



# ViPNet Coordinator KB 4

Общее описание

1991–2018 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.465614.001РЭ1

Версия продукта 4.2.0

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

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

ViPNet® является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

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

ОАО «ИнфоТеКС»

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

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

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

Электронный адрес службы поддержки: [hotline@infotecs.ru](mailto:hotline@infotecs.ru)

# Содержание

<b>Введение</b> .....	<b>5</b>
О документе.....	6
Для кого предназначен документ.....	6
Соглашения документа.....	6
Связанные документы.....	7
Комплект поставки.....	8
Что нового в версии 4.2.0.....	9
Обратная связь.....	11
<b>Глава 1. Общая информация</b> .....	<b>12</b>
Защищенная сеть ViPNet.....	13
Назначение ViPNet Coordinator KB.....	14
Функции координатора в защищенной сети.....	15
Сервер IP-адресов.....	15
Маршрутизатор VPN-пакетов.....	16
Сервер соединений.....	17
VPN-шлюз.....	18
Транспортный сервер.....	20
Межсетевой экран.....	21
Лицензирование ViPNet Coordinator KB.....	23
Количество связей ViPNet Coordinator KB с ViPNet-узлами.....	24
Режимы подключения ViPNet Coordinator KB к внешней сети.....	25
Подключение через межсетевой экран со статической трансляцией адресов.....	25
Подключение через межсетевой экран с динамической трансляцией адресов.....	26
Подключение без использования внешнего межсетевого экрана.....	26
Обработка сетевого трафика в соответствии с его приоритетом.....	28
Назначение и принципы работы системы защиты от сбоев.....	29
Работа системы защиты от сбоев в одиночном режиме.....	29
Работа системы защиты от сбоев в режиме кластера горячего резервирования.....	29
<b>Глава 2. Описание исполнений ViPNet Coordinator KB</b> .....	<b>31</b>
Исполнение ViPNet Coordinator KB100.....	32
Аппаратная платформа KB100 N1.....	32
Исполнение ViPNet Coordinator KB1000.....	34
Аппаратная платформа KB1000 Q6.....	34

Исполнение ViPNet Coordinator KB2000 .....	36
Аппаратная платформа KB2000 Q4 .....	36
Исполнение ViPNet Coordinator KB5000 .....	38
Аппаратная платформа KB5000 Q1 .....	38
<b>Глава 3. Возможности управления ViPNet Coordinator KB .....</b>	<b>40</b>
Способы управления ViPNet Coordinator KB .....	41
Назначение командного интерпретатора .....	42
Режимы работы в командном интерпретаторе .....	43
Аутентификация пользователя .....	44
Экстренное стирание ключевой информации .....	45
<b>Приложение А. Глоссарий .....</b>	<b>46</b>



# Введение

О документе	6
Связанные документы	7
Комплект поставки	8
Что нового в версии 4.2.0	9
Обратная связь	11

# О документе

В документе описывается назначение и применение программно-аппаратного комплекса ViPNet Coordinator KB (далее — ViPNet Coordinator KB) в составе защищенных сетей ViPNet, способы настройки и управления, приводится описание существующих исполнений ViPNet Coordinator KB, их аппаратных платформ и условий лицензирования.

## Для кого предназначен документ

Документ предназначен для администраторов, отвечающих за настройку и эксплуатацию ViPNet Coordinator KB.

## Соглашения документа

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

Таблица 1. Обозначения, используемые в примечаниях




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

Таблица 2. Обозначения, используемые для выделения информации в тексте

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

# Связанные документы

В таблице ниже перечислены документы, входящие в комплект документации ViPNet Coordinator KB помимо данного документа, и описаны основные сведения, которые содержит каждый из этих документов.

Таблица 3. Связанные документы

Документ	Содержание
«ViPNet Coordinator KB 4. Настройка с помощью командного интерпретатора»	Настройка подключения к сети (настройка сетевых интерфейсов Ethernet, дополнительных IP-адресов (алиасов), виртуальных сетевых интерфейсов VLAN)  Настройка даты и времени  Настройка сервисных функций (DHCP-, DNS-, NTP-сервер, функциональность L2OverIP)  Настройка подключения ViPNet Coordinator KB к внешней сети через межсетевой экран  Настройка статической и динамической маршрутизации  Настройка сетевых фильтров  Настройка трансляции IP-адресов  Настройка транспортного модуля MFTP  Просмотр журнала конвертов MFTP  Развертывание системы защиты от сбоев  Настройка протоколирования событий и просмотр журналов (журналы устранения неполадок, журнал IP-пакетов)
«ViPNet Coordinator KB 4. Справочник команд и конфигурационных файлов»	Описание команд ViPNet Coordinator KB  Описание конфигурационных файлов управляющего демона и системы защиты от сбоев
«ViPNet Coordinator KB 4. Лицензионные соглашения на компоненты сторонних производителей»	Лицензионные соглашения на компоненты сторонних производителей, которые использовались при разработке ПО для ViPNet Coordinator KB

# Комплект поставки

В комплект поставки ViPNet Coordinator KB входят следующие компоненты:

- Программно-аппаратный комплекс ViPNet Coordinator KB, в зависимости от исполнения (см. [Описание исполнений ViPNet Coordinator KB](#) на стр. 31).
- Документация в формате PDF:
  - «Программно-аппаратный комплекс ViPNet Coordinator KB 4. Правила пользования».
  - «ViPNet Coordinator KB. Общее описание».
  - «ViPNet Coordinator KB. Настройка с помощью командного интерпретатора».
  - «ViPNet Coordinator KB. Справочник команд и конфигурационных файлов».
  - «ViPNet Coordinator KB. Лицензионные соглашения на компоненты сторонних производителей».
- Документация в печатном виде:
  - «Программно-аппаратный комплекс ViPNet Coordinator KB 4. Формуляр».
  - Копии сертификатов соответствия ФСБ России на программно-аппаратный комплекс ViPNet Coordinator KB 4.



# Что нового в версии 4.2.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Coordinator KB версии 4.2.0 по сравнению с более ранними версиями.

- **Поддержка новых исполнений**

Теперь ViPNet Coordinator KB поставляется в одном из четырех исполнений (см. [Описание исполнений ViPNet Coordinator KB](#) на стр. 31):

- ViPNet Coordinator KB100 — на базе аппаратной платформы KB100 N1.
- ViPNet Coordinator KB1000 — на базе аппаратной платформы KB1000 Q6.
- ViPNet Coordinator KB2000 — на базе аппаратной платформы KB2000 Q4.
- ViPNet Coordinator KB5000 — на базе аппаратной платформы KB5000 Q1.

- **Добавлен режим кластера горячего резервирования**

Для повышения отказоустойчивости обеспечена работа системы защиты от сбоев ViPNet Coordinator KB в режиме кластера горячего резервирования. Исполнение ViPNet Coordinator KB100 не поддерживает данный режим.

Подробное описание настройки кластера горячего резервирования изложено в документе «ViPNet Coordinator KB. Настройка с помощью командного интерпретатора».

- **Объединение сегментов сетей на канальном уровне в едином адресном пространстве**

В новой версии ViPNet Coordinator KB реализована поддержка технологии L2OverIP, которая позволяет объединить на канальном уровне до 31 сегмента сети, использующих одно и то же адресное пространство.

В результате объединения узлы из разных сегментов будут взаимодействовать друг с другом так, как будто они находятся в одной локальной сети.

Подробное описание настройки технологии L2OverIP изложено в документе «ViPNet Coordinator KB. Настройка с помощью командного интерпретатора».

- **Поддержка совместной работы с ПО ViPNet Policy Manager**

Теперь ViPNet Coordinator KB может принимать и обрабатывать политики безопасности, присланные из программы ViPNet Policy Manager.

