



ViPNet Coordinator HW 4

Подготовка к работе



1991–2016 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00130-03 90 02

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

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

VIPNet® является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

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

ОАО «ИнфоТеКС»

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

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

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

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение.....	5
О документе.....	6
Для кого предназначен документ	6
Соглашения документа.....	6
Связанные документы	8
О программно-аппаратном комплексе ViPNet Coordinator HW.....	9
Подготовка ViPNet Coordinator HW к работе.....	10
Обратная связь.....	11
Глава 1. Развертывание виртуального образа ViPNet Coordinator HW.....	12
Требования к виртуальной среде.....	13
Установка ViPNet Coordinator HW-VA на платформу виртуализации	14
VMware vSphere ESXi.....	14
Oracle VM VirtualBox.....	19
Глава 2. Установка, обновление и удаление справочников и ключей.....	22
Способы установки и подготовка к установке справочников и ключей.....	23
Подготовка к установке справочников и ключей с помощью ноутбука по Ethernet-каналу и протоколу TFTP	24
Подготовка к установке справочников и ключей с помощью внешнего устройства	26
Установка справочников и ключей	27
Начало установки.....	27
Настройка часового пояса, даты и времени.....	28
Установка дистрибутива ключей на ViPNet Coordinator HW.....	30
Настройка сетевых интерфейсов.....	32
Настройка DNS-сервера	33
Настройка NTP-сервера	34
Настройка имени компьютера и диапазона виртуальных адресов.....	35
Настройка подключения к внешней сети через межсетевой экран	36
Проверка связи с другим сетевым узлом.....	40
Завершение установки	42
Обновление и удаление справочников и ключей	43
Глава 3. Обновление программного обеспечения	45
Особенности обновления ПО.....	46

Удаленное обновление ПО.....	47
Локальное обновление ПО.....	48
Обновление ПО ViPNet Coordinator HW на кластере горячего резервирования.....	50
Конвертация правил открытой и защищенной сети.....	52
Конвертация правил открытой сети при обновлении до версии 4.x.....	52
Конвертация правил защищенной сети при обновлении до версии 4.x.....	55
Совместимость ПО ViPNet Coordinator HW версий 3.x.....	58
Глава 4. Резервное копирование и восстановление настроек.....	59
Назначение экспорта и импорта справочников, ключей и настроек.....	60
Экспорт справочников, ключей и настроек.....	62
Импорт справочников, ключей и настроек.....	64
Глава 5. Замена элемента питания CMOS BIOS и установка SIM-карты.....	66
Замена элемента питания CMOS BIOS.....	67
Настройка параметров BIOS.....	72
Параметры настройки BIOS для ViPNet Coordinator HW1000.....	73
Параметры настройки BIOS для ViPNet Coordinator HW2000 Q3.....	76
Установка SIM-карты в ViPNet Coordinator HW50 N3 и HW100 N3.....	78
Приложение А. Глоссарий.....	80
Приложение В. Указатель.....	83



Введение

О документе	6
Связанные документы	8
О программно-аппаратном комплексе ViPNet Coordinator HW	9
Подготовка ViPNet Coordinator HW к работе	10
Обратная связь	11

О документе

В данном документе описан порядок действий по подготовке ViPNet Coordinator HW к использованию, а также развертывание виртуального образа ViPNet Coordinator HW, основные сценарии работы со справочниками и ключами узла, порядок обновления ПО, резервное копирование и восстановление настроек.

Для кого предназначен документ

Документ предназначен для администраторов, которые отвечают за эксплуатацию и сопровождение 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.
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# команда
```

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

```
hostname> команда
```

- Параметры, которые должны быть заданы пользователем, заключены в угловые скобки. Например:

```
команда <параметр>
```

- Необязательные параметры или ключевые слова заключены в квадратные скобки. Например:

```
команда <обязательный параметр> [необязательный параметр]
```

- Если при вводе команды можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой. Например:

```
команда {вариант-1 | вариант-2}
```

Связанные документы

В таблице ниже перечислены документы, входящие в комплект документации ViPNet Coordinator HW, помимо данного документа.

Таблица 3. Связанные документы

Документ	Содержание
«ViPNet Coordinator HW. Общее описание»	Описание общей информации по ViPNet Coordinator HW, а также существующих исполнений и характеристик аппаратных конфигураций
«ViPNet Coordinator HW. Настройка с помощью командного интерпретатора»	Описание основных сценариев настройки ViPNet Coordinator HW с помощью командного интерпретатора, работы с журналами и мониторинга ViPNet Coordinator HW
«ViPNet Coordinator HW. Настройка с помощью веб-интерфейса»	Описание основных сценариев настройки ViPNet Coordinator HW с помощью веб-интерфейса
«ViPNet Coordinator HW. Сценарии работы»	Описание практических сценариев использования ViPNet Coordinator HW, которые требуют комплексного применения различных команд и базовых схем настройки ViPNet Coordinator HW
«ViPNet Coordinator HW. Справочное руководство по командному интерпретатору»	Описание команд ViPNet Coordinator HW
«ViPNet Coordinator HW. Справочное руководство по конфигурационным файлам»	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

О программно-аппаратном комплексе ViPNet Coordinator HW

Программно-аппаратный комплекс ViPNet Coordinator HW представляет собой интегрированное решение на базе специализированной аппаратной платформы и программного обеспечения ViPNet, которое функционирует под управлением адаптированной ОС GNU/Linux.

ViPNet Coordinator HW выступает в роли VPN-сервера и предназначен для использования в IP-сетях, защита которых организуется с применением комплекса программных продуктов ViPNet.

ViPNet Coordinator HW в сети ViPNet реализует функции координатора, а также ряд дополнительных функций.

Описание всех функций ViPNet Coordinator HW см. в документе «ViPNet Coordinator HW. Общее описание».

Подготовка ViPNet Coordinator HW к работе

Для подготовки ViPNet Coordinator HW к эксплуатации выполните все действия из приведенной ниже таблицы в предложенном порядке.

Таблица 4. Порядок действий при подготовке ViPNet Coordinator HW к работе

Действие	Ссылка
<input type="checkbox"/> Установите и подключите ViPNet Coordinator HW к питанию и сетевому оборудованию. Если вы используете исполнение ViPNet Coordinator HW-VA, установите виртуальный образ на компьютер.	Развертывание виртуального образа ViPNet Coordinator HW (на стр. 12)
<input type="checkbox"/> Получите дистрибутив ключей сетевого узла (файл *.dst) и пароль у администратора вашей сети ViPNet.	
<input type="checkbox"/> Включите ViPNet Coordinator HW.	
<input type="checkbox"/> Выберите способ установки ключей и выполните необходимые подготовительные действия перед установкой.	Способы установки и подготовка к установке справочников и ключей (на стр. 23) Подготовка к установке справочников и ключей с помощью ноутбука по Ethernet-каналу и протоколу TFTP (на стр. 24) Подготовка к установке справочников и ключей с помощью внешнего устройства (на стр. 26)
<input type="checkbox"/> Установите на ViPNet Coordinator HW справочники и ключи.	Установка справочников и ключей (на стр. 27)
<input type="checkbox"/> Во время установки справочников и ключей выполните все необходимые настройки ViPNet Coordinator HW.	



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

Обратная связь

Дополнительная информация

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

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

Контактная информация

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

- Техническая поддержка для пользователей продуктов ViPNet: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки <http://www.infotecs.ru/support/request/>.
- Консультации по телефону для клиентов, имеющих расширенный уровень технического сопровождения:

8 (495) 737-6196,

8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

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

1

Развертывание виртуального образа ViPNet Coordinator HW

Требования к виртуальной среде	13
Установка ViPNet Coordinator HW-VA на платформу виртуализации	14

Требования к виртуальной среде

ViPNet Coordinator HW имеет программное виртуализированное решение — ПО ViPNet Coordinator HW-VA, предназначенное для развертывания координатора на виртуальной машине.

Преимуществом ViPNet Coordinator HW-VA является его независимость от изменений аппаратной платформы.

ViPNet Coordinator HW-VA можно установить на следующие платформы виртуализации, поддерживающие стандарт OVF (Open Virtualization Format):

- VMware vSphere 5.x (рекомендуемая версия — 5.5.0).
- VMware Workstation 11.x (рекомендуемая версия — 11.0.0).
- Oracle VM VirtualBox 4.x (рекомендуемая версия — 4.3.28).

Работа на других платформах виртуализации не гарантируется.

Виртуальная машина, на которую устанавливается ViPNet Coordinator HW-VA, должна быть сконфигурирована следующим образом:

- Процессор — один с количеством ядер 2.
- Объем оперативной памяти — не менее 2 Гбайт.
- Накопители — 2 диска: HDD не менее 2 Гбайт, HDD не менее 80 Гбайт.
- Сетевые интерфейсы — не менее 2.

Сетевому узлу, на который устанавливается ПО ViPNet Coordinator HW-VA, в программе ViPNet Центр управления сетью (далее — ЦУС) должна быть назначена роль «Coordinator HW-VA».

Установка ViPNet Coordinator HW-VA на платформу виртуализации

Для установки ViPNet Coordinator HW-VA на платформу виртуализации вам потребуется файл с образом виртуальной машины (файл с расширением *.ova), который входит в комплект поставки.

В следующих разделах приведены примеры установки ViPNet Coordinator HW-VA на следующие платформы виртуализации: [VMware vSphere ESXi](#) (на стр. 14) и [Oracle VM VirtualBox](#) (на стр. 19).

VMware vSphere ESXi

Для установки ViPNet Coordinator HW-VA на платформу виртуализации VMware vSphere ESXi выполните следующие действия:

- 1 В главном окне программы vSphere Client в меню **File** выберите пункт **Deploy OVF Template**. Откроется окно **Deploy OVF Template**, которое представляет собой мастер развертывания виртуальных машин из образов формата OVF.



Примечание. Если в меню **File** нет пункта **Deploy OVF Template**, убедитесь, что установлено расширение Client Integration (http://pubs.vmware.com/vsphere-55/index.jsp#com.vmware.vsphere.vm_admin.doc/GUID-3FC8F86B-7F4A-450C-9D1F-0275E403F71C.html#GUID-3FC8F86B-7F4A-450C-9D1F-0275E403F71C), добавляющее поддержку образов формата OVF.

- 2 На странице **OVF Template Details** ознакомьтесь с параметрами виртуальной машины и убедитесь, что на ваших накопителях достаточно свободного места для развертывания.
- 3 На странице **Source** укажите путь к файлу с расширением *.ova, содержащему образ виртуальной машины.

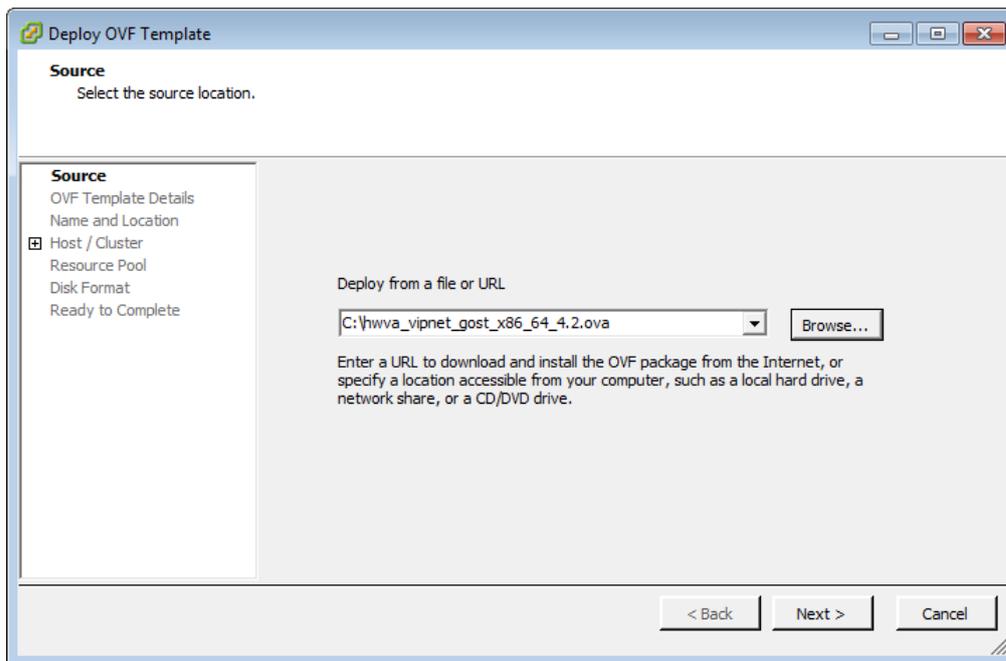


Рисунок 1. Задание файла с образом виртуальной машины

4 На странице **Name and Location** выполните следующие действия:

- В поле **Name** измените, если необходимо, имя виртуальной машины.



Примечание. Имена виртуальных машин в папке не должны повторяться.

- Выберите папку, в которой будет располагаться виртуальная машина.

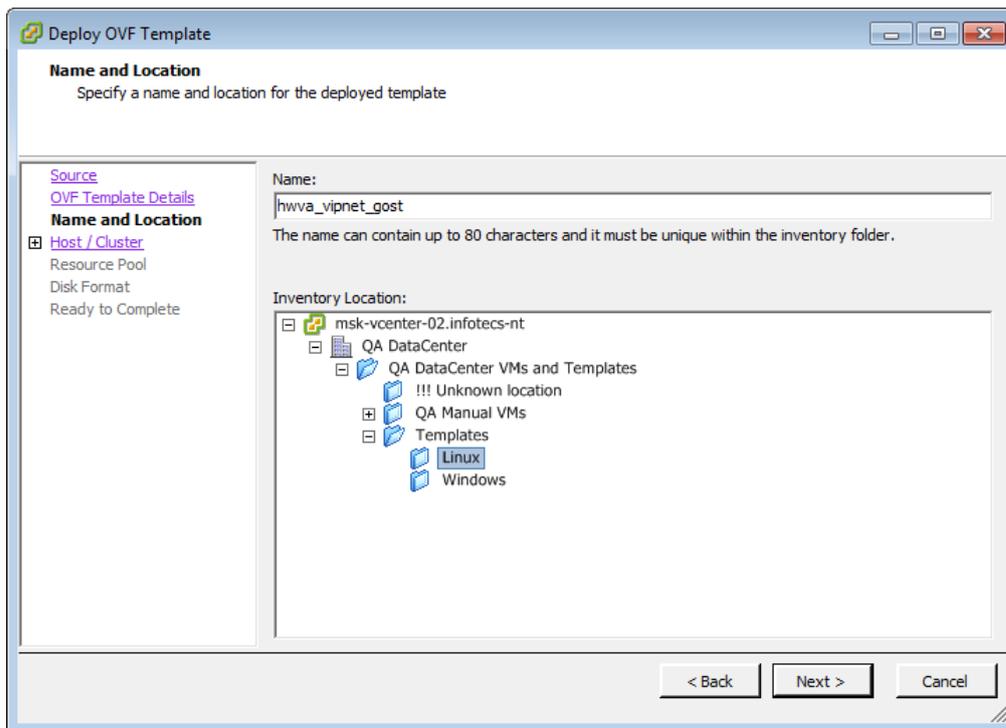


Рисунок 2. Задание имени и расположения виртуальной машины

- 5 При наличии на левой панели соответствующих пунктов выполните следующие действия:
 - 5.1 На странице **Host / Cluster** укажите сетевой узел, на котором будут храниться файлы виртуальной машины.
