



ViPNet Administrator 4

Руководство по установке



© ОАО «ИнфоТеКС», 2019

ФРКЕ.00109-07 90 01

Версия продукта 4.6.7

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 ОАО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

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

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 2 этаж

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

Веб-сайт: <https://infotecs.ru>

Служба технической поддержки: hotline@infotecs.ru

Содержание

Введение.....	5
О документе.....	6
Для кого предназначен документ	6
Соглашения документа.....	6
О программе	8
Системные требования	9
ViPNet Центр управления сетью	9
Серверное приложение	9
Клиентское приложение	10
ViPNet Удостоверяющий и ключевой центр	11
Комплект поставки.....	13
Обратная связь.....	14
 Глава 1. Общие сведения	15
Состав ПО ViPNet Administrator	16
Схемы размещения компонентов ПО ViPNet Administrator.....	17
Установка компонентов ViPNet Administrator на одном компьютере	17
Установка компонентов ViPNet Administrator на разных компьютерах	18
Размещение клиентского приложения ViPNet Центр управления сетью.....	19
Использование ViPNet Client для отправки данных на сетевые узлы	20
Лицензия на сеть ViPNet.....	22
 Глава 2. Установка программного обеспечения ViPNet Administrator	23
Порядок установки компонентов ПО ViPNet Administrator	24
Информация для администратора SQL.....	26
Установка серверного приложения ViPNet Центр управления сетью.....	28
Установка клиентского приложения ViPNet Центр управления сетью	32
Установка программы ViPNet Удостоверяющий и ключевой центр	35
Установка обновлений для стороннего ПО.....	36
 Глава 3. Начало работы	37
Первый запуск программы ViPNet Центр управления сетью	38
Создание дополнительных учетных записей администраторов ЦУСа	41
Первый запуск программы ViPNet Удостоверяющий и ключевой центр.....	43
Первичная инициализация программы ViPNet Удостоверяющий и ключевой центр	44

Глава 4. Обновление программного обеспечения ViPNet Administrator	55
Порядок обновления компонентов ПО ViPNet Administrator	56
Обновление приложений ViPNet Центр управления сетью	57
Обновление программы ViPNet Удостоверяющий и ключевой центр	59
Глава 5. Удаление программного обеспечения ViPNet Administrator	60
Когда требуется удаление компонентов ПО ViPNet Administrator	61
Удаление приложений ViPNet Центр управления сетью	62
Удаление программы ViPNet Удостоверяющий и ключевой центр	63
Приложение А. Возможные неполадки и методы их устранения	64
Не устанавливаются приложения сторонних производителей	64
Невозможно установить серверное или клиентское приложение ЦУСа	65
Невозможно запустить клиентское приложение ЦУСа	66
Некорректная инициализация УКЦ	66
Невозможно обновить компоненты ЦУСа по причине отсутствия прав доступа к экземпляру SQL-сервера	67
После обновления невозможно запустить ЦУС или УКЦ	68
Некорректно отображаются символы в УКЦ	68
Невозможно запустить УКЦ	68
Невозможно изменить путь установки по умолчанию для приложения ЦУС	69
Невозможно обновить базу данных ЦУС	69
Приложение В. Региональные настройки	70
Региональные настройки в ОС Windows 7, Windows Server 2008 R2	71
Региональные настройки в ОС Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10	75
Приложение С. Внешние устройства	79
Общие сведения	79
Список поддерживаемых внешних устройств	79
Алгоритмы и функции, поддерживаемые внешними устройствами	83
Приложение D. Глоссарий	85



Введение

О документе	6
О программе	8
Системные требования	9
Комплект поставки	13
Обратная связь	14

О документе

В данном документе подробно описывается процесс установки и первичной настройки компонентов программного обеспечения **ViPNet Administrator** (см. глоссарий, стр. 85). Приводятся схемы установки, даются рекомендации по размещению компонентов. Также представлена информация об обновлении программ, входящих в состав ViPNet Administrator, приведены решения возможных проблем.

Если ранее в вашей сети использовалось программное обеспечение ViPNet Administrator версии 3.2.x, и вы переходите на использование ПО ViPNet Administrator версии 4.x, вам необходимо также ознакомиться с документом «ViPNet Administrator. Руководство по обновлению с версии 3.2.x на версию 4.x».

Для кого предназначен документ

Настоящий документ предназначен для администраторов, осуществляющих установку, обновление и первичную настройку программного обеспечения ViPNet Administrator®.

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.

Обозначение	Описание
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

ПО ViPNet Administrator® предназначено для администрирования [сетей ViPNet](#) (см. глоссарий, стр. 89) и состоит из двух компонентов:

- [ViPNet Центр управления сетью \(ЦУС\)](#) (см. глоссарий, стр. 85).
- [ViPNet Удостоверяющий и ключевой центр \(УКЦ\)](#) (см. глоссарий, стр. 85).

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](#) (см. глоссарий, стр. 88). Она выполняет функции [удостоверяющего центра](#) (см. глоссарий, стр. 89) и предоставляет ключи, необходимые для работы в сети ViPNet.

Системные требования

Для установки программ, входящих в состав ПО ViPNet Administrator, компьютеры должны удовлетворять ряду требований.

Компьютер, на который будет установлено несколько программ ViPNet Administrator, должен соответствовать максимальным требованиям из числа указанных.

ViPNet Центр управления сетью

Серверное приложение

Требования к аппаратному обеспечению компьютера для установки серверного приложения ViPNet Центр управления сетью:

- Процессор — Intel Core 2 Quad или другой схожий по производительности x86-совместимый процессор с количеством ядер 4 и более.
- Объем оперативной памяти — не менее 4 Гбайт.

Примечание. При большом количестве узлов и связей в сети ViPNet рекомендуется использовать более мощный компьютер:



- Процессор — Intel Core i7 или другой схожий по производительности x86-совместимый процессор с количеством ядер 8 и более.
- Объем оперативной памяти — не менее 16 Гбайт.
- Редакция Microsoft SQL Server выше, чем Express Edition.

-
- Свободное место на жестком диске — не менее 20 Гбайт.
 - Операционная система — Windows 7 (32/64-разрядная), Windows Server 2008 R2 (64-разрядная), Windows 8 (32/64-разрядная), Windows Server 2012 (64-разрядная), Windows 8.1 (32/64-разрядная), Windows Server 2012 R2 (64-разрядная), Windows 10 (32/64-разрядная).

Для операционной системы должен быть установлен самый последний пакет обновлений.

- При использовании Internet Explorer — версия 8 или выше.



Примечание. Перед установкой серверного приложения ViPNet Центр управления сетью убедитесь, что на вашем компьютере в разделе **Программы и компоненты** > **Включение или отключение компонентов Windows** включен компонент **.Net Framework 3.5**.

Для установки и функционирования серверного приложения ViPNet Центр управления сетью необходимо следующее программное обеспечение сторонних производителей:

- На компьютере должны быть установлены следующие приложения:
 - Microsoft .NET Framework версии 4.6.2 (программная платформа).
 - Microsoft Visual C++ 2010 Redistributable Package (набор компонентов среды выполнения библиотек Visual C++).

Указанные приложения включены в комплект поставки программного обеспечения ViPNet Центр управления сетью.

- Для размещения базы данных на компьютере с серверным приложением или на другом компьютере, доступном по сети, должна быть установлена система управления базами данных (СУБД). Поддерживаются следующие версии СУБД:
 - Microsoft SQL Server 2008 SP3 и выше.
 - Microsoft SQL Server 2008 R2 SP1 и выше.
 - Microsoft SQL Server 2012.
 - Microsoft SQL Server 2014 (рекомендуется).
 - Microsoft SQL Server 2017.

Редакция указанных СУБД может быть любой, в том числе и Express Edition. В комплект поставки программного обеспечения ViPNet Центр управления сетью включена СУБД Microsoft SQL Server 2014 Express. При необходимости она может быть автоматически установлена вместе с серверным приложением (см. [Информация для администратора SQL](#) на стр. 26).



Внимание! В процессе эксплуатации программы ViPNet Центр управления сетью необходимо отслеживать выпуск обновлений безопасности для указанного ПО Microsoft и своевременно их устанавливать.

Клиентское приложение

Требования к аппаратному обеспечению компьютера для установки клиентского приложения ViPNet Центр управления сетью:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 1 Гбайт (при использовании 64-разрядных версий ОС Microsoft Windows — не менее 2 Гбайт).
- Свободное место на жестком диске — не менее 1 Гбайт.
- Операционная система — Windows 7 (32/64-разрядная), Windows Server 2008 R2 (64-разрядная), Windows 8 (32/64-разрядная), Windows Server 2012 (64-разрядная), Windows 8.1 (32/64-разрядная), Windows Server 2012 R2 (64-разрядная), Windows 10 (32/64-разрядная).

Для операционной системы должен быть установлен самый последний пакет обновлений.

- При использовании программы Internet Explorer — версия 11.



Примечание. Перед установкой серверного приложения ViPNet Центр управления сетью убедитесь, что на вашем компьютере в разделе **Программы и компоненты > Включение или отключение компонентов Windows** включен компонент **.Net Framework 3.5**.

Для установки и функционирования клиентского приложения ViPNet Центр управления сетью на компьютере должно быть установлено следующее программное обеспечение сторонних производителей:

- Microsoft .NET Framework версии 4.6.2 (программная платформа).
- Microsoft Visual C++ 2010 Redistributable Package (набор компонентов среды выполнения библиотек Visual C++).

Указанные приложения включены в комплект поставки программного обеспечения ViPNet Центр управления сетью.



Внимание! В процессе эксплуатации программы ViPNet Центр управления сетью необходимо отслеживать выпуск обновлений безопасности для указанного ПО Microsoft и своевременно их устанавливать.

ViPNet Удостоверяющий и ключевой центр

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

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 1 Гбайт (при использовании 64-разрядных версий ОС Microsoft Windows — не менее 2 Гбайт).
- Свободное место на жестком диске — не менее 20 Гбайт.
- Операционная система — Windows 7 (32/64-разрядная), Windows Server 2008 R2 (64-разрядная), Windows 8 (32/64-разрядная), Windows Server 2012 (64-разрядная), Windows 8.1 (32/64-разрядная), Windows Server 2012 R2 (64-разрядная), Windows 10 (32/64-разрядная).

Для операционной системы должен быть установлен самый последний пакет обновлений.

- При использовании Internet Explorer — версия 8 или выше.

Дополнительные требования:

- Для возможности сохранения паролей пользователей в файлы на компьютере должен быть установлен виртуальный принтер Microsoft XPS Document Writer. Данный принтер по умолчанию присутствует в операционных системах Windows 7 SP1 (32/64-разрядная), Windows

8 (32/64-разрядная), Windows 8.1 (32/64-разрядная). Если используется одна из операционных систем Windows Server 2008 R2, Windows Server 2012 или Windows Server 2012 R2 SP1, виртуальный принтер следует устанавливать вручную.

- При печати паролей пользователей ViPNet на ПИН-конвертах рекомендуется использовать:
 - Специализированные принтеры для печати ПИН-конвертов или аналогичные матричные принтеры модели OKI ML5100FB.
 - Стандартные четырехслойные ПИН-конверты с расширенным полем для секретной информации.

Комплект поставки

В комплект поставки программного обеспечения ViPNet Administrator входит:

- Установочный файл серверного приложения ViPNet Центр управления сетью.
- Установочный файл клиентского приложения ViPNet Центр управления сетью.
- Приложения сторонних производителей, необходимые для работы компонентов программы ViPNet Центр управления сетью.
- Установочный файл программы ViPNet Удостоверяющий и ключевой центр.
- Документация в формате PDF:
 - «ViPNet Administrator. Руководство по установке».
 - «ViPNet Administrator. Руководство по обновлению с версии 3.2.x до версии 4.x».
 - «ViPNet Administrator. Руководство по миграции программного обеспечения на другой компьютер».
 - «ViPNet Administrator. Быстрый старт».
 - «ViPNet Центр управления сетью. Руководство администратора».
 - «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».
 - «ViPNet Administrator. Руководство по смене мастер-ключей в сети ViPNet».
 - «ViPNet CSP. Руководство пользователя».
 - «Развертывание сети с помощью ViPNet Administrator 4.x. Руководство администратора».
 - «Новые возможности ViPNet Administrator. Приложение к документации ViPNet».
 - «Печать сертификатов. Приложение к документации ViPNet».
 - «ViPNet Administrator. Лицензионные соглашения на компоненты сторонних производителей».



Примечание. Список необходимых для работы ЦУСа приложений сторонних производителей см. в разделе [Системные требования](#) (на стр. 9).

Обратная связь

Дополнительная информация

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

- Информация о продуктах ViPNet <https://infotecs.ru/product/>.
- Информация о решениях ViPNet <https://infotecs.ru/resheniya/>.
- Часто задаваемые вопросы <https://infotecs.ru/support/faq/>.
- Форум пользователей продуктов ViPNet <https://infotecs.ru/forum/>.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ОАО «ИнфоТеКС»:

- Единый многоканальный телефон:
+7 (495) 737-6192,
8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба технической поддержки: hotline@infotecs.ru.

Форма для обращения в службу технической поддержки через сайт
<https://infotecs.ru/support/request/>.

Консультации по телефону для клиентов с расширенной схемой технической поддержки:
+7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

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

1

Общие сведения

Состав ПО ViPNet Administrator	16
Схемы размещения компонентов ПО ViPNet Administrator	17
Использование ViPNet Client для отправки данных на сетевые узлы	20
Лицензия на сеть ViPNet	22

Состав ПО ViPNet Administrator

Программное обеспечение ViPNet Administrator состоит из двух основных компонентов:

- ViPNet Центр управления сетью (далее ЦУС).
- ViPNet Удостоверяющий и ключевой центр (далее УКЦ).

Программа ViPNet Центр управления сетью предназначена для формирования структуры сети ViPNet, задания основных параметров [сетевых узлов](#) (см. глоссарий, стр. 89) и пользователей, централизованной отправки [обновлений ключей](#) (см. глоссарий, стр. 88), [справочников](#) (см. глоссарий, стр. 89) и программного обеспечения на сетевые узлы ViPNet.

Программа ViPNet Центр управления сетью включает два компонента:

- Серверное приложение, с помощью которого осуществляется работа с базой данных, содержащей полную информацию о структуре и объектах сети ViPNet, их свойствах и настройках.
- Клиентское приложение, которое представляет собой удобный графический интерфейс для управления структурой сети ViPNet и свойствами сетевых объектов.

Возможно удаленное подключение клиентского приложения к серверному приложению, а также одновременное подключение нескольких клиентских приложений к серверному.

Программа ViPNet Удостоверяющий и ключевой центр предназначена для управления ключевой структурой сети ViPNet, а также для издания и обслуживания [сертификатов ключа проверки электронной подписи](#) (см. глоссарий, стр. 88), которые хранятся в базе данных. В соответствии с основными функциями УКЦ условно можно разделить на два компонента: ключевой центр и удостоверяющий центр.

Взаимодействие ЦУСа и УКЦ осуществляется посредством базы данных SQL. Программы независимо друг от друга обращаются к SQL-базе, в которой хранится необходимая информация. Изменения, выполненные в одной программе, незамедлительно отображаются в другой.



Рисунок 1. Взаимодействие компонентов ПО ViPNet Administrator

Схемы размещения компонентов ПО ViPNet Administrator

Перед установкой ПО ViPNet Administrator выберите компьютеры, на которых будут размещены следующие компоненты:

- База данных ViPNet Administrator.
- Серверное приложение ViPNet Центр управления сетью.
- Программа ViPNet Удостоверяющий и ключевой центр.
- Одно или несколько клиентских приложений ViPNet Центр управления сетью.

Указанные компоненты можно установить на один или несколько компьютеров сети в любой комбинации. Принципиальное различие между вариантами размещения заключается во взаимном расположении компонентов и базы данных ViPNet Administrator. Поэтому можно выделить две базовые схемы размещения компонентов ПО ViPNet Administrator:

- 1 [Установка компонентов ViPNet Administrator на одном компьютере](#) (на стр. 17).
- 2 [Установка компонентов ViPNet Administrator на разных компьютерах](#) (на стр. 18).

При использовании каждой схемы размещения вы можете установить одно или несколько клиентских приложений ЦУСа на любые компьютеры сети. Возможна установка серверного и клиентского приложений ЦУСа как на один компьютер, так и на разные. В случае установки на разные компьютеры клиентское приложение будет удаленно подключаться к серверному приложению. Также возможно одновременное подключение нескольких клиентских приложений к серверному. Подробную информацию о способах установки клиентского и серверного приложений ЦУСа см. в разделе [Размещение клиентского приложения ViPNet Центр управления сетью](#) (на стр. 19).

Установка компонентов ViPNet Administrator на одном компьютере

Эта схема является наиболее простой и подходит для небольших сетей с одним [администратором](#) (см. глоссарий, стр. 86), работающим и с ЦУСом, и с УКЦ. Она предполагает размещение ЦУСа, УКЦ и [SQL-сервера с базой данных ViPNet Administrator](#) (см. глоссарий, стр. 85) на одном компьютере, поэтому исключаются дополнительные трудности с развертыванием SQL-сервера.



Рисунок 2. Установка серверного приложения ЦУСа и УКЦ на одном компьютере

Установка компонентов ViPNet Administrator на разных компьютерах

Этой схемой разворачивания вы можете воспользоваться в том случае, если в вашей организации уже развернут SQL-сервер и планируется, что база данных ViPNet Administrator будет размещаться на нем. В этом случае все остальные компоненты ViPNet Administrator также размещаются на отдельных компьютерах (что удобно в том случае, если управлением сети занимаются несколько администраторов).

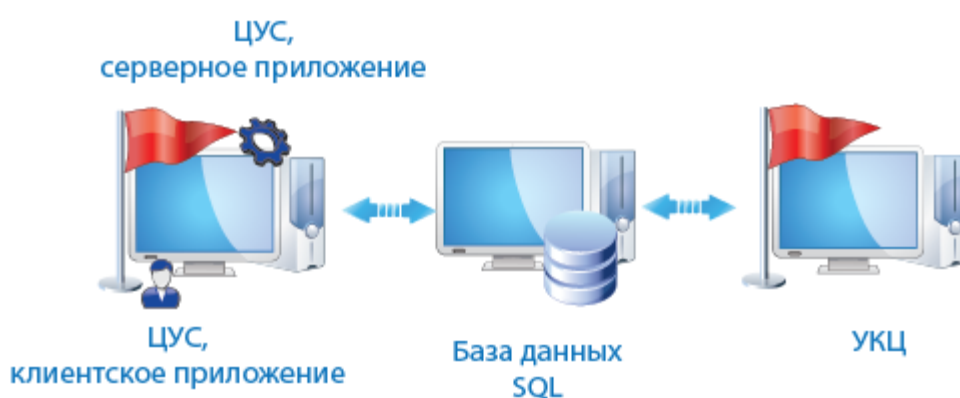


Рисунок 3. Установка серверного приложения ЦУСа и УКЦ на двух разных компьютерах

Размещение клиентского приложения ViPNet

Центр управления сетью

В рассмотренных основных схемах размещения компонентов ПО клиентское приложение ЦУСа может быть установлено на любом компьютере сети ViPNet. Существуют следующие возможности установки приложений:

- Серверное и клиентское приложения ЦУСа могут быть установлены как на один, так и на разные компьютеры.
- Клиентское приложение ЦУСа может быть установлено как на один, так и на несколько компьютеров.

