



Развертывание сети ViPNet

Руководство администратора

1991–2012 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00005-05 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
Обратная связь	7
Глава 1. Общее представление о сети ViPNet	8
Основные конфигурации сетей ViPNet	9
Описание узлов сети ViPNet (электронный документооборот).....	13
Защита электронного документооборота в сети ViPNet.....	15
Описание узлов сети ViPNet (частная виртуальная сеть).....	16
Защита информации в сети ViPNet.....	22
Глава 2. Подготовка к развертыванию сети ViPNet	24
Планирование сети.....	25
Развертывание рабочего места администратора.....	29
Рекомендации по установке	29
Установка ViPNet Administrator.....	30
Глава 3. Создание топологии сети в ViPNet Administrator	32
Создание сетевых узлов и пользователей	33
Рекомендации по созданию связей.....	35
Регистрация узлов в прикладных задачах	38
Создание дистрибутивов ключей.....	41
Глава 4. Развертывание координатора.....	42
Рекомендации по установке	43
Установка ViPNet Coordinator	45
Настройка ViPNet Coordinator.....	46
Глава 5. Развертывание абонентского пункта.....	47
Рекомендации по установке	48
Настройка ViPNet Client	50
Глава 6. Проверка функционирования сети ViPNet	51

Приложение А. Указатель	52
--------------------------------------	-----------



Введение

О документе	6
Обратная связь	7

О документе

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

Документ дает первое представление о сетях ViPNet и позволяет определить, какая конфигурация сети ViPNet более всего удовлетворяет задачам коммуникации и защиты данных, стоящих перед компанией. Также в документе содержится пошаговое руководство развертывания типовой сети ViPNet, включающей рабочее место администратора сети, координирующий сервер(ы) и клиентские рабочие места.

Для кого предназначен документ

Документ адресован высшим менеджерам компаний, руководителям IT-отделов, системным администраторам, желающим познакомиться с возможностями организации защищенных сетей ViPNet. Помимо этого, документ будет полезен IT-специалистам, выполняющим развертывание сети ViPNet, без необходимости погружения во все особенности и технические подробности технологий ViPNet.

Соглашения документа

Соглашения данного документа представлены в таблице ниже.

Таблица 1. Условные обозначения

Указатель	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.

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте компании «ИнфоТеКС». По предложенным ссылкам можно найти ответы на многие вопросы, возникающие в процессе эксплуатации продуктов ViPNet.

- 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 компании «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

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



1

Общее представление о сети ViPNet

Основные конфигурации сетей ViPNet	9
Описание узлов сети ViPNet (электронный документооборот)	13
Защита электронного документооборота в сети ViPNet	15
Описание узлов сети ViPNet (частная виртуальная сеть)	16
Защита информации в сети ViPNet	22

Основные конфигурации сетей

ViPNet

Программный комплекс ViPNet CUSTOM позволяет сформировать среду безопасного обмена информацией по общедоступным каналам связи различных типов. Это достигается путем создания логических контуров сети, защищенных криптографическими средствами высокой надежности. Контуров сетей могут быть двух типов:

- сеть ViPNet для организации электронного документооборота (частный вариант);
- сеть ViPNet со всеми функциями VPN.

Первый вид контура сети ViPNet позволяет организовать систему электронного документооборота со следующей функциональностью:

- конфиденциальный обмен информацией;
- юридическая значимость документов;
- гибкая настройка автоматической обработки исходящих и входящих документов (файлов);
- возможность плавного расширения сети до уровня VPN.

Типовая схема сети ViPNet (электронный документооборот) представлена на рисунке ниже.

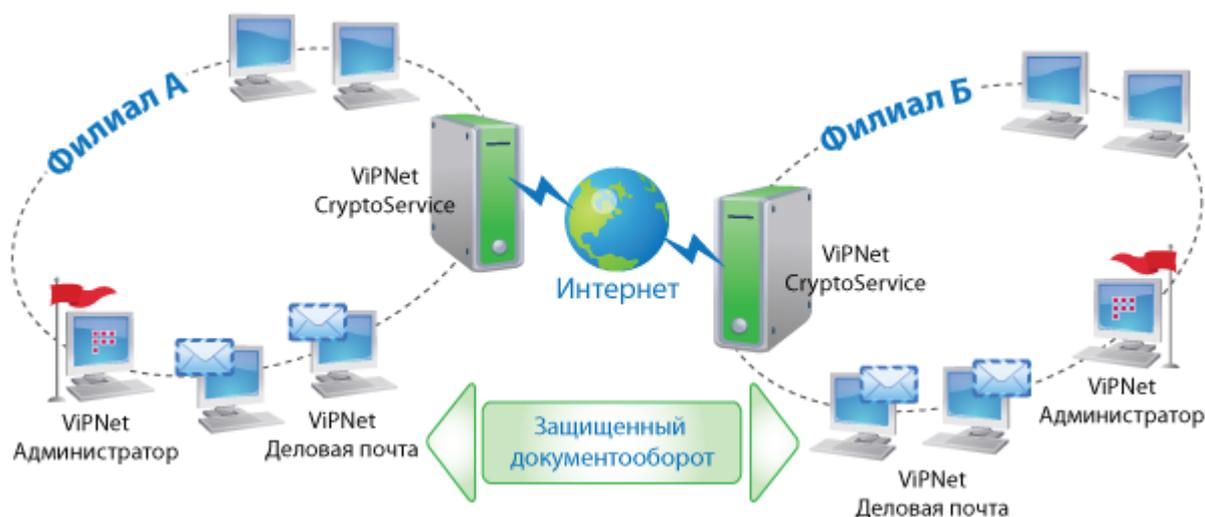


Рисунок 1: Схема сети ViPNet - электронный документооборот

Организация электронного обмена конфиденциальной информацией происходит следующим образом:

- Администратор сети ViPNet с помощью ПО ViPNet Administrator формирует ключи для защиты информации.
- Администратор сети ViPNet проводит настройку сервера CryptoService для взаимодействия узлов внутренней и внешней сети.
- Администраторы ViPNet-сетей филиалов «А» и «Б» обмениваются информацией для создания общих ключей защиты.
- Пользователь ПО ViPNet Деловая почта проводит первичную инициализацию ключей защиты. После этого пользователь получает возможность участвовать в защищенном документообороте:
 - Отправлять пользователям ПО ViPNet Деловая почта филиалов «А» и «Б» защищенные сообщения и сообщения с электронной подписью.
 - Настраивать правила автоматической обработки исходящих и входящих сообщений.

Второй тип контура сети ViPNet легко преобразуется из первого путем добавления соответствующих лицензий и установкой нужного ПО. Этот вид контура позволяет развертывать частные виртуальные сети любых конфигураций, обеспечивающих прозрачное взаимодействие компьютеров сети ViPNet независимо от способа, места и типа IP-адреса при их подключении к сети. При этом весь трафик, циркулирующий по виртуальному контуру этой сети, защищен криптографическими методами.

Основные преимущества и функционал сети ViPNet (контур частная виртуальная сеть):

- плавная интеграция в структуру существующей сети;
- гибкая настройка фильтрации закрытого (защищенного средствами ViPNet) и открытого трафика;
- широкие средства внутренней и внешней коммуникации (почта, чат, обмен файлами);
- организация юридически значимого электронного документооборота;
- система слежения за состоянием сети;
- дополнительный функционал по регистрации пользователей, публикации сертификатов в общедоступных хранилищах и др.