 - 5.2 На странице **Resource Pool** выберите «пул ресурсов», то есть группу носителей информации, выделяемых для хранения файлов виртуальной машины.

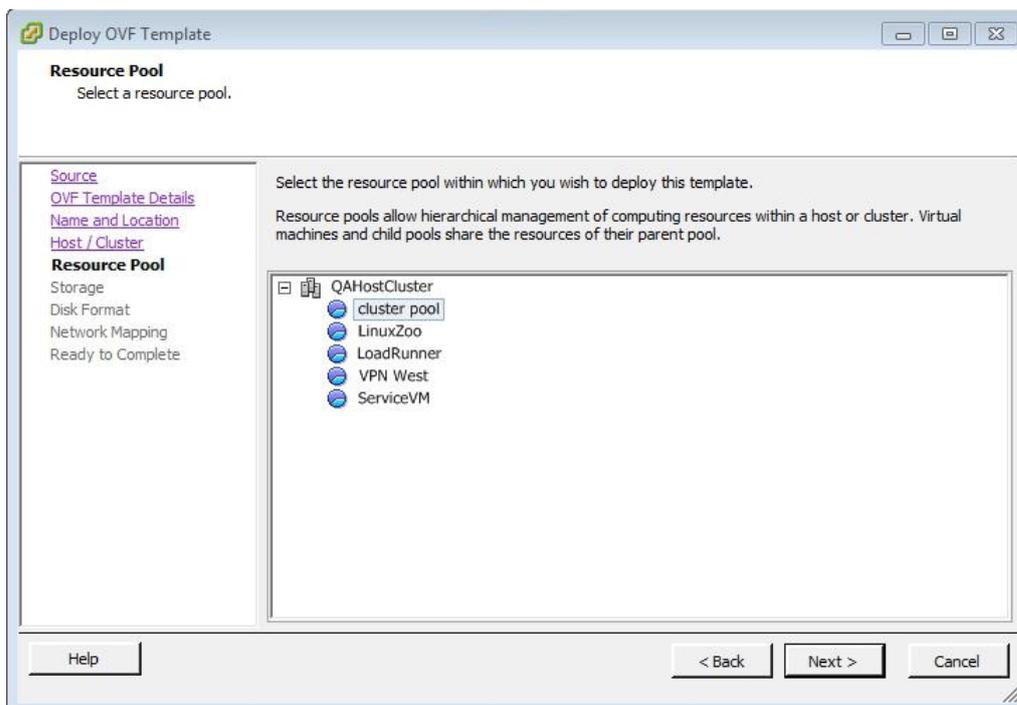


Рисунок 3. Выбор пула ресурсов

5.3 На странице **Storage** укажите жесткий диск или твердотельный накопитель из выбранного пула ресурсов, на котором будут храниться файлы виртуальной машины.

- 6 На странице **Disk Format** выберите необходимый формат виртуального диска (например, при выборе формата **Thin Provision** файл с виртуальным диском имеет переменный размер — файл увеличивается или уменьшается в зависимости от размера содержимого виртуального диска).

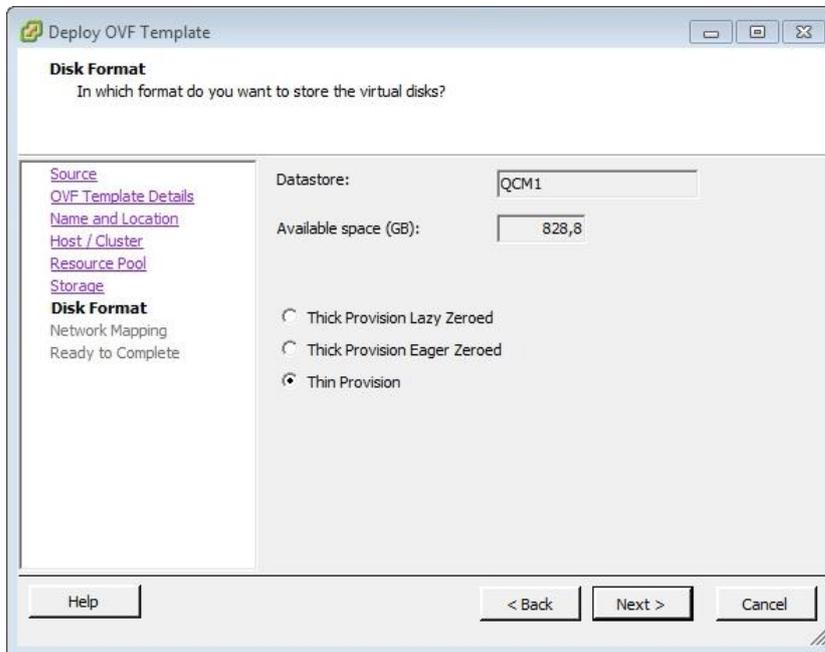


Рисунок 4. Выбор формата виртуального диска

- 7 На странице **Network Mapping** задайте физический или виртуальный сетевой коммутатор ESXi, который будет по умолчанию сопоставлен всем сетевым интерфейсам вашей виртуальной машины. Для этого сопоставьте его сети bridged. Впоследствии вам будет нужно сопоставить физический или виртуальный сетевой коммутатор каждому из сетевых интерфейсов ViPNet Coordinator HW-VA (см. шаг 10).

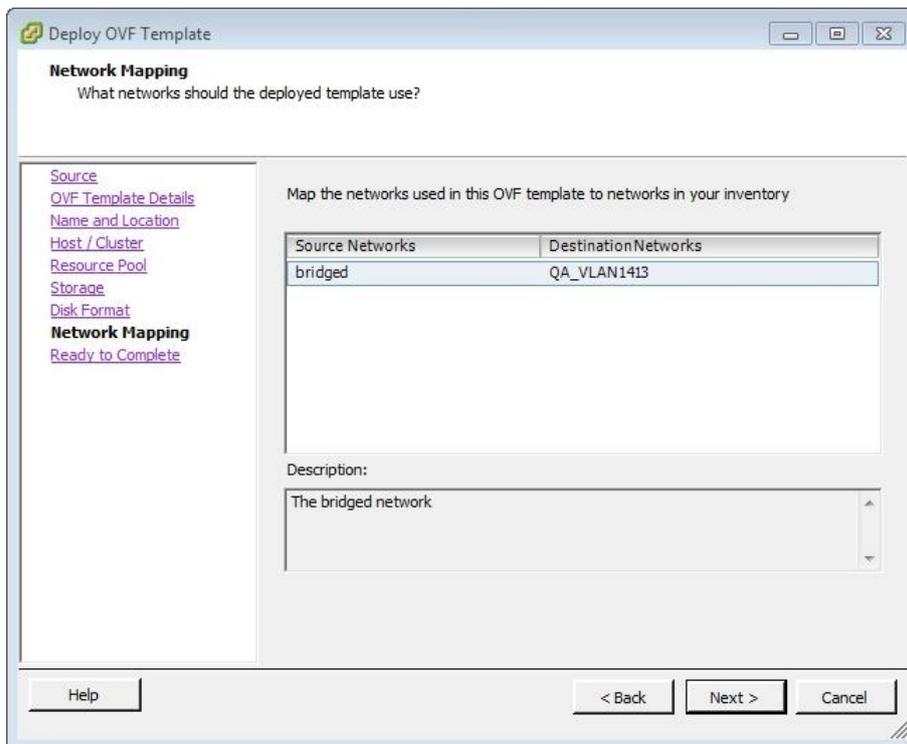


Рисунок 5. Настройка сетевых интерфейсов

- 8 На странице **Ready to Complete** выполните следующие действия:
 - Проверьте настройки развертывания виртуальной машины.
 - Если вы хотите, чтобы виртуальная машина запустилась автоматически после установки, установите флажок **Power on after deployment**.
 - Чтобы начать развертывание, нажмите кнопку **Finish**.
- 9 Дождитесь окончания развертывания. В результате в папке, указанной на шаге 4, будет создана виртуальная машина с заданным именем.
- 10 В главном окне программы vSphere Client перейдите на страницу **VMs and Templates** и выполните следующие действия:
 - Сопоставьте сетевым интерфейсам виртуальной машины физические или виртуальные сетевые коммутаторы. Параметры сетевых интерфейсов задаются в настройках виртуальной машины на вкладке **Hardware**.
 - Запустите виртуальную машину. Начнется загрузка операционной системы и всех необходимых служб.
- 11 После завершения загрузки ViPNet Coordinator HW-VA выполните установку справочников и ключей (см. «Установка, обновление и удаление справочников и ключей» на стр. 22).

Oracle VM VirtualBox

Для установки ViPNet Coordinator HW-VA на платформу виртуализации Oracle VM VirtualBox выполните следующие действия:

- 1 В главном окне программы Oracle VM VirtualBox в меню **Файл** выберите пункт **Импорт конфигураций**. Будет запущен мастер импорта конфигураций виртуальных машин.
- 2 На первой странице мастера укажите путь к файлу с расширением ***.ova**, содержащему образ виртуальной машины. Затем нажмите кнопку **Next**.

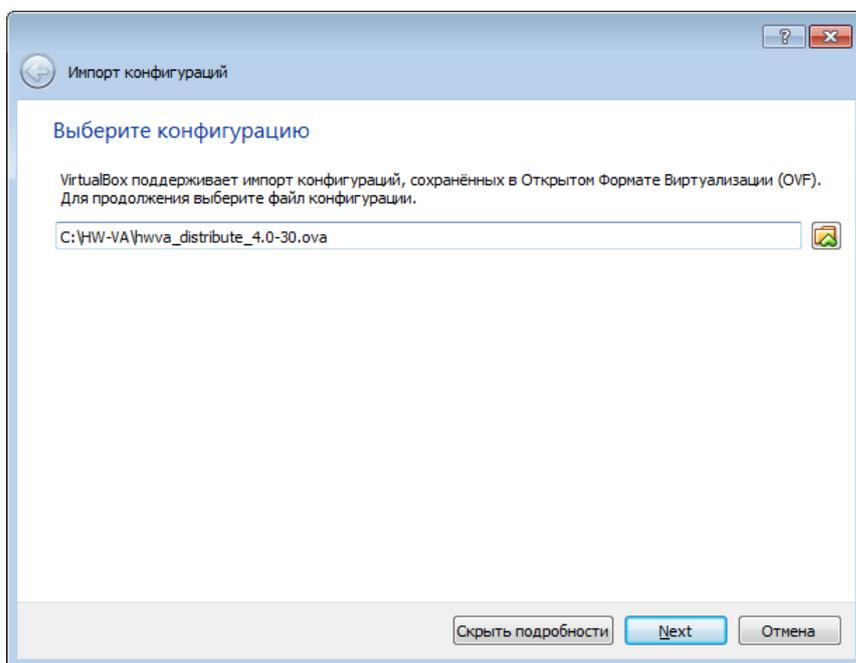


Рисунок 6. Выбор файла с образом виртуальной машины

- 3 На странице **Укажите параметры импорта** в поле **Имя** измените, если необходимо, имя виртуальной машины. Затем нажмите кнопку **Импорт**.



Внимание! Во время установки ViPNet Coordinator HW-VA на платформу виртуализации и при его дальнейшей эксплуатации не следует изменять используемый для виртуального образа контроллер жесткого диска. Корректная работа ViPNet Coordinator HW-VA гарантируется только при использовании IDE-контроллера жесткого диска.

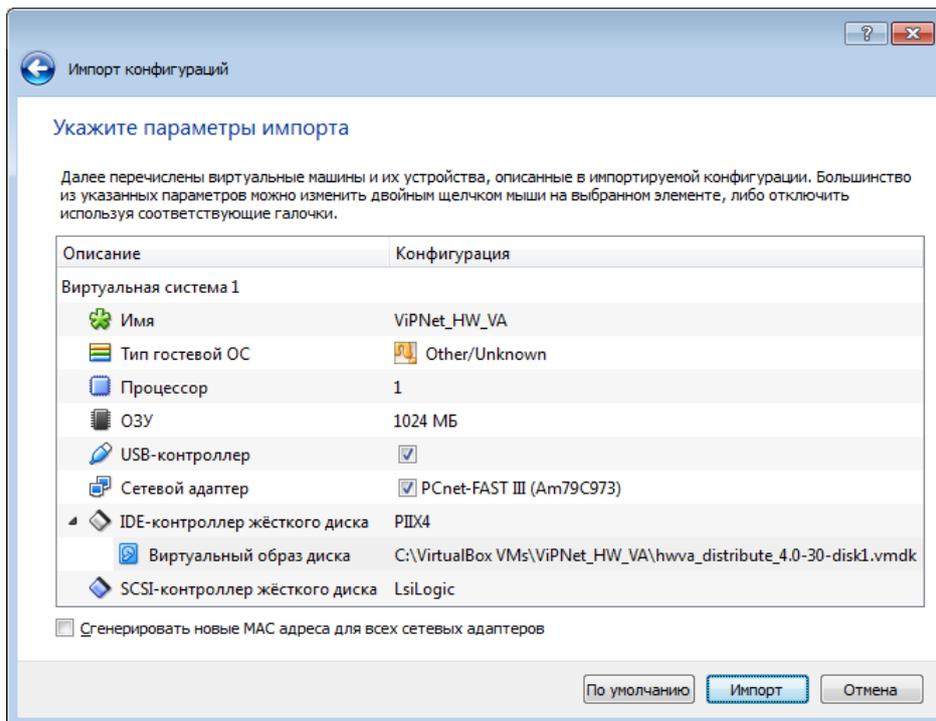


Рисунок 7. Изменение параметров виртуальной машины

В результате импорта будет создана виртуальная машина с указанным именем.

- 4 В настройках виртуальной машины включите поддержку процессором режима расширения физических адресов PAE (Physical Address Extension). Для этого в главном окне программы Oracle VM VirtualBox на панели инструментов нажмите кнопку **Настроить** , в окне **Настройки** выберите раздел **Система** и на вкладке **Процессор** установите флажок **Включить PAE/NX**.

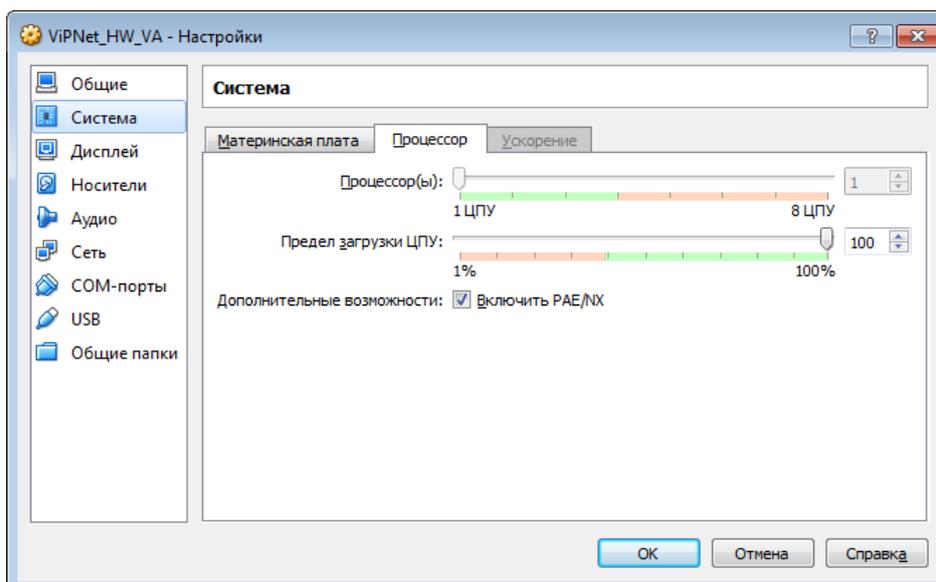


Рисунок 8. Включение поддержки процессором режима PAE



Примечание. На платформе виртуализации VMware Workstation поддержка режима PAE всегда включена.

- 5 Добавьте, если необходимо, сетевые интерфейсы. Параметры сетевых интерфейсов задаются в настройках виртуальной машины в разделе **Сеть**.
- 6 Запустите виртуальную машину. Начнется загрузка операционной системы и всех необходимых служб.

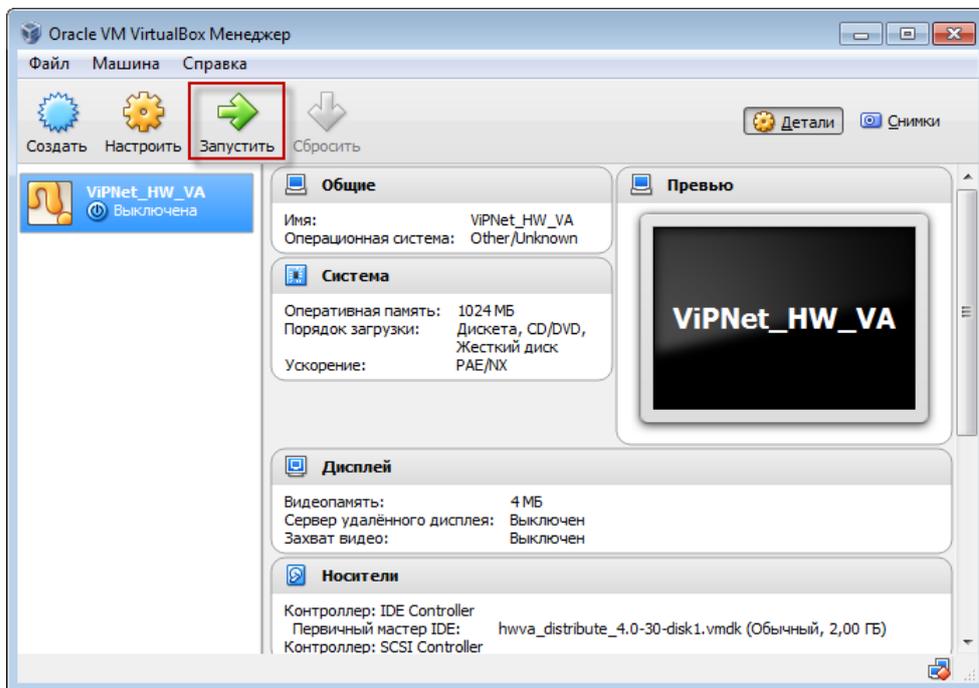


Рисунок 9. Запуск виртуальной машины

- 7 После завершения загрузки выполните установку справочников и ключей (см. «Установка справочников и ключей» на стр. 27).

2

Установка, обновление и удаление справочников и ключей

Способы установки и подготовка к установке справочников и ключей	23
Установка справочников и ключей	27
Обновление и удаление справочников и ключей	43

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. 82).

- 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 главе [Резервное копирование и восстановление настроек](#) (на стр. 59).

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

Способы подключения к ViPNet Coordinator HW при установке справочников и ключей



Рисунок 10. 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. «Подготовка к установке справочников и ключей с помощью ноутбука по Ethernet-каналу и протоколу TFTP» на стр. 24). Удобен, если вы подключаетесь к ViPNet Coordinator HW или виртуальному образу ViPNet Coordinator HW с ноутбука через сетевой кросс-кабель Ethernet и технологический адрес.
- Через внешнее устройство, которым может быть USB-носитель или CD-диск (см. «Подготовка к установке справочников и ключей с помощью внешнего устройства» на стр. 26). Удобен, если вы подключаетесь к ViPNet Coordinator HW или виртуальному образу ViPNet Coordinator HW через обычную консоль (с использованием монитора и клавиатуры) или COM-консоль (с использованием ноутбука).

Подготовка к установке справочников и ключей 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 TCP/IP (Simple TCP/IP services)**.

Кроме того, на время установки на ноутбуке с ОС Windows Vista 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 или компьютера, на котором развернут виртуальный образ 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 стандартного Telnet- или SSH-клиента) по адресу 169.254.241.1.



Примечание. Для корректного отображения символов при подключении по Telnet укажите тип терминала VT100 с помощью команды:
`telnet -t VT100 169.254.241.1`

Подготовка к установке справочников и ключей с помощью внешнего устройства

Перед началом установки справочников и ключей с помощью внешнего устройства выполните следующее:

1 При использовании USB-носителя:

1.1 Отформатируйте носитель в одну из поддерживаемых файловых систем: FAT32, ext2, ext3 или ext4.

1.2 Перенесите на носитель дистрибутив ключей (файл *.dst).

При использовании CD-диска запишите на него файл *.dst.

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

- Подключите монитор и клавиатуру к VGA-порту и PS/2-порту ПАК ViPNet Coordinator HW или компьютера, на котором развернут виртуальный образ ViPNet Coordinator HW.
- Подключите ноутбук к COM-порту RS-232 ПАК ViPNet Coordinator HW или компьютера, на котором развернут виртуальный образ ViPNet Coordinator HW.



Примечание. В исполнениях HW50 N1, N2, N3 и 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 ниже таблицы в предложенном порядке.

Таблица 5. Последовательность установки справочников и ключей

Действие	Ссылка
<input type="checkbox"/> Иницируйте установку справочников и ключей на ViPNet Coordinator HW	Начало установки (на стр. 27)
<input type="checkbox"/> Укажите часовой пояс, дату и время	Настройка часового пояса, даты и времени (на стр. 28)