- **Новые функции для работы с виртуальными локальными сетями**

Для обеспечения работы ViPNet Coordinator KB с разветвленной сетью, состоящей из нескольких виртуальных сетей, реализована поддержка технологии виртуальных локальных сетей (VLAN) в соответствии со стандартом IEEE 802.1q. Для создания нескольких виртуальных интерфейсов на базе одного физического интерфейса в новой версии ViPNet Coordinator KB произошло разделение интерфейсов на два класса — класс интерфейсов, используемых обычным образом, и класс интерфейсов, используемых для работы с VLAN. Подробное описание настройки интерфейсов изложено в документе «ViPNet Coordinator KB. Настройка с помощью командного интерпретатора».

- **Поддержка классификации сетевого трафика Differentiated Services (DiffServ)**

Для поддержки механизма обеспечения качества обслуживания (QoS) в новой версии ViPNet Coordinator KB реализована возможность обрабатывать трафик в соответствии с заданными приоритетом (см. [Обработка сетевого трафика в соответствии с его приоритетом](#) на стр. 28).

- **Новые функции маршрутизации IP-трафика**

В новой версии ViPNet Coordinator KB функции маршрутизации были доработаны следующим образом:

- Реализованы функции динамической маршрутизации IP-трафика с использованием протокола OSPF.
- Добавлена возможность настраивать приоритеты маршрутов, формируемых по различным протоколам, с помощью метрик.
- Добавлена возможность создания статического маршрута с несколькими шлюзами и настройки распределения нагрузки передаваемого IP-трафика между ними.

Подробное описание настройки новых функций маршрутизации IP-трафика изложено в документе «ViPNet Coordinator KB. Настройка с помощью командного интерпретатора».

- **Появилась возможность экстренного удаления ключевой информации**

Теперь ViPNet Coordinator KB может стереть всю ключевую информацию по нажатию специальной кнопки (см. [Экстренное стирание ключевой информации](#) на стр. 45), которая расположена на передней панели аппаратной платформы.

- **Датчик несанкционированного доступа**

Для предотвращения несанкционированного доступа внутрь корпуса в составе аппаратных платформ ViPNet Coordinator KB добавлен датчик несанкционированного доступа (ДНСД).

- **Прекращение поддержки устаревших исполнений**

Больше не поддерживаются следующие исполнения:

- Исполнение ViPNet Coordinator KB100 X2.
- Исполнение ViPNet Coordinator KB1000 Q2.

# Обратная связь

## Дополнительная информация

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

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

## Контактная информация

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

- Единый многоканальный телефон:  
+7 (495) 737-6192,  
8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба технической поддержки: [hotline@infotecs.ru](mailto:hotline@infotecs.ru).  
Форма для обращения в службу технической поддержки через сайт <https://infotecs.ru/support/request/>.  
Консультации по телефону для клиентов с расширенной схемой технической поддержки:  
+7 (495) 737-6196.
- Отдел продаж: [soft@infotecs.ru](mailto:soft@infotecs.ru).

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

# 1

## Общая информация

Защищенная сеть ViPNet	13
Назначение ViPNet Coordinator KB	14
Функции координатора в защищенной сети	15
Лицензирование ViPNet Coordinator KB	23
Режимы подключения ViPNet Coordinator KB к внешней сети	25
Обработка сетевого трафика в соответствии с его приоритетом	28
Назначение и принципы работы системы защиты от сбоев	29

# Защищенная сеть ViPNet

Программно-аппаратный комплекс ViPNet Coordinator KB предназначен для использования в защищенной сети ViPNet, построенной на основе комплекса продуктов ViPNet.

Сеть ViPNet представляет собой [виртуальную защищенную сеть](#) (см. глоссарий, стр. 47), которая может быть развернута поверх локальных или глобальных сетей любой структуры. В отличие от многих популярных VPN-решений, технология ViPNet обеспечивает защищенное взаимодействие между [сетевыми узлами](#) (см. глоссарий, стр. 50) по схеме «клиент-клиент».

Защита информации в сети ViPNet осуществляется с помощью специального программного обеспечения, которое выполняет две основные функции:

- Фильтрация всего IP-трафика сетевых узлов. Фильтрация трафика осуществляется в соответствии с заданными на узле правилами.
- Шифрование соединений между узлами сети ViPNet. Для шифрования трафика используются [симметричные ключи](#) (см. глоссарий, стр. 50), которые создаются и распределяются централизованно.

Для управления защищенной сетью ViPNet предназначено программное обеспечение ViPNet Administrator. С помощью ViPNet Administrator создаются сетевые узлы и связи между ними, настраиваются параметры отдельных узлов, создаются [дистрибутивы ключей](#) (см. глоссарий, стр. 48) для каждого узла, выполняется централизованное обновление справочников, ключей и программного обеспечения на узлах.

Сетевые узлы ViPNet делятся на два типа:

- [Клиент \(ViPNet-клиент\)](#) (см. глоссарий, стр. 48) — рабочее место пользователя сети ViPNet.
- [Координатор \(ViPNet-координатор\)](#) (см. глоссарий, стр. 48) — сервер сети ViPNet. Сетевой узел ViPNet Coordinator KB является координатором.

Также сеть ViPNet может включать открытые узлы (компьютеры без программного обеспечения ViPNet), соединения которых через Интернет или другие публичные сети защищаются ViPNet-координаторами с помощью [туннелирования на сетевом уровне](#) (см. глоссарий, стр. 51).

# Назначение ViPNet Coordinator KB

Программно-аппаратный комплекс ViPNet Coordinator KB распространяется в нескольких исполнениях. Каждое исполнение ViPNet Coordinator KB представляет собой интегрированное решение на базе специализированной аппаратной платформы, программного обеспечения ViPNet, которое функционирует под управлением адаптированной ОС GNU/Linux, а также роли, назначаемой сетевому узлу в программе [ViPNet Центр управления сетью \(ЦУС\)](#) (см. глоссарий, стр. 47) и накладывающей определенные лицензионные ограничения.

В качестве аппаратной платформы для исполнения ViPNet Coordinator KB используется полноценный сервер, устанавливаемый в стандартные стойки. Характеристики всех поддерживаемых исполнений приведены в главе [Описание исполнений ViPNet Coordinator KB](#) (на стр. 31).

ViPNet Coordinator KB выступает в роли VPN-сервера и предназначен для использования в IP-сетях, защита которых организуется с применением комплекса программных продуктов ViPNet. Описание всех основных функций ViPNet Coordinator KB приведено в разделе [Функции координатора в защищенной сети](#) (на стр. 15).

ViPNet Coordinator KB также обладает следующими дополнительными возможностями:

- Обработка протоколов прикладного уровня: FTP, DNS, H.323, SCCP.
- Поддержка виртуальных локальных сетей (VLAN IEEE 802.1Q).
- Приоритизация обработки IP-трафика в соответствии с протоколом DiffServ.
- Функции DHCP-, DNS- и NTP-сервера.
- Функции маршрутизатора IP-пакетов с возможностью настройки статической и динамической маршрутизации.
- Функции кластера горячего резервирования.
- Взаимодействие с источником бесперебойного питания.
- Совместимость с управляющим программным обеспечением ViPNet Administrator, ViPNet Policy Manager, ViPNet StateWatcher.