Построение сетей ViPNet на базе частных виртуальных сетей — процесс индивидуальный и дифференцированный. В первую очередь он зависит от существующей топологии сети и от тех коммуникационных задач, которые стоят перед организацией. Именно поэтому универсальную схему ViPNet сети изобразить сложно. В данном документе представлены схема и описание одного из типовых вариантов сети, построенной на базе комплекса ViPNet CUSTOM.

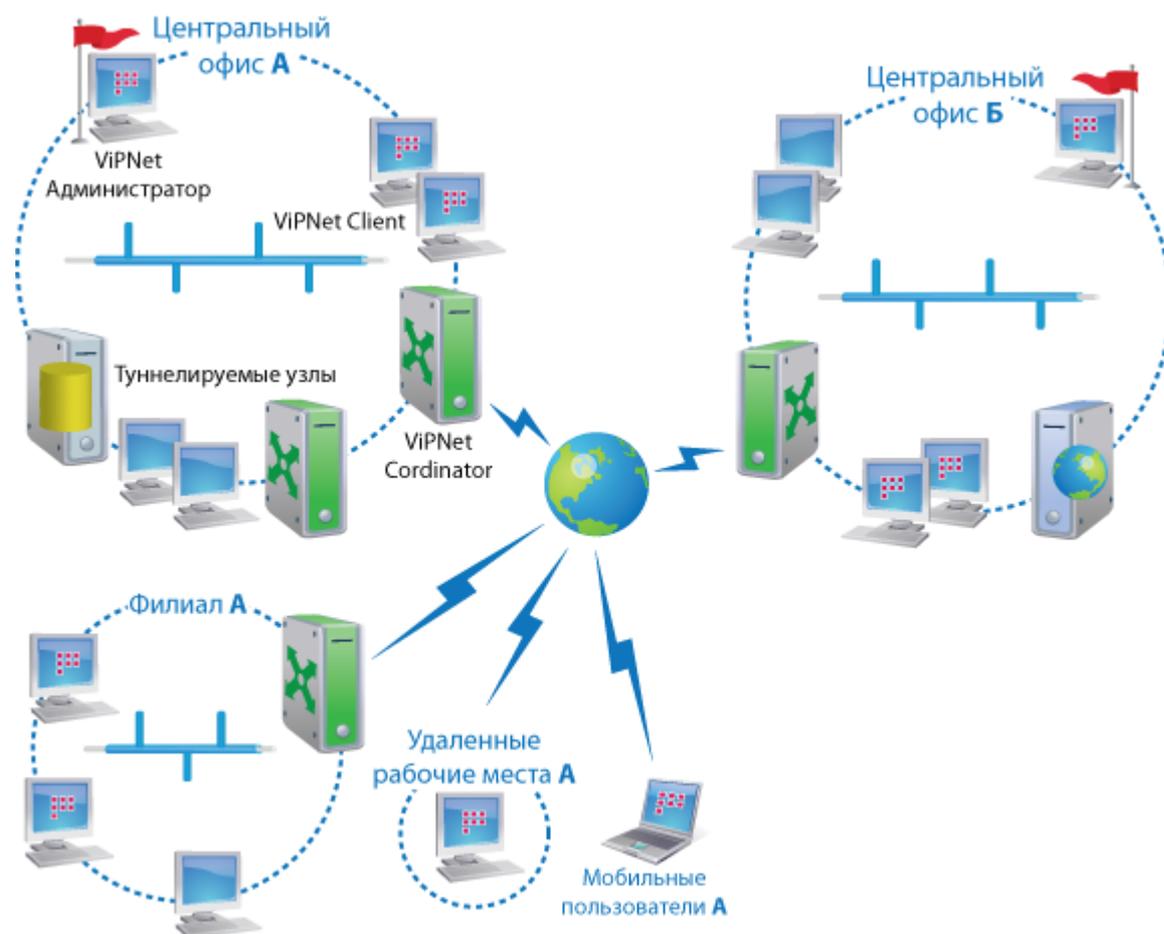


Рисунок 2: Схема сети на базе программного комплекса VipNet CUSTOM

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 единую 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 (электронный документооборот)

Сеть для организации защищенного документооборота строится путем установки на компьютеры пользователей (получателей и отправителей электронных сообщений) ПО ViPNet Деловая почта. На границе сети устанавливается компьютер (сервер) с ПО ViPNet CryptoService, который играет роль координатора. Административные функции сети выполняет компьютер с ПО ViPNet Administrator, состоящим из двух компонент: программы ViPNet Центр управления сетью (ЦУС) и программы ViPNet Удостоверяющий и ключевой центр (УКЦ). Кроме того, на компьютере администратора должно быть установлено ПО ViPNet CryptoService для организации защищенного обмена служебной информацией с другими узлами сети ViPNet.

Помимо установки ПО каждый из узлов сети должен быть зарегистрирован в соответствующей прикладной задаче, которая определяет его роль в сети. Состав и количество прикладных задач, доступных в конкретной конфигурации сети ViPNet, определяется файлом лицензии.

Назначение каждого из узлов сети ViPNet для организации электронного документооборота приводится в таблице ниже.

Узел сети ViPNet	Описание функционала
 ViPNet Центр управления сетью (ЦУС)	Выполняет следующие функции: <ul style="list-style-type: none">• создание и модификация топологии сети ViPNet;• отправка ключей, полученных из УКЦ, информации о топологии сети и обновлений на сетевые узлы. Прикладные задачи: «Центр управления сетью», «КриптоСервис».
 ViPNet Удостоверяющий и ключевой центр (УКЦ)	Выполняет следующие функции: <ul style="list-style-type: none">• формирование пользовательских ключей защиты информации;• создание и управление сертификатами пользователей. Описание и шаги по развертыванию рабочего места администратора (см. «Развертывание рабочего места администратора» на стр. 29). Прикладные задачи: «Удостоверяющий и ключевой центр», «КриптоСервис».



VipNet CryptoService

Роль узла с ПО VipNet CryptoService в сети определяется прикладной задачей, в которой зарегистрирован этот узел.

В данном случае играет роль почтового сервера-маршрутизатора, что подразумевает пересылку почтовых конвертов и управляющих конвертов, полученных из ЦУСа, на сетевые узлы.

Узел VipNet CryptoService должен быть зарегистрирован в сети как сервер-маршрутизатор. Это означает, что при создании сети VipNet в ЦУСе следует в обычном порядке создать сервер-маршрутизатор и зарегистрировать на нем другие узлы. После этого на узле с установленным ПО VipNet CryptoService нужно установить дистрибутив ключей сервера-маршрутизатора.



VipNet Деловая почта

Играет роль клиента сети и обеспечивает пользователю следующие возможности:

- шифрование исходящих сообщений и расшифрование входящих;
- постановка электронной подписи для обеспечения аутентичности и целостности сообщения;
- проверка электронной подписи входящих сообщений;
- получение подтверждений (квитанций) о доставке и использовании документов, предоставление информации о документе;
- ведение регистрационной нумерации документов;
- инструменты автоматической обработки исходящих и входящих сообщений (файлов).

Прикладная задача: «Деловая почта».

Описание и шаги по развертыванию рабочего места пользователя (см. «[Развертывание абонентского пункта](#)» на стр. 47).

Защита электронного документооборота в сети ViPNet

Развертывание контура сети ViPNet для организации электронного документооборота позволяет обеспечить защиту только следующих видов информации: почтовые сообщения и файлы (вложения к сообщениям). При этом остальная информация, передающаяся по сети, останется незащищенной.