<input type="checkbox"/> Выберите нужный дистрибутив ключей	Установка дистрибутива ключей на ViPNet Coordinator HW (на стр. 30)
<input type="checkbox"/> Настройте параметры всех сетевых интерфейсов ViPNet Coordinator HW	Настройка сетевых интерфейсов (на стр. 32)
<input type="checkbox"/> Настройте параметры DNS-сервера	Настройка DNS-сервера (на стр. 33)
<input type="checkbox"/> Настройте параметры NTP-сервера	Настройка NTP-сервера (на стр. 34)
<input type="checkbox"/> При необходимости измените настройки виртуальных адресов	Настройка имени компьютера и диапазона виртуальных адресов (на стр. 35)
<input type="checkbox"/> Выберите режим подключения ViPNet Coordinator HW к внешней сети через межсетевой экран	Настройка подключения к внешней сети через межсетевой экран (на стр. 36)
<input type="checkbox"/> Проверьте связь с одним или несколькими узлами сети ViPNet	Проверка связи с другим сетевым узлом (на стр. 40)
<input type="checkbox"/> Завершите установку справочников и ключей	Завершение установки (на стр. 42)



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

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 В ответ на предложение начать установку в консольном режиме `Would you like to start installing keys or restoring configuration? [y/n]` 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**.

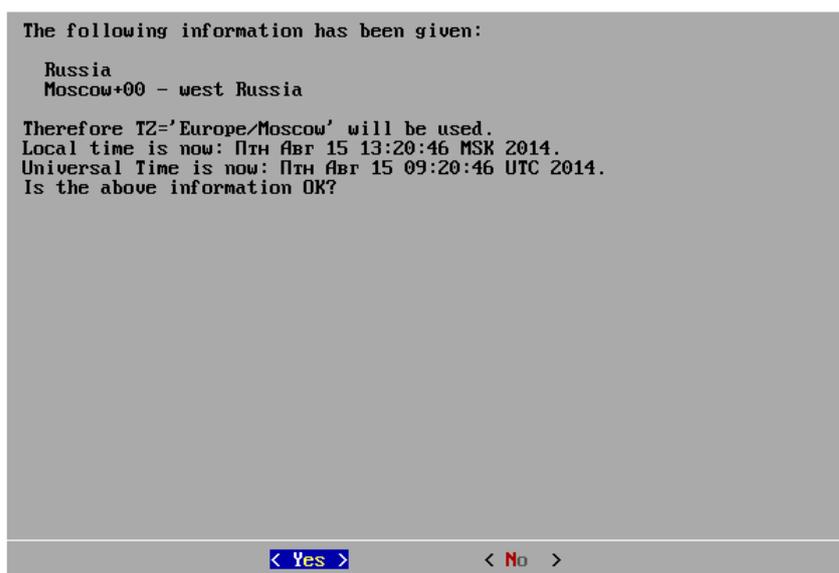


Рисунок 11. Запрос на установку часового пояса

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 час-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 «знак „плюс“», «знак „минус“», 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 импорта *.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:
 - o `t` — для переноса с ноутбука по протоколу TFTP;
 - o `u` — для переноса с USB-носителя;
 - o `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**.

Если вы выбрали способ переноса с USB-носителя или CD-диска, подключите устройство к одному из USB-разъемов ViPNet Coordinator HW (или компьютера, на котором развернут виртуальный образ ViPNet Coordinator HW) или вставьте диск в привод и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Next**.

- 3 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**.

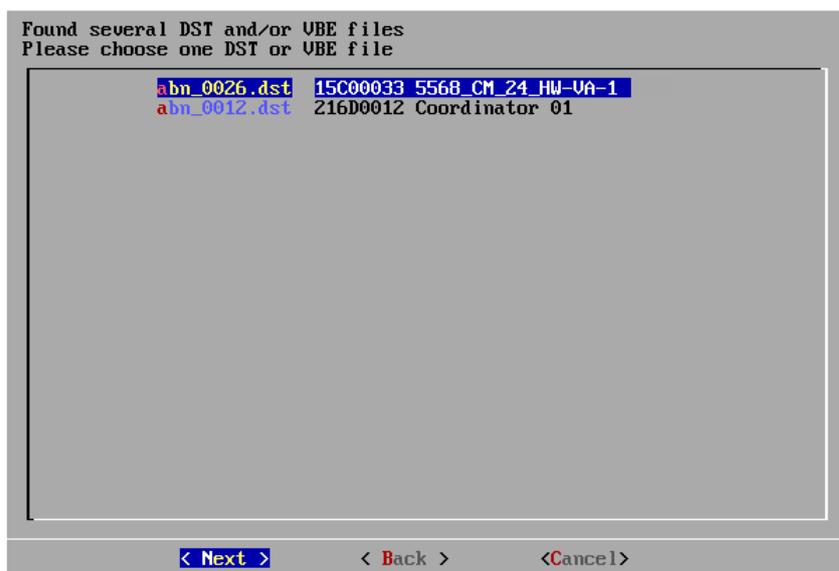


Рисунок 12. Выбор файла для установки справочников и ключей

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 (или компьютера, на котором развернут виртуальный образ ViPNet Coordinator HW) внешнее устройство, на котором сохранен персональный ключ пользователя (см. глоссарий, стр. 82).
 - 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 сможет быть найден, поэтому установка ключей не сможет быть 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. 32). По завершении установки справочников и ключей из файла экспорта мастер предложит перезагрузить компьютер (см. «[Завершение установки](#)» на стр. 42).

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. 42).

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>? [y/n]` 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. 33).

- 2 Установите для интерфейса режим DHCP, если это необходимо. Для этого в ответ на сообщение `Use dhcp on the interface eth<номер>? [y/n]` 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**.

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**.

Настройка DNS-сервера

Для настройки DNS-сервера 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? [y/n]` 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. 34).

- 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? [y/n]`.

- 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).

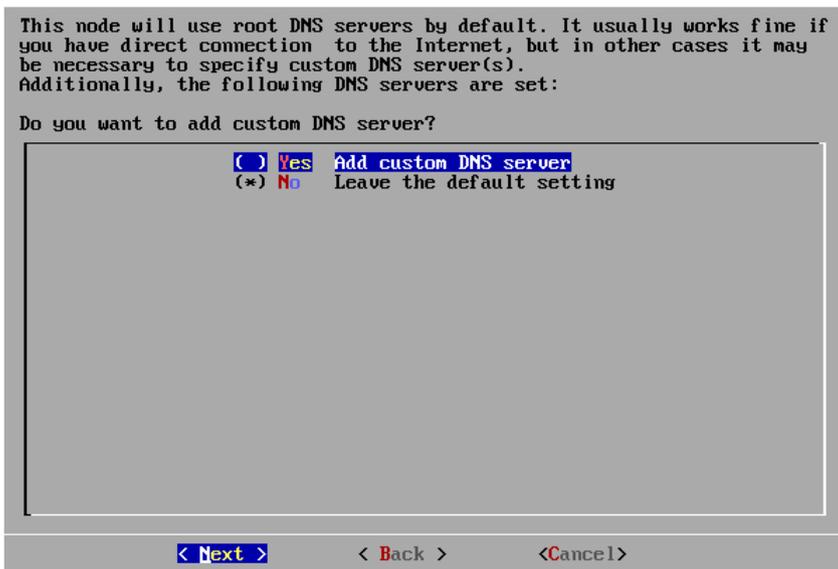


Рисунок 13. Запрос на добавление адреса DNS-сервера

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? [y/n]` 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. 35).

- 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? [y/n]`.
 - o 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).

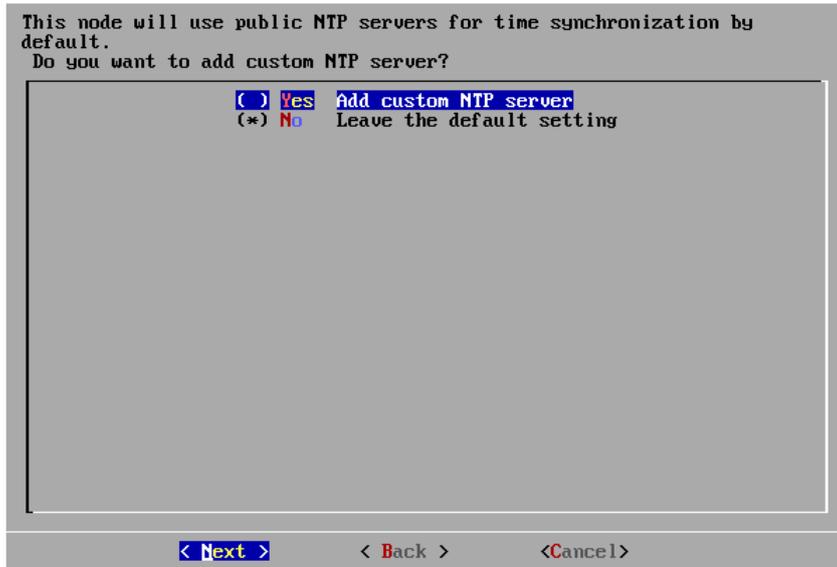


Рисунок 14. Запрос на добавление NTP-сервера

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? [y/n]`.



Примечание. По умолчанию предлагается диапазон виртуальных адресов 11.0.0.1-11.0.254.254. 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 «Принципы назначения виртуальных адресов».

Виртуальные адреса из указанного диапазона будут назначаться одиночным туннелируемым адресам. Для диапазонов туннелируемых узлов адреса берутся из следующего интервала: $\langle x+1 \rangle .0.0.1 - \langle x+1 \rangle .0.255.254$, 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 туннелируемых адресов».

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 нового диапазона виртуальных адресов и нажмите клавишу **Enter**. Например: 11.0.0.1-11.0.254.254. 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. 40) и при необходимости настроить подключение к внешней сети через межсетевой экран (см. «[Настройка подключения к внешней сети через межсетевой экран](#)» на стр. 36).

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. 32).
- 2 Дано согласие проверить соединение с одним из сетевых узлов ViPNet (см. «[Проверка связи с другим сетевым узлом](#)» на стр. 40).

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? [y/n]`.
 - 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.

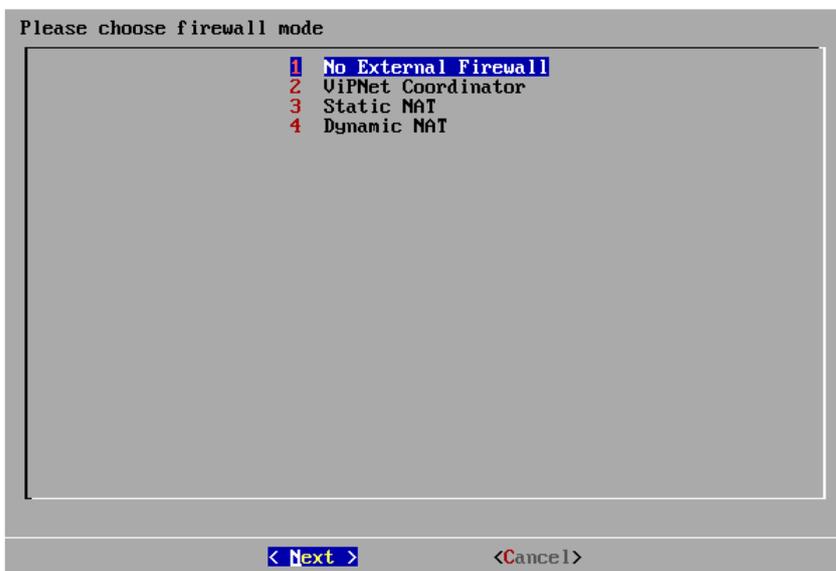


Рисунок 15. Выбор режима работы ViPNet Coordinator HW через межсетевой экран

- 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. Общее описание».

- 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. 40).
- 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.

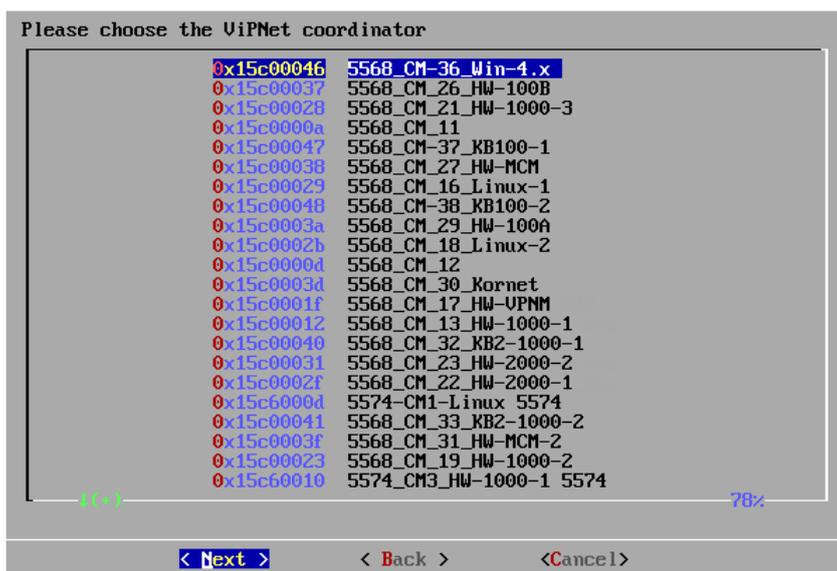


Рисунок 16. Выбор координатора для подключения к внешней сети

- 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? [y/n]`.



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? [y/n]` 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? [y/n]` 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.

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. 32).

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. 35) 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? [y/n]`. Выполните одно из действий:
 - Если проверку связи с узлом 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. 36). 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**.

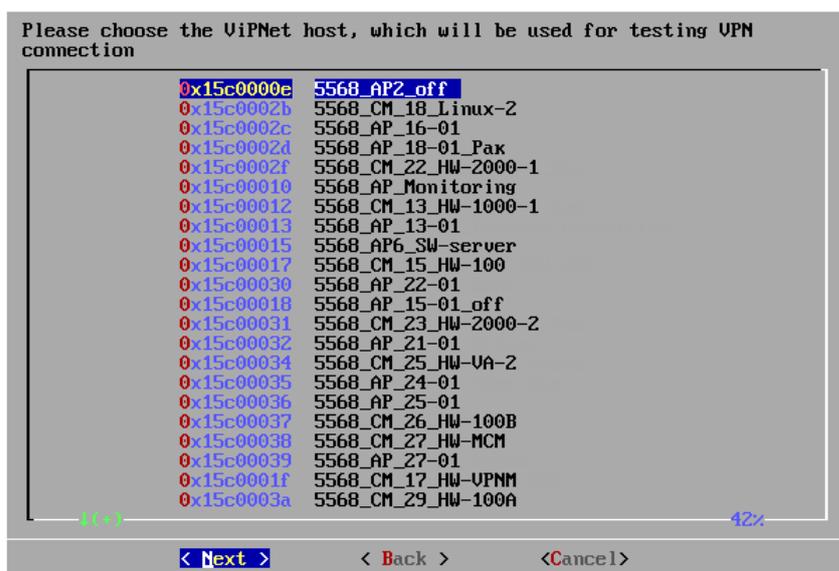


Рисунок 17. Выбор узла для проверки связи

- 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? [y/n].

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 конфигурационным файлам».

Нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **OK**. Мастер предложит запустить драйверы и демоны (см. «[Завершение установки](#)» на стр. 42).

- 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? [y/n].
 - 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 `.vbe`, то для корректного применения настроек появится сообщение с предложением перезагрузить компьютер. Для перезагрузки введите символ `y` и нажмите клавишу **Enter**. В полноэкранном режиме нажмите кнопку **Reboot**. Работа мастера будет завершена, и компьютер 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 `*.vbe`, произойдет только после перезагрузки. В случае отказа перезагрузите компьютер 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? [y/n]`. 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? [y/n]`. 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
```