Установка серверного и клиентского приложений ЦУСа на разные компьютеры дает возможность использовать отдельный мощный компьютер для размещения серверного приложения. Установка клиентских приложений на несколько компьютеров дает возможность администрирования в многопользовательском режиме. Вы можете выбрать расположение клиентского приложения ЦУСа, учитывая потребности вашей организации и необходимое количество администраторов сети.

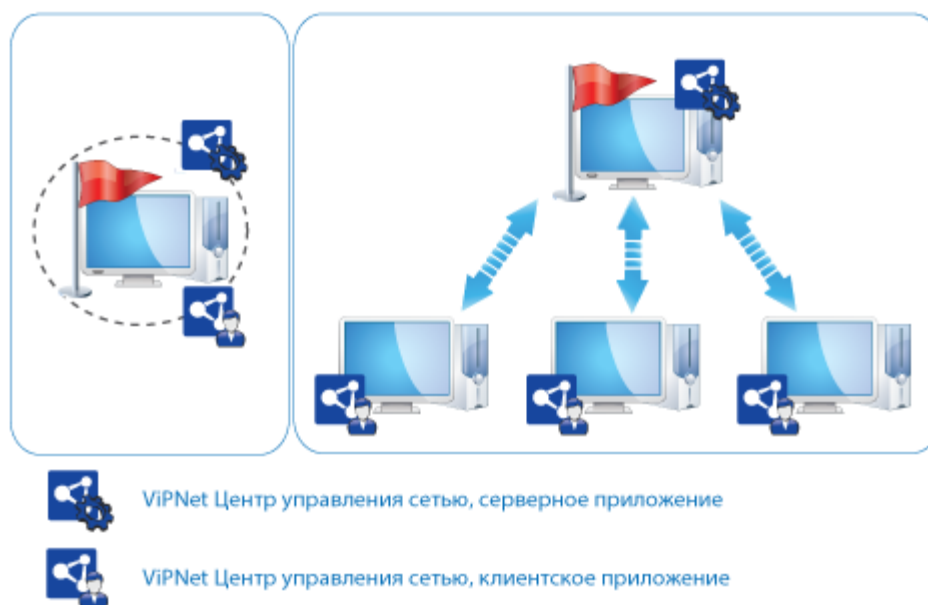


Рисунок 4. Варианты установки приложений ЦУСа

Использование ViPNet Client для отправки данных на сетевые узлы

Для функционирования сети ViPNet необходимо организовать передачу с рабочего места администратора на сетевые узлы ключей, справочников, сертификатов и обновлений программного обеспечения. Эти задачи может выполнить [транспортный модуль ViPNet MFTP](#) (см. глоссарий, стр. 89), входящий в состав ПО ViPNet Client.

ПО ViPNet Client необходимо установить на компьютер с серверным приложением ViPNet Центр управления сетью. Также, для упрощения организации соединения, ViPNet Client необходимо установить на компьютеры с клиентским приложением ЦУСа и с УКЦ. Для совместной работы с ПО ViPNet Administrator 4.x следует использовать ПО ViPNet Client версии 4.2 и выше.



Примечание. Установка ПО ViPNet Client на отдельный не подключенный к сети компьютер с УКЦ не обязательна, однако в этом случае на компьютере с серверным приложением ЦУСа в программе ViPNet Монитор (входящей в состав ПО ViPNet Client) необходимо создать сетевой фильтр для соединения с сетевым узлом УКЦ.

Использование ViPNet Client на компьютере с серверным приложением ЦУСа позволяет:

- Организовать защиту (шифрование) IP-трафика между рабочим местом администратора и другими узлами сети (см. схему ниже).
- Обеспечить защиту рабочего места администратора от несанкционированного доступа при работе в локальных и глобальных сетях с помощью встроенного [межсетевого экрана](#) (см. глоссарий, стр. 88).

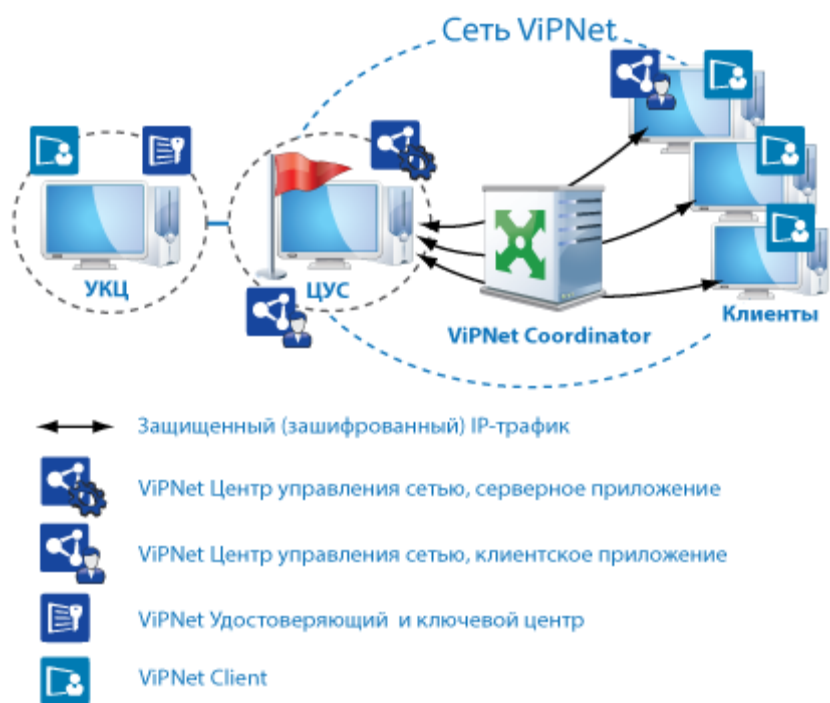


Рисунок 5. Использование программы ViPNet Client для отправки данных на сетевые узлы

Лицензия на сеть ViPNet

Для того чтобы развернуть сеть ViPNet, необходима соответствующая [лицензия](#) (см. глоссарий, стр. 87), которую можно приобрести в ОАО «ИнфоТекС» (см. [Обратная связь](#) на стр. 14).

Лицензия на сеть ViPNet находится в специальном файле *.itcslic или infotecs.reg, без этого файла работа программного обеспечения ViPNet Administrator будет невозможна.

Файл лицензии содержит следующую информацию:

- Номер сети ViPNet и номера подчиненных сетей — в том случае, если лицензия предполагает создание иерархии сетей ViPNet.
- Сведения о владельце сети.
- Возможность использования функций удостоверяющего центра и максимальное число сертификатов ключа проверки электронной подписи, которое может быть издано в УКЦ для внешних пользователей и пользователей ViPNet.
- Список ролей, разрешенных для использования в сети ViPNet и ограничения на количество узлов с различными ролями.
- Ограничения на версии и период использования программного обеспечения для ролей.
- Общий срок действия лицензии.

Лицензии могут быть двух типов:

- С поддержкой иерархии сетей ViPNet.
- Без поддержки иерархии сетей ViPNet.

Если вы обладаете лицензией с поддержкой иерархии сетей ViPNet, вы можете создать помимо главной одну или несколько подчиненных сетей. Для получения более подробной информации см. документ «ViPNet Центр управления сетью. Руководство администратора».

При увеличении числа клиентов сети может потребоваться расширение лицензии. Для этого обратитесь к представителю ОАО «ИнфоТекС» (на стр. 14) и закажите новую лицензию, дополнительно сообщив номер сети ViPNet и желаемые параметры новой лицензии. Чтобы узнать номер сети, в клиентском приложении ЦУСа или в УКЦ в меню **Справка** выберите пункт **О программе**.

После обработки запроса на расширение лицензии вы получите новый файл *.itcslic или infotecs.reg. В окне клиентского приложения ViPNet Центр управления сетью в меню **Лицензия** выберите пункт **Обновить лицензию** и укажите местоположение обновленного файла лицензии, затем перезапустите программу. После перезапуска программы будет использоваться расширенная лицензия.

2

Установка программного обеспечения ViPNet Administrator

Порядок установки компонентов ПО ViPNet Administrator	24
Информация для администратора SQL	26
Установка серверного приложения ViPNet Центр управления сетью	28
Установка клиентского приложения ViPNet Центр управления сетью	32
Установка программы ViPNet Удостоверяющий и ключевой центр	35
Установка обновлений для стороннего ПО	36

Порядок установки компонентов ПО ViPNet Administrator

Для успешного развертывания ПО ViPNet Administrator требуется выполнить все действия из приведенного ниже списка.



Внимание! Программы ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр разных версий могут быть несовместимы друг с другом.

Таблица 3. Порядок установки компонентов ПО ViPNet Administrator

Действие	Ссылка
<input type="checkbox"/> Продумайте схему размещения компонентов ПО ViPNet Administrator.	Схемы размещения компонентов ПО ViPNet Administrator (на стр. 17)
<input type="checkbox"/> Определите количество компьютеров, на которых будет установлено клиентское приложение ЦУСа.	Размещение клиентского приложения ViPNet Центр управления сетью (на стр. 19)
<input type="checkbox"/> Подготовьте нужное количество компьютеров и организуйте их подключение к физической сети.	
<input type="checkbox"/> Убедитесь, что располагаете файлом лицензии на сеть ViPNet *.itcslic или infotecs.reg.	Лицензия на сеть ViPNet (на стр. 22)
<input type="checkbox"/> Разверните SQL-сервер на выделенном компьютере, если требуется, чтобы база данных размещалась отдельно от компонентов ViPNet Administrator.	См. эксплуатационную документацию на SQL-сервер.
<input type="checkbox"/> Выполните установку серверного приложения ЦУСа с учетом выбранного варианта установки приложений ЦУСа. Если база данных ViPNet Administrator размещена на отдельном компьютере, в процессе установки серверного приложения подключитесь к ней.	Установка серверного приложения ViPNet Центр управления сетью (на стр. 28)
<input type="checkbox"/> Выполните установку клиентского приложения ЦУСа с учетом выбранного варианта установки приложений ЦУСа.	Установка клиентского приложения ViPNet Центр управления сетью (на стр. 32)
<input type="checkbox"/> Установите обновления безопасности для используемого ПО сторонних производителей	Установка обновлений для стороннего ПО (на стр. 36)
<input type="checkbox"/> Выполните установку УКЦ с учетом выбранной схемы размещения компонентов ПО ViPNet Administrator.	Установка программы ViPNet Удостоверяющий и ключевой центр (на стр. 35)

- | | | |
|--------------------------|---|--|
| <input type="checkbox"/> | Установите ПО ViPNet Client версии 4.2 и выше на компьютеры с серверным и клиентским приложениями ЦУСа, а также на компьютер с УКЦ. | См. раздел «Установка ПО ViPNet Client» в документе «ViPNet Client Монитор. Руководство пользователя». |
| <input type="checkbox"/> | Выполните первый запуск клиентского приложения ЦУСа и создайте структуру сети ViPNet. | Первый запуск программы ViPNet Центр управления сетью (на стр. 38) |
| <input type="checkbox"/> | Выполните первый запуск и первичную инициализацию УКЦ. | Первый запуск программы ViPNet Удостоверяющий и ключевой центр (на стр. 43)
Первичная инициализация программы ViPNet Удостоверяющий и ключевой центр (на стр. 44) |



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

Информация для администратора SQL

В программном обеспечении ViPNet Administrator серверное приложение ViPNet Центр управления сетью и программа ViPNet Удостоверяющий и ключевой центр обмениваются данными друг с другом через базу данных SQL-сервера, в которой хранится информация о структуре и настройках сети ViPNet. В процессе работы с помощью программы ViPNet Удостоверяющий и ключевой центр вы можете создавать резервные копии этой базы данных, чтобы при необходимости вернуться к той или иной конфигурации сети (подробнее см. в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», в главе «Административные функции»).

База данных создается автоматически при установке серверного приложения ЦУСа. Для размещения базы данных можно использовать существующий именованный экземпляр SQL-сервера (instance), который установлен на локальный или удаленный компьютер. Поддерживаемые версии SQL-сервера приведены в разделе [Серверное приложение](#) (на стр. 9).

Если подходящего SQL-сервера нет, можно установить SQL-сервер, входящий в комплект поставки ViPNet Administrator. В этом случае при установке серверного приложения ЦУСа автоматически устанавливается английская версия программы Microsoft SQL Server 2014 Express и создается именованный экземпляр SQL-сервера с названием по умолчанию WINNCCSQL. Название можно изменить в процессе установки серверного приложения ЦУСа (см. [Установка серверного приложения ViPNet Центр управления сетью](#) на стр. 28).



Примечание. Установка именованного экземпляра на компьютер, на котором ранее уже был установлен другой экземпляр, никак не повлияет на его работу. Два экземпляра будут работать параллельно.

При установке серверного приложения ЦУСа на SQL-сервере создаются:

- База данных с именем `ViPNetAdministrator`.
- База данных с именем `ViPNetJournals`, в которой хранятся журналы аудита программы ViPNet Центр управления сетью.
- Учетная запись пользователя с правами администратора базы данных для пользователя, от имени которого был запущен файл установки серверного приложения ЦУСа.
- Две учетные записи пользователей `KcaUser` и `NccUser`, под которыми осуществляется подключение УКЦ и серверного приложения ЦУСа к базе данных соответственно. Серверное приложение ЦУСа подключается к базе данных при его первом запуске (см. [Первый запуск программы ViPNet Центр управления сетью](#) на стр. 38). Подробное описание подключения УКЦ к базе данных см. в разделе [Первичная инициализация программы ViPNet Удостоверяющий и ключевой центр](#) (на стр. 44).

Параметры созданной базы данных приведены в таблице ниже.

Таблица 4. Параметры базы данных

Параметр	Значение параметра
Параметры сортировки (collation)	Cyrillic_General_CI_AS
Модель восстановления (recovery model)	Full



Внимание! Не изменяйте настройки, структуру и информацию непосредственно в базе данных ViPNet Administrator. Подобные действия могут привести к серьезным неполадкам в работе ПО ViPNet Administrator.

Именованный экземпляр SQL-сервера должен иметь параметры, приведенные в таблице ниже. При установке SQL-сервера из комплекта поставки ViPNet Administrator эти параметры автоматически устанавливаются в требуемые значения.

Таблица 5. Параметры SQL-сервера


Параметр	Значение
FILESTREAM	<p>Разрешить FILESTREAM при доступе через Transact-SQL (Enable FILESTREAM for Transact-SQL access)</p> <p>Разрешить FILESTREAM при потоковом доступе файлового ввода-вывода (Enable FILESTREAM for file I/O streaming access)</p> <p>Разрешить удаленным клиентам потоковый доступ к данным FILESTREAM (Allow remote clients to have streaming access to FILESTREAM data)</p>
Протокол Shared Memory	Включено (Enabled)
Протокол Named pipes	Включено (Enabled)
Протокол TCP/IP	Включено (Enabled)
Состояние службы SQL Server Browser	Работает (Running)
Тип запуска службы SQL Server Browser	Автоматически (Automatic)

Установка серверного приложения ViPNet Центр управления сетью

После выбора схемы размещения компонентов ПО ViPNet Administrator (см. [Схемы размещения компонентов ПО ViPNet Administrator](#) на стр. 17) можно приступить к установке серверного приложения ЦУСа.

Прежде чем начать установку программы, убедитесь, что располагаете установочным файлом серверного приложения ViPNet Центр управления сетью.

Для установки приложения выполните следующие действия:

- 1 Из папки установочного комплекта серверного приложения ViPNet Центр управления сетью двойным щелчком запустите установочный файл .
- 2 В окне **Установка ViPNet Administrator [Центр управления сетью]** будет предложено установить необходимое программное обеспечение (см. [Серверное приложение](#) на стр. 9). Список необходимого ПО зависит от ранее установленных на компьютер программ. Чтобы начать установку, нажмите кнопку **Продолжить**.

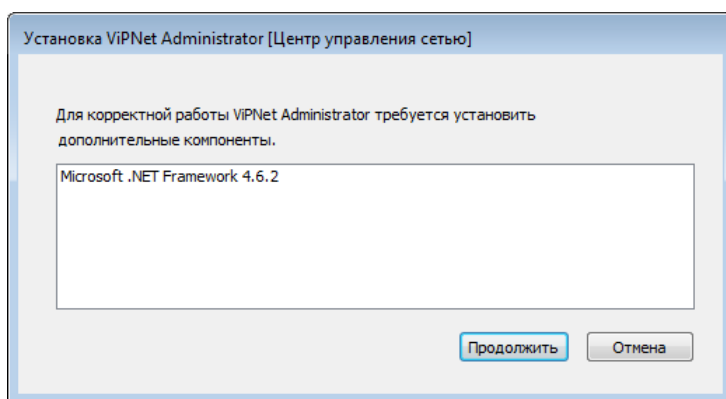


Рисунок 6. Установка необходимого программного обеспечения



Примечание. Установка необходимого программного обеспечения может занять продолжительное время.

- 3 Если после установки требуется перезагрузка компьютера, программа выдаст соответствующее сообщение. Выполните перезагрузку. После перезагрузки установка серверного приложения ЦУСа будет продолжена автоматически.
- 4 В появившемся окне выберите язык для программы ViPNet Центр управления сетью и нажмите **Продолжить**.

- 5 На странице **Лицензионное соглашение** ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку **Продолжить**.
- 6 На странице **Установка продукта** задайте параметры подключения к базе данных. Если вы не укажете имя существующего SQL-сервера, на компьютере будет установлен SQL-сервер из комплекта поставки и создан именованный экземпляр с именем WINNCCSQL (см. [Информация для администратора SQL](#) на стр. 26). При необходимости вы можете задать другое имя экземпляра.

