



Развертывание сети ViPNet CUSTOM 4.x

Руководство администратора

1991–2013 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00110-03 32 02

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

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

ViPNet является зарегистрированной торговой маркой программного обеспечения, разрабатываемого ОАО «ИнфоТеКС».

Все торговые марки и названия программ являются собственностью их владельцев.

ОАО «ИнфоТеКС»

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

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

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

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение.....	5
О документе	6
Для кого предназначен документ	6
Соглашения документа.....	6
Обратная связь	8
Глава 1. Общее представление о сети ViPNet.....	9
Конфигурации сети ViPNet	10
Описание узлов сети ViPNet.....	12
Защита IP-трафика в сети ViPNet.....	19
Глава 2. Подготовка к развертыванию сети ViPNet	21
Планирование сети.....	22
Перечень вопросов для определения оптимальной конфигурации сети ViPNet.....	24
Развертывание рабочих мест администраторов	26
Рекомендации по установке	26
Установка ViPNet Administrator.....	28
Глава 3. Создание топологии сети в ViPNet Administrator	30
Создание сетевых узлов и пользователей	31
Создание сети с помощью мастера.....	31
Дополнительная настройка сети.....	33
Рекомендации по созданию связей.....	33
Добавление ролей на сетевые узлы	37
Настройка свойств сетевых узлов.....	39
Создание дистрибутивов ключей.....	40
Глава 4. Развертывание координатора.....	41
Рекомендации по установке	42
Установка ПО ViPNet Coordinator	44
Настройка ПО ViPNet Coordinator	46

Глава 5. Развертывание клиента	47
Рекомендации по установке	48
Настройка ПО ViPNet Client.....	50
Глава 6. Проверка функционирования сети ViPNet	51
Приложение А. Глоссарий.....	52
Приложение В. Указатель	55



Введение

О документе	6
Обратная связь	8

О документе

Данный документ входит в комплект пользовательской документации к программному комплексу ViPNet CUSTOM.

Документ дает общее представление о сетях ViPNet и позволяет определить, какая конфигурация сети ViPNet более всего удовлетворяет задачам защиты данных и коммуникации, стоящим перед вашей компанией. Также в документе содержится пошаговое руководство по развертыванию типовой сети ViPNet, включающей рабочее место администратора сети, один или несколько координаторов и клиентские рабочие места.

Для кого предназначен документ

Документ адресован высшему руководству компаний, руководителям IT-отделов, системным администраторам, желающим ознакомиться с некоторыми способами организации сетей ViPNet. Помимо этого, документ будет полезен IT-специалистам, выполняющим развертывание сети ViPNet, без необходимости погружения во все особенности и технические подробности технологии ViPNet.

Соглашения документа

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

Таблица 1. Обозначения, используемые в примечаниях




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

Таблица 2. Обозначения, используемые для выделения информации в тексте

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

Обратная связь

Дополнительная информация

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

- Веб-портал документации ViPNet <http://docs.infotecs.ru>.
- Сборник часто задаваемых вопросов (FAQ) <http://www.infotecs.ru/support/faq/>.
- Законодательная база в сфере защиты информации <http://www.infotecs.ru/laws/>.
- Информация о решениях ViPNet <http://www.infotecs.ru/solutions/vpn/>.

Контактная информация

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

- Электронный адрес службы поддержки: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки <http://www.infotecs.ru/support/request/>.
- Форум ОАО «ИнфоТеКС» <http://www.infotecs.ru/forum>.
- 8 (495) 737-6196 — «горячая линия» службы технической поддержки.
- 8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

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



1

Общее представление о сети ViPNet

Конфигурации сети ViPNet	10
Описание узлов сети ViPNet	12
Защита IP-трафика в сети ViPNet	19

Конфигурации сети ViPNet

Программный комплекс ViPNet CUSTOM позволяет развертывать частные виртуальные сети любых конфигураций, обеспечивающие прозрачное взаимодействие узлов сети независимо от способа их подключения, расположения и типов IP-адресов. Сети ViPNet (см. «Сеть ViPNet» на стр. 54) позволяют безопасно передавать информацию по общедоступным каналам связи различных типов. Это достигается путем создания логических сетей, защищенных криптографическими средствами высокой надежности.

Сети ViPNet обеспечивают следующие возможности:

- Плавная интеграция в структуру существующей сети.
- Защита трафика путем шифрования.
- Гибкая настройка фильтрации защищенного и открытого трафика.
- Централизованное управление политиками безопасности (см. «[Политика безопасности](#)» на стр. 53).
- Широкий выбор средств коммуникации между защищенными узлами (см. «[Защищенный узел](#)» на стр. 52) (почта, чат, обмен файлами).
- Система слежения за состоянием сети.
- Организация иерархической системы сетей.
- Организация удостоверяющего центра, издание сертификатов открытых ключей подписи (см. «[Сертификат открытого ключа подписи пользователя](#)» на стр. 54).
- Дополнительные возможности по регистрации пользователей, публикации сертификатов в общедоступных хранилищах.

Построение сетей ViPNet — процесс, имеющий свои особенности в каждом конкретном случае. В первую очередь он зависит от существующей топологии сети и от тех коммуникационных задач, которые стоят перед организацией. Именно поэтому универсальной схемы сети ViPNet не существует. В данном документе представлено описание лишь одного из типовых вариантов сети, построенной на базе программного комплекса ViPNet CUSTOM.

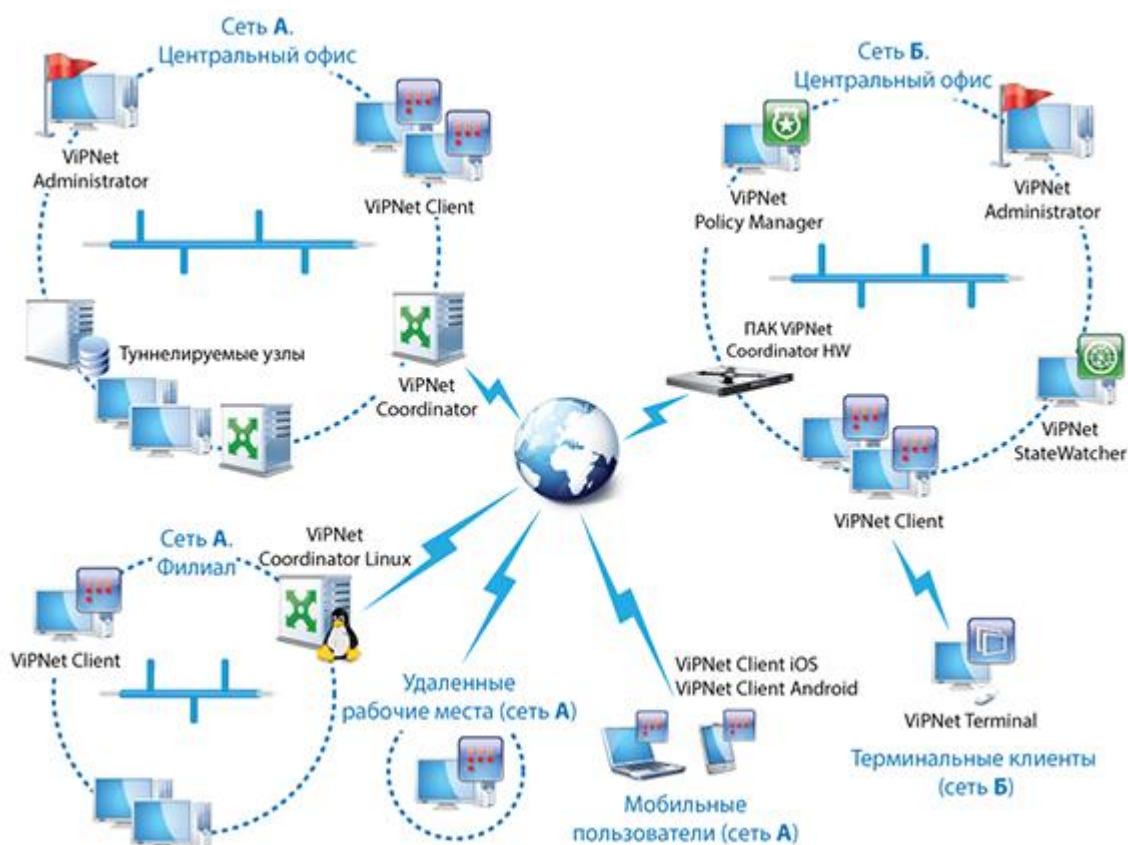


Рисунок 1: Схема сети на базе программного комплекса ViPNet CUSTOM

В приведенном на схеме примере технология ViPNet позволяет объединить центральный офис компании «А», филиалы, удаленных пользователей (например, сотрудников, работающих на дому) и мобильных пользователей (сотрудников в командировке, на выезде) в защищенную сеть. Кроме того, можно организовать защищенное взаимодействие сети компании «А» с сетью компании «Б», если в сети последней также используется технология ViPNet.

Описание узлов сети ViPNet

Для обеспечения безопасности корпоративной сети необходима установка программного обеспечения ViPNet, которое позволяет защитить сетевой трафик, письма и файлы, передаваемые по сети, а также информацию, хранящуюся на компьютерах. При этом доступ к защищенному компьютеру открытых или других защищенных компьютеров может быть в той или иной степени ограничен.