Обновление и удаление справочников и ключей

Если администратор сети ViPNet вносит какие-либо изменения в структуру сети или настройки отдельных сетевых узлов, например, создает новые связи между сетевыми узлами, то автоматически изменяются справочники и ключи, и их требуется обновить на сетевых узлах. Справочники и ключи также требуется обновлять на узлах при компрометации (см. глоссарий, стр. 81) или смене мастер-ключей в сети (см. глоссарий, стр. 82).

Обновления справочников и ключей могут быть созданы и централизованно отправлены на сетевые узлы, которых коснулись изменения, администратором сети с помощью программы ViPNet Administrator. Поступившие обновления справочников и ключей на ViPNet Coordinator HW будут приняты в автоматическом режиме.

Внимание! При компрометации и смене мастер-ключей в сети ViPNet обновления справочников и ключей на ViPNet Coordinator HW могут быть приняты только в том случае, если на узле есть [резервный набор персональных ключей \(РНПК\)](#). Узнать о наличии или отсутствии файла с РНПК на узле вы можете при просмотре информации о ключах с помощью команды `iplir show key-info`.



Если файла с РНПК нет, добавьте его на ViPNet Coordinator HW с помощью команды `admin add spare keys`. В противном случае вы сможете выполнить обновление справочников и ключей только вручную.

Подробнее о просмотре ключей и добавлении РНПК см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», в разделах главы «Настройка параметров безопасности».

Информация о принятых обновлениях записывается в журнал обновления справочников и ключей. Для просмотра этого журнала выполните команду:

```
hostname# iplir show keys-upgrade-log
```

Если по каким-либо причинам обновление справочников и ключей не может быть принято по сети, например, при отсутствии файла с РНПК на узле, вы можете обновить справочники и ключи вручную с помощью дистрибутива ключей.



Внимание! После обновления справочников и ключей с помощью дистрибутива ключей будут потеряны все настройки ViPNet Coordinator HW, произведенные вручную, и их необходимо будет задать заново. Некоторые настройки вы можете задать в процессе установки справочников и ключей из нового дистрибутива, остальные необходимые настройки потребуются задать после завершения обновления.

Если файл с РНПК содержится на узле, то в процессе обновления он будет удален.

Для этого выполните следующие действия:

- 1 Получите новый дистрибутив ключей у администратора сети ViPNet.
- 2 Завершите работу демонов `iplircfg`, `failoverd`, `algd` и `mftpd` с помощью команды:

```
hostname# vpn stop
```
- 3 Удалите текущие справочники и ключи с помощью команды:

```
hostname# admin remove keys
```
- 4 Установите справочники и ключи из нового дистрибутива ключей (см. «Установка, обновление и удаление справочников и ключей» на стр. 22). В конце процедуры установки согласитесь с запуском демонов и командного интерпретатора.
- 5 Задайте настройки, которые были потеряны в процессе обновления справочников и ключей.
- 6 Добавьте файл с РНПК, если он отсутствовал в новом дистрибутиве ключей.

3

Обновление программного обеспечения

Особенности обновления ПО	46
Удаленное обновление ПО	47
Локальное обновление ПО	48
Обновление ПО ViPNet Coordinator HW на кластере горячего резервирования	50
Конвертация правил открытой и защищенной сети	52
Совместимость ПО ViPNet Coordinator HW версий 3.x	58

Особенности обновления ПО

При обновлении ПО ViPNet Coordinator HW до версии 4.x необходимо учитывать следующие изменения:

- Если у вас установлено ПО версии ниже 3.3, сначала необходимо выполнить обновление до этой версии, а после — до версии 4.x.

Внимание! Удаленное обновление ПО ViPNet Coordinator HW100 X1 не поддерживается. В этом случае необходимо использовать локальное обновление.



Удаленное обновление ПО ViPNet Coordinator HW100 X8 с версии 3.3 или 3.5 до версии 4.2 не поддерживается. В этом случае необходимо сначала удаленно обновить ПО до версии 4.1, после чего провести удаленное обновление до версии 4.2.

Чтобы узнать тип вашей аппаратной платформы ViPNet Coordinator HW, выполните команду `version` (см. документ «ViPNet Coordinator HW. Справочное руководство по командному интерпретатору»).

-
- С версии 4.x для аутентификации пользователя используется учетная запись `user`, тогда как в более ранних версиях — учетная запись `vipnet`. После обновления ПО до версии 4.x используйте для аутентификации новую учетную запись.
 - В процессе обновления ПО с версии 3.x до версии 4.x производится конвертация правил фильтрации защищенной и открытой сети в новый формат (см. «[Конвертация правил открытой и защищенной сети](#)» на стр. 52).
 - В версии 4.x изменился способ настройки фиксированных альтернативных каналов. Теперь они задаются с помощью множественных адресов доступа и их метрик, секция `[channels]` и параметр `group` в секциях `[id]` больше не используются.

При обновлении ПО до версии 4.x настройки фиксированных альтернативных каналов не конвертируются. Если раньше вы использовали альтернативные каналы доступа для каких-либо узлов, после обновления выполните аналогичные настройки новым способом. Пример настройки см. в документе «ViPNet Coordinator HW. Сценарии работы», в разделе «Использование нескольких каналов доступа к защищенному узлу». Подробнее о принципах назначения метрик см. в документе «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», в разделе «Настройка IP-адресов доступа к узлу и их приоритета».

- В процессе обновления ПО с версии 4.0.x или с более ранней версии все созданные копии конфигурации VPN будут удалены, поскольку они не совместимы с форматом конфигурации VPN новой версии ПО. Для сохранения настроек ПО версии 4.0.x или более ранней версии перед обновлением экспортируйте эти настройки (см. «[Экспорт справочников, ключей и настроек](#)» на стр. 62).

Удаленное обновление ПО

Удаленное обновление ПО ViPNet Coordinator HW производится с помощью программы ViPNet Центр управления сетью (далее — ЦУС). Администратор сети ViPNet получает у представителей ОАО «ИнфоТекС» файл формата LZH с новой версией ПО и из ЦУСа рассылает файл обновления на все координаторы ViPNet Coordinator HW, на которых необходимо выполнить обновление.

Для разных исполнений ViPNet Coordinator HW передаются следующие файлы обновления ПО:

- для HW50 — hw50_vipnet_base_<Platform>_driv_<Major>.<Minor>.<Subminor>-<Build>.lzh;
- для HW100 — hw100_vipnet_base_<Platform>_driv_<Major>.<Minor>.<Subminor>-<Build>.lzh;
- для HW1000 — hw1000_vipnet_base_<Platform>_driv_<Major>.<Minor>.<Subminor>-<Build>.lzh;
- для HW2000 — hw2000_vipnet_base_<Platform>_driv_<Major>.<Minor>.<Subminor>-<Build>.lzh;
- для HW5000 — hw5000_vipnet_base_<Platform>_driv_<Major>.<Minor>.<Subminor>-<Build>.lzh;
- для HW-VA — coordinatorhw_vipnet_base_<Platform>_driv_<Major>.<Minor>.<Subminor>-<Build>.lzh.

Процедура удаленного обновления ПО подробно описана в документе «ViPNet Центр управления сетью. Руководство администратора». На ViPNet Coordinator HW обновление принимается и выполняется автоматически, после обновления выполняется перезагрузка. Перед обновлением настоятельно рекомендуется сделать экспорт справочников, ключей и настроек ViPNet Coordinator HW в файл *.vbe (см. «[Экспорт справочников, ключей и настроек](#)» на стр. 62). Это позволит вам восстановить их на ViPNet Coordinator HW, если обновление ПО пройдет некорректно (см. «[Импорт справочников, ключей и настроек](#)» на стр. 64).

Внимание! Перед началом удаленного обновления обязательно ознакомьтесь с рекомендациями раздела [Особенности обновления ПО](#) (на стр. 46).

Удаленное обновление ПО ViPNet Coordinator HW100 X1 не поддерживается. В этом случае необходимо использовать локальное обновление.



Удаленное обновление ПО ViPNet Coordinator HW100 X8 с версии 3.3 или 3.5 до версии 4.2 не поддерживается. В этом случае необходимо сначала удаленно обновить ПО до версии 4.1, после чего провести удаленное обновление до версии 4.2.

Чтобы узнать тип вашей аппаратной платформы ViPNet Coordinator HW, выполните команду `version` (см. документ «ViPNet Coordinator HW. Справочное руководство по командному интерпретатору»).

Локальное обновление ПО

Прежде чем начать локальное обновление ПО на ViPNet Coordinator HW выполните следующие действия:

- Ознакомьтесь с рекомендациями раздела [Особенности обновления ПО до версии 4.x](#) (см. «[Особенности обновления ПО](#)» на стр. 46).

В случае обновления ПО с версии 3.x до версии 4.x также ознакомьтесь с особенностями конвертации правил фильтрации трафика (см. «[Конвертация правил открытой и защищенной сети](#)» на стр. 52).

- У администратора сети получите файл обновления ПО ViPNet Coordinator HW (файл *.lzh) и файл *.md5 для проверки подлинности и целостности файла обновления.
- Вычислите контрольную сумму файла обновления по алгоритму MD5, а затем сравните ее с контрольной суммой, приведенной в файле с расширением *.md5. Если суммы совпали, запишите файл обновления на USB-носитель.



Примечание. На один USB-носитель можно записать несколько файлов обновления, предназначенных для различных исполнений ViPNet Coordinator HW (разместив их в разных каталогах). При выполнении локального обновления производится анализ содержимого USB-носителя и становится доступным для использования только тот дистрибутив, который соответствует данному исполнению ViPNet Coordinator HW.

- Выполните экспорт справочников, ключей и настроек ViPNet Coordinator HW в файл *.vbe (см. «[Экспорт справочников, ключей и настроек](#)» на стр. 62). Это позволит вам восстановить их на ViPNet Coordinator HW, если обновление ПО пройдет некорректно (см. «[Импорт справочников, ключей и настроек](#)» на стр. 64).

Для локального обновления ПО выполните следующие действия:

- 1 На ViPNet Coordinator HW выполните команду:

```
hostname# admin upgrade software usb
```

При этом появится предложение подключить USB-носитель.

- 2 Подключите USB-носитель к USB-разъему ViPNet Coordinator HW или компьютера, на котором развернут виртуальный образ ViPNet Coordinator HW, и подтвердите подключение.

Если USB-носитель не найден, появится соответствующее сообщение, выполнение команды завершается, обновление не производится.

- 3 На USB-носителе производится поиск файлов LZH:

- Если файлов нет, появляется соответствующее сообщение и выполнение команды завершается, обновление не производится.
- Если файлы найдены:

- Проверяется целостность каждого из файлов.
- Для каждого файла, прошедшего проверку целостности, также проверяется, соответствует ли он данному исполнению ViPNet Coordinator HW.
- Выводится пронумерованный список отобранных файлов. Выберите файл, в имени которого указана нужная версия обновления ПО.

4 Введите номер выбранного файла обновления и нажмите клавишу **Enter**.



Внимание! При использовании кластера горячего резервирования локальное обновление ПО должно быть произведено на обоих серверах кластера (см. «[Обновление ПО ViPNet Coordinator HW на кластере горячего резервирования](#)» на стр. 50).

5 Дождитесь появления сообщения о результате обновления.

6 После обновления перезагрузите ViPNet Coordinator HW, чтобы обновление вступило в силу.



Примечание. При обновлении ПО ViPNet Coordinator HW с версии 3.x до версии 4.x будут автоматически изменены временные зоны в связи с переходом на зимнее время 26.10.2014. После обновления ПО проверьте корректность установленного времени и при необходимости измените его.

Если было произведено обновление с версии 3.x до версии 4.x, то во время загрузки ViPNet Coordinator HW правила защищенной и открытой сети будут конвертированы в соответствующие сетевые фильтры и правила трансляции адресов.

Обновление ПО ViPNet Coordinator HW на кластере горячего резервирования

Обновление ПО ViPNet Coordinator HW на кластере горячего резервирования может производиться удаленно или локально. Удаленное обновление выполняется автоматически на обоих серверах кластера. Локальное обновление на кластере имеет ряд особенностей, порядок его выполнения приведен ниже.

Для локального обновления ПО на кластере выполните следующие действия:

- 1 Выключите интерфейс резервного канала на обоих серверах кластера с помощью команды:

```
hostname# inet ifconfig <интерфейс> down
```

Затем отсоедините кросс-кабель от компьютеров.

- 2 Обновите ПО на пассивном ViPNet Coordinator HW (так же, как при работе в одиночном режиме (см. «[Локальное обновление ПО](#)» на стр. 48)) с помощью команды:

```
hostname# admin upgrade software usb
```

Информацию о текущем режиме ViPNet Coordinator HW можно получить с помощью команды
`hostname> failover show info.`

- 3 После обновления перезагрузите пассивный ViPNet Coordinator HW. Для этого в ответ на предложение перезагрузки нажмите клавишу **Enter**.

Убедитесь в стабильной работе ViPNet Coordinator HW:

- Проверьте текущее состояние служб ViPNet с помощью команды:

```
hostname> failover show info
```

Все службы должны быть запущены, система защиты от сбоев должна работать в режиме кластера.

- В течение некоторого времени (около 15 минут) следите за работой пассивного ViPNet Coordinator HW и убедитесь, что он не перезагружается.

- 4 Перезагрузите активный ViPNet Coordinator HW, для этого выполните команду:

```
hostname> machine reboot
```

В результате пассивный ViPNet Coordinator HW (с обновленным ПО) перейдет в активный режим, а ViPNet Coordinator HW со старой версией ПО окажется в пассивном режиме.

- 5 Обновите ПО на пассивном ViPNet Coordinator HW, для этого выполните команду:

```
hostname# admin upgrade software usb
```

- 6 После обновления перезагрузите пассивный ViPNet Coordinator HW и убедитесь в его стабильной работе (как на шаге 3).