Рисунок 3: Защита документов и сообщений в сети ViPNet

При создании данного вида ViPNet сети необходимо определить круг пользователей, которые будут участвовать в электронном документообороте, и разместить в сети сервер, играющий роль координатора. При этом необходимо учитывать, что координатор (компьютер с ПО ViPNet CryptoService) должен иметь внешний статический IP-адрес для взаимодействия с координаторами других сетей.

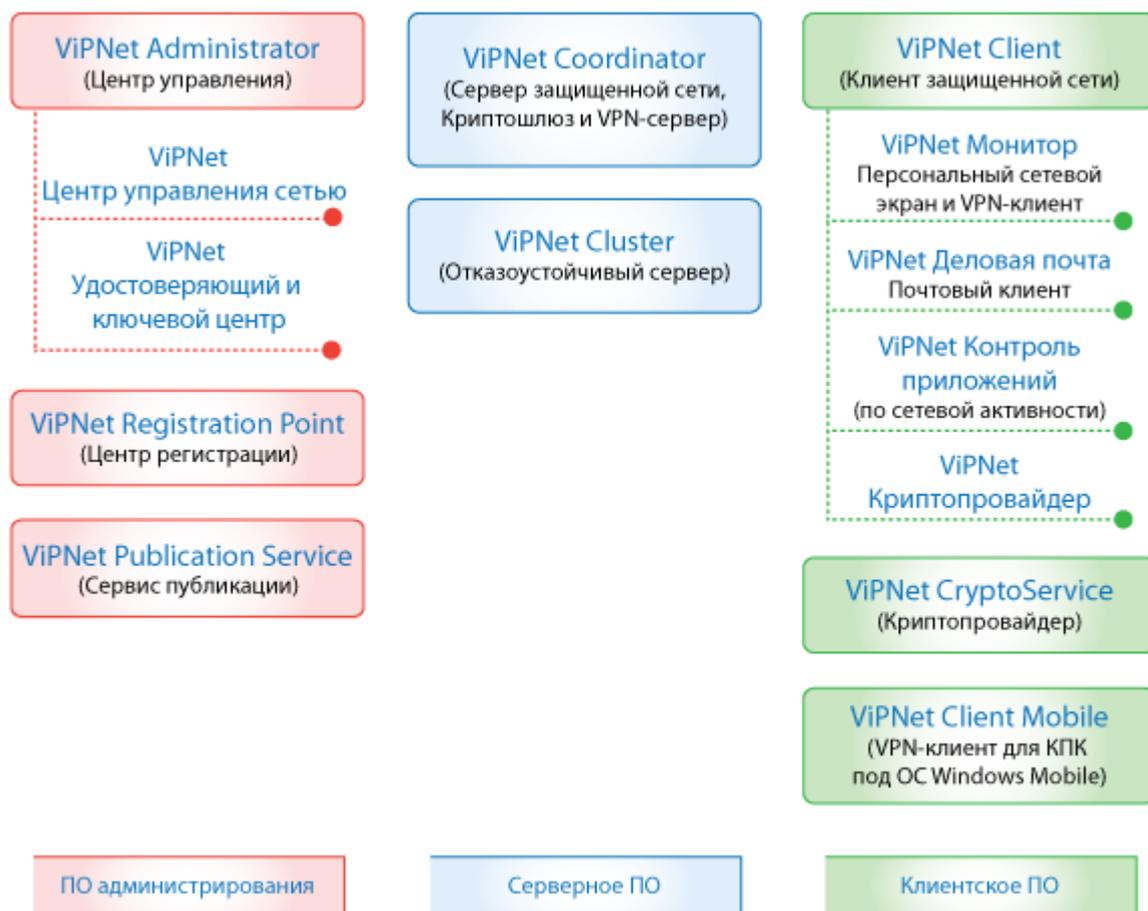
Описание узлов сети ViPNet (частная виртуальная сеть)

Для обеспечения полной безопасности корпоративной сети необходима установка программного обеспечения ViPNet, которое позволяет защитить не только корреспонденцию, передаваемую по сети, но и весь сетевой трафик, а также информацию, хранящуюся на компьютерах. При этом доступ к защищенному компьютеру с 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 ViPNet сети с установленным ПО:
 - ViPNet Administrator, состоящий из двух компонентов:
 - ViPNet Центр управления сетью (ЦУС),
 - ViPNet Удостоверяющий и ключевой центр (УКЦ);
 - ViPNet Client или ViPNet CryptoService для организации обмена служебной информацией с другими узлами сети ViPNet.
- Сервер(ы) с установленным ПО ViPNet Coordinator, размещенный на границе сети или на границах участков сети. В зависимости от своей роли в сети координатор может выполнять различные функции (см. таблицу).
- Компьютеры пользователей с установленным клиентским ПО ViPNet Client или ViPNet CryptoService.

Помимо перечисленных базовых элементов, в сети ViPNet могут присутствовать и другие функциональные компоненты, решающие задачи резервирования, мониторинга, общего доступа к сертификатам и другие. Разновидности ПО ViPNet в зависимости от назначения и роли в сети представлены на схеме ниже.



Описание роли и функций всех узлов, из которых может состоять сеть ViPNet приведено в таблице.

Узел сети ViPNet	Описание
 ViPNet Центр управления сетью (ЦУС)	Обязательный компонент сети ViPNet. Выполняет следующие основные функции: <ul 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 и обновлений на сетевые узлы. Прикладные задачи: «Центр управления сетью», «Защита трафика».
 ViPNet Удостоверяющий и	Обязательный компонент сети ViPNet. Выполняет следующие основные функции: <ul style="list-style-type: none"> • формирование пользовательских ключей защиты информации; • создание и управление сертификатами пользователей.

ключевой центр
(УКЦ)

УКЦ в сети ViPNet взаимодействует только с ЦУСом — получает информацию об узлах и пользователях сети и отправляет ключевую информацию для защиты данных. Поэтому по соображениям безопасности рекомендуется не включать компьютер с УКЦ в общую сеть ViPNet, а обеспечить связь только с компьютером ЦУСа.

Прикладные задачи: «Удостоверяющий и ключевой центр», «Защита трафика».

Описание и шаги по развертыванию рабочего места администратора (см. [«Развертывание рабочего места администратора»](#) на стр. 29).



ViPNet Coordinator

Обязательный компонент сети ViPNet. Узел с ПО ViPNet Coordinator (координатор) в зависимости от круга задач в корпоративной сети может выполнять следующие функции:

- Проксирование защищенного трафика (организация безопасной связи между защищенными сетями через публичные сети).
- Фильтрация открытого и туннелируемого трафика (межсетевой экран).
- Оповещение узлов о параметрах доступа друг к другу (сервер IP-адресов).
- Организация защищенного взаимодействия с открытым ресурсом в локальной сети (туннелирование).
- Выполнение функций почтовых серверов для программы «Деловая почта» и управления из ЦУСа.
- Организация защищенного доступа в Интернет в полном соответствии с указом Президента РФ от 12 мая 2004 года N 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена».

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. [«Развертывание координатора»](#) на стр. 42).



ViPNet Cluster

ViPNet Cluster — это группа узлов ViPNet Coordinator, объединенных высокоскоростными каналами связи и функционирующих как единое целое. Кластер является координатором и обладает всей его функциональностью, а кроме того:

- обеспечивает более высокую производительность координатора;
- обладает системой обеспечения отказоустойчивости и резервирования.



