



ViPNet Administrator 4

Быстрый старт

Версия продукта: 4.6.11



© АО «ИнфоТеКС», 2023

ФРКЕ.00109-08 34 01

Версия продукта 4.6.11

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

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

ViPNet[®] является зарегистрированным товарным знаком АО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

АО «ИнфоТеКС»

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

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение.....	5
О документе.....	6
Для кого предназначен документ	6
Соглашения документа.....	6
О программе	7
Обратная связь.....	8
 Глава 1. Краткий обзор комплекта документации	9
 Глава 2. Установка ViPNet Administrator и начало работы.....	12
Последовательность установки	13
Рекомендации по размещению компонентов.....	15
Первый запуск программы ViPNet Центр управления сетью	17
Первый запуск программы ViPNet Удостоверяющий и ключевой центр.....	21
 Глава 3. Обновление с версии 3.2.x до версии 4.x	22
Обновление до версии 4.x: порядок действий	23
Конвертация данных программы ViPNet Центр управления сетью 3.2.x	25
Конвертация данных программы ViPNet Удостоверяющий и ключевой центр 3.2.x	26
Обновление справочников и ключей	27
 Глава 4. Создание новой сети ViPNet.....	28
Создание сети ViPNet: порядок действий.....	29
Создание структуры сети ViPNet с помощью мастера.....	31
Первичная инициализация программы ViPNet Удостоверяющий и ключевой центр	32
Создание дистрибутивов ключей	34
 Глава 5. Создание и изменение сетевых объектов	35
Добавление сетевых объектов.....	36
Добавление сетевого узла	36
Добавление пользователя	37
Изменение свойств сетевых объектов	39
Настройка параметров подключения к сети.....	39
Добавление ролей на сетевой узел	40
Изменение связей между узлами.....	40
Изменение связей между пользователями.....	41

Добавление туннелируемого узла	42
Глава 6. Управление сетью ViPNet	43
Отправка обновления справочников и ключей	44
Отправка обновления программного обеспечения	46
Межсетевое взаимодействие	47
Инициация межсетевого взаимодействия	47
Прием входящей межсетевой информации администратором доверенной сети	48
Прием ответной межсетевой информации	49
Обновление списка аннулированных сертификатов и сертификата администратора.....	51
Приложение А. Термины и сокращения	53



Введение

О документе	6
О программе	7
Обратная связь	8

О документе

В данном документе содержатся краткие указания для начала работы с программным обеспечением **ViPNet Administrator** и приводится описание основных сценариев создания и администрирования сети **ViPNet®**.

Для кого предназначен документ

Настоящий документ предназначен для администраторов сетей **ViPNet**, начинающих работу с программами **ViPNet® Центр управления сетью** и **ViPNet® Удостоверяющий и ключевой центр**. Документ поможет максимально быстро создать и настроить типовую **сеть ViPNet** без необходимости изучения дополнительной информации.

Более подробное описание этапов создания сети **ViPNet** и ее настройки можно получить в документах «**ViPNet Центр управления сетью. Руководство администратора**» и «**ViPNet Удостоверяющий и ключевой центр. Руководство администратора**».

Если ранее вами уже была создана сеть **ViPNet** с помощью программного обеспечения **ViPNet Administrator 3.2.x**, то подробную информацию о переходе на **ViPNet Administrator** версии 4.x см. в документе «**ViPNet Administrator. Руководство по обновлению с версии 3.2.x до версии 4.x**».

Соглашения документа

Обозначение	Описание
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская ее, нажмите вторую
Меню > Команда	Последовательность элементов или действий
Код	Имя файла, путь, фрагмент кода или команда в командной строке

**Примечание.** В документе могут присутствовать снимки интерфейса из предыдущих версий продукта. Поэтому некоторые элементы интерфейса, которые не влияют на понимание текста, могут выглядеть не так, как в продукте.

О программе

ПО ViPNet Administrator® предназначено для администрирования [сетей ViPNet](#) и состоит из двух компонентов:

- [ViPNet Центр управления сетью \(ЦУС\)](#).
- [ViPNet Удостоверяющий и ключевой центр \(УКЦ\)](#).

Программа ViPNet Центр управления сетью предназначена для формирования структуры защищенной сети ViPNet, настройки параметров сетевых узлов, регистрации пользователей на сетевых узлах и управления объектами сети.

Программа ViPNet Удостоверяющий и ключевой центр предназначена для издания и обслуживания сертификатов ключа проверки электронной подписи. Она выполняет функции удостоверяющего центра и предоставляет ключи для работы в сети ViPNet.

Обратная связь

Контактная информация

- Единый многоканальный телефон:
+7 (495) 737-6192,
8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба поддержки: hotline@infotecs.ru.
Форма для обращения в службу поддержки через сайт.
Телеграм-канал поддержки: t.me/vhd21
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

- [О продуктах ViPNet.](#)
- [О решениях ViPNet.](#)
- [Часто задаваемые вопросы.](#)
- [Форум пользователей продуктов ViPNet.](#)

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

1

Краткий обзор комплекта документации

Данный раздел поможет вам сориентироваться в комплекте документации ViPNet Administrator. В таблице ниже указаны документы и основные сведения, которые в них содержатся.

Таблица 1. Описание комплекта документации

Документ	Сведения
«ViPNet Administrator. Быстрый старт»	Указания для начала работы с программным обеспечением ViPNet Administrator. Основные сценарии создания и администрирования сети ViPNet.
«Развертывание сети под управлением ViPNet Administrator. Руководство администратора»	Общие сведения о сетях ViPNet под управлением программного обеспечения ViPNet Administrator. Рекомендации по выбору конфигурации сети ViPNet. Руководство по развертыванию типовой сети ViPNet.
«ViPNet Administrator. Руководство по обновлению с версии 3.2.x до версии 4.x»	Инструкция по обновлению программного обеспечения ViPNet с версии 3.2.x до версии 4.x. Информация о возможных проблемах при обновлении программного обеспечения ViPNet Administrator и способах их решения.
«ViPNet Administrator. Руководство по установке»	Описание состава программного обеспечения ViPNet Administrator и возможных схем размещения его компонентов.

Документ	Сведения
	Описание процесса установки и первичной настройки компонентов программного обеспечения ViPNet Administrator. Информация об обновлении программ, входящих в состав программного обеспечения ViPNet Administrator.
«ViPNet Administrator. Руководство по миграции программного обеспечения на другой компьютер»	Описание сценариев миграции рабочего программного обеспечения ViPNet Administrator версии 4.x с одного компьютера на другой.
«ViPNet Центр управления сетью. Руководство администратора»	Подробное описание сценариев работы администратора сети ViPNet с программой ViPNet Центр управления сетью, в том числе: • создание сети ViPNet, • управление структурой сети ViPNet, • настройка параметров сетевых объектов, • организация межсетевого взаимодействия.
«ViPNet Удостоверяющий и ключевой центр. Руководство администратора»	Подробное описание сценариев работы администратора сети ViPNet с программой ViPNet Удостоверяющий и ключевой центр, в том числе: • режимы работы в программе, • управление ключевой структурой ViPNet, • изменение свойств объектов сети, • управление сертификатами, • организация межсетевого взаимодействия, • установление доверительных отношений с другими удостоверяющими центрами.
«ViPNet Administrator. Руководство по смене мастер-ключей в сети ViPNet»	Описание действий администратора сети ViPNet при смене мастер-ключей в сети ViPNet под управлением программного обеспечения ViPNet Administrator версий 3.2 и 4.6.
«ViPNet CSP. Руководство пользователя»	Информация о криптопровайдере ViPNet CSP и основных сценариях работы с ним.
«Печать сертификатов. Приложение к документации ViPNet»	Рекомендации для печати сертификатов в программе ViPNet Удостоверяющий и ключевой центр.
«Новые возможности ViPNet Administrator. Приложение к документации ViPNet»	Описание новых функциональных возможностей программного обеспечения ViPNet Administrator 4.x по сравнению с 3.2.x.

Документ	Сведения
«ViPNet Administrator. Лицензионные соглашения на компоненты сторонних производителей»	Лицензионные соглашения на компоненты сторонних производителей, которые использовались при разработке ПО для ViPNet Administrator.

2

Установка ViPNet Administrator и начало работы

Последовательность установки	13
Рекомендации по размещению компонентов	15
Первый запуск программы ViPNet Центр управления сетью	17
Первый запуск программы ViPNet Удостоверяющий и ключевой центр	21

Последовательность установки

Для развертывания ПО ViPNet Administrator выполните все действия из приведенного ниже списка.

Таблица 2. Последовательность установки ПО ViPNet Administrator

Действие	Ссылка
☐ Продумайте схему развертывания ПО ViPNet Administrator 4.x, включая: • расположение серверного приложения ViPNet Центр управления сетью с базой данных; • количество и местоположение узлов с клиентскими приложениями ViPNet Центр управления сетью; • расположение программы ViPNet Удостоверяющий и ключевой центр.	Рекомендации по размещению компонентов
☐ Подготовьте нужное количество компьютеров и организуйте их подключение к физической сети.	
☐ Убедитесь, что располагаете файлом лицензии *.itcslic или infotecs.reg.	
☐ Выполните установку серверного приложения ViPNet Центр управления сетью на компьютере, который будет выполнять функции Центра управления сетью.	«ViPNet Administrator. Руководство по установке», раздел «Установка серверного приложения ViPNet Центр управления сетью»
☐ Установите клиентское приложение ViPNet Центр управления сетью на всех компьютерах, с которых будет осуществляться управление структурой сети ViPNet.	«ViPNet Administrator. Руководство по установке», раздел «Установка клиентского приложения ViPNet Центр управления сетью»
☐ Установите программу ViPNet Удостоверяющий и ключевой центр.	«ViPNet Administrator. Руководство по установке», раздел «Установка программы ViPNet Удостоверяющий и ключевой центр»
☐ Выполните первый запуск клиентского приложения ViPNet Центр управления сетью. Сформируйте структуру новой сети либо загрузите структуру существующей сети.	Первый запуск программы ViPNet Центр управления сетью
☐	Первый запуск программы ViPNet Удостоверяющий и ключевой центр Создание сети ViPNet: порядок действий

Выполните первый запуск программы ViPNet Удостоверяющий и ключевой центр. Настройте новую базу данных либо импортируйте базу данных программы ViPNet Удостоверяющий и ключевой центр 3.2.x.

