



ViPNet Coordinator KB 4

Подготовка к работе

Версия продукта: 4.3.3

© АО «ИнфоТеКС», 2024

ФРКЕ.465614.001РЭ1

Версия продукта 4.3.3, документация обновлена 17.05.2024

Этот документ входит в комплект поставки продукта ViPNet, 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 АО «ИнфоТеКС».

ViPNet[®] является зарегистрированным товарным знаком АО «ИнфоТеКС».

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

АО «ИнфоТеКС»

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

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение.....	6
О документе.....	7
Для кого предназначен документ	7
Соглашения документа.....	7
Комплект поставки.....	8
Что нового в версии 4.3.3.....	9
Обратная связь.....	10
 Глава 1. Общая информация	11
Назначение ViPNet Coordinator KB.....	12
Защищенная сеть ViPNet	13
Основные функции ViPNet Coordinator KB.....	15
Сервер IP-адресов.....	15
Маршрутизатор VPN-пакетов	16
Сервер соединений	16
VPN-шлюз.....	17
Межсетевой экран	18
Транспортный сервер MFTP.....	19
Дополнительные возможности ViPNet Coordinator KB.....	21
Способы подключения ViPNet Coordinator KB к внешней сети	22
Подключение без использования внешнего меж сетевого экрана	22
Подключение через межсетевой экран со статической трансляцией адресов	22
Подключение через межсетевой экран с динамической трансляцией адресов.....	23
 Глава 2. Описание исполнений	25
Исполнения ViPNet Coordinator KB100	26
Аппаратная платформа KB100 N1	26
Аппаратные платформы KB100 Q1/Q2.....	27
Исполнения ViPNet Coordinator KB1000	29
Аппаратная платформа KB1000 Q6.....	29
Аппаратная платформа KB1000 Q8.....	30
Исполнения ViPNet Coordinator KB2000	32
Аппаратная платформа KB2000 Q4.....	32
Аппаратная платформа KB2000 Q5.....	33
Исполнения ViPNet Coordinator KB5000	35

Аппаратная платформа KB5000 Q1	35
Аппаратная платформа KB5000 Q2	36
Коммутация сетевых портов SFP+	38
Поддерживаемое дополнительное оборудование	39
Меры безопасности и предосторожности	41
Глава 3. Ввод в эксплуатацию.....	43
Порядок действий.....	44
Установка справочников и ключей	45
Начало установки	45
Настройка часового пояса, даты и времени.....	46
Установка дистрибутива ключей на ViPNet Coordinator KB	48
Настройка сетевых интерфейсов.....	50
Настройка DNS-сервера	51
Настройка NTP-сервера	52
Настройка имени ViPNet Coordinator KB и диапазона виртуальных адресов	53
Настройка подключения к внешней сети через межсетевой экран	54
Проверка связи с другим узлом сети ViPNet.....	57
Завершение установки	59
Использование ключевого блокнота ДСДР	61
Назначение ключевых блокнотов ДСДР	61
Установка ключевого блокнота ДСДР	62
Смена ключевого блокнота ДСДР	62
Просмотр информации об установленных ключах.....	66
Обновление справочников и ключей	67
Глава 4. Возможности управления	68
Способы управления ViPNet Coordinator KB.....	69
Управление с помощью административного ПО ViPNet.....	70
Управление с помощью командного интерпретатора	71
Работа с учетной записью пользователя ViPNet Coordinator KB	72
Управление с помощью веб-интерфейса.....	73
Режимы работы	74
Экстренное стирание ключевой информации.....	75
Глава 5. Лицензирование и функциональные ограничения	76
Лицензирование ViPNet Coordinator KB.....	77
Ограничения на количество связей с ViPNet-узлами.....	78
Ограничения при использовании ViPNet Coordinator KB в защищенной сети ViPNet	79

Каскадная схема включения	79
Подключение через промежуточный ViPNet Coordinator KB.....	80
Прочие ограничения при использовании в сети ViPNet	80
Глава 6. История версий ViPNet Coordinator KB	82
Что нового в версии 4.3.2	83
Что нового в версии 4.3.1	84
Что нового в версии 4.3.0	85
Что нового в версии 4.2.1	88
Что нового в версии 4.2.0	89
Приложение А. Глоссарий	91
Приложение В. Изменения в документации.....	97



Введение

О документе	7
Комплект поставки	8
Что нового в версии 4.3.3	10
Обратная связь	10

О документе

В документе описывается назначение и применение программно-аппаратного комплекса ViPNet Coordinator KB 4 (далее — ViPNet Coordinator KB) в составе защищенных сетей ViPNet, способы его настройки и управления. Приводится описание существующих исполнений ViPNet Coordinator KB, их аппаратных платформ и условий лицензирования.

Для кого предназначен документ

Документ предназначен для администраторов ViPNet Coordinator KB.