- 7 Соедините оба ViPNet Coordinator HW (или оба компьютера, на которых развернуты виртуальные образы ViPNet Coordinator HW) кросс-кабелем и включите интерфейс резервного канала с помощью команды:

```
hostname# inet ifconfig <интерфейс> up
```

- 8 Убедитесь, что резервный канал функционирует нормально. Для этого измените какую-либо настройку в файле конфигурации на активном ViPNet Coordinator HW и через некоторое время проверьте наличие этих же изменений на пассивном ViPNet Coordinator HW. Чтобы изменения попали на пассивный ViPNet Coordinator HW, необходимо включить резервирование группы файлов конфигурации в файле `failover.ini` в секции `[sendconfig]`.

Конвертация правил открытой и защищенной сети

В связи с изменением формата сетевых фильтров и правил трансляции IP-адресов при обновлении ПО ViPNet Coordinator HW с версии 3.x до версии 4.x производится конвертация имеющихся правил фильтрации защищенной и открытой сети в новый формат. Конвертация осуществляется автоматически во время первого запуска ПО после обновления.

Перед выполнением обновления ПО ViPNet Coordinator HW с версии 3.x до версии 4.x ознакомьтесь с информацией следующих разделов:

- [Конвертация правил открытой сети при обновлении до версии 4.x](#) (на стр. 52).
- [Конвертация правил защищенной сети при обновлении до версии 4.x](#) (на стр. 55).



Внимание! Обратная конвертация сетевых фильтров и правил трансляции в прежний формат не поддерживается. Поэтому перед обновлением с версии 3.x до версии 4.x настоятельно рекомендуется создать резервную копию настроек ПО (см. «[Резервное копирование и восстановление настроек](#)» на стр. 59).

Конвертация правил открытой сети при обновлении до версии 4.x

В ViPNet Coordinator HW версий ниже 4.0 правила обработки открытых (незашифрованных) IP-пакетов содержались в файле `firewall.conf`. Чтобы изменить эти правила, необходимо было отредактировать этот конфигурационный файл. В ViPNet Coordinator HW версий 4.x правила обработки переименованы в сетевые фильтры. Фильтры хранятся в виде таблиц в нескольких файлах `*.xml`, редактирование которых выполняется с помощью командного интерпретатора или веб-интерфейса. В связи с этим при обновлении ViPNet Coordinator HW до версии 4.x с более ранних версий происходит конвертация правил обработки открытых IP-пакетов в фильтры открытой сети.

- В качестве адреса назначения локальных фильтров открытой сети, созданных в результате преобразования правил обработки открытых IP-пакетов из секции `[broadcast]` файла `firewall.conf`, указывается системная группа объектов `broadcast`.
- Последовательность применения правил сохраняется.
- Не конвертируются:
 - правила, содержащие синтаксические ошибки;
 - комментарии к правилам;
 - расписания, заданные для правил;

- правила, для которых в адресах отправителя и получателя заданы порты, но не указан протокол TCP или UDP.
- Если в условии правила, пропускающего или блокирующего пакеты, указаны оба протокола (TCP, UDP) и несколько портов узла отправителя и получателя, это правило преобразуется в сетевой фильтр с несколькими условиями.

Например, правило до конвертации:

```
rule= num 1 proto tcp,udp from any:(80,2525) to any:(368,53) pass
```

Соответствующие сетевые фильтры после конвертации:

Num	Name	Option	
Act	Source	Destination	Protocol
1	RuleName1	User	
pass	@any	@any	udp: from 80 to 368 udp: from 80 to 53 udp: from 2525 to 368 udp: from 2525 to 53 tcp: from 80 to 368 tcp: from 80 to 53 tcp: from 2525 to 368 tcp: from 2525 to 53

- Правила, содержащие несколько адресов отправителей или получателей в виде <IP-адрес>:<порт>, преобразуются в несколько сетевых фильтров. То есть, если в правиле в полях from и to задано по два адреса, оно конвертируется в четыре сетевых фильтра.

Например, правило до конвертации:

```
rule= proto tcp from 192.168.1.1:80,192.168.1.5:2525 to 192.168.30.3:80,192.168.4.2:443 pass
```

Соответствующие сетевые фильтры после конвертации:

Num	Name		Option
Act	Source	Destination	Protocol
1	RuleName1		User
pass	192.168.1.1	192.168.30.3	tcp: from 80 to 80
2	RuleName2		User
pass	192.168.1.1	192.168.4.2	tcp: from 80 to 443
3	RuleName3		User
pass	192.168.1.5	192.168.30.3	tcp: from 2525 to 80
4	RuleName4		User
pass	192.168.1.5	192.168.4.2	tcp: from 2525 to 443

- Режимы безопасности (кроме 2-го, который игнорируется) преобразуются в локальные фильтры открытой сети. Если используется несколько сетевых интерфейсов, для каждого из которых задан свой режим безопасности, при конвертации создаются сетевые фильтры для каждого интерфейса:

Num	Name		Option
Act	Source	Destination	Protocol
1	[интерфейс]:Mode1		User
	<i>(1 режим безопасности — блокировать IP-пакеты всех соединений)</i>		
drop	@any [интерфейс]	@iface [интерфейс]	@any
2	[интерфейс]:Mode2		User
	<i>(3 режим безопасности — пропускать все исходящие соединения кроме запрещенных)</i>		
pass	@iface [интерфейс]	@remote	@any
3	[интерфейс]:Mode3		User
	<i>(4 режим безопасности — пропускать все соединения)</i>		
pass	@any [интерфейс]	@any [интерфейс]	@any



Внимание! Если на момент обновления ViPNet Coordinator HW сетевой интерфейс неактивен (по умолчанию имеет 2 режим безопасности), то при конвертации он игнорируется. При необходимости после конвертации вы можете создать соответствующий локальный фильтр открытой сети вручную.

Конвертация правил защищенной сети при обновлении до версии 4.x

В ViPNet Coordinator HW версий ниже 4.0 правила обработки IP-пакетов защищенной сети содержатся в файлах `iplir.conf` и `iplir.serv`. Чтобы изменить эти правила, необходимо отредактировать конфигурационный файл `iplir.conf`. В версии 4.x правила обработки переименованы в сетевые фильтры. Фильтры хранятся в виде таблиц в нескольких файлах `*.xml`, редактирование которых выполняется с помощью командного интерпретатора или веб-интерфейса. В связи с этим при обновлении ViPNet Coordinator HW до версии 4.x с более ранних версий происходит конвертация правил обработки IP-пакетов защищенной сети в фильтры защищенной сети. Учтите также следующие особенности конвертации правил:

- Правила обработки IP-пакетов защищенной сети преобразуются в фильтры защищенной сети.
- Правила для широковещательного защищенного трафика преобразуются в соответствующие сетевые фильтры (блокирующие или пропускающие). При этом дополнительно создается общий широковещательный фильтр с противоположным действием.
- Не конвертируются:
 - правила, содержащие синтаксические ошибки;
 - комментарии к правилам;
 - расписания, заданные для правил;
 - правила, для которых в адресах источника и назначения заданы порты, но не указан протокол TCP или UDP.
- Каждое правило с направлением пакетов `any` преобразуется в два фильтра: фильтр для входящих пакетов и фильтр для исходящих пакетов. Это связано с тем, что в версии 4.x отсутствует атрибут направления пакета (например, `send/recv/any`).
- Если у нескольких сетевых узлов есть одинаковые правила, то эти узлы объединяются в группы, для каждой из которых создаются соответствующие сетевые фильтры.
- Преобразование правил защищенной сети для групп сетевых узлов выполняется следующим образом:
 - Если в правило для группы сетевых узлов, содержащее разрешающий фильтр по умолчанию, были добавлены блокирующие фильтры, то после конвертации будут созданы только соответствующие блокирующие сетевые фильтры.

- Если в правило для группы узлов, содержащее блокирующий фильтр по умолчанию, были добавлены разрешающие фильтры, то после конвертации будут созданы соответствующие разрешающие сетевые фильтры и блокирующий сетевой фильтр. При этом у блокирующего сетевого фильтра будет самый низкий приоритет.
- Преобразование правила «IP-пакеты всех адресатов» в главном фильтре защищенной сети выполняется следующим образом:
 - Если в это правило, содержащее блокирующий фильтр по умолчанию, добавлены разрешающие фильтры, то после конвертации будут созданы соответствующие разрешающие фильтры с самым низким приоритетом.
 - Если в этом правиле содержится блокирующий фильтр по умолчанию и отсутствуют дополнительные фильтры, то после конвертации будет создан соответствующий блокирующий фильтр с самым высоким приоритетом.
 - Если в это правило, содержащее разрешающий фильтр по умолчанию, добавлены блокирующие фильтры, то после конвертации будут созданы соответствующие разрешающий фильтр с самым низким приоритетом и блокирующие фильтры с самым высоким приоритетом.
 - Если в этом правиле содержится разрешающий фильтр по умолчанию и отсутствуют дополнительные фильтры, то после конвертации будет создан соответствующий разрешающий фильтр с низким приоритетом.

Например, если главный фильтр защищенной сети содержит разрешающий фильтр по умолчанию и дополнительные блокирующие фильтры, соответствующая запись в файле `iplir.conf` имеет вид:

```
[id]
id= 0xffffffffe
name= MainFilter
filterdefault= pass
filtertcp= <port> drop, send
[id]
id= <идентификатор узла 1>
name= <имя узла 1>
filterdefault= drop
filtertcp= <port> pass, send
[id]
id= <идентификатор узла 2>
name= <имя узла 2>
filterdefault= pass
filtertcp= <port> drop, send
```

В этом случае после конвертации будут созданы следующие сетевые фильтры:

Num	Name	Option	
Act	Source	Destination	Protocol
1	Main Converted Rule	User	
drop	local	@any	tcp: from <port>
2	Converted Rule	User	
pass	local	<ID1>	tcp: from <port>
3	Converted Rule	User	
drop	local	<ID1>	
4	Converted Rule	User	
drop	<ID1>	@any	tcp: from <port>
5	Converted Rule	User	
drop	local	<ID2>	tcp: from <port>
6	Main Converted Rule	User	
pass	@any	@any	

Совместимость ПО ViPNet Coordinator HW версий 3.x

Программное обеспечение версии 3.0, установленное на ViPNet Coordinator HW, несовместимо с более поздними версиями ПО при использовании режима шифрования GOST-CTR. Если в вашей сети ViPNet установлено несколько ViPNet Coordinator HW версии 3.0 и вы планируете перейти на более позднюю версию или установить в сети ViPNet Coordinator HW более поздней версии, то во избежание несовместимости на всех имеющихся ViPNet Coordinator HW обновите ПО до версии 3.1 или более поздней. Все версии ПО, начиная с 3.1, полностью совместимы между собой при использовании режима шифрования CTR.

Чтобы на время проведения обновления сохранить совместимость ПО версии 3.0 с более поздними версиями, рекомендуется перед началом обновления временно перейти на использование режима шифрования GOST-CFB. Для установки нужного режима шифрования используйте команду:

```
hostname# iplir set cipher-mode {gost-ctr | gost-cfb}
```

После обновления ПО на всех ViPNet Coordinator HW, установленных в сети, вы можете снова использовать режим шифрования CTR.

4

Резервное копирование и восстановление настроек

Назначение экспорта и импорта справочников, ключей и настроек	60
Экспорт справочников, ключей и настроек	62
Импорт справочников, ключей и настроек	64

Назначение экспорта и импорта справочников, ключей и настроек

Вы можете использовать экспорт и импорт справочников, ключей и настроек ViPNet Coordinator HW в следующих ситуациях:

- Сохранение и восстановление данных на ViPNet Coordinator HW в случае некорректного обновления ПО.
- Перенос справочников, ключей и настроек с одного сервера ViPNet Coordinator HW на другой, например, в случае замены аппаратной платформы. Это позволяет упростить подготовку нового ViPNet Coordinator HW к работе, так как не требуется выполнять установку справочников и ключей и необходимые настройки вручную.

В этом случае оба сервера ViPNet Coordinator HW должны иметь одинаковые исполнение и тип лицензии. Кроме этого, по завершении импорта сервер, с которого переносятся данные, должен быть отключен от сети или на нем должны быть удалены справочники и ключи. Это связано с тем, что в сети ViPNet не допускается функционирование нескольких узлов с одинаковыми справочниками и ключами.

В состав экспортируемой информации входят следующие данные:

- файлы, содержащие ключи шифрования для связанных с ViPNet Coordinator HW узлов;
- резервный набор персональных ключей (файл *.pk, при наличии);
- файлы, содержащие информацию о связанных с ViPNet Coordinator HW узлах (справочники);
- настройки защищенной сети (файл `iplir.conf`);
- настройки сетевых интерфейсов (IP-адрес, маска подсети, файл `iplir.conf-<интерфейс>`);
- настройки маршрутизации и статические маршруты, если такие созданы;
- настройки часового пояса;
- сетевые фильтры и правила трансляции адресов;
- настройки параметров обработки прикладных протоколов;
- настройки системы защиты от сбоев (файл `failover.ini`);
- настройки транспортного модуля (файл `mftp.conf`);
- настройки протоколирования;
- настройки дополнительных сервисов (DHCP-сервера и других);
- настройки взаимодействия с UPS;
- настройки туннелирования канального уровня (L2OverIP);
- текущие ключи для соединений по протоколу SSH2.



