ViPNet Coordinator HW 4

Подготовка к работе

infotecs

ФРКЕ.00130-03 90 02

Версия продукта 4.3.2; документ обновлен 11.02.2022

АО «ИнфоТеКС»

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

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

Веб-сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

В документе описывается назначение и применение программно-аппаратного комплекса ViPNet Coordinator HW® (далее — ViPNet Coordinator HW) в составе защищенных сетей ViPNet, способы настройки и управления, приводится описание существующих исполнений ViPNet Coordinator HW, их аппаратных платформ и условий лицензирования. Также в документе описан порядок действий по подготовке ViPNet Coordinator HW к использованию, основные сценарии работы со справочниками и ключами узла.

Для кого предназначен документ

Документ предназначен для администраторов ViPNet Coordinator HW.

Соглашения документа

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

Таблица 1. Обозначения, используемые в примечаниях

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

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.

Обозначение	Описание
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

При описании команд в данном документе используются следующие условные обозначения:

- Команды, которые могут быть выполнены только в режиме администратора, содержат приглашение с символом «#». Например:

  ```
  hostname# admin config list
  ```

- Команды, которые могут быть выполнены в режиме и пользователя, и администратора, содержат приглашение с символом «>». Например:

  ```
  hostname> alg restart
  ```

- При описании в документе параметры, которые должны быть заданы пользователем, заключены в угловые скобки «<>»:

  ```
  inet bonding delete <номер>
  ```

  При вводе в командный интерпретатор параметры, которые должны быть заданы пользователем, вводятся без угловых скобок:

  ```
  hostname# inet bonding delete 1
  ```

- При описании в документе необязательные параметры или ключевые слова заключены в квадратные скобки «[]». Например:

  ```
  firewall <тип> add name @<имя> <состав> [exclude <исключения>]
  ```

  При вводе в командный интерпретатор необязательные параметры или ключевые слова вводятся без квадратных скобок. Например:

  ```
  hostname# firewall interface-object add name @intgroup interface eth0 interface eth1
  ```

- Если при вводе команды можно указать один из нескольких параметров, при описании в документе допустимые варианты заключены в фигурные скобки «{}» и разделены вертикальной чертой «|». Например:

  ```
  inet ntp mode {on | off}
  ```

  Если при вводе команды можно указать один из нескольких параметров, то при вводе в командный интерпретатор выбранные варианты параметров вводятся без фигурных скобок. Например:

  ```
  hostname# inet ntp mode off
  ```

Связанные документы

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

Таблица 3. Связанные документы

Документ и его назначение	Содержание
«ViPNet Coordinator HW. Настройка с помощью командного интерпретатора». В документе описаны основные сценарии настройки ViPNet Coordinator HW с помощью командного интерпретатора, а также работа с журналами ViPNet Coordinator HW.	Настройка даты и времени Настройка подключения к сети (настройка сетевых интерфейсов Ethernet, дополнительных IP-адресов (алиасов), виртуальных сетевых интерфейсов VLAN, агрегированных сетевых интерфейсов, настройка подключения к сети 3G или Wi-Fi, использование динамических интерфейсов) Настройка сервисных функций (DHCP-, DNS-, NTP-сервер, прокси-сервер, функциональность L2OverIP) Настройка подключения ViPNet Coordinator HW 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 Организация обеспечения электропитания от UPS Настройка протоколирования событий и просмотр журналов (системный журнал, журнал IP-пакетов) Обновление ПО ViPNet Coordinator HW, в том числе на кластере горячего резервирования Резервное копирование и восстановление настроек
«ViPNet Coordinator HW. Настройка с помощью веб-интерфейса». В документе описана настройка ViPNet Coordinator HW с помощью веб-интерфейса. Документ предназначен для администраторов и пользователей, которые планируют работать с ViPNet Coordinator HW, используя веб-интерфейс.	Настройка даты и времени Настройка подключения к сети (настройка сетевых интерфейсов Ethernet, дополнительных IP-адресов (алиасов), виртуальных сетевых интерфейсов VLAN, агрегированных сетевых интерфейсов, настройка подключения к сети 3G или Wi-Fi) Настройка статической и динамической маршрутизации Настройка сервисных функций (DHCP-, DNS-, NTP-сервер, прокси-сервер, функциональность L2OverIP) Настройка сетевых фильтров Настройка трансляции IP-адресов Работа со списком защищенных узлов, связанных с ViPNet Coordinator HW Мониторинг состояния ViPNet Coordinator HW и просмотр журнала IP-пакетов

Документ и его назначение	Содержание
«ViPNet Coordinator HW. Справочное руководство по командному интерпретатору и конфигурационным файлам».	Описание команд ViPNet Coordinator HW Описание конфигурационных файлов управляющего демона и системы защиты от сбоев
«ViPNet Coordinator HW. Лицензионные соглашения на компоненты сторонних производителей»	Лицензионные соглашения на компоненты сторонних производителей, которые использовались при разработке ПО для ViPNet Coordinator HW
«ViPNet Coordinator HW. История версий»	Информация об изменениях в предыдущих версиях ViPNet Coordinator HW

Комплект поставки

В комплект поставки ViPNet Coordinator HW входят следующие компоненты:

- В зависимости от исполнения (см. Описание исполнений ViPNet Coordinator HW на стр. 29):
  - в случае исполнений ViPNet Coordinator HW — программно-аппаратный комплекс ViPNet Coordinator HW.
- Файл обновления в формате LZH, необходимый для обновления ПО ViPNet Coordinator HW с более ранней версии на текущую.
- Документация в формате PDF:
  - «ViPNet Coordinator HW. Подготовка к работе».
  - «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».
  - «ViPNet Coordinator HW. Настройка с помощью веб-интерфейса».
  - «ViPNet Coordinator HW. Справочное руководство по командному интерпретатору и конфигурационным файлам».
  - «ViPNet Coordinator HW. Лицензионные соглашения на компоненты сторонних производителей».
  - «ViPNet Coordinator HW. История версий».

Что нового в версии 4.3.2 hotfix 1

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Coordinator HW версии 4.3.2 hotfix 1 по сравнению с версией 4.3.2.

- **Поддержка новых аппаратных платформ**

  Добавлены аппаратные платформы HW1000 Q7, Q8, Q9 (на стр. 40) и HW5000 Q2 (на стр. 47).

- **Повышение производительности и стабильности работы**

  В ПО ViPNet Coordinator HW новой версии повышена производительность и стабильность работы ViPNet Coordinator HW.

- **Исправление ошибок**

  Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий ПО.

Обратная связь

Дополнительная информация

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

- Информация о продуктах ViPNet.
- Информация о решениях ViPNet.
- Часто задаваемые вопросы.
- Форум пользователей продуктов ViPNet.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ИнфоТеКС:

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба поддержки: hotline@infotecs.ru.

  Форма для обращения в службу поддержки через сайт.

  Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

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

1

Общая информация

Назначение ViPNet Coordinator HW

ViPNet Coordinator HW 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 HW приведено в разделе Функции координатора в защищенной сети (на стр. 17).

ViPNet Coordinator HW распространяется в нескольких исполнениях. Каждое исполнение ViPNet Coordinator HW представляет собой интегрированное решение на базе специализированной аппаратной платформы и 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. 107) и накладывающей определенные лицензионные ограничения (см. Лицензирование ViPNet Coordinator HW на стр. 51).

В качестве аппаратной платформы для исполнения ViPNet Coordinator HW используется компактный компьютер или сервер, устанавливаемый в стандартные стойки. Характеристики всех поддерживаемых исполнений приведены в главе Описание исполнений ViPNet Coordinator HW (на стр. 29).

Защищенная сеть ViPNet

ViPNet Coordinator HW предназначен для использования в защищенной сети ViPNet, построенной на основе комплекса продуктов ViPNet.

Сеть ViPNet представляет собой виртуальную защищенную сеть (см. глоссарий, стр. 107), 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 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 (см. глоссарий, стр. 111). Для шифрования трафика используются симметричные ключи, которые создаются и распределяются централизованно.

Для управления защищенной сетью ViPNet предназначено программное обеспечение ViPNet Administrator (см. глоссарий, стр. 107). С помощью ViPNet Administrator создаются сетевые узлы ViPNet и связи между ними, настраиваются параметры отдельных узлов, создаются дистрибутивы ключей (см. глоссарий, стр. 108) для каждого узла, выполняется централизованное обновление справочников, ключей (см. глоссарий, стр. 111) и программного обеспечения на узлах.

Сетевые узлы ViPNet делятся на два типа:

- Клиент (ViPNet-клиент) (см. глоссарий, стр. 108) — рабочее место пользователя сети ViPNet.
- Координатор (ViPNet-координатор) (см. глоссарий, стр. 109) — сервер сети ViPNet. Сетевой узел ViPNet Coordinator HW 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. 112).

Функции координатора в защищенной сети

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

- Сервер IP-адресов (на стр. 17). Обеспечивает взаимодействие защищенных узлов ViPNet (см. глоссарий, стр. 108). Сервер IP-адресов сообщает сетевым узлам информацию об адресах и параметрах доступа других узлов.
- Маршрутизатор VPN-пакетов (на стр. 19). Обеспечивает маршрутизацию транзитного защищенного IP-трафика, проходящего через координатор на другие защищенные узлы.
- Сервер соединений (на стр. 19). Обеспечивает соединение клиентов и координаторов друг с другом кратчайшим путем.
- VPN-шлюз (на стр. 20). 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. 22). Обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений справочников, ключей и программного обеспечения из программы ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 107), а также обмен прикладными транспортными конвертами (см. глоссарий, стр. 112) между узлами.
- Защищенный Интернет-шлюз (на стр. 23). Обеспечивает раздельный доступ защищенных узлов в Интернет и к ресурсам защищенной сети ViPNet, если этого требует политика безопасности организации.

Сервер IP-адресов

При подключении любого клиента с программой ViPNet Client (см. глоссарий, стр. 108) к сети или изменении его параметров подключения эти параметры сообщаются координатору, который играет роль сервера IP-адресов (см. глоссарий, стр. 111) 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, координатор переводит клиент в статус «Недоступен».

Аналогичным образом происходит обмен информацией о параметрах доступа между координаторами. Периодически (по умолчанию — каждые 15 минут) координатор отсылает 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 данный координатор в качестве сервера IP-адресов) координатор 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 координатор считает этот клиент недоступным и рассылает информацию об этом.
- В случае взаимодействия координатора с другой сетью ViPNet на шлюзовой координатор (см. глоссарий, стр. 112) другой сети высылается информация о состоянии всех узлов своей сети, связанных с узлами другой сети ViPNet. При получении такой информации из другой сети ViPNet координатор рассылает эту информации на все координаторы своей сети, а также на свои клиенты, связанные с узлами другой сети.

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 (см. глоссарий, стр. 109) транзитного защищенного трафика, передаваемого на другие защищенные сетевые узлы. Маршрутизация осуществляется как внутри одной сети ViPNet, так и при взаимодействии с другими сетями 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. 112). 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 (см. глоссарий, стр. 111). 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 сервер соединений для клиента служит также сервером IP-адресов (см. Сервер IP-адресов на стр. 17).

Сервер соединений

Координатор может выступать в качестве сервера соединений (см. глоссарий, стр. 111) 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

На сервере соединений можно настроить TCP-туннель, который будет соединять клиентов из внешних сетей с другими узлами ViPNet в том случае, если интернет-провайдер блокирует протокол UDP.

Рисунок 4. Функция TCP-туннеля

Таким образом, когда удаленный клиент не может получить доступ к сети ViPNet по протоколу UDP, он автоматически устанавливает связь через TCP-туннель своего сервера соединений. На сервере полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узлы назначения по UDP-протоколу.

VPN-шлюз

Координаторы в роли VPN-шлюзов защищают соединения между узлами локальных сетей, которые обмениваются информацией через публичные сети. Защита реализуется с помощью технологии туннелирования (см. Туннелирование на стр. 112), 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 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 5. 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. 106)) 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 6. Защита соединения на канальном уровне модели OSI

Функции туннелирования на канальном уровне не ограничиваются лицензией, при этом не поддерживаются исполнениями ViPNet Coordinator HW50 A, B и HW100 A, B. 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 ViPNet управляющих сообщений, обновлений справочников и ключей и программного обеспечения из программы ViPNet Центр управления сетью, а также обмен прикладными транспортными конвертами (см. глоссарий, стр. 112) 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.

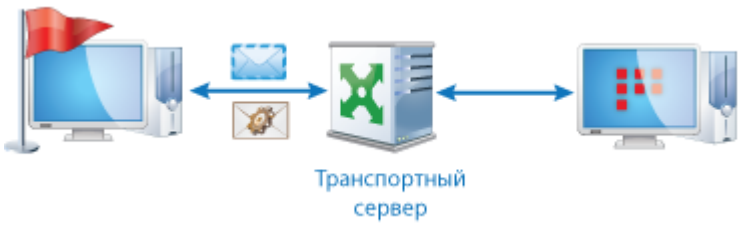

Рисунок 7. Роль транспортного сервера в сети ViPNet

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.

Защищенный Интернет-шлюз

Технология «Открытый Интернет» позволяет разделить доступ защищенных узлов в Интернет и к ресурсам защищенной сети ViPNet. Таким образом обеспечивается доступ в Интернет с максимальным уровнем безопасности, возможным без физического отключения компьютера от корпоративной сети.

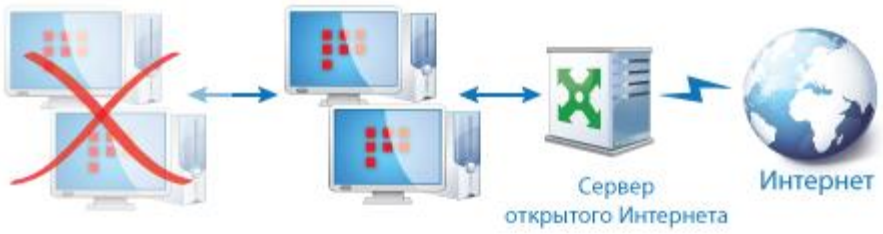

Рисунок 8. Роль сервера открытого Интернета в сети ViPNet

Клиенты, имеющие связь с сервером открытого Интернета, могут работать только в одном из двух режимов:

- Работа в Интернете, при этом ресурсы корпоративной защищенной сети недоступны, хотя компьютер не отключен от сети физически.
- Работа в локальной сети, при этом доступ в Интернет полностью заблокирован, но без физического отключения от внешней сети.

Такое разделение на два непересекающихся режима исключает любые атаки в реальном времени на компьютеры корпоративной сети через компьютеры, имеющие доступ к Интернету.

Чтобы использовать на координаторе технологию «Открытый Интернет», в программе ViPNet Центр управления сетью для этого координатора следует включить функцию сервера открытого Интернета. Подробнее см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».

Функции межсетевого экрана ViPNet Coordinator HW

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 имеется система защиты от одной из распространенных сетевых атак — спуфинга.

Рисунок 9. Роль межсетевого экрана в сети ViPNet

Координатор также может осуществлять трансляцию сетевых адресов (NAT) для проходящего через него открытого трафика (см. глоссарий, стр. 112).

Примечание. Трансляция сетевых адресов для защищенного трафика осуществляется автоматически (см. Маршрутизатор VPN-пакетов на стр. 19).

Функция NAT для открытого трафика позволяет задать правила трансляции сетевых 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 IP-адресами получать доступ к Интернету от имени публичного IP-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 IP-адреса, могут быть доступны пользователям Интернета по публичным IP-адресам.

  Для решения этой задачи используется трансляция адреса назначения.

Подробнее об использовании NAT для открытого трафика см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора» и «ViPNet Coordinator HW. Настройка с помощью веб-интерфейса».

Также межсетевой экран ViPNet Coordinator HW обладает следующими возможностями:

- Обработка протоколов прикладного уровня: FTP, DNS, H.323, SCCP, SIP.
- Поддержка виртуальных локальных сетей (VLAN IEEE 802.1Q).
- Объединение нескольких физических сетевых интерфейсов в один логический — агрегированный интерфейс — для увеличения пропускной способности, повышения надежности, резервирования каналов связи.
- Приоритизация обработки IP-трафика в соответствии с протоколом DiffServ (см. Обработка сетевого трафика в соответствии с его приоритетом на стр. 26).
- Функции DHCP-, DNS- и NTP-сервера.
- Реализация функций прокси-сервера с возможностью фильтрации HTTP-трафика по его содержимому и антивирусной проверки.
- Реализация функций клиента и точки доступа Wi-Fi.
- Функции маршрутизатора IP-пакетов с возможностью настройки статической и динамической маршрутизации.
- Функции кластера горячего резервирования (см. Функции системы защиты от сбоев на стр. 27).
- Взаимодействие с источником бесперебойного питания UPS.
- Совместимость с программным обеспечением для управления и мониторинга: ViPNet Administrator, ViPNet Policy Manager, ViPNet StateWatcher.

Обработка сетевого трафика в соответствии с его приоритетом

В ViPNet Coordinator HW реализована поддержка протокола классификации сетевого трафика DiffServ (см. глоссарий, стр. 105). Использование этого протокола предполагает, что в заголовок каждого IP-пакета может быть добавлена DSCP-метка, задающая приоритет обработки пакета.

Когда на ViPNet Coordinator HW 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.

При этом, при зашифровании и расшифровании (инкапсуляциии и декапсуляции) IP-пакета DSCP-метка перемещается соответственно из закрытой в открытую или из открытой в закрытую часть IP-пакета. Поэтому в случае, когда на ViPNet Coordinator HW приходит открытый IP-пакет с DSCP-меткой, ViPNet Coordinator HW его шифрует и отправляет далее получателю, по пути следования IP-пакета его DSCP-метка может быть снята или изменена и останется такой после расшифрования.

ViPNet Coordinator HW поддерживает следующие политики обработки трафика с учетом приоритета в соответствии с RFC 2474 и RFC 2475:

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

ViPNet Coordinator HW гарантирует обработку трафика в соответствии с его приоритетом в том случае, если на сетевом оборудовании (например, коммутаторе), подключенном к ViPNet Coordinator HW, 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 HW, обработка трафика с заданным приоритетом не гарантируется.

Функции системы защиты от сбоев

Назначение и принципы работы системы защиты от сбоев

Система защиты от сбоев предназначена для контроля работоспособности ПО ViPNet Coordinator HW и создания отказоустойчивого решения на базе узлов ViPNet Coordinator HW. Данная система может работать в одиночном режиме (см. Работа системы защиты от сбоев в одиночном режиме на стр. 27) или в режиме кластера горячего резервирования.

Настройка системы защиты от сбоев выполняется путем редактирования конфигурационного файла `failover.ini`. Подробнее о параметрах, содержащихся в этом файле см. в документе «ViPNet Coordinator HW. Справочное руководство по командному интерпретатору и конфигурационным файлам».

Работа системы защиты от сбоев в одиночном режиме

По умолчанию в ViPNet Coordinator HW система защиты от сбоев работает в одиночном режиме и выполняет следующие функции:

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

Работа системы защиты от сбоев в режиме кластера горячего резервирования

Помимо контроля работоспособности программы ViPNet Coordinator HW (см. Работа системы защиты от сбоев в одиночном режиме на стр. 27), в режиме кластера горячего резервирования система защиты от сбоев позволяет передавать функции вышедшего из строя узла другому (резервному) узлу. Кластер горячего резервирования состоит из двух взаимосвязанных узлов ViPNet Coordinator HW:

- активного узла — который работает в активном режиме и выполняет функции координатора ViPNet (подробнее см. в разделе Функции координатора в защищенной сети (на стр. 17));

- пассивного узла — который работает в пассивном режиме, то есть в режиме ожидания.

В случае сбоев, критичных для работоспособности ViPNet Coordinator HW на активном узле, пассивный узел переключается в активный режим и выполняет функции сбойного узла, который переключается в пассивный режим.

При работе в режиме кластера горячего резервирования некоторые функции ViPNet Coordinator HW недоступны (см. Функции ViPNet Coordinator HW, недоступные в режиме кластера горячего резервирования на стр. 28).

Функции ViPNet Coordinator HW, недоступные в режиме кластера горячего резервирования

В режиме кластера недоступны следующие сетевые службы ViPNet Coordinator HW:

- Wi-Fi.
- 3G-модем.

