сертификаты, изданные по инициативе администратора УКЦ**.
- В составе обновления получены ключи, сформированные администратором программы ViPNet Удостоверяющий и ключевой центр без запроса со стороны пользователя и содержащие новый сертификат пользователя и ключ электронной подписи.

При появлении окна с таким предупреждением:

1. Выберите одно из предложенных действий:
   - **Открыть настройки электронной подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Электронная подпись**, с помощью которой можно просмотреть сведения о текущем сертификате, а также управлять сертификатами.
   - **Отправить запрос на обновление сертификата** — для формирования запроса на обновление текущего сертификата с помощью мастера обновления сертификатов (см. «Процедура обновления ключа электронной подписи и сертификата» на стр. 145).

     Отправлять запрос на обновление сертификата следует в том случае, если политика безопасности вашей организации запрещает использовать ключ электронной подписи, сформированный не вами лично, а на сетевом узле администратора. В результате обновления вам будет доставлен сертификат, который будет соответствовать ключу электронной подписи, сформированному на вашем компьютере.
2. Нажмите кнопку **OK**.

E

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 ОС Windows XP, Server 2003

Для установки поддержки кириллицы на ОС Windows XP, Server 2003 выполните следующие действия:

1. Откройте **Панель управления** (**Control Panel**).
2. Щелкните **Язык и региональные стандарты** (**Regional and Language Options**).
3. В окне **Язык и региональные стандарты** (**Regional and Language Options**) перейдите на вкладку **Дополнительно** (**Advanced**).
4. Далее в списке выберите **Русский** (**Russian**).
5. Установите флажок **Применить эти параметры для текущей учетной записи и для стандартного профиля пользователя** (**Apply all settings to the current user account and to the default user profile**).

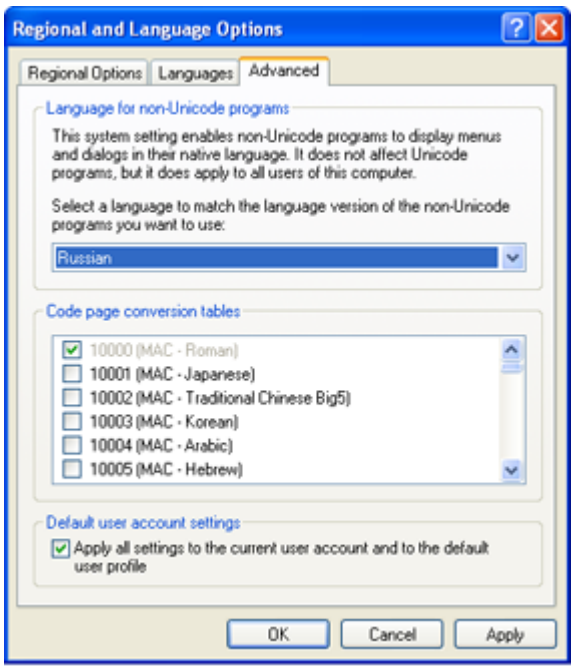


Рисунок 101. Выбор языка для программ, не поддерживающих Юникод, в Windows XP

6. Нажмите кнопку **OK**. Возможно, потребуется перезагрузка.

Региональные настройки в ОС Windows Vista, Server 2008, Windows 7, Server 2008 R2

Для установки поддержки кириллицы на ОС Windows Vista, Server 2008, Windows 7, Server 2008 R2 выполните следующие действия:

1 Откройте **Панель управления** (**Control Panel**) > **Часы, язык и регион** (**Clock, Language, and Region**) > **Язык и региональные стандарты** (**Region and Language**).

2 В окне **Язык и региональные стандарты** (**Region and Language**) перейдите на вкладку **Дополнительно** (**Administrative**).