ViPNet Client

Узел с ПО ViPNet Client (клиент, или абонентский пункт) выполняет следующие функции:

- фильтрация открытого трафика — персональный сетевой экран (компонент ViPNet Монитор);
- шифрование сетевого трафика компьютера;
- предоставление дополнительных сервисных функций для оперативного защищенного обмена сообщениями, проведения конференций, файлового обмена и др.;
- предоставление статистических данных и средств мониторинга;
- организация защищенной передачи электронных документов (компонент ViPNet Деловая почта);
- защита от несанкционированной активности программ, установленных на компьютере (компонент ViPNet Контроль приложений).

Набор прикладных задач, которые задаются для клиента, может быть различным, в зависимости от его роли и выполняемых функций в сети. Для типового случая это задачи: «Защита трафика», «Деловая почта».

Описание и шаги по разворачиванию клиентского рабочего места (см. «[Разворачивание абонентского пункта](#)» на стр. 47).



ViPNet
CryptoService

Роль узла с ПО ViPNet CryptoService в сети определяется прикладной задачей, в которой зарегистрирован этот узел.

В случае виртуальной частной сети это облегченная версия клиентского узла, которая позволяет работать с сертификатами пользователя и осуществлять криптографическую защиту файлов и сообщений в прикладных программах (например, в пакете MS Office).

В ViPNet CryptoService не включена функция защиты всего трафика.

Прикладная задача: «КриптоСервис».



ViPNet Деловая
почта

Играет роль клиентского ПО и обеспечивает пользователю возможность участия в защищенном электронном документообороте. Защита остального трафика не предусмотрена.

Прикладная задача: «Деловая почта».



ViPNet Registration
Point
(Центр
регистрации)

Выполняет функции по расширенному управлению сертификатами и ключевой информацией пользователя:

- регистрация пользователей;
- создание запроса на сертификат, на отзыв сертификата и на приостановление его действия;
- создание запроса на формирование ViPNet-ключей защиты для пользователя.

Кроме того, использование Центра регистрации в больших сетях

целесообразно для равномерного распределения нагрузки между УКЦ и Центром регистрации путем делегирования части полномочий Удостоверяющего центра.

Прикладная задача: «Центр регистрации», «Защита трафика» (или «КриптоСервис»).

Подробнее о программе см. документ «ViPNet Registration Point. Руководство администратора».



ViPNet Publication Service

(Сервис публикации)

Основное назначение программы — публикация сертификатов и СОС в общедоступных хранилищах данных. Публикация сертификатов применяется при организации документооборота между пользователями сети ViPNet и пользователями, не входящими в сеть ViPNet.

Прикладная задача: «Центр регистрации», «Защита трафика» (или «КриптоСервис»).

Подробнее о программе см. документ «ViPNet Publication Service. Руководство администратора».



ViPNet StateWatcher

(Мониторинг защищенной сети)

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 событий на них.
- Разграничение доступа к информации и управлению системой мониторинга.

Подробнее о программе см. пакет документов «Система централизованного мониторинга сети ViPNet».



ViPNet PolicyManager

(Управление политиками безопасности)

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.

Подробнее о программе см. документ «ViPNet Policy Manager. Руководство администратора».



Открытые или туннелируемые узлы

Открытые узлы сети ViPNet — узлы, на которых невозможно или нецелесообразно устанавливать ПО ViPNet. Информация на таких узлах может быть защищена при помощи технологии туннелирования. Данная технология предполагает направление исходящего и входящего трафика узла через ViPNet Coordinator, где трафик фильтруется и защищается криптографическими методами (см. «[Защита информации в сети ViPNet](#)» на стр. 22).

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

Защита информации в сети ViPNet

Как правило, задачи по защите и доступу 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 выполняет функции по шифрованию 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 4: Обмен информацией между узлами ViPNet Client

При организации доступа к сети Интернет ViPNet Coordinator осуществляет многоуровневую фильтрацию входящего трафика таким образом, чтобы оградить пользователей ViPNet Client от потенциально опасной информации. Кроме того, ViPNet Coordinator выполняет функции по трансляции IP-адресов (NAT), и нет необходимости устанавливать дополнительные NAT-устройства на границе локальной и публичной сети. Если же такое устройство необходимо, можно настроить его взаимодействие с ViPNet Coordinator.



Рисунок 5: 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. ViPNet Coordinator, установленный на границе локальной и публичной сети, возьмет на себя все функции по защите сетевого трафика, а также функции маршрутизации и трансляции адресов.

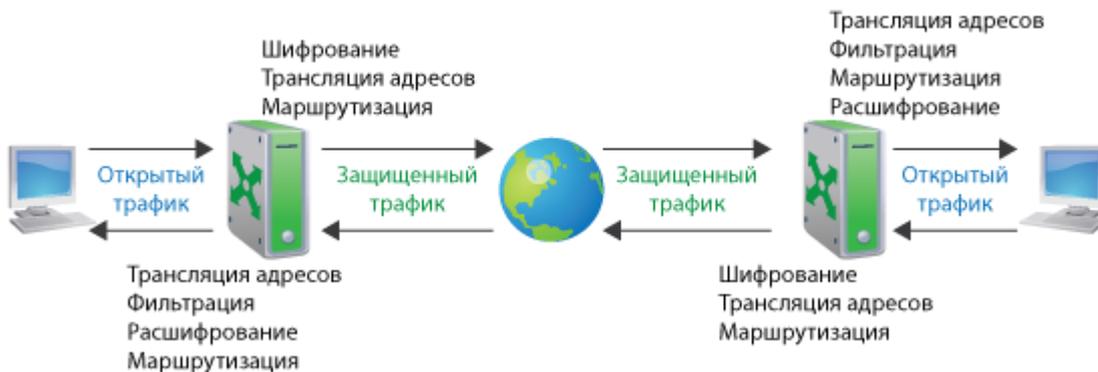


Рисунок 6: Обмен информацией между открытыми узлами через Интернет

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 предоставят специалисты компании Инфотекс (см. «Обратная связь» на стр. 7).

После определения и согласования всех описанных факторов можно переходить к планированию сети (см. «Планирование сети» на стр. 25).



2

Подготовка к развертыванию сети ViPNet

Планирование сети	25
Развертывание рабочего места администратора	29

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 систему Центров управления сетью, чтобы централизованно управлять распределением лицензий в подчиненных сетях из головного Центра управления сетью.

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.

Логическая структура создаваемой сети ViPNet (в первую очередь, это привязка абонентских пунктов 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, играющие роль серверов сети ViPNet, в зависимости от потребностей и применяемой политики безопасности могут выполнять следующие задачи:

- **Сервер IP-адресов** – используется для регистрации активных абонентских пунктов и их информирования о текущих IP-адресах других абонентских пунктов.
- **VPN-шлюз** – координатор, установленный в точке подключения локальной сети к Интернету, может быть использован мобильными и удаленными пользователями в качестве точки доступа к сети ViPNet.
- **VPN NAT-сервер** – координатор, установленный на границе сегмента сети, обеспечивает работу абонентских пунктов, находящихся в этом сегменте, от имени внешнего IP-адреса координатора. Можно также состыковать сеть ViPNet с другой системой VPN, шлюз которой должен быть присоединен к одному из сетевых адаптеров координатора.

- **Туннелирующий сервер** – координатор можно использовать для создания защищенного канала (туннеля) посредством шифрования трафика открытых сетевых узлов.

В сегментированных сетях можно использовать каскадную схему установки координаторов.