Соглашения документа

Обозначение	Описание
	Внимание! Содержит критически важную информацию
	Примечание. Содержит рекомендательную информацию
	Совет. Содержит полезные приемы и хорошие практики
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская ее, нажмите вторую
Меню > Команда	Последовательность элементов или действий
Код	Имя файла, путь, фрагмент кода или команда в командной строке



Примечание. В документе могут присутствовать снимки интерфейса из предыдущих версий продукта. Поэтому некоторые элементы интерфейса, которые не влияют на понимание текста, могут выглядеть не так, как в продукте.

Комплект поставки

В комплект поставки ViPNet Coordinator KB входят следующие компоненты:

- Программно-аппаратный комплекс ViPNet Coordinator KB 4, в зависимости от исполнения (см. [Описание исполнений](#) на стр. 25).
- Документация в формате PDF:
 - «ViPNet Coordinator KB 4. Правила пользования».
 - «ViPNet Coordinator KB 4. Подготовка к работе».
 - «ViPNet Coordinator KB 4. Настройка с помощью командного интерпретатора».
 - «ViPNet Coordinator KB 4. Настройка с помощью веб-интерфейса».
 - «ViPNet Coordinator KB 4. Справочник команд и конфигурационных файлов».
 - «ViPNet Coordinator KB 4. Лицензионные соглашения на компоненты сторонних производителей».
 - Копии сертификатов соответствия ФСБ России на программно-аппаратный комплекс ViPNet Coordinator KB 4.
- Документация в печатном виде:
 - «ViPNet Coordinator KB 4. Формуляр».

Что нового в версии 4.3.3

- **Поддержка новых аппаратных платформ**

Добавлена поддержка новых аппаратных платформ:

- KB100 Q1.
- KB100 Q2.

Технические характеристики платформ приведены в разделе [«Аппаратные платформы KB100 Q1/Q2»](#).

- **Расширенная инвентаризация**

В новой версии ViPNet Coordinator KB добавлена дополнительная информация об аппаратных и программных компонентах. В командном интерпретаторе и веб-интерфейсе выводится следующая информация:

- Наименование продукта и исполнения;
- Серийный номер;
- Серийный номер ДНСД.
- Дополнительная маркировка — на корпусе размещен QR-код со следующей информацией:
 - Наименование продукта и исполнения.
 - Серийный номер продукта.
 - Серийный номер ДНСД.
 - Регистрационный номер СКЗИ.

- **Удаленная смена мастер-ключей**

Теперь при смене мастер-ключей в сети ViPNet вы можете удаленно обновить справочно-ключевую информацию на ViPNet Coordinator KB.

- **Локальное обновление справочников и ключей**

Добавлена возможность локального обновления справочников и ключей без удаления настроек. Для этого в ViPNet Coordinator KB добавлена команда `admin keys update`.

- **Поддержка нового токена**

Новая версия ViPNet Coordinator KB поддерживает токен Рутокен Lite 1010.

- **Обновлен список NTP-серверов по умолчанию**

Список NTP-серверов по умолчанию теперь включает: `ntp1.vniiftri.ru`, `ntp1.vniiftri.ru`, `ntp.ix.ru`.

- **Исправление ошибок**

Исправлены ошибки, выявленные в ходе эксплуатации предыдущих версий ViPNet Coordinator KB, повышена стабильность работы.

Обратная связь

Дополнительная информация

Сведения о продуктах ViPNet, частые вопросы и полезная информация на сайте ИнфоТеКС:

- [Информация о продуктах ViPNet.](#)
- [Информация о решениях ViPNet.](#)
- [Часто задаваемые вопросы.](#)
- [Форум пользователей продуктов ViPNet.](#)

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ИнфоТеКС:

- Единый многоканальный телефон:
+7 (495) 737-6192,
8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба поддержки: hotline@infotecs.ru.
[Форма для обращения в службу поддержки через сайт.](#)
Канал поддержки в Telegram: t.me/vhd21
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

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

1

Общая информация

Назначение ViPNet Coordinator KB	12
Защищенная сеть ViPNet	13
Основные функции ViPNet Coordinator KB	15
Дополнительные возможности ViPNet Coordinator KB	21
Способы подключения ViPNet Coordinator KB к внешней сети	22

Назначение ViPNet Coordinator KB

ViPNet Coordinator KB — шлюз безопасности (криптошлюз), обеспечивающий защиту и конфиденциальность при передаче информации. ViPNet Coordinator KB использует технологию ViPNet VPN и при выполнении требований и рекомендаций, изложенных в документации, обеспечивает защиту информации по классу KB требований ФСБ России к средствам криптографической защиты информации (СКЗИ).

ViPNet Coordinator KB выступает в роли VPN-сервера и предназначен для использования в виртуальной защищенной сети, построенной на основе комплекса продуктов ViPNet. Сеть ViPNet обеспечивает защищенную передачу информации между узлами по схеме «клиент-клиент» и может разворачиваться поверх локальных или глобальных сетей любой структуры. Подробное описание функций ViPNet Coordinator KB приведено в разделе [Основные функции ViPNet Coordinator KB](#) (на стр. 15).