# Функции координатора в защищенной сети

В защищенной сети ViPNet координатор выступает в роли VPN-сервера. Функции координатора определяются структурой и задачами этой сети и могут быть следующими:

- **Сервер IP-адресов** (на стр. 15). Функция, которая позволяет обеспечить взаимодействие защищенных узлов ViPNet. Сервер IP-адресов сообщает сетевым узлам информацию об адресах и параметрах доступа других узлов.
- **Маршрутизатор VPN-пакетов** (на стр. 16). Функция, которая позволяет обеспечить маршрутизацию транзитного защищенного IP-трафика, проходящего через координатор на другие защищенные узлы.
- **Сервер соединений**. Функция, которая обеспечивает соединение клиентов и координаторов друг с другом кратчайшим путем.
- **VPN-шлюз**. Функция, которая позволяет организовать защищенные соединения между узлами локальных сетей (на которых не установлено ПО ViPNet) и между сегментами сетей с помощью защищенных каналов (туннелей).
- **Транспортный сервер** (на стр. 20). Функция, которая обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений справочников, ключей и программного обеспечения из программы **ViPNet Центр управления сетью (ЦУС)** (см. глоссарий, стр. 47), а также обмен прикладными **транспортными конвертами** (см. глоссарий, стр. 51) между узлами.
- **Межсетевой экран**. Функция, которая позволяет обеспечить фильтрацию IP-трафика. Одновременно координатор может выполнять функции трансляции адресов для проходящего через него открытого трафика.

## Сервер IP-адресов

При подключении любого клиента с программой **ViPNet Client** (см. глоссарий, стр. 48) к сети или изменении его параметров подключения эти параметры сообщаются ViPNet Coordinator KB, который играет роль сервера IP-адресов для данного клиента. В свою очередь, сервер IP-адресов отправляет на клиент информацию о параметрах подключения и о состоянии всех узлов, с которыми у данного клиента имеется связь.

Таким образом, роль сервера IP-адресов заключается:

- в сборе сведений о сетевых узлах;
- в информировании о параметрах доступа и состоянии тех узлов сети, с которыми у данного клиента имеется связь.



Рисунок 1. Сервер IP-адресов в сети ViPNet

Чтобы подтвердить свое присутствие в сети, клиент периодически (по умолчанию — каждые 5 минут) отправляет на сервер сообщение о своей активности. Если такое сообщение не поступило, ViPNet Coordinator KB переводит клиент в статус «Недоступен».

Аналогичным образом происходит обмен информацией о параметрах доступа между координаторами. Периодически (по умолчанию — каждые 15 минут) ViPNet Coordinator KB на другие связанные с ним координаторы подтверждение о своей активности. Кроме того, координаторы обеспечивают рассылку информации об узлах, для которых они выполняют функцию сервера IP-адресов.

Сервер IP-адресов работает по следующей логике:

- При появлении новой информации о своем клиенте (то есть о клиенте, который использует ViPNet Coordinator KB в качестве сервера IP-адресов) ViPNet Coordinator KB рассылает ее на другие свои клиенты и связанные координаторы.
- При появлении новой информации о клиентах других координаторов рассылает эту информацию на свои клиенты, которые связаны с клиентами другого координатора.
- При отсутствии информации от своего клиента по истечении периода опроса ViPNet Coordinator KB считает этот клиент недоступным и рассылает информацию об этом.

По умолчанию для клиента роль сервера IP-адресов выполняет его транспортный сервер (координатор, на котором клиент зарегистрирован в программе ViPNet Центр управления сетью). В отличие от транспортного сервера, сервер IP-адресов можно сменить, выбрав любой другой координатор, с которым у данного клиента есть связь.

## Маршрутизатор VPN-пакетов

Координатор выполняет маршрутизацию транзитного защищенного трафика, который проходит через координатор на другие защищенные сетевые узлы. Маршрутизация осуществляется внутри одной сети ViPNet.





Рисунок 2. Функция маршрутизации защищенного трафика в сети ViPNet

Маршрутизация защищенного трафика осуществляется на основании идентификаторов защищенных узлов, содержащихся в открытой части IP-пакетов, которая защищена от подделки, и на основании защищенного протокола динамической маршрутизации трафика. Одновременно с этим для защищенного трафика выполняется [трансляция сетевых адресов \(NAT\)](#) (см. глоссарий, стр. 51). Все транзитные защищенные пакеты, поступающие на координатор, отправляются на другие узлы от имени IP-адреса координатора. Трансляция адресов для защищенного трафика выполняется автоматически в соответствии с параметрами, которые не могут быть изменены.

Если на границе сети ViPNet установлено стороннее устройство, выполняющее фильтрацию и трансляцию трафика, то в этом случае координатор может выступать в роли сервера соединений. С помощью сервера соединений клиенты устанавливают соединения друг с другом в том случае, если напрямую установить соединения они не могут. Для каждого клиента может быть назначен свой сервер соединений. По умолчанию сервером соединений для клиента выбран [сервер IP-адресов](#) (на стр. 15).

## Сервер соединений

ViPNet Coordinator KB может выступать в качестве [сервера соединений](#) (см. глоссарий, стр. 50) и устанавливать соединения между клиентами и координаторами по кратчайшему пути, если они находятся в разных подсетях и не могут соединиться друг с другом напрямую. Для каждого клиента может быть назначен свой сервер соединений. По умолчанию сервер соединений для клиента служит также сервером IP-адресов. Для координаторов также при необходимости может быть выбран сервер соединений.



Рисунок 3. Организация соединений между сетевыми узлами ViPNet

## VPN-шлюз

Координаторы в роли VPN-шлюзов позволяют защитить соединения между узлами локальных сетей, которые обмениваются информацией через публичные сети. Защита реализуется с помощью технологии туннелирования, в основе которой лежит инкапсуляция и шифрование проходящего через координаторы трафика. При этом координатор может выполнять туннелирование как на сетевом уровне (уровень 3 модели OSI), так и на канальном уровне (уровень 2 модели OSI).

Туннелирование трафика на сетевом уровне позволяет организовать защищенное соединение между открытым узлом и защищенным узлом ViPNet или между двумя открытыми узлами, которые туннелируются разными координаторами. В роли защищенного узла может быть узел с установленным ПО ViPNet Client или открытый узел, стоящий за ПАК Coordinator HW, который туннелирует этот узел. В этом случае указанный узел будет иметь защищенный доступ через сеть связи общего пользования к туннелируемым ресурсам, находящимся за ПАК ViPNet Coordinator KB, в соответствии с установленной политикой безопасности для этого узла.

В результате это позволяет включить открытые узлы в защищенную сеть ViPNet без установки на них программного обеспечения ViPNet. Туннелирование трафика на сетевом уровне выполняется следующим образом:

- На координатор поступают открытые IP-пакеты от туннелируемых узлов, которые обрабатываются сетевыми фильтрами.
- Обработанные IP-пакеты на координаторе зашифровываются и упаковываются в новые IP-пакеты, после чего передаются на защищенные узлы назначения либо на другой координатор.
- Если на координатор поступают зашифрованные IP-пакеты, предназначенные для туннелируемых узлов, из них извлекаются исходные IP-пакеты, расшифровываются, обрабатываются сетевыми фильтрами и передаются на узлы назначения в открытом виде.



Рисунок 4. Защита соединения на сетевом уровне модели OSI

Чтобы координатор мог осуществлять туннелирование на сетевом уровне, администратор сети ViPNet в программе ViPNet Центр управления сетью (ЦУС) задает максимальное разрешенное число одновременных туннелируемых соединений на данном координаторе. Также в ЦУСе либо на самом координаторе задаются IP-адреса туннелируемых устройств.

Туннелирование на канальном уровне (или технология [L2OverIP](#) (см. глоссарий, стр. 46)) позволяет организовать защищенное соединение между узлами удаленных друг от друга сегментов сети, обеспечивая прямую связь между ними по протоколу Ethernet. С помощью этой технологии можно связывать различные сегменты в единую сеть вне зависимости от того, какие сетевые протоколы будут использоваться в этой сети (IP, IPX, MPLS, IEEE 802.2 и другие). При использовании протокола IP связанные через L2OverIP сегменты образуют единое адресное пространство в пределах одной IP-подсети.

Технология L2OverIP работает следующим образом:

- Координаторы, установленные на границе разных сегментов сети, перехватывают Ethernet-кадры, передаваемые между сегментами.
- Перехваченные Ethernet-кадры на координаторах упаковываются в IP-пакеты специального формата и передаются по защищенному каналу.
- Из полученных IP-пакетов на координаторах извлекаются исходные кадры и передаются узлам сегмента назначения.