Перед переключением в режим кластера горячего резервирования необходимо отключить перечисленные функции.

2

Описание исполнений ViPNet Coordinator HW

Исполнения ViPNet Coordinator HW50

Исполнения ViPNet Coordinator HW50 имеют компактные габаритные размеры и небольшой вес, поэтому их использование особенно оправдано в местах, где физическое пространство ограничено. Исполнения могут быть использованы для защиты небольших удаленных офисов и удаленных рабочих мест.

Аппаратные платформы, на которых распространяются исполнения ViPNet Coordinator HW50, приведены в таблице ниже.

Таблица 4. Аппаратные платформы для исполнений ViPNet Coordinator HW50

Исполнение	Аппаратные платформы
ViPNet Coordinator HW50 A	HW50 N1, N2, N3, N4
ViPNet Coordinator HW50 B	HW50 N1, N2, N3, N4

Аппаратные платформы HW50 N1, N2, N3 представляют собой мини-компьютеры NCA-1010A с низким уровнем тепловыделения и энергопотребления, производимые компанией Lanner Electronics Incorporated, и различаются наличием дополнительных расширений:

- HW50 N1 — компьютер NCA-1010A без расширений.
- HW50 N2 — компьютер NCA-1010A с Wi-Fi-адаптером.
- HW50 N3 — компьютер NCA-1010A с 3G-модемом.

Примечание. Размеры платформ указаны без учета навесных элементов и подключенных кабелей. Допуск 5 мм.

Таблица 5. Характеристики HW50 N1, N2, N3 (компьютер Lanner NCA-1010A)

Характеристика	Описание
Форм-фактор	Мини-компьютер
Размеры (ШхВхГ)	125,1x20,3x120 мм
Масса	0,5 кг (без адаптера переменного тока)
Питание	Внешний блок питания, 220 В
Потребляемая мощность	До 36 Вт
Источник постоянного тока	12 В, 3 А
Процессор	Intel Atom E3815 (1 ядро)

Характеристика	Описание
Оперативная память	2 Гбайт
Накопители	SSD 2 Гбайт
Сетевые порты	3 порта Ethernet RJ45 10/100/1000 Мбит/с
3G-модем	Только в аппаратной платформе HW50 N3
Адаптер Wi-Fi	Только в аппаратной платформе HW50 N2
Порты ввода-вывода	1 порт HDMI 1 служебный порт RJ45 1 порт USB 2.0 1 порт USB 3.0

Аппаратная платформа HW50 N4 представляет собой мини-компьютер NCA-1020C с низким уровнем тепловыделения и энергопотребления, производимый компанией Lanner Electronics Incorporated, и поставляется без дополнительных расширений.

Таблица 6. Характеристики HW50 N4 (компьютер Lanner NCA-1020C)

Характеристика	Описание
Форм-фактор	Мини-компьютер
Размеры (ШхВхГ)	137x20x120 мм
Масса	0,5 кг (без адаптера переменного тока)
Питание	Внешний блок питания, 220 В
Потребляемая мощность	До 36 Вт
Источник постоянного тока	12 В, 3 А
Процессор	Intel Celeron N3010 (2 ядра)
Оперативная память	2 Гбайт
Накопители	SSD 2 Гбайт
Сетевые порты	3 порта Ethernet RJ45 10/100/1000 Мбит/с
Порты ввода-вывода	1 порт HDMI 1 служебный порт RJ45 1 порт USB 2.0 1 порт USB 3.0

На передней панели аппаратных платформ HW50 N1, N2, N3, N4 расположен разъем USB 2.0, порт HDMI, а также служебный разъем RJ45, предназначенный для подключения компьютера (ноутбука) при установке справочников и ключей.

Рисунок 10. Передняя панель ViPNet Coordinator HW50

Остальные коммуникационные разъемы находятся на задней панели:

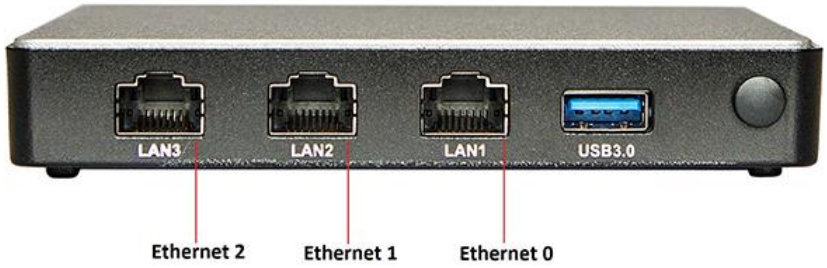

Рисунок 11. Задняя панель ViPNet Coordinator HW50

Примечание. Чтобы вставить SIM-карту оператора связи во встроенный 3G-модем аппаратной платформы HW50 N3, необходимо разобрать корпус мини-компьютера (см. раздел Установка SIM-карты в HW50 N3 и HW100 N3 (на стр. 57)).

Исполнения ViPNet Coordinator HW100

Исполнения ViPNet Coordinator HW100 имеют компактные габаритные размеры и небольшой вес, поэтому их использование особенно оправдано в местах, где физическое пространство ограничено. Исполнения могут быть использованы для защиты филиалов компаний и небольших удаленных офисов.

Аппаратные платформы, на которых распространяются исполнения ViPNet Coordinator HW100, приведены в таблице ниже.

Примечание. Исполнения ViPNet Coordinator HW100 A и ViPNet Coordinator HW100 B распространяются на одних и тех же аппаратных платформах, но имеют различные ограничения на максимальное число туннелируемых соединений на сетевом уровне (см. Лицензирование ViPNet Coordinator HW на стр. 51).

Таблица 7. Аппаратные платформы для исполнений ViPNet Coordinator HW100

Исполнение	Аппаратные платформы	Максимальное число туннелируемых соединений на сетевом уровне
ViPNet Coordinator HW100 A	HW100 X1, X8	2
ViPNet Coordinator HW100 B	HW100 X1, X8	5
ViPNet Coordinator HW100 C	HW100 X2, X3, N1, N2, N3	Задается в ЦУСе

Аппаратные платформы для исполнений ViPNet Coordinator HW100 представляют собой мини-компьютеры с пассивным охлаждением (без вентилятора охлаждения), производимые компаниями Lex Computech и Lanner с низким уровнем тепловыделения и энергопотребления.

Технические характеристики аппаратных платформ для исполнений ViPNet Coordinator HW100 приведены в следующих разделах:

- Аппаратные платформы HW100 X1, X2, X3, X8 (на стр. 34).
- Аппаратные платформы HW100 N1, N2, N3 (на стр. 35).

Примечание. Размеры платформ указаны без учета навесных элементов и подключенных кабелей. Допуск 5 мм.

Аппаратные платформы HW100 X1, X2, X3, X8

Аппаратные платформы HW100 X1, X2, X3, X8 имеют следующие технические характеристики:

Таблица 8. Характеристики HW100 X1, X2, X3, X8

Характеристика	Описание
Модель	Компьютер BK3741S-00C серии BRIK (HW100 X1, X2) Компьютер BK3791S-00C серии BRIK (HW100 X3, X8)
Форм-фактор	Мини-компьютер
Размеры (ШхВхГ)	187x130x50 мм
Масса	1 кг (без адаптера переменного тока)
Питание	Внешний блок питания, 220 В
Потребляемая мощность	До 25 Вт
Источник постоянного тока	12 В, 5 А
Процессор	Intel Atom N270 (HW100 X1, X2) (1 ядро) Intel Atom N2600 (HW100 X3, X8) (2 ядра)
Оперативная память	От 1 Гбайт (HW100 X1, X2) От 2 Гбайт (HW100 X3, X8)
Накопители	SSD от 1 Гбайт (HW100 X1, X2) SSD от 2 Гбайт (HW100 X3, X8) HDD от 80 Гбайт (HW100 X2, X3)
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с
Порты ввода-вывода	VGA 2 порта USB 2.0 COM-порт RS-232 (только в аппаратных платформах HW100 X3, X8)

Все коммуникационные разъемы расположены на задней панели компьютера. На конкретном устройстве расположение разъемов может немного отличаться от представленного на рисунке ниже.

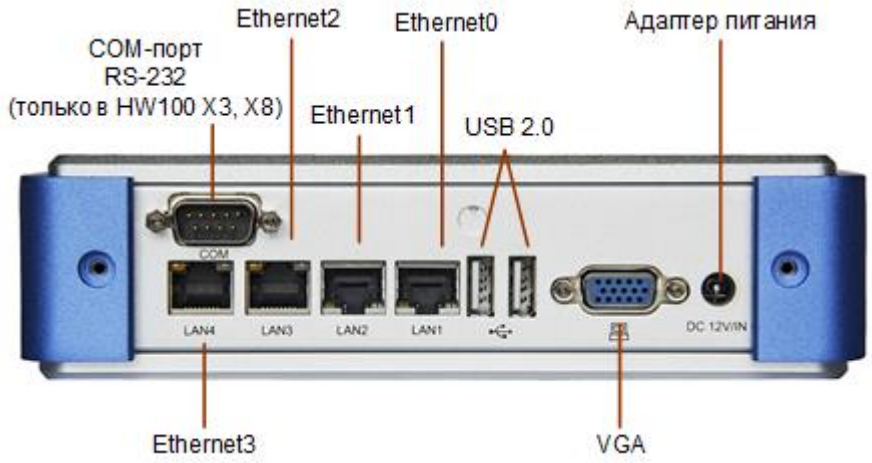

Рисунок 12. Задняя панель HW100 X1, X2, X3, X8

Аппаратные платформы HW100 N1, N2, N3

Аппаратные платформы HW100 N1, N2, N3 различаются наличием дополнительных расширений:

- HW100 N1 — компьютер Lanner LEC-6032-IT2 без расширений.
- HW100 N2 — компьютер Lanner LEC-6032-IT2 с Wi-Fi-адаптером.
- HW100 N3 — компьютер Lanner LEC-6032-IT2 с 3G-модемом.

Аппаратные платформы HW100 N1, N2, N3 имеют следующие технические характеристики:

Таблица 9. Характеристики HW100 N1, N2, N3 (компьютер Lanner LEC-6032-IT2)

Характеристика	Описание
Форм-фактор	Мини-компьютер
Размеры (ШхВхГ)	173,8x43,7x138,5 мм
Масса	0,5 кг (без адаптера переменного тока)
Питание	Внешний блок питания, 220 В
Источник постоянного тока	24 В, 2,5 А
Процессор	Intel Celeron N2807 (2 ядра)
Оперативная память	От 2 Гбайт
Накопители	SSD от 2 Гбайт HDD от 80 Гбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с 1 порт Ethernet SFP 1 Гбит/с
3G-модем	Только в аппаратной платформе HW100 N3

Характеристика	Описание
Адаптер Wi-Fi	Только в аппаратной платформе HW100 N2
Порты ввода-вывода	1 порт VGA 1 служебный порт RJ45 1 порт USB 2.0 1 порт USB 3.0

Все коммуникационные разъемы расположены на задней панели компьютера. На конкретном устройстве расположение разъемов может немного отличаться от представленного на рисунке ниже.

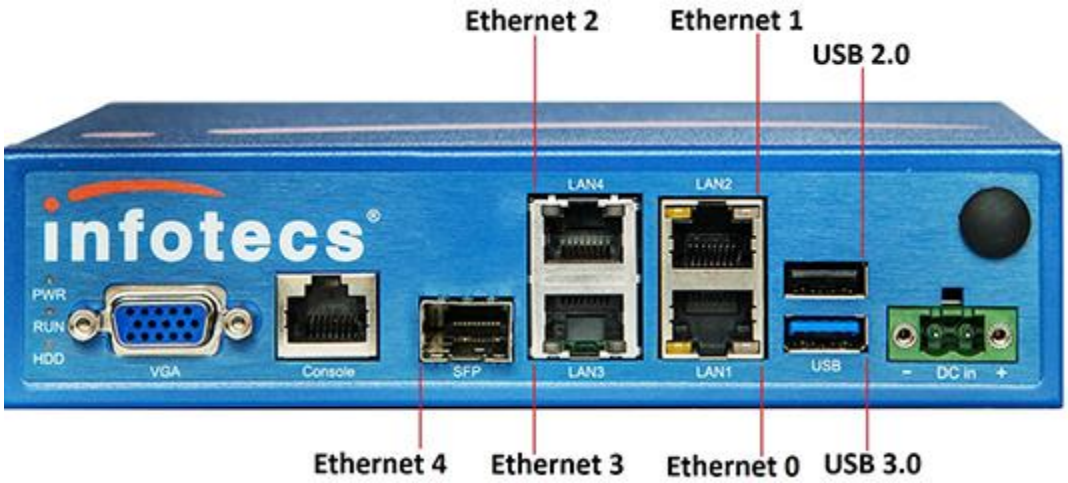

Рисунок 13. Задняя панель HW100 N1, N2, N3

Примечание. Чтобы вставить SIM-карту оператора связи во встроенный 3G-модем аппаратной платформы HW100 N3, необходимо разобрать корпус мини-компьютера (см. раздел Установка SIM-карты в HW50 N3 и HW100 N3 (на стр. 57)).

Исполнение ViPNet Coordinator HW1000

Исполнения ViPNet Coordinator HW1000 устанавливаются в телекоммуникационную стойку 19″ и могут быть использованы для защиты компьютерных сетей масштаба предприятия.

Таблица 10. Аппаратные платформы для исполнений ViPNet Coordinator HW1000

Исполнение	Аппаратные платформы
ViPNet Coordinator HW1000	HW1000 Q2, Q3, Q4, Q7
ViPNet Coordinator HW1000 C	HW1000 Q5, Q8
ViPNet Coordinator HW1000 D	HW1000 Q6, Q9

Аппаратные платформы для исполнений ViPNet Coordinator HW1000 представляют собой серверы Аквариус серии T40 и T41 производства ГК «Аквариус».

Технические характеристики аппаратных платформ приведены в разделах:

- Аппаратные платформы HW1000 Q2, Q3 (на стр. 37).
- Аппаратные платформы HW1000 Q4, Q5, Q6 (на стр. 38).
- Аппаратные платформы HW1000 Q7, Q8, Q9 (на стр. 40).

Примечание. Размеры платформ указаны без учета навесных элементов и подключенных кабелей. Допуск 5 мм.

Аппаратные платформы HW1000 Q2, Q3

Аппаратные платформы HW1000 Q2 и Q3 имеют следующие технические характеристики:

Таблица 11. Характеристики HW1000 Q2, Q3 (сервер Аквариус T40 S44)

Характеристика	Описание
Форм-фактор	19″ Rack 1U
Размеры (ШхВхГ)	430x44x380 мм
Масса	6,5 кг
Питание	Встроенный блок питания мощностью 220 Вт, 110–220 В
Потребляемая мощность	До 155 Вт

Характеристика	Описание
Источник постоянного тока	Отсутствует
Процессор	Intel Core i3-530 (HW1000 Q2) (2 ядра) Intel Core i5-750 (HW1000 Q3) (4 ядра)
Оперативная память	От 2 Гбайт
Накопители	SSD от 2 Гбайт HDD от 240 Гбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с
Порты ввода-вывода	VGA PS/2-совместимая клавиатура, PS/2-совместимая мышь COM-порт RS-232 4 порта USB 2.0 1 порт IPMI

На передней панели HW1000 Q2, Q3 расположены 2 разъема USB 2.0, остальные коммуникационные разъемы находятся на задней панели.

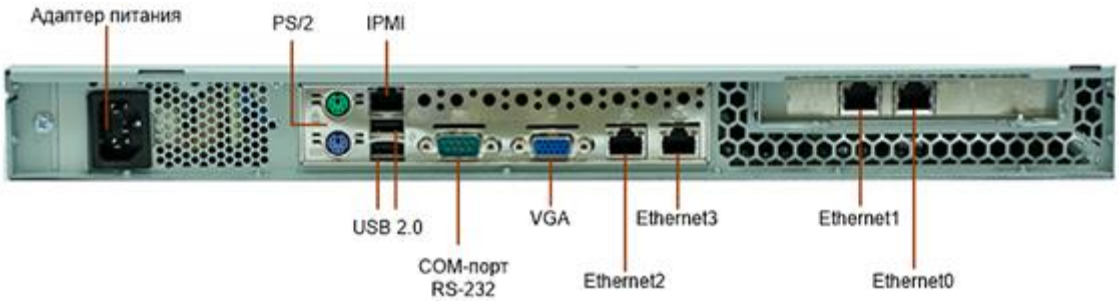

Рисунок 14. Задняя панель ViPNet Coordinator HW1000 Q2/Q3

Аппаратные платформы HW1000 Q4, Q5, Q6

Аппаратные платформы HW1000 Q4, Q5, Q6 имеют следующие технические характеристики:

Таблица 12. Характеристики HW1000 Q4, Q5, Q6 (сервер Аквариус T41 S24)

Характеристика	Описание
Форм-фактор	19” Rack 1U
Размеры (ШхВхГ)	430x44x380 мм
Масса	7,2 кг
Питание	Встроенный блок питания мощностью 250 Вт, 100–240 В

Характеристика	Описание
Потребляемая мощность	150 Вт
Источник постоянного тока	Отсутствует
Процессор	HW1000 Q4: Intel Celeron G1820 (2 ядра) HW1000 Q5, Q6: Intel Core i3-4360 (2 ядра)
Оперативная память	От 2 Гбайт
Накопители	SSD от 2 Гбайт HDD от 500 Гбайт
Сетевые порты	HW1000 Q4: 4 порта Ethernet RJ45 10/100/1000 Мбит/с HW1000 Q5: 6 портов Ethernet RJ45 10/100/1000 Мбит/с HW1000 Q6: 4 порта Ethernet RJ45 10/100/1000 Мбит/с 2 порта Intel Ethernet SFP 1 Гбит/с
Порты ввода-вывода	2 порта VGA 1 порт PS/2 для подключения клавиатуры или мыши COM-порт RS-232 4 порта USB 2.0 2 порта USB 3.0

На передней панели HW1000 Q4, Q5, Q6 расположены COM-порт, 2 разъема USB 2.0 и порт VGA.

Рисунок 15. Передняя панель HW1000 Q4, Q5, Q6

Остальные коммуникационные разъемы находятся на задней панели.