Для организации такой защиты необходимы следующие базовые элементы сети:

- Рабочее место администратора сети ViPNet со следующим установленным ПО:
 - ПО ViPNet Administrator, состоящее из следующих компонентов:
 - серверное приложение ViPNet Центр управления сетью (ЦУС);
 - одно или несколько клиентских приложений ЦУСа;
 - программа ViPNet Удостоверяющий и ключевой центр (УКЦ).
 - ПО ViPNet Client для организации обмена служебной информацией с другими узлами сети ViPNet (см. «Сетевой узел ViPNet» на стр. 54).
- Один или несколько серверов с установленным ПО ViPNet Coordinator, ViPNet Coordinator Linux или программно-аппаратных комплексов ViPNet Coordinator HW. Обычно такие узлы (далее «координаторы») устанавливаются на границе сети или на границах участков сети. В зависимости от своих задач в сети такие узлы могут выполнять различные функции (см. таблицу).
- Компьютеры пользователей с установленным ПО ViPNet Client, ViPNet Terminal или ViPNet CryptoService (далее «клиенты»).

Помимо перечисленных базовых элементов, в сети ViPNet могут присутствовать и другие функциональные компоненты, например компоненты, решающие задачи резервирования, мониторинга, управления политиками безопасности, общего доступа к сертификатам. Разновидности ПО ViPNet, используемого при организации частных виртуальных сетей, представлены на схеме ниже.

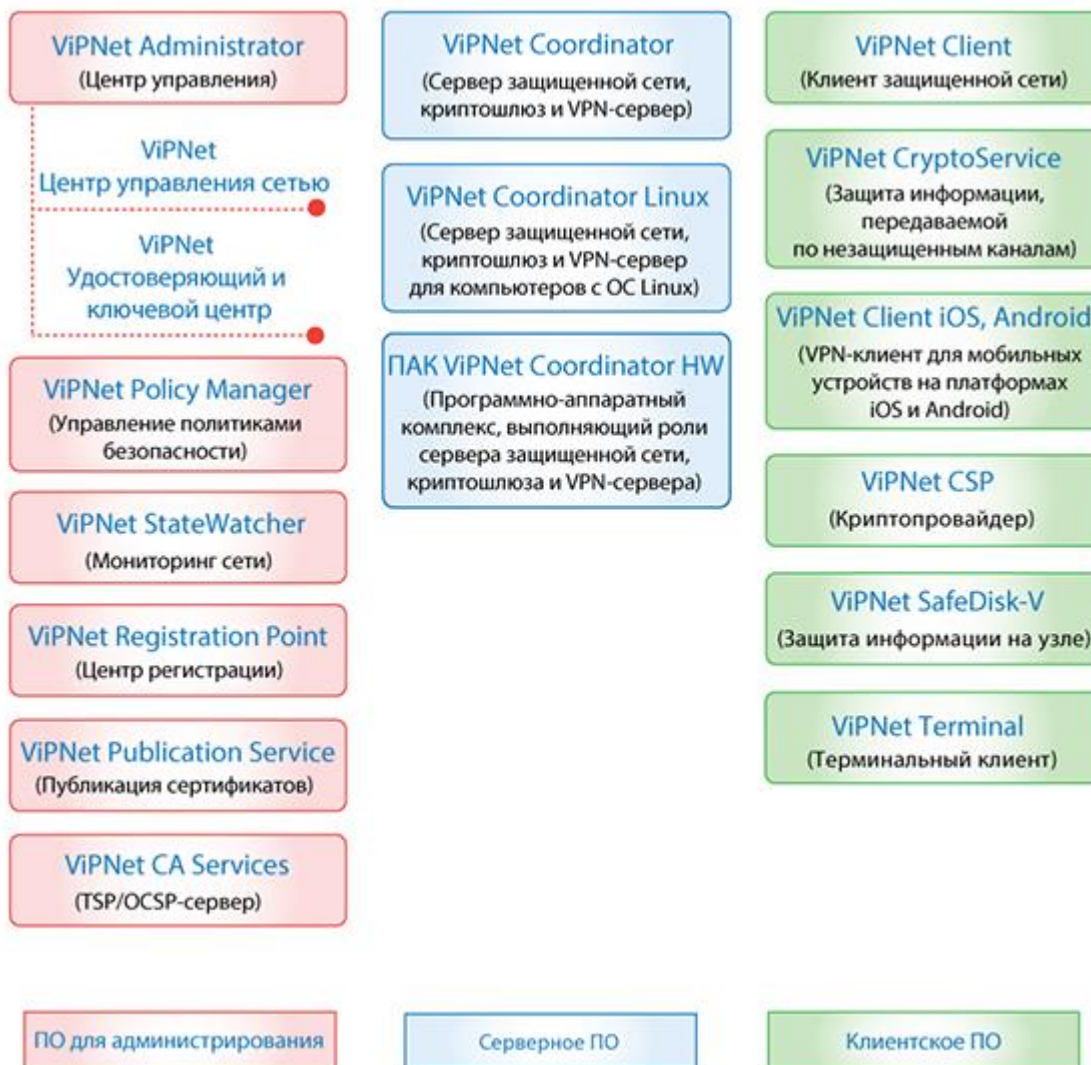




Рисунок 2: Программное обеспечение ViPNet, используемое при организации частных виртуальных сетей

Описание функций и ролей (см. «Роль» на стр. 53) узлов, из которых может состоять защищенная сеть ViPNet, приведено в таблице.

Таблица 3. Назначение узлов сети ViPNet

Узел сети ViPNet	Описание
 <p data-bbox="279 539 486 636">ViPNet Центр управления сетью (ЦУС)</p>	<p data-bbox="571 394 1372 456">Обязательный компонент сети ViPNet. Выполняет следующие основные функции:</p> <ul data-bbox="571 472 1372 629" style="list-style-type: none"> • Создание и модификация топологии сети ViPNet. • Разграничение уровней полномочий пользователей сети. • Отправка ключей, полученных из УКЦ, информации о топологии сети, а также обновлений ключей и ПО на сетевые узлы. <p data-bbox="571 651 1372 680">Роли: «Центр управления сетью», «VPN-клиент».</p> <p data-bbox="571 703 1372 766">Описание развертывания рабочего места администратора см. в разделе Развертывание рабочих мест администраторов (на стр. 26).</p> <p data-bbox="571 788 1372 846">Подробную информацию о программе вы найдете в документе «ViPNet Центр управления сетью. Руководство администратора».</p>
 <p data-bbox="279 1014 486 1144">ViPNet Удостоверяющий и ключевой центр (УКЦ)</p>	<p data-bbox="571 869 1372 931">Обязательный компонент сети ViPNet. Выполняет следующие функции:</p> <ul data-bbox="571 947 1372 1227" style="list-style-type: none"> • Формирование ключевой структуры сети. • Издание и управление сертификатами пользователей, в том числе квалифицированными сертификатами в формате, соответствующем требованиям приказа ФСБ РФ от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи» и требованиям Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». <p data-bbox="571 1249 1372 1507">УКЦ в сети ViPNet взаимодействует только с базой данных SQL, находящейся на компьютере с серверным приложением ЦУСа. УКЦ получает из базы данных информацию об узлах и пользователях сети, на основе которой формирует ключи, а затем отправляет их обратно в базу данных. Поэтому из соображений безопасности рекомендуется не включать компьютер с УКЦ в общую сеть ViPNet, а обеспечить связь только с компьютером, на котором размещено серверное приложение ЦУСа.</p> <p data-bbox="571 1529 1372 1559">Роли: если компьютер с УКЦ подключен к сети — «VPN-клиент».</p> <p data-bbox="571 1581 1372 1644">Описание развертывания рабочего места администратора см. в разделе Развертывание рабочих мест администраторов (на стр. 26).</p> <p data-bbox="571 1666 1372 1760">Подробную информацию о программе вы найдете в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».</p> <p data-bbox="571 1783 1372 1872">Для автоматической выдачи сертификатов по запросам пользователей и управления их жизненным циклом, вы можете также установить на узел с УКЦ веб-службу ViPNet CA Web Service.</p>

Подробную информацию о веб-службе ViPNet CA Web Service вы найдете в документе «ViPNet CA Web Service. Руководство администратора».

Чтобы организовать информирование пользователей, для которых в УКЦ изданы сертификаты, а также администраторов УКЦ о событиях, связанных с сертификатами, вы можете также установить на узел с УКЦ программу ViPNet CA Informing.

Подробную информацию о программе ViPNet CA Informing вы найдете в документе «ViPNet CA Informing. Руководство администратора».



ViPNet Policy Manager

Программа предназначена для централизованного управления политиками безопасности узлов, входящих в состав сети ViPNet. Централизованное управление особенно актуально для больших сетей, состоящих из сотен и тысяч узлов, однородных по выполняемой задаче и характеру сетевого окружения.

Роли: «Policy Manager», «VPN-клиент».

Подробную информацию о программе вы найдете в документе «ViPNet Policy Manager. Руководство администратора».



ViPNet StateWatcher

Система централизованного мониторинга сети ViPNet. Выполняет следующие основные функции:

- Сбор информации о текущем состоянии узлов сети ViPNet и установленных на них компонентов ПО ViPNet.
- Анализ информации для определения состояния узлов и выявления критических событий на них.
- Оповещение администратора о сбоях в работе узлов и критических событиях на них.
- Разграничение доступа к информации и управлению системой мониторинга.

Роли: «StateWatcher», «VPN-клиент».

Подробную информацию о программе вы найдете в документе «ViPNet StateWatcher. Руководство администратора».