Рисунок 5. Защита соединения на канальном уровне модели OSI

Функции туннелирования на канальном уровне не ограничиваются лицензией. Для туннелирования требуется выполнить только ряд специальных настроек на координаторах, установленных на границе удаленных сегментов сети.

## Транспортный сервер

В программе ViPNet Центр управления сетью каждый создаваемый клиент регистрируется на координаторе. Этот координатор является для клиента транспортным сервером. Пользователь сетевого узла не может изменить заданный транспортный сервер на какой-либо другой.

Роль транспортного сервера в сети ViPNet состоит в доставке на сетевые узлы управляющих сообщений, обновлений справочников и ключей и программного обеспечения из программы ViPNet Центр управления сетью, а также обмен прикладными транспортными конвертами между узлами.

Маршрутизация прикладных и управляющих конвертов осуществляется с помощью транспортного модуля ViPNet MFTP, работающего на прикладном уровне. Транспортный модуль на координаторе принимает конверты от других узлов сети ViPNet и пересылает их на узел назначения.



Рисунок 6. Роль транспортного сервера в сети ViPNet

При поступлении прикладного или управляющего конверта транспортный сервер в соответствии с маршрутными таблицами определяет дальнейший путь передачи этого конверта. Если конверт многоадресный, он дробится сервером на соответствующие части. Получив конверт, транспортный сервер выполняет одно из действий, в зависимости от заданных параметров:

- Устанавливает соединение с сетевым узлом (по умолчанию такая логика действует при отправке конверта на другой транспортный сервер).
- Ожидает, когда соединение установит получатель конверта (по умолчанию эта логика действует при наличии конвертов для клиентов).

Кроме того, можно задать период опроса других узлов независимо от наличия для них конвертов. При разрывах соединений передача информации всегда продолжается с точки разрыва, что особенно важно на коммутируемых каналах.

## Межсетевой экран

Координатор выполняет фильтрацию IP-пакетов на каждом сетевом интерфейсе по адресам, протоколам и портам в соответствии с настроенными сетевыми фильтрами. С помощью сетевых фильтров можно не только заблокировать нежелательные соединения, но и разрешить соединения с открытыми узлами, не входящими в сеть ViPNet.

Помимо настраиваемых фильтров в программе имеется система защиты от одной из распространенных сетевых атак — спуфинга.



Рисунок 7. Роль межсетевого экрана в сети ViPNet

Координатор также может осуществлять трансляцию сетевых адресов (NAT) для проходящего через него открытого трафика (см. глоссарий, стр. 51).



**Примечание.** Трансляция адресов для защищенного трафика осуществляется автоматически (см. [Маршрутизатор VPN-пакетов](#) на стр. 16).

---

Функция NAT для открытого трафика позволяет задать правила трансляции адресов для решения двух основных задач:

- Для подключения локальной сети к Интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг Интернета количество публичных IP-адресов. Таким образом, NAT позволяет компьютерам с локальными адресами получать доступ к Интернету от имени публичного адреса координатора.

Для решения этой задачи используется трансляция адреса источника.

- Для организации доступа к локальным ресурсам из внешней сети. В результате применения технологии NAT узлы локальной сети, имеющие частные адреса, могут быть доступны пользователям Интернета по публичным IP-адресам.

Для решения этой задачи используется трансляция адреса назначения.

Подробнее о настройке сетевых фильтров и использовании NAT для открытого трафика см. в документе «ViPNet Coordinator KB. Настройка с помощью командного интерпретатора».

Подробнее о настройках параметров узлов сети в случае, когда ViPNet Coordinator KB, установленный в сети ViPNet, выполняет функцию межсетевого экрана и в этой сети есть другой координатор, к которому подключены клиенты см. в документе «ViPNet Coordinator KB. Настройка с помощью командного интерпретатора» в разделе «Особенности использования ViPNet Coordinator KB в качестве межсетевого экрана».

# Лицензирование ViPNet Coordinator KB

Лицензирование ViPNet Coordinator KB осуществляется с помощью назначения сетевому узлу соответствующей роли в программе ViPNet Центр управления сетью (ЦУС). В таблице ниже приведены допустимые роли для различных исполнений ViPNet Coordinator KB. Соответствие исполнения назначенной роли проверяется при установке на ViPNet Coordinator KB справочников и ключей.

Таблица 4. Исполнения ViPNet Coordinator KB и их аппаратные платформы

Исполнение ViPNet Coordinator KB	Аппаратные платформы	Название роли
ViPNet Coordinator KB100	KB100 N1	Coordinator KB100
ViPNet Coordinator KB1000	KB1000 Q6	Coordinator KB1000
ViPNet Coordinator KB2000	KB2000 Q4	Coordinator KB2000
ViPNet Coordinator KB5000	KB5000 Q1	Coordinator KB5000

Роль может накладывать ограничения на использование ViPNet Coordinator KB в кластере горячего резервирования. В таблице ниже приведены ограничения, накладываемые ролями.

Таблица 5. Лицензионные ограничения, накладываемые ролями

Название роли	Использование в кластере горячего резервирования
Coordinator KB100	Нет
Coordinator KB1000	Да
Coordinator KB2000	Да
Coordinator KB5000	Да



**Внимание!** Для совместной работы в кластере вы можете использовать только одинаковые исполнения и аппаратные платформы ViPNet Coordinator KB.

# Количество связей ViPNet Coordinator KB с ViPNet-узлами

В таблице ниже указано максимальное количество сетевых узлов, с которыми ViPNet Coordinator KB может быть связан, в зависимости от исполнения. Приведенные значения были получены в результате тестирования в следующих условиях:

- максимальное количество связей сетевого узла ViPNet Coordinator KB с другими ViPNet-узлами, в том числе зарегистрированными за другими координаторами;
- максимальное количество связей сетевого узла ViPNet Coordinator KB с туннелирующими координаторами (координаторами с одним заданным диапазоном туннелируемых IP-адресов);
- максимальное количество заданных диапазонов туннелируемых IP-адресов.

Превышение указанного количества связей может привести к снижению производительности ViPNet Coordinator KB.

Таблица 6. Максимальное количество ViPNet-клиентов, связанных с ViPNet Coordinator KB

Исполнение	Максимальное количество связей с ViPNet-узлами	Максимальное количество связей с туннелирующими координаторами	Максимальное количество заданных диапазонов туннелируемых узлов
ViPNet Coordinator KB100	400	40	800
ViPNet Coordinator KB1000	8000	800	800
ViPNet Coordinator KB2000	12000	4000	800
ViPNet Coordinator KB5000	12000	4000	800



# Режимы подключения ViPNet Coordinator KB к внешней сети

## Coordinator KB к внешней сети

Для ViPNet Coordinator KB вы можете настроить один из следующих режимов подключения к внешней сети:

- Подключение без использования внешнего межсетевого экрана (на стр. 26).
- Подключение через межсетевой экран со статической трансляцией адресов (на стр. 25).
- Подключение через межсетевой экран с динамической трансляцией адресов (на стр. 26).

Подробное описание настройки каждого из режимов приведено в документе «ViPNet Coordinator KB. Настройка с помощью командного интерпретатора».

## Подключение через межсетевой экран со статической трансляцией адресов

Если на границе локальной сети установлен межсетевой экран, выполняющий трансляцию сетевых адресов (NAT) и позволяющий настроить статические правила трансляции, между этим межсетевым экраном и узлами локальной сети следует установить координатор. На координаторе в этом случае должны быть настроены параметры подключения через межсетевой экран со статической трансляцией адресов. Для клиентов локальной сети данный координатор следует использовать в качестве сервера соединений.