Существуют координаторы на платформах Windows и Linux, а также программно-аппаратные комплексы ViPNet Coordinator HW и MiniGate. Для создания отказоустойчивого решения на основе ViPNet Coordinator для Windows можно использовать ПО ViPNet Cluster. Для создания отказоустойчивого решения на базе ПО ViPNet Coordinator Linux или ПАК ViPNet Coordinator HW1000 предназначена система защиты от сбоев ViPNet Failover.

ПО ViPNet Coordinator или ViPNet Client, установленное на сервере, можно использовать для защиты трафика определенных (или всех сразу) служб и приложений (например, контроллер домена, SMTP/FTP/Web-серверы, сервер базы данных).

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 пользователя.

В сети ViPNet существует возможность централизованного управления политиками безопасности на сетевых узлах. В Центре управления политиками безопасности для отдельных узлов или групп формируются шаблоны политики безопасности, содержащие настройки фильтрации открытого IP-трафика и других параметров ПО ViPNet.

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 терминалы, мобильные абонентские пункты на платформах iOS и Android, другие специализированные решения.

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

- Сколько сетей ViPNet нужно создать и требуется ли иерархическая структура Центров управления сетью?
- 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 станций, серверов и сегментов локальной сети нуждаются в защите трафика?
- На какие рабочие станции достаточно установить ПО ViPNet CryptoService?
- Какие открытые узлы должны туннелироваться координаторами?
- Какая логическая структура VPN-соединений наиболее полно отвечает существующей физической структуре сети?
- Сколько должно быть координаторов? Какие типы координаторов следует использовать?
- 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 абонентские пункты между координаторами?
- Как осуществляется доступ к серверам и шлюзам 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 приложения планируется защищать с помощью VPN (базы данных, CRM/CMS/ERP системы, Web-приложения 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 правила для этих устройств. Трафик от других сетевых узлов ViPNet не блокируется.

- Будут ли использоваться другие средства защиты информации (сетевые экраны, антивирусное и другое ПО)?

Развертывание рабочего места администратора

Рекомендации по установке

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

- ViPNet Центр управления сетью (ЦУС) — предназначен для регистрации сетевых узлов и пользователей сети ViPNet, создания связей между ними, определения полномочий пользователей, централизованной рассылки обновлений ключевой информации и программного обеспечения и так далее.
- ViPNet Удостоверяющий и ключевой центр (УКЦ) — предназначен для создания ключевой информации и издания сертификатов открытого ключа подписи. Администратор УКЦ называется уполномоченным лицом.

Для установки ПО ViPNet Administrator требуется соответствующий установочный файл, а также файлы лицензии `infotecs.re` и `infotecs.reg`. Лицензия определяет ограничения на количество сетевых узлов, одновременно туннелируемых соединений и на прикладные задачи, которые могут выполняться на сетевых узлах.

ЦУС и УКЦ можно установить на одном компьютере или на двух разных компьютерах, если этого требует политика безопасности. Если установка ЦУСа и УКЦ производится на разных компьютерах, то в ЦУСе для них должны быть созданы два абонентских пункта (АП ЦУС и АП УКЦ). На компьютере, на котором установлен ЦУС, нужно задать папки для обмена информацией между ЦУСом и УКЦ; для компьютера, на котором установлен УКЦ, нужно открыть сетевой доступ к этим папкам. На АП ЦУС нужно обязательно установить ViPNet Client или ViPNet CryptoService (если защита трафика не требуется). На АП 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 АП ЦУС).

Центры управления сетью нескольких сетей ViPNet можно объединить в иерархическую структуру. Такая необходимость может возникнуть, если несколько удаленных филиалов организации имеют свои собственные сети ViPNet. В этом случае в головном ЦУСе осуществляется централизованное управление лицензиями подчиненных сетей.

Для организации иерархической системы Центров управления сетью требуется специальный файл лицензии `infotecs.reg`, в котором указаны суммарные лицензионные ограничения на головную и подчиненные сети ViPNet, а также номера головной и подчиненных сетей. Сначала необходимо установить в головной сети ViPNet Administrator, воспользовавшись для этого специальным общим файлом лицензии. Затем в головном ЦУСе следует распределить лицензионные ограничения для подчиненных сетей и сформировать для них файлы лицензии. После этого можно выполнять развертывание подчиненных сетей.

Для подготовки рабочего места администратора сети ViPNet выполните следующие действия:

- 1 Установите на рабочем месте администратора ПО ViPNet Administrator. В случае необходимости установите компоненты ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр на разные компьютеры.
- 2 В ЦУСе создайте структуру защищенной сети ViPNet (см. «[Регистрация узлов в прикладных задачах](#)» на стр. 38, «[Создание сетевых узлов и пользователей](#)» на стр. 33).
- 3 В УКЦ сформируйте дистрибутив ключей (см. «[Создание дистрибутивов ключей](#)» на стр. 41) для АП администратора (или два дистрибутива для АП ЦУС и АП УКЦ).
- 4 На компьютере, на котором установлен ЦУС, выполните установку ПО ViPNet Client. Если защита IP-трафика на рабочем месте администратора не требуется, вместо ViPNet Client можно установить ViPNet CryptoService.

Установка ViPNet Administrator

Перед установкой ПО ViPNet Administrator на компьютере администратора убедитесь, что на этом компьютере выполнены стандартные сетевые настройки, а также правильно заданы часовой пояс, дата и время. Установку должен выполнять пользователь, обладающий правами администратора в ОС Windows.

Для установки ПО ViPNet Administrator:

- 1 Скопируйте файлы лицензии в одну папку с программой установки `setup.exe`. Тогда при установке они автоматически будут помещены в нужные папки: в папку установки ЦУСа (`\NCC`) — файлы `infotecs.re` и `infotecs.reg`, в папку установки УКЦ (`\KC`) — `infotecs.re`. В противном случае после установки ViPNet Administrator необходимо вручную поместить файлы лицензии в указанные папки.

- 2 Двойным щелчком запустите программу установки `setup.exe` .

3 Следуйте указаниям мастера установки.

Если компоненты ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр требуется установить на разные компьютеры, то в процессе установки выполните следующие действия:

- На странице **Тип установки** выберите пункт **Выборочная установка**.
- На странице **Компоненты программного продукта** при установке ЦУСа снимите флажок **ViPNet Удостоверяющий и ключевой центр**. При установке УКЦ снимите флажок **ViPNet Центр управления сетью**.

4 По окончании установки перезагрузите компьютер.

Если перед установкой ViPNet Administrator файлы лицензии не были скопированы в одну папку с программой установки, поместите в подпапку \NCC в папке установки программы файлы `infotecs.re` и `infotecs.reg`, а в подпапку \KC — файл `infotecs.re`.

Если ЦУС и УКЦ были установлены на разные компьютеры, на обоих компьютерах нужно выполнить настройку папок для обмена информацией между ЦУСом и УКЦ:

- При первом запуске ЦУСа в окне **Настройка путей** укажите папки для обмена файлами с УКЦ (это окно можно вызвать с помощью меню **Управление > Пути**). Рекомендуем оставить папки по умолчанию: `..\FOR_NCC\` и `..\FROM_NCC\`.
- Используя средства операционной системы, откройте сетевой доступ к указанным папкам обмена для компьютера, на котором установлен УКЦ.
- В УКЦ в мастере первичной инициализации или в настройках УКЦ (раздел **Папки ViPNet Администратора** в окне **Настройка**) укажите сетевой путь к папкам обмена на компьютере, где установлен ЦУС.



Примечание. Первичную инициализацию УКЦ следует выполнять после того, как в ЦУСе создана структура сети и сформированы справочники для УКЦ.