[Обновление с версии 3.2.x до версии 4.x](#)

- Установите ПО ViPNet Client, необходимое для отправки данных на сетевые узлы, на компьютер с серверным приложением ViPNet Центр управления сетью.

«ViPNet Client Монитор. Руководство пользователя», раздел «Установка ПО ViPNet Client»

Также установите данное ПО на компьютеры с клиентскими приложениями ViPNet Центр управления сетью и программой ViPNet Удостоверяющий и ключевой центр.

[Рекомендации по размещению компонентов](#)

Рекомендации по размещению компонентов

Существует две основных схемы размещения компонентов ViPNet Administrator:

- Установка всех компонентов ViPNet Administrator на одном компьютере.

Данная схема является наиболее простой и подходит для небольших сетей с одним администратором, работающим и с ЦУСом, и с УКЦ.



Рисунок 1. Установка серверного приложения ЦУСа и УКЦ на одном компьютере

- Установка компонентов ViPNet Administrator на разных компьютерах.

Данная схема удобна в том случае, если в организации уже развернут SQL-сервер и планируется, что база данных ViPNet Administrator будет размещаться на нем.



Рисунок 2. Установка серверного приложения ЦУСа и УКЦ на двух разных компьютерах

Клиентское приложение ViPNet Центр управления сетью можно устанавливать на любой компьютер или несколько компьютеров, если в организации будет несколько администраторов, которые будут управлять сетью ViPNet с разных рабочих мест.



Рисунок 3. Варианты установки приложений ЦУСа

Для обмена данными с узлами сети ViPNet на компьютер с серверным приложением ViPNet Центр управления сетью в обязательном порядке устанавливается программное обеспечение ViPNet Client. Также данное ПО необходимо установить на все клиенты вашей сети и на узел с программой ViPNet Удостоверяющий и ключевой центр.

Подробнее о схемах размещения ПО ViPNet Administrator и использовании дополнительного ПО ViPNet см. в документе «ViPNet Administrator. Руководство по установке», в главе «Общие сведения».

Первый запуск программы ViPNet Центр управления сетью

Чтобы начать работу с программой ViPNet Центр управления сетью, выполните следующие действия:

- 1 Запустите клиентское приложение программы ViPNet Центр управления сетью. Для этого на начальном экране откройте список приложений и выберите **ViPNet > Центр управления сетью**.



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

Если серверное и клиентское приложения ЦУСа установлены на одном компьютере, то подключение к базе данных будет выполнено автоматически. Если серверное и клиентское приложения установлены на разных компьютерах, появится окно **ViPNet Центр управления сетью** с сообщением о невозможности установить соединение с сервером.

Для установления соединения с SQL-сервером укажите DNS-имя или IP-адрес компьютера с серверным приложением в соответствующем поле и нажмите кнопку **Продолжить**.

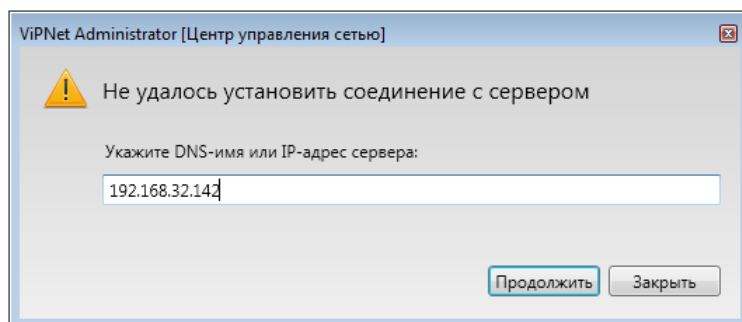


Рисунок 4. Сообщение при отсутствии соединения с SQL-сервером

- 2 В появившемся окне введите имя и пароль администратора и нажмите кнопку **Продолжить**. При первом запуске следует указать имя `Administrator` и пароль `Administrator`.

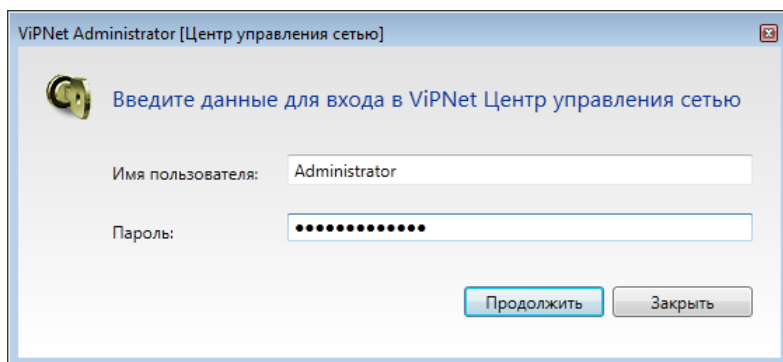


Рисунок 5. Ввод данных администратора для входа в программу ViPNet Центр управления сетью

- 3 После загрузки программы будет предложено сменить пароль.

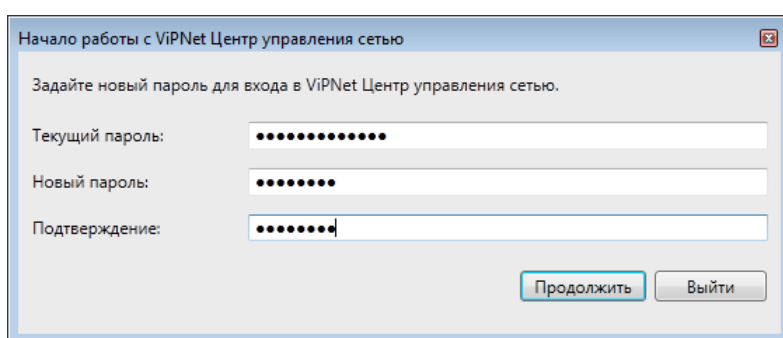


Рисунок 6. Смена пароля администратора ViPNet Центр управления сетью

Чтобы сменить пароль, введите текущий пароль (Administrator) и новый пароль, затем нажмите кнопку **Продолжить**.

- 4 В окне **Начало работы с ViPNet Центр управления сетью** с помощью кнопки **Обзор** укажите путь к файлу лицензии на сеть ViPNet (*.itcslic или infotecs.reg) и нажмите кнопку **Продолжить**.

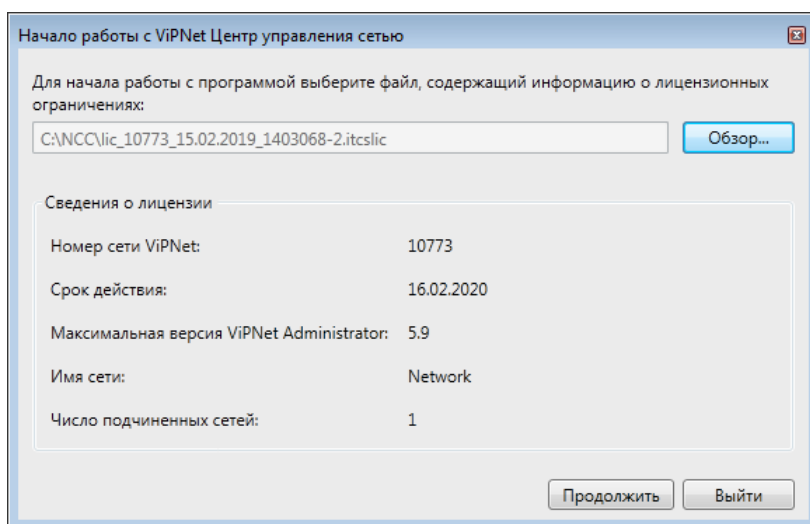


Рисунок 7. Указание пути к файлу лицензии

- 5 В появившемся окне выберите один из возможных сценариев работы в программе:

- **Сформировать структуру защищенной сети автоматически** для создания сети ViPNet с помощью мастера. При выборе данного варианта будет запущен мастер создания сети ViPNet (см. [Создание структуры сети ViPNet с помощью мастера](#)).
- **Загрузить структуру существующей сети** для конвертации сети ViPNet, которая ранее находилась под управлением программы ViPNet Центр управления сетью 3.2.x. При выборе данного варианта будет запущена программа конвертации данных (см. [Конвертация данных программы ViPNet Центр управления сетью 3.2.x](#)).
- **Настроить структуру защищенной сети самостоятельно** для запуска программы ViPNet Центр управления сетью с базой данных, не содержащей объектов сети ViPNet. В результате появится главное окно программы.