ViPNet Registration Point

Программа предназначена для регистрации пользователей ViPNet и хранения их регистрационных данных, а также для выдачи сертификатов подписи и дистрибутивов ключей, создаваемых в программе ViPNet Удостоверяющий и ключевой центр по соответствующим запросам.

Роль: «Registration Point», «VPN-клиент».

Подробную информацию о программе вы найдете в документе «ViPNet Registration Point. Руководство администратора».



ViPNet Publication Service

Основное назначение программы — публикация сертификатов и списков отзыванных сертификатов в общедоступных хранилищах данных. Публикация сертификатов применяется в процессе защищенного обмена информацией между пользователями сети ViPNet и пользователями, не входящими в сеть ViPNet.

Роли: «Publication Service», при необходимости — «ViPNet Client».

Подробную информацию о программе вы найдете в документе «ViPNet Publication Service. Руководство администратора».



ViPNet CA Services

Программа позволяет развернуть на узле сети ViPNet TSP/OCSP-сервер и осуществляет выдачу штампов времени пользователям по TSP-запросам.

Роль: «Сервер TSP/OCSP».

Подробную информацию о программе вы найдете в документе «ViPNet CA Services. Руководство администратора».



ViPNet Coordinator

Координатором в терминологии ViPNet называется сервер с ПО ViPNet Coordinator (или ViPNet Coordinator Linux) либо программно-аппаратный комплекс ViPNet Coordinator HW. Координатор является обязательным компонентом сети ViPNet. В зависимости от круга задач в корпоративной сети он может выполнять следующие функции:

- Сервер IP-адресов.
- Маршрутизатор VPN-пакетов.
- VPN-шлюз.
- Сервер-маршрутизатор.
- Межсетевой экран.



ViPNet Coordinator Linux

Для получения более подробной информации см. раздел [Планирование сети](#) (на стр. 22).



ПАК ViPNet Coordinator HW

Набор прикладных задач, которые задаются для координатора, может быть различным в зависимости от его роли и выполняемых функций в сети.

Описание и шаги по развертыванию координатора см. в разделе Развертывание координатора (на стр. 41).

Подробную информацию о координаторах ViPNet вы найдете в документах «ViPNet Coordinator. Руководство администратора», «ViPNet Coordinator Linux. Руководство администратора», «ПАК ViPNet Coordinator HW. Руководство администратора».



ViPNet Client

Сетевой узел с ПО ViPNet Client выполняет следующие основные функции:

- Шифрование сетевого трафика компьютера.
- Фильтрация трафика (персональный сетевой экран — компонент ViPNet Монитор).
- Предоставление дополнительных функций для оперативного защищенного обмена сообщениями, проведения конференций, обмена файлами, обмена электронными письмами (компонент ViPNet Деловая почта).
- Защита от несанкционированной сетевой активности программ, установленных на компьютере (компонент ViPNet Контроль приложений).

Набор ролей, которые могут быть добавлены на клиент, может быть различным, в зависимости от его задач и выполняемых функций в сети. Для типового случая это роли «VPN-клиент» и «Деловая почта».

Описание и шаги по развертыванию рабочего места пользователя см. в разделе [Развертывание клиента](#) (на стр. 47).

Подробную информацию о программе вы найдете в документе «ViPNet Client. Руководство администратора».



ViPNet Terminal

Сетевой узел с программным обеспечением ViPNet Terminal выполняет роль терминального клиента и позволяет организовать защищенный доступ к удаленному рабочему столу, опубликованным службам и приложениям на терминальном сервере.

Роль: «ViPNet Terminal».

Подробную информацию о программе вы найдете в документе «ViPNet Terminal. Руководство администратора».



ViPNet CryptoService

Основная задача, выполняемая ПО ViPNet CryptoService — использование криптографических функций при обмене письмами и файлами. Благодаря наличию транспортного модуля, с помощью данного ПО можно автоматически обновлять сертификаты. В ViPNet CryptoService не включена функция защиты IP-трафика.

Роль: «CryptoService».

Подробную информацию о программе вы найдете в документе «ViPNet CryptoService. Руководство пользователя».



ViPNet Client iOS,
ViPNet Client Android

Приложения предназначены для защиты сетевого трафика при подключении мобильных устройств Apple и Android к сети ViPNet или к Интернету. Защита трафика выполняется благодаря функции шифрования, расшифрования и фильтрации IP-пакетов.

Роль: «VPN-клиент для мобильных устройств».

Подробную информацию о программе вы найдете в документах «ViPNet Client iOS. Руководство администратора», «ViPNet Client Android. Руководство администратора».



ViPNet CSP

Программа ViPNet CSP обеспечивает вызов криптографических функций из других приложений, то есть представляет собой криптопровайдер. Программа ViPNet CSP необходима для корректной работы большинства программ ViPNet и входит в их комплекты поставки.

На узле с программой ViPNet CSP пользователь может создавать запросы на сертификат для отправки в удостоверяющий центр и работать с полученным сертификатом.

Подробную информацию о программе вы найдете в документе «ViPNet CSP. Руководство пользователя».



ViPNet SafeDisk-V

Программа ViPNet SafeDisk-V предназначена для совместного использования с программой ViPNet Client и позволяет разграничить доступ пользователей к конфиденциальной информации, находящейся на сетевом узле.

Роли: «SafeDisk», «VPN-клиент».

Подробную информацию о программе вы найдете в документе «ViPNet SafeDisk-V. Руководство пользователя».



Открытые или
туннелируемые узлы

Открытые узлы сети ViPNet — это узлы, с которыми обмен информацией происходит в незашифрованном виде. Соединения с участием таких узлов могут быть защищены с помощью технологии туннелирования. Данная технология предполагает направление исходящего и входящего трафика узла через ViPNet Coordinator, где трафик фильтруется и защищается криптографическими методами (см. «[Защита IP-трафика в сети ViPNet](#)» на стр. 19).

Таким образом, перед развертыванием сети ViPNet необходимо определить круг задач, которые требуется решить в корпоративной сети, выбрать ПО ViPNet для решения этих задач и построить оптимальную логическую схему сети.

Защита IP-трафика в сети ViPNet

Обычно задачи по защите и разграничению доступа к информации не требуют тотальной защиты абсолютно всех узлов сети. Достаточно обеспечить защищенный обмен информацией на участках сети, не имеющих той степени доверия, которая регламентируется политикой безопасности компании. Таким образом, необходимо определить, какие участки сети являются небезопасными, и построить логическую сеть ViPNet так, чтобы на данных участках конфиденциальная информация была полностью защищена.

Рассмотрим, какой функциональностью по обмену и защите информации обладают узлы сети ViPNet.

Компьютер с установленным ПО ViPNet Client осуществляет шифрование исходящего трафика, а также функции по фильтрации и расшифрованию входящего трафика. Таким образом, информация, проходящая между двумя компьютерами с установленным ПО ViPNet Client, полностью защищена.



Рисунок 3: Обмен информацией между узлами ViPNet Client

При организации доступа к сети Интернет координатор ViPNet выступает в качестве межсетевого экрана и осуществляет фильтрацию открытого трафика для защиты локальных сетевых узлов. Кроме того, ViPNet Coordinator выполняет функции трансляции IP-адресов (NAT), и нет необходимости устанавливать дополнительные NAT-устройства на границе локальной и публичной сети. Если же такое устройство необходимо, можно настроить подключение координатора к Интернету через это устройство.



Рисунок 4: Обмен информацией между узлом ViPNet Client и Интернетом

Если требуется защитить информацию, которая проходит небезопасный участок сети (например, сеть Интернет), а внутри локальной сети защита не требуется, можно воспользоваться технологией туннелирования. Координатор, установленный между сетями, возьмет на себя все функции защиты сетевого трафика, а также функции маршрутизации.



Рисунок 5: Обмен информацией между открытыми узлами через Интернет

Таким образом, при составлении логической структуры сети ViPNet следует учитывать, на каких участках сети передача информации может быть небезопасной и каким способом ее требуется защитить.

Квалифицированную и детальную консультацию по структуре и составу сети предоставляют специалисты ОАО «ИнфоТеКС» (см. «[Обратная связь](#)» на стр. 8).

После определения и согласования всех описанных факторов можно переходить к планированию сети (см. «[Планирование сети](#)» на стр. 22).



2

Подготовка к развертыванию сети ViPNet

Планирование сети	22
Развертывание рабочих мест администраторов	26

Планирование сети

При планировании сети ViPNet следует исходить из задач, которые требуется решить с помощью комплекса ViPNet CUSTOM, существующей физической структуры сети организации и применяемой политики информационной безопасности.

Если организация, в которой планируется внедрить комплекс ViPNet CUSTOM, имеет несколько филиалов, в этих филиалах можно развернуть собственные сети ViPNet и установить между ними межсетевое взаимодействие. В этом случае целесообразно создать иерархическую структуру сетей ViPNet, чтобы централизованно управлять распределением лицензий в подчиненных сетях из главного Центра управления сетью (ЦУСа).

Логическая структура создаваемой сети ViPNet (в первую очередь, это привязка клиентов к координаторам) в большинстве случаев определяется существующей физической структурой сети. Комплекс ViPNet CUSTOM позволяет создавать структуры, объединяющие в единую защищенную виртуальную сеть произвольное количество локальных подсетей, удаленных и мобильных пользователей.