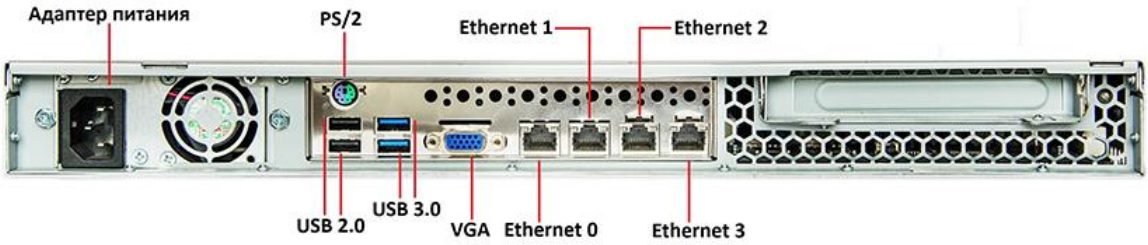

Рисунок 16. Задняя панель HW1000 Q4

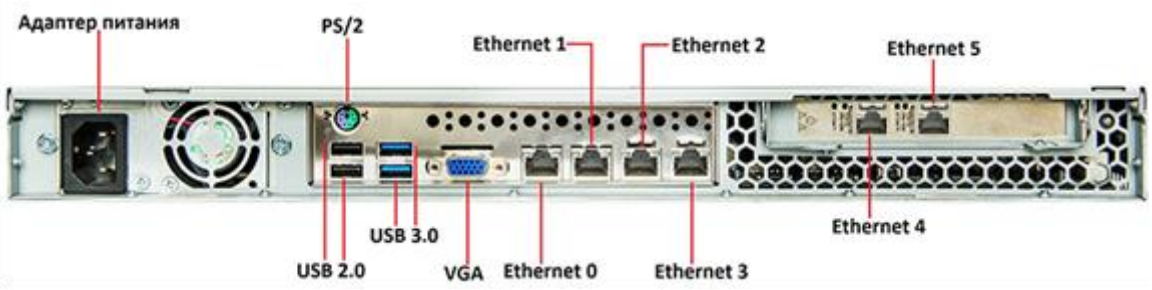

Рисунок 17. Задняя панель HW1000 Q5

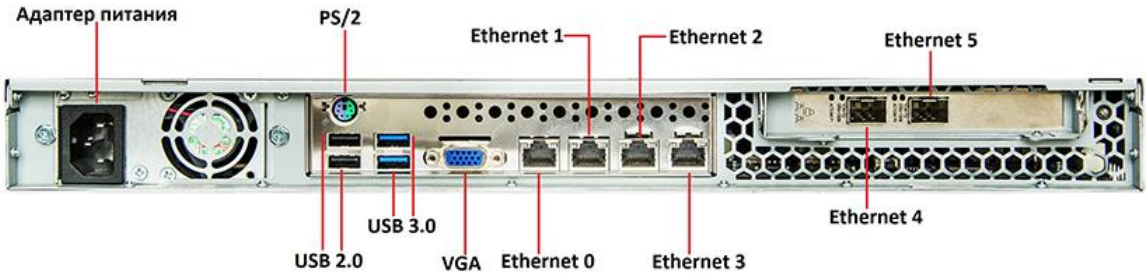

Рисунок 18. Задняя панель HW1000 Q6

Аппаратные платформы HW1000 Q7, Q8, Q9

Аппаратные платформы HW1000 Q7, Q8, Q9 имеют следующие технические характеристики:

Таблица 13. Характеристики HW1000 Q7, Q8, Q9 (сервер Аквариус T41 S102DF-V R51, R52, R53)

Характеристика	Описание
Форм-фактор	19" Rack 1U
Размеры (ШхВхГ)	430x44x434 мм
Масса	HW1000 Q7, Q8: 6,8 кг HW1000 Q9: 7,8 кг

Характеристика	Описание
Питание	HW1000 Q7, Q8: 1 блок питания мощностью 250 Вт, 100–240 В HW1000 Q9: 2 блока питания мощностью 300 Вт, 100–240 В
Потребляемая мощность	HW1000 Q7, Q8: 130 Вт HW1000 Q9: 160 Вт
Процессор	HW1000 Q7: Intel Celeron G4900 (2 ядра) HW1000 Q8, Q9: Intel Core i3-8100 (4 ядра)
Оперативная память	HW1000 Q7: 4 Гбайт HW1000 Q8, Q9: 16 Гбайт
Накопители	SSD 4 Гбайт HDD 1 Тбайт
Сетевые порты	HW1000 Q7: 6 портов Ethernet RJ45 10/100/1000 Мбит/с HW1000 Q8: 8 портов Ethernet RJ45 10/100/1000 Мбит/с HW1000 Q9: 8 портов Ethernet RJ45 10/100/1000 Мбит/с 4 порта Intel Ethernet SFP 1 Гбит/с
Порты ввода-вывода	порт VGA COM-порт RS-232 6 портов USB 3.1

На передней панели HW1000 Q7 и HW1000 Q8 расположены: сетевые порты Ethernet, разъемы PS/2, USB 3.1, COM-порт RS-232 и порт VGA.

Рисунок 19. Передняя панель HW1000 Q7

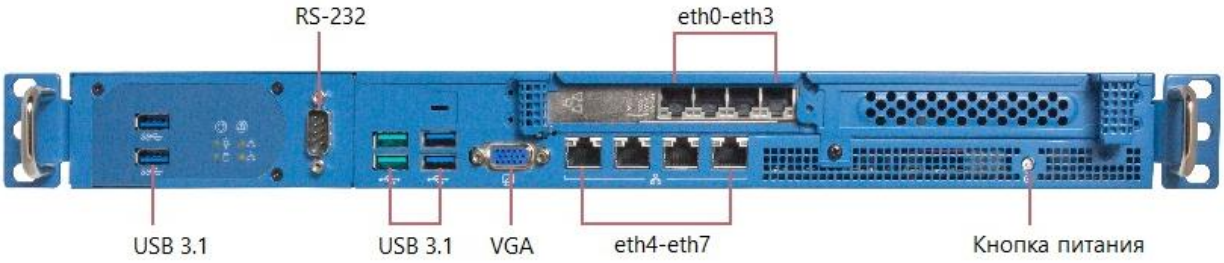

Рисунок 20. Передняя панель HW1000 Q8

На задней панели HW1000 Q7, Q8 находится разъем адаптера питания.

Рисунок 21: Задняя панель HW1000 Q7, Q8

На передней панели HW1000 Q9 расположены: сетевые порты Ethernet и Ethernet SFP, разъемы PS/2, USB 3.1, COM-порт RS-232 и порт VGA.

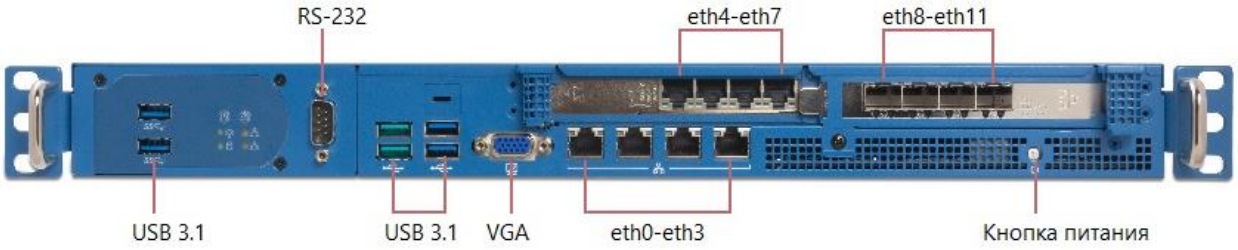

Рисунок 22. Передняя панель HW1000 Q9

На задней панели HW1000 Q9 расположены разъемы адаптеров питания.

Рисунок 23. Задняя панель HW1000 Q9

Исполнение ViPNet Coordinator HW2000

Исполнение ViPNet Coordinator HW2000 устанавливается в телекоммуникационную стойку 19”. Благодаря использованию серверов с процессорами Intel Xeon и высокоскоростных сетевых интерфейсов, исполнение ViPNet Coordinator HW2000 может быть использовано для защиты магистральных каналов связи, организации защищенного доступа в ЦОДы (центры обработки данных) и к ресурсам облачных вычислений.

Примечание. Исполнение ViPNet Coordinator HW2000 на аппаратной платформе HW2000 Q4 имеет укороченный корпус.

Исполнение ViPNet Coordinator HW2000 распространяется на аппаратных платформах HW2000 Q2, HW2000 Q3 и HW2000 Q4.

Аппаратные платформы для исполнений ViPNet Coordinator HW2000 представляют собой серверы Аквариус серии T50 производства ГК «Аквариус».

Технические характеристики аппаратных платформ для исполнения ViPNet Coordinator HW2000 приведены в следующих разделах:

- Аппаратная платформа HW2000 Q2 (на стр. 43).
- Аппаратная платформа HW2000 Q3 (на стр. 45).
- Аппаратная платформа HW2000 Q4 (на стр. 46).

Примечание. Размеры платформ указаны без учета навесных элементов и подключенных кабелей. Допуск 5 мм.

Аппаратная платформа HW2000 Q2

Аппаратная платформа HW2000 Q2 имеет следующие технические характеристики:

Таблица 14. Характеристики HW2000 Q2 (сервер Аквариус T50 D57)

Характеристика	Описание
Форм-фактор	19” Rack 1U
Размеры (ШхВхГ)	444x44x614 мм
Масса	15 кг

Характеристика	Описание
Питание	Встроенный блок питания мощностью 600 Вт, 100–240 В
Потребляемая мощность	470 Вт
Источник постоянного тока	Отсутствует
Процессор	2 процессора Intel Xeon E5645 (6 ядер каждый)
Оперативная память	От 4 Гбайт
Накопители	SSD от 2 Гбайт HDD от 480 Гбайт
Сетевые порты	2 порта Ethernet RJ45 10/100/1000 Мбит/с 4 порта Ethernet SFP+ 10 Гбит/с
Порты ввода-вывода	VGA PS/2-совместимая клавиатура, PS/2-совместимая мышь COM-порт RS-232 4 порта USB 2.0 1 порт IPMI

На передней панели HW2000 Q2 расположены 2 разъема USB 2.0:

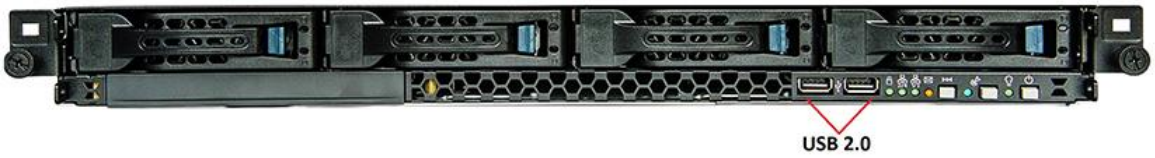

Рисунок 24. Передняя панель ViPNet Coordinator HW2000 Q2, Q3

Остальные коммуникационные разъемы находятся на задней панели:

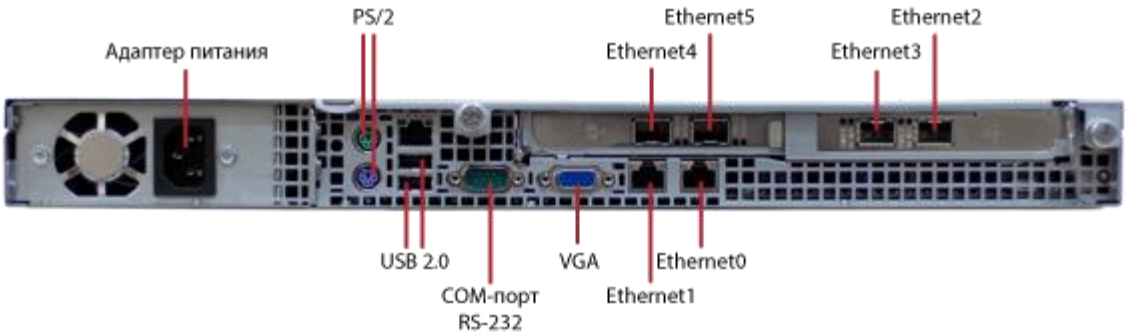

Рисунок 25. Задняя панель ViPNet Coordinator HW2000 Q2

Аппаратная платформа HW2000 Q3

Аппаратная платформа HW2000 Q3 имеет следующие технические характеристики:

Таблица 15. Характеристики HW2000 Q3 (сервер Аквариус T50 D14)

Характеристика	Описание
Форм-фактор	19" Rack 1U
Размеры (ШхВхГ)	444x44x614 мм
Масса	15 кг
Питание	Встроенный блок питания мощностью 600 Вт, 100–240 В
Потребляемая мощность	До 440 Вт
Источник постоянного тока	Отсутствует
Процессор	2 процессора Intel Xeon E5-2620 v2 (6 ядер каждый)
Оперативная память	От 8 Гбайт
Накопители	SSD от 2 Гбайт HDD от 1000 Гбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с 4 порта Ethernet SFP+ 10 Гбит/с
Порты ввода-вывода	VGA PS/2-совместимая клавиатура, PS/2-совместимая мышь COM-порт RS-232 4 порта USB 2.0

Аналогично аппаратной платформе HW2000 Q2 (см. рисунок на стр. 44), на передней панели HW2000 Q3 расположены 2 разъема USB.

Остальные коммуникационные разъемы находятся на задней панели:

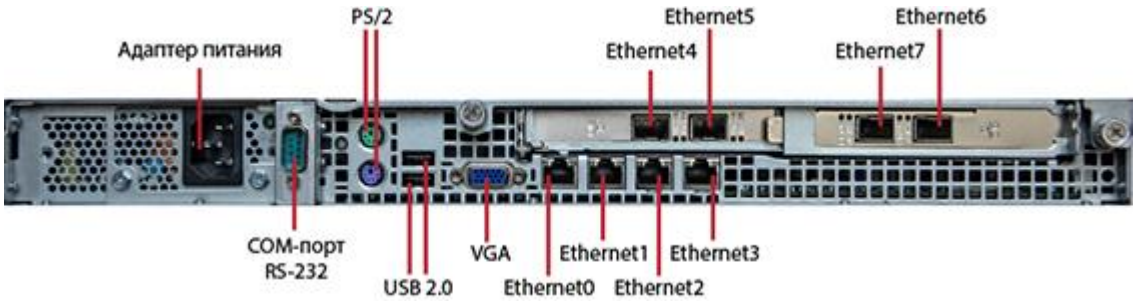

Рисунок 26. Задняя панель ViPNet Coordinator HW2000 Q3

Аппаратная платформа HW2000 Q4

Аппаратная платформа HW2000 Q4 имеет следующие технические характеристики:

Таблица 16. Характеристики HW2000 Q4 (сервер Аквариус T51 D14)

Характеристика	Описание
Форм-фактор	1U в укороченном корпусе
Размеры (ШхВхГ)	444x44x380 мм
Масса	8 кг
Питание	Встроенный блок питания мощностью 500 Вт, 100-127 В/200-240 В
Потребляемая мощность	310 Вт
Источник постоянного тока	Отсутствует
Процессор	2 процессора Intel Xeon E5-2609v3 (6 ядер каждый)
Оперативная память	От 4 Гбайт
Накопители	SSD от 2 Гбайт HDD от 500 Гбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с 2 порта Intel Ethernet SFP+ 10 Гбит/с 2 порта Broadcom Ethernet SFP+ 10 Гбит/с
Порты ввода-вывода	VGA PS/2-порт для подключения клавиатуры или мыши COM-порт RS-232 2 порта USB 3.0

На задней панели HW2000 Q4 расположен COM-порт RS-232.

Остальные коммуникационные разъемы находятся на передней панели:

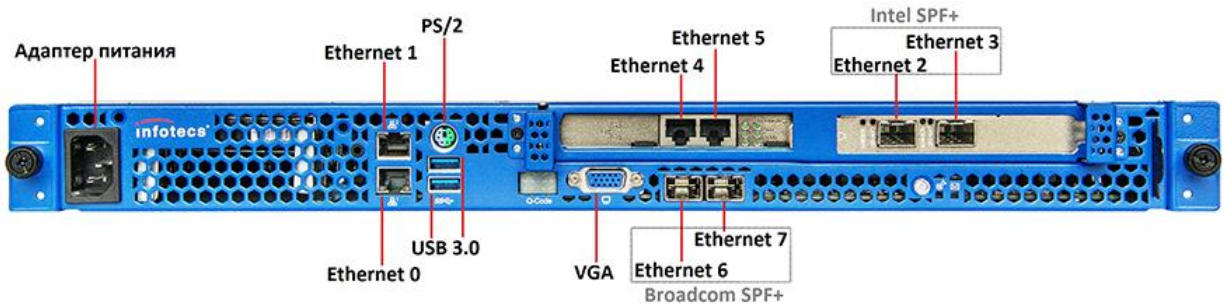

Рисунок 27. Передняя панель ViPNet Coordinator HW2000 Q4

Исполнение ViPNet Coordinator HW5000

Исполнение ViPNet Coordinator HW5000 устанавливается в телекоммуникационную стойку 19" и имеет укороченный корпус. Поскольку сервер оснащен процессором Intel Xeon и высокоскоростными сетевыми интерфейсами, исполнение ViPNet Coordinator HW5000 подходит для защиты магистральных каналов связи, организации защищенного доступа в центры обработки данных (ЦОДы) и к ресурсам облачных вычислений в ограниченном пространстве телекоммуникационных стоек.

Исполнение ViPNet Coordinator HW5000 распространяется на аппаратных платформах HW5000 Q1 и HW5000 Q2 производства «Аквариус».

Примечание. Размеры платформ указаны без учета навесных элементов и подключенных кабелей. Допуск 5 мм.

Аппаратная платформа HW5000 Q1

Таблица 17. Характеристики HW5000 Q1 (сервер Аквариус T51 D15)

Характеристика	Описание
Форм-фактор	19" Rack 1U в укороченном корпусе
Размеры (ШхВхГ)	444x44x380 мм
Масса	8 кг
Питание	Встроенный блок питания мощностью 500 Вт, 100-127 В/200-240 В
Потребляемая мощность	310 Вт
Источник постоянного тока	Отсутствует
Процессор	2 процессора Intel Xeon E5-2620v3 (6 ядер каждый)
Оперативная память	8 Гбайт
Накопители	SSD 2 Гбайт, HDD 500 Гбайт
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с 2 порта Intel Ethernet SFP+ 10 Гбит/с 2 порта Broadcom Ethernet SFP+ 10 Гбит/с

Характеристика	Описание
Порты ввода-вывода	VGA PS/2-порт для подключения клавиатуры или мыши COM-порт RS-232 2 порта USB 3.0

На передней панели HW5000 Q1 находятся: сетевые порты Ethernet и Ethernet SFP+, дублирующий разъем адаптера питания, разъемы PS/2, USB 3.0 и VGA.

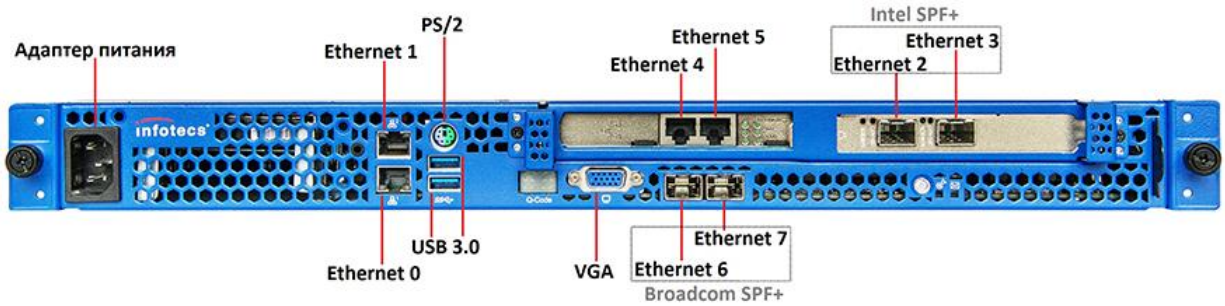

Рисунок 28. Передняя панель HW5000 Q1

На задней панели HW5000 Q1 расположены COM-порт RS-232 и разъем адаптера питания.

Рисунок 29. Задняя панель HW5000 Q1

Аппаратная платформа HW5000 Q2

Таблица 18. Характеристики HW5000 Q2 (сервер Аквариус T41 S102DF-V R55)

Характеристика	Описание
Форм-фактор	19” Rack 1U в укороченном корпусе
Размеры (ШхВхГ)	444x44x380 мм
Масса	7,9 кг
Питание	2 блока питания мощностью 300 Вт (каждый)
Потребляемая мощность	130 Вт
Источник постоянного тока	Отсутствует
Процессор	процессор Intel Xeon E-2278GE (8 ядер)
Оперативная память	64 Гбайт
Накопители	SSD 4 Гбайт, HDD 2 Тбайт

Характеристика	Описание
Сетевые порты	4 порта Ethernet RJ45 10/100/1000 Мбит/с 8 портов Intel Ethernet SFP+ 10 Гбит/с
Порты ввода-вывода	порт VGA COM-порт RS-232 6 портов USB 3.1

На передней панели HW5000 Q2 находятся: сетевые порты Ethernet и Ethernet SFP+, разъемы PS/2, USB 3.1, COM-порт RS-232 и порт VGA.

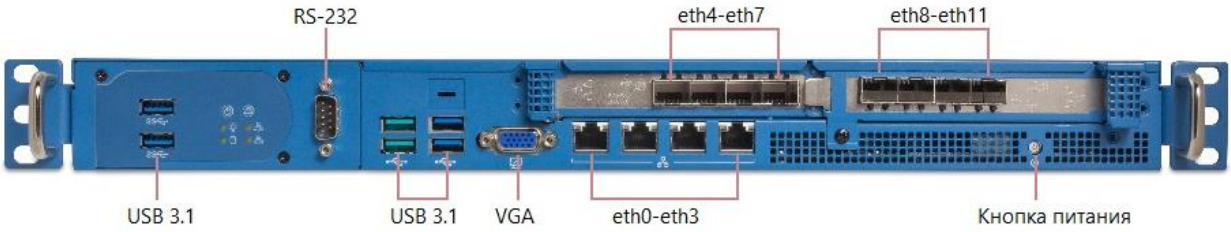

Рисунок 30. Передняя панель HW5000 Q2

На задней панели HW5000 Q2 расположены разъемы адаптеров питания.