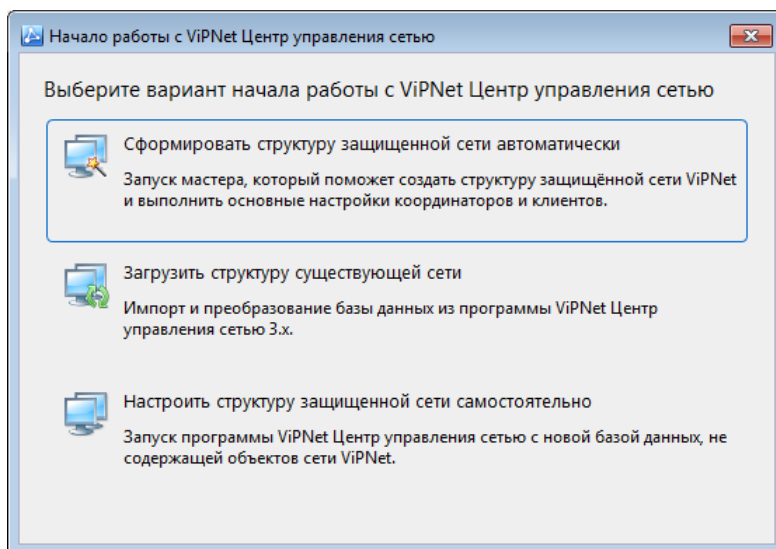


Рисунок 8. Выбор действия для начала работы с программой ViPNet Центр управления сетью

- 6 При создании новой сети, если ваша лицензия предполагает создание иерархии сетей ViPNet, появится сообщение с предложением распределить лицензионные ограничения между сетями. Подробнее об иерархии сетей ViPNet см. в документе «ViPNet Центр управления сетью. Руководство администратора», в главе «Иерархическая система сетей ViPNet».

В окне сообщения нажмите кнопку **Распределить лицензию**.

- 7 В окне **Распределение лицензий** укажите возможность использования функциональности удостоверяющего центра, задайте количество сертификатов пользователей, одновременно туннелируемых соединений и максимальное количество узлов для каждой роли для своей и подчиненных сетей, затем нажмите кнопку **ОК**.

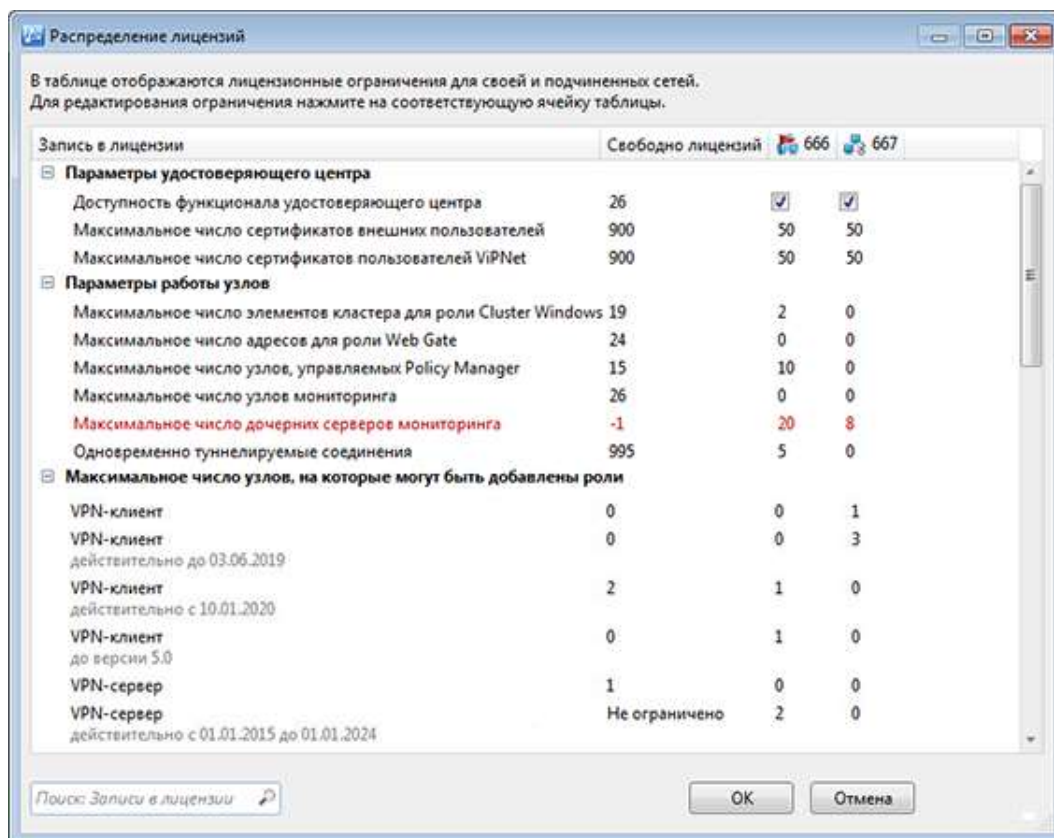


Рисунок 9. Распределение лицензионных ограничений

- 8 В появившемся окне с сообщением об обновлении лицензии нажмите кнопку **Заккрыть**. Теперь вы можете создать структуру сети ViPNet (см. [Создание сети ViPNet: порядок действий](#)).

Первый запуск программы ViPNet Удостоверяющий и ключевой центр

Чтобы начать работу с программой ViPNet Удостоверяющий и ключевой центр, выполните следующие действия:

- 1 Запустите программу ViPNet Удостоверяющий и ключевой центр.



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

- 2 В появившемся окне **Начало работы с программой Удостоверяющий и ключевой центр** выберите:
 - **Настройка новой базы данных** для подключения к базе данных SQL, созданной при установке серверного приложения ViPNet Центр управления сетью, и проведения первичной инициализации программы ViPNet Удостоверяющий и ключевой центр. При выборе данного действия запустится мастер первичной инициализации (см. [Первичная инициализация программы ViPNet Удостоверяющий и ключевой центр](#)).
 - **Импорт базы данных программы Удостоверяющий и ключевой центр версии 3.2.x** для конвертации данных программы ViPNet Удостоверяющий и ключевой центр 3.2.x в случае обновления до версии 4.x. При выборе данного действия запустится мастер конвертации данных (см. [Конвертация данных программы ViPNet Удостоверяющий и ключевой центр 3.2.x](#)).

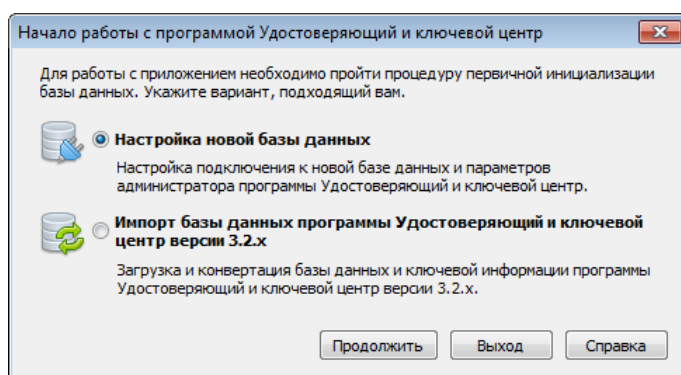


Рисунок 10. Выбор действия для начала работы с программой ViPNet Удостоверяющий и ключевой центр

- 3 При создании новой сети ViPNet или при регистрации новых пользователей на сетевых узлах создайте дистрибутивы ключей для сетевых узлов (см. [Создание дистрибутивов ключей](#)).

3

Обновление с версии 3.2.x до версии 4.x

Обновление до версии 4.x: порядок действий	23
Конвертация данных программы ViPNet Центр управления сетью 3.2.x	25
Конвертация данных программы ViPNet Удостоверяющий и ключевой центр 3.2.x	26
Обновление справочников и ключей	27

Обновление до версии 4.x: порядок действий

При обновлении сети с версии 3.2.x до версии 4.x сохраняются ее структура, настройки, сведения о сетевых объектах и доверенных сетях. Для обновления вам потребуется содержимое папок \NCC и \КС.

Обновление до версии 4.x возможно только с версий 3.2.x. Если же ранее в сети было развернуто ПО ViPNet Administrator версии 3.1.x и ниже, то сначала необходимо выполнить обновление до версии 3.2.x.

Для обновления на ViPNet Administrator с версии 3.2.x до версии 4.6.11:

- 1 Сначала перейдите на версию 4.6.4.

См. порядок обновления ниже. Для конвертации данных УКЦ с 3.2.x до версии 4.6.4 установите криптопровайдер ViPNet CSP версии 4.2.8.51670. Эта версия криптопровайдера входит в инсталлятор ViPNet Удостоверяющий и ключевой центр версии 4.6.4.

- 2 Затем обновите версию 4.6.4 до версии 4.6.11.

См. «ViPNet Administrator. Руководство по установке», раздел «Обновление программного обеспечения ViPNet Administrator».

Для успешного обновления ПО ViPNet Administrator с версии 3.2.x до версии 4.6.7 и ниже выполните все действия из приведенного ниже списка.