Координаторы, выступающие в качестве серверов сети ViPNet, в зависимости от потребностей и применяемой политики безопасности могут выполнять следующие задачи:

- **Сервер IP-адресов** — функция, которая в автоматическом режиме обеспечивает взаимодействие защищенных узлов (клиентов и координаторов) как внутри данной виртуальной сети, так и при взаимодействии с другими виртуальными сетями ViPNet. Это возможно благодаря использованию специального протокола динамической маршрутизации VPN-трафика, реализующего обмен информацией о параметрах доступа узлов друг к другу. Данный протокол обеспечивает маршрутизацию VPN-трафика между узлами в сети ViPNet тем методом, который наиболее оптимален для используемого способа подключения узла к сети.
- **Маршрутизатор VPN-пакетов** — функция, обеспечивающая маршрутизацию транзитного VPN-трафика, проходящего через координатор, на другие защищенные узлы. Маршрутизация осуществляется на основании идентификаторов защищенных узлов, содержащихся в открытой части VPN-пакетов, которая защищена от подделки, и на основании защищенного протокола динамической маршрутизации VPN-трафика. Одновременно выполняется функция трансляции адресов для VPN-трафика, и все пакеты, поступающие на координатор, отправляются на другие узлы от имени IP-адреса координатора. В случае фильтрации и трансляции трафика

сторонними устройствами координатор может выступать в роли координатора соединений (см. «[Координатор соединений](#)» на стр. 52).

- **VPN-шлюз** — стандартная для классических VPN функция, реализующая создание защищенных каналов (туннелей) посредством шифрования трафика открытых узлов, размещенных за координатором, и передачи этого трафика на другие VPN-шлюзы или защищенные клиенты. VPN-шлюз интегрирован с межсетевым экраном для защищенных и открытых соединений, который осуществляет фильтрацию незашифрованного трафика, а также трафика внутри защищенного соединения.
- **Сервер-маршрутизатор** — функция, которая обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений ключей и программного обеспечения из программы ViPNet Центр управления сетью, а также обмен прикладными транспортными конвертами между узлами.
- **Межсетевой экран** — функция, благодаря которой координатор выполняет фильтрацию открытых транзитных и локальных сетевых соединений по IP-адресам, протоколам, портам, направлениям соединений и другим параметрам на основании заданных правил. Одновременно координатор может выполнять функции трансляции адресов для проходящего через него открытого трафика.

Координаторы, работающие под ОС Windows, могут также выполнять функцию TCP-туннеля, то есть обеспечивать получение IP-пакетов по протоколу TCP и их дальнейшую передачу по протоколу UDP.

В сегментированных сетях можно использовать каскадную схему установки координаторов.

В качестве координаторов могут выступать серверы с установленным ПО ViPNet Coordinator и ViPNet Coordinator Linux, а также программно-аппаратные комплексы ViPNet Coordinator HW. Для создания отказоустойчивого решения на базе ПО ViPNet Coordinator Linux и ПАК ViPNet Coordinator HW предназначена система защиты от сбоев ViPNet Failover.

ПО ViPNet Coordinator или ViPNet Client, установленное на прикладном сервере, можно использовать для защиты трафика определенных прикладных серверов (например, контроллер домена, SMTP/FTP/веб-серверы, сервер базы данных).

В сети ViPNet существует возможность централизованного управления политиками безопасности на сетевых узлах. С помощью программы ViPNet Policy Manager, установленной на одном из клиентов, для отдельных узлов или групп формируются шаблоны политики безопасности, содержащие сетевые фильтры и правила трансляции.

С помощью ПО ViPNet Publication Service, входящего в состав комплекса ViPNet CUSTOM, можно организовать публикацию сертификатов пользователей сети ViPNet в общедоступных хранилищах сертификатов. Это может быть необходимо при взаимодействии со сторонними удостоверяющими центрами. Также в сети ViPNet с помощью ПО ViPNet Registration Point можно создать один или несколько центров регистрации пользователей.

Если на каких-либо рабочих местах защита трафика не требуется, можно установить на них ПО ViPNet CryptoService, обеспечивающее возможность использования криптографических функций в прикладных программах, а также работу с ключами подписи пользователя.

Для наблюдения за состоянием сетевых узлов в сети ViPNet можно развернуть комплекс мониторинга защищенной сети ViPNet StateWatcher. Сервер мониторинга собирает информацию о состоянии сетевых узлов и установленных на них компонентах ПО ViPNet. При обнаружении сбоев система оповещает об этом администратора сети.

Кроме того, сеть ViPNet может включать терминальные клиенты для организации защищенных удаленных рабочих мест пользователя, мобильные клиенты на платформе iOS или Android и другие специализированные решения.

Перечень вопросов для определения оптимальной конфигурации сети ViPNet

Чтобы определить оптимальную конфигурацию сети ViPNet, необходимо ответить на следующие вопросы:

- Сколько сетей ViPNet нужно создать, и требуется ли иерархическая система сетей ViPNet?
- Требуется ли установить ПО ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр на разные компьютеры?
- Будут ли в сети использоваться центры регистрации пользователей и сервис публикаций?
- Будет ли в сети использоваться система централизованного мониторинга, централизованное управление политиками безопасности?
- Сколько рабочих мест пользователей, серверов и сегментов локальной сети нуждаются в защите трафика?
- Какие открытые узлы должны туннелироваться координаторами?

- Какая логическая структура VPN-соединений наиболее полно отвечает существующей физической структуре сети?
- Сколько должно быть координаторов?
- Будет ли в сети использоваться система резервирования координаторов?
- Какие IP-адреса (публичные или частные) будут иметь координаторы?
- Требуется ли устанавливать координаторы на отдельные компьютеры или их можно совместить с какими-либо существующими серверами или рабочими станциями?
- Как оптимально распределить клиенты между координаторами?
- Как осуществляется доступ к координаторам из внешней сети? Как организована маршрутизация входящего и исходящего трафика и трансляция адресов? Какие типы сетевых экранов используются, осуществляется ли трансляция адресов? Желательно изобразить подробную схему топологии сети.
- Какие прикладные серверы планируется защищать с помощью VPN (серверы с базами данных, CRM/CMS/ERP-системами, веб-серверы и так далее)?
- Каков характер трафика между сегментами, серверами, рабочими станциями (используемые службы, номера портов и протоколов)?
- Как должны быть настроены интегрированные в ПО ViPNet сетевые экраны для правильной работы сети и сетевых сервисов? Например, клиенты и координаторы по умолчанию будут блокировать входящий нешифрованный трафик. Если на каких-либо сетевых устройствах, обеспечивающих работу общих сетевых сервисов, не установлено ПО ViPNet, то узлы ViPNet будут блокировать входящий трафик от этих устройств. Чтобы клиенты и координаторы могли обмениваться трафиком с такими сетевыми устройствами, в их интегрированных сетевых экранах должны быть заданы пропускающие фильтры для этих устройств. Трафик от других сетевых узлов ViPNet не блокируется.

Развертывание рабочих мест администраторов

Рекомендации по установке

Администрирование защищенной сети ViPNet осуществляется с помощью ПО ViPNet Administrator, которое включает два компонента:

- ViPNet Центр управления сетью (ЦУС) — предназначен для регистрации сетевых узлов и пользователей сети ViPNet, создания связей между ними, определения полномочий пользователей, централизованного обновления справочников (см. «Справочники» на стр. 54), ключей, программного обеспечения и так далее. ЦУС, в свою очередь, состоит из серверного и одного или нескольких клиентских приложений.
- ViPNet Удостоверяющий и ключевой центр (УКЦ) — предназначен для создания ключей и издания сертификатов открытого ключа подписи.

Для установки ПО ViPNet Administrator требуется соответствующий установочный комплект, а также файл лицензии `infotecs.reg`. Лицензия определяет ограничения на количество сетевых узлов, одновременно туннелируемых соединений, на роли, которые могут быть добавлены на сетевые узлы, и на количество сертификатов, которые могут быть изданы.

Серверное приложение ЦУСа и программу УКЦ можно установить на одном компьютере или на двух разных компьютерах, если этого требует политика безопасности. Одно или несколько клиентских приложений ЦУСа можно установить как на компьютер с остальными приложениями, входящими в ПО ViPNet Administrator, так и на отдельные компьютеры.

На компьютер с серверным приложением ЦУСа нужно обязательно установить ПО ViPNet Client.

На отдельных компьютерах с клиентскими приложениями ЦУСа следует выполнить следующие действия:

- 1 Установите ПО ViPNet Client.
- 2 Создайте в программе ViPNet Монитор (компонент ПО ViPNet Client) на компьютере с серверным приложением сетевой фильтр, разрешающий входящие соединения с открытыми узлами, на которых установлены клиентские приложения.

На отдельном компьютере с УКЦ установка ViPNet Client требуется только в случае необходимости в защите IP-трафика компьютера (этот компьютер можно не подключать к сети, соединив его только с компьютером с серверным приложением ЦУСа посредством кросс-кабеля).

Несколько сетей ViPNet можно объединить в иерархическую систему. Такая необходимость может возникнуть, если несколько удаленных филиалов организации имеют свои собственные сети ViPNet. В этом случае в главном ЦУСе осуществляется централизованное управление лицензиями подчиненных сетей.

Для организации иерархической системы сетей ViPNet требуется специальный файл лицензии `infotecs.reg` с поддержкой иерархии сетей, в котором указаны общие лицензионные ограничения на главную и подчиненные сети ViPNet, а также номера главной и подчиненных сетей. Сначала необходимо установить в главной сети ПО ViPNet Administrator, воспользовавшись для этого специальным общим файлом лицензии. Затем в главном ЦУСе следует распределить лицензионные ограничения для подчиненных сетей и сформировать для них файлы лицензии. После этого можно выполнять развертывание подчиненных сетей.