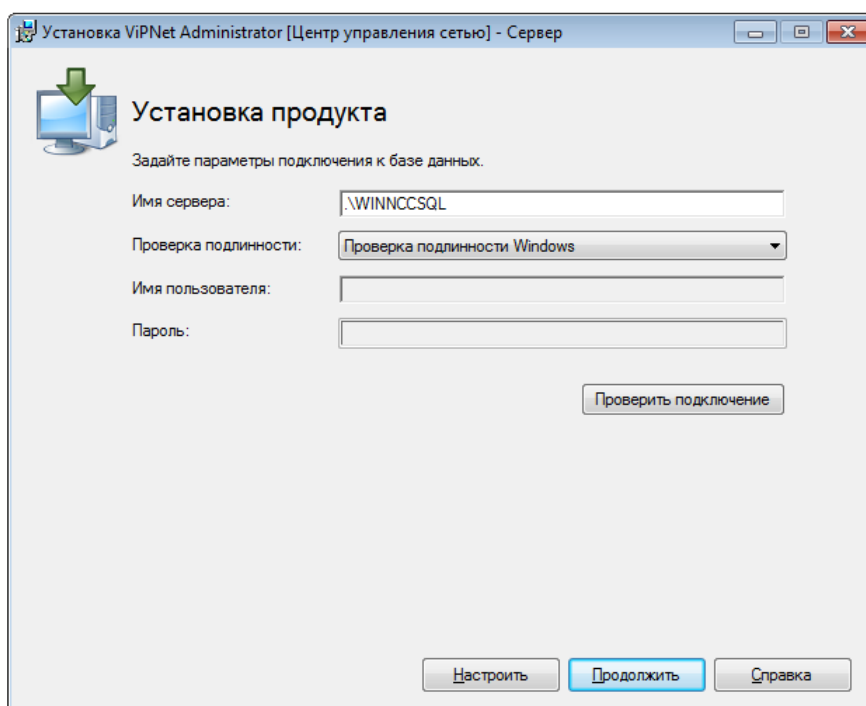


Рисунок 7. Настройка параметров подключения к базе данных

Чтобы использовать существующий именованный экземпляр SQL-сервера, выполните следующие действия:

- В поле **Имя сервера** вместо WINNCCSQL укажите название существующего именованного экземпляра SQL-сервера. Если SQL-сервер находится на удаленном компьютере, вместо точки укажите IP-адрес или DNS-имя удаленного компьютера.
- В поле **Проверка подлинности** выберите режим [аутентификации](#) (см. глоссарий, стр. 86) при подключении к SQL-серверу. Если SQL-сервер размещен на этом же компьютере, рекомендуется выбрать режим **Проверка подлинности Windows**. В этом случае аутентификация будет осуществляться операционной системой с использованием учетной записи пользователя Windows. При удаленном размещении SQL-сервера режим аутентификации зависит от политики безопасности, принятой на этом сервере. Если аутентификация осуществляется по учетным данным пользователя SQL-сервера, выберите режим **Проверка подлинности SQL Server** и укажите имя и пароль учетной записи пользователя SQL-сервера. Чтобы узнать режим аутентификации на удаленном SQL-сервере и учетные данные, обратитесь к администратору SQL-сервера.

- Для проверки соединения с SQL-сервером нажмите кнопку **Проверить подключение**. Если вы указали размещение SQL-сервера и при этом SQL-сервер с указанным именем не существует или недоступен, появится сообщение о невозможности подключения к базе данных с указанными параметрами. Нажмите кнопку **Заккрыть**, проверьте правильность выбранного имени сервера и повторите проверку.

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

- Путь к папке установки программы на компьютере.

Папка установки программы по умолчанию:

C:\Program Files\InfoTeCS\ViPNet Administrator — для 32-разрядных ОС;

C:\Program Files (x86)\InfoTeCS\ViPNet Administrator — для 64-разрядных ОС.



Внимание! Компоненты ПО ViPNet Administrator являются 32-разрядными приложениями. Рекомендуется использовать папку установки по умолчанию, предложенную инсталлятором.

- Имя пользователя и название организации.
- Название папки программы и ее расположение в меню **Пуск**.

8 Чтобы начать установку, нажмите кнопку **Продолжить**.

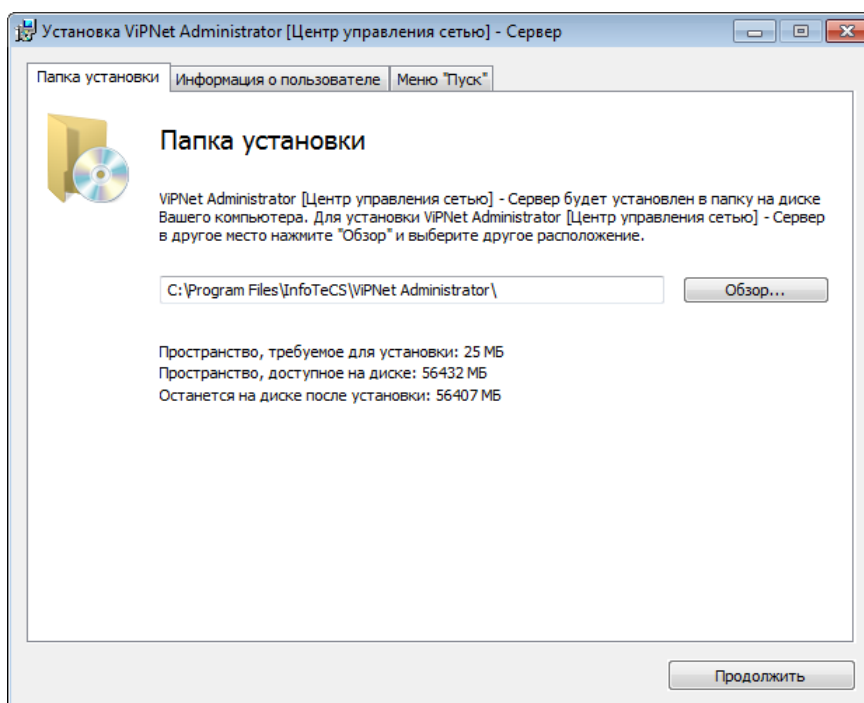


Рисунок 8. Настройка параметров установки серверного приложения ЦУСа

- 9 В появившемся окне проверьте выбранные параметры установки. Чтобы начать установку, нажмите кнопку **Установить сейчас**.
- 10 Если база данных ViPNet Administrator должна размещаться на выделенном SQL-сервере, то укажите имя развернутого SQL-сервера. Если вы не укажете имя существующего SQL-сервера,

появится сообщение с предложением создать сервер базы данных с заданным именем. Для создания сервера в окне сообщения нажмите кнопку **Да**.

- 11 После создания сервера базы данных требуется перезагрузка компьютера, программа выдаст соответствующее сообщение. Выполните перезагрузку. После перезагрузки установка серверного приложения ЦУСа будет продолжена автоматически.
- 12 В появившемся окне выберите язык для программы ViPNet Центр управления сетью и нажмите **Продолжить**.
- 13 На странице **Установка продукта** нажмите кнопку **Продолжить**.
- 14 В появившемся окне проверьте выбранные параметры установки. Чтобы начать установку, нажмите кнопку **Установить сейчас**.
- 15 По завершении установки нажмите кнопку **Заккрыть**.


В результате серверное приложение ЦУСа будет установлено на компьютер. Далее вы можете установить одно или несколько клиентских приложений ЦУСа (см. [Установка клиентского приложения ViPNet Центр управления сетью](#) на стр. 32).

Установка клиентского приложения ViPNet Центр управления сетью

После установки серверного приложения ЦУСа установите одно или несколько клиентских приложений ЦУСа на рабочих местах администраторов создаваемой сети.

Прежде чем начать установку программы убедитесь, что располагаете установочным файлом клиентского приложения ViPNet Центр управления сетью.

Для установки приложения выполните следующие действия:

- 1 Из папки установочного комплекта клиентского приложения ViPNet Центр управления сетью двойным щелчком запустите установочный файл .
- 2 При установке клиентского и серверного приложений на разные компьютеры в окне **Установка ViPNet Administrator [Центр управления сетью]** будет предложено установить необходимое программное обеспечение. Состав устанавливаемого ПО зависит от имеющихся на компьютере программ.

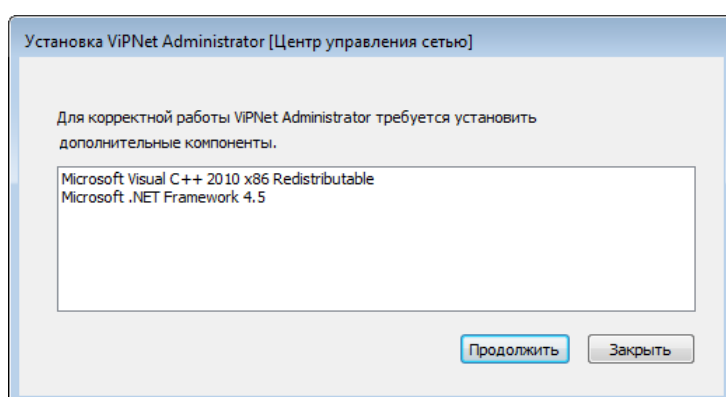


Рисунок 9. Установка дополнительного программного обеспечения



Примечание. Программные компоненты, необходимые для работы серверного приложения, включают компоненты, необходимые для работы клиентского приложения. Поэтому при установке клиентского приложения на один компьютер с серверным устанавливать эти компоненты повторно не требуется.

- 3 Чтобы начать установку, нажмите кнопку **Продолжить**.



Примечание. Установка необходимого программного обеспечения может занять продолжительное время.

- 4 Если после установки требуется перезагрузка компьютера, программа выдаст соответствующее сообщение. Выполните перезагрузку. После перезагрузки установка клиентского приложения ЦУСа будет продолжена автоматически.
- 5 В появившемся окне выберите язык для программы установки ViPNet Центр управления сетью и нажмите **Продолжить**.



Примечание. В данном случае выбирается язык только для программы установки ViPNet Центр управления сетью. Язык интерфейса клиентского приложения совпадает с языком, выбранным для интерфейса серверного приложения ЦУСа (см. [Установка серверного приложения ViPNet Центр управления сетью](#) на стр. 28).

- 6 На странице **Лицензионное соглашение** ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку **Продолжить**.
- 7 Если вы хотите настроить параметры установки, нажмите кнопку **Настроить** на странице **Способ установки** и укажите:
 - Путь к папке установки программы на компьютере.
Папка установки программы по умолчанию:
`C:\Program Files\InfoTeCS\ViPNet Administrator` — для 32-разрядных ОС;
`C:\Program Files (x86)\InfoTeCS\ViPNet Administrator` — для 64-разрядных ОС.
 - Имя пользователя и название организации.
 - Название папки программы и ее расположение в меню **Пуск**.
- 8 Чтобы начать установку, нажмите кнопку **Установить сейчас**.

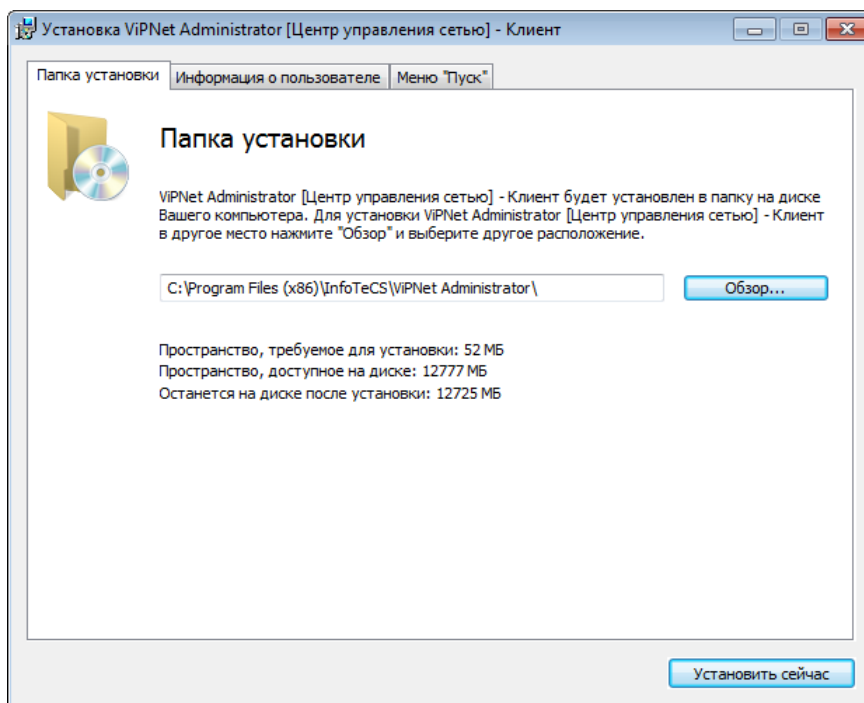


Рисунок 10. Настройки параметров установки клиентского приложения ЦУСа

9 По завершении установки нажмите кнопку **Заккрыть**.

В результате клиентское приложение ЦУСа будет установлено на компьютер. Установите клиентские приложения ЦУСа на рабочие места всех администраторов вашей сети в соответствии с выбранной схемой размещения компонентов ПО ViPNet Administrator (см. [Схемы размещения компонентов ПО ViPNet Administrator](#) на стр. 17). Далее вы можете установить УКЦ (см. [Установка программы ViPNet Удостоверяющий и ключевой центр](#) на стр. 35).

Установка программы ViPNet Удостоверяющий и ключевой центр

После установки серверного (см. [Установка серверного приложения ViPNet Центр управления сетью](#) на стр. 28) и клиентского приложений ЦУСа (см. [Установка клиентского приложения ViPNet Центр управления сетью](#) на стр. 32) можно приступить к установке УКЦ.


Прежде чем начать установку программы:

- Убедитесь, что на компьютере выполнены стандартные региональные настройки, а также правильно заданы часовой пояс, дата и время (см. [Региональные настройки](#) на стр. 70). Иначе возможны проблемы с отображением символов.
- Убедитесь, что располагаете установочным файлом программы ViPNet Удостоверяющий и ключевой центр.



Примечание. Вся информация о лицензионных ограничениях (см. [Лицензия на сеть ViPNet](#) на стр. 22) поступит при подключении к базе данных SQL, созданной при установке серверного приложения ЦУСа.

Для установки программы выполните следующие действия:

- 1 Из папки установочного комплекта программы ViPNet Удостоверяющий и ключевой центр двойным щелчком запустите установочный файл .
- 2 Подождите, пока на компьютер будет автоматически установлено необходимое программное обеспечение, в том числе программа ViPNet CSP.
- 3 В окне **Установка ViPNet Administrator [Удостоверяющий и ключевой центр]** на странице **Лицензионное соглашение** ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку **Продолжить**.
- 4 Если вы хотите настроить параметры установки, на странице **Способ установки** нажмите кнопку **Настроить** и укажите:
 - Путь к папке установки программы на компьютере.
 - Имя пользователя и название организации.
 - Название папки программы и ее расположение в меню **Пуск**.
- 5 Чтобы начать установку, нажмите кнопку **Установить сейчас**.
- 6 По окончании установки нажмите кнопку **Заккрыть**.
- 7 Если после установки требуется перезагрузка компьютера, программа выдаст соответствующее сообщение. Выполните перезагрузку. После этого можно начинать работу с ПО ViPNet Administrator (см. [Начало работы](#) на стр. 37).

Установка обновлений для стороннего ПО

Программное обеспечение сторонних производителей, которое необходимо для работы программы ViPNet Центр управления сетью, может содержать уязвимости. Чтобы избежать влияния возможных уязвимостей на работу программы, необходимо своевременно устанавливать обновления безопасности, выпускаемые производителями стороннего ПО.

После установки серверного и клиентских приложений ViPNet Центр управления сетью выполните следующие действия:

- 1 Проверьте наличие обновлений безопасности или новых версий стороннего программного обеспечения:
 - Microsoft .NET Framework версии 4.6.2.
 - Microsoft Visual C++ 2010 Redistributable Package.
 - Используемой версии Microsoft SQL Server.
- 2 При наличии обновлений установите их.
- 3 В процессе эксплуатации программы ViPNet Центр управления сетью регулярно устанавливайте выпускаемые обновления ПО сторонних производителей.

3

Начало работы

Первый запуск программы ViPNet Центр управления сетью	38
Первый запуск программы ViPNet Удостоверяющий и ключевой центр	43

Первый запуск программы ViPNet

Центр управления сетью

После установки компонентов ПО ViPNet Administrator убедитесь, что располагаете файлом лицензии на сеть ViPNet *.itcslic или infotecs.reg (см. [Лицензия на сеть ViPNet](#) на стр. 22) и запустите программу ViPNet Центр управления сетью. Серверное приложение ЦУСа состоит из служб NccService и NccFilewatcherService, которые автоматически запускаются после загрузки операционной системы. Чтобы запустить клиентское приложение ЦУСа:

1 Выполните одно из действий:

- Если вы используете операционную систему Windows 7 или Windows Server 2008 R2, в меню **Пуск** выберите **Все программы > ViPNet > ViPNet Administrator > Центр управления сетью**.
- Если вы используете операционную систему Windows 8, Windows 10 или Windows Server 2012, 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.

2 При запуске клиентское приложение автоматически подключается к серверному приложению. По умолчанию подключение выполняется по адресу локального компьютера.

Если клиентское и серверное приложения установлены на разных компьютерах, появится сообщение об отсутствии соединения с сервером. Такое же сообщение появится в случае, если службы серверного приложения не запущены (см. [Невозможно запустить клиентское приложение ЦУСа](#) на стр. 66).

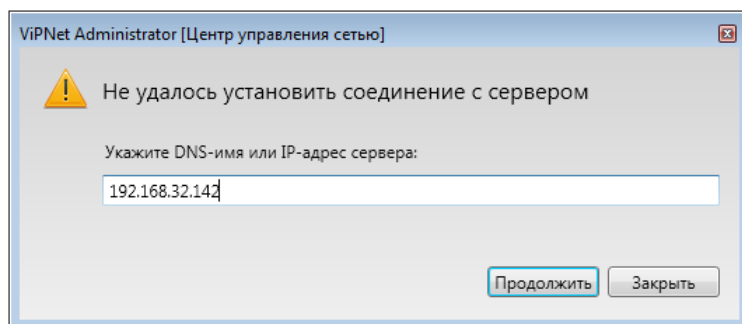


Рисунок 11. Сообщение при отсутствии соединения с SQL-сервером

В этом случае в окне сообщения введите IP-адрес или DNS-имя компьютера, на котором установлено серверное приложение ViPNet Центр управления сетью, и нажмите кнопку **Продолжить**.

3 В окне входа в программу ViPNet Центр управления сетью введите учетные данные администратора:

- Имя пользователя: Administrator.
- Пароль: Administrator.