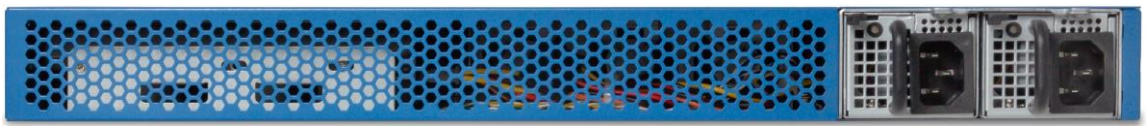

Рисунок 31. Задняя панель HW5000 Q2

3

Лицензирование и функциональные ограничения

Лицензирование ViPNet Coordinator HW

Лицензирование ViPNet Coordinator HW 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 HW. Соответствие исполнения назначенной роли проверяется при установке на ViPNet Coordinator HW справочников и ключей.

Исполнениям ViPNet Coordinator HW на аппаратных платформах HW50 N1, N2, N3, N4 и HW100 X1, X8 могут быть назначены различные роли: Coordinator HW50 A, Coordinator HW50 B и Coordinator HW100 A, Coordinator HW100 B.

Таблица 19. Исполнения ViPNet Coordinator HW и их аппаратные платформы

Исполнение ViPNet Coordinator HW	**Аппаратные платформы**	**Название роли**
ViPNet Coordinator HW50 A	HW50 N1, N2, N3, N4	Coordinator HW50 A, Coordinator HW50 AU
ViPNet Coordinator HW50 B	HW50 N1, N2, N3, N4	Coordinator HW50 B
ViPNet Coordinator HW100 A	HW100 X1, X8	Coordinator HW100 A
ViPNet Coordinator HW100 B	HW100 X1, X8	Coordinator HW100 B
ViPNet Coordinator HW100 C	HW100 X2, X3, N1, N2, N3	Coordinator HW100 C Coordinator HW100 CU
ViPNet Coordinator HW1000	HW1000 Q2, Q3, Q4, Q7	Coordinator HW1000
ViPNet Coordinator HW1000 C	HW1000 Q5, Q8	Coordinator HW1000 C
ViPNet Coordinator HW1000 D	HW1000 Q6, Q9	Coordinator HW1000 D
ViPNet Coordinator HW2000	HW2000 Q2, Q3, Q4	Coordinator HW2000
ViPNet Coordinator HW5000	HW5000 Q1, Q2	Coordinator HW5000

Роль может накладывать ограничения на поддержку функций транспортного сервера и туннелирования соединений на канальном и сетевом уровне. В таблице ниже приведены ограничения, накладываемые ролями.

Таблица 20. Лицензионные ограничения, накладываемые ролями

Название роли	Функции транспортного сервера	Использование в кластере горячего резервирования	Максимальное число туннелируемых соединений на сетевом уровне	Туннелирование на канальном уровне
Coordinator HW50 A	Нет	Да	2	Нет
Coordinator HW50 B	Нет	Да	5	Нет
Coordinator HW50 AU	Нет	Да	Без ограничений	Нет
Coordinator HW100 A	Нет	Да	2	Нет
Coordinator HW100 B	Нет	Да	5	Нет
Coordinator HW100 C	Да	Да	10	Да
Coordinator HW100 CU	Да	Да	Без ограничений	Да
Coordinator HW1000	Да	Да	Без ограничений	Да
Coordinator HW1000 C	Да	Да	Без ограничений	Да
Coordinator HW1000 D	Да	Да	Без ограничений	Да
Coordinator HW2000	Да	Да	Без ограничений	Да
Coordinator HW5000	Да	Да	Без ограничений	Да

Существуют следующие особенности ролей исполнений ViPNet Coordinator HW:

- Для организации кластера горячего резервирования на основе исполнений ViPNet Coordinator HW50 A, B или ViPNet Coordinator HW100 A, B, C необходимо дополнительно назначить сетевому узлу роль Failover100.
- Для совместной работы в кластере вы можете использовать только одинаковые аппаратные платформы ViPNet Coordinator HW. Например, исполнение ViPNet Coordinator HW2000 представлено на трех аппаратных платформах — HW2000 Q2, HW2000 Q3 и HW2000 Q4. В этом случае вы можете использовать в кластере либо два ViPNet Coordinator HW на аппаратной платформе HW2000 Q2, либо два ViPNet Coordinator HW на аппаратной платформе HW2000 Q3, либо два ViPNet Coordinator HW на аппаратной платформе HW2000 Q4. Однако вы не можете использовать для совместной работы в кластере исполнения на аппаратных платформах HW2000 Q2 и HW2000 Q3 (а также HW2000 Q2 и HW2000 Q4 или HW2000 Q3 и HW2000 Q4).
- В исполнениях ViPNet Coordinator HW50 A, B и ViPNet Coordinator HW100 A, B не поддерживаются функции шлюзового координатора (см. глоссарий, стр. 112) и транспортного

сервера (см. глоссарий, стр. 112). Вследствие этого возникают следующие ограничения при формировании структуры сети ViPNet:

- Координатор, созданный для одного из этих исполнений, нельзя регистрировать в качестве шлюзового координатора в другие сети ViPNet. В противном случае работоспособность ViPNet Coordinator HW может быть нарушена.
- Клиенты ViPNet нельзя регистрировать за таким координатором. Координатор в данном случае может использоваться для туннелирования открытого IP-трафика (см. глоссарий, стр. 112).

Максимальное количество сетевых интерфейсов для различных аппаратных платформ

Количество интерфейсов, которое вы можете одновременно использовать на ViPNet Coordinator HW, ограничено в соответствии с используемой аппаратной платформой (см. таблицу ниже). В ViPNet Coordinator HW могут использоваться следующие типы сетевых интерфейсов:

- eth — по количеству физических разъемов Ethernet аппаратной платформы;
- wlan (если присутствует на аппаратной платформе) — 1;
- loopback-интерфейс (localhost) — 1;
- bond (если созданы агрегированные каналы) — 3;
- vlan и alias (интерфейс, который создается при добавлении дополнительного адреса для интерфейса eth) — количество, не превышающее в сумме с другими интерфейсами число в таблице ниже.

Таблица 21. Максимальное количество сетевых интерфейсов для различных аппаратных платформ ViPNet Coordinator HW

Аппаратная платформа	Максимальное количество сетевых интерфейсов
HW50 N1, N2, N3, N4	32
HW100 X1	8
HW100 X2, X3, X8	32
HW100 N1, N2, N3	128
HW1000 Q2, Q3, Q4, Q5, Q6, Q7, Q8, Q9	128
HW2000 Q2, Q3, Q4	128
HW5000 Q1, Q2	128

Количество связей ViPNet Coordinator HW с ViPNet-узлами

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

- оптимальное число клиентов, зарегистрированных на ViPNet Coordinator HW;
- количество связей сетевого узла ViPNet Coordinator HW с другими ViPNet-узлами, в том числе зарегистрированными за другими координаторами;
- максимальное количество связей сетевого узла ViPNet Coordinator HW 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 HW.

Таблица 22. Максимальное количество ViPNet-клиентов, связанных с ViPNet Coordinator HW

Исполнение	Оптимальное число клиентов, зарегистрированных на координаторе	Максимальное количество связей с ViPNet-узлами	Максимальное количество связей с туннелирующими координаторами	Максимальное количество заданных диапазонов туннелируемых узлов
ViPNet Coordinator HW50	0	500	50	1000
ViPNet Coordinator HW100 A, 100 B	0	500	50	1000
ViPNet Coordinator HW100 C	10	1000	50	1000
ViPNet Coordinator HW1000	500	5000	100	1000
ViPNet Coordinator HW1000 C, 1000 D	1000	10000	1000	1000
ViPNet Coordinator HW2000	5000	15000	5000	1000
ViPNet Coordinator HW5000	6000	15000	5000	1000

4

Подготовка к работе

Установка SIM-карты в HW50 N3 и HW100 N3

Аппаратные платформы ViPNet Coordinator HW50 N3 и HW100 N3 оснащены 3G-модемами. Чтобы подключиться к сети 3G, необходимо установить SIM-карту в соответствующий разъем. Для этого выполните следующие действия:

1. Убедитесь, что ViPNet Coordinator HW выключен. В противном случае выключите его.
2. Открутите крепежные винты и разберите корпус ViPNet Coordinator HW.
3. На материнской плате найдите плату mini-PCIe, открутите крепежный винт и снимите ее.

Рисунок 32. Плата mini-PCIe на HW50 N3 и HW100 N3

4. На аппаратной платформе HW50 разъем для крепления SIM-карты находится на плате mini-PCIe. Вставьте SIM-карту в разъем.

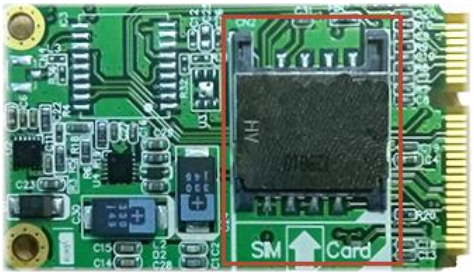

Рисунок 33. Разъем для установки SIM-карты на HW50 N3

5 На аппаратной платформе HW100 N3 разъем для крепления SIM-карты расположен на материнской плате под платой mini-PCIe. Откройте крышку разъема и установите SIM-карту.

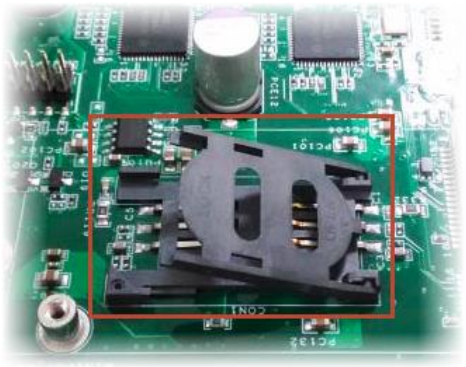

Рисунок 34. Разъем для установки SIM-карты на HW100 N3

6 Установите плату mini-PCIe в исходное положение и зафиксируйте ее крепежным винтом.

7 Соберите корпус ViPNet Coordinator HW.

Установка, обновление и удаление справочников и ключей

Способы установки и подготовка к установке справочников и ключей

Перед началом эксплуатации ViPNet Coordinator HW на нем необходимо установить справочники и ключи сетевого узла ViPNet. Без этого работа ViPNet Coordinator HW и управление устройством будут невозможны. Вы можете установить справочники и ключи в следующих случаях:

- Первоначальная инициализация справочников и ключей с помощью дистрибутива ключей сетевого узла (файла `*.dst`).

  Файл `*.dst` и пароль вы можете получить у администратора сети ViPNet. Если администратор сети при создании дистрибутива ключей указал для пользователя ViPNet Coordinator HW способ аутентификации «Устройство», получите также внешнее устройство, на котором сохранен персональный ключ пользователя (см. глоссарий, стр. 110).

- Восстановление справочников, ключей и настроек на ViPNet Coordinator HW после некорректного обновления ПО или их перенос с другого ViPNet Coordinator HW того же исполнения (например, при замене аппаратной платформы). Для выполнения данных операций требуется файл `*.vbe`, в который были экспортированы справочники, ключи и настройки с другого действующего ViPNet Coordinator HW. Подробнее об этом см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», разделе «Резервное копирование и восстановление настроек».

Существует несколько способов установки справочников и ключей на ViPNet Coordinator HW. Способ установки зависит от способа подключения к ViPNet Coordinator HW.

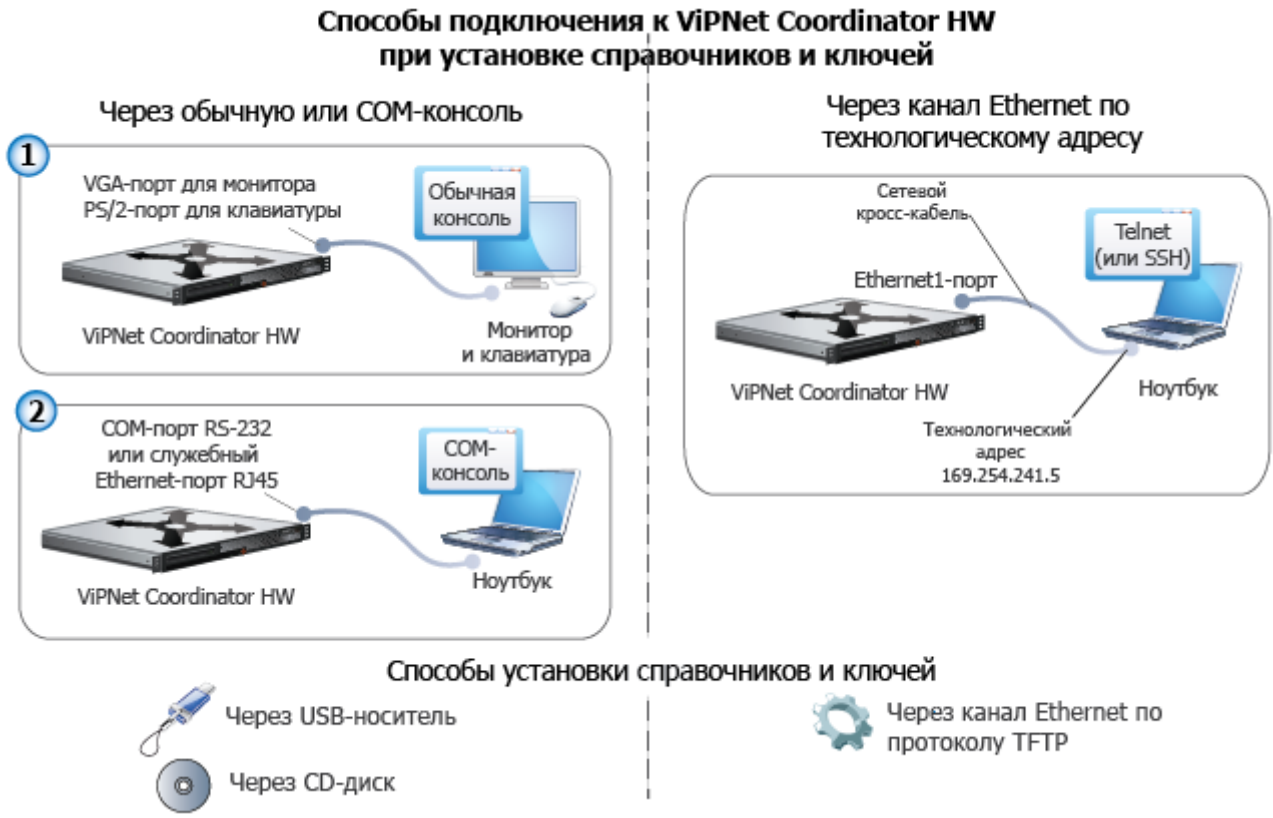

Рисунок 35. Способы подключения и установки справочников и ключей на ViPNet Coordinator HW

Вы можете выбрать один из следующих способов установки:

- Через ноутбук по каналу Ethernet и протоколу TFTP (см. Установка с помощью ноутбука по Ethernet-каналу и протоколу TFTP на стр. 60). Удобен, если вы подключаетесь к ViPNet Coordinator HW с ноутбука через сетевой кросс-кабель Ethernet и технологический адрес.
- Через внешнее устройство, которым может быть USB-носитель или CD-диск (при наличии внешнего CD-привода) (см. Установка с помощью внешнего устройства на стр. 61). Удобен, если вы подключаетесь к ViPNet Coordinator HW через обычную консоль (с использованием монитора и клавиатуры) или COM-консоль (с использованием ноутбука).

Установка с помощью ноутбука по Ethernet-каналу и протоколу TFTP

Для установки справочников и ключей данным способом вам понадобится следующее:

- ноутбук с сетевой картой Ethernet и ОС Windows или GNU/Linux любых версий;
- сетевой кросс-кабель Ethernet для соединения ноутбука с ViPNet Coordinator HW.

На ноутбуке должны быть включены стандартные службы Telnet (или SSH) и TFTP, которые необходимы для выполнения следующих функций:

- для подключения к ViPNet Coordinator HW (Telnet или SSH);
- для переноса дистрибутива ключей на ViPNet Coordinator HW (TFTP).

В ОС Windows XP и GNU/Linux эти службы по умолчанию включены. В ОС Windows Vista и выше эти службы по умолчанию отключены и их необходимо включить вручную. Для включения служб в ОС Windows Vista и выше выполните следующее:

1 Выберите **Пуск** (**Start**) > **Панель управления** (**Control Panel**) > **Программы и компоненты** (**Programs and Features**).

2 Зайдите в меню **Включение или отключение компонентов Windows** (**Turn Windows features on or off**) и установите флажки рядом с названием служб **Клиент TFTP** (**TFTP Client**) и **Простые службы TCPIP** (**Simple TCPIP services**).

Внимание! Убедитесь, что в используемом вами TFTP-клиенте установлен двоичный режим передачи данных. Это необходимо для корректного взаимодействия с ViPNet Coordinator HW по протоколу TFTP.

Кроме того, на время установки на ноутбуке с ОС Windows Vista и выше отключите следующие службы безопасности (если они включены):

- Брандмауэр Windows (Windows Firewall);
- Защитник Windows (Windows Defender);
- Центр обновления Windows (Windows Update);
- в меню **Свойства обозревателя** (**Internet Options**) на вкладке **Безопасность** (**Security**) отключите защиту по всем параметрам.

Перед началом установки справочников и ключей выполните следующие действия:

1 Перенесите на ноутбук дистрибутив ключей (файл `*.dst`).

2 С помощью кросс-кабеля подключите ноутбук к порту Ethernet1 ПАК ViPNet Coordinator HW.

3 Установите вручную на сетевом интерфейсе ноутбука технологический IP-адрес 169.254.241.5.

4 Подключитесь к ViPNet Coordinator HW по Telnet либо по протоколу SSH (с помощью Telnet- или SSH-клиента) по адресу `169.254.241.1`. Для корректной работы на Telnet- или SSH-клиенте должны быть заданы следующие параметры (далее для примера приведены настройки клиента PuTTY):

   - Тип терминала VT100 (**Terminal** > **Keyboard** > **VT100+**).
   - Кодировка символов KOI8-R (**Window** > **Translation**, в списке **Remote character set** выберите **KOI8-R** или **KOI8-U**).
   - Метод ввода linux (**Connection** > **Data** > **Terminal type string**, введите **linux**).
   - Ширина окна по умолчанию 120 символов (**Windows** > **Columns**, введите **120**).

Установка с помощью внешнего устройства

Выполните предварительные действия:

1 Отформатируйте USB-носитель в одну из файловых систем: FAT32, ext2, ext3 или ext4.

2 Запишите на USB-носитель или CD-диск дистрибутив ключей (файл *.dst).

3 При подключении COM-консоли укажите параметры COM-порта и настройки клиента:

- Speed (скорость обмена данными) — 38400;
- Data (размер данных) — 8;
- Parity (четность) — None;
- Stopbits (стоповые биты) — 1:
- Тип терминала — VT100+;
- Flow Control — None;
- Remote character set (кодировка) — KOI8-R или KOI8-U.

4 Подключитесь к ViPNet Coordinator HW через обычную или COM-консоль:

- Подключите монитор и клавиатуру к VGA-порту и PS/2-порту ПАК или компьютера ViPNet Coordinator HW.
- Подключите ноутбук к COM-порту RS-232 ПАК или компьютера ViPNet Coordinator HW.

Примечание. В исполнениях ViPNet Coordinator HW50 A, B и ViPNet Coordinator HW100 C (на аппаратных платформах HW100 N1, N2, N3) вместо COM-порта присутствует служебный порт RJ45 для подключения ноутбука.

Установка справочников и ключей

Для установки справочников и ключей на координатор ViPNet Coordinator HW выполните все действия из приведенной таблицы.