Для подготовки одного или нескольких рабочих мест администраторов сети ViPNet выполните следующие действия:

- 1 Установите на одном или нескольких компьютерах ПО ViPNet Administrator, для этого:
 - Установите серверное приложение ViPNet Центр управления сетью и программу ViPNet Удостоверяющий и ключевой центр на один и тот же или на разные компьютеры.
 - Установите на компьютер с серверным приложением или на любой другой компьютер сети клиентское приложение ViPNet Центр управления сетью.
 - В случае необходимости установите клиентские приложения на другие компьютеры сети.
- 2 В ЦУСе создайте структуру защищенной сети ViPNet (см. [«Создание топологии сети в ViPNet Administrator»](#) на стр. 30). В случае организации нескольких рабочих мест администраторов ЦУСа создайте учетную запись для каждого администратора.

- 3 В УКЦ сформируйте дистрибутивы ключей (см. «[Дистрибутив ключей](#)» на стр. 52) для узлов с серверным приложением ЦУСа, программой УКЦ и для узлов с клиентским приложением ЦУСа, на которых установлено ПО ViPNet Client.
- 4 На компьютерах, на которых установлено серверное приложение ЦУСа, установите ПО ViPNet Client.
- 5 На компьютерах, на которых установлено клиентское приложение ЦУСа, установите ПО ViPNet Client либо на компьютере с серверным приложением создайте сетевой фильтр, разрешающий входящие и соединения с открытыми узлами, на которых установлены клиентские приложения.

Установка ViPNet Administrator

Перед установкой компонентов ПО ViPNet Administrator убедитесь, что на компьютерах, на которых будет производиться установка, выполнены стандартные сетевые настройки, правильно заданы часовой пояс, дата и время. Отключите контроль учетных записей в соответствующей категории панели управления. Установку должен выполнять пользователь, обладающий правами администратора в ОС Windows.

Чтобы развернуть программное обеспечение ViPNet Центр управления сетью, требуется установить два компонента: серверное приложение и клиентское приложение. Для этого выполните следующие действия:

- 1 Убедитесь, что вы располагаете установочным комплектом программы ViPNet Центр управления сетью и файлом лицензии на сеть ViPNet. Выберите схему размещения компонентов программы ViPNet Центр управления сетью.
- 2 На рабочее место администратора или на специально выделенный сервер установите серверное приложение ViPNet Центр управления сетью. При установке серверного приложения:
 - На компьютер будут автоматически установлены сторонние программы, необходимые для работы серверного приложения.
 - Программа установки запросит файл лицензии `infotecs.reg`. Без этого файла продолжение установки будет невозможно.
 - Будут созданы экземпляр SQL-сервера и база данных для хранения структуры и параметров сети ViPNet.
- 3 На компьютер, на котором установлено серверное приложение, или на отдельный компьютер установите клиентское приложение ViPNet Центр управления сетью.

Вместе с клиентским приложением на компьютер будут автоматически установлены сторонние программы, необходимые для его работы.

- 4 Если требуется, установите клиентское приложение ViPNet Центр управления сетью на дополнительных рабочих местах администраторов.
- 5 Установите на компьютер с серверным приложением ViPNet Центр управления сетью программное обеспечение ViPNet Client, которое требуется для отправки обновлений из Центра управления сетью на сетевые узлы ViPNet.

После создания сети ViPNet и дистрибутивов ключей для сетевых узлов установите на компьютер с серверным приложением дистрибутив ключей для сетевого узла — Центра управления сетью.
- 6 При необходимости настройте подключение клиентских приложений к серверному приложению и создайте дополнительные учетные записи администраторов.

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

- 1 Установите программу ViPNet Удостоверяющий и ключевой центр на компьютер с серверным приложением ЦУСа или на отдельный компьютер. Файл лицензии при установке не запрашивается, так как лицензионные ограничения вступают в силу после подключения к базе данных, находящейся на компьютере с серверным приложением ЦУСа.
- 2 Выполните первый запуск программы. Во время первого запуска запустите мастер первичной инициализации или произведите конвертацию имеющейся у вас базы данных 3.x. Подробная информация о конвертации базы данных содержится в документе «ViPNet Administrator. Руководство по миграции с версии 3.x на версию 4.0».



Внимание! Выполнять первичную инициализацию целесообразно только после создания сети ViPNet в ЦУСе.

- 3 В процессе первичной инициализации:
 - Производится подключение к SQL-серверу, заполняется база данных.
 - Создается учетная запись администратора программы.
 - Издается сертификат администратора.
 - Создаются мастер-ключи.

Подробная информация об установке и первоначальной настройке ПО ViPNet Administrator содержится в документе «ViPNet Administrator. Руководство по установке».



3

Создание топологии сети в ViPNet Administrator

Создание сетевых узлов и пользователей	31
Добавление ролей на сетевые узлы	37
Настройка свойств сетевых узлов	39
Создание дистрибутивов ключей	40

Создание сетевых узлов и пользователей

Создание сети с помощью мастера

Структуру сети ViPNet удобнее всего создавать с помощью специального мастера **Создание сети ViPNet**, хотя также существует возможность создания структуры вручную. Для создания сетевых узлов и пользователей сети ViPNet с помощью мастера выполните следующие действия:

- 1 При первом запуске программы ViPNet Центр управления сетью в окне **Начало работы с ViPNet Центр управления сетью** щелкните ссылку **Сформировать структуру защищенной сети автоматически**, будет запущен мастер **Создание сети ViPNet**.



Примечание. Впоследствии, в случае необходимости, мастер можно будет запустить из главного окна клиентского приложения ViPNet Центр управления сетью. Для этого в меню **Моя сеть** выберите пункт **Создать сеть ViPNet**.

- 2 На странице **Координаторы защищенной сети ViPNet** укажите желаемое количество координаторов в сети ViPNet и задайте роли (см. [«Добавление ролей на сетевые узлы»](#) на стр. 37), которые будут добавлены на координаторы при их создании, установив соответствующие флажки.



Примечание. При задании количества сетевых узлов и добавлении ролей следует учитывать текущие лицензионные ограничения. Если ограничение на количество узлов с какой-либо ролью будет превышено, появится соответствующее предупреждение.

- 3 На странице **Клиенты защищенной сети ViPNet** укажите количество клиентов, которые должны быть зарегистрированы на каждом координаторе. Задайте роли, которые будут добавлены на клиенты при их создании, установив для этого соответствующие флажки.

- 4 На странице **Связи между объектами защищенной сети ViPNet** с помощью переключателя установите нужный тип организации связей между защищенными узлами. По умолчанию выбран вариант **Связать все сетевые узлы**.

Рекомендуется задать связи между пользователями связанных сетевых узлов, для этого установите соответствующий флажок.

На каждый созданный сетевой узел будет добавлен один пользователь, имя которого совпадает с именем сетевого узла.

- 5 На странице **Подготовка к созданию сети ViPNet завершена** установите флажок **Создать справочники для сетевых узлов**.

После того как процесс формирования первичной структуры сети будет завершен, будет создана следующая структура сети ViPNet:

- На каждом сетевом узле будет создано по одному пользователю.
- Первый созданный клиент будет зарегистрирован как Центр управления сетью.
- Между сетевыми узлами будут образованы связи, тип которых был указан при установке.
- Для всех сетевых узлов будут созданы справочники (на стр. 54).
- Между всеми координаторами будут образованы межсерверные каналы.



Примечание. Межсерверные каналы используются для обмена прикладными и управляющими конвертами (см. «[Прикладной конверт](#)» на стр. 53) между координаторами, выступающими в роли серверов-маршрутизаторов. После окончания работы мастера вы можете вручную настроить межсерверные каналы, например соединить все координаторы с одним центральным (схема «звезда») или соединить все координаторы по схеме «кольцо». Необходимо, однако, чтобы от каждого координатора к каждому существовал маршрут, иначе создание справочников будет невозможно.


После создания первичной структуры сети необходимо сделать дополнительные настройки (см. «[Дополнительная настройка сети](#)» на стр. 33).

Дополнительная настройка сети

После того как в мастере сформирована первичная структура сети, можно приступить к настройке параметров сетевых узлов и пользователей:

- Чтобы добавить пользователя на сетевой узел или удалить пользователя с сетевого узла, используйте окно свойств узла.
- Чтобы узлы могли взаимодействовать, необходимо создать связи между пользователями узлов. Информацию по созданию связей см. в разделе [Рекомендации по созданию связей](#) (на стр. 33).
- Информацию по добавлению ролей на сетевые узлы см. в разделе [Добавление ролей на сетевые узлы](#) (на стр. 37).
- Информацию по настройке свойств сетевых узлов см. в разделе [Настройка свойств сетевых узлов](#) (на стр. 39).

Если вы добавили сетевые узлы после окончания работы мастера, повторно создайте справочники для узлов. Для этого на панели управления нажмите кнопку **Создать**

справочники  и в окне **Создание справочников** нажмите кнопку **Создать для всего списка**.

После создания справочников информация о структуре сети становится доступной в программе ViPNet Удостоверяющий и ключевой центр. Создайте в УКЦ дистрибутивы ключей (см. «[Создание дистрибутивов ключей](#)» на стр. 40) для сетевых узлов и передайте их доверенным способом пользователям для установки на сетевых узлах ViPNet (подробнее см. документы «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», «ViPNet Coordinator. Руководство администратора», «ViPNet Client. Руководство пользователя», «ViPNet CryptoService. Руководство пользователя»).