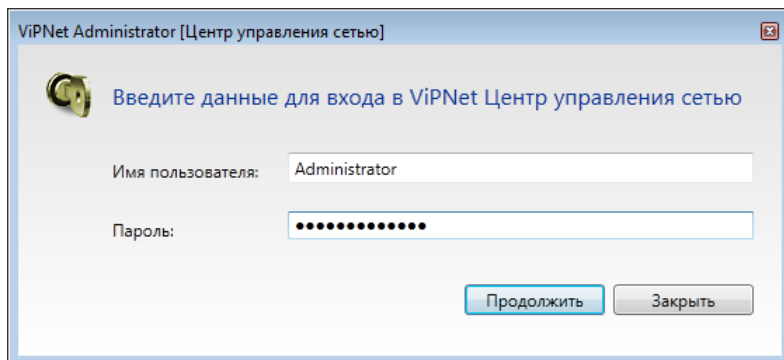


Рисунок 12. Ввод данных администратора для входа в программу ViPNet Центр управления сетью

После ввода данных нажмите кнопку **Продолжить**.

4 При первом входе в программу ViPNet Центр управления сетью в целях безопасности требуется сменить пароль. В окне **Смена пароля** введите текущий пароль, затем задайте новый пароль и подтвердите его.

Пароль должен содержать не менее восьми символов.



Совет. Рекомендуется задавать сложные пароли, содержащие не менее восьми символов, в состав которых входят буквы в разных регистрах, цифры и специальные символы.

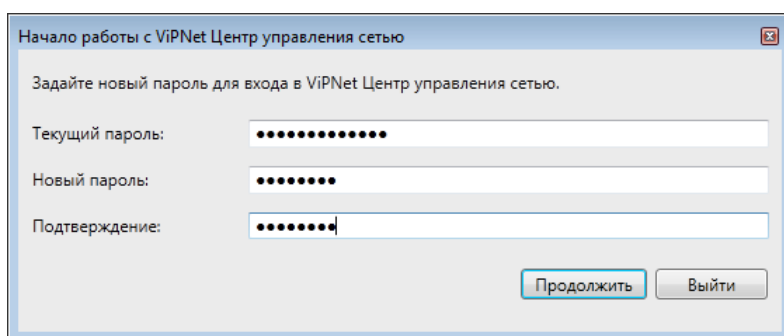


Рисунок 13. Смена пароля администратора ViPNet Центр управления сетью

5 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 (см. [Лицензия на сеть ViPNet](#) на стр. 22) и нажмите кнопку **Продолжить**.

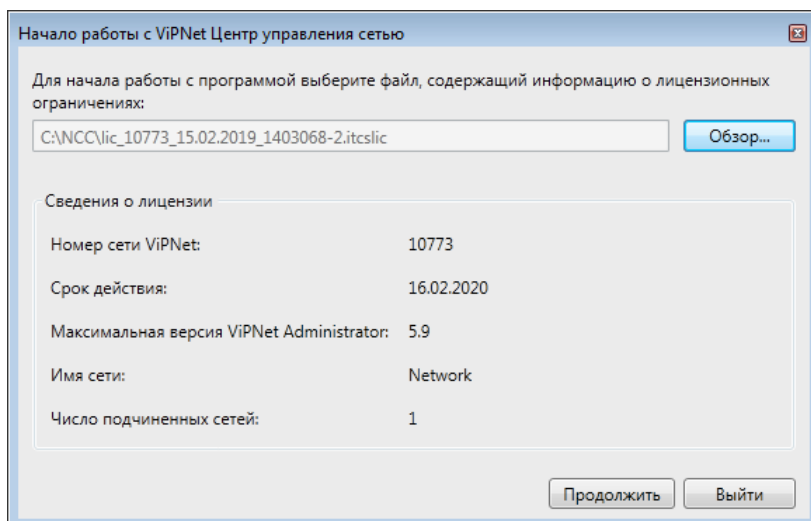


Рисунок 14. Указание пути к файлу лицензии

- 6 В появившемся окне выберите один из возможных сценариев работы в программе:
- Если сеть ViPNet создается заново, то для автоматического формирования структуры сети и выполнения основных настроек **координаторов** (см. глоссарий, стр. 87) и **клиентов** (см. глоссарий, стр. 86) с помощью мастера выберите **Сформировать структуру защищенной сети автоматически**.
 - Если сеть ViPNet уже развернута и в процессе работы с ЦУСом 4.x будут использоваться данные, созданные в ЦУСе 3.2.x, выполните импорт и конвертацию базы данных ЦУСа 3.2.x. Для этого выберите **Загрузить структуру существующей сети**. Подробнее о том, как выполнить конвертацию, см. документ «ViPNet Administrator. Руководство по обновлению с версии 3.2.x на версию 4.x», раздел «Конвертация данных Центра управления сетью 3.2.x».
 - Если сеть ViPNet создается заново, то для формирования структуры сети и выполнения основных настроек координаторов и клиентов вручную выберите **Настроить структуру защищенной сети самостоятельно**.

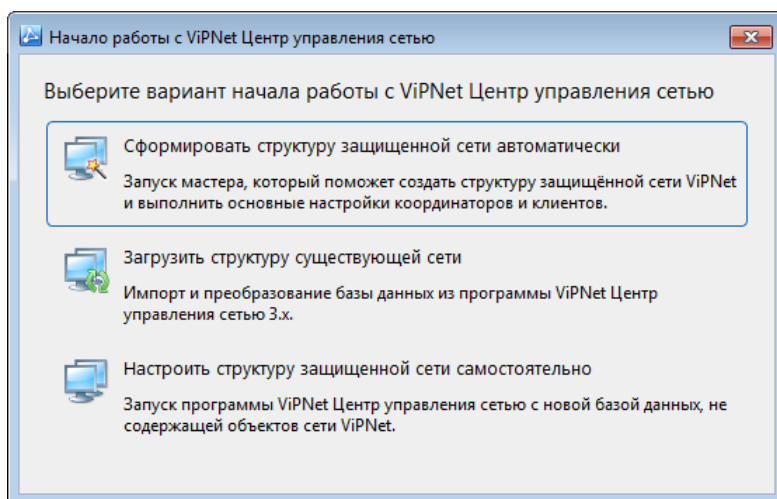


Рисунок 15. Выбор действия для начала работы с программой ViPNet Центр управления сетью

- 7 При создании новой сети, если ваша лицензия на сеть ViPNet предполагает создание иерархии сетей (см. [Лицензия на сеть ViPNet](#) на стр. 22), появится сообщение с предложением распределить лицензионные ограничения между сетями.

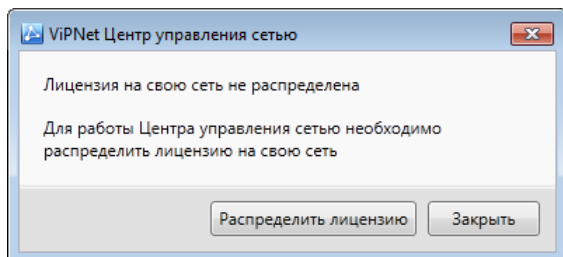



Рисунок 16. Окно с запросом на распределение лицензии

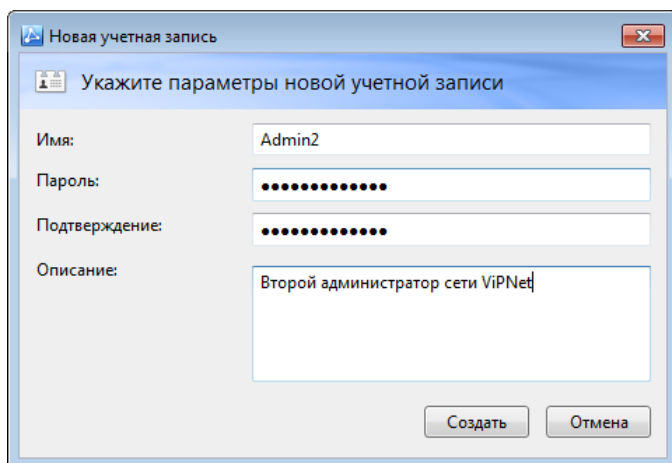
Информацию о распределении лицензии см. в документе «ViPNet Центр управления сетью. Руководство администратора».

- 8 Начните работу в программе в соответствии с выбранным сценарием. Для получения более подробной информации см. документ «ViPNet Центр управления сетью. Руководство администратора».
- 9 В случае необходимости создайте дополнительные учетные записи для работы в Центре управления сетью (см. [Создание дополнительных учетных записей администраторов ЦУСа](#) на стр. 41).

Создание дополнительных учетных записей администраторов ЦУСа

Если в вашей сети будут работать несколько администраторов ЦУСа, после первого запуска клиентского приложения ЦУСа создайте для каждого из них отдельную учетную запись администратора. Это позволит производить журналирование и мониторинг всех действий, выполняемых каждым из них. Все администраторы должны при аутентификации в любом клиентском приложении ЦУСа использовать только свои учетные данные. Для создания учетной записи администратора:

- 1 В представлении **Администрирование** в разделе **Учетные записи** на панели просмотра нажмите кнопку .
- 2 В окне **Новая учетная запись** задайте параметры новой учетной записи и нажмите кнопку **Создать**.



Новая учетная запись

Укажите параметры новой учетной записи

Имя: Admin2

Пароль:

Подтверждение:

Описание: Второй администратор сети ViPNet

Создать Отмена

Рисунок 17. Создание новой учетной записи администратора

Администратор, для которого создана учетная запись, сможет использовать ее для входа в ЦУС в любом клиентском приложении.

Первый запуск программы ViPNet Удостоверяющий и ключевой центр

После установки УКЦ выполните первый запуск программы. Для этого:

1 Выполните одно из действий:

- Если вы используете операционную систему Windows 7 или Windows Server 2008 R2, в меню **Пуск** выберите **Все программы > ViPNet > ViPNet Administrator > Удостоверяющий и ключевой центр**.
- Если вы используете операционную систему Windows 8 или Windows Server 2012, на начальном экране откройте список приложений и выберите **ViPNet > Удостоверяющий и ключевой центр**.



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

2 В окне **Начало работы с программой Удостоверяющий и ключевой центр** выберите один из возможных сценариев дальнейшей работы в программе:

- Если сеть ViPNet создается заново и в УКЦ будут формироваться новые данные, установите переключатель в положение **Настройка новой базы данных** и нажмите кнопку **Продолжить**. Будет запущен мастер первичной инициализации. Выполните процедуру первичной инициализации программы (см. [Первичная инициализация программы ViPNet Удостоверяющий и ключевой центр](#) на стр. 44).

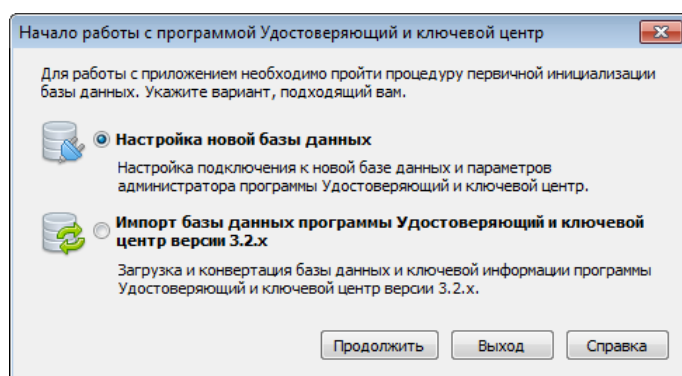


Рисунок 18. Выбор действия для начала работы с программой ViPNet Удостоверяющий и ключевой центр

- Если сеть ViPNet уже развернута и в процессе работы с УКЦ 4.x будут использоваться данные, созданные в УКЦ 3.2.x, выполните импорт и конвертацию базы данных УКЦ 3.2.x.

Для этого установите переключатель в положение **Импорт базы данных программы Удостоверяющий и ключевой центр версии 3.2.x** и нажмите кнопку **Продолжить**, будет запущена программа конвертации данных. Подробнее о том, как выполнить конвертацию, см. документ «ViPNet Administrator. Руководство по обновлению с версии 3.2.x на версию 4.x», раздел «Конвертация данных Удостоверяющего и ключевого центра 3.2.x».

Первичная инициализация программы ViPNet Удостоверяющий и ключевой центр

Если при первом запуске программы ViPNet Удостоверяющий и ключевой центр (см. [Первый запуск программы ViPNet Удостоверяющий и ключевой центр](#) на стр. 43) в окне **Начало работы с программой Удостоверяющий и ключевой центр** переключатель был установлен в положение **Настройка новой базы данных**, будет запущен мастер первичной инициализации.

Чтобы провести первичную инициализацию Удостоверяющего и ключевого центра, выполните следующие действия:

- 1 На первой странице мастера инициализации нажмите кнопку **Далее**.
- 2 Появится [электронная рулетка](#) (см. глоссарий, стр. 90), если она еще не запускалась в рамках текущего сеанса работы программы. Следуйте указаниям в окне **Электронная рулетка**.

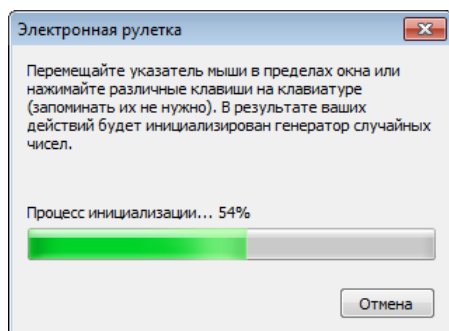


Рисунок 19: Запуск электронной рулетки

- 3 На странице **Подключение к базе данных ViPNet Administrator** укажите сетевой адрес экземпляра SQL-сервера и имя базы данных.

Если УКЦ и SQL-сервер установлены на один компьютер с серверным приложением ЦУСа, адрес экземпляра SQL-сервера — `.\winccsql`. Если УКЦ установлен на другой компьютер, вместо точки укажите IP-адрес или DNS-имя компьютера, на котором установлен SQL-сервер, например, `192.168.32.152\winccsql`.



Примечание. В процессе установки серверного приложения ЦУСа название экземпляра SQL-сервера могло быть изменено (см. [Установка серверного приложения ViPNet Центр управления сетью](#) на стр. 28). В этом случае вместо WINCCSQL укажите заданное название.

Имя базы данных по умолчанию — `ViPNetAdministrator`.

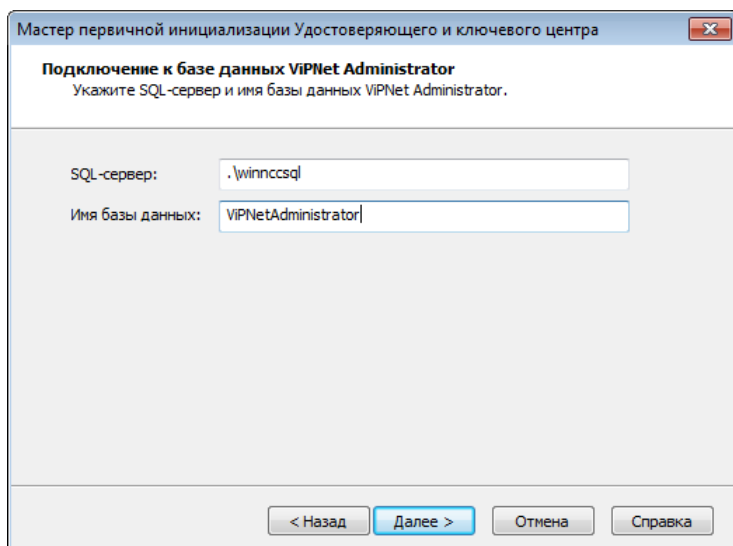


Рисунок 20. Задание параметров подключения к базе данных SQL



Внимание! При первичной инициализации не следует изменять имя базы данных, иначе дальнейший процесс инициализации будет невозможен.

- 4 Выберите режим аутентификации при подключении к SQL-серверу и нажмите кнопку **Далее**.

По умолчанию выбран режим **По имени и паролю пользователя SQL-сервера** и указано имя пользователя, под учетной записью которого будет осуществляться подключение к SQL-серверу, и пароль. Данная учетная запись создается при установке серверного приложения ЦУСа. Не рекомендуется менять ее параметры (имя — KcaUser, пароль — Number1).

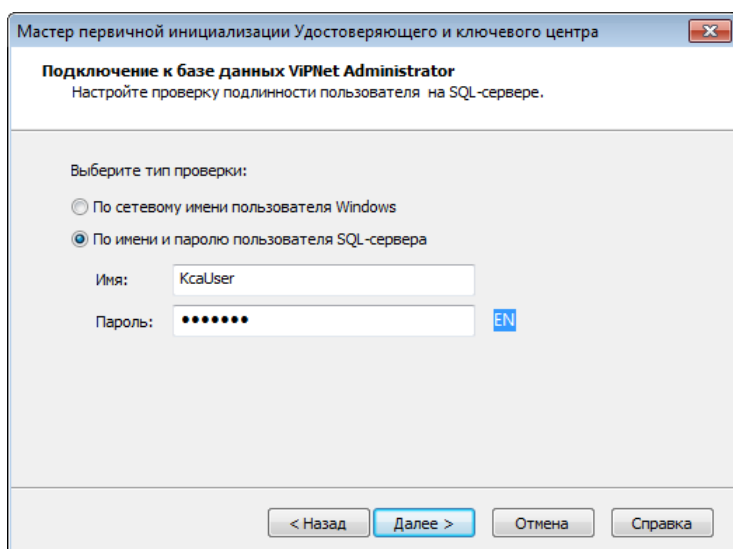


Рисунок 21. Выбор типа аутентификации при подключении к SQL-серверу

После этого нажмите кнопку **Далее**. Будет установлено соединение с SQL-сервером. Если установить соединение не получится, проверьте правильность всех ранее указанных параметров.

- 5 На странице **Создание администратора сети ViPNet** задайте имя учетной записи администратора УКЦ, под которой вы будете работать в программе.
- 6 Если в вашей лицензии доступна функциональность удостоверяющего центра, укажите информацию, необходимую для издания корневого сертификата администратора. В противном случае перейдите к шагу 11.
- 7 На первых страницах мастера **Сведения о владельце сертификата** укажите имя администратора и другие необходимые данные, которые впоследствии будут добавлены в его сертификат, и нажмите кнопку **Далее**.

Мастер первичной инициализации Удостоверяющего и ключевого центра

Сведения о владельце сертификата
Заполните сведения о владельце запрашиваемого сертификата.

Имя: ОАО "Мобильные решения"

Фамилия: Кузнецов Виктор Петрович

Приобретенное имя:

ИНН:

СНИЛС:

Электронная почта: kuznetsov@mobile.ru

< Назад Далее > Отмена Справка

Рисунок 22. Указание сведений об администраторе, для которого создается сертификат

- 8 На странице **Дополнительные сведения о владельце сертификата** при необходимости отредактируйте дополнительные сведения о владельце. Для этого в списке выберите соответствующие атрибуты, нажмите кнопку **Изменить** и внесите необходимую информацию. Затем нажмите кнопку **Далее**.