Таблица 23. Последовательность установки справочников и ключей

	Действие	Ссылка
☐	Инициируйте установку справочников и ключей на ViPNet Coordinator HW	Начало установки (на стр. 63)
☐	Укажите часовой пояс, дату и время	Настройка часового пояса, даты и времени (на стр. 64)
☐	Выберите нужный дистрибутив ключей	Установка дистрибутива ключей на ViPNet Coordinator HW (на стр. 66)
☐	Настройте параметры всех сетевых интерфейсов ViPNet Coordinator HW	Настройка сетевых интерфейсов (на стр. 68)
☐	Настройте параметры DNS-сервера	Настройка DNS-сервера (на стр. 69)
☐	Настройте параметры NTP-сервера	Настройка NTP-сервера (на стр. 71)

	Действие	Ссылка
☐	При необходимости измените настройки виртуальных адресов	Настройка имени компьютера и диапазона виртуальных адресов (на стр. 72)
☐	Выберите режим подключения ViPNet Coordinator HW к внешней сети через межсетевой экран	Настройка подключения к внешней сети через межсетевой экран (на стр. 73)
☐	Проверьте связь с одним или несколькими узлами сети ViPNet	Проверка связи с другим сетевым узлом (на стр. 77)
☐	Завершите установку справочников и ключей	Завершение установки (на стр. 79)

Начало установки

Установка справочников и ключей производится с помощью мастера установки, который запускается автоматически после авторизации в операционной системе. Мастер установки может работать в одном из двух режимов:

- обычный консольный режим;
- полноэкранный режим с эмуляцией графического интерфейса.

Выбрать режим работы предлагается сразу после запуска мастера. При описании установки справочников и ключей приведены оба варианта работы с мастером — в консольном режиме и в полноэкранном режиме.

Внимание! При работе в полноэкранном режиме не поддерживаются «горячие клавиши».

В полноэкранном режиме для управления установкой предусмотрены следующие кнопки:

- **Next** — переход к следующему шагу.
- **Back** — возврат к предыдущему шагу.
- **Cancel** — прерывание установки. В случае прерывания установки состояние системы не изменяется — она остается в том состоянии, в котором была до начала установки.

Для управления установкой в полноэкранном режиме также могут использоваться следующие клавиши:

- **Tab** — переход между элементами интерфейса.
- «пробел» — выбор пункта меню.
- «стрелка вверх», «стрелка вниз», «+», «–» — задание числовых значений (например, времени), переход между элементами интерфейса.

Для начала установки справочников и ключей выполните следующие действия:

1 Введите имя пользователя `user` и пароль `user`. После авторизации в системе автоматически будет запущен мастер установки.

2 Выберите режим работы мастера в ответ на сообщение `Please select setup wizard operating mode`:

- `1` — консольный;
- `2` — полноэкранный.

3 Ознакомьтесь с лицензионным соглашением с конечным пользователем на использование ПО ViPNet Coordinator HW. Для просмотра лицензионного соглашения вы можете использовать клавиши **PageUp** и **PageDown**. Введите символ `Y`, если вы согласны принять соглашение с пользователем, или символ `N` в противном случае.

Примечание. Текст лицензионного соглашения отображается в кодировке KOI8-R, поэтому в случае, если вы подключены к ViPNet Coordinator HW через COM-консоль, Telnet или SSH и текст лицензионного соглашения отображается неверно, убедитесь, что на вашем консольном клиенте заданы верные параметры (см. Установка с помощью ноутбука по Ethernet-каналу и протоколу TFTP на стр. 60).

4 В ответ на предложение начать установку в консольном режиме `Would you like to start installing keys or restoring configuration? [Yes/No]` введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Next**. Следуйте указаниям мастера.

Настройка часового пояса, даты и времени

Следующие шаги предназначены для задания часового пояса (временной зоны), текущих даты и времени. Часовой пояс должен соответствовать географическому местоположению ViPNet Coordinator HW. При установке справочников и ключей из файла `*.vbe` эти шаги выполняются автоматически, так как настройки часового пояса импортируются из файла экспорта.

Для настройки часового пояса, даты и времени ViPNet Coordinator HW выполните следующие действия:

1 Выберите континент. Для этого введите номер континента из предложенного списка и нажмите клавишу **Enter**. В полноэкранном режиме выберите континент в списке и нажмите кнопку **Next**.

Если на ViPNet Coordinator HW необходимо установить время UTC, выберите в списке последний элемент. В этом случае сразу выводится информация о текущем времени UTC и запрашивается подтверждение на его установку.

2 Выберите страну. Для этого введите номер страны из предложенного списка и нажмите клавишу **Enter**. В полноэкранном режиме выберите страну в списке и нажмите кнопку **Next**. Список содержит страны, расположенные на выбранном континенте.

3 Выберите часовой пояс. Для этого введите номер пояса и нажмите клавишу **Enter**. В полноэкранном режиме выберите часовой пояс в списке и нажмите кнопку **Next**. Список содержит часовые пояса, имеющиеся в выбранной стране.

Если в выбранной на предыдущем шаге стране есть только один часовой пояс, он выбирается автоматически.

4 Подтвердите установку выбранного часового пояса. Если выбран нужный часовой пояс, в ответ на сообщение с информацией о текущем времени в этом поясе и вопросом `Is the above information OK?` введите символ `1` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Yes**.

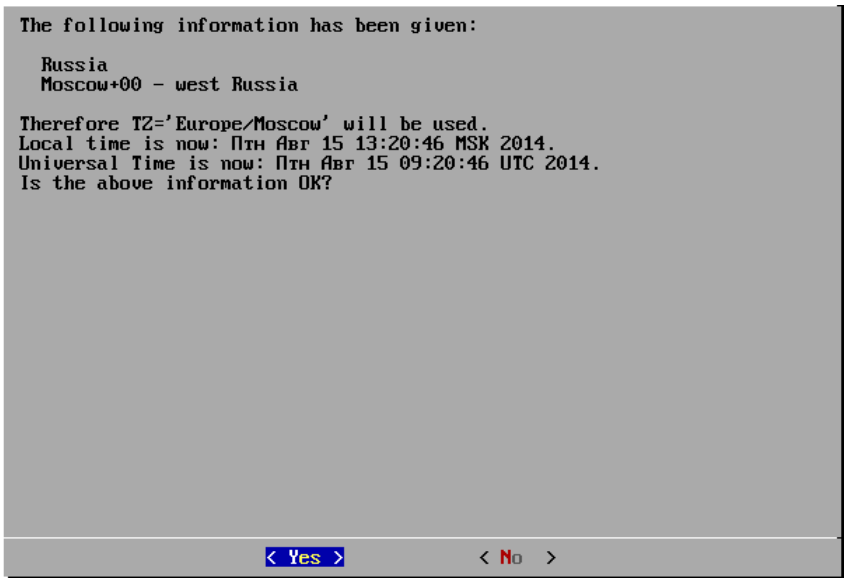

Рисунок 36. Запрос на установку часового пояса в полноэкранном режиме

Если необходимо установить другой часовой пояс, введите символ `2` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **No**. После отказа от установки этого часового пояса мастер вернется к выбору континента.

5 Если требуется изменить текущую дату и время, введите их в формате `YYYY-MM-DD hh:mm:ss` (`год-месяц-день часы-минуты-секунды`) и нажмите клавишу **Enter**.

Примечание. Если требуется изменить только время, то дату вы можете не вводить.

В полноэкранном режиме на одной странице установите нужную дату с помощью календаря, на следующей странице установите время с помощью клавиш «стрелка вверх», «стрелка вниз» или «+», «-», после чего нажмите кнопку **Next**.

Если дату и время изменять не нужно, нажмите клавишу **Enter**. В полноэкранном режиме 2 раза нажмите кнопку **Next**.

Установка дистрибутива ключей на ViPNet Coordinator HW

Для переноса и установки дистрибутива ключей `*.dst` или файла экспорта `*.vbe` на ViPNet Coordinator HW выполните следующие действия:

1. Выберите один из предложенных способов переноса файла. Для этого в ответ на сообщение `Would you like installing keys from TFTP, USB or CD storage device? [t/u/c]` введите один из символов:
   - `t` — для переноса с ноутбука по протоколу TFTP;
   - `u` — для переноса с USB-носителя;
   - `c` — для переноса с CD-диска.

   В полноэкранном режиме установите переключатель в нужное положение с помощью клавиши «пробел» и нажмите кнопку **Next**.
2. Перенесите файл выбранным способом.

   Если вы выбрали способ переноса по TFTP, выполните на ноутбуке команду:

   `tftp -i 169.254.241.1 put <имя файла>`,

   после чего нажмите на консоли клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Next**.
3. Если вы выбрали способ переноса с USB-носителя или CD-диска (при наличии внешнего CD-привода), подключите устройство к одному из USB-разъемов ViPNet Coordinator HW или вставьте диск в привод и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Next**.
   Если на USB-носителе будет обнаружен только один файл, то в консольном режиме он будет выбран для установки автоматически. В полноэкранном режиме список будет содержать только этот файл.

   Если обнаружено несколько файлов `*.dst` и `*.vbe`, появится пронумерованный список `Found several dst and vbe files`. Для файлов `*.dst` дополнительно указываются имена и идентификаторы сетевых узлов, которым они соответствуют. В этом случае выберите файл для установки. Для этого введите номер файла из предложенного списка и нажмите клавишу **Enter**. Если номер не введен или введен некорректный номер, появится сообщение с предложением заново ввести номер файла.

   В полноэкранном режиме выберите файл в списке и нажмите кнопку **Next**.

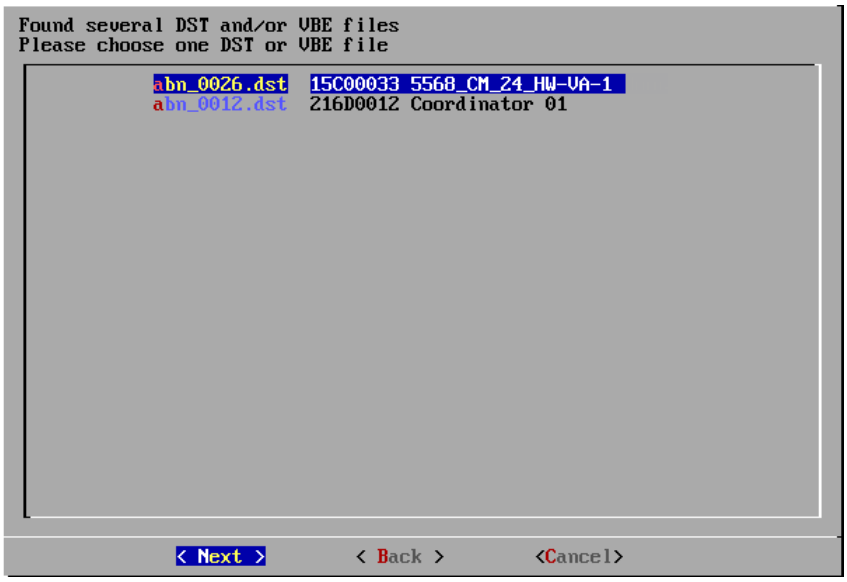

Рисунок 37. Выбор файла для установки справочников и ключей

В консольном режиме, если найдено больше 20 файлов, список выводится постранично по 20 файлов на странице. На каждой странице появляется предложение выбрать нужный файл либо перейти к следующей или первой странице.

Совет. В полноэкранном режиме длинные имена файлов могут быть не видны в списке полностью. Чтобы увидеть полное имя, выберите файл в списке — его имя будет отображено под окном мастера.

Если файлов нет, появится сообщение `DST or VBE files are not found`. Заново выберите способ переноса файла. В полноэкранном режиме нажмите в окне сообщения кнопку **Back**, произойдет возврат к предыдущему шагу.

4 Введите пароль к дистрибутиву ключей или пароль доступа к файлу экспорта в ответ на сообщение `Enter password` и нажмите клавишу **Enter**. В полноэкранном режиме после ввода пароля нажмите кнопку **Next**.

Если введенный пароль верен, то начнется установка справочников и ключей из выбранного файла.

5 Если администратор сети при создании дистрибутива ключей указал для пользователя ViPNet Coordinator HW способ аутентификации «Устройство», в ответ на сообщение `Insert token and enter PIN Code` выполните следующие действия:

- Подключите к одному из USB-разъемов ViPNet Coordinator HW внешнее устройство, на котором сохранен персональный ключ пользователя (см. глоссарий, стр. 110).
- Введите ПИН-код доступа к подключенному устройству.

Внимание! На подключенном устройстве должен быть только один контейнер, в котором содержится персональный ключ пользователя. При наличии нескольких контейнеров на устройстве персональный ключ пользователя не удастся найти, поэтому установка ключей не будет продолжена, о чем оповестит появившееся сообщение.

Если введенный ПИН-код верен, то появится соответствующее сообщение и установка справочников и ключей из выбранного файла будет продолжена.

По завершении установки справочников и ключей из дистрибутива ключей появится информация об узле, и мастер перейдет к следующему шагу (см. Настройка сетевых интерфейсов на стр. 68). По завершении установки справочников и ключей из файла экспорта мастер предложит перезагрузить компьютер (см. Завершение установки на стр. 79).

Настройка сетевых интерфейсов

При импорте справочников и ключей из файла `*.vbe` следующие шаги вплоть до завершения установки пропускаются, так как все настройки импортируются из файла экспорта. В результате успешного импорта и после перезагрузки компьютера на ViPNet Coordinator HW будут установлены те настройки, которые были на момент выполнения экспорта (см. Завершение установки на стр. 79).

При установке справочников и ключей из файла `*.dst` следующие шаги вам необходимо выполнить для каждого сетевого интерфейса ViPNet Coordinator HW.

Для настройки сетевых интерфейсов ViPNet Coordinator HW выполните следующие действия:

1 Включите интерфейс, если это необходимо. Для этого в консоли в ответ на сообщение `Configure interface eth<номер>? [Yes/No]` введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **UP** с помощью клавиши «пробел» и нажмите кнопку **Next**.

После включения интерфейса мастер перейдет к следующему шагу.

Если интерфейс включать не надо, введите символ `n` и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **DOWN** и нажмите кнопку **Next**. Мастер предложит настроить следующий сетевой интерфейс. В случае отказа от конфигурации последнего сетевого интерфейса, мастер перейдет к настройке DNS-сервера (см. Настройка DNS-сервера на стр. 69).

2 Установите для интерфейса режим DHCP, если это необходимо. Для этого в ответ на сообщение `Use dhcp on the interface eth<номер>? [Yes/No]` введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **DHCP** и нажмите кнопку **Next**.

Если для интерфейса нужно задать статические параметры, введите символ `n` и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **StaticIP** и нажмите кнопку **Next**.

3 Если для интерфейса не был выбран режим DHCP, введите последовательно IP-адрес и маску интерфейса и нажмите клавишу **Enter**. В полноэкранном режиме введите параметры

интерфейса в соответствующие поля, используя для перехода между полями ввода клавишу «стрелка вниз», после чего нажмите кнопку **Next**.

Внимание! При задании IP-адреса действуют следующие ограничения:

- нельзя задать IP-адрес 0.0.0.0;
- нельзя задать маски подсети 0.0.0.0, 255.255.255.254 и 255.255.255.255;
- для разных сетевых интерфейсов нельзя задать IP-адреса, относящиеся к одной подсети.

Также невозможно установить файл конфигурации (`*.vbe`), если он содержит настройки IP-адресов сетевых интерфейсов, в которых не соблюдаются описанные ограничения.

Если сконфигурированный на данном шаге интерфейс не последний, мастер переходит к конфигурированию следующего интерфейса.

4 Если ни для одного включенного интерфейса не был задан режим DHCP, введите IP-адрес шлюза по умолчанию и нажмите клавишу **Enter**. В полноэкранном режиме после ввода адреса нажмите кнопку **Next**.

Если хотя бы для одного включенного интерфейса задан режим DHCP, после установки справочников и ключей проверьте, что от DHCP-сервера был получен маршрут по умолчанию (см. глоссарий, стр. 109). Для этого выполните одно из действий:

- Выполните команду:

  ```
  hostname> inet show routing
  ```

  Если маршрут по умолчанию не был получен, будет выведено соответствующее предупреждение. В этом случае задайте статический маршрут по умолчанию (см. документ «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», раздел «Настройка маршрутизации»).

- В веб-интерфейсе в разделе **Сетевые настройки** > **Маршрутизация** проверьте наличие маршрута по умолчанию (он имеет вид 0.0.0.0/0).

  Если такого маршрута нет, задайте статический маршрут по умолчанию (см. документ «ViPNet Coordinator HW. Настройка с помощью веб-интерфейса», раздел «Настройка маршрутизации»).

Внимание! Убедитесь, что заданный в маршруте шлюз по умолчанию доступен для сетевого узла ViPNet Coordinator HW. Если шлюз по умолчанию окажется недоступен, многие функции ViPNet Coordinator HW не будут работать (например, виртуальные IP-адреса, обработка прикладных протоколов, сетевые службы и другие).

Настройка DNS-сервера

Для настройки DNS-сервера (см. глоссарий, стр. 106) выполните следующие действия:

1 Включите автоматический запуск DNS-сервера при загрузке ViPNet Coordinator HW, если это необходимо. Для этого в ответ на сообщение `Do you want to use DNS server? [Yes/No]` введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме установите

переключатель в положение **ON (Enable starting the DNS server at boot)** и нажмите кнопку **Next**.

После включения автоматического запуска DNS-сервера мастер перейдет к следующему шагу.

Если DNS-сервер запускать не нужно, введите символ `n` и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **OFF (Disable starting the DNS server at boot)** и нажмите кнопку **Next**. В этом случае мастер перейдет к настройке NTP-сервера (см. Настройка NTP-сервера на стр. 71).

2 Появится сообщение, что при наличии подключения к Интернету в качестве DNS-серверов по умолчанию используются корневые DNS-серверы. При этом вы можете принять или отклонить предложение добавить DNS-сервер `Do you want to add custom DNS server? [Yes/No].`

- Если необходимо добавить конкретный DNS-сервер, введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **Yes (Add custom DNS server)** и нажмите кнопку **Next**.

  После этого введите IP-адрес DNS-сервера и нажмите клавишу **Enter**. В полноэкранном режиме после ввода адреса нажмите кнопку **Next**.

- Если DNS-сервер добавлять не нужно, введите символ `n` и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **No (Leave the default setting)** и нажмите кнопку **Next**. В этом случае будут использоваться либо настройки по умолчанию, либо текущие настройки (если это не первая установка справочников и ключей).

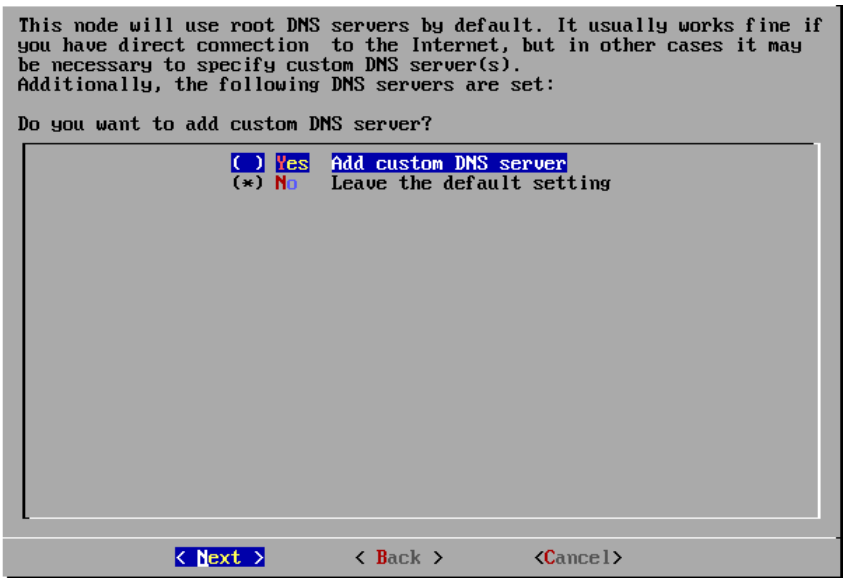

Рисунок 38. Запрос на добавление IP-адреса DNS-сервера в полноэкранном режиме

После отказа от добавления DNS-сервера мастер перейдет к настройке NTP-сервера.

Настройка NTP-сервера

Для настройки NTP-сервера выполните следующие действия:

1 Включите автоматический запуск NTP-сервера при загрузке ViPNet Coordinator HW, если это необходимо. Для этого в ответ на сообщение `Do you want to use NTP daemon to synchronize the time? [Yes/No]` введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **ON (Enable starting the NTP server at boot)** и нажмите кнопку **Next**.