Для получения более подробной инструкции по созданию сетевой структуры см. документ «ViPNet Центр управления сетью. Руководство администратора».

Рекомендации по созданию связей

После создания первичной структуры сети можно просмотреть и изменить списки сетевых узлов, с которыми связан клиент или координатор. Для этого выполните следующие действия:

- 1 В окне **ViPNet Центр управления сетью** выберите представление **Моя сеть**.

2 На панели навигации выберите раздел **Клиенты** или **Координаторы**, в зависимости от типа узла, который требуется настроить.

3 На панели просмотра дважды щелкните сетевой узел, связи которого требуется изменить.

4 В окне свойств сетевого узла на левой панели выберите раздел **Связи с узлами**.

На правой панели в разделе **Сетевые узлы, с которыми установлена связь** будет отображен список узлов своей и доверенных сетей, с которыми связан данный сетевой узел.

Связи с узлами, имена которых отображаются серым цветом, являются обязательными. Список можно редактировать, удаляя и добавляя связи.

Следующие рекомендации по созданию связей относятся к сетевым узлам, на которые добавлены роли «VPN-клиент» или «VPN-сервер».



Примечание. В данном разделе под выражением «клиенты данного координатора» подразумевается «клиенты, для которых данный координатор является сервером IP-адресов».

Для установления соединения между двумя клиентами сети необходимо, чтобы эти клиенты обладали информацией о параметрах доступа друг к другу. Такую информацию каждый клиент получает от своего сервера IP-адресов. Клиент также сообщает серверу IP-адресов информацию о собственных параметрах доступа. По умолчанию в качестве сервера IP-адресов используется координатор, на котором клиент зарегистрирован в ЦУСе, то есть его сервер-маршрутизатор. На клиенте в качестве сервера IP-адресов можно выбрать и другой координатор.

Координаторы обмениваются информацией о клиентах, для которых они являются серверами IP-адресов, с учетом связей, установленных между клиентами. Для обеспечения этого обмена в ЦУСе также должны быть установлены связи между координаторами, выполняющими функции сервера IP-адресов. Вы можете связать каждый координатор со всеми координаторами своей и чужих сетей, но в больших сетях это приведет к загрузке каналов служебной информацией, а координаторы будут загружены ее обработкой.

При задании связей между координаторами следует учитывать следующие особенности обмена служебной информацией между серверами IP-адресов:

- Координатор «А», являющийся сервером IP-адресов клиента «В», отправляет информацию об этом клиенте на координатор «С», если клиент «В» связан с координатором «С» или с клиентами координатора «С».

- Координатор «С», получивший информацию о клиенте «В» от координатора «А» своей сети ViPNet:
 - Никогда не передает ее третьему координатору своей сети, то есть цепочка передачи информации о клиентах в одной сети всегда состоит только из двух координаторов.
 - Если координатор «А» не связан с координаторами другой сети ViPNet, а клиент «В» связан с узлами другой сети, то координатор «С» передает полученную информацию на один из доступных координаторов этой сети (координатор «D»).
- Координатор «D», получивший информацию о клиенте «В» от координатора «С» другой сети, передает ее на координатор «Е» своей сети, если клиент «В» связан с координатором «Е» или с клиентами координатора «Е».

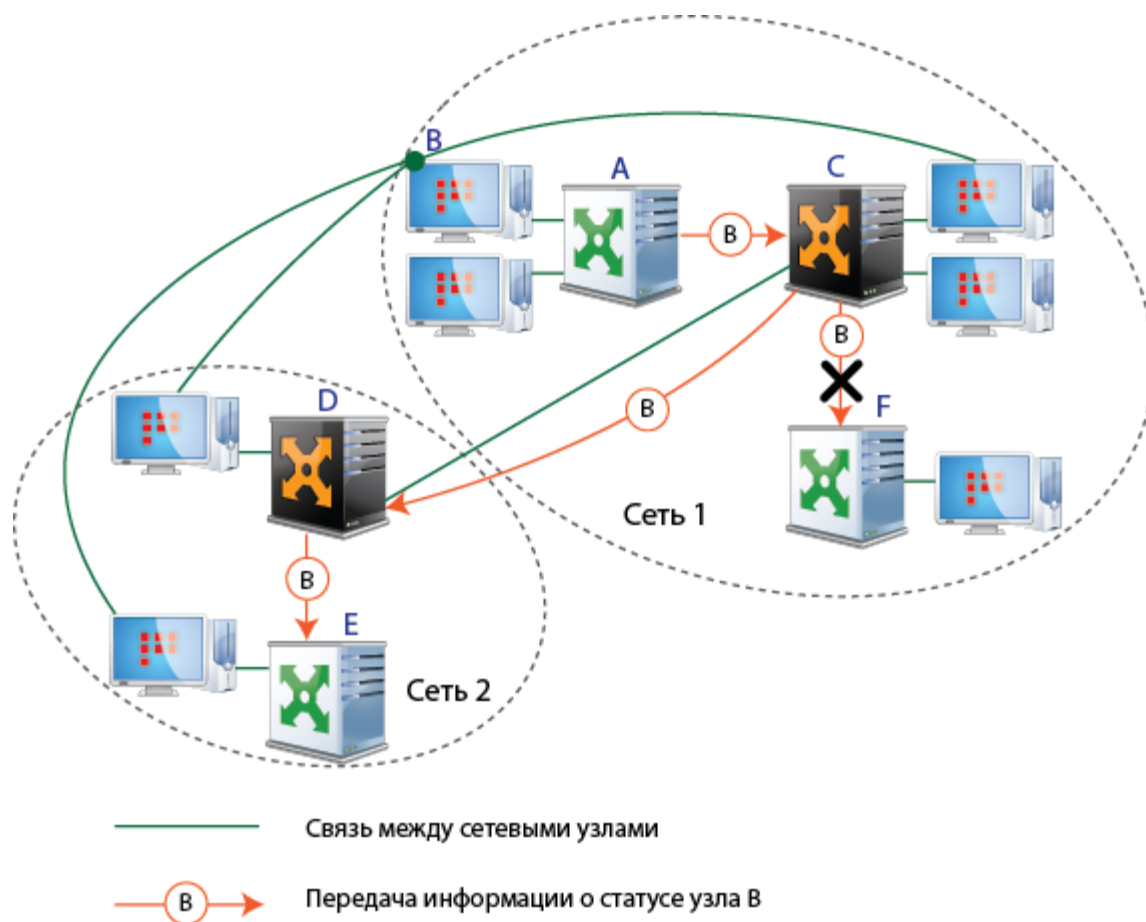


Рисунок 6: Особенности обмена служебной информацией в сетях ViPNet

Исходя из указанных свойств, при задании связей следует руководствоваться следующими требованиями и рекомендациями:

- 1 Если координаторы «А» и «С» из одной сети ViPNet являются серверами IP-адресов для клиентов, которые связаны между собой, то координаторы «А» и «С» необходимо также связать между собой.
- 2 Если клиент зарегистрирован в ЦУСе на координаторе «А», то нет необходимости явным образом устанавливать между ними связь. Такая связь создается автоматически.
- 3 Если координатор «С» из сети 1 и координатор «D» из сети 2 являются шлюзовыми между сетями 1 и 2, то нет необходимости явным образом устанавливать связь между этими координаторами. Такая связь создается автоматически.
- 4 Если клиенту координатора «А» не требуется устанавливать соединение с координатором «F» или его туннелируемыми узлами, то не рекомендуется устанавливать связь этого клиента с координатором «F».
- 5 Если клиент сети 1 связан с клиентом сети 2, то его сервер IP-адресов в сети 1 должен быть либо шлюзовым в сеть 2, либо связан со шлюзовым координатором сети 1 в сеть 2, либо связан со шлюзовым координатором сети 2 в сеть 1.
- 6 Если координатор «К» сети 1, который не является шлюзовым координатором в сеть 2, связан с координатором «L» сети 2 (например, для взаимодействия между туннелируемыми узлами координаторов), то координатор «К» необходимо связать также со всеми другими координаторами сети 1, клиенты которых связаны с узлами сети 2.
- 7 Если требуется создать резервный сервер IP-адресов для группы клиентов, необходимо связать эти клиенты с некоторым координатором. Клиенты при необходимости смогут выбрать этот координатор в качестве резервного сервера IP-адресов. Для такого координатора должны быть заданы такие же связи, как и для резервируемого координатора.

Добавление ролей на сетевые узлы

Роли (см. «Роль» на стр. 53) определяют, какие программы ViPNet могут работать на тех или иных сетевых узлах, а также функциональность программ ViPNet. В ходе создания защищенной сети ViPNet в ЦУСе необходимо добавить роли на клиенты и координаторы.

На все сетевые узлы при создании могут быть автоматически добавлены роли, если установить соответствующие флажки в мастере **Создание сети ViPNet**. Чтобы просмотреть или изменить список ролей сетевого узла, выполните следующие действия:

- 1 В окне **ViPNet Центр управления сетью** выберите представление **Моя сеть**.
- 2 На панели навигации выберите раздел **Клиенты** или **Координаторы**, в зависимости от типа сетевого узла, который требуется настроить.
- 3 На панели просмотра дважды щелкните сетевой узел, список ролей которого нужно просмотреть или изменить.
- 4 В окне свойств сетевого узла на левой панели выберите раздел **Роли**. На правой панели в разделе **Роли клиента (координатора)** будет отображен список ролей, добавленных на текущий сетевой узел. Этот список можно редактировать, добавляя и удаляя роли, а также изменяя свойства ролей.