Мастер первичной инициализации Удостоверяющего и ключевого центра

Дополнительные сведения о владельце сертификата
Укажите дополнительные сведения о владельце сертификата.

Атрибуты	Значения
Серийный номер	
Псевдоним	
Неструктурированное имя	
Инициалы	
Компонента доменного имени	
Неструктурированный адрес	
Телефон	
Департамент	
ОГРНИП	
Описание	

Изменить

< Назад Далее > Отмена Справка

Рисунок 23. Указание дополнительных сведений об администраторе, для которого создается сертификат

- 9 На странице **Параметры ключа электронной подписи** выберите криптопровайдер в соответствии с приведенной ниже таблицей либо другой криптопровайдер, установленный на компьютере. Выбранный криптопровайдер определит алгоритм подписи, по которому будет создаваться ключ электронной подписи и ключ проверки электронной подписи и вычисляться хэш-функция.

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

Таблица 6. 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 (https://tools.ietf.org/html/rfc4357) Стандарт электронной подписи, основанный на арифметике эллиптических кривых OID «1.2.643.2.2.19»	ГОСТ Р 34.10 - 2001. Параметры по умолчанию (рекомендуется) OID «1.2.643.2.2. 35.1» ГОСТ Р 34.10 - 2001 Параметры подписи В OID «1.2.643.2.2. 35.2» ГОСТ Р 34.10 - 2001. Параметры подписи С 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 длиной ключа электронной подписи 256 бит OID «1.2.643.7.1.1.1.1»	ГОСТ Р 34.10 - 2001. Параметры по умолчанию (рекомендуется) OID «1.2.643.2.2. 35.1» ГОСТ Р 34.10 - 2001 Параметры подписи В OID «1.2.643.2.2. 35.2» ГОСТ Р 34.10 - 2001. Параметры подписи С OID «1.2.643.2.2. 35.3»	512 бит ГОСТ Р 34.11-2012/256
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



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

Рисунок 24. Настройка параметров ключа электронной подписи

- 10 На странице **Место хранения контейнеров ключа электронной подписи и ключа защиты УКЦ** выберите место хранения контейнера ключей администратора: **В файле** или **На внешнем устройстве**. Если выбрано хранение контейнера ключа на внешнем устройстве, то далее выберите внешнее устройство хранения данных, предварительно подключив его и установив для него драйвер. При необходимости введите ПИН-код внешнего устройства.

В зависимости от выбранного места хранения будет определен срок действия ключа электронной подписи и, соответственно, срок его плановой смены. При хранении ключа электронной подписи в файле на компьютере либо на внешнем устройстве без аппаратной поддержки алгоритма ГОСТ 34.10-2001/2012 плановая смена ключа электронной подписи должна производиться каждые 15 месяцев, период действия ключа электронной подписи для обновления CRL составляет 54 месяца.

Если ключ электронной подписи хранится на устройстве с аппаратной поддержкой ГОСТ Р 34.10-2001/2012 (был непосредственно сформирован на нем), то смена ключа должна производиться каждые 3 года, период действия ключа электронной подписи для обновления CRL составляет 72 месяца.

По истечении срока действия должна быть произведена плановая смена ключа электронной подписи. При этом под сроком действия понимается срок использования ключа электронной подписи для подписи издаваемых сертификатов пользователей.

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

- 11 На странице **Срок действия сертификата** любым удобным способом задайте срок действия сертификата.

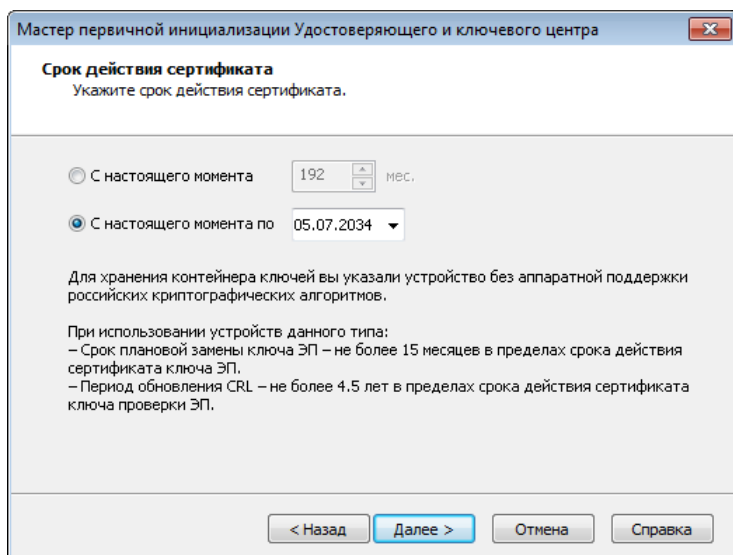


Рисунок 25. Задание срока действия сертификата

- 12 Если требуется, на странице **Сведения о точках распространения** создайте [точку распространения](#) (см. глоссарий, стр. 89) для издаваемого сертификата или для списка аннулированных сертификатов (CRL), который будет сформирован после издания сертификата. Информация о созданных точках будет помещаться в сертификаты пользователей, заверенные данным сертификатом администратора. Кроме этого, заданные точки будут перенесены в настройки программы. Задать или изменить их вы можете в настройках программы. Подробнее см. в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», в разделе «Настройка списка точек распространения».
- 13 Если в УКЦ требуется издавать [квалифицированные сертификаты](#) (см. глоссарий, стр. 86) (работа в режиме [аккредитованного удостоверяющего центра](#) (см. глоссарий, стр. 86)), на странице **Программные средства** установите флажок **Функционировать в режиме аккредитованного удостоверяющего центра** и с помощью кнопки **Настроить** укажите средства, используемые вашим удостоверяющим центром. Подробную информацию о работе в режиме аккредитованного удостоверяющего центра см. в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», в разделе «Издание квалифицированных сертификатов».

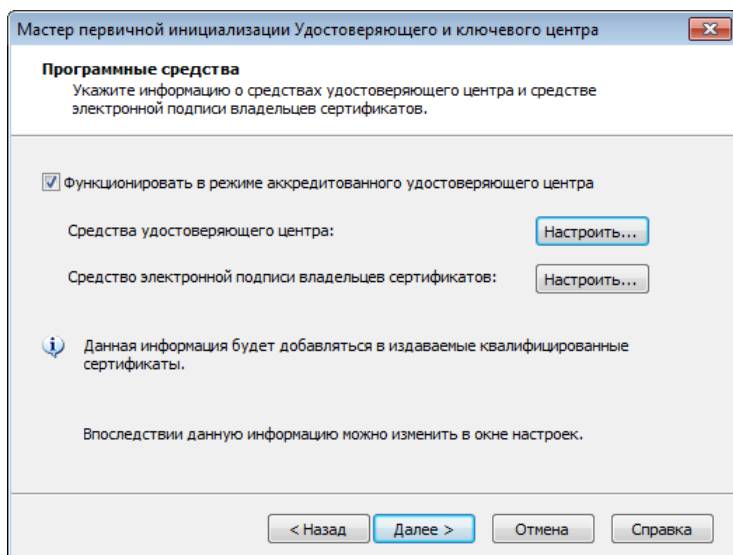


Рисунок 26. Настройка параметров работы УКЦ в режиме аккредитованного удостоверяющего центра

При необходимости на данной странице вы также можете дополнительно указать информацию о средстве электронной подписи владельцев сертификатов (пользователей).



Примечание. Установить флажок и указать все необходимые сведения об используемых средствах можно и после проведения первичной инициализации в настройках программы, но в данном случае стоит учесть, что ранее изданный для вас сертификат ключа проверки электронной подписи не будет соответствовать формату квалифицированного сертификата.

14 На странице **Автоматический режим работы** выполните одно из действий:

- Измените время неактивности администратора, по истечении которого будет осуществляться переход УКЦ в автоматический режим работы (по умолчанию — 15 минут).
- Чтобы в случае, когда администратор не совершает никаких действий, переход УКЦ в автоматический режим работы не производился, снимите соответствующий флажок.

Подробную информацию о работе УКЦ в автоматическом режиме см. в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», в главе «Режимы работы в программе ViPNet Удостоверяющий и ключевой центр».

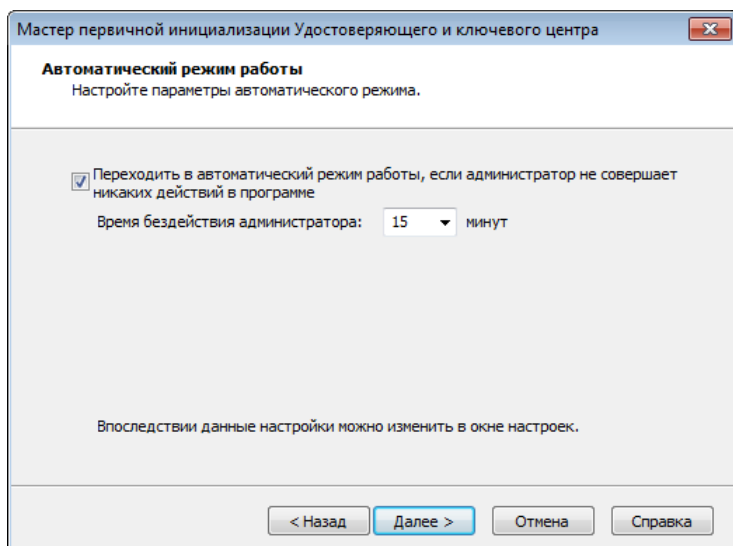


Рисунок 27. Настройка параметров автоматического режима работы



Примечание. Настроить параметры автоматического режима работы УКЦ можно и после проведения первичной инициализации в настройках программы.

- 15 Если на предыдущем шаге вы выбрали переход УКЦ в автоматический режим работы в случае неактивности администратора, настройте операции, которые должны выполняться в автоматическом режиме работы УКЦ. Для этого выберите операцию, нажмите кнопку **Настроить** и в появившемся окне установите соответствующий флажок. Для операций создания ключей узлов, загрузки списков аннулированных сертификатов доверенных сетей ViPNet или обновления списков аннулированных сертификатов укажите, когда эта операция должна выполняться.

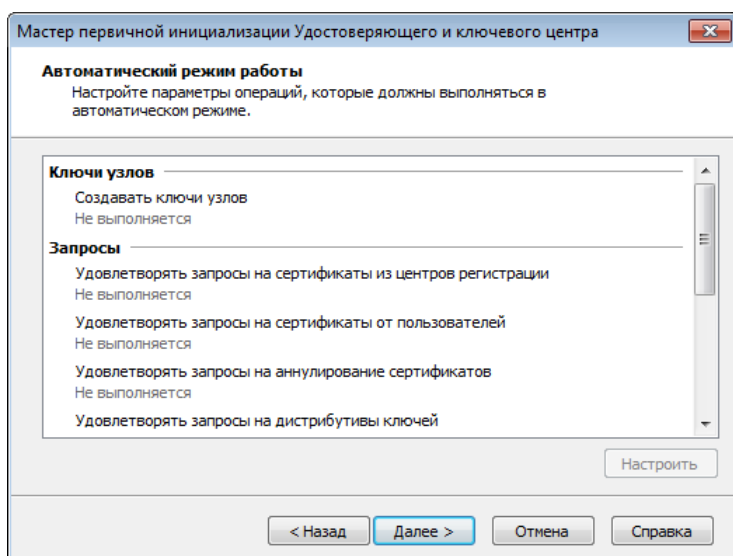


Рисунок 28. Выбор операций для выполнения в автоматическом режиме



Примечание. Если у вас отсутствует лицензия на работу УКЦ в роли удостоверяющего центра (подробнее см. в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», в главе «Общие сведения»), для выполнения в автоматическом режиме работы программы вы можете выбрать только операции создания ключей узлов и удовлетворения запросов на дистрибутивы ключей.

16 На странице **Настройка паролей** укажите следующие параметры:

- Тип создаваемых паролей:
 - **Собственный пароль** — пароль, определяемый администратором.
 - **Случайный пароль на основе парольной фразы** — пароль, формируемый автоматически на основе парольной фразы.



Примечание. Указанный тип паролей будет сохранен в настройках программы и будет учитываться при создании других паролей. Если вы хотите, чтобы остальные пароли создавались другого типа, измените соответствующие настройки.

- Способ выдачи паролей пользователям ViPNet:
 - **Сохранять пароль в файл XPS в папку** — для выдачи паролей в файлах. Укажите папку, в которой будут сохраняться файлы с паролями.
 - **Печатать пароль на принтере** — для выдачи паролей в распечатанном виде. В списке принтеров выберите принтер, который будет использоваться для печати.

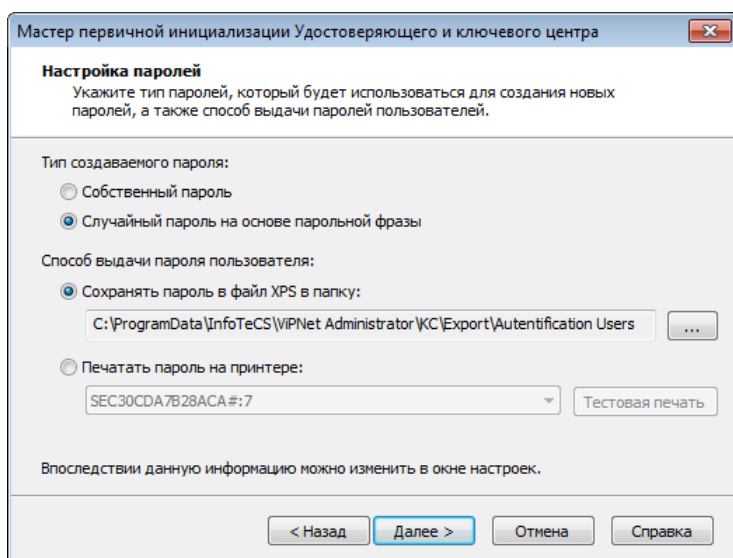


Рисунок 29. Настройка параметров паролей

17 Если на предыдущем шаге выбран тип **Собственный пароль**, то на появившейся странице задайте пароль администратора и подтвердите его. Пароль должен содержать не менее 8 символов.

Внимание! Рекомендуется задавать сложные пароли, содержащие не менее восьми символов, в состав которых входят буквы в разных регистрах, цифры и специальные символы.



Не создавайте пароль длиной в 32 символа. В дальнейшем произвести аутентификацию по паролю с такой длиной будет невозможно. Данное ограничение связано с существующим алгоритмом передачи пароля в криптопровайдер. В соответствии с этим алгоритмом длина пароля не должна превышать 31 символ.

Если был выбран тип одного из случайных паролей, то при появлении [электронной рулетки](#) (см. глоссарий, стр. 90) поводите указателем в пределах окна и на появившейся странице запомните новый пароль (или парольную фразу).

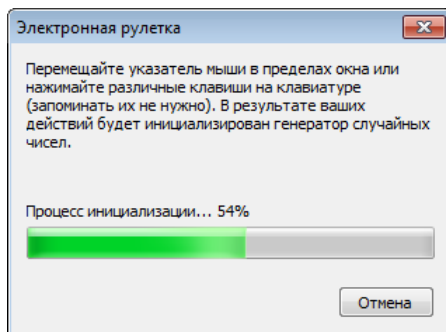




Рисунок 30. Запуск электронной рулетки

При необходимости измените параметры случайного пароля и создайте другой.

- 18 На странице готовности к завершению первичной инициализации УКЦ убедитесь в правильности параметров, заданных на предыдущих страницах мастера. Чтобы отправить эти параметры на печать, нажмите кнопку **Печать**. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.

Для продолжения работы нажмите кнопку **Далее**. Появится электронная рулетка, если она еще не запускалась в процессе первичной инициализации. Поводите указателем в пределах окна **Электронная рулетка**.

- 19 При успешном завершении инициализации на последней странице мастера появится соответствующее сообщение и напротив каждой выполненной операций отобразится значок . Если при инициализации какие-то операции выполнены с ошибками, они будут отмечены значком .

Убедитесь, что первичная инициализация успешно завершена, после чего нажмите кнопку **Заккрыть**.

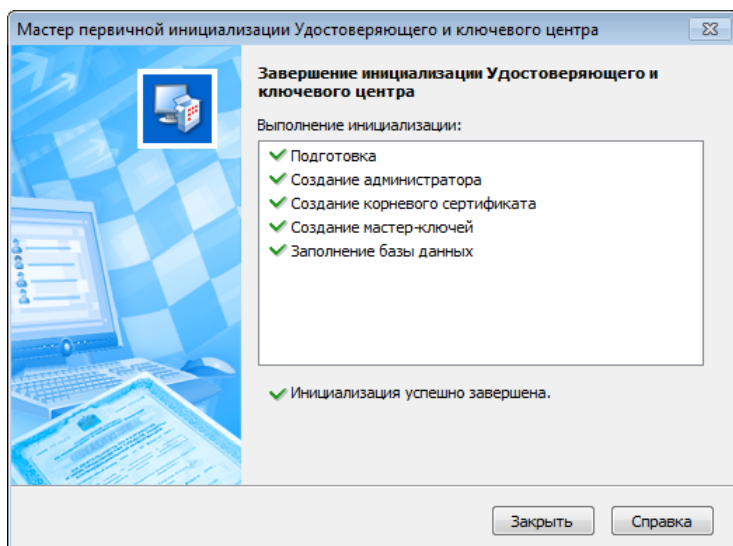


Рисунок 31. Завершение первичной инициализации

При успешном проведении первичной инициализации будут выполнены следующие операции:

- Создана учетная запись администратора УКЦ.
- Создан ключ электронной подписи и издан [сертификат администратора УКЦ](#) (см. глоссарий, стр. 88) (при наличии разрешения использования функциональности удостоверяющего центра).



Примечание. Сертификат, изданный для нового администратора, будет самоподписанным. Если УКЦ выступает в роли [подчиненного удостоверяющего центра](#) (см. глоссарий, стр. 88) и в соответствии с регламентом такой сертификат нельзя использовать для электронной подписи издаваемых сертификатов пользователей, получите другой сертификат в [вышестоящем удостоверяющем центре](#) (см. глоссарий, стр. 86) по специальному запросу (см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», глава «Установление доверительных отношений с другими удостоверяющими центрами»).

Кроме этого, если вы задали параметры работы УКЦ как аккредитованного удостоверяющего центра, то изданный сертификат будет соответствовать формату квалифицированного сертификата.

- Созданы [мастер-ключи](#) (см. глоссарий, стр. 88).
- Установлено соединение с базой данных SQL и произведено ее заполнение данными.

В случае корректной инициализации появится главное окно программы. Можно приступить к работе с УКЦ.

Если инициализация была проведена некорректно, установите причину неудачи (см. [Некорректная инициализация УКЦ](#) на стр. 66), переустановите УКЦ с предварительным удалением текущей версии программы и повторно проведите первичную инициализацию.