Рисунок 8. Подключение координатора через межсетевой экран со статической трансляцией адресов

## Подключение через межсетевой экран с динамической трансляцией адресов

Если на границе локальной сети установлен межсетевой экран, выполняющий трансляцию сетевых адресов (NAT), и на нем затруднительно настроить статические правила трансляции, то для защиты IP-трафика локальной сети, в том числе и при инициативных соединениях снаружи, на координаторе можно настроить подключение через межсетевой экран с динамической трансляцией адресов.

Для координатора с данным типом подключения должен существовать постоянно доступный ViPNet-координатор, расположенный во внешней сети, который будет являться [сервером соединений](#) (см. глоссарий, стр. 50).



Рисунок 9. Подключение координатора через межсетевой экран с динамической трансляцией адресов

Сервер соединений должен быть доступен из внешней сети по публичному IP-адресу. Через него будет устанавливаться соединение между координатором локальной сети и удаленными узлами до тех пор, пока не будет установлено соединение напрямую.

## Подключение без использования внешнего межсетевого экрана

Подключение без использования межсетевого экрана следует настраивать на координаторе в том случае, если ни один из его сетевых интерфейсов не находится за устройством NAT, то есть когда координатор доступен из маршрутизируемой сети. Если координатор должен быть доступен для других узлов, находящихся во внешних сетях, то один из его интерфейсов должен иметь публичный IP-адрес.



Рисунок 10. Подключение координатора без использования межсетевого экрана

# Обработка сетевого трафика в соответствии с его приоритетом

В ViPNet Coordinator KB реализована поддержка протокола классификации сетевого трафика [DiffServ](#) (см. глоссарий, стр. 46). Использование этого протокола предполагает, что в заголовок каждого IP-пакета может быть добавлена [DSCP-метка](#) (см. глоссарий, стр. 46), задающая приоритет обработки пакета.

Когда на ViPNet Coordinator KB поступают IP-пакеты с DSCP-метками, по значению метки определяется принадлежность каждого IP-пакета к одному из 8 классов приоритета. IP-пакеты, принадлежащие к классу с более высоким приоритетом, всегда обрабатываются раньше пакетов, принадлежащих к менее приоритетным классам.

ViPNet Coordinator KB поддерживает следующие политики обработки трафика с учетом приоритета в соответствии с RFC 2474 (<https://tools.ietf.org/html/rfc2474>) и RFC 2475 (<https://tools.ietf.org/html/rfc2475>):

- Assured Forwarding — гарантированная переадресация.
- Class Selector — политика, обеспечивающая обратную совместимость с полем IP Precedence.
- Default PHB (Best Effort) — негарантированная доставка.

ViPNet Coordinator KB гарантирует обработку трафика в соответствии с его приоритетом в том случае, если на сетевом оборудовании (например, коммутаторе), подключенном к ViPNet Coordinator KB, поддерживается эта функция, а также включено управление потоком передачи данных (Ethernet Flow Control).



**Примечание.** Если количество поступающего трафика более чем на 20% превышает пропускную способность ViPNet Coordinator KB, обработка трафика с заданным приоритетом не гарантируется.

---

# Назначение и принципы работы системы защиты от сбоев

Система защиты от сбоев предназначена для контроля работоспособности ViPNet Coordinator KB и создания отказоустойчивого решения на базе узлов ViPNet Coordinator KB. Данная система может работать в одиночном режиме (см. [Работа системы защиты от сбоев в одиночном режиме](#) на стр. 29) или в режиме кластера горячего резервирования (см. [Работа системы защиты от сбоев в режиме кластера горячего резервирования](#) на стр. 29).

Настройка системы защиты от сбоев выполняется путем редактирования конфигурационного файла `failover.ini`. Подробнее о параметрах, содержащихся в этом файле см. в документе «ViPNet Coordinator KB. Справочник команд и конфигурационных файлов».

## Работа системы защиты от сбоев в одиночном режиме

По умолчанию в ViPNet Coordinator KB система защиты от сбоев работает в одиночном режиме. При этом данная система обеспечивает постоянную работоспособность ViPNet Coordinator KB, выполняя следующие функции:

- контроль собственной работоспособности;
- контроль работоспособности демонов и драйверов ViPNet Coordinator KB, ведение статистики использования системных ресурсов;
- контроль сбоев при обработке пакетов драйвером ViPNet.

## Работа системы защиты от сбоев в режиме кластера горячего резервирования

Помимо контроля работоспособности ViPNet Coordinator KB (см. [Работа системы защиты от сбоев в одиночном режиме](#) на стр. 29), в режиме кластера горячего резервирования система защиты от сбоев позволяет передавать функции вышедшего из строя сервера другому (резервному) серверу. Кластер горячего резервирования состоит из двух взаимосвязанных ViPNet Coordinator KB:

- активного сервера — который работает в активном режиме и выполняет функции координатора ViPNet;
- пассивного сервера — который работает в пассивном режиме, то есть в режиме ожидания.

В случае сбоев, критичных для работоспособности ViPNet Coordinator KB на активном сервере, пассивный сервер переключается в активный режим и выполняет функции сбойного сервера, который после перезагрузки переходит в пассивный режим.

При работе в режиме кластера горячего резервирования недоступна служба DHCP-сервера ViPNet Coordinator KB. Перед переключением в режим кластера горячего резервирования необходимо остановить DHCP-сервер.

# 2

## Описание исполнений ViPNet Coordinator KB

Исполнение ViPNet Coordinator KB100	32
Исполнение ViPNet Coordinator KB1000	34
Исполнение ViPNet Coordinator KB2000	36
Исполнение ViPNet Coordinator KB5000	38

# Исполнение ViPNet Coordinator KB100

Исполнение ViPNet Coordinator KB100 имеет компактные габаритные размеры и небольшой вес, поэтому использование данного исполнения особенно оправдано в местах, где физическое пространство ограничено. Исполнение может быть использовано для защиты филиалов компаний и небольших удаленных офисов.

В исполнении ViPNet Coordinator KB100 в качестве аппаратной платформы применяется KB100 N1, которое представляет собой мини-компьютер с низким уровнем тепловыделения и энергопотребления и с пассивным охлаждением (без вентилятора охлаждения), производимое компанией Lanner.

## Аппаратная платформа KB100 N1

Аппаратная платформа KB100 N1, имеет следующие технические характеристики:

Таблица 7. Характеристики KB100 N1

Характеристика	Описание
Форм-фактор	Компьютер Lanner LEC-6032-IT3
Размеры (ШxВxГ)	170,0x138,0x41,5 мм
Масса	0,5 кг (без адаптера переменного тока)
Питание	Внешний блок питания, 220 В
Источник постоянного тока	24 В; 2,5 А
Датчик вскрытия корпуса	Есть
Кнопка экстренного стирания ключевой информации	Есть
Процессор	Intel Celeron N2807
Оперативная память	2 Гбайт
Накопители	SSD 8 Гбайт HDD 500 Гбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с 1 порт Ethernet SFP 1 Гбит/с



Характеристика	Описание
Порты ввода-вывода	1 порт VGA
	1 порт USB 2.0
	1 порт USB 3.0

На твердотельном накопителе (SSD) установлено ПО ViPNet Coordinator KB, функционирующее под управлением адаптированной ОС на базе ядра Linux.

Все коммуникационные разъемы расположены на задней панели аппаратной платформы.