Таблица 3. Порядок обновления с версии 3.2.x до версии 4.x

Действие	Ссылка
☐ Убедитесь, что ваша лицензия позволяет установить ПО ViPNet Administrator версии 4.x. При необходимости обновите лицензию.	«ViPNet Administrator. Руководство по обновлению с версии 3.2.x до версии 4.x», раздел «Обновление лицензии на сеть ViPNet»
☐ Продумайте схему развертывания ПО ViPNet Administrator 4.x и выполните установку его компонентов.	Последовательность установки
☐ Обновите программное обеспечение ViPNet Client и ViPNet Coordinator до версии 4.x на всех клиентах и координаторах сети.	«ViPNet Administrator. Руководство по обновлению с версии 3.2.x до версии 4.x», раздел «Особенности обновления ПО ViPNet Client (Coordinator) до версии 4.x»
☐ Проведите конвертацию данных программы ViPNet Центр управления сетью версии 3.2.x.	Конвертация данных программы ViPNet Центр управления сетью 3.2.x

- | | |
|--|---|
| ☐ Проведите конвертацию данных программы ViPNet Удостоверяющий и ключевой центр версии 3.2.x. | Конвертация данных программы ViPNet Удостоверяющий и ключевой центр 3.2.x |
| ☐ Проверьте корректность выполненного обновления. | «ViPNet Administrator. Руководство по обновлению с версии 3.2.x до версии 4.x», раздел «Проверка корректности обновления» |
| ☐ В случае успешного обновления отправьте справочники и ключи на сетевые узлы. | Обновление справочников и ключей |
| ☐ Если в программе ViPNet Центр управления сетью 3.2.x было установлено межсетевое взаимодействие , после успешного обновления отправьте межсетевую информацию в доверенные сети. | |

Конвертация данных программы ViPNet Центр управления сетью 3.2.x

Чтобы конвертировать данные программы ViPNet Центр управления сетью 3.2.x, выполните следующие действия:

- 1 Запустите клиентское приложение ViPNet Центр управления сетью 4.x (см. [Первый запуск программы ViPNet Центр управления сетью](#)).

- 2 В окне **Начало работы с ViPNet Центр управления сетью** выберите вариант **Загрузить структуру существующей сети**.

Будет запущена программа конвертации данных. При необходимости программу конвертации также можно запустить из главного окна программы ViPNet Центр управления сетью (меню **Моя сеть > Загрузить структуру сети ViPNet**).

- 3 Выполните конвертацию данных программы ViPNet Центр управления сетью 3.2.x, указав путь к папке \NCC и следуя указаниям программы конвертации.

Подробное описание процесса конвертации данных программы ViPNet Центр управления сетью 3.2.x см. в документе «ViPNet Administrator. Руководство по обновлению с версии 3.2.x до версии 4.x», в разделе «Конвертация данных Центра управления сетью 3.2.x».

- 4 После успешной конвертации данных в программе ViPNet Центр управления сетью выполните настройку конфигурации сконвертированной сети (см. [Создание и изменение сетевых объектов](#)).

В результате вы сможете работать в программе ViPNet Центр управления сетью 4.x с ранее созданной структурой сети ViPNet.

Конвертация данных программы ViPNet Удостоверяющий и ключевой центр 3.2.x

Чтобы конвертировать данные программы ViPNet Удостоверяющий и ключевой центр 3.2.x, выполните следующие действия:

- 1 Запустите программу ViPNet Удостоверяющий и ключевой центр 4.x (см. [Первый запуск программы ViPNet Удостоверяющий и ключевой центр](#)).
- 2 В появившемся окне установите переключатель в положение **Импорт базы данных программы Удостоверяющий и ключевой центр версии 3.2.x** и нажмите кнопку **Продолжить**.
Будет запущен мастер конвертации данных.
- 3 С помощью мастера выполните конвертацию данных программы ViPNet Удостоверяющий и ключевой центр 3.2.x, указав путь к папке \КС.



Примечание. Если программа УКЦ версии 3.2.x была установлена на другом компьютере, то предварительно подготовьте данные УКЦ 3.2.x для конвертации с помощью утилиты `copy_kc_for_convert_kca4.cmd`. Подробнее см. документ «ViPNet Administrator. Руководство по обновлению с версии 3.2.x до версии 4.x», раздел «Перенос данных УКЦ 3.2.x при помощи специальной утилиты».

Подробное описание процесса конвертации данных программы ViPNet Удостоверяющий и ключевой центр 3.2.x см. в документе «ViPNet Administrator. Руководство по обновлению с версии 3.2.x до версии 4.x», в разделе «Конвертация данных Удостоверяющего и ключевого центра 3.2.x».

В результате вы сможете работать в программе ViPNet Удостоверяющий и ключевой центр 4.x с ранее созданной структурой сети ViPNet.

Обновление справочников и ключей

После успешного обновления ПО требуется отправить на сетевые узлы справочники и ключи. Для этого выполните следующие действия:

- 1 В программе ViPNet Центр управления сетью сформируйте справочники.
- 2 В программе ViPNet Удостоверяющий и ключевой центр сформируйте новые ключи узлов.
- 3 С помощью ЦУСа отправьте сформированные справочники и ключи узлов на все узлы вашей сети ViPNet (см. [Отправка обновления справочников и ключей](#)).
- 4 Если до обновления в ЦУСе было установлено межсетевое взаимодействие, то создайте межсетевую информацию, которая содержит новые справочники и ключи узлов, и отправьте ее в доверенные сети (см. [Межсетевое взаимодействие](#)).

В результате после обновления ПО до версии 4.x сетевые узлы смогут устанавливать защищенные соединения друг с другом.

4

Создание новой сети ViPNet

Создание сети ViPNet: порядок действий	29
Создание структуры сети ViPNet с помощью мастера	31
Первичная инициализация программы ViPNet Удостоверяющий и ключевой центр	32
Создание дистрибутивов ключей	34

Создание сети ViPNet: порядок действий

Чтобы создать новую сеть ViPNet, сформируйте ее структуру, настройте [сетевые объекты](#), создайте справочники и дистрибутивы ключей для сетевых узлов. Для этого выполните действия из приведенного ниже списка.

Таблица 4. Порядок создания сети ViPNet с помощью ПО ViPNet Administrator

Действие	Ссылка
☐ Создайте первоначальную структуру сети ViPNet с помощью мастера Создание сети ViPNet . Перед созданием сети ViPNet вы можете настроить параметры добавления сетевых узлов по умолчанию в меню Сервис > Параметры .	Создание структуры сети ViPNet с помощью мастера «ViPNet Центр управления сетью. Руководство администратора», раздел «Настройка параметров программы по умолчанию»
☐ Выполните первичную инициализацию программы ViPNet Удостоверяющий и ключевой центр.	Первичная инициализация программы ViPNet Удостоверяющий и ключевой центр
☐ Если требуется, для созданных узлов настройте параметры подключения к сети. При необходимости для клиентских узлов измените сервер IP-адресов .	Настройка параметров подключения к сети
☐ Если требуется, выполните настройки туннелирования на координаторах.	Добавление туннелируемого узла
☐ Если на некоторых узлах предусмотрена работа нескольких пользователей, создайте на таких узлах дополнительных пользователей.	Добавление пользователя
☐ При необходимости измените связи между узлами и пользователями.	Изменение связей между узлами Изменение связей между пользователями
☐ При необходимости измените роли узлов, добавленные на них в процессе создания сети.	Добавление ролей на сетевой узел
☐ Сформируйте справочники для сетевых узлов.	
☐ Создайте дистрибутивы ключей пользователей.	Создание дистрибутивов ключей

Действие	Ссылка
☐ На сетевых узлах установите ПО ViPNet и дистрибутивы ключей.	См. раздел «Установка и удаление программы» в документах: «ViPNet Client for Windows. Руководство пользователя» «ViPNet Coordinator for Windows. Руководство администратора»



Примечание. Настройки сетевых объектов, указанные в списке, не являются обязательными и в каждом случае производятся индивидуально. Их выполнение зависит от требований и условий, которые предъявляются к создаваемой сети ViPNet.

В результате будет создана и настроена сеть ViPNet. После развертывания дистрибутивов ключей на сетевых узлах сеть начнет функционировать, и вы сможете использовать ПО ViPNet для защиты информации на этих узлах, а также управлять сетью ViPNet с помощью программ ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр (см. [Управление сетью ViPNet](#)).

Создание структуры сети ViPNet с помощью мастера

Чтобы сформировать структуру защищенной сети и выполнить первичную настройку ее параметров с помощью мастера **Создание сети ViPNet**, выполните следующие действия:

- 1 Запустите мастер создания сети. Для этого в программе ViPNet Центр управления сетью в меню **Моя сеть** выберите пункт **Создать сеть ViPNet**. Следуйте указаниям мастера создания сети.
- 2 На странице **Координаторы защищенной сети ViPNet** укажите количество координаторов в сети и маску, по которой будут формироваться их имена. Также задайте роли, которые будут добавлены на координаторы при их создании. Если требуется, для роли «CryptoService» измените [уровень полномочий](#).
- 3 На странице **Клиенты защищенной сети ViPNet** укажите количество клиентских узлов, регистрируемых на каждом координаторе, маску их имени и роли, которые будут добавлены на них. Если требуется, для некоторых ролей измените уровень полномочий.
- 4 На странице **Связи между объектами защищенной сети ViPNet** выберите один из типов связей между узлами создаваемой сети. Для организации связи между пользователями связанных узлов установите соответствующий флажок. Данные связи позволят пользователям вести конфиденциальную переписку в программе ViPNet Деловая почта.
- 5 Чтобы удалить ранее созданную структуру сети ViPNet и учетные записи администраторов УКЦ, в окне с сообщением о создании новой защищенной сети установите флажок **Удалить структуру ранее созданной сети**, после чего нажмите кнопку **Создать сеть**.
- 6 На последней странице нажмите кнопку **Готово**, чтобы завершить работу мастера.