4

Обновление программного обеспечения ViPNet Administrator



Внимание! Если вы реплицируете таблицы базы данных ПО ViPNet Administrator, производитель не гарантирует работоспособность ПО ViPNet Administrator и при обновлении ПО могут возникнуть ошибки при работе с базой данных. Чтобы обновить ПО ViPNet Administrator, отключите репликацию баз данных.

Порядок обновления компонентов ПО ViPNet Administrator	56
Обновление приложений ViPNet Центр управления сетью	57
Обновление программы ViPNet Удостоверяющий и ключевой центр	59

Порядок обновления компонентов ПО ViPNet Administrator



Внимание! После получения обновлений для компонентов ViPNet Administrator обязательно обновите как приложения ViPNet Центр управления сетью, так и программу ViPNet Удостоверяющий и ключевой центр. Программы ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр разных версий могут быть несовместимы друг с другом.

Обновление компонентов программного обеспечения ViPNet Administrator рекомендуется выполнять в следующем порядке:

- 1 Обновите серверное приложение ViPNet Центр управления сетью (см. [Обновление приложений ViPNet Центр управления сетью](#) на стр. 57).
- 2 Обновите клиентское приложение ViPNet Центр управления сетью (см. [Обновление приложений ViPNet Центр управления сетью](#) на стр. 57).
- 3 Обновите программу ViPNet Удостоверяющий и ключевой центр (см. [Обновление программы ViPNet Удостоверяющий и ключевой центр](#) на стр. 59).

Прежде чем начать обновление компонентов ViPNet Administrator, убедитесь, что ваша лицензия разрешает использование новой версии. Для этого в программе ViPNet Центр управления сетью в меню **Лицензия** выберите пункт **Сведения о лицензии для своей сети**. В появившемся окне на вкладке **Общая информация** указаны сведения о максимальной версии ViPNet Administrator.

Кроме того, перед обновлением рекомендуется создать с помощью программы ViPNet Удостоверяющий и ключевой центр резервную копию конфигурации сети, которая позволит восстановить данные в случае возникновения проблем после обновления. Подробнее создание и восстановлении резервных копий описано в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», в главе «Административные функции».

Обновление приложений ViPNet


Центр управления сетью

Обновление серверного и клиентского приложений ЦУСа различается тем, что при обновлении серверного приложения необходимо указать параметры подключения к базе данных. Это связано с тем, что вместе с серверным приложением обновляется база данных, в которой хранятся данные о конфигурации сети ViPNet и настройках программ ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр.



Внимание! Перед обновлением серверного приложения ЦУСа необходимо завершить работу УКЦ.

Чтобы обновить одно из приложений, выполните следующие действия:

- 1 Двойным щелчком запустите файл  из установочного комплекта новой версии приложения.
- 2 В появившемся окне выберите язык для программы ViPNet Центр управления сетью и нажмите **Продолжить**.
- 3 На странице **Изменение установленных компонентов** выберите **Обновить** и нажмите кнопку **Продолжить**.

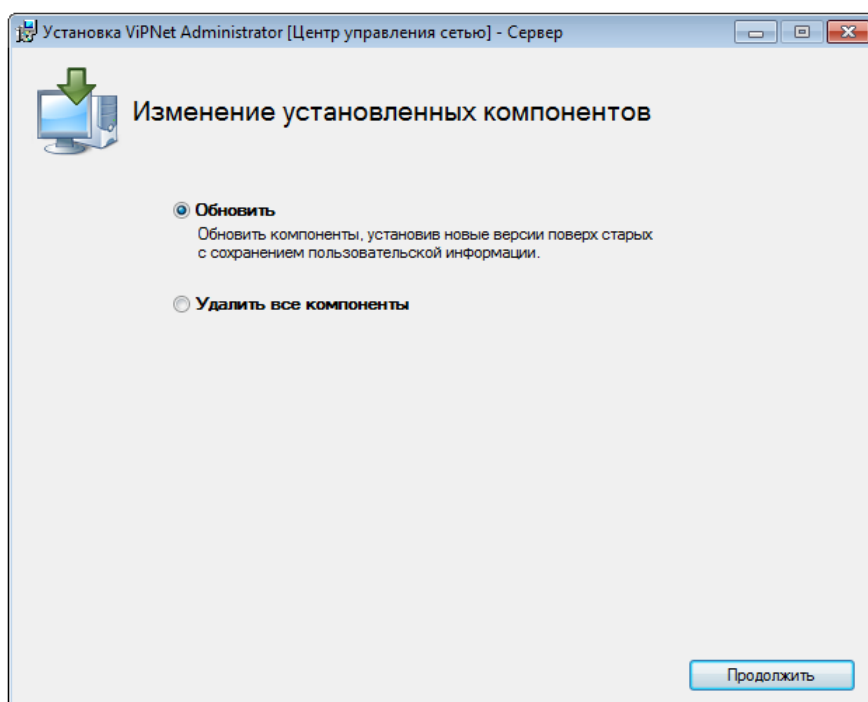


Рисунок 32. Страница изменения установленных компонентов

- 4 На странице **Обновление продукта** задайте параметры подключения к базе данных. Эта страница появляется только при обновлении серверного приложения.

Для проверки соединения с SQL-сервером нажмите кнопку **Проверить подключение**. Если проверка подключения выполнена успешно, для продолжения нажмите кнопку **Обновить**. В противном случае задайте правильные параметры подключения к базе данных.

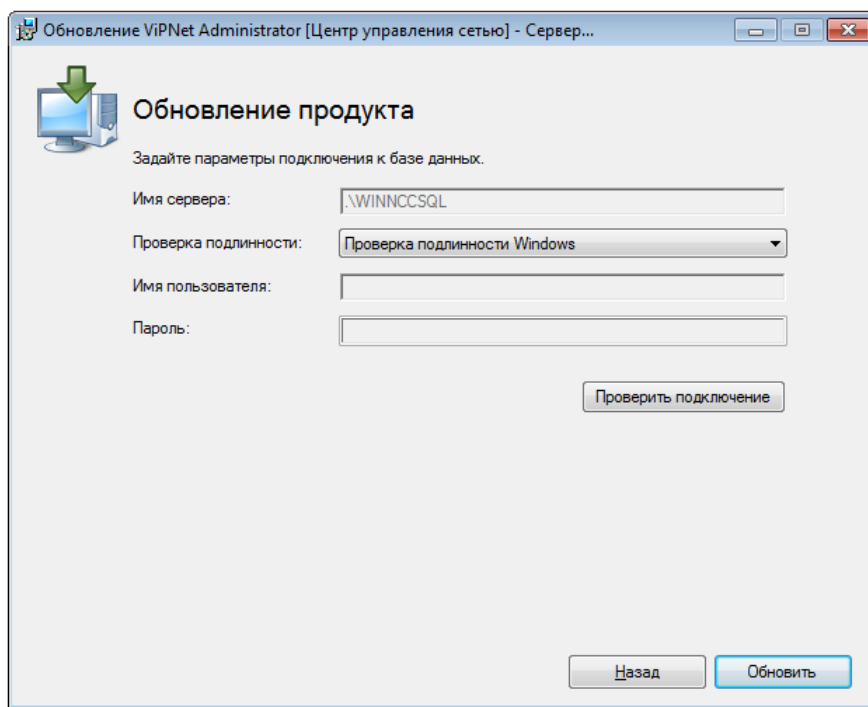



Рисунок 33. Задание параметров подключения к базе данных

- 5 Дождитесь окончания процесса обновления.

После обновления серверного и клиентских приложений обновите УКЦ (см. [Обновление программы ViPNet Удостоверяющий и ключевой центр](#) на стр. 59).

Обновление программы ViPNet Удостоверяющий и ключевой центр

Для обновления программы ViPNet Удостоверяющий и ключевой центр:

- 1 На компьютере с программой ViPNet Удостоверяющий и ключевой центр двойным щелчком запустите файл  из установочного комплекта новой версии программы.
- 2 На странице **Обновление** мастера установки ViPNet Удостоверяющий и ключевой центр нажмите кнопку **Начать обновление**.

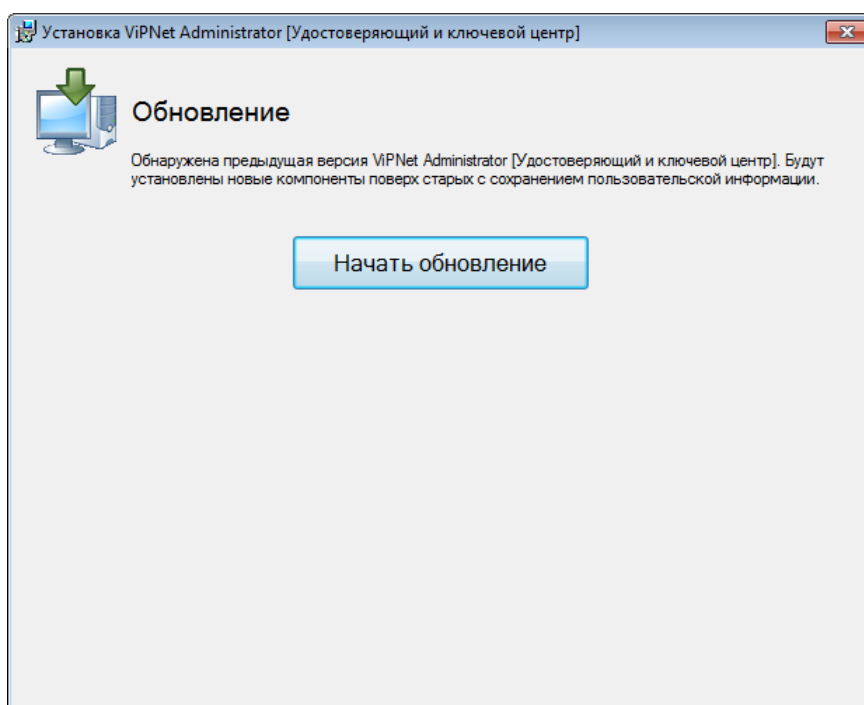


Рисунок 34. Страница "Обновление" мастера установки ViPNet Удостоверяющий и ключевой центр

- 3 Дождитесь завершения процесса обновления и нажмите кнопку **Заккрыть**.
- 4 По окончании установки может появиться окно с предложением перезагрузить компьютер. В этом случае перезагрузите компьютер.

Теперь можно приступить к администрированию сети, используя обновленную программу.

5

Удаление программного обеспечения ViPNet Administrator

Когда требуется удаление компонентов ПО ViPNet Administrator	61
Удаление приложений ViPNet Центр управления сетью	62
Удаление программы ViPNet Удостоверяющий и ключевой центр	63

Когда требуется удаление компонентов ПО ViPNet Administrator

Удаление компонентов программного обеспечения ViPNet Administrator требуется после успешной миграции программного обеспечения на новый компьютер (подробнее см. «ViPNet Administrator. Руководство по миграции программного обеспечения на другой компьютер»). При необходимости сценарием удаления вы также можете воспользоваться при некорректном обновлении компонентов программного обеспечения.

В первом случае вместе с компонентами программного обеспечения в обязательном порядке должна быть удалена база данных ViPNet Administrator и все пользовательские данные. Во втором случае удаление базы данных и пользовательских данных определяется на усмотрение администратора.

Базу данных ViPNet Administrator вы можете удалить в процессе удаления серверного приложения ЦУСа, в том случае если установите соответствующий флажок. Удаление пользовательских данных вы можете произвести при удалении каждого компонента ViPNet Administrator также при наличии соответствующих флажков (см. сценарии удаления ниже).

Удаление приложений ViPNet

Центр управления сетью

В текущей версии программы удаление серверного и клиентского приложений ViPNet Центр управления сетью возможно только средствами операционной системы.

Чтобы удалить одно из приложений ЦУСа, выполните следующие действия:

- 1 В меню **Пуск** выберите пункт **Панель управления**.
- 2 На странице **Настройка параметров компьютера** выберите категорию **Программы и компоненты**.
- 3 На странице **Удаление или изменение программы** выберите в списке нужное приложение и нажмите кнопку **Удалить**.
- 4 В появившемся окне на странице **Изменение установленных компонентов** выберите **Удалить все компоненты** и нажмите кнопку **Продолжить**.
- 5 На странице **Удаление продукта** для удаления пользовательских данных установите соответствующий флажок. Если при удалении серверного приложения установлен данный флажок, то вместе с пользовательскими данными будет удалена база данных ViPNet Administrator. В случае необходимости вы можете проверить связь с базой данных перед ее удалением.
- 6 Нажмите кнопку **Удалить**.
- 7 Дождитесь завершения процесса удаления приложения и нажмите кнопку **Заккрыть**.

Удаление программы ViPNet Удостоверяющий и ключевой центр

Для удаления программы ViPNet Удостоверяющий и ключевой центр:

- 1 Выполните одно из действий:
 - Если вы используете операционную систему Windows 7 или Windows Server 2008 R2, в меню **Пуск** выберите **Все программы > ViPNet > ViPNet Administrator > Установка ViPNet Удостоверяющий и ключевой центр**.
 - Если вы используете операционную систему Windows 8 или Windows Server 2012, на начальном экране откройте список приложений и выберите **ViPNet > Установка ViPNet Удостоверяющий и ключевой центр**.



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

- 2 На странице **Изменение установленных компонентов** выберите **Удалить все компоненты** и нажмите кнопку **Продолжить**.
- 3 На странице **Удаление продукта** установите флажок **Удалить пользовательские данные**, если вместе с программой вы хотите удалить файлы ключей администратора УКЦ и другие служебные файлы. Нажмите кнопку **Удалить**.
- 4 Дождитесь завершения процесса удаления программы и нажмите кнопку **Заккрыть**.



Возможные неполадки и методы их устранения

При установке и обновлении ПО ViPNet Administrator могут возникать следующие неполадки:

- Не устанавливаются приложения сторонних производителей (на стр. 64).
- Невозможно установить серверное или клиентское приложение ЦУСа (на стр. 65).
- Невозможно запустить клиентское приложение ЦУСа (на стр. 66).
- Некорректная инициализация УКЦ (на стр. 66).
- После обновления невозможно запустить ЦУС или УКЦ (на стр. 68).
- Некорректно отображаются символы в УКЦ (на стр. 68).
- Невозможно запустить УКЦ (на стр. 68).
- Невозможно изменить путь установки по умолчанию для приложения ЦУС (на стр. 69).
- Невозможно обновить базу данных ЦУС (на стр. 69).

Не устанавливаются приложения сторонних производителей

Возможно, на жестком диске компьютера недостаточно свободного места. Освободите необходимое дисковое пространство (см. [Системные требования](#) на стр. 9) и повторите попытку установки.

Невозможно установить серверное или клиентское приложение ЦУСа

Возможные причины:

- Не установлены актуальные обновления для операционной системы.
- Параметры выбранного экземпляра SQL-сервера не соответствуют указанным в разделе [Информация для администратора SQL](#) (на стр. 26). Обратитесь к администратору SQL-сервера.
- Служба серверного приложения ЦУСа `NccService` не может быть запущена. Обратитесь к администратору SQL-сервера и проверьте параметры выбранного экземпляра SQL-сервера (см. [Информация для администратора SQL](#) на стр. 26).

Если служба по-прежнему не может быть запущена, выполните следующее:

- На компьютер, на котором находится SQL-сервер, установите среду SQL Server Management Studio 2014 или выше, если она отсутствует. Загрузить программу можно на сайте компании Microsoft <https://www.microsoft.com/ru-ru/download/details.aspx?id=42299>.



Внимание! Среда SQL Server Management Studio должна быть установлена на компьютере после создания сервера базы данных, иначе установка серверного приложения ЦУСа будет невозможна.

- Запустите среду SQL Server Management Studio с помощью меню **Пуск**.
- Подключитесь к установленному SQL-серверу.
- Откройте окно свойств установленного SQL-сервера и выполните следующие настройки:
 - на панели навигации **Выбор страницы** выберите раздел **Дополнительно (Advanced)** и на панели просмотра в группе **FILESTREAM** в списке **Уровень доступа FILESTREAM (Filestream Access Level)** выберите **Включен полный доступ (Full access enabled)**;
 - на панели навигации **Выбор страницы** выберите раздел **Безопасность (Security)** и на панели просмотра в группе **Серверная проверка подлинности (Server authentication)** установите значение **Проверка подлинности SQL Server и Windows (SQL Server and Windows Authentication mode)**.
- Компьютер, на который вы пытаетесь установить серверное приложение ЦУСа и систему управления базами данных (СУБД), является контроллером домена. Из соображений безопасности компания Microsoft не рекомендует устанавливать SQL-сервер на контроллер домена [https://msdn.microsoft.com/ru-ru/library/ms143506\(v=sql.100\).aspx](https://msdn.microsoft.com/ru-ru/library/ms143506(v=sql.100).aspx). Установите СУБД на компьютер, не являющийся контроллером домена.
- Возникли ошибки установки дополнительного ПО сторонних производителей, не связанные с ПО ViPNet Administrator. Чтобы исключить ошибки установки дополнительного ПО, обновите или установите вручную следующее дополнительное ПО из папки установочного комплекта ПО ViPNet Центр управления сетью:
 - Microsoft .NET Framework версии 4.6.2 (программная платформа).

- Microsoft Visual C++ 2010 Redistributable Package (набор компонентов среды выполнения библиотек Visual C++).
- Microsoft SQL Server 2014 Express. При установке должны быть указаны параметры SQL-сервера, как описано в разделе [Информация для администратора SQL](#) (на стр. 26).

При запуске установщика дополнительного ПО могут появиться сообщения об ошибках. Необходимо следовать рекомендациям, которые приведены в сообщениях. При необходимости обратитесь за дополнительными сведениями по устранению неполадок к документации на сайте компании Microsoft.

Невозможно запустить клиентское приложение ЦУСа

Возможные причины:

- Службы серверного приложения ЦУСа `NccService` и `NccFilewatcherService` не запустились автоматически после загрузки операционной системы. Запустите эти службы, для этого:
 - Запустите «Диспетчер задач Windows» с помощью сочетания клавиш **Ctrl+Shift+Esc**.
 - В окне **Диспетчер задач Windows** перейдите на вкладку **Службы**.
 - В списке найдите службу `NccService`, щелкните эту службу правой кнопкой мыши и в контекстном меню выберите пункт **Запустить службу**.
 - Таким же образом запустите службу `NccFilewatcherService`.
- Компьютер с серверным приложением ЦУСа выключен.
- Отсутствует соединение между компьютерами с клиентским и серверным приложениями ЦУСа. Для проверки соединения между компьютерами воспользуйтесь командой `ping`.
- На компьютере с клиентским или серверным приложением ЦУСа запущен межсетевой экран, блокирующий соединение (например, брандмауэр Windows). Проверьте настройки межсетевых экранов.
- Ваш компьютер не подключен к сети.