Примечание. Файлы экспорта, созданные в ViPNet Coordinator HW 3.1 и более ранних версий, включали также дополнительные данные: журнал IP-пакетов, журнал транспортных конвертов MFTP и очередь почтовых конвертов. Начиная с версии 3.2, при импорте таких файлов указанные дополнительные данные игнорируются.

Экспорт справочников, ключей и настроек

Экспорт справочников, ключей и настроек требуется выполнять в следующих случаях:

- Перед обновлением ПО на ViPNet Coordinator HW (см. «[Обновление программного обеспечения](#)» на стр. 45), а также периодически для возможности восстановления данных в случае сбоев в работе.



Примечание. Периодичность резервирования данных на ViPNet Coordinator HW определяется регламентом безопасности вашей организации.

- При переносе справочников, ключей и настроек на другой ViPNet Coordinator HW аналогичного исполнения (например, при замене аппаратной платформы).

Экспорт справочников, ключей и настроек вы можете выполнить только при непосредственном доступе к ViPNet Coordinator HW или виртуальному образу ViPNet Coordinator HW одним из следующих способов:

- На ноутбук, подключенный через сетевой кросс-кабель Ethernet и технологический адрес.
- На USB-носитель при подключении через обычную консоль (с использованием монитора и клавиатуры) или COM-консоль (с использованием ноутбука). Перед началом экспорта этим способом отформатируйте USB-носитель в одну из поддерживаемых файловых систем: FAT32, ext2, ext3 или ext4.



Внимание! Экспортировать справочники, ключи и настройки в удаленной SSH-сессии запрещено.

На время выполнения экспорта с использованием ноутбука (после ввода команды) автоматически изменяются настройки сетевых интерфейсов ViPNet Coordinator HW: на интерфейсе Ethernet1 устанавливается технологический IP-адрес 169.254.241.1, все остальные интерфейсы ViPNet Coordinator HW выключаются. Восстановление настроек интерфейсов ViPNet Coordinator HW производится только при успешном завершении экспорта.

Для экспорта справочников, ключей и настроек выполните следующие действия:

- 1 Завершите работу демонов `iplircfg` и `mftpd` с помощью команд:

```
hostname# iplir stop
```

```
hostname# mftp stop
```

- 2 Выберите место сохранения файла экспорта с помощью команды:

```
hostname# admin export keys binary-encrypted {tftp | usb}, где:
```

- o `tftp` — экспорт на ноутбук по протоколу TFTP.
- o `usb` — экспорт на USB-носитель.

При успешном выполнении команды появится сообщение, что файл экспорта сформирован и сохранен в каталоге `/tmp/vipnet/`:

```
Configuration file will be saved to tmp/vipnet/<имя файла экспорта>
```



Примечание. Имя файла экспорта формируется по следующему шаблону:
<название ViPNet Coordinator HW>-<идентификатор узла>-<дата экспорта>.vbe,

где <название ViPNet Coordinator HW> — наименование исполнения без последних двух символов.

Файл экспорта автоматически зашифровывается на текущем пароле пользователя.

3 Перенесите сформированный файл экспорта на ноутбук или USB-носитель.

Для переноса файла на ноутбук выполните на нем команду:

```
tftp -i 169.254.241.1 get <имя файла экспорта>
```

Для переноса файла на USB-носитель выполните следующие действия:

3.1 Подключите USB-носитель к одному из USB-разъемов ViPNet Coordinator HW или компьютера, на котором развернут виртуальный образ ViPNet Coordinator HW в ответ предложение

```
Put <имя файла экспорта> file onto USB drive.
```

```
Insert USB drive and press Enter.
```

3.2 Появится пронумерованный список всех обнаруженных устройств. Выберите USB-носитель для переноса на него файла экспорта. Для этого в ответ на сообщение `Select target partition [1-1] or 0 to abort` введите цифру, соответствующую USB-носителю в списке, и нажмите клавишу **Enter**.

3.3 При успешной записи файла экспорта на USB-носитель появится сообщение с разрешением извлечь устройство:

```
You may remove the USB drive.
```



Внимание! Необходимо дождаться этого сообщения прежде, чем извлечь USB-носитель из разъема.

4 Запустите демоны `iplircfg` и `mftpd` с помощью команд:

```
hostname# iplirc start
```

```
hostname# mftpd start
```

Импорт справочников, ключей и настроек

Импорт справочников, ключей и настроек требуется выполнять в следующих случаях:

- Для восстановления данных при некорректном обновлении ПО на ViPNet Coordinator HW (см. «[Обновление программного обеспечения](#)» на стр. 45).
- Для загрузки справочников, ключей и настроек с одного ViPNet Coordinator HW на другой (например, при замене аппаратной платформы).

Способы импорта справочников, ключей и настроек на ViPNet Coordinator HW описаны в разделе [Способы установки и подготовка к установке справочников и ключей](#) (на стр. 23).

Перед началом импорта убедитесь в наличие файла *.vbe, полученного в результате экспорта справочников, ключей и настроек на действующем ViPNet Coordinator HW. Вместе с файлом *.vbe вам должен быть предоставлен пароль, на котором он зашифрован. Данный пароль потребуется ввести при выполнении импорта данных из файла *.vbe.



Примечание. При экспорте файл *.vbe автоматически зашифровывается на текущем пароле пользователя.

Кроме этого, если импорт справочников, ключей и настроек выполняется на ViPNet Coordinator HW, на котором уже установлены справочники и ключи, то удалите их перед началом импорта с помощью команды:

```
hostname# admin remove keys
```

В противном случае, импорт данных будет невозможен.



Примечание. При удалении справочников и ключей удаляется информация об используемом способе аутентификации пользователя ViPNet Coordinator HW. Если до удаления справочников и ключей использовался способ аутентификации по устройству, то после удаления и импорта данных из файла *.vbe будет доступен только способ аутентификации по паролю. Для возврата способа аутентификации по устройству следует вручную изменить способ аутентификации. Подробнее см. документ «ViPNet Coordinator HW. Настройка с помощью командного интерпретатора», раздел «Настройка параметров безопасности».

Для импорта справочников, ключей и настроек на координатор ViPNet Coordinator HW выполните все действия из приведенной ниже таблицы в предложенном порядке.

Таблица 6. Последовательность импорта справочников, ключей и настроек

Действие	Ссылка
<input type="checkbox"/> Иницируйте импорт справочников, ключей и настроек на ViPNet Coordinator HW	Начало установки (на стр. 27)
<input type="checkbox"/> Укажите часовой пояс, дату и время	Настройка часового пояса, даты и времени (на стр. 28)
<input type="checkbox"/> Выберите файл экспорта *.vbe	Установка дистрибутива ключей на ViPNet Coordinator HW (на стр. 30)
<input type="checkbox"/> Перезагрузите компьютер	Завершение установки (на стр. 42)

5

Замена элемента питания CMOS BIOS и установка SIM-карты

Замена элемента питания CMOS BIOS	67
Установка SIM-карты в ViPNet Coordinator HW50 N3 и HW100 N3	78