Примечание. Возможность изменения свойств доступна не для всех ролей.

Роль «Центр управления сетью» по умолчанию добавляется на первый клиент первого координатора. На этом клиенте должно быть установлено серверное приложение ViPNet Центр управления сетью. Роль «Центр управления сетью» можно добавить только на один клиент.



Примечание. В случае если одно или несколько клиентских приложений ЦУСа установлены на отдельных компьютерах, для их корректной работы добавления на эти узлы специальных ролей не требуется.

При необходимости измените следующие свойства ролей:

- 1 На клиентах, на которые добавлены роли «VPN-клиент», «Деловая почта» и «CryptoService», измените уровень полномочий. Уровень полномочий определяет

допустимость изменения пользователем различных настроек ПО ViPNet на сетевом узле. Подробнее см. документ «Классификация полномочий. Приложение к документации ViPNet CUSTOM».

- 2 На клиентах, на которые добавлена роль «Registration Point», установите ограничения числа запросов на дистрибутивы и сертификаты.
- 3 На клиентах, на которые добавлена роль «Policy Manager», укажите списки узлов, политиками безопасности которых требуется управлять.
- 4 На клиентах, на которые добавлена роль «StateWatcher», задайте ограничения на число узлов мониторинга и дочерних серверов.
- 5 В случае если вы хотите воспользоваться технологией Открытый Интернет (на стр. 53), на одном или нескольких координаторах, на которые добавлена роль «VPN-сервер», укажите, что они являются серверами Открытого Интернета.

Для получения более подробной информации о добавлении ролей на сетевые узлы см. документ «ViPNet Центр управления сетью. Руководство администратора», глава «Настройка параметров сетевых узлов», раздел «Добавление ролей на сетевые узлы».

Кроме свойств ролей существует ряд параметров, которые можно изменить в окне свойств сетевых узлов. Задание этих параметров рассмотрено в разделе [Настройка свойств сетевых узлов](#) (на стр. 39).

Настройка свойств сетевых узлов

Ряд параметров сетевых узлов можно задать в окне свойств клиентов и координаторов.

В окне свойств координаторов можно задать следующие параметры:

- Собственные IP-адреса (раздел **Адреса во внешних сетях**).
- Параметры подключения координатора к внешней сети (раздел **Межсетевой экран**).
- Настройки межсетевого экрана для клиентов, зарегистрированных на этом координаторе (раздел **Межсетевой экран клиентов**).
- Адреса туннелируемых соединений и максимальное число одновременно туннелируемых адресов (раздел **Туннелирование**).

В окне свойств клиентов можно задать следующие параметры:

- IP-адреса клиентов, указываются при необходимости (раздел **Адреса во внешних сетях**).
- Специальные параметры для клиентов, у которых настройки межсетевого экрана должны отличаться от заданных на сервере IP-адресов (раздел **Межсетевой экран**).

Для получения более подробной информации о настройках сетевых узлов см. документ «ViPNet Центр управления сетью. Руководство администратора», глава «Настройка параметров сетевых узлов».

Создание дистрибутивов ключей

Для развертывания сетевых узлов необходимо создать дистрибутивы ключей. Для этого выполните следующие действия:

- 1 В ЦУСе создайте справочники.
- 2 В главном окне программы ViPNet Удостоверяющий и ключевой центр выполните следующие действия:
 - Выберите представление **Ключевой центр** и перейдите в раздел **Моя сеть > Сетевые узлы**.
 - На панели инструментов нажмите кнопку **Создать дистрибутивы ключей**.Будет запущен процесс создания дистрибутивов.
- 3 Задайте пароль администратора для группы «Вся сеть» (в эту группу по умолчанию входят все сетевые узлы), который используется для входа в режим администратора на сетевых узлах.

Созданные дистрибутивы будут отображены в УКЦ в представлении **Ключевой центр** в разделе **Моя сеть > Сетевые узлы > Дистрибутивы ключей**.

Используйте созданные дистрибутивы ключей для установки ПО ViPNet на сетевых узлах. Для этого выполните следующие действия:

- 1 Перенесите дистрибутивы (файлы *.dst) на съемный носитель (с помощью команды **Перенести в папку** в контекстном меню).
- 2 Скопируйте на этот же носитель пароли пользователей (меню **Сервис > Сохранить пароли в файле > Пароли пользователей**).
- 3 Защищенным способом передайте дистрибутивы ключей на компьютеры, на которых планируется развертывание сетевых узлов, и выполните установку ПО ViPNet.

Установка и настройка ПО ViPNet на сетевых узлах описана в разделах [Развертывание координатора](#) (на стр. 41) и [Развертывание клиента](#) (на стр. 47).



4

Развертывание координатора

Рекомендации по установке	42
Установка ПО ViPNet Coordinator	44
Настройка ПО ViPNet Coordinator	46

Рекомендации по установке

В данной главе описывается установка и настройка программного обеспечения ViPNet Coordinator для ОС Windows. Чтобы получить информацию об установке и настройке ViPNet Coordinator Linux или программно-аппаратного комплекса ViPNet Coordinator HW, обратитесь к документации соответствующих продуктов.

Требования к аппаратному и программному обеспечению компьютеров, на которых устанавливается ПО ViPNet Coordinator, содержатся в документе «ViPNet Coordinator Монитор. Руководство администратора».



Внимание! На компьютере, на котором устанавливается ПО ViPNet Coordinator, не должны быть установлены никакие сторонние межсетевые экраны и приложения, обеспечивающие преобразование сетевых адресов (NAT). Использование ViPNet Coordinator одновременно с такими программами может привести к конфликтам и вызвать проблемы с доступом в сеть.

Компьютер, на котором устанавливается ПО ViPNet Coordinator, может быть подключен к любым локальным или глобальным IP-сетям. Подключение к Интернету может осуществляться с помощью xDSL, ISDN, GPRS, UMTS, Wi-Fi, WiMAX или любым другим способом. Возможно подключение к сети через различные межсетевые экраны и устройства, осуществляющие трансляцию адресов (NAT).

Компьютер может иметь несколько сетевых интерфейсов. Если координатор планируется использовать для подключения к сети ViPNet удаленных пользователей или в качестве шлюза при взаимодействии с другими сетями ViPNet, по крайней мере один сетевой интерфейс координатора должен иметь публичный IP-адрес или находиться за межсетевым экраном со статической трансляцией адресов.

Для правильной работы координатора в ОС Windows должна быть включена функция маршрутизации IP-пакетов. Если маршрутизация IP-пакетов отключена, она будет автоматически включена во время установки ПО ViPNet Coordinator.

ViPNet Coordinator можно установить на специально выделенном для этого компьютере или на каком-либо существующем сервере. В последнем случае весь IP-трафик сервера будет защищен. Кроме того, будет проще организовать обмен трафиком между этим сервером и другими сетевыми узлами ViPNet, так как по умолчанию между защищенными узлами разрешены любые соединения и настройка сетевых фильтров не требуется.

Установка ПО ViPNet Coordinator описана в следующем разделе. После установки в программе ViPNet Coordinator нужно выполнить ряд настроек (см. «[Настройка ПО ViPNet Coordinator](#)» на стр. 46).

Установка ПО ViPNet Coordinator



Примечание. Процесс установки ПО ViPNet Client ничем не отличается от установки ПО ViPNet Coordinator. Поэтому указания, содержащиеся в данном разделе, относятся к обоим перечисленным программам.

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


Если ViPNet Coordinator или ViPNet Client устанавливается на компьютер с операционной системой Windows, локализация которой отличается от русской, для правильного отображения кириллицы в интерфейсе ViPNet Coordinator или ViPNet Client нужно изменить региональные настройки Windows.

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

Для установки ViPNet Coordinator или ViPNet Client требуются:

- Установочный файл программы.
- **Дистрибутив ключей** (на стр. 52) для сетевого узла (файл *.dst). Если на узле планируется работа нескольких пользователей, для каждого из них нужен отдельный дистрибутив ключей.
- Пароль пользователя сетевого узла или внешнее устройство аутентификации.
Дистрибутивы и пароли пользователей создаются в программе ViPNet Удостоверяющий и ключевой центр (см. «[Создание дистрибутивов ключей](#)» на стр. 40).

Для установки ViPNet Coordinator или ViPNet Client выполните следующие действия:

- 1 Запустите установочный файл . Дождитесь завершения подготовки к установке.
- 2 Следуйте указаниям программы установки.
- 3 По завершении установки перезагрузите компьютер.

- 4 После перезагрузки установите справочники и ключи пользователя сетевого узла (см. «[Дистрибутив ключей](#)» на стр. 52).

Подробно установка ПО ViPNet Coordinator описана в документе «ViPNet Coordinator Монитор. Руководство администратора».