В результате в программе ViPNet Центр управления сетью будет сформирована первичная структура защищенной сети, на каждом сетевом узле будет создано по одному пользователю, первый созданный клиентский узел будет зарегистрирован как Центр управления сетью . Независимо от выбора типа связи, клиенты будут связаны со своими координаторами, между всеми координаторами будут образованы межсерверные каналы, все клиенты и координаторы будут связаны с узлом, на котором установлен Центр управления сетью.

Подробное описание мастера создания сети ViPNet представлено в документе «ViPNet Центр управления сетью. Руководство администратора», в главе «Начало работы с программой ViPNet Центр управления сетью», в разделе «Создание структуры сети ViPNet с помощью мастера».

Первичная инициализация программы ViPNet Удостоверяющий и ключевой центр

Если конвертация данных программы ViPNet Удостоверяющий и ключевой центр версии 3.2.x не требуется, при первом запуске программы ViPNet Удостоверяющий и ключевой центр 4.x следует провести первичную инициализацию, во время которой будет настроено подключение к базе данных SQL и создана учетная запись администратора УКЦ. Для этого выполните следующие действия:

- 1 Запустите программу ViPNet Удостоверяющий и ключевой центр (см. [Первый запуск программы ViPNet Удостоверяющий и ключевой центр](#)).
- 2 В появившемся окне установите переключатель в положение **Настройка новой базы данных** и нажмите кнопку **Продолжить**. Будет запущен мастер первичной инициализации.
- 3 Появится электронная рулетка, если она еще не запускалась в рамках текущего сеанса работы программы. Следуйте указаниям в окне **Электронная рулетка**.

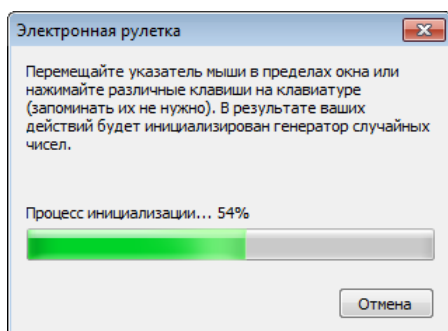


Рисунок 11. Запуск электронной рулетки

- 4 В мастере настройте подключение к базе данных SQL. Для этого на страницах **Подключение к базе данных ViPNet Administrator** оставьте настройки по умолчанию, а именно:
 - 4.1 SQL-сервер — `.\winccsql`, имя базы данных — `ViPNetAdministrator`.
 - 4.2 Режим аутентификации по имени и паролю пользователя SQL-сервера, имя пользователя — `KcaUser`, пароль — `Number1`.
- 5 Следуя указаниям мастера, создайте учетную запись администратора УКЦ и, если в вашей лицензии доступна функциональность удостоверяющего центра, укажите информацию, необходимую для издания сертификата администратора.
- 6 На страницах **Автоматический режим работы** при необходимости настройте параметры работы УКЦ в автоматическом режиме.

Подробную информацию о первичной инициализации см. в документе «ViPNet Administrator. Руководство по установке», в соответствующем разделе «Первичная инициализация программы ViPNet Удостоверяющий и ключевой центр».

После успешной инициализации появится главное окно программы, и вы сможете начать работу с программой ViPNet Удостоверяющий и ключевой центр.

Создание дистрибутивов ключей

При создании новой сети ViPNet или при регистрации новых пользователей на сетевых узлах необходимо сформировать дистрибутивы ключей для пользователей в программе ViPNet Удостоверяющий и ключевой центр. С помощью дистрибутива ключей производится развертывание узла, на котором зарегистрирован пользователь сети ViPNet.

Перед тем как создавать дистрибутивы ключей рекомендуется настроить параметры их создания в окне **Сервис > Настройка** в разделе **Дистрибутивы ключей**.

Чтобы создать дистрибутив ключей для пользователя, выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр выберите представление **Ключевой центр** и на панели навигации перейдите в раздел **Моя сеть > Сетевые узлы**.
- 2 В списке сетевых узлов на панели просмотра выберите узел пользователя (или несколько узлов), для которого требуется создать дистрибутив.
- 3 Щелкните узел правой кнопкой мыши и в контекстном меню выберите пункт **Выдать новый дистрибутив ключей**.

Будет запущен процесс создания дистрибутивов ключей. Следуйте его указаниям.

- 4 Созданные дистрибутивы ключей будут сохранены в заданную папку. Если была настроена печать паролей, пароль пользователя будет передан на печать.

Подробную информацию о создании дистрибутивов ключей см. в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», в разделе «Работа с дистрибутивами ключей».

- 5 Созданные дистрибутивы ключей и пароли передайте пользователям сети ViPNet любым защищенным способом для их дальнейшей установки на сетевых узлах.

Подробнее об установке дистрибутивов ключей на сетевых узлах см. в документах «ViPNet Client for Windows. Руководство пользователя» и «ViPNet Coordinator for Windows. Руководство администратора», в разделе «Установка и удаление программы».



5

Создание и изменение сетевых объектов

Добавление сетевых объектов	36
Изменение свойств сетевых объектов	39

Добавление сетевых объектов

В программе ViPNet Центр управления сетью вы можете создавать различные сетевые объекты: сетевые узлы, группы узлов, пользователей либо группы пользователей.

Параметры добавления и удаления сетевых объектов вы можете настроить в меню **Сервис > Параметры** в разделе **Работа с объектами**.

В данном документе рассматривается добавление в сеть ViPNet:

- Сетевых узлов (см. [Добавление сетевого узла](#)).
- Пользователей (см. [Добавление пользователя](#)).

О добавлении групп узлов и групп пользователей см. в документе «ViPNet Центр управления сетью. Руководство администратора», в разделах «Работа с группами узлов» и «Работа с группами пользователей».

Добавление сетевого узла

Чтобы добавить в сеть ViPNet новый координатор или клиент, выполните следующие действия:

- 1 В окне **ViPNet Центр управления сетью** в представлении **Моя сеть** выберите раздел **Координаторы** или **Клиенты**.
- 2 На панели просмотра в разделе **Координаторы** или **Клиенты** нажмите кнопку **+**.
- 3 В окне **Новый координатор** или **Новый клиент** выполните следующие действия:
 - 3.1 В соответствующее поле введите имя координатора или клиента.
 - 3.2 При создании клиента в поле **Координатор** с помощью кнопки **Выбрать** укажите координатор, на котором требуется зарегистрировать новый клиент.
 - 3.3 Чтобы создать пользователя для координатора или клиента, установите флажок **Создать одноименного пользователя на новом узле автоматически**.
 - 3.4 Нажмите кнопку **Создать**.
- 4 Для созданного сетевого узла выполните следующие настройки:
 - Добавьте на сетевой узел роли (см. [Добавление ролей на сетевой узел](#)).
 - Создайте связи с другими сетевыми узлами (см. [Изменение связей между узлами](#)).
 - Добавьте на сетевой узел одного или несколько пользователей (см. [Добавление пользователя](#)).
 - Настройте параметры подключения сетевого узла к сети (см. [Настройка параметров подключения к сети](#)).
- 5 При создании координатора дополнительно выполните следующие настройки:

- Создайте межсерверные каналы для обмена служебной информацией с другими координаторами.
 - Добавьте на координатор клиенты.
 - При необходимости добавьте адреса туннелируемых соединений (см. [Добавление туннелируемого узла](#)).
- 6 После создания сетевого узла и выполнения необходимых настроек, сформируйте справочники. Для этого нажмите кнопку **Справочники и ключи**  и выберите пункт **Создать справочники**.
- 7 В программе ViPNet Удостоверяющий и ключевой центр создайте дистрибутив ключей для нового сетевого узла (см. [Создание дистрибутивов ключей](#)).
- 8 Если ключи узлов не создаются в автоматическом режиме, создайте их вручную.
- Подробнее о работе в УКЦ см. в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», в главах «Режимы работы в программе ViPNet Удостоверяющий и ключевой центр» и «Управление ключевой структурой ViPNet».

В результате в сеть ViPNet будет добавлен новый координатор или клиент. Теперь установите дистрибутив ключей на новом сетевом узле, на другие сетевые узлы отправьте обновление ключей и справочников (см. [Отправка обновления справочников и ключей](#)). Об установке дистрибутива ключей на координаторе или клиенте см. в документе «ViPNet Coordinator for Windows. Руководство администратора» или «ViPNet Client for Windows. Руководство пользователя», в разделе «Установка и удаление программы».

Добавление пользователя

Чтобы добавить нового пользователя сети ViPNet, выполните следующие действия:

- 1 В окне **ViPNet Центр управления сетью** в представлении **Моя сеть** выберите раздел **Пользователи**.
- 2 На панели просмотра нажмите кнопку .
- 3 В окне **Новый пользователь** выполните следующие действия:
 - 3.1 В соответствующее поле введите имя пользователя.
 - 3.2 Если требуется, в поле **Сетевой узел** с помощью кнопки **Выбрать** укажите узел, на который требуется добавить нового пользователя.
 Добавить созданного пользователя на сетевой узел можно позже в окне свойств пользователя или в окне свойств узла.
 - 3.3 Нажмите кнопку **Создать**.
- 4 При необходимости добавьте созданного пользователя на сетевые узлы.
- 5 Задайте связи созданного пользователя с другими пользователями и группами пользователей (см. [Изменение связей между пользователями](#)).