Некорректная инициализация УКЦ

Возможные причины:

- Некорректная работа электронной рулетки.
- Случайное или умышленное повреждение (удаление) базы данных.
- Заданы неверные учетные данные пользователя базы SQL. По умолчанию для УКЦ заданы следующие учетные данные:
 - Имя пользователя: `KcaUser`.

- Пароль: Number1.

После установления причины ошибки повторно проведите первичную инициализацию программы ViPNet Удостоверяющий и ключевой центр. Если при запуске программы мастер первичной инициализации не вызывается автоматически, удалите папку `C:\ProgramData\Infotecs\ViPNet Administrator\KC` вместе с ее содержимым.

Невозможно обновить компоненты ЦУСа по причине отсутствия прав доступа к экземпляру SQL-сервера

При обновлении компонентов ViPNet Центр управления сетью может появиться следующее сообщение:

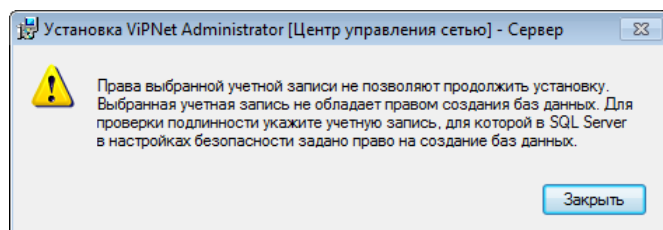


Рисунок 35. Невозможно обновить серверное или клиентское приложение ЦУСа по причине отсутствия прав учетной записи

Это означает, что вы не можете обновить компоненты ЦУСа по причине отсутствия прав доступа к экземпляру SQL-сервера, на котором развернута база данных ViPNet Administrator. Данная проблема может возникать в том случае, если вы удалили учетную запись администратора в ОС Windows, под которой первоначально разворачивались компоненты ЦУСа и база данных SQL, либо стали использовать доменную учетную запись.

В этом случае для устранения указанной проблемы выполните следующие действия:

- 1 Обратитесь в службу технического сопровождения «ИнфоТеКС» для получения утилиты `NccRegistrator.exe`, с помощью которой вы сможете получить доступ к базе данных ViPNet Administrator под вашей текущей учетной записью.
- 2 Скопируйте утилиту на компьютер, на котором установлено серверное приложение ЦУСа.
- 3 Запустите исполняемый файл утилиты.
- 4 В появившемся окне введите имя и пароль администратора ЦУСа, который вы обычно указываете при запуске клиентского приложения ЦУСа. Если вы при разворачивании компонентов ЦУСа изменяли имя SQL-сервера, укажите это имя в поле **Имя экземпляра баз данных**.

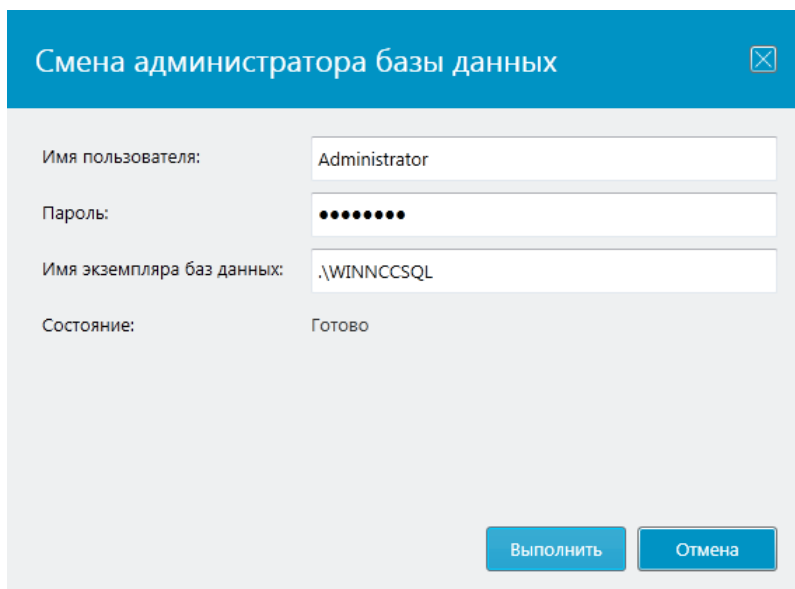


Рисунок 36. Подключение к базе данных SQL для получения прав доступа

- 5 Нажмите кнопку **Выполнить**.
- 6 Если в поле **Состояние** появилось сообщение «Готово», то вы можете повторить попытку обновления компонентов ЦУСа (см. [Обновление программного обеспечения ViPNet Administrator](#) на стр. 55). Если в этом поле появилось сообщение об ошибке, проверьте правильность введенных данных.

После обновления невозможно запустить ЦУС или УКЦ

Возможно, обновлены не все компоненты ПО ViPNet Administrator. Убедитесь, что обновлены все приложения, входящие в состав ПО ViPNet Administrator: клиентское и серверное приложение ЦУСа, УКЦ.

Некорректно отображаются символы в УКЦ

Возможно, не выполнены стандартные региональные настройки в ОС Windows (см. [Региональные настройки](#) на стр. 70). Откройте панель управления и выполните необходимые настройки.

Невозможно запустить УКЦ

Возможны следующие причины:

- Компьютер с серверным приложением ЦУСа и базой SQL выключен.

- Отсутствует соединение между компьютерами с серверным приложениями ЦУСа и УКЦ. Для проверки соединения между компьютерами воспользуйтесь командой `ping`.
- На компьютере с УКЦ или серверным приложением ЦУСа запущен межсетевой экран, блокирующий соединение (например, брандмауэр Windows). Проверьте настройки межсетевых экранов.
- Ваш компьютер не подключен к сети.

Невозможно изменить путь установки по умолчанию для приложения ЦУС

Приложения ЦУС имеют следующие папки установки по умолчанию:

- `C:\Program Files\InfoTeCS\ViPNet Administrator` — для 32-разрядных ОС;
- `C:\Program Files (x86)\InfoTeCS\ViPNet Administrator` — для 64-разрядных ОС.

В случае если была выбрана папка установки, отличная от папки по умолчанию, а приложение установлено в папку по умолчанию, то это могло произойти, если в качестве папки установки была выбрана системная папка ОС, не предназначенная для этого.

Рекомендуется использовать папку установки по умолчанию, предложенную инсталлятором.

Компоненты ПО ViPNet Administrator являются 32-разрядными приложениями. При их установке на 64-разрядных ОС не допускается использование системных папок ОС, предназначенных для размещения 64-разрядных приложений (`C:\Program Files\`), а также не предназначенных для установки сторонних приложений (например, `C:\Windows`), так как при установке в такую папку указанный путь будет изменён встроенными в ОС средствами контроля на указанный по умолчанию без каких-либо уведомлений.



Внимание! Не допускается установка ПО ViPNet Administrator на сетевой диск или внешний накопитель (USB-флэш или USB-HDD).

Невозможно обновить базу данных ЦУС

Если вы реплицируете таблицы базы данных ПО ViPNet Administrator, производитель не гарантирует работоспособность ПО ViPNet Administrator и при обновлении ПО могут появиться сообщения об ошибках. Чтобы обновить ПО ViPNet Administrator, отключите репликацию базы данных ПО ViPNet Administrator. Таблицы базы данных ПО ViPNet Administrator не рекомендуется модифицировать. База данных ПО ViPNet Administrator не поддерживают репликацию баз данных.

В

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 понадобятся 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 7, Windows Server 2008 R2

Для установки поддержки кириллицы на ОС Windows 7, Windows Server 2008 R2 выполните следующие действия:

- 1 Откройте панель управления (Control Panel) и в категории **Часы, язык и регион (Clock, Language, and Region)** выберите параметр **Язык и региональные стандарты (Region and Language)**.
- 2 В окне **Язык и региональные стандарты (Region and Language)** перейдите на вкладку **Дополнительно (Administrative)**.

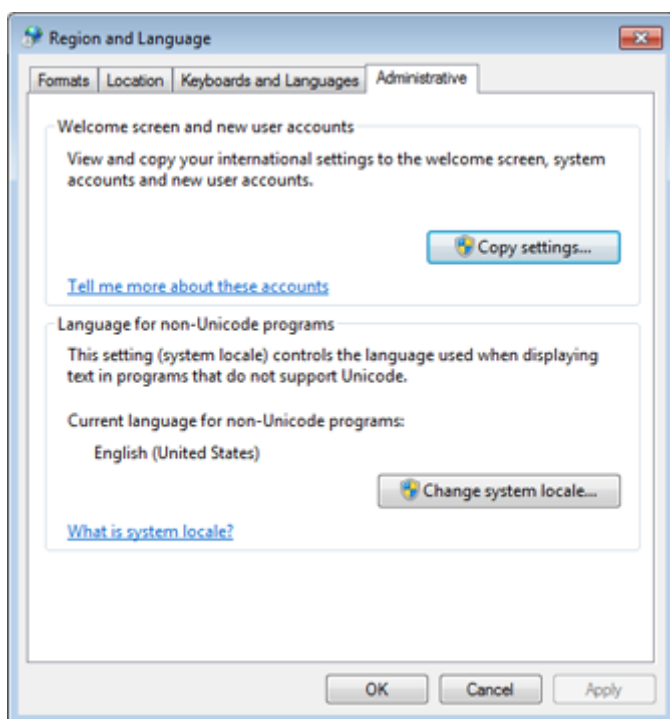


Рисунок 37. Дополнительные языковые параметры

- 3 На вкладке **Дополнительно (Administrative)** нажмите кнопку **Изменить язык системы (Change system locale)**.
- 4 В появившемся окне в списке **Current system locale** выберите **Русский (Россия) (Russian (Russia))**.

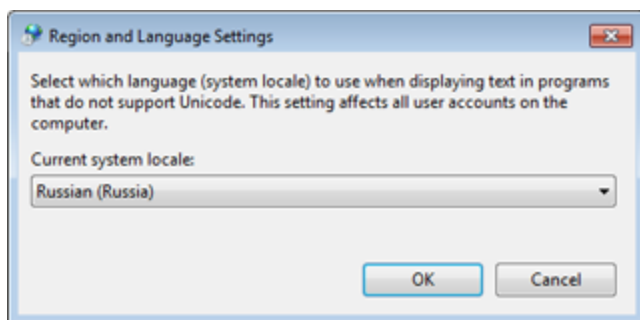


Рисунок 38. Выбор языка системы

- 5 Нажмите кнопку **ОК**. Перезагрузите компьютер.
- 6 Дождитесь завершения перезагрузки компьютера, откройте панель управления (Control Panel) и в категории **Часы, язык и регион (Clock, Language, and Region)** выберите параметр **Язык и региональные стандарты (Region and Language)**.
- 7 В окне **Язык и региональные стандарты (Region and Language)** перейдите на вкладку **Дополнительно (Administrative)** (см. рисунок на стр. 71).
- 8 На вкладке **Дополнительно (Administrative)** нажмите кнопку **Копировать параметры (Copy settings)**.
- 9 В открывшемся окне в списке **Копировать текущие параметры в (Copy your current settings to)** установите флажок **Экран приветствия и системные учетные записи (Welcome screen and system accounts)** и нажмите кнопку **ОК**.

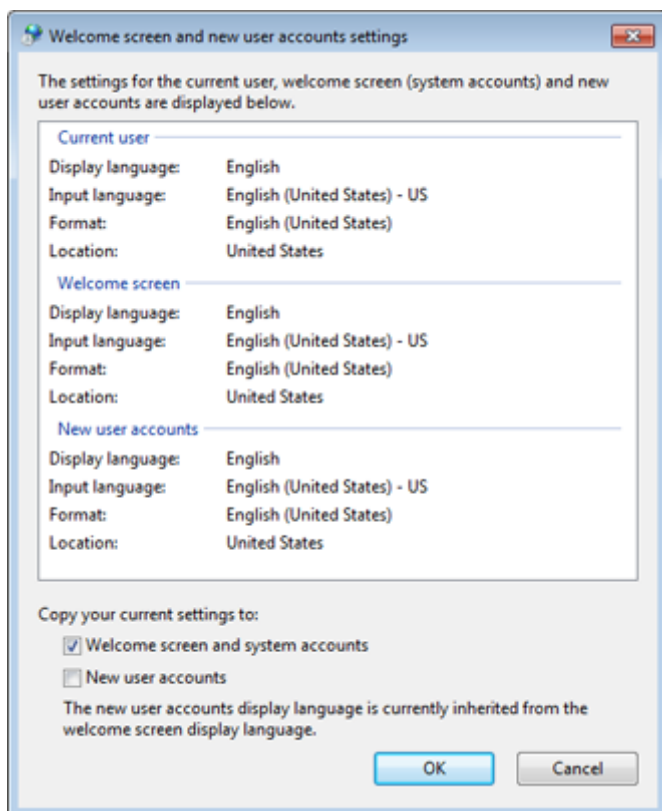


Рисунок 39. Копирование параметров

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))**.

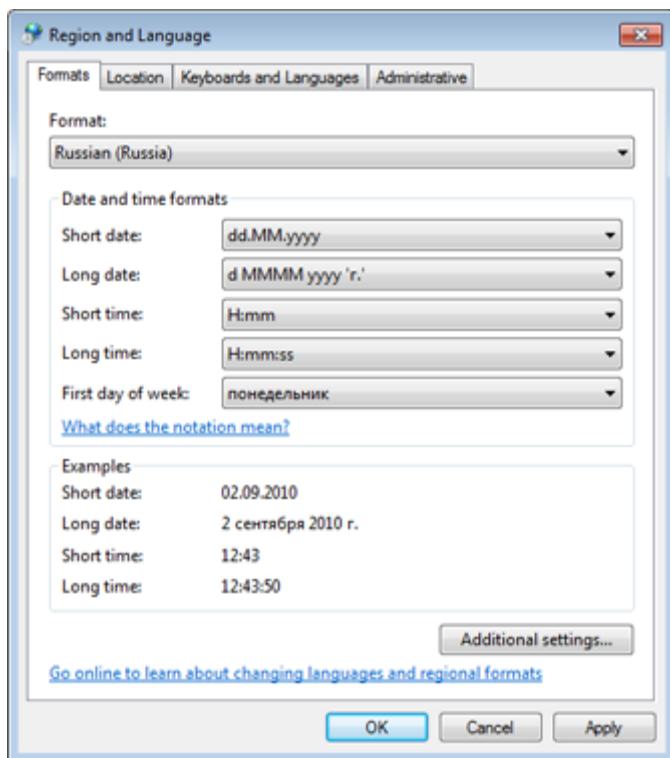


Рисунок 40. Настройка форматов

- 2 В окне **Язык и региональные стандарты (Region and Language)** на вкладке **Расположение (Location)** в списке **Текущее расположение (Current location)** выберите **Россия (Russia)**.

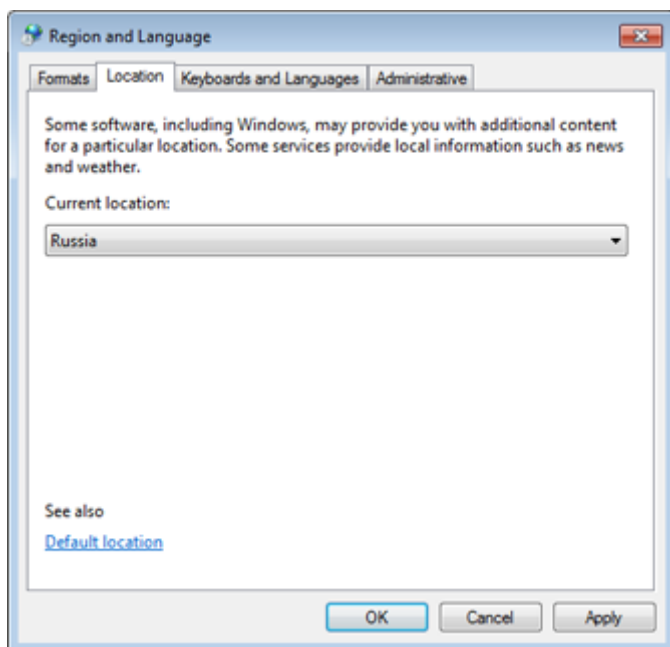


Рисунок 41. Выбор текущего расположения

Региональные настройки в ОС Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10

Для установки поддержки кириллицы на ОС Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10 выполните следующие действия:

- 1 Откройте панель управления (Control Panel) и в категории **Часы, язык и регион (Clock, Language, and Region)** выберите параметр **Изменение форматов даты, времени и чисел (Change date, time, or number formats)**.
- 2 В окне **Регион (Region)** перейдите на вкладку **Дополнительно (Administrative)**.

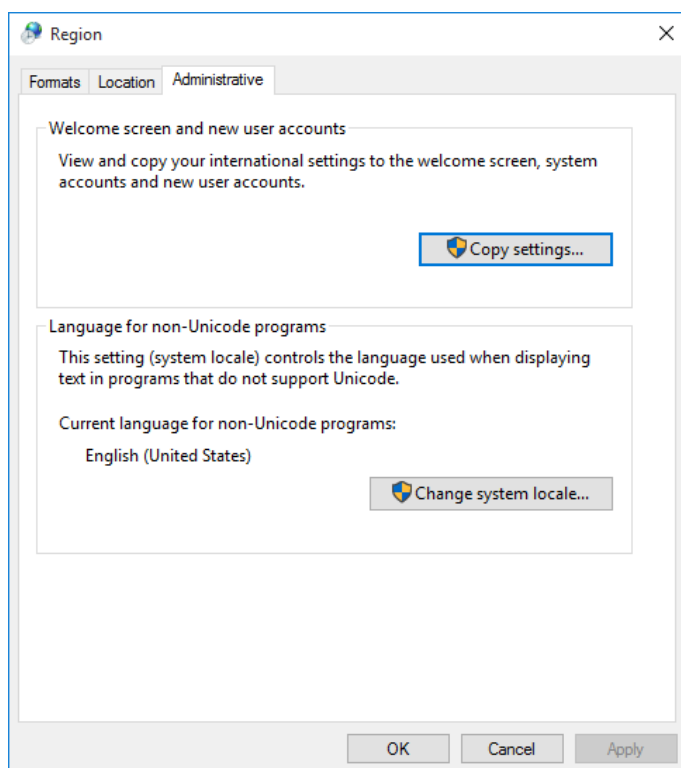


Рисунок 42. Дополнительные языковые параметры

- 3 На вкладке **Дополнительно (Administrative)** нажмите кнопку **Изменить язык системы (Change system locale)**.
- 4 В появившемся окне в списке выберите **Русский (Россия) (Russian (Russia))**.