ViPNet Coordinator KB распространяется в нескольких исполнениях. Каждое исполнение ViPNet Coordinator KB представляет собой решение на базе специализированной аппаратной платформы и специального программного обеспечения ViPNet (СПО ViPNet Coordinator KB), которое функционирует под управлением адаптированной ОС GNU/Linux, а также роли, назначаемой сетевому узлу в программе [ViPNet Центр управления сетью \(ЦУС\)](#) и накладывающей определенные лицензионные ограничения (см. [Лицензирование ViPNet Coordinator KB](#) на стр. 77).

В качестве аппаратных платформ для исполнений ViPNet Coordinator KB используется компактный компьютер или сервер, устанавливаемый в стандартные телекоммуникационные стойки. Характеристики всех поддерживаемых исполнений приведены в главе Описание исполнений ViPNet Coordinator KB (см. [Описание исполнений](#) на стр. 25).

Защищенная сеть ViPNet

Сеть ViPNet — виртуальная защищенная сеть, которая может быть развернута поверх локальных и глобальных IP-сетей. Технология ViPNet обеспечивает создание защищенных VPN-туннелей между узлами сети ViPNet с помощью протоколов трех типов: IP/241, UDP и TCP, в которые инкапсулируются пакеты любых других IP-протоколов. Данные, передаваемые в VPN-туннелях, зашифровываются с помощью симметричных ключей; ключи шифрования создаются и распределяются централизованно. Каждая сеть ViPNet имеет свой уникальный идентификатор.

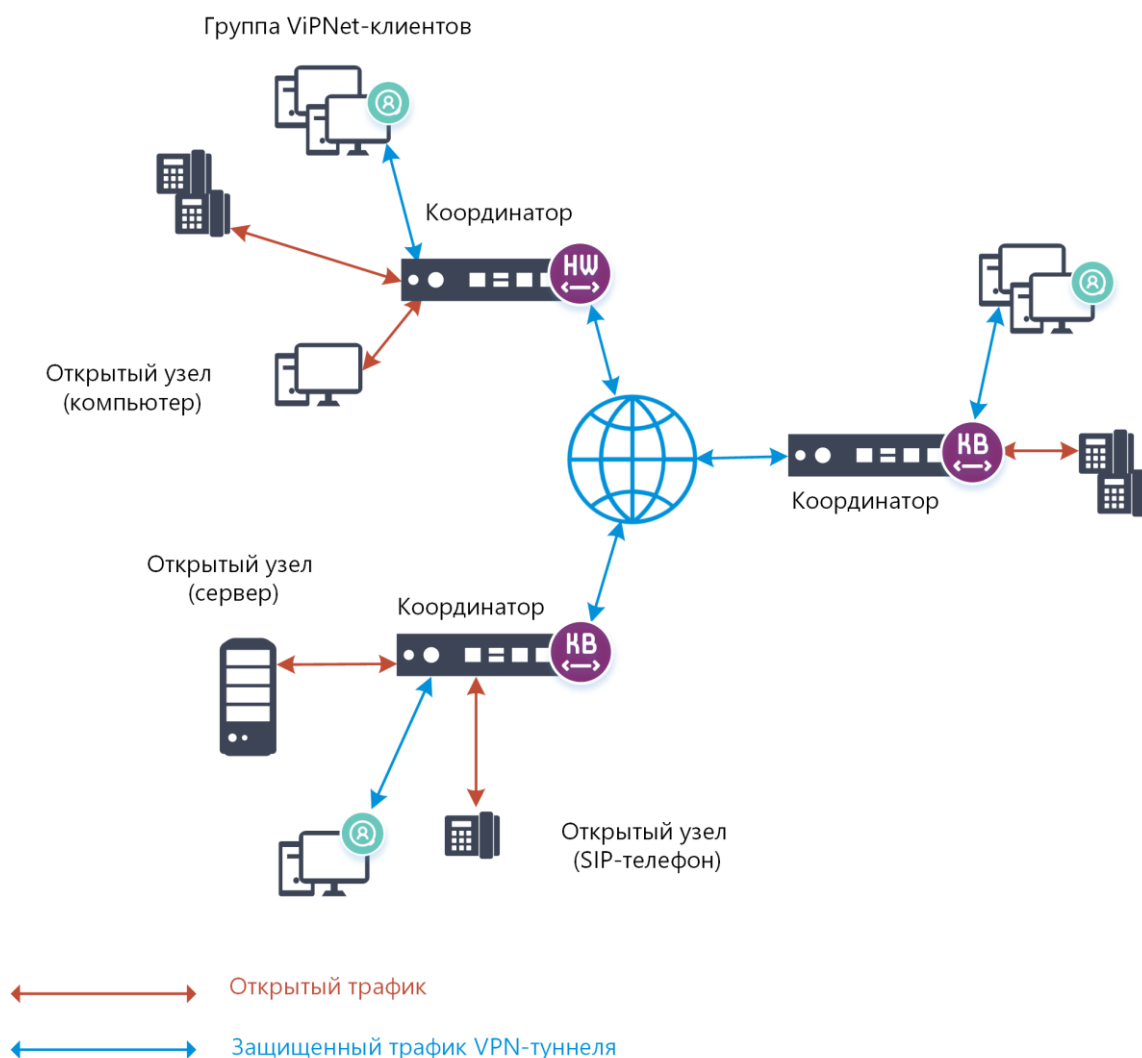


Рисунок 1. Типы узлов сети ViPNet

Типы узлов сети ViPNet:

- **ViPNet-клиент** — компьютер или мобильное устройство с установленным клиентским ПО ViPNet для рабочих станций (Windows, Linux, macOS) и мобильных платформ (iOS, Android или Аврора).

- ViPNet-координатор — исполнение ViPNet Coordinator KB на специализированной аппаратной платформе. В сети ViPNet координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.
- Открытый узел — компьютер без ПО ViPNet или другое устройство, например SIP-телефон, расположенные в сети «за ViPNet-координатором».

ViPNet Coordinator KB совместим со следующими версиями продуктов ViPNet:

- ViPNet Client версии 4.5.3 и выше.
- ViPNet Client for Linux версии 4.8.0 и выше.
- ViPNet Client for Android версии 4.0.0 и выше.
- ViPNet Client for iOS версии 4.1.1 и выше.
- ViPNet Client for Aurora версии 3.1 и выше.
- ViPNet Administrator версии 4.6.4 и выше.
- ViPNet PolicyManager версии 4.5.1 и выше.
- ViPNet StateWatcher версии 4.9.1 и выше.
- ViPNet Coordinator HW версии 4.3.2 и выше.
- ViPNet xFirewall версии 5.4.0 и выше.
- Все предыдущие версии ViPNet Coordinator KB.

Настройка и управление сетью ViPNet выполняется с помощью административного ПО [ViPNet Administrator](#). Основные функции:

- Создание узлов сети ViPNet и связей между ними.
- Настройка узлов сети ViPNet.
- Создание дистрибутивов ключей для узлов сети ViPNet.
- Централизованное обновление справочников и ключей.

Управление [политиками безопасности](#) узлов сети ViPNet выполняется централизованно с помощью [ViPNet Policy Manager](#). Для мониторинга состояния узлов сети ViPNet используется [ViPNet StateWatcher](#).

Основные функции ViPNet Coordinator KB

К основным функциям ViPNet Coordinator KB, обеспечивающим работу сети ViPNet, относятся:

- **Сервер IP-адресов** (на стр. 15). Обеспечить взаимодействие защищенных узлов ViPNet. Сервер IP-адресов сообщает сетевым узлам информацию об адресах и параметрах доступа других узлов.
- **Маршрутизатор VPN-пакетов** (на стр. 16). Функция, которая позволяет обеспечить маршрутизацию транзитного защищенного IP-трафика, проходящего через координатор на другие защищенные узлы.
- **Сервер соединений** (на стр. 16). Функция, которая обеспечивает соединение клиентов и координаторов друг с другом кратчайшим путем.
- **VPN-шлюз** (на стр. 17). Функция, которая позволяет организовать защищенные соединения между узлами локальных сетей (на которых не установлено ПО ViPNet) и между сегментами сетей с помощью защищенных каналов (туннелей).
- **Межсетевой экран** (на стр. 18). Функция, которая позволяет обеспечить фильтрацию IP-трафика. Одновременно координатор может выполнять функции трансляции сетевых адресов для проходящего через него открытого трафика.
- **Транспортный сервер** (см. Транспортный сервер MFTP на стр. 19). Функция, которая обеспечивает доставку на сетевые узлы ViPNet управляющих сообщений, обновлений справочников, ключей и программного обеспечения из программы ViPNet Центр управления сетью (ЦУС), а также обмен прикладными **транспортными конвертами** между узлами.

Сервер IP-адресов

Клиенту для взаимодействия с другими защищенными узлами требуется информация об адресах и параметрах доступа. Данную информацию клиент получает автоматически от координатора, который выполняет функцию сервера IP-адресов.

Принцип работы сервера IP-адресов:

- При появлении новой информации о клиенте, который использует данный координатор в качестве сервера IP-адресов, координатор рассылает ее на связанные клиенты и координаторы.
- При появлении новой информации о клиентах других координаторов, координатор рассылает эту информацию на свои клиенты, которые связаны с клиентами другого координатора.
- В случае взаимодействия координатора с другой сетью ViPNet на шлюзовой координатор другой сети высылаются информация о состоянии всех узлов своей сети, связанных с узлами другой сети ViPNet. При получении такой информации из другой сети ViPNet координатор

рассылает эту информацию на все координаторы своей сети, а также на свои клиенты, связанные с узлами другой сети.