В результате в сеть ViPNet будет добавлен новый пользователь. Если новый пользователь не был добавлен на сетевой узел или нужно изменить список сетевых узлов пользователя, добавьте этого пользователя на нужный сетевой узел следующим образом:

- 1 В окне **ViPNet Центр управления сетью** в представлении **Моя сеть** выберите раздел **Пользователи**.
- 2 На панели просмотра дважды щелкните пользователя, которого требуется зарегистрировать на сетевом узле.
- 3 В окне свойств пользователя на панели навигации выберите раздел **Сетевые узлы**.
- 4 Чтобы добавить сетевой узел в список узлов пользователя или удалить сетевой узел, воспользуйтесь кнопками **Добавить** и **Удалить**.
- 5 Чтобы сохранить настройки, нажмите кнопку **ОК**.

В результате новый пользователь будет зарегистрирован на сетевом узле. Чтобы пользователь смог начать работу, для сетевых узлов, на которые добавлен пользователь, в программе ViPNet Центр управления сетью создайте справочники, в программе ViPNet Удостоверяющий и ключевой центр — дистрибутивы ключей. Затем установите дистрибутивы ключей на этих узлах.

Изменение свойств сетевых объектов

Настройка параметров подключения к сети

Чтобы сетевые узлы могли устанавливать соединения друг с другом, а также при необходимости работать с внешними сетями (например, с Интернетом), следует настроить параметры подключения этих узлов к сети: IP-адреса и DNS-имена узлов и параметры внешнего межсетевого экрана.

Чтобы настроить параметры подключения узла к сети, выполните следующие действия:

- 1 В окне **ViPNet Центр управления сетью** в представлении **Моя сеть** выберите пункт **Координаторы** или **Клиенты**, в зависимости от типа настраиваемого узла.
- 2 На панели просмотра дважды щелкните сетевой узел, который требуется настроить.
- 3 В окне свойств сетевого узла на панели навигации выберите раздел **Адреса во внешних сетях**.
- 4 В соответствующие списки добавьте IP-адреса и DNS-имена сетевого узла.
- 5 При настройке клиента в поле **Сервер IP-адресов** укажите координатор, который будет сервером IP-адресов для клиента.
При настройке координатора сервер IP-адресов указывать не нужно.
- 6 В окне свойств узла на панели навигации выберите раздел **Межсетевой экран**.
- 7 Если подключение к внешней сети осуществляется через межсетевой экран, нажмите кнопку раскрытия списка и выберите тип межсетевого экрана или отключите его использование, если межсетевой экран не используется.
- 8 В зависимости от выбранного типа межсетевого экрана, задайте дополнительные параметры: внешние IP-адреса межсетевого экрана, порт доступа и так далее.
- 9 Если для координатора задано использование межсетевого экрана, из соответствующего списка выберите IP-адрес сетевого адаптера, со стороны которого установлен межсетевой экран.
- 10 При настройке координатора в случае необходимости задайте параметры межсетевого экрана для клиентов, которые используют данный координатор в качестве сервера IP-адресов.
Для этого в окне свойств координатора на левой панели выберите раздел **Межсетевой экран клиентов**. Настройки в этом разделе производятся аналогично настройкам в разделе **Межсетевой экран**.
- 11 Чтобы сохранить настройки, нажмите кнопку **ОК**.
- 12 После выполнения необходимых настроек сформируйте справочники и отправьте их на сетевой узел (см. [Отправка обновления справочников и ключей](#)).

В результате сетевые узлы смогут взаимодействовать друг с другом и с внешними сетями. Подробнее о настройке параметров подключения узлов к сети см. в документе «ViPNet Центр управления сетью. Руководство администратора», в главе «Настройка параметров сетевых узлов».

Добавление ролей на сетевой узел

Роли сетевого узла определяют, какие программы ViPNet могут работать на этом узле и какие задачи узел может выполнять. Некоторые роли имеют свойства, такие как уровень полномочий пользователя сетевого узла.

Чтобы добавить роли для сетевого узла, выполните следующие действия:

- 1 В окне **ViPNet Центр управления сетью** в представлении **Моя сеть** выберите пункт **Координаторы** или **Клиенты**, в зависимости от типа настраиваемого узла.
- 2 На панели просмотра дважды щелкните сетевой узел, на который требуется добавить роли.
- 3 В окне свойств сетевого узла на панели навигации выберите раздел **Роли узла**.
- 4 С помощью кнопок **Добавить** и **Удалить** измените список ролей сетевого узла.
- 5 Чтобы изменить свойства роли, например, изменить уровень полномочий пользователя, дважды щелкните роль или нажмите кнопку **Свойства** и в открывшемся окне выполните необходимые настройки.
- 6 Чтобы сохранить настройки, в окне свойств узла нажмите кнопку **ОК**.
- 7 После изменения ролей сетевого узла сформируйте справочники и отправьте их на этот узел (см. [Отправка обновления справочников и ключей](#)).

В результате сетевые узлы смогут выполнять задачи в соответствии с добавленными ролями. Подробнее о ролях сетевых узлов см. в документе «ViPNet Центр управления сетью. Руководство администратора», в главе «Общие сведения о сетях ViPNet», раздел «Роли сетевых узлов».

Изменение связей между узлами

Связь между двумя сетевыми узлами дает возможность этим узлам установить защищенное соединение друг с другом. Чтобы изменить связи сетевого узла, выполните следующие действия:

- 1 В окне **ViPNet Центр управления сетью** в представлении **Моя сеть** выберите раздел **Координаторы** или **Клиенты**, в зависимости от типа настраиваемого узла.
- 2 На панели просмотра дважды щелкните сетевой узел, связи которого требуется изменить.
- 3 В окне свойств сетевого узла на панели навигации выберите раздел **Связи с узлами**.
- 4 С помощью кнопок **Добавить** и **Удалить** измените список связей сетевого узла.



Примечание. Невозможно удалить связи с узлами, имена которых выделены серым цветом. Эти связи являются обязательными и создаются автоматически.

5 Выполнив необходимые изменения, нажмите кнопку **ОК**.

В результате связи между сетевыми узлами будут изменены. Теперь создайте справочники, в программе ViPNet Удостоверяющий и ключевой центр создайте ключи узлов. Затем отправьте на узлы, связи которых были изменены, справочники и ключи (см. [Отправка обновления справочников и ключей](#)).

Подробнее о связях между сетевыми узлами см. в документе «ViPNet Центр управления сетью. Руководство администратора», в разделе «Изменение связей между сетевыми узлами».

Изменение связей между пользователями

Связь между двумя пользователями, заданная в программе ViPNet Центр управления сетью, позволяет этим пользователям вести конфиденциальную переписку в программе ViPNet Деловая почта, в то время как связь между двумя сетевыми узлами позволяет пользователю одного сетевого узла адресовать зашифрованное сообщение одновременно всем пользователям второго сетевого узла.

Пользователь также может иметь связь с группой пользователей. В этом случае он сможет обмениваться персональными зашифрованными письмами в программе ViPNet Деловая почта с участниками этой группы, если узел пользователя связан с узлами участников группы.

Чтобы изменить связи пользователя, выполните следующие действия:

- 1 В окне **ViPNet Центр управления сетью** в представлении **Моя сеть** выберите раздел **Пользователи**.
- 2 На панели просмотра дважды щелкните запись пользователя, связи которого требуется изменить.
- 3 В окне свойств пользователя на панели навигации выберите раздел **Связи с пользователями**.
- 4 Для добавления связи с определенными пользователями нажмите кнопку **Добавить** и в меню выберите пункт **Связи с пользователями**.
- 5 Чтобы скопировать связи другого пользователя, нажмите кнопку **Добавить** и в меню выберите пункт **Связи по образцу**.
- 6 Для удаления связей с пользователями воспользуйтесь кнопкой **Удалить**.
- 7 Если установлено межсетевое взаимодействие с другими сетями ViPNet, для изменения статуса связи между настраиваемым пользователем своей сети и выбранным пользователем доверенной сети нажмите кнопку **Связи** и выберите в меню нужное действие.



Примечание. При изменении связей между пользователями своей и доверенной сети связи между узлами, на которых они зарегистрированы, будут изменены автоматически.

- 8 Чтобы изменить связи пользователя с группами пользователей, в окне свойств пользователя на панели навигации выберите раздел **Связи с группами пользователей** и выполните действия, аналогичные изменению связей с пользователями.
- 9 Выполнив необходимые изменения, нажмите кнопку **ОК**.

В результате связи между пользователями будут изменены. Подробнее о связях между пользователями сети ViPNet см. в документе «ViPNet Центр управления сетью. Руководство администратора», в разделе «Создание пользователя и настройка его параметров».

Добавление туннелируемого узла

Туннелирование — это шифрование трафика открытых узлов (то есть узлов, на которых не установлены программы ViPNet Client и ViPNet Coordinator) для передачи через публичные сети. Туннелирование осуществляется координаторами.

Чтобы добавить IP-адреса туннелируемых узлов, выполните следующие действия:

- 1 В окне **ViPNet Центр управления сетью** в представлении **Моя сеть** выберите раздел **Координаторы**.
- 2 На панели просмотра дважды щелкните координатор, который будет туннелировать узлы.
- 3 В окне свойств координатора на панели навигации выберите раздел **Туннелирование**.
- 4 В соответствующем поле задайте максимальное число одновременно туннелируемых соединений для настраиваемого координатора.

Если это число равно нулю, координатор не может осуществлять туннелирование.
- 5 С помощью кнопок **Добавить** и **Удалить** измените список туннелируемых IP-адресов.
- 6 Чтобы сохранить настройки, нажмите кнопку **ОК**.