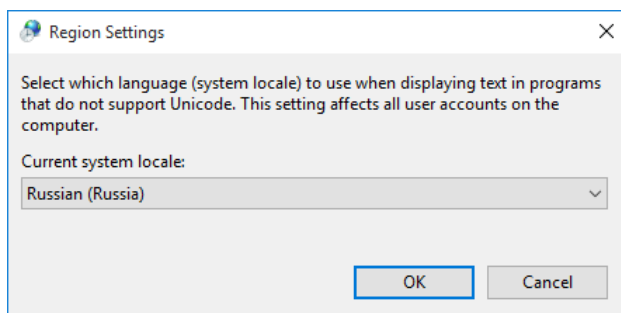


Рисунок 43. Выбор языка системы

- 5 Нажмите кнопку **ОК**. Перезагрузите компьютер.
- 6 Дождитесь завершения перезагрузки компьютера, откройте панель управления (Control Panel) и в категории **Часы, язык и регион (Clock, Language, and Region)** выберите параметр **Изменение форматов даты, времени и чисел (Change date, time, or number formats)**.
- 7 В окне **Регион (Region)** перейдите на вкладку **Дополнительно (Administrative)** (см. рисунок на стр. 75).
- 8 На вкладке **Дополнительно (Administrative)** нажмите кнопку **Копировать параметры (Copy settings)**.
- 9 В открывшемся окне в списке **Копировать текущие параметры в (Copy your current settings to)** установите флажок **Экран приветствия и системные учетные записи (Welcome screen and system accounts)** и нажмите кнопку **ОК**.



Рисунок 44. Копирование параметров

Также для исключения проблем с кодировкой в некоторых системах мы рекомендуем выполнить следующие действия:

- 1 В окне **Регион (Region)** на вкладке **Форматы (Formats)** в списке **Формат (Format)** выберите **Русский (Россия) (Russian (Russia))**.

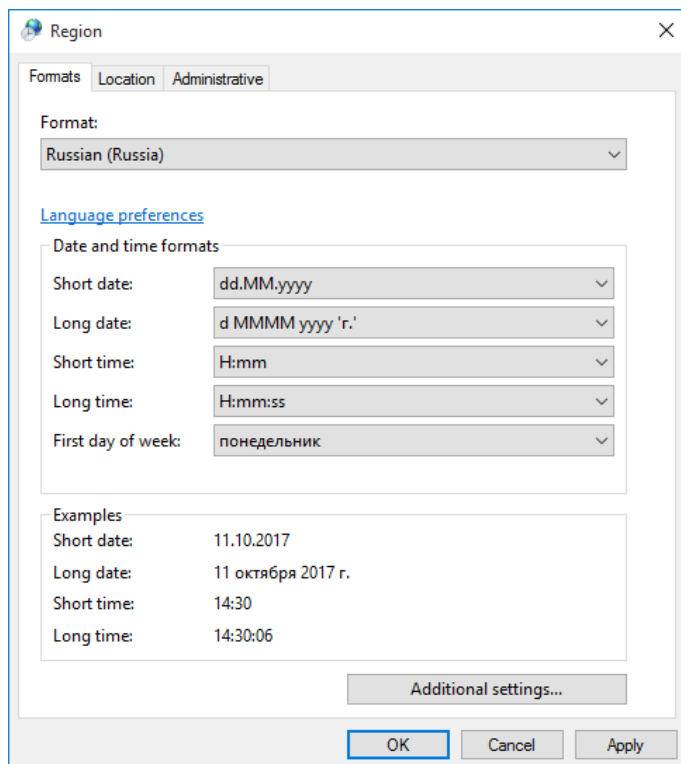


Рисунок 45. Настройка форматов

- 2 В окне **Регион (Region)** на вкладке **Местоположение (Location)** в списке **Основное расположение (Home location)** выберите **Россия (Russia)**.



Примечание. В Windows 10 версии 1809 и выше нет вкладки **Location**, поэтому указанный параметр настраивать не нужно.

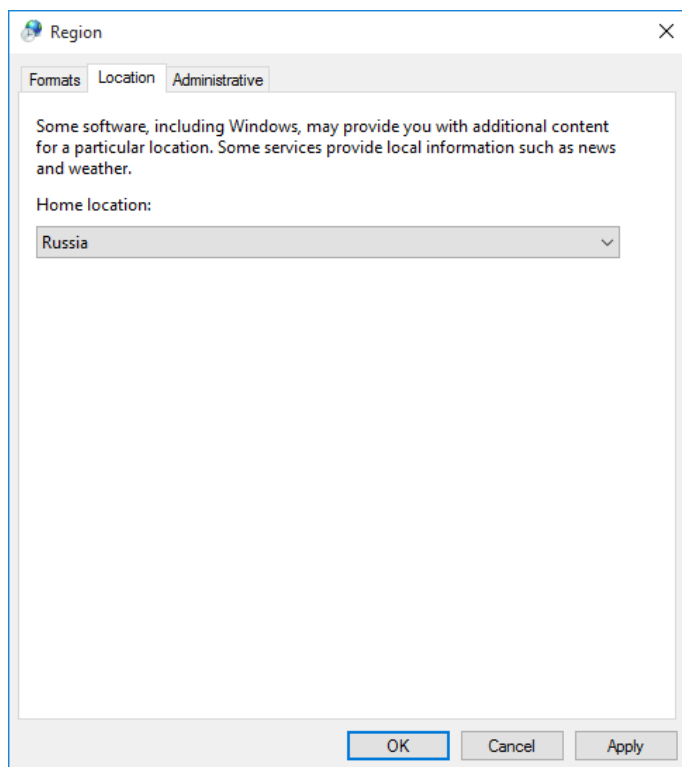


Рисунок 46. Выбор текущего расположения

С

Внешние устройства

Общие сведения

Внешние устройства предназначены для хранения контейнеров ключей, которые вы можете использовать для аутентификации, формирования [электронной подписи](#) (см. глоссарий, стр. 90) или для других целей.

На внешнем устройстве могут храниться ключи, созданные по различным алгоритмам в программном обеспечении ViPNet или в сторонних программах. Максимальное количество контейнеров ключей, которое может храниться на одном внешнем устройстве, зависит от объема памяти устройства.

Все операции с контейнерами ключей и внешними устройствами вы можете выполнить в программе ViPNet CSP. Чтобы использовать какое-либо внешнее устройство, на компьютер необходимо установить драйверы этого устройства. Перед записью ключей на устройство убедитесь, что оно отформатировано.

Список поддерживаемых внешних устройств

В следующей таблице перечислены внешние устройства, которые могут быть использованы в программном обеспечении ViPNet. Для каждого семейства устройств в таблице приведено описание, указаны условия и особенности работы с устройствами.

Таблица 7. Поддерживаемые внешние устройства

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
ESMART Token	Смарт-карты и токены типов ESMART Token , ESMART Token ГОСТ	<p>На компьютере должно быть установлено ПО ESMART PKI Client для Windows (рекомендуемая версия — 4.3 R1).</p> <p>Устройства типа ESMART Token необходимо отформатировать с помощью ПО ESMART PKI Client для Windows с профилем ViPNet2.</p> <p>Перенос ключей подписи с устройства и на устройство ESMART Token ГОСТ невозможен, так как на устройстве используется аппаратная криптография с неизвлекаемым ключом.</p> <p>На устройстве типа ESMART Token ГОСТ нельзя создать запрос на сертификат, в поле «назначение» которого присутствует «шифрование».</p>
Infotecs Software Token	Infotecs Software Token — программная реализация стандарта PKCS#11	<p>Необходимое ПО входит в поставку ViPNet CSP. С помощью программы token_manager.exe на компьютере должен быть создан программный токен.</p> <p>Подробную информацию о работе с программным токеном см. в документе «ViPNet SoftToken. Руководство разработчика», раздел «Использование утилиты token_manager для работы с программными токенами».</p>
A-Key	Смарт-карты aKey S1000 , aKey S1003 , aKey S1004 производства компании Ak Kamal Security	<p>На компьютере должна быть установлена библиотека akpkcs11.dll, предоставленная компанией Ak Kamal Security.</p> <p>Устройство имеет два ПИН-кода: администратора и пользователя. Значение этих ПИН-кодов по умолчанию — 12345678.</p> <p>Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.</p>
ViPNet HSM	Программно-аппаратный комплекс ViPNet HSM производства ОАО «ИнфоТеКС»	В программе ViPNet CSP необходимо задать параметры подключения к серверу ViPNet HSM.

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
JaCarta	Персональные электронные ключи и смарт-карты JaCarta PKI и JaCarta PKI/ГОСТ производства компании «Аладдин Р.Д.»	<p>На компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая версия — 2.9.0.1531).</p> <p>Устройства JaCarta PKI/ГОСТ определяются как принадлежащие одновременно к семействам JaCarta и eToken GOST/JaCarta GOST. Во избежание возникновения проблем рекомендуется запретить опрос неиспользуемого семейства устройств.</p> <p>При использовании устройства JaCarta PKI/ГОСТ во избежание появления ошибок не следует сохранять ПИН-коды этого устройства на компьютере.</p>
JCDS	Смарт-карты Gemalto Optelio Contactless D72, KONA 131 72K и токен JaCarta LT с апплетом от компании «Аладдин Р.Д.»	<p>На карту или токен должен быть загружен апплет Datastore, позволяющий модулю jcpkcs11ds.dll (рекомендуемая версия — 1.1.3.20) производства компании «Аладдин Р.Д.» работать с картой или токеном.</p> <p>Для администрирования токенов JaCarta LT на компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая версия — 2.9.0.1531).</p>
Siemens CardOS	Смарт-карты CardOS/M4.01a, CardOS V4.3B, CardOS V4.2B, CardOS V4.2B DI, CardOS V4.2C, CardOS V4.4 производства компании Atos (Siemens)	<p>На компьютере должно быть установлено ПО Siemens CardOS API V5.0.</p> <p>Смарт-карты должны быть особым образом размечены. Обратитесь к производителю устройств.</p>
eToken GOST/JaCarta GOST	Персональные электронные ключи eToken ГОСТ и JaCarta ГОСТ , а также персональные электронные ключи и смарт-карты JaCarta PKI/ГОСТ производства компании «Аладдин Р.Д.»	<p>Для работы с указанными устройствами на компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая версия — 2.9.0.1531).</p> <p>Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.</p> <p>Устройства JaCarta PKI/ГОСТ определяются как принадлежащие одновременно к семействам JaCarta и eToken GOST/JaCarta GOST. Во избежание возникновения проблем рекомендуется запретить опрос неиспользуемого семейства устройств.</p>

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
Rutoken ECP/ Rutoken Lite	Электронные идентификаторы Рутокен ЭЦП , Рутокен ЭЦП 2.0 и Рутокен Lite производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.6.0.0). Перенос ключей подписи с устройств, а также на устройства Рутокен ЭЦП и Рутокен ЭЦП 2.0 невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.
Rutoken/ Rutoken S	Электронные идентификаторы Рутокен и Рутокен S производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.6.0.0).
SafeNet eToken (eToken Aladdin)	Персональные электронные ключи Gemalto SafeNet eToken 5100/5105, 5200/5205, 5110, 7300 , смарт-карта Gemalto SafeNet eToken 4100 производства компании Gemalto (SafeNet) Персональные электронные ключи eToken PRO (Java) , eToken PRO , смарт-карты eToken PRO (Java) , eToken PRO , JaCarta PRO производства компании «Аладдин Р.Д.»	Если компьютер работает под управлением ОС Windows 10, на нем должно быть установлено ПО SafeNet Authentication Client (рекомендуемая версия — 10.4.40). Если компьютер работает под управлением другой ОС, на нем должно быть установлено либо ПО PKI Client версии 5.1 SP1, либо ПО SafeNet Authentication Client (рекомендуемая версия — 10.4.40). Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC-совместимым устройством считывания карт. Для работы смарт-карты JaCarta PRO на компьютере должно быть установлено ПО JC-PROClient версии 1.0.6 и должен быть включен режим совместимости с eToken. Примечание. Если вам необходимо работать с устройством из семейства SafeNet eToken (eToken Aladdin) , а также с устройством из семейства JaCarta , JCDS или eToken GOST/JaCarta GOST , то во избежание появления ошибок при выполнении криптографических операций не устанавливайте на компьютер одновременно ПО «Единый Клиент JaCarta» и ПО SafeNet Authentication Client.



Примечание. Список поддерживаемых операционных систем для каждого из приведенных устройств вы найдете на официальном веб-сайте производителя этого устройства.

Алгоритмы и функции, поддерживаемые внешними устройствами

В следующей таблице перечислены криптографические алгоритмы, поддерживаемые внешними устройствами, приведена информация о возможности использования устройств в качестве датчиков случайных чисел, а также информация о поддержке стандарта PKCS#11.



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

Таблица 8. Алгоритмы и функции, поддерживаемые внешними устройствами

Название семейства устройств в программе ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Использование ДСЧ в ViPNet CSP	Поддержка PKCS#11
ESMART Token	ESMART Token — отсутствует; ESMART Token ГОСТ — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (может не поддерживаться на старых устройствах)	ESMART Token — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 ESMART Token ГОСТ — отсутствует	Нет	Да
Infotecs Software Token	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (изолированная программная реализация)	отсутствует	Нет	Да
A-Key	aKey S1000, aKey S1003, aKey S1004 — ГОСТ Р 34.10-2012; aKey S1000, aKey S1003 — ГОСТ Р 34.10-2001	отсутствует	Нет	Да
ViPNet HSM	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	отсутствует	Нет	Да
JaCarta	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да

Название семейства устройств в программе ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Использование ДСЧ в ViPNet CSP	Поддержка PKCS#11
JCDS	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
Siemens CardOS	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
eToken GOST/ JaCarta GOST	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	отсутствует	Да	Да
Rutoken ECP/ Rutoken Lite	Рутокен ЭЦП — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ); Рутокен ЭЦП 2.0 — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012; Рутокен Lite — отсутствует	Рутокен ЭЦП — отсутствует; Рутокен ЭЦП 2.0 — отсутствует; Рутокен Lite — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	ЭЦП — да; ЭЦП 2.0 — да; Lite — нет	Да
Rutoken/ Rutoken S	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
SafeNet eToken (eToken Aladdin)	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да



Примечание. Выработка ключей шифрования (функция `C_DeriveKey` интерфейса PKCS#11) поддерживается не всеми перечисленными устройствами. Для получения более подробной информации см. документацию по необходимому устройству.



Глоссарий

SQL-сервер

Сервер базы данных, который работает под управлением программного обеспечения Microsoft SQL Server.

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 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.

Аккредитованный удостоверяющий центр

Удостоверяющий центр, прошедший аккредитацию в уполномоченном федеральном органе исполнительной власти <http://minsvyaz.ru/ru/activity/govservices/2/#section-list-of-accredited-centers> в соответствии с требованиями Федерального закона от 6 апреля 2011г. № 63-ФЗ «Об электронной подписи».

Аутентификация

Процесс идентификации пользователя, как правило, на основании его учетной записи. Аутентификация служит для подтверждения того, что входящий в систему пользователь является тем, за кого себя выдает, но процесс аутентификации не затрагивает права доступа пользователя (в отличие от авторизации).

Вышестоящий удостоверяющий центр

Удостоверяющий центр, который является вышестоящим по отношению к другому удостоверяющему центру в иерархической системе доверительных отношений между удостоверяющими центрами. При этом может быть подчиненным по отношению к третьему удостоверяющему центру, если не является головным.

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 проверки электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом проверки электронной подписи называется открытый ключ, который является не секретной частью пары асимметричных ключей и представляет собой уникальную

последовательность символов, однозначно связанную с закрытым ключом и предназначенную для проверки подлинности электронной подписи.

Ключ электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом электронной подписи называется закрытый ключ, который является секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Ключи пользователя ViPNet

Совокупность ключей, которые необходимы пользователю для аутентификации в сети ViPNet и шифрования других ключей, и к которым имеет доступ только данный пользователь.

Ключи пользователя могут содержать:

- действующий персональный ключ пользователя;
- ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи;
- хэш пароля пользователя.

Содержимое ключей пользователя формируется в зависимости от типа аутентификации пользователя.

Ключи узла ViPNet

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

Координатор (ViPNet-координатор)

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

Лицензия на сеть

Разрешение на пользование определенным набором функций продуктовой линейки ViPNet. В частности, лицензия на сеть ViPNet определяет следующее: номер сети, максимальное количество координаторов и клиентов, максимальное суммарное количество адресов, туннелируемых координаторами сети, максимальное количество узлов, на которые можно добавить ту или иную роль, максимальную разрешенную версию программного обеспечения ViPNet, срок действия лицензии и другие параметры.

Мастер-ключ

Ключ, который администратор сети ViPNet использует для формирования симметричных ключей пользователей и узлов. В сети ViPNet формируется три вида мастер-ключей:

- мастер-ключ ключей обмена;
- мастер-ключ ключей защиты ключей обмена;
- мастер-ключ персональных ключей пользователей.

Мастер-ключ формируется с помощью датчика случайных чисел. Он хранится в программе ViPNet Удостоверяющий и ключевой центр в полной секретности, поскольку компрометация мастер-ключа приводит к компрометации всех ключей, сформированных на его основе.

Межсетевой экран

Устройство на границе локальной сети, служащее для предотвращения несанкционированного доступа из одной сети в другую. Межсетевой экран проверяет весь входящий и исходящий IP-трафик, после чего принимается решение о возможности дальнейшего направления трафика к пункту назначения. Межсетевой экран обычно осуществляет преобразование внутренних адресов в адреса, доступные из внешней сети (выполняет NAT).

Обновление ключей узла

Совокупность файлов, к которым относятся справочники сертификатов администраторов УКЦ (файл *.tr1), списки аннулированных сертификатов своей и доверенных сетей (файлы *.crl, *.p7s), контрольные суммы паролей администраторов, корневые сертификаты администраторов доверенных сетей и служебная информация о пользователе узла, на котором обновляются ключи (право подписи). Фактически, обновление ключей узла является неполным вариантом ключей узла ViPNet.

Подчиненный удостоверяющий центр

Удостоверяющий центр, сертификат администратора которого заверен вышестоящим удостоверяющим центром.

Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью.

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 устройствами. 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.

Справочники и ключи

Справочники, ключи узла и ключи пользователя.

Точка распространения данных

Источник, доступный по общеизвестным протоколам (например, HTTP или LDAP), используемый для размещения сформированной в удостоверяющем центре информации (сертификатов издателей и списков аннулированных сертификатов).

Транспортный модуль (MFTP)

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

Удостоверяющий центр

Организация, осуществляющая выпуск сертификатов ключей проверки электронной подписи, а также сертификатов другого назначения.

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. Полученная последовательность используется при формировании ключей узла.