3

Создание топологии сети в ViPNet Administrator

Создание сетевых узлов и пользователей	33
Регистрация узлов в прикладных задачах	38
Создание дистрибутивов ключей	41

Создание сетевых узлов и пользователей

Перед созданием логической структуры сети ViPNet рекомендуется задать настройки по умолчанию для новых сетевых узлов и типов коллективов. Эти настройки позволяют автоматизировать действия администратора при создании объектов сети ViPNet. Чтобы задать настройки по умолчанию:

- 1 В программе ViPNet Центр управления сетью в меню **Службы** выберите пункт **Настройки по умолчанию**. Откроется окно **Настройки по умолчанию** (это окно также открывается при первом запуске ЦУСа).
- 2 Установите или снимите флажок **Автоматически связывать новый ТК со всеми другими ТК**.
- 3 Установите или снимите флажок **Автоматически создавать ТК и пользователя для нового узла**.
- 4 В группе **Уровень полномочий** задайте для новых сетевых узлов уровень полномочий, который будет по умолчанию установлен в прикладных задачах «Защита трафика», «Деловая почта» и «КриптоСервис».
- 5 В группе **Автоматически регистрировать новые СУ** выберите прикладные задачи по умолчанию для новых сетевых узлов.
- 6 При необходимости измените другие настройки.

Для создания сетевых узлов в меню **Службы** выберите пункт **Адресная администрация**, затем выберите **Структура сети ViPNet**. В окне **ViPNet. Администрация сетевого уровня** выполните следующие действия:

- 1 Создайте необходимое количество координаторов (серверов-маршрутизаторов).
- 2 На каждом координаторе зарегистрируйте необходимое количество абонентских пунктов.
- 3 Создайте межсерверные каналы для связи координаторов между собой. Каждый канал связывает два координатора. Можно связать все координаторы с одним центральным (схема «звезда»), все координаторы между собой или использовать другие схемы.

Необходимо, чтобы все координаторы были логически связаны. Если связи заданы таким образом, что существует несколько путей для передачи информации между двумя координаторами, маршрутизация будет выполняться по кратчайшему пути.

Для проверки наличия необходимых связей можно выбрать пункт **Выдать таблицы маршрутизации**. Если связей будет недостаточно, программа выдаст предупреждение.

- 4 При необходимости создайте группы сетевых узлов и добавьте в них сетевые узлы. В группы можно объединять сетевые узлы, которые однозначно должны быть связаны между собой. На группе можно зарегистрировать тип коллектива.



Примечание. Для создания сетевой структуры можно воспользоваться функцией автоматической генерации сетевых узлов (меню **Службы > Адресная администрация > Автоматическая генерация**). При автоматической генерации создается заданное количество координаторов, на каждом из которых зарегистрировано заданное количество абонентских пунктов. Имена сетевых узлов формируются на основе заданных префиксов.

Для регистрации типов коллективов и пользователей выполните следующие действия:

- 1 В окне **Каталог типов коллективов** (меню **Службы > Прикладная администрация > Регистрация типов коллективов**) добавьте новые типы коллективов. При создании типа коллективов для него нужно указать область действия — сетевой узел или группу сетевых узлов.



Примечание. Если в окне настроек по умолчанию установлен флажок **Автоматически создавать ТК и пользователя для нового узла**, на всех созданных сетевых узлах уже зарегистрировано по одному типу коллектива, в каждом из которых зарегистрировано по одному пользователю.

- 2 Задайте связи между типами коллективов, следуя приведенным ниже рекомендациям (см. «[Рекомендации по созданию связей](#)» на стр. 35).



Примечание. Если в окне настроек по умолчанию установлен флажок **Автоматически связывать новый ТК со всем другими ТК**, все созданные типы коллективов будут автоматически связаны между собой.

- 3 В окне **Каталог пользователей** (меню **Службы > Прикладная администрация > Регистрация пользователей**) добавьте новых пользователей.

Для каждого пользователя нужно указать по крайней мере один тип коллективов, можно указать несколько типов коллективов. Если для пользователя выбран тип коллективов, зарегистрированный на группе сетевых узлов, нужно дополнительно указать сетевые узлы из этой группы.

- 4 При необходимости установите для пользователей атрибуты коллективов. Если пользователь зарегистрирован в нескольких коллективах, один из них должен быть назначен главным коллективом.

Также коллектив может быть открытым или скрытым: если для некоторого пользователя коллектив определен как скрытый, другие пользователи коллектива не будут видеть данного пользователя в адресных справочниках.

- 5 При необходимости задайте списки рассылки копий и СОС (в меню **Службы > Прикладная администрация** пункты **Списки рассылки копий** и **Список рассылки СОС**).

Примечание. В программе ViPNet Центр управления сетью версии 3.2.3 произошли изменения в меню:



- Пункты **Регистрация типов коллективов** и **Регистрация пользователей** находятся в меню **Службы**.
 - Пункты **Списки рассылки копий** и **Список рассылки СОС** находятся в меню **Службы > Списки рассылки**.
-

Более подробные инструкции по созданию сетевой структуры содержатся в документе «ViPNet Administrator Центр управления сетью. Руководство администратора».

Рекомендации по созданию связей

Примечание. В данном разделе допущены следующие упрощения:



- Под выражением «связи между сетевыми узлами» подразумевается «связи между типами коллективов, зарегистрированными на сетевых узлах».
 - Под выражением «абонентские пункты данного координатора» подразумевается «абонентские пункты, использующие данный координатор в качестве сервера IP-адресов».
-

Данные рекомендации относятся к сетевым узлам, зарегистрированным в прикладной задаче «Защита IP-трафика».

Для установления соединения между двумя абонентскими пунктами необходимо, чтобы эти абонентские пункты обладали информацией о параметрах доступа друг к другу. Такую информацию каждый абонентский пункт получает от своего сервера IP-адресов. Абонентский пункт также сообщает серверу IP-адресов информацию о собственных параметрах доступа. По умолчанию в качестве сервера IP-адресов используется координатор, на котором абонентский пункт зарегистрирован в ЦУСе. На абонентском пункте в качестве сервера IP-адресов можно выбрать другой координатор.

Координаторы обмениваются между собой информацией об абонентских пунктах, для которых они являются серверами IP-адресов, с учетом установленных между абонентскими пунктами связей. Для обеспечения этого обмена между координаторами в ЦУСе также должны быть установлены необходимые связи. Естественно, для решения этой задачи можно связать каждый координатор со всеми координатами 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:

- Координатор «А», являющийся сервером IP-адресов абонентского пункта «В», отправляет информацию об этом абонентском пункте на координатор «С», если абонентский пункт «В» связан с координатором «С» или с абонентскими пунктами координатора «С».
- Координатор «С», получивший информацию об абонентском пункте «В» от координатора «А» своей сети ViPNet:
 - Никогда не передает ее третьему координатору своей сети, то есть цепочка передачи информации об абонентских пунктах в одной сети всегда состоит только из двух координаторов.
 - Если координатор «А» не связан с координаторами другой сети ViPNet, а абонентский пункт «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 об абонентском пункте «В» от координатора «С» другой сети, передает ее на координатор «E» своей сети, если абонентский пункт «В» связан с координатором «E» или с абонентскими пунктами координатора «E».