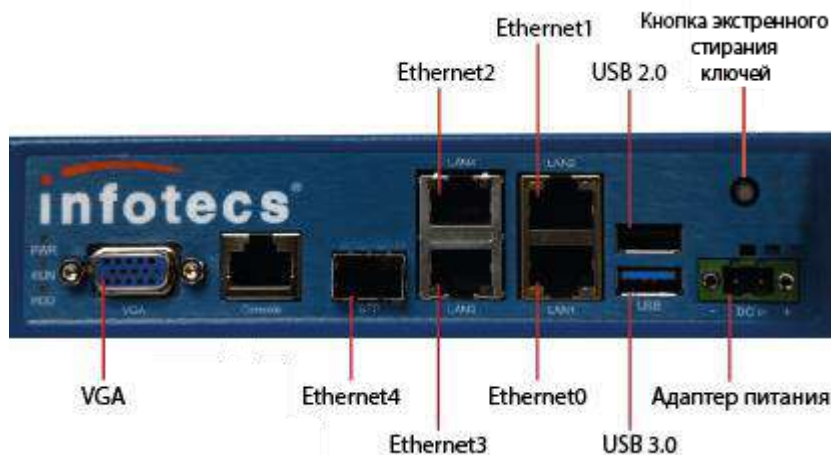


Рисунок 11. Задняя панель KB100 N1

Аппаратная платформа KB100 N1 имеет однопортовый сетевой адаптер SFP (порт Ethernet 4), с которым совместим SFP-трансивер модели AFBR 5710PZ производства Avago Technologies.

# Исполнение ViPNet Coordinator KB1000

Исполнение ViPNet Coordinator KB1000 устанавливается в телекоммуникационную стойку 19" и может быть использовано для защиты компьютерных сетей масштаба предприятия.

В исполнении ViPNet Coordinator KB1000 в качестве аппаратной платформы применяется KB1000 Q6, которая представляет собой сервер AquaServer серии T41 производства ГК «Аквариус».

## Аппаратная платформа KB1000 Q6

Аппаратная платформа KB1000 Q6 имеет следующие технические характеристики:

Таблица 8. Характеристики KB1000 Q6

Характеристика	Описание
Форм-фактор	Сервер AquaServer T41 S24 19" Rack 1U
Размеры (ШхВхГ)	430,0х43,4х380,0 мм
Масса	7,2 кг
Питание	Встроенный блок питания мощностью 250 Вт, напряжением от 100 до 240 В
Потребляемая мощность	150 Вт
Источник постоянного тока	Отсутствует
Датчик вскрытия корпуса	Есть
Кнопка экстренного стирания ключевой информации	Есть
Процессор	Intel Core i3-4360
Оперативная память	2 Гбайт
Накопители	SSD объемом 2 Гбайт HDD объемом 500 Гбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с 2 порта Intel Ethernet SFP 1 Гбит/с
Порты ввода-вывода	2 порта VGA PS/2-порт для подключения клавиатуры или мыши

Характеристика	Описание
	4 порта USB 2.0
	2 порта USB 3.0

На твердотельном накопителе (SSD) установлено ПО ViPNet Coordinator KB, функционирующее под управлением адаптированной ОС на базе ядра Linux.

На передней панели KB1000 Q6 расположены 2 разъема USB 2.0 и порт VGA.



Рисунок 12. Передняя панель KB1000 Q6

Остальные коммуникационные разъемы находятся на задней панели.

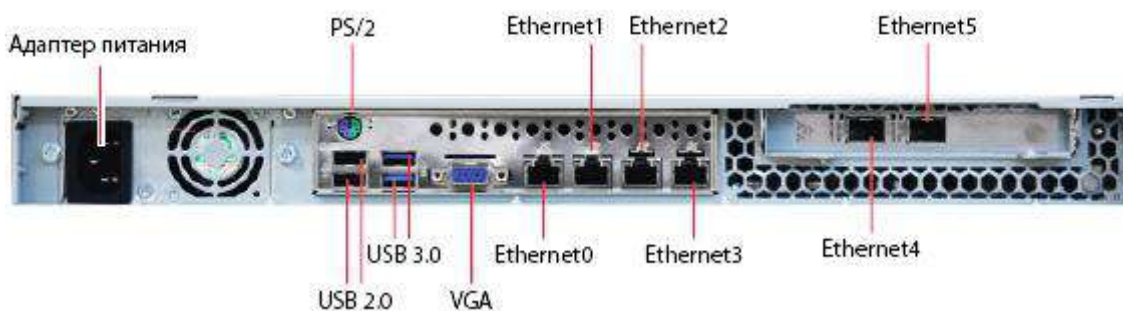


Рисунок 13. Задняя панель KB1000 Q6

Аппаратная платформа KB1000 Q6 имеет двухпортовый сетевой адаптер (порты Ethernet 4 и Ethernet 5), с которым совместим SFP-трансивер модели Avago AFBR 5710PZ.

# Исполнение ViPNet Coordinator KB2000

Исполнение ViPNet Coordinator KB2000 устанавливается в телекоммуникационную стойку 19". Благодаря использованию серверов с процессорами Intel Xeon и высокоскоростных сетевых интерфейсов, исполнение ViPNet Coordinator KB2000 может быть использовано для защиты магистральных каналов связи, организации защищенного доступа к ЦОД (центр обработки данных) и к ресурсам облачных вычислений.



**Примечание.** Исполнение ViPNet Coordinator KB2000 имеет укороченный корпус.

Исполнение ViPNet Coordinator KB2000 распространяется на аппаратной платформе KB2000 Q4, которая представляют собой сервер AquaServer серии T51 производства ГК «Аквариус» и имеет двухпортовые сетевые адаптеры Intel Ethernet SPF+, с которыми может быть использован SFP-трансивер AFBR-709SMZ/SFBR-709SMZ производства Avago Technologies.

## Аппаратная платформа KB2000 Q4

Аппаратная платформа KB2000 Q4 имеет следующие технические характеристики:

Таблица 9. Характеристики KB2000 Q4

Характеристика	Описание
Форм-фактор	Сервер AquaServer T51 D14 — 1U (в укороченном корпусе)
Размеры (ШхВхГ)	444x44x383 мм
Масса	13 кг
Питание	Встроенный блок питания мощностью 500 Вт, напряжением от 100 до 120 В, либо от 200 до 240 В
Потребляемая мощность	310 Вт
Источник постоянного тока	Отсутствует
Датчик вскрытия корпуса	Есть
Кнопка экстренного стирания ключевой информации	Есть
Процессор	Intel Xeon E5-2609v3 (2 шт.)
Оперативная память	4 Гбайт

Характеристика	Описание
Накопители	SSD объемом 2 Гбайт HDD объемом 1 Тбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с 4 порта Intel Ethernet SFP+ 10 Гбит/с
Порты ввода-вывода	VGA PS/2-порт для подключения клавиатуры или мыши 2 порта USB 3.0

На твердотельном накопителе (SSD) установлено ПО ViPNet Coordinator KB, функционирующее под управлением адаптированной ОС на базе ядра Linux.

Коммуникационные разъемы находятся на передней панели:

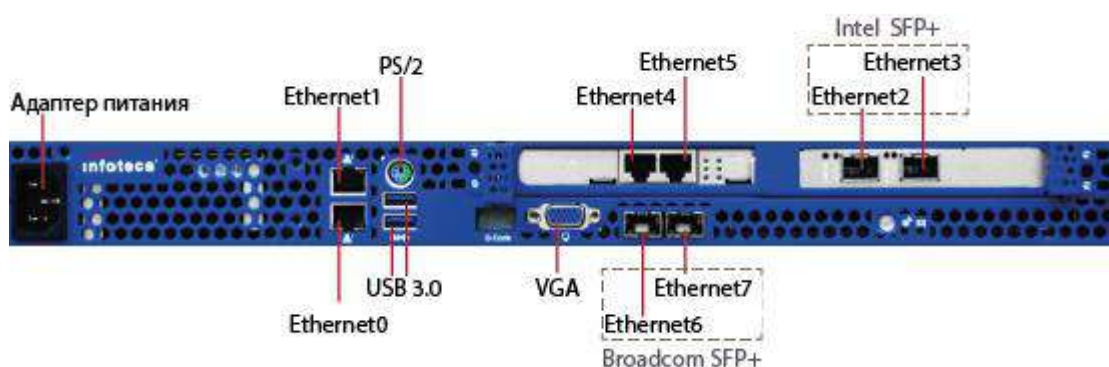


Рисунок 14. Передняя панель ViPNet Coordinator KB2000 Q4

Аппаратная платформа KB2000 Q4 имеет четыре сетевых интерфейса (порты Ethernet 2, Ethernet 3, Ethernet 6 и Ethernet 7), с которыми совместим SFP+-трансивер модели Avago AFBR 709SMZ.