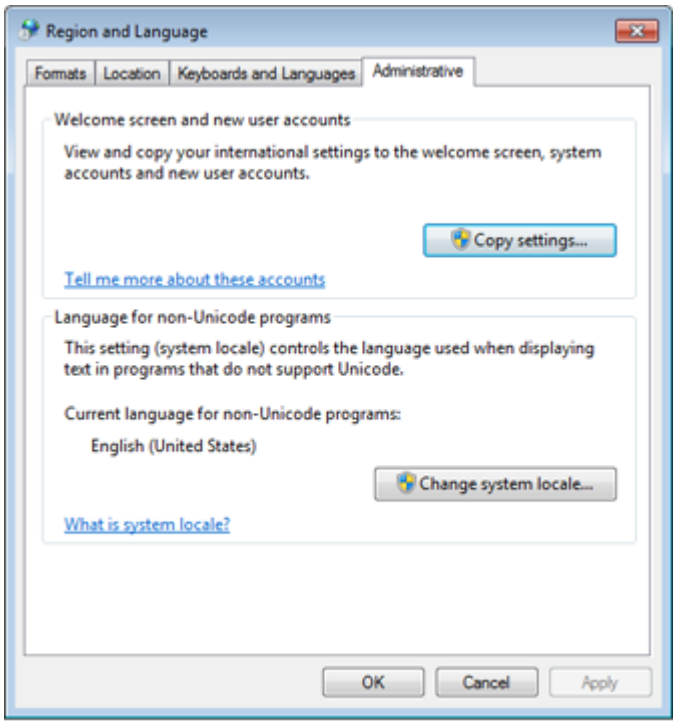


Рисунок 102. Дополнительные языковые параметры

3 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Изменить язык системы** (**Change system locale**).

4 В появившемся окне в списке выберите **Русский (Россия)** (**Russian (Russia)**).

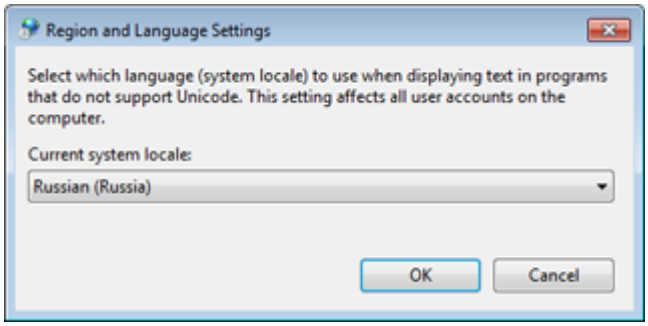


Рисунок 103. Выбор языка системы

5 Нажмите кнопку **OK**. Потребуется перезагрузка.

6 После перезагрузки откройте **Панель управления** (**Control Panel**) > **Часы, язык и регион** (**Clock, Language, and Region**) > **Язык и региональные стандарты** (**Region and Language**).

7 В окне **Язык и региональные стандарты** (**Region and Language**) перейдите на вкладку **Дополнительно** (**Administrative**).

8 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Копировать параметры** (**Copy settings**).

9 В открывшемся окне установите флажок **Экран приветствия и системные учетные записи** (**Welcome screen and system accounts**) и нажмите кнопку **OK**.