Также сервер IP-адресов рассылает информацию о статусе сетевого узла. Чтобы подтвердить свое присутствие в сети, клиент периодически (по умолчанию — каждые 5 минут) отправляет на сервер сообщение о своей активности. Если такое сообщение не поступило, координатор переводит клиент в статус «Недоступен» и оповещает другие узлы, с которыми у данного клиента есть связь.

Аналогичным образом происходит обмен информацией о параметрах доступа между координаторами. Периодически (по умолчанию — каждые 15 минут) координатор отсылает на другие связанные с ним координаторы подтверждение о своей активности.

По умолчанию для клиента в качестве сервера IP-адресов выступает координатор, на котором клиент зарегистрирован в ViPNet Administrator. Сервер IP-адресов можно сменить, выбрав другой координатор, с которым у данного клиента есть связь.

Маршрутизатор VPN-пакетов

Координатор выполняет **маршрутизацию** транзитного защищенного трафика, передаваемого на другие защищенные узлы. Трафик маршрутизируется как внутри одной сети ViPNet, так и при взаимодействии с другими сетями ViPNet.

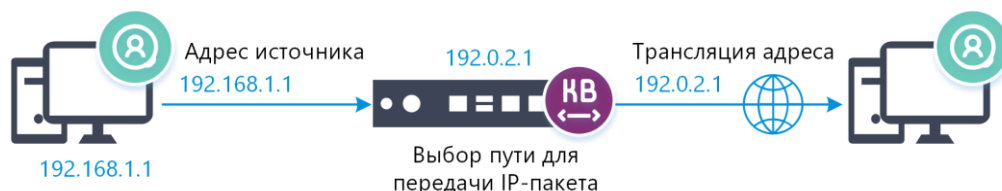


Рисунок 2. Функция маршрутизации защищенного трафика в сети ViPNet

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

Сервер соединений

Когда на границе сети ViPNet установлено стороннее устройство, выполняющее фильтрацию и трансляцию трафика, клиенты не могут установить соединение напрямую. В таком случае соединение устанавливается через координатор, выполняющий функцию **сервера соединений**.

Для каждого сетевого узла (клиента и координатора) можно назначить свой сервер соединений. По умолчанию сервером соединений для клиента служит координатор, выполняющий функцию сервера IP-адресов.



Рисунок 3. Организация соединений между сетевыми узлами ViPNet

Когда удаленный клиент не может получить доступ к сети ViPNet по протоколу UDP (интернет-провайдер блокирует протокол UDP), он автоматически устанавливает связь через TCP-туннель своего сервера соединений. На сервере полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узлы назначения по протоколу UDP.



Рисунок 4. Доступ удаленного клиента к сети ViPNet через TCP-туннель

VPN-шлюз

Координатор защищает соединения между узлами сети, которые обмениваются информацией через публичные сети. Для защиты соединения используется [туннелирование](#). Координатор может выполнять туннелирование на сетевом (L3) или канальном (L2) уровнях модели OSI.

Туннелирование на сетевом уровне позволяет организовать защищенное соединение между открытым и защищенным узлом или между двумя открытыми узлами, которые туннелируются разными координаторами. Туннелирование на сетевом уровне выполняется следующим образом:

- 1 IP-пакеты от открытых узлов поступают на координатор и обрабатываются сетевыми фильтрами.
- 2 Обработанные IP-пакеты зашифровываются и инкапсулируются в новые IP-пакеты, после чего передаются:
 - На защищенные узлы назначения.
 - На другой координатор для открытых узлов назначения.
- 3 На другом координаторе из зашифрованных IP-пакетов извлекаются исходные IP-пакеты, расшифровываются, обрабатываются сетевыми фильтрами и передаются на открытые узлы назначения.

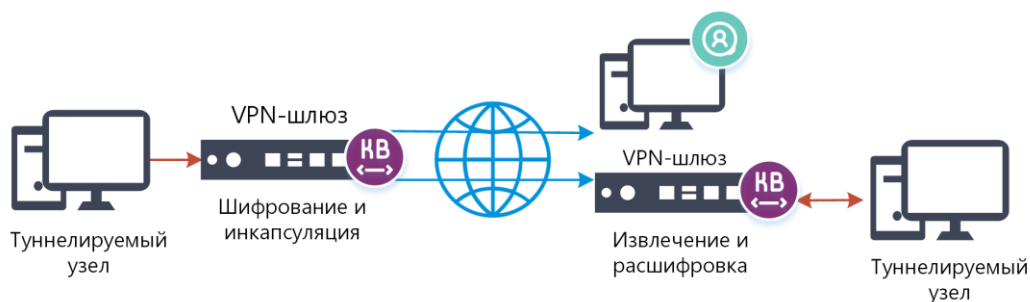


Рисунок 5. Защита соединения на сетевом уровне модели OSI

Туннелирование на канальном уровне, или **L2OverIP**, позволяет организовать защищенное соединение между узлами удаленных друг от друга сегментов сети так, что они находятся в одном широковещательном домене. На узлах сегментов сети, связанных через L2OverIP, используется адресное пространство в пределах одной IP-подсети.