На задней панели аппаратной платформы расположена кнопка экстренного стирания ключевой информации.



Рисунок 15. Задняя панель ViPNet Coordinator KB2000 Q1

# Исполнение ViPNet Coordinator KB5000

Исполнение ViPNet Coordinator KB5000 устанавливается в телекоммуникационную стойку 19". Благодаря использованию серверов с процессорами Intel Xeon и высокоскоростных сетевых интерфейсов, исполнение ViPNet Coordinator KB5000 может быть использовано для защиты магистральных каналов связи, организации защищенного доступа к ЦОД (центр обработки данных) и к ресурсам облачных вычислений.



**Примечание.** Исполнение ViPNet Coordinator KB5000 имеет укороченный корпус.

В исполнении ViPNet Coordinator KB5000 в качестве аппаратной платформы применяется KB5000 Q1, которая представляет собой сервер AquaServer серии T51 D15 производства ГК «Аквариус» и имеет двухпортовые сетевые адаптеры Intel Ethernet SPF+, с которыми может быть использован SFP-трансивер AFBR-709SMZ/SFBR-709SMZ производства Avago Technologies.

## Аппаратная платформа KB5000 Q1

Аппаратная платформа KB5000 Q1 имеет следующие технические характеристики:

Таблица 10. Характеристики KB5000 Q1

Характеристика	Описание
Форм-фактор	Сервер AquaServer T51 D15— 1U (в укороченном корпусе)
Размеры (ШхВхГ)	444x44x383 мм
Масса	13 кг
Питание	Встроенный блок питания мощностью 500 Вт, напряжением от 100 до 120 В, либо от 200 до 240 В
Потребляемая мощность	310 Вт
Источник постоянного тока	Отсутствует
Датчик вскрытия корпуса	Есть
Кнопка экстренного стирания ключевой информации	Есть
Процессор	Intel Xeon E5-2620v3 (2 шт.)
Оперативная память	8 Гбайт

Характеристика	Описание
Накопители	SSD объемом 2 Гбайт HDD объемом 1 Тбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с 4 порта Intel Ethernet SFP+ 10 Гбит/с
Порты ввода-вывода	VGA PS/2-порт для подключения клавиатуры или мыши 2 порта USB 3.0

На твердотельном накопителе (SSD) установлено ПО ViPNet Coordinator KB, функционирующее под управлением адаптированной ОС на базе ядра Linux.

Коммуникационные разъемы находятся на передней панели:

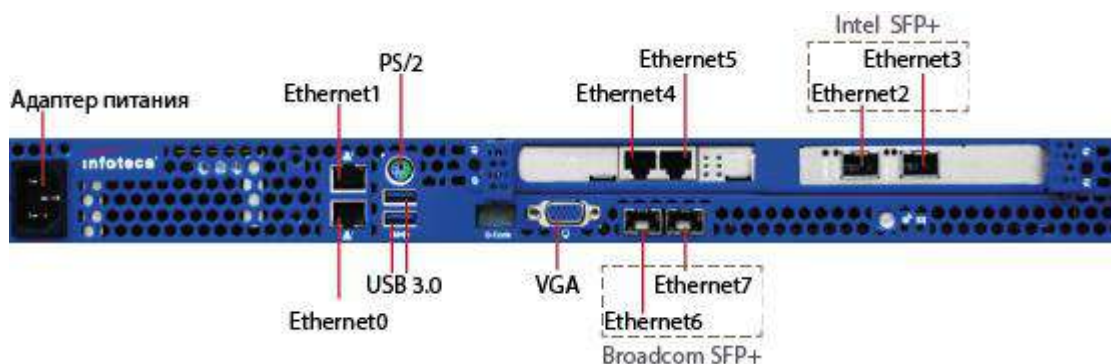


Рисунок 16. Передняя панель ViPNet Coordinator KB5000 Q1

Аппаратная платформа KB5000 Q1 имеет четыре сетевых интерфейса (порты Ethernet 2, Ethernet 3, Ethernet 6 и Ethernet 7), с которым совместим SFP+-трансивер модели Avago AFBR 709SMZ.

На задней панели аппаратной платформы расположена кнопка экстренного стирания ключевой информации.



Рисунок 17. Задняя панель ViPNet Coordinator KB5000 Q1

# 3

## Возможности управления ViPNet Coordinator KB

Способы управления ViPNet Coordinator KB	41
Назначение командного интерпретатора	42
Режимы работы в командном интерпретаторе	43
Аутентификация пользователя	44
Экстренное стирание ключевой информации	45



# Способы управления ViPNet Coordinator KB

Для настройки параметров ViPNet Coordinator KB вы можете использовать следующие средства:

- Административное программное обеспечение ViPNet — программы [ViPNet Центр управления сетью \(ЦУС\)](#) (см. глоссарий, стр. 47) и [ViPNet Policy Manager](#) (см. глоссарий, стр. 47).

Выполнение настройки ViPNet Coordinator KB в ЦУСе облегчает управление и позволяет оповестить об изменении параметров сетевые узлы ViPNet, связанные с ViPNet Coordinator KB, путем отправки на эти узлы справочников и ключей. Программа ViPNet Policy Manager позволяет централизованно управлять встроенными сетевыми экранами узлов, в том числе координаторов ViPNet Coordinator KB.

- Командный интерпретатор ViPNet Coordinator KB.

Вы можете использовать командную оболочку ViPNet. Командный интерпретатор предоставляет наиболее полные возможности по администрированию ViPNet Coordinator KB.

# Назначение командного интерпретатора

С помощью командного интерпретатора ViPNet Coordinator KB вы можете выполнять следующие действия:

- Настройка системных функций ViPNet Coordinator KB: настройка даты и времени, создание копий конфигурации и другое.
- Настройка подключения ViPNet Coordinator KB к сети.
- Настройка режимов подключения ViPNet Coordinator KB к сети через межсетевой экран.
- Управление межсетевым экраном путем настройки сетевых фильтров и правил трансляции адресов.
- Управление обработкой прикладных протоколов.
- Настройка VPN: настройка видимости узлов, туннелирования адресов и другие.
- Настройка защиты соединения по технологии L2OverIP.
- Настройка транспортного модуля: выбор канала передачи конвертов между узлами, настройка протоколирования событий транспортного модуля и другое.
- Настройка сетевых служб: встроенного DHCP-, DNS- и NTP-сервера.
- Настройка статической и динамической маршрутизации.
- Настройка системы защиты от сбоев.
- Резервирование справочников, ключей и настроек ViPNet Coordinator KB.
- Просмотр журналов регистрации IP-пакетов, транспортных конвертов, устранения неполадок.
- Настройка параметров удаленного мониторинга по протоколу SNMP и другое.
- Настройка взаимодействия ViPNet Coordinator KB с источником бесперебойного питания.

Командный интерпретатор ViPNet Coordinator KB запускается автоматически после аутентификации пользователя.

# Режимы работы в командном интерпретаторе

Вы можете работать с командным интерпретатором ViPNet Coordinator KB в одном из двух режимов:

- Режим наблюдения. Данный режим становится активным по умолчанию после [аутентификации на ViPNet Coordinator KB](#) (на стр. 44). При работе с командным интерпретатором в данном режиме пользователю недоступно изменение настроек ViPNet Coordinator KB. В командном интерпретаторе в качестве приглашения командной строки в этом режиме используется символ >.
- Режим управления. В этом режиме в командном интерпретаторе доступны все настройки. В командном интерпретаторе в качестве приглашения командной строки в этом режиме используется символ #. Чтобы перейти в режим управления, в командном интерпретаторе требуется выполнить авторизацию с использованием пароля администратора.