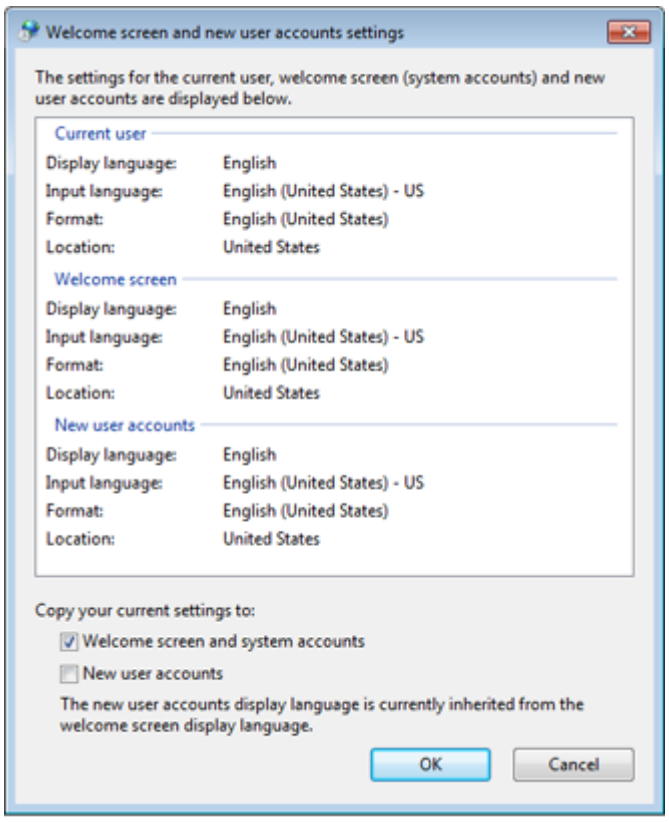


Рисунок 104. Копирование параметров

Также для исключения проблем с кодировкой в некоторых системах мы рекомендуем выполнить следующие действия:

1 В окне **Язык и региональные стандарты** (**Region and Language**) на вкладке **Форматы** (**Formats**) в списке **Формат** (**Format**) выберите **Русский (Россия)** (**Russian (Russia)**).

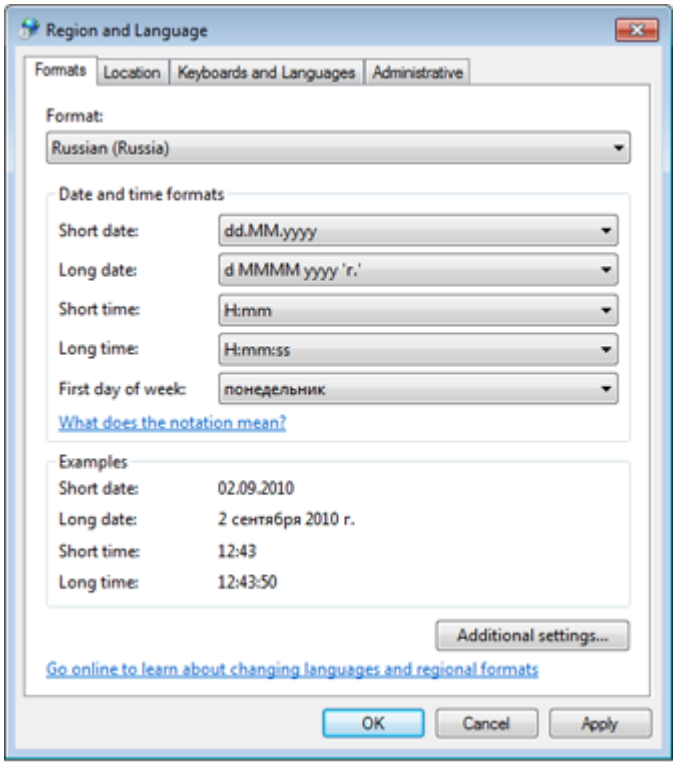


Рисунок 105. Настройка форматов

2 В окне **Язык и региональные стандарты** (**Region and Language**) на вкладке **Расположение** (**Location**) в списке **Текущее расположение** (**Current location**) выберите **Россия**.