После включения автоматического запуска NTP-сервера мастер перейдет к следующему шагу.

Если NTP-сервер запускать не нужно, введите символ `n` и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **OFF (Disable starting the NTP server at boot)** и нажмите кнопку **Next**. В этом случае мастер перейдет к настройке имени компьютера (см. Настройка имени компьютера и диапазона виртуальных адресов на стр. 72).

2 Появится сообщение, что для синхронизации системного времени по умолчанию будут использоваться публичные NTP-серверы точного времени. При этом вы можете принять или отклонить предложение добавить NTP-сервер `Do you want to add custom NTP server? [Yes/No]`.

- Если необходимо добавить конкретный NTP-сервер, введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **Yes (Add custom NTP server)** и нажмите кнопку **Next**.

  После этого введите IP-адрес или DNS-имя NTP-сервера и нажмите клавишу **Enter**. В полноэкранном режиме после ввода нажмите кнопку **Next**.

- Если NTP-сервер добавлять не нужно, введите символ `n` и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **No (Leave the default setting)** и нажмите кнопку **Next**. В этом случае будут использоваться либо настройки по умолчанию, либо текущие настройки (если это не первая установка справочников и ключей).

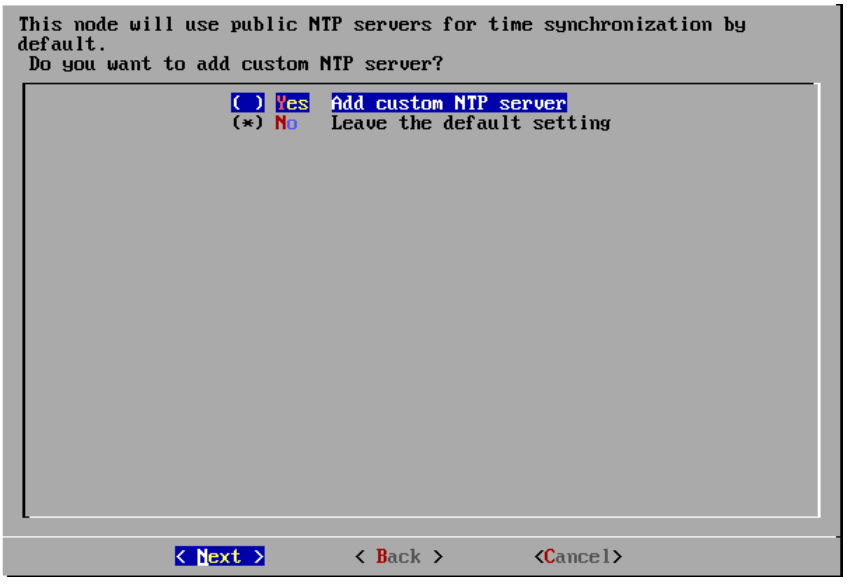

Рисунок 39. Запрос на добавление NTP-сервера в полноэкранном режиме

После отказа от добавления NTP-сервера мастер перейдет к установке имени компьютера.

Настройка имени компьютера и диапазона виртуальных адресов

Для настройки имени компьютера и диапазона виртуальных адресов выполните следующие действия:

1 Введите имя компьютера, если вы не хотите оставить имя, заданное по умолчанию, и нажмите клавишу **Enter**. В полноэкранном режиме введите нужное имя и нажмите кнопку **Next**.

   По умолчанию предлагается имя, сформированное по шаблону <исполнение ViPNet Coordinator HW>-<идентификатор узла>. Например: HW1000-270E033A.

   Если имя изменять не нужно, нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Next**.

2 Мастер перейдет к настройке виртуальных адресов. Появится текущий диапазон виртуальных адресов, назначаемых узлам сети, и предложение его изменить `Do you want to specify custom virtual IP address range? [Yes/No].`

   

   Примечание. По умолчанию предлагается диапазон виртуальных адресов 11.0.0.1/8 (в нотации CIDR, что соответствует диапазону 11.0.0.1-11.255.255.254) Если этот диапазон пересекается с диапазоном IP-адресов, который используется для адресации в вашей сети, измените его.

   Подробнее о виртуальных адресах см. документ «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», раздел «Общие принципы назначения виртуальных адресов».

   Виртуальные адреса из указанного диапазона будут назначаться одиночным туннелируемым адресам. Для диапазонов туннелируемых узлов адреса берутся из следующего интервала: <x+1>.0.0.1–<x+1>.255.255.254, где x — первый октет заданного диапазона виртуальных адресов.

   Подробнее о задании виртуальных адресов для туннелируемых узлов см. документ «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», раздел «Настройка видимости туннелируемых узлов».

   Выполните одно из действий:

   - Если необходимо задать другой диапазон виртуальных адресов, введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **Yes (Set custom virtual IP range)** и нажмите кнопку **Next**.

     После этого введите начальный и конечный адреса (или только начальный адрес в нотации CIDR) нового диапазона виртуальных адресов и нажмите клавишу **Enter**. Например: 11.0.0.1-11.0.254.254 (или 11.0.0.1/16). В полноэкранном режиме после ввода нажмите кнопку **Next**.

- Если диапазон виртуальных адресов изменять не нужно, введите символ `n` и нажмите клавишу **Enter**. В полноэкранном режиме установите переключатель в положение **No (Leave the default setting)** и нажмите кнопку **Next**.

3 Если на предыдущем этапе вы настроили хотя бы один сетевой интерфейс, мастер предложит проверить соединение с узлом сети ViPNet (см. Проверка связи с другим сетевым узлом на стр. 77) и при необходимости настроить подключение к внешней сети через межсетевой экран (см. Настройка подключения к внешней сети через межсетевой экран на стр. 73).

Настройка подключения к внешней сети через межсетевой экран

Настроить подключение ViPNet Coordinator HW к внешней сети через межсетевой экран вы можете только в том случае, если на предыдущих этапах были выполнены следующие действия:

1 Настроен хотя бы один сетевой интерфейс (см. Настройка сетевых интерфейсов на стр. 68).

2 Дано согласие проверить соединение с одним из сетевых узлов ViPNet (см. Проверка связи с другим сетевым узлом на стр. 77).

Чтобы настроить подключение ViPNet Coordinator HW к внешней сети, выполните следующие действия:

1 После того, как вы согласились выполнить проверку соединения с узлом ViPNet, появится сообщение с предложением задать режим подключения ViPNet Coordinator HW к сети через межсетевой экран `Do you want to configure firewall mode? [Yes/No].`

- Если вы хотите использовать настройки подключения к сети через межсетевой экран, заданные в файле дистрибутива ключей, режим подключения ViPNet Coordinator HW через межсетевой экран задавать не нужно. В этом случае введите символ `n` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **No**.

  После отказа от задания режима подключения ViPNet Coordinator HW к сети через межсетевой экран появляется сообщение с предложением выбрать сетевой интерфейс, через который необходимо проверить соединение с другим узлом.

- Если необходимо задать режим подключения ViPNet Coordinator HW к сети через межсетевой экран, введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Yes**.

2 Выберите режим подключения ViPNet Coordinator HW к внешней сети через межсетевой экран.

Внимание! Не рекомендуем использовать режимы подключения «Без использования межсетевого экрана» и «Координатор», так как они являются устаревшими и будут удалены в следующих версиях продукта.

Если вы выбрали один из этих режимов, внесите изменения в файл iplir.conf. Подробнее см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора» раздел «Настройка параметров сетевого подключения координатора».

Вместо устаревших режимов рекомендуем использовать:

- режим «Со статической трансляцией адресов» вместо режима «Без межсетевого экрана»;
- режим «С динамической трансляцией адресов» вместо режима «Координатор».

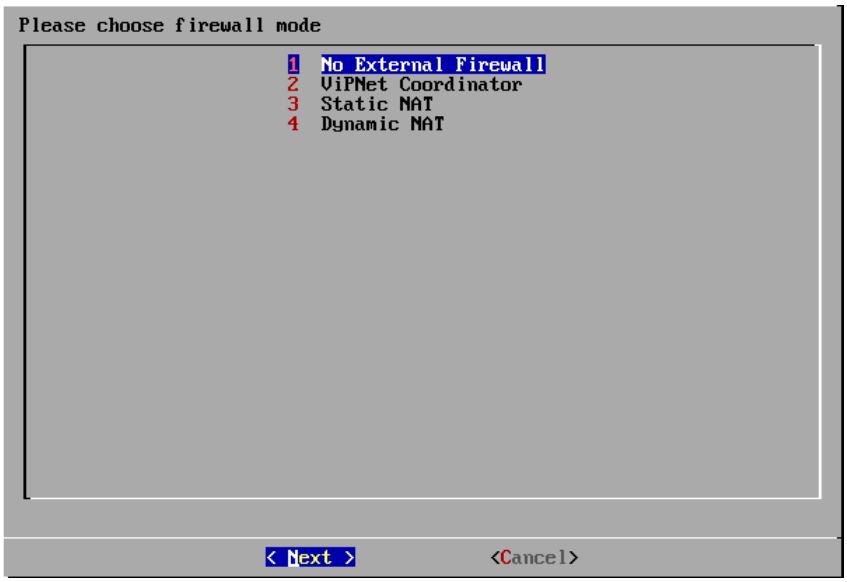

Рисунок 40. Выбор режима работы ViPNet Coordinator HW через межсетевой экран

- Чтобы выбрать режим «Без использования межсетевого экрана», введите цифру `1` и нажмите клавишу **Enter**. В полноэкранном режиме выберите режим **1 (No External Firewall)** и нажмите кнопку **Next**.
- Чтобы выбрать режим «Координатор», введите цифру `2` и нажмите клавишу **Enter**. В полноэкранном режиме выберите режим **2 (ViPNet Coordinator)** и нажмите кнопку **Next**.
- Чтобы выбрать режим «Со статической трансляцией адресов», введите цифру `3` и нажмите клавишу **Enter**. В полноэкранном режиме выберите режим **3 (Static NAT)** и нажмите кнопку **Next**.
- Чтобы выбрать режим «С динамической трансляцией адресов», введите цифру `4` и нажмите клавишу **Enter**. В полноэкранном режиме выберите режим **4 (Dynamic NAT)** и нажмите кнопку **Next**.

Подробнее о режимах подключения к сети через межсетевой экран см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».

3 Если был выбран режим **Без использования межсетевого экрана**, то перейдите к проверке связи с другим узлом ViPNet (см. Проверка связи с другим сетевым узлом на стр. 77).

4 Если был выбран режим **Координатор**, выполните следующие действия:

4.1 В ответ на сообщение `Please choose the network interface which will be use as external` выберите сетевой интерфейс, который будет являться внешним. Для этого введите цифру, соответствующую нужному сетевому интерфейсу в предложенном списке, и нажмите клавишу **Enter**. В полноэкранном режиме выберите нужный сетевой интерфейс и нажмите кнопку **Next**.

4.2 В ответ на сообщение `Please choose the ViPNet Coordinator` выберите координатор, через который ViPNet Coordinator HW будет подключаться к сети. Для этого введите номер координатора, приведенный в списке, и нажмите клавишу **Enter**. В полноэкранном режиме выберите нужный координатор и нажмите кнопку **Next**.

В списке выводятся только те координаторы, с которыми у ViPNet Coordinator HW есть связи. Информация о связях содержится в справочниках, установленных на ViPNet Coordinator HW.

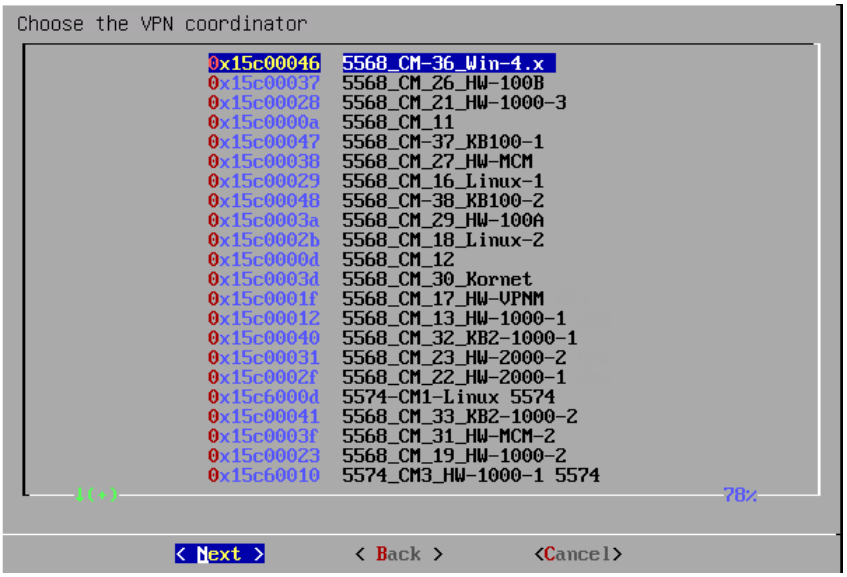

Рисунок 41. Выбор координатора для подключения к внешней сети

4.3 Если в справочниках не указан IP-адрес для выбранного координатора, мастер предложит вручную задать IP-адрес для него `The IP address of the ViPNet host has not been found. Do you want to specify one? [Yes/No].`

Примечание. Если в установленных справочниках не будут обнаружены связи ViPNet Coordinator HW с другими координаторами сети ViPNet, появится сообщение `Your VPN host has no links with VPN coordinators`. В этом случае вы можете отменить настройку режима подключения или настроить другой режим.

Чтобы задать IP-адрес координатора, введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Yes**. Затем введите IP-адрес и нажмите клавишу **Enter**. В полноэкранном режиме введите IP-адрес и нажмите кнопку **Next**.

4.4 После этого перейдите к проверке связи с другим узлом ViPNet.

5 Если был выбран режим **Со статической трансляцией адресов**, выполните следующие действия:

5.1 В ответ на сообщение `Do you want to specify custom UDP port? [Yes/No]` укажите, следует ли изменить номер порта отправки (порт источника) и порта получения (порт назначения) IP-пакетов, преобразованных в UDP-формат, на ViPNet Coordinator HW. По умолчанию используется порт 55777.

Примечание. Изменять номер порта нужно в том случае, если внутри локальной сети через один межсетевой экран (или NAT-устройство) работает несколько узлов с ПО ViPNet. У всех таких узлов номера портов должны быть разными.

Если необходимо изменить номер порта, введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Yes**. Затем введите номер порта и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Next**.

Если номер порта менять не нужно, введите символ `n` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **No**.

5.2 В ответ на сообщение `Do you want to specify fixed IP address of the external firewall? [Yes/No]` укажите, следует ли задать фиксированный IP-адрес внешнего межсетевого экрана.

Примечание. Фиксированный IP-адрес межсетевого экрана нужно задавать тогда, когда требуется, чтобы входящие пакеты поступали на определенный адрес межсетевого экрана независимо от того, с какого адреса были отправлены исходящие пакеты.

Не рекомендуем задавать фиксированный IP-адрес, так как режим со статической трансляцией адресов и фиксированным IP-адресом внешнего межсетевого экрана является устаревшим и будет удален в следующих версиях продукта.

Если необходимо задать IP-адрес, введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Yes**. Затем введите IP-адрес и нажмите клавишу **Enter**. В полноэкранном режиме введите IP-адрес и нажмите кнопку **Next**.

Если IP-адрес задавать не нужно, введите символ `n` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **No**. После этого перейдите к проверке связи с другим узлом ViPNet.

5.3 Выберите сетевой интерфейс, который будет являться внешним (аналогично п. 4.1).

6 Если был выбран режим **С динамической трансляцией адресов**, выполните следующие действия:

6.1 Выберите координатор, через который ViPNet Coordinator HW будет подключаться к сети (аналогично п. 4.2).

6.2 Задайте IP-адрес координатора, через который будет производиться подключение, если в установленных справочниках не обнаружены связи ViPNet Coordinator HW с другими координаторами сети ViPNet (аналогично п. 4.3).

6.3 Выберите сетевой интерфейс, который будет являться внешним (аналогично п. 4.1).

Проверка связи с другим сетевым узлом

Проверить связь с другим узлом ViPNet вы можете только в том случае, если на предыдущем этапе был настроен хотя бы один сетевой интерфейс (см. Настройка сетевых интерфейсов на стр. 68).

Для проверки связи с узлом ViPNet выполните следующие действия:

1. Если в процессе установки ключей вы изменяли параметры сетевых интерфейсов, то после настройки диапазона виртуальных адресов (см. Настройка имени компьютера и диапазона виртуальных адресов на стр. 72) появится сообщение с предложением выполнить проверку связи с одним из узлов сети ViPNet `Do you want to probe VPN-connection with some host in order to verify the configuration you've just made? [Yes/No]`. Выполните одно из действий:
   - Если проверку связи с узлами выполнять не нужно, введите символ `n` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **No**. В этом случае установка справочников и ключей будет завершена.
   - Если необходимо выполнить проверку связи с другим узлом, введите символ y и нажмите клавишу Enter. В полноэкранном режиме нажмите кнопку **Yes**.

   Примечание. Проверку связи с другими узлами сети ViPNet рекомендуется выполнять во избежание возможной потери доступа к ViPNet Coordinator HW при завершении установки справочников и ключей.

   В этом случае мастер предложит настроить подключение ViPNet Coordinator HW к внешней сети. Если требуется, выполните данную настройку (см. Настройка подключения к внешней сети через межсетевой экран на стр. 73). В противном случае настройки подключения к сети будут скопированы из дистрибутива ключей без изменения.
2. Появится список сетевых узлов ViPNet, с которыми ViPNet Coordinator HW имеет связи. Информация о связях содержится в справочниках, установленных на ViPNet Coordinator HW.

   Выберите сетевой узел, связь с которым вы хотите проверить. Для этого в ответ на сообщение

   `Please choose the ViPNet host by number [<диапазон цифр, соответствующих узлам в списке>] or [q] to cancel or press Enter for next page`

   введите цифру, соответствующую сетевому узлу в списке, и нажмите клавишу **Enter**. В полноэкранном режиме выберите нужный сетевой узел и нажмите кнопку **Next**.

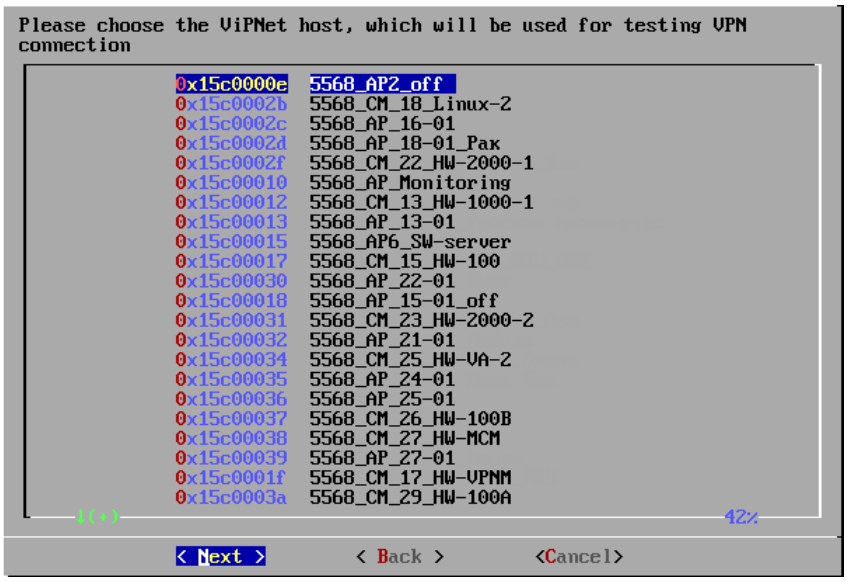

Рисунок 42. Выбор узла ViPNet для проверки связи

3 Если в справочниках не указан IP-адрес для выбранного сетевого узла, появится сообщение с предложением вручную задать для этого узла IP-адрес `The IP address of the ViPNet host has not been found. Do you want to specify one? [Yes/No].`

Чтобы задать IP-адрес для сетевого узла, введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Yes**. Затем введите IP-адрес и нажмите клавишу **Enter**. В полноэкранном режиме введите IP-адрес и нажмите кнопку **Next**.

4 Начнется проверка связи с выбранным сетевым узлом ViPNet.