В результате выбранный координатор начнет туннелировать заданные **сетевые узлы**. Подробнее о туннелировании см. в документе «ViPNet Центр управления сетью. Руководство администратора», в разделе «Настройка параметров координатора».

6

Управление сетью ViPNet

Отправка обновления справочников и ключей	44
Отправка обновления программного обеспечения	46
Межсетевое взаимодействие	47
Обновление списка аннулированных сертификатов и сертификата администратора	51

Отправка обновления справочников и ключей

При добавлении, удалении или изменении свойств объектов сети ViPNet требуется отправка информации об изменениях на узлы своей сети ViPNet.

Сведения о необходимости обновления справочников и ключей и их статус указаны в окне программы ViPNet Центр управления сетью в списках клиентов и координаторов в столбце **Справочники и ключи**:

- Статус **Требуется создать** указывает, что необходимо создать справочники.
- Статус **Ожидаются ключи** указывает, что необходимо создать ключи в программе ViPNet Удостоверяющий и ключевой центр.
- Статус **Готовы к отправке** указывает, что необходимо отправить справочники и ключи на сетевой узел.
- Статус **Отправлены** указывает, что справочники и ключи отправлены на сетевой узел.
- Статус **Доставлены** указывает, что справочники и ключи доставлены на сетевой узел.
- Статус **Приняты/Не приняты** указывает, что справочники и ключи были приняты либо не приняты пользователем на сетевом узле.

Справочники и ключи узлов требуется создать при изменении структуры сети, связей между объектами сети либо при обновлении до версии 4.x. Обновления ключей узлов требуется создать при смене пароля администратора узла или группы узлов, при издании сертификата администратора УКЦ, при обновлении списка аннулированных сертификатов либо при получении сертификатов администраторов УКЦ и списков аннулированных сертификатов из доверенных сетей. Подробнее о ключах узлов и обновлениях ключей см. в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», в главе «Управление ключевой структурой ViPNet».

Чтобы отправить обновления справочников и ключей узлов либо новые ключи узлов на сетевые узлы, выполните следующие действия:

- 1 Если требуется, в программе ViPNet Центр управления сетью создайте справочники, нажав на панели инструментов кнопку **Справочники и ключи**  и выбрав пункт **Создать справочники**.
- 2 Если требуется, в программе ViPNet Удостоверяющий и ключевой центр создайте ключи узлов и перенесите их в программу ViPNet Центр управления сетью. Для этого:
 - 2.1 В окне программы ViPNet Удостоверяющий и ключевой центр в представлении **Ключевой центр** выберите раздел **Сетевые узлы**.
 - 2.2 На панели просмотра щелкните правой кнопкой мыши сетевой узел (или узлы), для которых необходимо создать ключи или передать CRL. В контекстном меню выберите пункт **Создать и передать ключи в ЦУС** или пункт **Передать все CRL в ЦУС**.

- 3 В окне программы ViPNet Центр управления сетью на панели инструментов нажмите кнопку **Справочники и ключи**  и выберите пункт **Отправить справочники и ключи**.

В окне **Отправка справочников и ключей** будет отображен список сетевых узлов, для которых есть обновления.

- 4 Чтобы отправить справочники и ключи на все узлы в списке, нажмите кнопку **Отправить на весь список**.
- 5 Чтобы отправить справочники и ключи на определенные узлы, выберите их в списке и нажмите кнопку **Отправить**.

В результате обновления справочников и ключей узлов или новые ключи узлов будут отправлены на выбранные сетевые узлы. Подробнее об отправке обновлений справочников и ключей см. в документе «ViPNet Центр управления сетью. Руководство администратора», в разделе «Отправка обновлений на сетевые узлы».

Отправка обновления программного обеспечения

Чтобы отправить обновление программного обеспечения на сетевые узлы, выполните следующие действия:

- 1 В окне **ViPNet Центр управления сетью** в меню **Моя сеть** выберите пункт **Обновить программное обеспечение на узлах**. Будет запущен мастер обновления программного обеспечения.
- 2 Следуя указаниям мастера, загрузите архив в формате **LZH** с обновлением для программного обеспечения, которое необходимо обновить. Для этого на странице **Выберите обновление для отправки на узлы** нажмите кнопку **Загрузить файл обновления**.
- 3 После того, как будет загружено обновление, выберите программное обеспечение, которое вы хотите отправить, и нажмите кнопку **Далее**.
- 4 Следуя указаниям мастера, выберите сетевые узлы, на которые нужно отправить обновление программного обеспечения, задайте время и дату вступления обновления в действие и отправьте обновление.
- 5 После того как обновление будет отправлено, нажмите кнопку **Готово**.

В результате обновление программного обеспечения будет выслано на выбранные сетевые узлы. Обновление программного обеспечения будет полностью завершено после его вступления в действие на всех выбранных сетевых узлах. Подробнее об обновлении ПО см. в документе «ViPNet Центр управления сетью. Руководство администратора», в разделе «Отправка обновлений на сетевые узлы».

Межсетевое взаимодействие

Межсетевое взаимодействие позволяет устанавливать защищенное соединение между узлами разных сетей ViPNet. Организация межсетевого взаимодействия между двумя сетями состоит из следующих этапов:

- 1 Администратор первой сети ViPNet, инициирующий межсетевое взаимодействие, создает файл с межсетевой информацией и межсетевой мастер-ключ.
- 2 Администратор второй сети ViPNet принимает межсетевую информацию, импортирует межсетевой мастер-ключ, затем создает файл с ответной межсетевой информацией и передает его администратору первой сети.
- 3 Администратор первой сети завершает организацию взаимодействия приемом ответной межсетевой информации.
- 4 Администраторы отправляют на узлы своих сетей обновления справочников и новые ключи узлов.

После этого узлы доверенных сетей, участвующие во взаимодействии, могут устанавливать защищенные соединения друг с другом.



Рисунок 12. Схема настройки межсетевого взаимодействия

Инициация межсетевого взаимодействия

Чтобы инициировать организацию межсетевого взаимодействия:

- 1 В программе ViPNet Центр управления сетью в меню **Доверенные сети** выберите пункт **Установить взаимодействие**. Будет запущен мастер **Установка межсетевого взаимодействия**.
- 2 Следуя указаниям мастера, введите необходимую информацию о сети ViPNet, с которой требуется установить взаимодействие, задайте **шлюзовой координатор** своей сети, выберите узлы и пользователей своей сети для взаимодействия, затем сохраните межсетевую информацию в файл.
- 3 В программе ViPNet Удостоверяющий и ключевой центр выполните следующие действия:
 - 3.1 В представлении **Ключевой центр** в разделе **Межсетевое взаимодействие** выберите сеть, для которой собираетесь создать симметричный межсетевой мастер-ключ, или раздел **Асимметричные мастер-ключи**, если вы хотите организовать связь с несколькими сетями ViPNet. Подробнее см. в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», в разделе «Типы межсетевых мастер-ключей».
 - 3.2 На панели инструментов нажмите кнопку **Создать**.
 - 3.3 При создании асимметричного мастер-ключа появится окно, в котором укажите алгоритм для формирования согласованного ключа и параметры алгоритма, затем нажмите кнопку **Создать мастер-ключ**.
 - 3.4 Экспортируйте созданный межсетевой мастер-ключ. Для этого на панели просмотра щелкните правой кнопкой мыши по нужному мастер-ключу и в контекстном меню выберите пункт **Экспорт**.
 - 3.5 При создании симметричного межсетевого мастер-ключа появится окно **Пароль для экспорта межсетевого мастер-ключа**, в котором введите пароль для сохранения межсетевого мастер-ключа и нажмите кнопку **ОК**.

По умолчанию созданный мастер-ключ будет предложено поместить в папку
C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Export\Master keys.
- 4 Передайте созданный файл с межсетевой информацией, межсетевой мастер-ключ и пароль к нему администратору доверенной сети.

Прием входящей межсетевой информации администратором доверенной сети

Чтобы принять файл с первичной межсетевой информацией и межсетевой мастер-ключ:

- 1 В окне программы ViPNet Центр управления сетью в меню **Доверенные сети** выберите пункт **Установить взаимодействие**. Будет запущен мастер **Установка межсетевого взаимодействия**.
- 2 На первой странице мастера выберите вариант **Я принимаю файл с межсетевой информацией** и нажмите кнопку **Далее**.
- 3 На странице **Загрузка межсетевой информации из файла** укажите файл с межсетевой информацией, полученной от администратора сети ViPNet, который инициировал межсетевое взаимодействие. Затем нажмите кнопку **Установить взаимодействие**.

- 4 Следуя указаниям мастера, выберите шлюзовой координатор своей сети и завершите обработку межсетевой информации.
- 5 В представлении **Доверенные сети** для узлов и пользователей новой доверенной сети задайте связи с пользователями своей сети.



Внимание! Для создания защищенного канала между узлом своей сети и узлом доверенной сети необходимо создать связи между их пользователями (см. [Изменение связей между пользователями](#)).

- 6 В программе ViPNet Удостоверяющий и ключевой центр импортируйте межсетевой мастер-ключ. Для этого:
 - 6.1 В представлении **Ключевой центр** в разделе **Межсетевое взаимодействие** выберите сеть, от которой был получен межсетевой мастер-ключ.
 - 6.2 На панели инструментов нажмите кнопку **Загрузить**.
 - 6.3 При импорте симметричного межсетевого мастер-ключа введите пароль, на котором был зашифрован мастер-ключ.