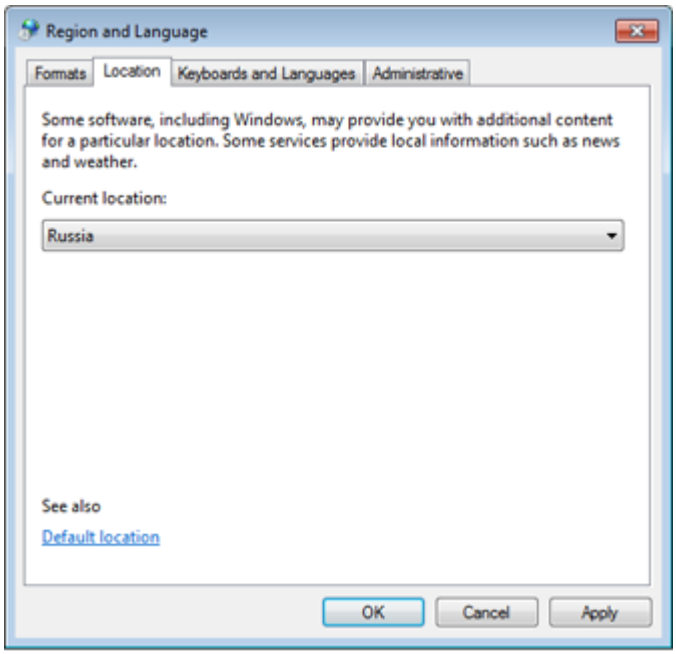


Рисунок 106. Выбор текущего расположения

F

Глоссарий

Active Directory (AD)

Служба каталогов, разработанная Microsoft для доменных сетей Windows. Эта служба интегрирована в большинство операционных систем Windows Server.

Active Directory является центром администрирования и обеспечения безопасности сети. Она служит для аутентификации и авторизации всех пользователей и компьютеров внутри сети доменного типа Windows. При помощи Active Directory задаются и применяются политики безопасности для всех компьютеров в сети, а также устанавливается или обновляется программное обеспечение на компьютерах сети. Active Directory хранит данные и настройки среды в централизованной базе данных.

CMS (Cryptographic Message Syntax)

Стандарт криптографической защиты сообщений, разработанный сообществом IETF (Internet Engeneering Task Force — Инженерный Совет Интернета). CMS может использоваться для подписи, аутентификации или шифрования электронных данных любого типа.

CMS основан на формате PKCS#7, который, в свою очередь, основан на стандарте PEM (Privacy Enhanced Mail). Спецификация на последнюю версию CMS (2009 г.) представлена в RFC 5652.

CMS используется как основной криптографический компонент во многих других криптографических стандартах, таких как S/MIME, PKCS#12 и других.

PKI (инфраструктура открытых ключей)

От англ. 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.

ViPNet Administrator

Набор программного обеспечения для администрирования сети ViPNet, включающий в себя серверное и клиентское приложения ViPNet Центр управления сетью, а также программу ViPNet Удостоверяющий и ключевой центр.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Администратор УКЦ формирует и обновляет ключи для сетевых узлов ViPNet, а также управляет сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

ViPNet Центр управления сетью — это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

Администратор ViPNet Registration Point

Лицо, обладающее правом доступа в программу ViPNet Registration Point и отвечающее за регистрацию пользователей ViPNet, формирование запросов на создание дистрибутивов ключей, издание сертификатов, их аннулирование, приостановление и возобновление действия.

Перед отправкой в ViPNet Удостоверяющий и ключевой центр все запросы на сертификаты подписываются ключом действующего администратора ViPNet Registration Point.

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.

Администратор ЦУСа

Лицо, обладающее правом доступа к программе ViPNet Центр управления сетью (ЦУС) и отвечающее за создание и настройку сети ViPNet, создание и рассылку адресных справочников,

обновление ключей, обновление программного обеспечения 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).

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.

Возобновление действия сертификата

Признание сертификата действительным в том случае, если его действие было приостановлено.

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.

Журнал событий

Файл или группа файлов, предназначенных для хранения сведений о событиях программы.

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 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.

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 проверки электронной подписи

Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключ проверки электронной подписи является открытой (не секретной) частью пары асимметричных ключей.

Ключ электронной подписи

Уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ электронной подписи является закрытой (секретной) частью пары асимметричных ключей.