Примечание. Проверка связи с сетевым узлом ViPNet может занять несколько минут.

---

5 По окончании появляется сообщение о результатах проверки связи с выбранным узлом.

- Если связь с узлом была установлена, все выполненные настройки сохраняются в конфигурационный файл `iplir.conf`. Подробнее о файле `iplir.conf` см. в документе «ViPNet Coordinator HW. Справочное руководство по командному интерпретатору и конфигурационным файлам».

  Нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **OK**. Мастер предложит запустить драйверы и демоны (см. Завершение установки на стр. 79).

- Если установить связь с сетевым узлом не удалось, появляется сообщение с предложением просмотреть журнал регистрации IP-пакетов `Do you want to view IP packet log in order to investigate the issue? [Yes/No].`

  - Для просмотра журнала введите символ `y`. На экране появится окно журнала IP-пакетов. Подробнее о работе с журналом см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».
  - Для отказа от просмотра журнала введите символ `n`.

После этого будет предложено выполнить повторную проверку связи с другим узлом сети ViPNet.

Завершение установки

Для завершения установки справочников и ключей выполните следующие действия:

1 Если производится импорт справочников, ключей и настроек из файла экспорта `*.vbe`, то для корректного применения настроек появится сообщение с предложением перезагрузить ViPNet Coordinator HW.

Для перезагрузки введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Reboot**. Работа мастера установки будет завершена, и ViPNet Coordinator HW перезагрузится.

Если вы хотите отказаться от немедленной перезагрузки, введите символ `n` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Continue**.

Примечание. Применение всех настроек, импортированных из файла экспорта `*.vbe`, произойдет только после перезагрузки. В случае отказа перезагрузите ViPNet Coordinator HW вручную.

2 Появится сообщение с предложением автоматически запустить драйверы и демоны ViPNet Coordinator HW после завершения установки `Do you want to start VPN services before leaving the installation wizard? [Yes/No]`. Для запуска введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Yes**.

Если драйверы и демоны запускать не нужно, введите символ n и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **No**. В этом случае после установки ключей необходимо вручную запустить демоны и драйверы с помощью команды:

```
hostname# vpn start
```

3 Появится сообщение об успешном завершении установки, и мастер предложит запустить командный интерпретатор `Do you want to start the command shell now? [Yes/No]`. Чтобы запустить командный интерпретатор, введите символ y и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Run Command shell**.

Если командный интерпретатор запускать не нужно, введите символ `n` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Finish**. Работа мастера будет завершена без запуска командного интерпретатора.

4 Если при установке ключей были настроены DNS- и NTP-серверы, запустите их с помощью команд:

```
hostname# inet dns start
hostname# inet ntp start
```

Теперь вы можете выполнить необходимую настройку ViPNet Coordinator HW с помощью командного интерпретатора или веб-интерфейса в соответствии с требуемыми сценариями

использования. Подробнее см. документы «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора» и «ViPNet Coordinator HW. Настройка с помощью веб-интерфейса».

Замена элемента питания CMOS BIOS

В процессе эксплуатации некоторых аппаратных платформ ViPNet Coordinator HW в связи с израсходованием заряда может возникнуть необходимость замены элемента питания CMOS BIOS на материнской плате. Это относится к следующим аппаратным платформам ViPNet Coordinator HW:

- HW100 X1, X2, X3, X8;
- HW1000 Q2, Q3;
- HW2000 Q2, Q3.

Чтобы заменить элемент питания CMOS BIOS, выполните следующие действия:

1. Убедитесь, что ViPNet Coordinator HW выключен. В противном случае выключите ViPNet Coordinator HW одним из следующих способов:
   - Авторизуйтесь в ViPNet Coordinator HW и в командном интерпретаторе введите:

     ```
     hostname> machine halt
     ```

   - Нажмите кнопку питания на передней панели ViPNet Coordinator HW.
2. Отключите кабель питания от корпуса ViPNet Coordinator HW.
3. Снимите крышку корпуса ViPNet Coordinator HW:
   - Открутите винты на корпусе, как показано на одном из следующих рисунков в зависимости от аппаратной платформы ViPNet Coordinator HW:

Рисунок 43. Расположение винтов на HW100

Рисунок 44. Расположение трех винтов на корпусе HW1000

Рисунок 45. Расположение двух винтов на задней панели HW2000

- Сдвиньте крышку в сторону задней панели на расстояние около 2 см и отсоедините ее от корпуса.

4 Чтобы заменить элемент питания CMOS BIOS, определите его положение на материнской плате ViPNet Coordinator HW с помощью одного из следующих рисунков в зависимости от аппаратной платформы ViPNet Coordinator HW:

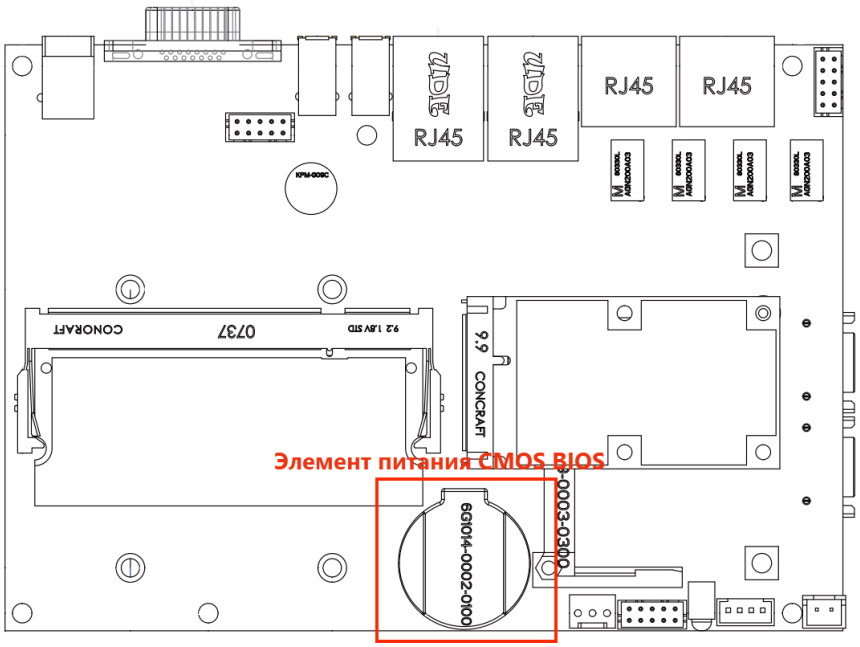

Рисунок 46. Расположение элемента питания на материнской плате HW100

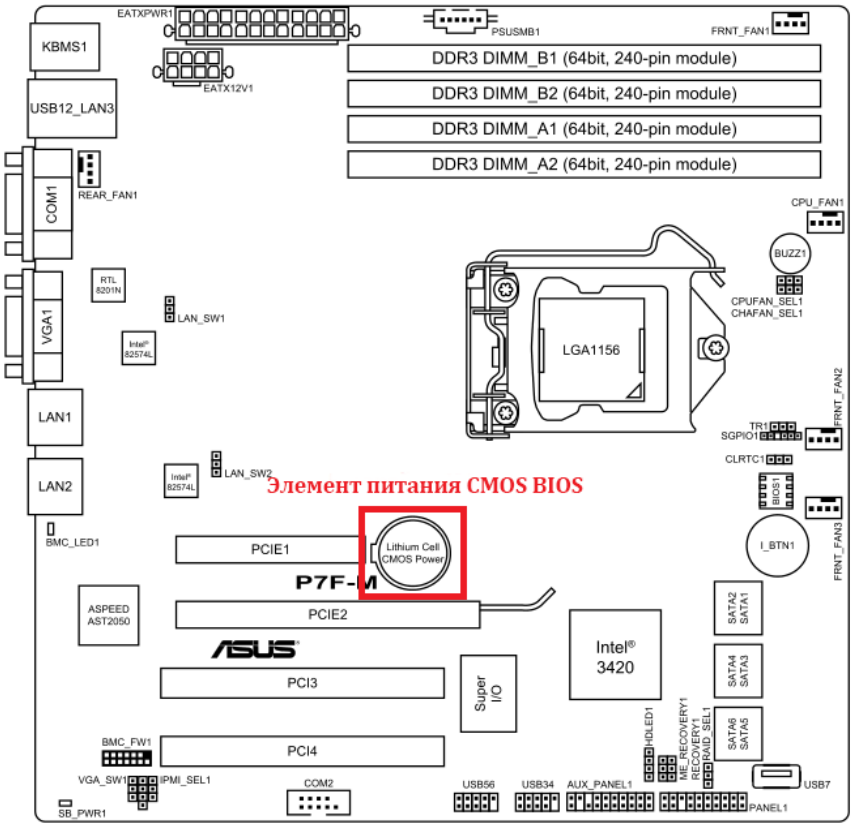

Рисунок 47. Расположение элемента питания на материнской плате HW1000

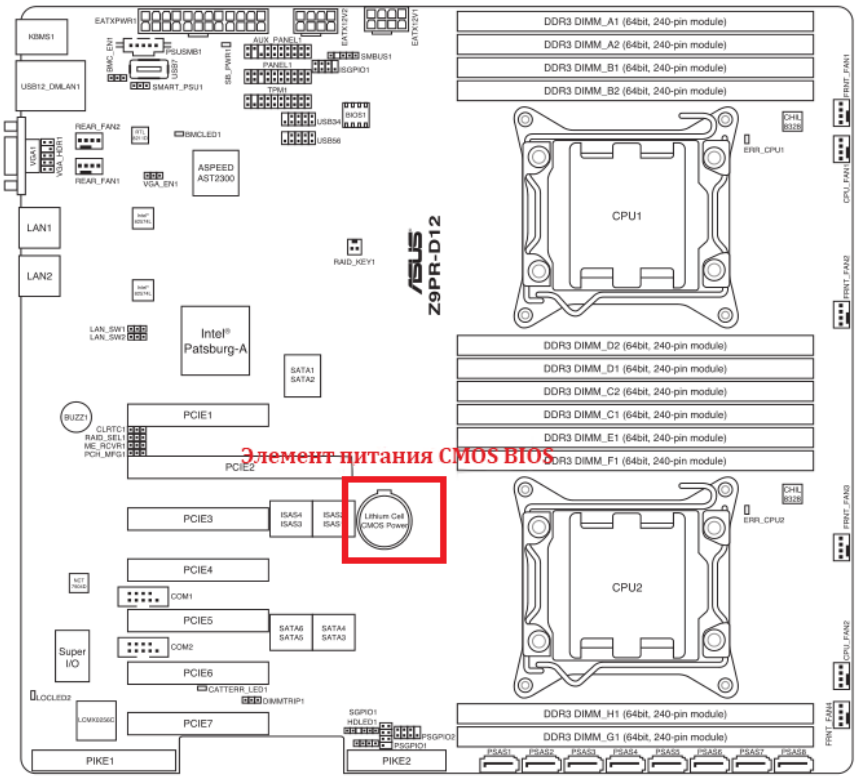

Рисунок 48. Расположение элемента питания на материнской плате HW2000

5 С помощью пинцета или отвертки с плоским наконечником отогните защелку гнезда элемента питания и извлеките элемент питания:

Рисунок 49. Извлечение элемента питания CMOS BIOS из гнезда на материнской плате

6 Вставьте новый элемент питания CMOS BIOS. Подойдет один из следующих видов элемента питания CMOS BIOS:

- CR2016 (емкость 80 мА·ч);
- CR2025 (емкость 150 мА·ч);
- CR2032 (емкость 230 мА·ч) — рекомендуем использовать именно такой элемент питания CMOS BIOS.

7 Установите крышку на корпус и нанесите защитные пломбы, как показано на одном из следующих рисунков в зависимости от аппаратной платформы ViPNet Coordinator HW:

Рисунок 50. Нанесение пломбы на корпус HW100

Рисунок 51. Нанесение пломбы на корпус HW1000

Рисунок 52. Нанесение пломбы на корпус HW2000

8 Подключите кабель питания и включите питание ViPNet Coordinator HW.

9 Настройте параметры BIOS (см. «Настройка параметров BIOS» на стр. 85).

Замена элемента питания CMOS BIOS завершена. Теперь вы можете включить ViPNet Coordinator HW.

Настройка параметров BIOS

После замены элемента питания CMOS BIOS все параметры BIOS возвращаются к заводским настройкам, поэтому необходимо заново произвести настройку параметров BIOS и задать пароли для защиты настроек BIOS от изменения.

Внимание! Чтобы изменить настройки BIOS, используйте обычную консоль (см. глоссарий, стр. 110).

Параметры настроек BIOS зависят от аппаратной платформы ViPNet Coordinator HW и приведены в соответствующих разделах:

- Параметры настройки BIOS для HW100 X1, X2, X3, X8 (на стр. 86)
- Параметры настройки BIOS для HW1000 Q2, Q3 (на стр. 88).
- Параметры настройки BIOS для HW2000 Q2, Q3 (на стр. 89).

Пароли для защиты настроек BIOS должны удовлетворять следующим условиям:

- пароль должен состоять не менее чем из шести символов;
- пароль может быть сформирован из случайной парольной фразы с использованием генератора паролей ViPNet Password Generator;
- пароль должен содержать различные латинские и цифровые символы, использование трех и более идущих подряд одинаковых символов недопустимо.

Параметры настройки BIOS для HW100 X1, X2, X3, X8

Таблица 24. Параметры настройки BIOS для аппаратных платформ HW100 X1, X2

Пункт меню/подменю	Параметр	Значение	Примечание
Standard CMOS Features	Halt on	All but keyboard	
Advanced BIOS Features	Quick Power On Self Test	Disabled	
	Hard Disk Boot Priority	[1] — AFAYA CF 1Gb [2] — ST9160314AS	В качестве первого устройства для загрузки ОС должна быть указана карта памяти Compact Flash (AFAYA CF)
	First Boot Device	Hard Disk	
	Second Boot Device	Disabled	
	Third Boot Device	Disabled	
	Boot Other Device	Disabled	
Integrated Peripherals > OnChip IDE Device	IDE DMA transfer access	Disabled	
	PATA DMA Mode	Auto	
	IDE Primary Master UDMA	Disabled	
	IDE Primary Slave UDMA	Disabled	

Пункт меню/подменю	Параметр	Значение	Примечание
	IDE Secondary Master UDMA	Disabled	
	IDE Secondary Slave UDMA	Disabled	
Integrated Peripherals > USB Device Settings	USB 1.0 Controller	Enabled	
	USB 2.0 Controller	Enabled	
	USB Keyboard Function	Enabled	
	USB Storage Function	Enabled	
Set Supervisor Password			Необходимо задать пароль `vipnet`
Set User Password			Необходимо удалить пароль, если он задан

Таблица 25. Параметры настройки BIOS для аппаратных платформ HW100 X3, X8

Пункт меню/подменю	Параметр	Значение	Примечание
Standard CMOS Features	Halt on	All but keyboard	
Avanced BIOS Features	Quick Power On Self Test	Disabled	
	Hard Disk Boot Priority	[1] — mSATA mini 3SE [2] — ST9250315AS	В качестве первого устройства для загрузки ОС должен быть указан твердотельный накопитель SSD (mSATA mini 3SE)
	First Boot Device	Hard Disk	
	Second Boot Device	Disabled	
	Third Boot Device	Disabled	
	Boot Other Device	Disabled	
	Hyper-Threading Technology	Enabled	
Integrated Peripherals > OnChip IDE Device	IDE DMA transfer access	Disabled	
	IDE Primary Master UDMA	Disabled	

Пункт меню/подменю	Параметр	Значение	Примечание
	IDE Primary Slave UDMA	Disabled	
	IDE Secondary Master UDMA	Disabled	
	IDE Secondary Slave UDMA	Disabled	
Integrated Peripherals > USB Device Settings	USB 1.0 Controller	Enabled	
	USB 2.0 Controller	Enabled	
	USB Keyboard Function	Enabled	
	USB Storage Function	Enabled	
Set Supervisor Password			Необходимо задать пароль `vipnet`
Set User Password			Необходимо удалить пароль, если он задан

Параметры настройки BIOS для HW1000 Q2, Q3

Таблица 26. Параметры настройки BIOS для аппаратных платформ HW1000 Q2, Q3

Пункт меню/подменю	Параметр	Значение	Примечание
Main > Storage Configuration	SATA Configuration	Enhanced	
	Configure SATA as	AHCI	
Advanced > Onboard Devices Configuration	Onboard LAN1 Boot ROM	Disabled	
	Onboard LAN2 Boot ROM	Disabled	
	Interrupt 19 Capture	Disabled	
Advanced > ACPI Configuration > Advanced ACPI Configuration	Headless Mode	Disabled	
Advanced > CPU Configuration	Intel Virtualization Technology	Disabled	
Server > Remote Access Configuration	Remote Access	Disabled	

Пункт меню/подменю	Параметр	Значение	Примечание
Boot > Hard Disk Drives	1st Drive	[HDD: PO-CSS ...]	В качестве первого накопителя должен быть указан SSD-диск
Boot > Boot Device Priority	1st Boot Device	[HDD: PO-CSS ...]	В качестве первого устройства для загрузки ОС должен быть указан первый накопитель (то есть SSD-диск)
	2nd Boot Device	Disabled	Второе устройство должно быть отключено
Boot > Boot Settings Configuration	Quick boot	Disabled	
Boot > Security	Password Check	Setup	
	Change Supervisor Password		Необходимо задать пароль `vipnet`
	Change User Password		Необходимо удалить пароль, если он задан

Параметры настройки BIOS для HW2000 Q2, Q3

Таблица 27. Параметры настройки BIOS для аппаратной платформы HW2000 Q2

Пункт меню/подменю	Параметр	Значение	Примечание
Main > IDE Configuration	SATA Configuration	Enhanced	
	Configure SATA as	AHCI	
Advanced > CPU Configuration	Intel Virtualization Tech	Disabled	
	Intel(R) HT Technology	Enabled	
Advanced Legacy Device Configuration	Onboard floppy controller	Disabled	
Advanced > Power On Configuration	Restore on AC Power Loss	Power On	
Advanced > CPU Configuration	Intel Virtualization Technology	Disabled	

Пункт меню/подменю	Параметр	Значение	Примечание
Server > Remote Access Configuration	Remote Access	Disabled	
Boot > Hard Disk Drives	1st Drive	[SATA: PM-TS2GS …]	В качестве первого накопителя должен быть указан SSD-диск
Boot > Boot Device Priority	1st Boot Device	[[SATA: PM-TS2GS …]	В качестве первого устройства для загрузки ОС должен быть указан первый накопитель (то есть SSD-диск)
	2nd Boot Device	Disabled	Второе устройство должно быть отключено
Boot > Boot Settings Configuration	Quick boot	Disabled	
Boot > Security	Password Check	Setup	
	Change Supervisor Password		Необходимо задать пароль `vipnet`
	Change User Password		Необходимо удалить пароль, если он задан

Таблица 28. Параметры настройки BIOS для аппаратной платформы HW2000 Q3

Пункт меню/подменю	Параметр	Значение	Примечание
Advanced > CPU Configuration	Intel Virtualization Technology	Disabled	
	Hyper-threading	Enabled	
Advanced > Chipset Configuration > CPU IIO Bridge Configuration	VGA Priority	Onboard	
Advanced > Chipset Configuration > Intel(R) VT for Directed I/O Configuration	VT-d	Disabled	
Advanced > Trusted Computing	TPM Support	Disabled	
	Security Device Support	Disabled	

Пункт меню/подменю	Параметр	Значение	Примечание
Advanced > ACPI Settings	Enable Hibernation	Disabled	
Advanced > NCT6779D Super IO Configuration	Serial Port 2 Configuration	Disabled	
Advanced > Intel LAN I210 Configuration	Intel LAN ROM Type	Disabled	
Advanced > APM	Restore AC Power Loss	Power On	
Advanced > Serial Port Console Redirection	COM1 Console Redirection COM2 Console Redirection	Disabled Disabled	
Advanced > Onboard LAN Configuration	Intel W82574L OpROM[1-4]	Disabled	
Advanced > PCI Subsystem Settings	Load RT32 Image	Disabled	
Advanced > Network Stack Configuration	Network Stack Configuration	Disabled	
Advanced > USB Configuration	USB Mass Storage Driver Support	Disabled	
IntelRCSetup > IIO Configuration > PCIE Slot Option Rom Configuration	PCIE1 Option Rom PCIE2 Option Rom PCIE6 Option Rom MEZZ1 Option Rom	Disabled Disabled Disabled Disabled	
IntelRCSetup	Intel VT for Directed I/O (VT-d)	Disabled	
IntelRCSetup > Runtime Error Logging	WHEA Settings	Disabled	
Boot	Boot Device Seeking	Normal	
	Boot Option #1	[SATA P1: 2Gb SATA...]	В качестве первого устройства для загрузки ОС должно быть указано HDD-устройство
	Boot Option #2	Disabled	
	Boot Logo Display	Disabled	

Пункт меню/подменю	Параметр	Значение	Примечание
Boot > CD/DVD ROM Drive BBS Priorities	Boot Option #1	Disabled	
Boot > Floppy Drive BBS Priorities	Boot Option #1	Disabled	
Boot > CSM Parameters	Launch CSM	Always	
	Launch PXE OpROM policy	Do not launch	
	Launch Storage OpROM policy	Do not launch	
Security	Administrator Password		Необходимо задать пароль vipnet
	User Password		Необходимо удалить пароль, если он задан
Security > Secure Boot menu	Secure Boot	Disabled	

5

Возможности управления ViPNet Coordinator HW

Способы управления ViPNet Coordinator HW

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

- Административное программное обеспечение ViPNet — программы ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 107) и ViPNet Policy Manager (см. глоссарий, стр. 107).