Настройка ПО ViPNet Coordinator

Чтобы уменьшить количество настроек, выполняемых вручную непосредственно на координаторе, рекомендуется задать IP-адреса координаторов, туннелируемых узлов и настройки подключения координатора к сети в клиентском приложении ViPNet Центр управления сетью. Выполните следующие действия:

- 1 Настройте параметры межсетевого экрана:
 - Задайте необходимые сетевые фильтры (см. «ViPNet Coordinator Монитор. Руководство администратора», глава «Интегрированный сетевой экран», раздел «Создание сетевых фильтров»).
 - Включите или отключите антиспуфинг (см. «ViPNet Coordinator Монитор. Руководство администратора», глава «Интегрированный сетевой экран», раздел «Антиспуфинг»).
 - Задайте правила трансляции адресов (см. «ViPNet Coordinator Монитор. Руководство администратора», глава «Трансляция IP-адресов (NAT)»).
 - Настройте параметры обработки прикладных протоколов (см. «ViPNet Coordinator Монитор. Руководство администратора», глава «Настройка параметров обработки прикладных протоколов»).
- 2 Задайте IP-адреса других координаторов сети ViPNet (см. «ViPNet Coordinator Монитор. Руководство администратора», глава «Настройка доступа к узлам сети ViPNet», раздел «Настройка доступа к защищенным узлам»).
- 3 При необходимости задайте IP-адреса открытых узлов, туннелируемых координатором (см. «ViPNet Coordinator Монитор. Руководство администратора», глава «Защита трафика открытых узлов (туннелирование)»).
- 4 Если координатор должен подключаться к открытым узлам, которые туннелируются другими координаторами, задайте IP-адреса этих узлов (см. «ViPNet Coordinator Монитор. Руководство администратора», глава «Настройка доступа к узлам сети ViPNet», раздел «Настройка доступа к узлам, туннелируемым другим координатором»).



5

Развертывание клиента

Рекомендации по установке	48
Настройка ПО ViPNet Client	50

Рекомендации по установке

На клиенте сети следует установить одну из следующих программ ViPNet:

- ViPNet Client — выполняет функции VPN-клиента сети ViPNet и персонального сетевого экрана.
- ViPNet CryptoService — обеспечивает возможность использования криптографических функций в прикладных программах, но не обеспечивает защиту трафика.

Требования к аппаратному и программному обеспечению компьютеров, на которых устанавливается клиентское ПО ViPNet, содержатся в документах «ViPNet Client Монитор. Руководство администратора» и «ViPNet CryptoService. Руководство пользователя».



Внимание! На компьютере, на котором устанавливается ПО ViPNet Client, не должны быть установлены никакие сторонние межсетевые экраны и приложения, обеспечивающие преобразование сетевых адресов (NAT). Использование ViPNet Client одновременно с такими программами может привести к конфликтам и вызвать проблемы с доступом в сеть.

Компьютер, на котором устанавливается ПО ViPNet Client, может быть подключен к любым локальным сетям TCP/IP или к Интернету. Подключение к Интернету может осуществляться с помощью xDSL, ISDN, GPRS, UMTS, Wi-Fi, WiMAX или любым другим способом. Возможно подключение к сети через различные межсетевые экраны и устройства, осуществляющие трансляцию адресов (NAT).

ПО ViPNet Client можно установить на какой-либо сервер для обеспечения защиты трафика этого сервера. Кроме того, это позволяет легко организовать обмен трафиком между этим сервером и другими сетевыми узлами ViPNet, так как по умолчанию между защищенными узлами разрешены любые соединения и настройка правил фильтрации трафика не требуется.

Процесс установки ПО ViPNet Client и ViPNet CryptoService аналогичен процессу установки ПО ViPNet Coordinator (см. «[Установка ПО ViPNet Coordinator](#)» на стр. 44). Более подробно установка описана в документации указанных продуктов.

После установки в программе ViPNet Client нужно выполнить ряд настроек (см. «[Настройка ПО ViPNet Client](#)» на стр. 50). Специальная настройка ПО ViPNet CryptoService не требуется.

Настройка ПО ViPNet Client


Чтобы уменьшить количество настроек, выполняемых вручную непосредственно на клиентском компьютере, рекомендуется задать IP-адреса координаторов, туннелируемых узлов и настройки подключения клиента к сети в клиентском приложении ViPNet Центр управления сетью. Если необходимые настройки не были сделаны в ЦУСе, выполните следующие действия:

- 1** Настройте параметры межсетевого экрана (см. «ViPNet Client Монитор. Руководство пользователя», глава «Интегрированный сетевой экран»):
 - Задайте необходимые сетевые фильтры (см. «ViPNet Client Монитор. Руководство пользователя», глава «Интегрированный сетевой экран», раздел «Создание сетевых фильтров»).
 - Настройте параметры обработки прикладных протоколов (см. «ViPNet Client Монитор. Руководство пользователя», глава «Настройка параметров обработки прикладных протоколов»).
- 2** Задайте IP-адрес сервера IP-адресов, выбранного для данного клиента (см. «ViPNet Client Монитор. Руководство пользователя», глава «Настройка доступа к узлам сети ViPNet», раздел «Настройка доступа к защищенным узлам»).
- 3** Если клиент должен подключаться к туннелируемым узлам, задайте IP-адреса этих узлов (см. «ViPNet Client Монитор. Руководство пользователя», глава «Настройка доступа к узлам сети ViPNet», раздел «Настройка доступа к туннелируемым узлам»).

6

Проверка функционирования сети ViPNet

Чтобы убедиться в том, что сеть ViPNet развернута и настроена правильно, достаточно проверить возможность установления соединений между защищенными сетевыми узлами ViPNet, а также возможность подключения к туннелируемому узлам:

- Для проверки соединения с выбранными сетевыми узлами в программе ViPNet Монитор нажмите на панели инструментов кнопку **Проверить соединение** .
- Для проверки соединения с туннелируемыми узлами можно воспользоваться командой `ping`.

Для полноценного функционирования сети необходима возможность соединения между всеми координаторами, а также между клиентами и их серверами IP-адресов. Также следует проверить возможность подключения к сети ViPNet удаленных пользователей.

Если соединение между какими-либо узлами невозможно, убедитесь, что на этих узлах правильно заданы IP-адреса координаторов и параметры подключения к сети, а на используемых межсетевых экранах настроены необходимые правила трансляции адресов.



Глоссарий

Д

Дистрибутив ключей

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

См. также: [Сетевой узел ViPNet](#) (на стр. 54), [Справочники](#) (на стр. 54).

З

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

К

Координатор соединений

Координатор, с помощью которого клиенты организуют соединения друг с другом в том случае, если находятся в разных подсетях и не могут установить соединение напрямую. Для каждого клиента можно выбрать свой координатор соединений. По умолчанию координатором соединений для клиента назначен сервер IP-адресов.

О

Открытый Интернет

Технология, реализованная в программном обеспечении ViPNet. При подключении к Интернету узлы локальной сети изолируются от сети ViPNet, а при работе в сети ViPNet — от Интернета, что обеспечивает защиту от возможных сетевых атак извне без физического отключения компьютеров от локальной сети.

См. также: [Сеть ViPNet](#) (на стр. 54).

П

Политика безопасности

Набор параметров, регулирующих безопасность сетевого узла. В технологии ViPNet безопасность сетевых узлов обеспечивается с помощью сетевых фильтров и правил трансляции IP-адресов.

См. также: [Сетевой узел ViPNet](#) (на стр. 54).

Прикладной конверт

Файл, формируемый приложениями ViPNet (например, «Деловая почта», «Файловый обмен») для передачи другим сетевым узлам.

Р

Роль

Некоторая функциональность сетевого узла, предназначенная для решения целевых и служебных задач сети ViPNet. Роль используется в лицензировании сети с помощью файла `infotecs.reg` и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

Роли могут иметь атрибуты в виде количественных характеристик и полномочий, которые также влияют на функциональность.

Набор ролей для каждого сетевого узла задается администратором сети ViPNet в программе ViPNet Центр управления сетью.

С

Сертификат открытого ключа подписи пользователя

Электронный документ определенного формата, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Сертификат содержит информацию о владельце ключа, открытый ключ, сведения о его назначении и области применения, информацию о выпустившем сертификат удостоверяющем центре, период действия сертификата, а также некоторые дополнительные параметры. В программе ViPNet Удостоверяющий и ключевой центр сертификат создается в соответствии со стандартом X.509 v3 и заверяется электронной подписью администратора УКЦ.

В терминологии Федерального закона Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» сертификат открытого ключа подписи пользователя называют «сертификатом ключа проверки электронной подписи».

Сетевой узел ViPNet

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

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

См. также: [Сетевой узел ViPNet](#) (на стр. 54).

Справочники

Набор файлов, содержащих информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях. Эти файлы формируются в управляющих приложениях ViPNet, предназначенных для создания структуры и конфигурирования сети ViPNet (ViPNet Центр управления сетью, ViPNet Network Manager).



В

Указатель

Д

- Дистрибутив ключей - 27, 44, 45
- Добавление ролей на сетевые узлы - 31, 33
- Дополнительная настройка сети - 32

З

- Защита IP-трафика в сети ViPNet - 18
- Защищенный узел - 10

К

- Координатор соединений - 23

Н

- Настройка ПО ViPNet Client - 49
- Настройка ПО ViPNet Coordinator - 43
- Настройка свойств сетевых узлов - 33, 38

О

- Обратная связь - 20
- Открытый Интернет - 38

П

- Планирование сети - 16, 20
- Политика безопасности - 10
- Прикладной конверт - 32

Р

- Развертывание клиента - 17, 40
- Развертывание координатора - 16, 40

- Развертывание рабочих мест администраторов - 14
- Рекомендации по созданию связей - 33
- Роль - 13, 37

С

- Сертификат открытого ключа подписи пользователя - 10
- Сетевой узел ViPNet - 12, 52, 53, 55
- Сеть ViPNet - 10, 53, 54
- Создание дистрибутивов ключей - 33, 44
- Создание топологии сети в ViPNet Administrator - 27
- Справочники - 26, 32, 52

У

- Установка ПО ViPNet Coordinator - 48