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

- 1 Если абонентский пункт зарегистрирован в ЦУСе на координаторе «А», то нет необходимости явным образом устанавливать между ними связь. Такая связь создается автоматически.
- 2 Если координатор «А» из сети «М» и координатор «В» из сети «N» являются шлюзовыми между сетями «М» и «N», то нет необходимости явным образом устанавливать связь между этими координаторами. Такая связь создается автоматически.
- 3 Если абонентскому пункту координатора «А» не требуется устанавливать соединение с координатором «В» или его туннелируемыми узлами, то не рекомендуется устанавливать связь этого абонентского пункта с координатором «В».
- 4 Если координаторы «А» и «В» из одной сети ViPNet являются серверами IP-адресов для абонентских пунктов, которые связаны между собой, то координаторы «А» и «В» необходимо также связать между собой.
- 5 Если координатор «А» сети «М» не является шлюзовым координатором в сеть «N» и не связан с координаторами сети «N», но при этом сам координатор «А» или его абонентские пункты связаны с абонентскими пунктами сети «N», то координатор «А» необходимо связать со шлюзовым координатором сети «М» в сеть «N».
- 6 Если координатор «А» сети «М», который не является шлюзовым координатором в сеть «N», связан с координатором «В» сети «N» (например, для взаимодействия между туннелируемыми узлами координаторов), то координатор «А» необходимо связать также со всеми другими координаторами сети «М», абонентские пункты которых связаны с узлами сети «N».
- 7 Если требуется создать резервный сервер IP-адресов для группы абонентских пунктов, необходимо связать эти абонентские пункты с некоторым координатором. Абонентские пункты 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.

Регистрация узлов в прикладных задачах

Прикладные задачи определяют, какие прикладные программы ViPNet могут работать на тех или иных сетевых узлах. В ходе создания защищенной сети ViPNet в ЦУСе обязательно должна быть выполнена регистрация абонентских пунктов и координаторов в прикладных задачах.

Все сетевые узлы при создании могут быть автоматически зарегистрированы в основных прикладных задачах, если в окне настроек по умолчанию (меню **Службы > Настройки по умолчанию**) установлены соответствующие флажки.

Сначала зарегистрируйте в прикладных задачах абонентские пункты:

- 1 В меню **Службы** выберите пункт **Индивидуальная регистрация АП в ПЗ**.
- 2 В окне **Индивидуальная регистрация АП в прикладных задачах** укажите прикладные задачи для каждого абонентского пункта. Для этого выберите абонентский пункт в списке, нажмите кнопку **Регистрация** и в окне **Регистрация АП в ПЗ** установите флажки напротив нужных прикладных задач.
- 3 Абонентский пункт, на котором установлено ПО ViPNet Administrator, необходимо зарегистрировать в прикладных задачах «Центр управления сетью» и «Удостоверяющий и ключевой центр».

Если ЦУС и УКЦ установлены на разных компьютерах, нужно создать для них два абонентских пункта, один из которых должен быть зарегистрирован в прикладной задаче «Центр управления сетью», а другой — в задаче «Удостоверяющий и ключевой центр».

При этом в каждой из данных прикладных задач может быть зарегистрирован только один абонентский пункт.

Для настройки координаторов и указания параметров различных прикладных задач выполните следующие действия:

- 1 В меню **Службы** выберите пункт **Групповая регистрация СУ в ПЗ**.
В окне **Регистрация сетевых узлов в прикладных задачах** войдите в задачу **Сервер IP-адресов** и выполните следующие действия:
 - Добавьте координаторы, если они не присутствуют в списке по умолчанию.

- Для каждого координатора укажите собственные IP-адреса, адреса туннелируемых координатором открытых узлов (если необходимо), задайте параметры подключения координатора к сети и настройки межсетевого экрана для абонентских пунктов, зарегистрированных на этом координаторе.
Указанные параметры задаются с помощью специальных строк, добавляемых в список IP-адресов. Формат этих строк описан в документе «ViPNet Administrator Центр управления сетью. Руководство администратора» в разделе 12.5.1.
 - При необходимости задайте для координаторов максимальное число одновременно туннелируемых адресов.
 - При необходимости включите для координаторов функцию «Сервер открытого Интернета».
 - При необходимости задайте для координаторов списки терминалов, для которых они будут резервными серверами.
- 2** При необходимости зарегистрируйте определенные координаторы в таких задачах, как «ViPNet Cluster», «ViPNet Coordinator HW», «ViPNet Failover», «Сервер SGA» и другие.
- 3** При необходимости в окне прикладной задачи **Защита IP-трафика** укажите IP-адреса абонентских пунктов. Для абонентских пунктов, у которых настройки межсетевого экрана должны отличаться от заданных на сервере IP-адресов, можно указать специальные параметры.
Формат строк, используемых для настройки параметров межсетевого экрана, описан в документе «ViPNet Administrator Центр управления сетью. Руководство администратора» в разделе 12.5.1.
- 4** При необходимости измените уровень полномочий для сетевых узлов, зарегистрированных в задачах «Защита трафика», «Деловая почта» и «КриптоСервис».
Уровень полномочий определяет допустимость изменения пользователем различных настроек ПО ViPNet на сетевом узле. На вновь создаваемых сетевых узлах в перечисленных задачах устанавливается уровень полномочий, заданный в окне настроек по умолчанию (меню **Службы > Настройки по умолчанию**).
- 5** Для абонентских пунктов, зарегистрированных в прикладной задаче «Центр регистрации», установите ограничения числа запросов на дистрибутивы и сертификаты.
- 6** Для абонентских пунктов, зарегистрированных в прикладной задаче «Центр управления политиками», укажите списки узлов, которыми могут управлять эти центры.

- 7 Для абонентских пунктов, зарегистрированных в прикладной задаче «Сервер мониторинга», задайте ограничения на число узлов мониторинга и дочерних серверов.

Подробная информация о прикладных задачах содержится в документе «ViPNet Administrator Центр управления сетью. Руководство администратора».

Завершив регистрацию сетевых узлов в прикладных задачах, в меню **Службы** выберите пункт **Проверка конфигурации**, чтобы убедиться в отсутствии аномальных ситуаций в созданной структуре сети ViPNet. Если будут обнаружены ошибки в конфигурации, их описание будет выведено в отдельном окне.

Примечание. В программе ViPNet Центр управления сетью версии 3.2.3 были переименованы следующие пункты меню:



- Пункт **Индивидуальная регистрация АП в ПЗ** переименован в **Индивидуальная регистрация АП в задачах**.
 - Пункт **Групповая регистрация СУ в ПЗ** переименован в **Групповая регистрация узлов в задачах**.
 - Пункт **Проверка конфигурации** переименован в **Проверка конфигурации сети**.
-

Создание дистрибутивов ключей

После создания логической структуры сети в программе ViPNet Центр управления сетью в меню **Службы** выберите команду **Сформировать все справочники**. По этой команде будут сформированы и помещены в папку обмена информацией с УКЦ справочники, предназначенные для создания ключевой информации пользователей.

Затем проведите первичную инициализацию программы ViPNet Удостоверяющий и ключевой центр (эта процедура описана в документе «ViPNet Administrator Удостоверяющий и ключевой центр. Руководство администратора»).

Для развертывания сетевых узлов требуется создать дистрибутивы ключей. Для этого в УКЦ в меню **Сервис** выберите пункт **Автоматически создать**, затем щелкните

Дистрибутивы ключей (или нажмите кнопку **Создать дистрибутивы ключей**  на панели инструментов).