  Выполнение настроек в ЦУСе облегчает управление ViPNet Coordinator HW и позволяет оповестить об изменении параметров сетевые узлы ViPNet, связанные с ViPNet Coordinator HW, путем отправки на эти узлы справочников и ключей. Программа Policy Manager позволяет централизованно управлять встроенными сетевыми экранами узлов, в том числе координаторов ViPNet Coordinator HW (см. Управление с помощью административного ПО ViPNet на стр. 99).

- Веб-интерфейс.

  Вы можете подключиться с удаленного компьютера и настроить ViPNet Coordinator HW с помощью веб-браузера. Возможности управления ViPNet Coordinator HW с помощью веб-интерфейса ограничены (см. Управление с помощью веб-интерфейса на стр. 101).

- Командный интерпретатор ViPNet Coordinator HW.

  Вы можете использовать командную оболочку ViPNet локально или удаленно через протокол SSH. Командный интерпретатор предоставляет наиболее полные возможности по администрированию ViPNet Coordinator HW (см. Управление с помощью командного интерпретатора на стр. 103).

Полномочия при различных способах управления

Примечание. Microsoft Hyper-V и Oracle VM Server не поддерживают подключение USB-устройств к виртуальной машине. Поэтому аутентификация с помощью токена на этих платформах невозможна.

Таблица 29. Основные действия, доступные при различных способах управления ViPNet Coordinator HW

	Режимы подключения		
	Пользователь узла	**Администратор узла**	**Администратор сети**
	Доступ		
Интерфейс для управления ViPNet Coordinator HW	веб-интерфейс (удаленное управление) командный интерпретатор (локальное или удаленное управление)		программа ViPNet Центр управления сетью или ViPNet Policy Manager (удаленное управление)
Способ аутентификации	пароль пользователя или аутентификация с помощью токена	пароль пользователя, пароль администратора узла ViPNet	пароль администратора ViPNet Центр управления сетью или ViPNet Policy Manager
	Установка		
Локальное обновление ПО ViPNet	–	+	–
Удаленное обновление ПО ViPNet	–	–	+
	Обслуживание		
Настройка системных параметров	–	+	–
Настройка параметров сетевых интерфейсов	–	+	-
Настройка подключения к внешнему межсетевому экрану	–	+	+

	Режимы подключения		
	Пользователь узла	**Администратор узла**	**Администратор сети**
Настройка IP-адресов ViPNet Coordinator HW и туннелируемых им IP-адресов	–	+	+
Настройка встроенного межсетевого экрана	–	+	+
Запуск и завершение работы демонов и драйверов	+ (только для командного интерпретатора)	+	–
Настройка системных служб	–	+	–
Просмотр журналов и настроек	–	+	–

Режимы работы в командном интерпретаторе и веб-интерфейсе

Вы можете работать с командным интерпретатором и веб-интерфейсом ViPNet Coordinator HW в одном из двух режимов:

- Режим пользователя. Данный режим становится активным по умолчанию после аутентификации на ViPNet Coordinator HW (см. Способы аутентификации пользователя на стр. 98). При работе с командным интерпретатором или веб-интерфейсом в данном режиме пользователю недоступно изменение настроек ViPNet Coordinator HW. В командном интерпретаторе в качестве приглашения командной строки в этом режиме используется символ «>».
- Режим администратора. В этом режиме в командном интерпретаторе и веб-интерфейсе доступны все настройки. В командном интерпретаторе в качестве приглашения командной строки в этом режиме используется символ «#». Чтобы перейти в режим администратора, в командном интерпретаторе или веб-интерфейсе требуется авторизоваться с использованием пароля администратора сетевого узла.

Способы аутентификации пользователя

Прежде чем начать работу с ViPNet Coordinator HW с помощью командного интерпретатора или веб-интерфейса, требуется пройти аутентификацию. Возможно два способа аутентификации:

- «Пароль». При аутентификации требуется ввести имя учетной записи и пароль пользователя. Каждый раз при вводе пароля вычисляется парольный ключ, который используется для доступа к вашему персональному ключу (см. глоссарий, стр. 110).
- «Устройство». При аутентификации требуется ввести имя учетной записи, подключить устройство, на котором сохранен персональный ключ, и ввести ПИН-код доступа к устройству. Этот способ аутентификации применим только при подключении к ViPNet Coordinator HW с помощью обычной (см. глоссарий, стр. 110) или COM-консоли (см. глоссарий, стр. 105).

Внимание! В текущей версии ViPNet Coordinator HW для аутентификации могут использоваться только внешние устройства Rutoken Lite производства компании «Актив».

Способ аутентификации задается администратором сети в программе ViPNet Удостоверяющий и ключевой центр. Впоследствии он может быть изменен на самом ViPNet Coordinator HW с помощью командного интерпретатора. Причем изменить способ аутентификации на ViPNet Coordinator HW можно только на «Устройство». Изменение способа аутентификации с «Устройство» на «Пароль» запрещено по требованиям безопасности. Подробнее об изменении способа аутентификации см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».

При локальном подключении к ViPNet Coordinator HW аутентификация производится в командном интерпретаторе (см. Управление с помощью командного интерпретатора на стр. 103).

При подключении через веб-интерфейс (см. Управление с помощью веб-интерфейса на стр. 101) или удаленном подключении по протоколу SSH (см. Удаленное подключение с помощью протокола SSH на стр. 104) аутентификация состоит из двух этапов:

1. Сначала в соответствии с заданным способом выполняется аутентификация в ПО ViPNet, которое установлено на удаленном рабочем месте для защиты канала передачи данных с ViPNet Coordinator HW.
2. Затем выполняется аутентификация по паролю при непосредственном подключении к ViPNet Coordinator HW через веб-интерфейс или по протоколу SSH.

Управление с помощью административного ПО ViPNet

Для удаленной настройки параметров ViPNet Coordinator HW может использоваться следующее управляющее программное обеспечение ViPNet:

- ViPNet Центр управления сетью (ЦУС) (см. глоссарий, стр. 107).

  Данная программа, входящая в состав программного комплекса ViPNet Administrator (см. глоссарий, стр. 107), предназначена для формирования структуры сети ViPNet, задания основных параметров сетевых узлов, централизованной отправки справочников, ключей и программного обеспечения на сетевые узлы ViPNet (подробнее см. в документе «ViPNet Центр управления сетью. Руководство администратора»).

  В ЦУСе администратор сети ViPNet может настроить адреса доступа к ViPNet Coordinator HW, параметры подключения узла ViPNet Coordinator HW к внешней сети через межсетевой экран, адреса туннелируемых узлов. Настройки, выполненные в ЦУСе, применяются на узле ViPNet Coordinator HW после установки полученного доверенным способом файла `*.dst`, либо после получения справочников или ключей на этом узле по сети ViPNet.

- ViPNet Policy Manager (см. глоссарий, стр. 107).

  Данная программа предназначена для формирования политик безопасности (см. глоссарий, стр. 110) и их рассылки на узлы по сети ViPNet (подробнее см. в документе «ViPNet Policy Manager. Руководство администратора»). Политики безопасности могут включать в себя сетевые фильтры и правила трансляции IP-адресов. Фильтры и правила трансляции, полученные из программы ViPNet Policy Manager, недоступны для редактирования на узлах.

Работа с учетной записью пользователя ViPNet Coordinator HW

Чтобы удалить учетную запись пользователя, а также все настройки и справочно-ключевую информацию ViPNet Coordinator HW, выполните команду:

```
hostname# admin remove keys
```

Примечание. Вы можете выполнить эту команду только при подключении к ViPNet Coordinator HW через обычную или COM-консоль. Выполнение команды в удаленной SSH-сессии невозможно.

Чтобы сменить пароль пользователя ViPNet Coordinator HW, выполните команду:

```
hostname# admin passwd
```

Внимание! Все действия над учетной записью пользователя необходимо выполнять только локально на ViPNet Coordinator HW. Любые действия над учетной записью пользователя сетевого узла ViPNet Coordinator HW после установки дистрибутива ключей, выполняемые в ЦУС (смена пароля, удаление, добавление новых пользователей и другие), запрещены, так как могут привести к неработоспособности ViPNet Coordinator HW.

Управление с помощью веб-интерфейса

Для удаленного управления и частичной настройки ViPNet Coordinator HW вы можете использовать веб-интерфейс, который входит в его состав. С помощью веб-интерфейса ViPNet Coordinator HW вы можете выполнять следующие действия:

- Настройка даты и времени.
- Настройка подключения ViPNet Coordinator HW к сети: настройка сетевых интерфейсов, параметров подключения к сетям 3G, Wi-Fi.
- Управление межсетевым экраном путем настройки сетевых фильтров и правил трансляции адресов.
- Настройка туннелирования адресов.
- Настройка сетевых служб: встроенного DHCP-, DNS-, NTP- и прокси-сервера, DHCP-relay.
- Настройка защиты соединения по технологии L2OverIP.
- Настройка статической и динамической маршрутизации.
- Настройка функции MultiWAN.
- Работа со списком сетевых узлов ViPNet.
- Настройка параметров удаленного мониторинга по протоколу SNMP.
- Мониторинг состояния ViPNet Coordinator HW, настройка параметров протоколирования событий, просмотр системного журнала, журналов регистрации IP-пакетов, транспортных конвертов, переключений режимов кластера (в режиме кластера).

Подключение к веб-интерфейсу ViPNet Coordinator HW следует осуществлять только с других защищенных узлов ViPNet, связанных с ним. Связи между узлами сети ViPNet задаются в программе ViPNet Центр управления сетью — ЦУС.

Внимание! Предоставлять удаленный доступ к ViPNet Coordinator HW с незащищенных узлов запрещено. С помощью фильтров защищенной сети следует ограничить соединения между ViPNet Coordinator HW и рабочими местами администраторов, разрешив только удаленное управление и передачу данных по служебным протоколам ViPNet.

Возможно одновременное подключение к ViPNet Coordinator HW с нескольких защищенных узлов. Одновременно с веб-интерфейсом могут работать не более 5 пользователей, причем только один из них — в режиме администратора.

Примечание. Для подключения к веб-интерфейсу ViPNet Coordinator HW используйте браузеры Internet Explorer 11, Microsoft Edge, Google Chrome и Mozilla Firefox последних версий. В настройка браузера укажите следующие разрешения:

- разрешить сайтам сохранять и просматривать данные файлов Cookie;
- разрешить загружать с сайта и выполнять сценарии JavaScript.

Установите разрешение экрана 1360x768 пикселей или выше.

После обновления ViPNet Coordinator HW с предыдущей версии рекомендуется очистить кэш браузера. В противном случае возможны проблемы с подключением и использованием веб-интерфейса.

Подробнее о работе с веб-интерфейсом см. в документе «ViPNet Coordinator HW. Настройка с помощью веб-интерфейса».

Управление с помощью командного интерпретатора

Командный интерпретатор обеспечивает наиболее полные возможности администрирования ViPNet Coordinator HW по сравнению с другими вариантами управления. С помощью командного интерпретатора ViPNet вы можете выполнять следующие действия:

- Настройка системных функций ViPNet Coordinator HW: настройка даты и времени, создание копий конфигурации и другое.
- Настройка подключения ViPNet Coordinator HW к сети, настройка сетевых интерфейсов, параметров подключения к сетям 3G, Wi-Fi.
- Настройка режимов подключения ViPNet Coordinator HW 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, работа со списком сетевых узлов ViPNet 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-, NTP- и прокси-сервера, DHCP-relay.
- Настройка статической и динамической маршрутизации.
- Настройка системы защиты от сбоев.
- Настройка функции MultiWAN.
- Резервирование справочников, ключей и настроек ViPNet Coordinator HW, обновление ViPNet Coordinator HW.
- Настройка параметров протоколирования событий, просмотр системного журнала, журналов регистрации IP-пакетов, транспортных конвертов.
- Настройка параметров удаленного мониторинга по протоколу SNMP и другое.

Командный интерпретатор запускается автоматически после аутентификации пользователя ViPNet Coordinator HW. При этом он может быть запущен как локально с помощью COM-консоли (см. глоссарий, стр. 105) или обычной консоли (см. глоссарий, стр. 110), так и удаленно при подключении с других узлов сети ViPNet, связанных с ViPNet Coordinator HW, по протоколу SSH (см. Удаленное подключение с помощью протокола SSH на стр. 104).

Подробнее о настройке и обновлении ПО ViPNet Coordinator HW с помощью командного интерпретатора, а также об остальных операциях в командном интерпретаторе см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора».

Удаленное подключение с помощью протокола SSH

Настройку и управление ViPNet Coordinator HW с помощью командного интерпретатора можно производить не только через локальную консоль, но также с помощью удаленного подключения по протоколу SSH. Удаленное подключение к ViPNet Coordinator HW следует осуществлять только с других защищенных узлов ViPNet, связанных с ним. Связи между узлами сети ViPNet задаются в программе ViPNet Центр управления сетью — ЦУС.

Внимание! Предоставлять удаленный доступ к ViPNet Coordinator HW с незащищенных узлов запрещено. С помощью фильтров защищенной сети следует ограничить соединения между ViPNet Coordinator HW и рабочими местами администраторов, разрешив только удаленное управление и передачу данных по служебным протоколам ViPNet.

Возможно одновременное подключение к ViPNet Coordinator HW с нескольких узлов.

Примечание. При этом одновременно может быть запущено ограниченное количество удаленных сессий. Ограничения зависят от исполнения ViPNet Coordinator HW:

- 5 удаленных сессий — для всех исполнений HW50 и HW100.
- 30 удаленных сессий — для остальных исполнений ViPNet Coordinator HW.

Только в одной удаленной сессии можно работать в режиме администратора (независимо от исполнения).

Подробнее об удаленном подключении и его особенностях см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», в разделе «Работа с командным интерпретатором».

A

Глоссарий

COM-консоль

Ноутбук, подключенный к COM-порту, который используется для локальной настройки ViPNet Coordinator HW.

DAD (Duplicate address detection)

Duplicate address detection (обнаружение дублирования адреса) — метод проверки уникальности IP-адреса с помощью отправки специального ARP-запроса с указанием проверяемого IP-адреса и ожиданием ответа от этого IP-адреса. Результатом является получение от устройства с указанным IP-адресом ответа. Если в течение определенного времени ответ не поступил, считается, что такой адрес в сети не используется.

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.

DHCP-сервер

Сервер, автоматически администрирующий IP-адреса DHCP-клиентов и выполняющий соответствующую настройку для сети.

DiffServ (Differentiated Service)

Протокол, обеспечивающий классификацию сетевого трафика при помощи DSCP-меток, добавляемых в заголовки IP-пакетов.

DNS-сервер

Сервер, содержащий часть базы данных DNS, используемой для доступа к именам сетевых узлов в интернет-домене. Например, ns.domain.net. Как правило, информация о домене хранится на двух DNS-серверах, называемых «Primary DNS» и «Secondary DNS» (дублирование делается для повышения отказоустойчивости системы).

Также DNS-сервер называют сервером доменных имен, сервером имен DNS.

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 сети 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.

MTU (Maximum Transmission Unit)

Максимальный размер полезного блока данных пакета, который может быть передан через сетевой интерфейс без фрагментации.

NTP-сервер

Сервер точного времени, который необходим для синхронизации времени компьютеров, рабочих станций, серверов и прочих сетевых устройств. Этот сервер играет роль посредника между эталоном времени и сетью. Он получает время от эталона по специальному каналу (интерфейсу) и выдает его для любого узла сети, обеспечивая тем самым синхронизацию устройств.

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.

PPP (Point-to-Point Protocol)

Протокол канального уровня, использующийся для установления прямой связи между двумя узлами сети.

TCP-туннель

Способ соединения клиентов ViPNet, находящихся во внешних сетях, со своим сервером соединений, а затем и с другими узлами сети ViPNet по протоколу TCP. Используется в том случае, если соединение по протоколу UDP заблокировано провайдерами услуг интернета.

TCP-туннель настраивается на координаторе, который является для клиента сервером соединений.

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 для централизованного управления политиками безопасности узлов защищенной сети ViPNet.

ViPNet Центр управления сетью (ЦУС)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

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

Административная дистанция

Характеристика маршрута. Позволяет определить меру доверия к маршруту. Задается для любого маршрута в виде целого числа в диапазоне от 1 до 255.

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).

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла. Виртуальные IP-адреса узлу ViPNet (Б) назначаются непосредственно на узле А. На других узлах узлу ViPNet (Б) могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если сетевые узлы ViPNet работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удаленных узлов в приложениях ViPNet.

Динамический сетевой интерфейс

Разновидность сетевого интерфейса, который добавляется в процессе работы при наступлении некоторого события (например, при подключении встроенного или USB-модема, предоставляющего данный интерфейс).

Динамические интерфейсы объединяются в группы по типу интерфейса. Поэтому иногда может встречаться термин «групповой динамический интерфейс».

Существуют следующие группы динамических интерфейсов:

- `ppp` — группа интерфейсов для подключения к мобильной сети через встроенный модем;
- `wifi` — группа интерфейсов для подключения к беспроводной сети Wi-Fi с помощью внешних адаптеров Wi-Fi. В эту группу не входит встроенный интерфейс `wlan0` (для исполнений ПАК со встроенным модулем Wi-Fi).

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.

Защищенный узел

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

Клиент (ViPNet-клиент)

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

Ключи узла ViPNet

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

Компрометация ключей

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Координатор (ViPNet-координатор)

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

Маршрут по умолчанию

Путь следования IP-пакетов, для которых не был найден подходящий маршрут в таблице маршрутизации.

Маршрутизация

Процесс выбора пути для передачи информации в сети.

Мастер-ключ

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

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

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

Межсетевой экран

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

Метрика маршрута

Параметр, определяющий приоритет маршрута передачи IP-трафика.

Обычная консоль

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

Открытый интернет (Защищенный интернет-шлюз)

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

Начиная с версии ПО ViPNet Administrator ЦУС 4.6.3, технология «Открытый Интернет» называется «Защищенный интернет-шлюз».

Открытый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Пароль пользователя

Индивидуальный пароль пользователя для работы в приложениях ViPNet на сетевом узле ViPNet. Первоначально создается администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager. Этот пароль может быть изменен пользователем на сетевом узле ViPNet.

Персональный ключ пользователя

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

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 сетевых 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 устройствами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Справочники и ключи

Справочники, ключи узла и ключи пользователя.

Статический сетевой интерфейс

Сетевой интерфейс, для работы которого требуется задать секцию `[adapter]` в файле `iplir.conf` с описанием параметров этого интерфейса. К таким интерфейсам относятся физические (Ethernet) и виртуальные (VLAN) интерфейсы.

Трансляция сетевых адресов (NAT)

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

Транспортная квитанция

Файл, оповещающий отправителя о невозможности доставки конверта.

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.

Шлюзовой координатор

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