Туннелирование на канальном уровне работает следующим образом:

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

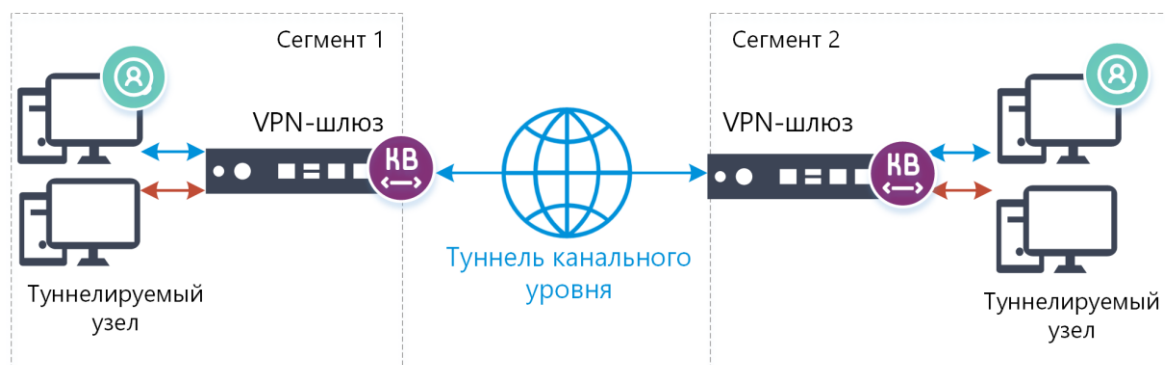


Рисунок 6. Защита соединения на канальном уровне модели OSI

Межсетевой экран

Координатор выполняет фильтрацию IP-пакетов на каждом сетевом интерфейсе по адресам, протоколам и портам в соответствии с настроенными сетевыми фильтрами. С помощью сетевых фильтров можно не только заблокировать нежелательные соединения, но и разрешить соединения с открытыми узлами, не входящими в сеть ViPNet. Также межсетевой экран защищает от одной из распространенных сетевых атак — спуфинга.

ViPNet Coordinator KB может осуществлять [трансляцию сетевых адресов \(NAT\)](#) для проходящего через него открытого трафика.



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

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

- Подключение локальной сети к интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг интернета количество публичных IP-адресов. В этом случае используется трансляция адреса источника, которая позволяет компьютерам с частными IP-адресами получать доступ к интернету от имени публичного IP-адреса координатора.
- Организация доступа к локальным ресурсам из внешней сети. В этом случае используется трансляция адреса назначения, которая позволяет узлам локальной сети, имеющим частные IP-адреса, быть доступными пользователям интернета по публичным IP-адресам.

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

Для поддержки пользовательских сетевых сервисов, например IP-телефонии, координатор выполняет обработку прикладных протоколов: FTP, DNS, H.323, SCCP, SIP.

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

Транспортный сервер MFTP

Защищенные сетевые узлы, поддерживающие работу с дистрибутивом ключей `dst`, обмениваются [транспортными конвертами MFTP](#), в которых содержатся:

- управляющие сообщения;
- обновления справочников и ключей из системы управления;
- сообщения служб и приложений.

Транспортный сервер MFTP принимает конверты от других узлов сети ViPNet и пересылает их на узел назначения.

При поступлении прикладного или управляющего конверта транспортный сервер MFTP в соответствии с маршрутными таблицами определяет дальнейший путь передачи этого конверта.

Получив конверт, транспортный сервер выполняет одно из действий, в зависимости от заданных параметров:

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

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

Функцию транспортного сервера MFTP выполняет координатор, на котором зарегистрирован клиент. Транспортный сервер изменить нельзя.

Дополнительные возможности ViPNet Coordinator KB

Помимо базовых функций, ViPNet Coordinator KB поддерживает дополнительные функции, расширяющие возможности по обработке сетевого трафика и интеграции со сторонним оборудованием (коммутаторами, маршрутизаторами, ИБП):

- Обработка протоколов прикладного уровня: FTP, DNS, H.323, SCCP.
- Работа с виртуальными локальными сетями VLAN IEEE 802.1Q.
- Агрегирование сетевых интерфейсов IEEE 802.3ad.
- Поддержка классификации сетевого трафика DiffServ для обеспечения качества обслуживания (QoS).
- Статическая и динамическая (DHCP, OSPF v2) маршрутизация IP-трафика.
- Распределение нагрузки между каналами связи и резервирование каналов связи.
- Встроенные DHCP-, DNS- и NTP-серверы.
- Система защиты от сбоев для контроля собственной работоспособности и создания кластера горячего резервирования на базе двух ViPNet Coordinator KB.
- Совместимость с управляющим программным обеспечением ViPNet Administrator, ViPNet Policy Manager, ViPNet StateWatcher.
- Взаимодействие с источником бесперебойного питания (ИБП).