# Аутентификация пользователя

Прежде чем начать работу с ViPNet Coordinator KB, требуется пройти аутентификацию.

Для аутентификации пользователя необходимо подключить к ViPNet Coordinator KB [токен](#) (см. глоссарий, стр. 51) и ввести [ПИН-код](#) (см. глоссарий, стр. 49). После этого командный интерпретатор ViPNet Coordinator KB перейдет в режим наблюдения.

Для того чтобы перейти в режим управления, необходимо выполнить команду `enable` и ввести [пароль администратора ViPNet Coordinator KB](#) (см. глоссарий, стр. 49).

# Экстренное стирание ключевой информации

При необходимости в процессе эксплуатации вы можете удалить ключевую информацию ViPNet Coordinator KB, для этого необходимо нажать на кнопку экстренного стирания ключей. После нажатия кнопки будут удалены все ключи и справочники, установленные в ViPNet Coordinator KB. После удаления ключевой информации потребуется повторно провести процедуру ввода ViPNet Coordinator KB в эксплуатацию. Подробное описание процедуры ввода в эксплуатацию изложено в документе «ViPNet Coordinator KB. Настройка с помощью командного интерпретатора».

# А

## Глоссарий

### DHCP (Dynamic Host Configuration Protocol)

Сетевой протокол прикладного уровня, позволяющий компьютерам автоматически получать IP-адреса и другие параметры, необходимые для работы в сети TCP/IP. К таким параметрам относятся маска подсети, IP-адрес шлюза, IP-адреса серверов DNS, IP-адреса серверов WINS.

### DiffServ (Differentiated Service)

Протокол, обеспечивающий классификацию сетевого трафика при помощи [DSCP-меток](#) (см. глоссарий, стр. 46), добавляемых в заголовки IP-пакетов.

### DSCP-метка

Информация о приоритете обработки IP-пакета, указанная в заголовке IP-пакета.

### L2OverIP

Технология, которая позволяет организовать защиту удаленных сегментов сети, использующих одно и то же адресное пространство, на канальном уровне модели OSI. В результате узлы из разных сегментов смогут взаимодействовать друг с другом так, как будто они находятся в одном сегменте с прямой видимостью по MAC-адресам. В основе технологии лежит перехват на канальном уровне модели OSI Ethernet-кадров, отправленных из одного сегмента сети в другой.

### MIME-тип

Тип данных, которые могут быть переданы с помощью Интернета с применением стандарта MIME.

## OSPF (Open Shortest Path First)

Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала для нахождения кратчайшего маршрута. Распространяет информацию о доступных маршрутах внутри автономной системы.

## ViPNet Administrator

Набор программного обеспечения для администрирования сети ViPNet, включающий в себя серверное и клиентское приложения ViPNet Центр управления сетью, а также программу ViPNet Удостоверяющий и ключевой центр.

## ViPNet Policy Manager

Программа, которая входит в состав программного комплекса ViPNet. Предназначена для централизованного управления политиками безопасности узлов защищенной сети ViPNet.

## ViPNet Центр управления сетью (ЦУС)

ViPNet Центр управления сетью — это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

## Администратор сети ViPNet

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

## Виртуальная защищенная сеть

Технология, позволяющая создать логическую сеть, чтобы обеспечить множественные сетевые соединения между компьютерами или локальными сетями через существующую физическую сеть. Уровень доверия к такой виртуальной сети не зависит от уровня доверия к физическим сетям благодаря использованию средств криптографии (шифрования, аутентификации и средств персонального и межсетевого экранирования).

## Дистрибутив ключей

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

## ДНСД (датчик несанкционированного доступа)

Электротехническое устройство, встраиваемое в устройство, несанкционированный доступ внутрь корпуса которого требуется контролировать. Обработка события несанкционированного доступа может обрабатываться независимо как самим датчиком, так промежуточным или самим контролируемым устройством с информированием администратора безопасности контролируемого устройства.

## Кластер горячего резервирования

Кластер горячего резервирования состоит из двух взаимосвязанных ПАК ViPNet Coordinator KB, один из которых (активный) выполняет функции координатора сети ViPNet, а другой (пассивный) находится в режиме ожидания.

В случае сбоя, критичных для работоспособности ViPNet Coordinator KB, выполняющего функции координатора сети ViPNet, второй ПАК, находившийся в режиме ожидания берет на себя выполнение функций координатора сети ViPNet (становится активным). При этом сбойный ПАК перезагружается и становится в режим ожидания (становится пассивным).

## Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. Клиент должен быть зарегистрирован на координаторе. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

## Ключевой блокнот ДСДР

Ключевой блокнот ДСДР предназначен для средств криптографической защиты данных, не содержащих сведений, составляющих государственную тайну. Ключевой блокнот ДСДР содержит ключевую информацию, которая используется для шифрования конфиденциальной информации.

## Координатор (ViPNet-координатор)

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



## Маршрутизация

Процесс выбора пути для передачи информации в сети.

## Межсетевой экран

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

## Обычная консоль

Монитор и клавиатура, которые используются для локальной настройки ViPNet Coordinator KB.

## Пароль ViPNet Coordinator KB

Пароль для включения режима управления ViPNet Coordinator KB. Первоначально создается администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр.

## Персональный ключ пользователя

Главный ключ защиты ключей, к которым имеет доступ пользователь. Действующий персональный ключ необходимо хранить в безопасном месте.

## ПИН-код

Код доступа к подключенному токenu, на котором записан персональный ключ пользователя.

## ПК ViPNet StateWatcher

Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher, который предназначен для наблюдения за состоянием узлов сетей ViPNet, мониторинга событий безопасности, происходящих на сетевых узлах, своевременного выявления неполадок в работе узлов и оперативного оповещения пользователей о возникающих проблемах.

## Политика безопасности

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

## Резервный набор персональных ключей (РНПК)

Набор из нескольких запасных персональных ключей, которые администратор УКЦ создает для пользователя. Имя этого файла имеет маску `AAAA.pk`, где `AAAA` — идентификатор пользователя ViPNet в рамках своей сети. Используется для удаленного обновления ключей пользователя при их компрометации и при смене мастер-ключа персональных ключей.

## Роль

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

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

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

## Сервер IP-адресов

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

## Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента можно выбрать свой сервер соединений. По умолчанию сервер соединений для клиента также является сервером IP-адресов.

## Сетевой узел ViPNet

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

## Сеть ViPNet

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

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

## Симметричный ключ

Последовательность битов заданной длины (для алгоритма ГОСТ 28147-89 — 256 бит), используемая как для зашифрования, так и для расшифрования информации.

В программном обеспечении ViPNet симметричные ключи используются для зашифрования и расшифрования IP-трафика, информации приложений (в том числе почтовой), служебных и прикладных конвертов.

## Токен

Компактное устройство аутентификации, предназначенное для обеспечения информационной безопасности пользователя.

## Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, используемые в одной сети, в адреса и порты, используемые в другой.

## Транспортный конверт

Зашифрованная информация служб или приложений, доставляемая на сетевые узлы ViPNet транспортным модулем ViPNet MFTP.

## Транспортный модуль (MFTP)

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

## Транспортный сервер

Функциональность координатора, обеспечивающая маршрутизацию транспортных конвертов между узлами сети ViPNet.

## Туннелирование

Технология, позволяющая защитить соединения между узлами локальных сетей, которые обмениваются информацией через Интернет или другие публичные сети, путем инкапсуляции и шифрования трафика этих узлов не самими узлами, а координаторами, которые установлены на границе их локальных сетей. При этом установка программного обеспечения ViPNet на эти узлы необязательна, то есть туннелируемые узлы могут быть как защищенными, так и открытыми.