Замена элемента питания CMOS BIOS

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

- ViPNet Coordinator HW1000 Q3;
- ViPNet Coordinator HW1000 Q4;
- ViPNet Coordinator HW2000 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 следующую команду:

```
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, для этого выполните следующие действия:
 - Открутите винты на корпусе, как показано на одном из следующих рисунков в зависимости от исполнения ViPNet Coordinator HW:



Рисунок 18. Расположение трех винтов на корпусе ViPNet Coordinator HW1000 Q3/Q4



Рисунок 19. Расположение двух винтов на задней панели ViPNet Coordinator HW2000 Q3

- Сдвиньте крышку в сторону задней панели на расстояние около 2 см и отсоедините ее от корпуса, как показано на одном из следующих рисунков в зависимости от исполнения ViPNet Coordinator HW:



Рисунок 20. Снятие верхней крышки корпуса ViPNet Coordinator HW1000 Q3/Q4



Рисунок 21. Снятие верхней крышки корпуса ViPNet Coordinator HW2000 Q3

- 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 исполнения ViPNet Coordinator HW:

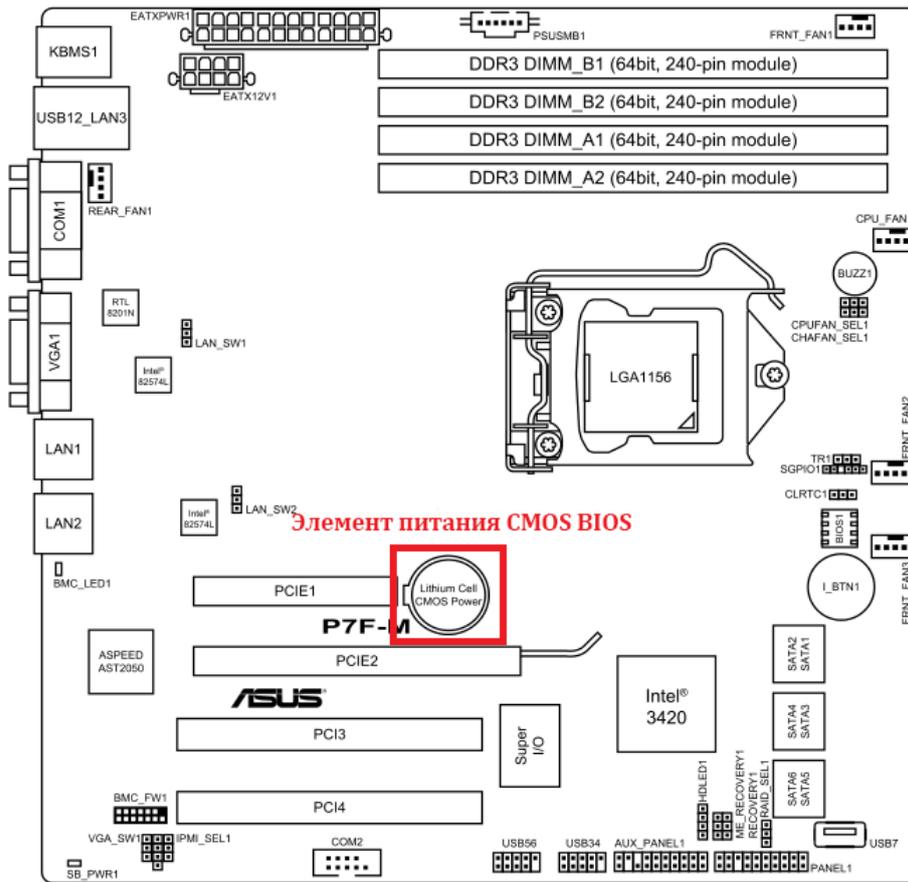


Рисунок 22. Расположение элемента питания на материнской плате ViPNet Coordinator HW1000 Q3

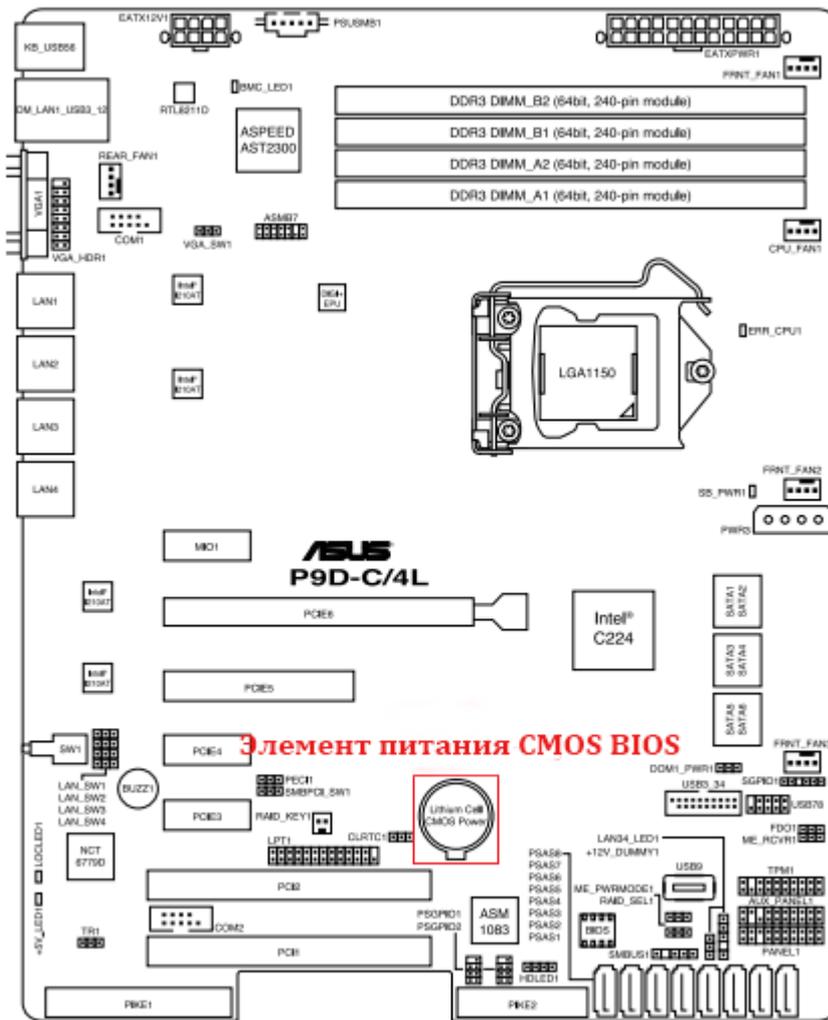
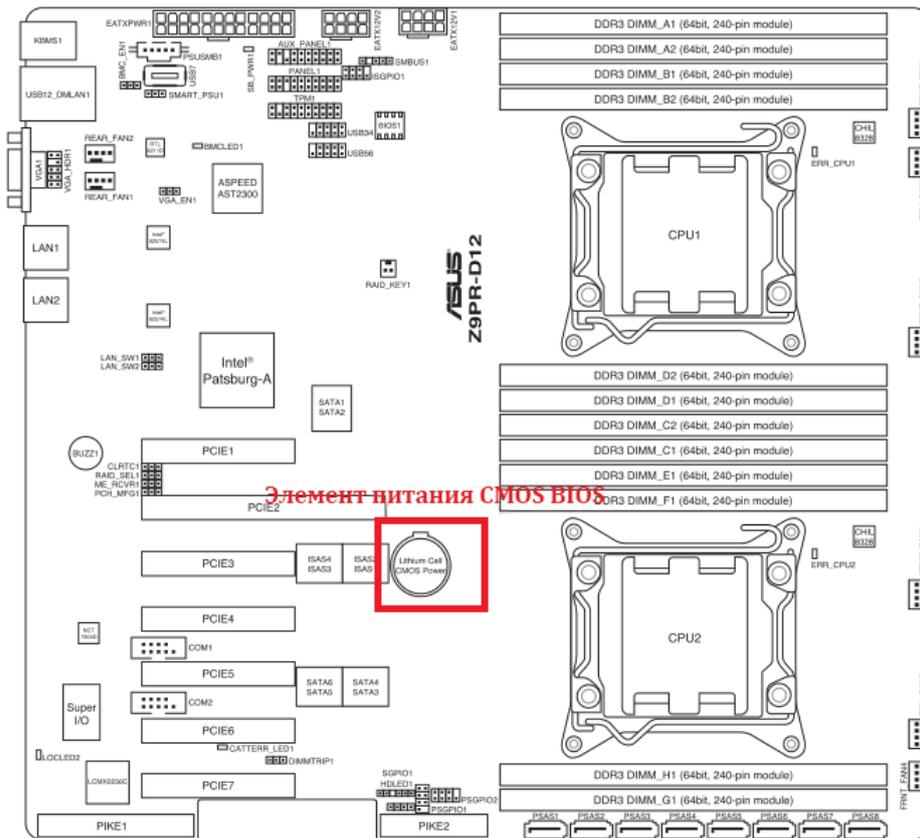


Рисунок 23. Расположение элемента питания на материнской плате ViPNet Coordinator HW1000 Q4



Элемент питания CMOS BIOS

Рисунок 24. Расположение элемента питания на материнской плате ViPNet Coordinator HW2000 Q3

- 5 С помощью пинцета или отвертки с плоским наконечником отогните защелку гнезда элемента питания и извлеките элемент питания, как показано на следующем рисунке:

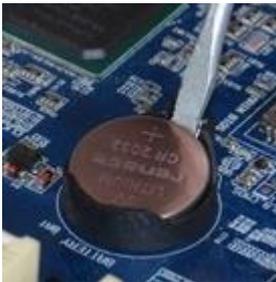


Рисунок 25. Извлечение элемента питания CMOS BIOS из гнезда на материнской плате

- 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 исполнения ViPNet Coordinator HW:



Рисунок 26. Нанесение пломбы на корпус ViPNet Coordinator HW1000 Q3/Q4



Рисунок 27. Нанесение пломбы на корпус ViPNet Coordinator HW2000 Q3

- 8 Подключите кабель питания и включите питание ViPNet Coordinator HW.
- 9 Настройте параметры BIOS (см. «[Настройка параметров BIOS](#)» на стр. 72).

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.

Параметры настроек BIOS зависят от исполнения ПАК ViPNet Coordinator HW и приведены в соответствующих разделах:

- [Параметры настройки BIOS для ViPNet Coordinator HW1000](#) (на стр. 73).
- [Параметры настройки BIOS для ViPNet Coordinator HW2000 Q3](#) (на стр. 76).

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 ViPNet Coordinator HW1000

Таблица 7. Параметры настройки BIOS для ViPNet Coordinator HW1000 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	
Server > Remote Access Configuration	Remote Access	Disabled	
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	

Пункт меню/подменю	Параметр	Значение	Примечание
Boot > Security	Change Supervisor Password		Необходимо задать пароль с максимальным числом символов
	Change User Password		Необходимо задать пароль с максимальным числом символов

Таблица 8. Параметры настройки BIOS для ViPNet Coordinator HW1000 Q4

Пункт меню/подменю	Параметр	Значение	Примечание
Advanced > CPU Configuration	Hyper-Threading	Enabled	
	Intel Virtualization Technology	Disabled	
Advanced > SATA Configuration	SATA Controller(s)	Enabled	
	SATA Mode Selection	AHCI	
Advanced > PCI Subsystem Settings	Above 4G Decoding	Disabled	
Advanced > TPM	TPM Support	Disabled	
Advanced > ACPI Settings	Enable Hibernation	Disabled	
	ACPI Sleep State	Suspend Disabled	
Advanced > NCT6779D Super IO Configuration > Serial Port 1 Configuration	Serial Port	Disabled	
Advanced > NCT6779D Super IO Configuration > Serial Port 2 Configuration	Serial Port	Enabled	
	Change Settings	IO=3F8h; IRQ=3,4,5,6,7,10,11,12	
Advanced > NCT6779D Super IO Configuration > Parallel Port Configuration	Parallel Port	Disabled	
Advanced > Onboard LAN Configuration	Intel I210 LAN1 OpROM	Disabled	

Пункт меню/подменю	Параметр	Значение	Примечание
	Intel I210 LAN2 OpROM	Disabled	
	Intel I210 LAN3 OpROM	Disabled	
	Intel I210 LAN4 OpROM	Disabled	
Advanced > Serial Port Console Redirection	COM2 Console Redirection	Disabled	
Advanced > Runtime Error Logging	Runtime Error Logging Support	Enabled	
Advanced > APM	Restore AC Power Loss	Power On	
Advanced > Network Stack	Network Stack	Disabled	
Event Logs> Change Smbios Event Log Settings	Smbios Event Log	Enabled	
	Erase event log	No	
	When Log is Full	Erase Immediately	
Boot	Boot Device Seeking	Normal	
Boot > Boot Option Priorities	Boot Option #1	[P2: 2GB Sata Flash ...]	
	Boot Option #2	Disabled	
Boot > Hard Drive BBS Priorities	Boot Option #1	[P2: 2GB Sata Flash ...]	Необходимо указать SSD-накопитель
	Boot Option #2	Disabled	Необходимо отключить
Boot > Network Device BBS Priorities	Boot Option #[1-4]	Disabled	Необходимо отключить все варианты загрузки
Boot > CSM Parameters	Launch CSM	Enabled	
	Boot option filter	Legacy only	
	Launch PXE OpROM policy	Do not launch	
	Launch Storage OpROM police	Do not launch	

Пункт меню/подменю	Параметр	Значение	Примечание
	Launch Video OpROM policy	Legacy only	
	Other PCI device ROM priority	Legacy OpROM	
Security > Administrator Password			Необходимо задать пароль с максимальным числом символов
Security > User Password			Необходимо задать пароль с максимальным числом символов
Security > Secure Boot menu	Secure Boot	Disabled	
Exit	Boot Override		Необходимо отключить все подпункты этого пункта меню
	Launch EFI Shell from filesystem device		Необходимо отключить

Параметры настройки BIOS для ViPNet Coordinator HW2000 Q3

Таблица 9. Параметры настройки BIOS для ViPNet Coordinator 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	
Advanced > ACPI Settings	Enable Hibernation	Disabled	

Пункт меню/подменю	Параметр	Значение	Примечание
Advanced > APM	Restore AC Power Loss	Power On	
Advanced > Serial Port Console Redirection	COM2 Console Redirection	Disabled	
Advanced > Onboard LAN Configuration	Intel W82574L OpROM[1-4]	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 > Hard Drive BBS Priorities	Boot Option #1	[SATA P1: 2Gb SATA...]	В качестве первого накопителя должен быть указан SSD-диск
	Boot Option #2	Disabled	
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 с максимальным числом символов
	User Password		Необходимо удалить пароль, если он задан
Security > Secure Boot menu	Secure Boot	Disabled	

Установка SIM-карты в ViPNet Coordinator HW50 N3 и HW100 N3

Исполнения 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-PCle, открутите крепежный винт и снимите ее.



Рисунок 28. Плата mini-PCle в исполнениях ViPNet Coordinator HW50 N3 и HW100 N3

- 4 В исполнении ViPNet Coordinator HW50 разъем для крепления SIM-карты находится на плате mini-PCle. Вставьте SIM-карту в разъем.

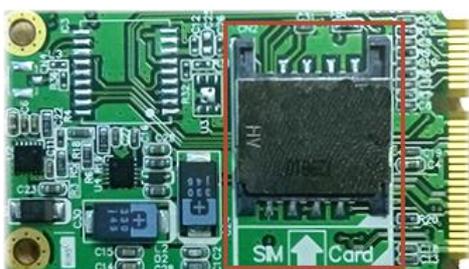


Рисунок 29. Разъем для установки SIM-карты в ViPNet Coordinator HW50 N3

- 5 В исполнении ViPNet Coordinator HW100 N3 разъем для крепления SIM-карты расположен на материнской плате под платой mini-PCIe. Откройте крышку разъема и установите SIM-карту.

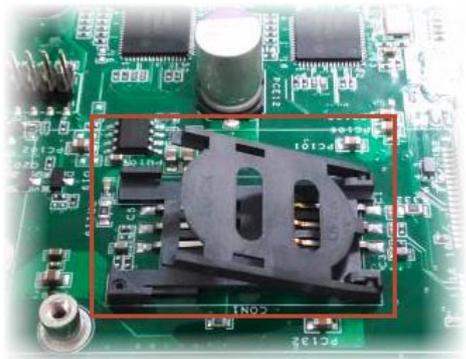


Рисунок 30. Разъем для установки SIM-карты в ViPNet Coordinator HW100 N3

- 6 Установите плату mini-PCIe в исходное положение и зафиксируйте ее крепежным винтом.
- 7 Соберите корпус ViPNet Coordinator HW.

А

Глоссарий

DHCP-сервер

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

DNS-сервер

Сервер, содержащий часть базы данных DNS, используемой для доступа к именам компьютеров 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.

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.

ViPNet Центр управления сетью (ЦУС)

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

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;

- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

Администратор сети ViPNet

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

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 узлы работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удаленных узлов в приложениях ViPNet.

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.

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).

Мастер-ключ

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

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

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

Межсетевой экран

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

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.

Сервер IP-адресов

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

Справочники и ключи

Справочники, ключи узла и ключи пользователя.

Транспортный сервер

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

В

Указатель

О

Oracle VM VirtualBox - 14

У

VMware vSphere ESXi - 14

З

Завершение установки - 27, 32, 41, 65

И

Импорт справочников, ключей и настроек - 47, 48

К

Компрометация ключей - 43

Конвертация правил защищенной сети при обновлении до версии 4.x - 52

Конвертация правил открытой и защищенной сети - 46, 48

Конвертация правил открытой сети при обновлении до версии 4.x - 52

Л

Локальное обновление ПО - 50

М

Мастер-ключ - 43

Н

Настройка DNS-сервера - 27, 32

Настройка NTP-сервера - 27, 33

Настройка имени компьютера и диапазона виртуальных адресов - 27, 34, 40

Настройка параметров BIOS - 72

Настройка подключения к внешней сети через межсетевой экран - 27, 36, 40

Настройка сетевых интерфейсов - 27, 32, 36, 40

Настройка часового пояса, даты и времени - 27, 65

Начало установки - 27, 65

О

Обновление ПО ViPNet Coordinator HW на кластере горячего резервирования - 49

Обновление программного обеспечения - 62, 64

Особенности обновления ПО - 47, 48

П

Параметры настройки BIOS для ViPNet

Coordinator HW1000 - 72

Параметры настройки BIOS для ViPNet

Coordinator HW2000 Q3 - 72

Персональный ключ пользователя - 23, 31

Подготовка к установке справочников и
ключей с помощью внешнего устройства - 10,
24

Подготовка к установке справочников и
ключей с помощью ноутбука по Ethernet-
каналу и протоколу TFTP - 10, 24

Проверка связи с другим сетевым узлом - 27,
36, 38

Р

Развертывание виртуального образа ViPNet

Coordinator HW - 10

Резервное копирование и восстановление
настроек - 23, 52

С

Способы установки и подготовка к установке
справочников и ключей - 10, 64

У

Установка дистрибутива ключей на ViPNet

Coordinator HW - 27, 65

Установка справочников и ключей - 10, 21

Установка, обновление и удаление
справочников и ключей - 18, 44

Э

Экспорт справочников, ключей и настроек -
46, 47, 48