Способы подключения ViPNet Coordinator KB к внешней сети

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

- Подключение без использования внешнего межсетевого экрана (на стр. 22).
- Подключение через межсетевой экран со статической трансляцией адресов (на стр. 22).
- Подключение через межсетевой экран с динамической трансляцией адресов (на стр. 23).

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

Подключение без использования внешнего межсетевого экрана

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



Рисунок 7. Подключение координатора без использования межсетевого экрана

Подключение через межсетевой экран со статической трансляцией адресов

Если на границе локальной сети установлен межсетевой экран, выполняющий трансляцию сетевых адресов (NAT) и позволяющий настроить статические правила трансляции, между этим межсетевым экраном и узлами локальной сети следует установить координатор. На координаторе

в этом случае должны быть настроены параметры подключения через межсетевой экран со статической трансляцией адресов. Схема взаимодействия узлов сети приведена на рисунке ниже.

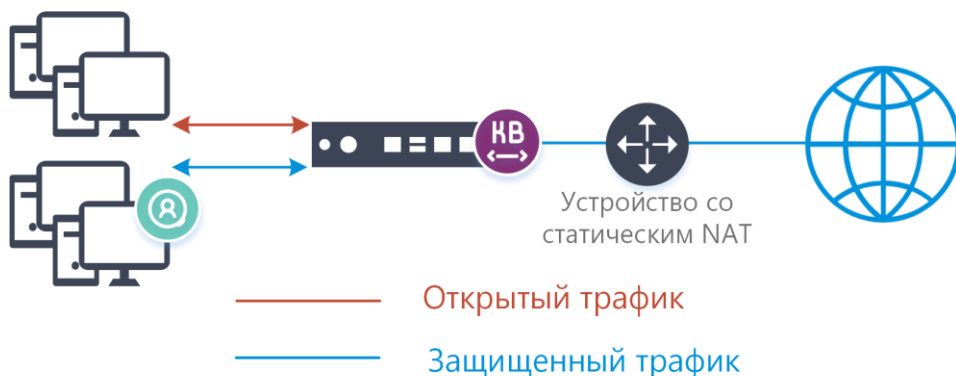


Рисунок 8. Подключение координатора через межсетевой экран со статической трансляцией адресов

Для клиентов локальной сети данный координатор следует использовать в качестве сервера соединений.

Подключение через межсетевой экран с динамической трансляцией адресов

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

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

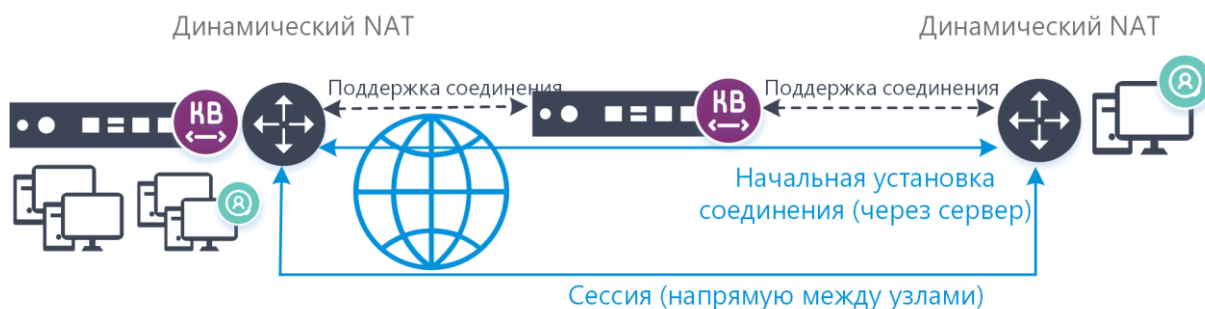


Рисунок 9. Подключение координатора через межсетевой экран с динамической трансляцией адресов

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

2

Описание исполнений

Исполнение ViPNet Coordinator KB100	26
Исполнения ViPNet Coordinator KB1000	29
Исполнения ViPNet Coordinator KB2000	32
Исполнения ViPNet Coordinator KB5000	35
Коммутация сетевых портов SFP+	38
Поддерживаемое дополнительное оборудование	39
Меры безопасности и предосторожности	41

Исполнения ViPNet Coordinator KB100

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

В исполнениях ViPNet Coordinator KB100 применяются аппаратные платформы KB100 N1, KB100 Q1, KB100 Q2 с низким энергопотреблением и с пассивным охлаждением.



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

Аппаратная платформа KB100 N1

Таблица 1. Характеристики KB100 N1

Характеристика	Описание
Форм-фактор	Мини-компьютер
Размеры (ШхВхГ)	173,8 x 42 x 151,8 мм
Масса	1 кг (без адаптера питания)
Питание	Внешний блок питания выходной мощностью 60 Вт, напряжением от 100 до 240 В, 1,5 А, 50-60 Гц
Датчик вскрытия корпуса	Есть
Кнопка экстренного стирания ключевой информации	Есть
Сетевые интерфейсы	4 x Ethernet RJ45 10/100/1000 Мбит/с 1 x Ethernet SFP 1 Гбит/с (eth4)
Порты ввода-вывода	1 порт VGA 1 порт USB 2.0 1 порт USB 3.0
Дополнительное оборудование	Кабель питания с литыми разъёмами VDE 10A, разъём евровилка Schuko C13 Самоклеющиеся наклейки «ножки»

Все коммуникационные разъёмы расположены на передней панели аппаратной платформы.