При импорте асимметричного мастер-ключа будет произведен поиск сертификата администратора доверенной сети, которым был подписан данный ключ. Мастер-ключ будет импортирован только в том случае, если будет найден сертификат администратора.
- 7 В программе ViPNet Центр управления сетью в представлении **Доверенные сети** в разделе **Свойства сетей** создайте межсетевую информацию для новой доверенной сети и сохраните ее в файл.
- 8 Передайте созданный файл администратору доверенной сети.
- 9 После подтверждения связей администратором первой сети, создайте справочники и новые ключи узлов и отправьте их на узлы своей сети (см. [Отправка обновления справочников и ключей](#)).

Прием ответной межсетевой информации

Чтобы принять ответную межсетевую информацию и завершить организацию взаимодействия:

- 1 В окне **Центр управления сетью** в меню **Доверенные сети** выберите пункт **Загрузить межсетевую информацию**. Будет запущен мастер **Загрузка межсетевой информации из файла**.
- 2 С помощью мастера подтвердите связи, предложенные администратором доверенной сети, и загрузите межсетевую информацию.
- 3 Сформируйте и передайте администратору доверенной сети ответную межсетевую информацию с подтвержденными связями.
- 4 Создайте справочники и новые ключи узлов и отправьте их на узлы своей сети (см. [Отправка обновления справочников и ключей](#)).

В результате между вашей и доверенной сетью ViPNet будет установлено межсетевое взаимодействие. Подробная информация об организации межсетевого взаимодействия содержится в документе «ViPNet Центр управления сетью. Руководство администратора», в главе «Межсетевое взаимодействие».

Обновление списка аннулированных сертификатов и сертификата администратора

Если в вашей сети ViPNet используется инфраструктура PKI, каждый администратор УКЦ имеет сертификат ключа проверки электронной подписи (или несколько сертификатов), которым он заверяет издаваемые им сертификаты пользователей. При издании сертификата администратора УКЦ создается список аннулированных сертификатов (далее — CRL), в котором содержится информация об аннулировании или приостановлении действия сертификатов пользователей, изданных данным администратором. Сертификат администратора УКЦ и CRL служат для проверки сертификатов пользователей на сетевых узлах.

Сертификаты администратора и CRL имеют ограниченный срок действия, поэтому их требуется регулярно обновлять и отправлять на сетевые узлы. Срок действия CRL при переиздании задается в программе ViPNet Удостоверяющий и ключевой центр в меню **Сервис > Настройка** в разделе **Сертификаты > Список аннулированных сертификатов**. Срок действия сертификата администратора задается при его издании.

После истечения срока действия ключа электронной подписи администратора необходимо издать новый сертификат. Для этого выполните следующие действия:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в представлении **Администрирование** перейдите в раздел **Моя сеть > Администраторы**.
- 2 На панели просмотра в разделе **Администраторы** выполните одно из действий:
 - Если текущий сертификат администратора УКЦ является **корневым**, щелкните запись текущего администратора правой кнопкой мыши, в контекстном меню выберите **Создать корневой сертификат**. Будет запущен **Мастер создания сертификата администратора сети ViPNet**, следуйте его указаниям.
 - Если сертификат администратора УКЦ издан вышестоящим удостоверяющим центром, щелкните текущего администратора правой кнопкой мыши, в контекстном меню выберите **Создать запрос на кросс-сертификат**. Будет запущен **Мастер создания запроса на кросс-сертификат**, следуйте его указаниям.
- 3 Если сертификат администратора был издан в вышестоящем удостоверяющем центре, то необходимо вручную создать обновления ключей узлов и отправить их на сетевые узлы. Если же сертификат был издан самим администратором УКЦ, то обновления ключей узлов создаются автоматически.
- 4 Если установлено межсетевое взаимодействие с сетями ViPNet, то необходимо обновить межсетевую информацию и отправить ее в доверенные сети.

В результате будет издан новый сертификат администратора УКЦ. Подробнее об обновлении сертификата администратора см. в документе «ViPNet Удостоверяющий и ключевой центр».

Руководство администратора», в разделе «Плановая смена ключа электронной подписи и сертификата администратора».

CRL необходимо обновлять до истечения его срока действия. В случае отсутствия CRL на сетевых узлах будет невозможно удостоверять подлинность сертификатов пользователей сети. Обновление CRL может производиться с определенной периодичностью в автоматическом режиме работы УКЦ, то есть без участия администратора.

Для обновления CRL вручную:

- 1 В окне программы ViPNet Удостоверяющий и ключевой центр в представлении **Администрирование** перейдите в раздел **Изданные сертификаты > Списки аннулированных сертификатов**.
- 2 На панели просмотра щелкните нужный CRL правой кнопкой мыши, в контекстном меню выберите **Обновить**.

В результате CRL будет обновлен. Теперь создайте обновления ключей и отправьте их на сетевые узлы. Подробнее об обновлении CRL см. в документе «ViPNet Удостоверяющий и ключевой центр», в главе «Работа со списками аннулированных сертификатов».



Термины и сокращения

PKI (Public Key Infrastructure)

Инфраструктура открытых ключей — комплекс аппаратных и программных средств, политик и процедур, обеспечивающих доверие к открытым ключам (в том числе ключам проверки электронной подписи) путём издания сертификатов ключей проверки электронной подписи и поддержания 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. Предназначена для формирования и обновления ключей сетевых узлов ViPNet, а также для управления сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

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 Удостоверяющего и ключевого центра;
- задание полномочий пользователей сетевых узлов ViPNet.

Администратор сети ViPNet

Лицо, отвечающее за управление сетью ViPNet, создание и обновление справочников и ключей для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями и обладающее правом доступа к программе ViPNet Центр управления сетью и (или) ViPNet Удостоверяющий и ключевой центр.

Администратор УКЦ

Лицо, обладающее правом доступа к программе ViPNet Удостоверяющий и ключевой центр (УКЦ), отвечающее за создание ключей для сетевых узлов ViPNet, создание и обслуживание сертификатов ViPNet, обеспечение взаимодействия с доверенными сетями ViPNet.

Группа узлов

Множество сетевых узлов ViPNet, объединенное под общим именем для удобства администрирования. Например, позволяет задать единый пароль администратора для всех сетевых узлов ViPNet, входящих в данную группу.

Дистрибутив ключей

Файл с расширением *.dst, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии для первичного запуска и последующей работы программы ViPNet на сетевом узле. Для работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Доверенная сеть

Сеть ViPNet, с узлами которой узлы собственной сети ViPNet осуществляют защищенное взаимодействие.

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.

Ключи узла ViPNet

Совокупность ключей, с использованием которых производится шифрование трафика, служебной информации и писем программы ViPNet Деловая почта.

Координатор (ViPNet-координатор)

Сетевой узел ViPNet, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или программно-аппаратный комплекс. В сети ViPNet-координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Корневой сертификат

Самоподписанный сертификат головного удостоверяющего центра. Используется для подписи сертификатов, издаваемых головным удостоверяющим центром, с целью обеспечения доверия к ним.

Межсетевая информация

Информация о доверенной сети или своей сети, предназначенная для организации или изменения межсетевого взаимодействия. В состав межсетевой информации входят связи между сетевыми объектами, параметры сетевых узлов ViPNet и служебная информация (сертификаты издателей, списки аннулированных сертификатов).

Межсетевое взаимодействие

Информационное взаимодействие, организованное между сетями ViPNet. Позволяет узлам различных сетей ViPNet обмениваться информацией по защищенным каналам. Для организации взаимодействия между узлами различных сетей ViPNet администраторы этих сетей обмениваются межсетевой информацией.

Полномочия пользователя

Разрешения на определенные действия пользователей на сетевом узле ViPNet по изменению настроек некоторых программ ViPNet.

Администратор ЦУСа задает полномочия для всех пользователей сетевого узла ViPNet в свойствах ролей.

Пользователь сети ViPNet

Пользователь, зарегистрированный в ЦУСе сети ViPNet. Администратор сети ViPNet создает для пользователя дистрибутив ключей и пароль пользователя.

Внешний пользователь — пользователь, которому выдан контейнер с ключами подписи, созданный, например, в ПО ViPNet Registration Point.

Внутренний пользователь сети ViPNet — пользователь, зарегистрированный в ЦУСе.

Внутренний пользователь может выступать в роли внешнего, если у него есть право подписи и сертификат ключа проверки электронной подписи.

Роль

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 IP-адресов

Функциональность координатора, обеспечивающая регистрацию, рассылку и предоставление информации о состоянии защищенных узлов.

Сетевой объект

Сетевой узел, пользователь, группа узлов или группа пользователей.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в управляющем ПО.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищенных узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Справочники

Набор файлов, содержащих информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях. Эти файлы формируются в программе ViPNet Центр управления сетью, предназначенной для создания структуры и конфигурирования сети ViPNet.

Туннелирование

Технология для защиты соединений между устройствами локальных сетей, которые связаны через интернет или другие публичные сети. Шифрование трафика устройств выполняется координаторами, установленными на границах локальных сетей.

Туннелируемый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне, но его трафик на потенциально опасном участке сети зашифровывается и расшифровывается на координаторе, за которым он стоит.

Шлюзовой координатор

Координатор, через который осуществляется обмен транспортными конвертами между сетями ViPNet, установившими межсетевое взаимодействие. Шлюзовые координаторы назначаются в ViPNet Administrator каждой сети при организации взаимодействия между двумя различными сетями ViPNet.