Будет запущен процесс создания дистрибутивов. При этом программа предложит задать пароль администратора для группы «Вся сеть» (в эту группу входят все сетевые узлы), который используется для входа в режим администратора на сетевых узлах. Созданные дистрибутивы будут отображены в УКЦ в папке **Ключевой центр\Своя сеть ViPNet\Ключи\Дистрибутивы ключей**.

Используйте созданные дистрибутивы ключей для установки ПО ViPNet на сетевых узлах. Для этого рекомендуется выполнить 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 На съемном носителе доставьте дистрибутивы 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. 42) и [Развертывание абонентского пункта](#) (на стр. 47).



4

Развертывание координатора

Рекомендации по установке	43
Установка ViPNet Coordinator	45
Настройка 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, программно-аппаратных комплексов ViPNet Coordinator HW и ViPNet MiniGate, 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 сетям TCP/IP или к Интернету. Способ подключения к Интернету может быть любым: xDSL, ISDN, GPRS, UMTS, Wi-Fi, WiMAX и другие. 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 правил фильтрации трафика не требуется.

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

Установка ViPNet Coordinator

Процесс установки клиентского ПО ViPNet (ViPNet Client и ViPNet CryptoService) ничем не отличается от установки ViPNet Coordinator. Поэтому указания, содержащиеся в данном разделе, относятся ко всем перечисленным программам.

Перед установкой компонентов ПО ViPNet убедитесь, что на компьютере выполнены стандартные сетевые настройки, а также правильно заданы часовой пояс, дата и время. Установку должен выполнять пользователь, обладающий правами администратора в ОС Windows.

Для установки ViPNet Coordinator или клиентского ПО ViPNet требуются:

- Соответствующий комплект установки.
- Дистрибутив ключей для сетевого узла.
- Пароль пользователя сетевого узла.

Дистрибутивы и пароли пользователей создаются в программе ViPNet Удостоверяющий и ключевой центр (см. «[Создание дистрибутивов ключей](#)» на стр. 41).

Для установки одного из компонентов ПО ViPNet выполните следующие действия:

- 1 Двойным щелчком запустите программу установки setup.exe .
- 2 Следуйте указаниям мастера установки.
- 3 По окончании установки перезагрузите компьютер.
- 4 После перезагрузки выполните первичную инициализацию справочно-ключевой информации.

Подробно установка компонентов ПО ViPNet описана в следующих документах: «ViPNet Coordinator Монитор. Руководство администратора», «ViPNet Client Монитор. Руководство пользователя», «ViPNet CryptoService. Руководство пользователя».

Настройка ViPNet Coordinator

Чтобы уменьшить количество ручных настроек, выполняемых непосредственно на координаторе, рекомендуется задать IP-адреса координаторов, туннелируемых узлов и настройки подключения координатора к сети в ЦУСе во время регистрации сетевых узлов в прикладных задачах (см. «[Регистрация узлов в прикладных задачах](#)» на стр. 38). Если необходимые настройки не были сделаны в ЦУСе, выполните следующие действия:

- 1 Настройте параметры межсетевого экрана (см. «ViPNet Coordinator Монитор. Руководство администратора», глава 3).
- 2 Задайте IP-адреса других координаторов сети ViPNet (см. «ViPNet Coordinator Монитор. Руководство администратора», глава 3, раздел «Настройка доступа к защищенным узлам»).
- 3 При необходимости задайте IP-адреса открытых узлов, туннелируемых координатором (см. «ViPNet Coordinator Монитор. Руководство администратора», глава 8).
- 4 Если координатор должен подключаться к открытым узлам, которые туннелируются другими координаторами, задайте IP-адреса этих узлов (см. «ViPNet Coordinator Монитор. Руководство администратора», глава 3, раздел «Настройка доступа к узлам, туннелируемым другим координатором»).

Также при необходимости выполните на координаторе следующие настройки:

- 1 Задайте правила трансляции адресов (см. «ViPNet Coordinator Монитор. Руководство администратора», глава 7).
- 2 Настройте интегрированный межсетевой экран:
 - Установите режимы безопасности на сетевых интерфейсах (см. «ViPNet Coordinator Монитор. Руководство администратора», глава 5, раздел «Режимы безопасности»).
 - Настройте параметры антиспуфинга (см. «ViPNet Coordinator Монитор. Руководство администратора», глава 5, раздел «Антиспуфинг»).
 - Задайте правила фильтрации открытого и защищенного трафика (см. «ViPNet Coordinator Монитор. Руководство администратора», глава 5, раздел «Правила фильтрации трафика»).
- 3 Настройте параметры обработки прикладных протоколов и веб-фильтры (см. «ViPNet Coordinator Монитор. Руководство администратора», глава 6).



5

Развертывание абонентского пункта

Рекомендации по установке	48
Настройка ViPNet Client	50

Рекомендации по установке

На абонентском пункте следует установить один из двух компонентов ПО 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. Способ подключения к Интернету может быть любым: xDSL, ISDN, GPRS, UMTS, Wi-Fi, WiMAX и другие. 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.

Краткое описание установки ПО ViPNet Client и ViPNet CryptoService приведено в разделе [Установка ViPNet Coordinator](#) (на стр. 45). Более подробно установка описана в документации указанных продуктов.

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

Настройка ViPNet Client

Чтобы уменьшить количество ручных настроек, выполняемых непосредственно на абонентском пункте, рекомендуется задать IP-адреса координаторов, туннелируемых узлов и настройки подключения абонентского пункта к сети в ЦУСе во время регистрации сетевых узлов в прикладных задачах (см. «[Регистрация узлов в прикладных задачах](#)» на стр. 38). Если необходимые настройки не были сделаны в ЦУСе, выполните следующие действия:

- 1 Настройте параметры межсетевого экрана (см. «ViPNet Client Монитор. Руководство пользователя», глава 2).
- 2 Задайте IP-адрес сервера IP-адресов, выбранного для данного абонентского пункта (см. «ViPNet Client Монитор. Руководство пользователя», глава 3, раздел «Настройка доступа к защищенным узлам»).
- 3 Если абонентский пункт должен подключаться к туннелируемым узлам, задайте IP-адреса этих узлов (см. «ViPNet Client Монитор. Руководство пользователя», глава 3, раздел «Настройка доступа к туннелируемым узлам»).

Также на абонентском пункте необходимо выполнить следующие настройки:

- 1 Настройте интегрированный сетевой экран:
 - Установите режим безопасности (см. «ViPNet Client Монитор. Руководство пользователя», глава 4, раздел «Режимы безопасности»).
 - Задайте правила фильтрации открытого и защищенного трафика (см. «ViPNet Client Монитор. Руководство пользователя», глава 4, раздел «Правила фильтрации трафика»).
- 2 Настройте параметры обработки прикладных протоколов и веб-фильтры (см. «ViPNet Client Монитор. Руководство пользователя», глава 5).

6

Проверка функционирования сети ViPNet

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

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

Для полноценного функционирования сети необходима возможность соединения между всеми координаторами, а также между абонентскими пунктами 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.



Указатель

З

Защита информации в сети ViPNet - 20

Н

Настройка ViPNet Client - 49

Настройка ViPNet Coordinator - 44

О

Обратная связь - 23

П

Планирование сети - 23

Р

Развертывание абонентского пункта - 14,
19, 41

Развертывание координатора - 18, 41

Развертывание рабочего места
администратора - 13, 17

Регистрация узлов в прикладных задачах
- 30, 46, 50

Рекомендации по созданию связей - 34

С

Создание дистрибутивов ключей - 30, 45

Создание сетевых узлов и пользователей
- 30

У

Установка ViPNet Coordinator - 48