Контейнер ключей

Файл, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

Координатор (ViPNet-координатор)

Сетевой узел, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator или ViPNet Coordinator Linux) или специальный программно-аппаратный комплекс. В рамках сети ViPNet координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Корневой сертификат

Самоподписанный 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.

Маршрутизация

Процесс выбора пути для передачи информации в сети.

Папка ключей пользователя

Папка, в которой находятся ключи пользователя ViPNet.

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.

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.

Пользователь ViPNet

Лицо, которое использует программное обеспечение ViPNet и имеет ключи для работы с ним.

Приостановление действия сертификата

Временное ограничение действия сертификата до истечения его срока действия.

Расширения сертификата ключа проверки электронной подписи

Дополнительные атрибуты сертификата, такие как использование ключа, политики сертификата, базовые ограничения, ограничения имени и другие. Расширение может быть критичным или некритичным. Система, использующая сертификаты, должна отвергать сертификат, если она встретила критичное расширение, которое не в состоянии распознать; однако некритичные расширения могут игнорироваться, если они не распознаются. Каждое расширение сертификата должно иметь соответствующий идентификатор объекта (OID).

Резервный набор персональных ключей (РНПК)

Набор из нескольких запасных персональных ключей, которые администратор УКЦ или ViPNet Network Manager 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.

Роль

Некоторая функциональность сетевого узла, предназначенная для решения целевых и служебных задач сети ViPNet. Роль используется в лицензировании сети с помощью файла лицензии и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

Роли могут иметь атрибуты в виде количественных характеристик и полномочий, которые также влияют на функциональность.

Набор ролей для каждого сетевого узла задается администратором сети ViPNet в программе ViPNet Центр управления сетью.

Сервер-маршрутизатор

Функциональность координатора, обеспечивающая маршрутизацию транспортных конвертов между узлами сети ViPNet.

Сертификат издателя

Сертификат уполномоченного лица 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.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Симметричный ключ

Последовательность битов заданной длины (для алгоритма ГОСТ 28147-89 — 256 битов), 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 были аннулированы или приостановлены администратором удостоверяющего центра и недействительны на момент, указанный в данном списке аннулированных сертификатов.

Справочники и ключи

Справочники, ключи узла и ключи пользователя.

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, использующиеся в одной сети, в адреса и порты, использующиеся в другой.

Транспортный модуль (MFTP)

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

Удостоверяющий центр

В широком смысле, удостоверяющий центр — организация, осуществляющая выпуск сертификатов ключей проверки электронной подписи, а также сертификатов другого назначения. В сетях ViPNet сертификаты выпускаются в программе ViPNet Удостоверяющий и ключевой центр (УКЦ).

В контексте сети ViPNet, термином «Удостоверяющий центр» также обозначается сетевой узел с установленной программой ViPNet Удостоверяющий и ключевой центр.

Центр регистрации

Компонент удостоверяющего центра. Центру регистрации делегируется часть функций удостоверяющего центра: регистрация пользователей, предоставление пользователям сертификатов ключа проверки электронной подписи, изданных в удостоверяющем центре, и выполнение других операций.

Цепочка сертификации

Упорядоченная последовательность сертификатов, соответствующая иерархии издателей этих сертификатов. Сертификат считается действительным, если цепочка сертификации полна (то есть завершается корневым сертификатом) и все входящие в нее сертификаты также действительны.

Шаблон пользователя

Структура данных, содержащая набор соответствующих атрибутов. Используется для заполнения сведений о пользователе при регистрации в программе ViPNet Registration Point.

Шаблон сертификата

Частично заполненная структура, содержащая набор расширений, которые определяют назначение сертификата.

Используется при создании запросов на сертификаты и издании сертификатов.

Электронная подпись

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, который позволяет инициализировать датчик случайных чисел на основе действий пользователя.

Указатель

Л

Н

О

П

Р

С

Т

У

Ф

Ц

Ш

Э