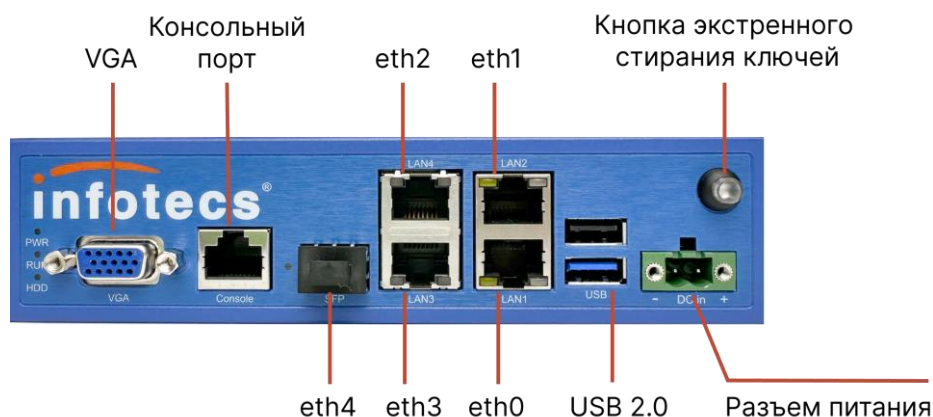


Рисунок 10. Передняя панель KB100 N1

Аппаратные платформы KB100 Q1/Q2

Таблица 2. Характеристики KB100 Q1/Q2

Характеристика	Описание
Форм-фактор	Мини-компьютер
Размеры (ШхВхГ)	250,0 x 44,0 x 232,2 мм
Масса	2,2 кг
Питание	Внешний блок питания выходной мощностью 60 Вт, напряжением от 100 до 240 В, 1,5 А, 50-60 Гц
Датчик вскрытия корпуса	Есть
Кнопка экстренного стирания ключевой информации	Есть
Сетевые интерфейсы	4 x Ethernet RJ45 10/100/1000 Мбит/с 2 x Ethernet SFP 1 Гбит/с (eth4, eth5)
Порты ввода-вывода	VGA Консольный порт RJ45 2 x USB 3.0
Дополнительное оборудование	Кабель питания с литыми разъёмами VDE 10A, разъём евровилка Schuko C13 Самоклеющиеся наклейки «ножки»

Все коммуникационные разъёмы расположены на передней панели аппаратной платформы.

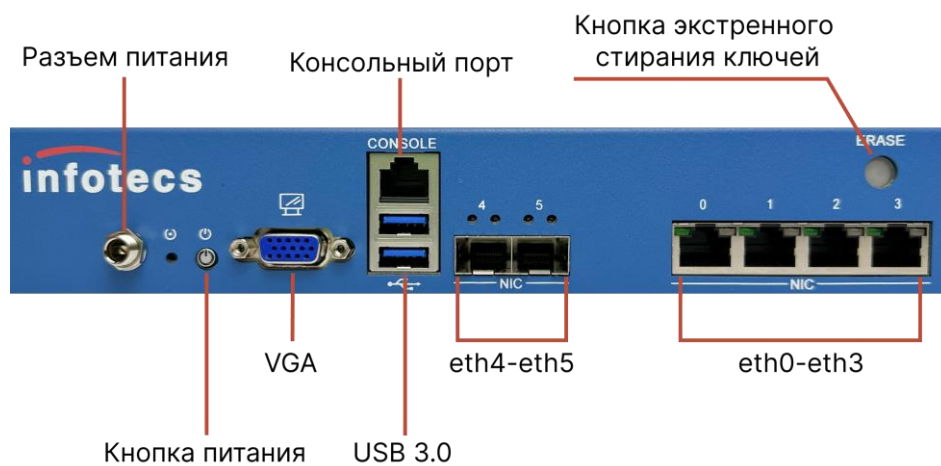


Рисунок 11. Передняя панель KB100 Q1/Q2

Исполнения ViPNet Coordinator KB1000

Исполнения ViPNet Coordinator KB1000 устанавливаются в телекоммуникационную стойку 19" и могут быть использованы для защиты компьютерных сетей масштаба предприятия.



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

Аппаратная платформа KB1000 Q6

Таблица 3. Характеристики KB1000 Q6

Характеристика	Описание
Форм-фактор	19" Rack 1U
Размеры (ШхВхГ)	429,0 x 44,0 x 381,0 мм
Масса	6 кг
Питание	Встроенный блок питания выходной мощностью 250 Вт, напряжением от 100 до 240 В, 4 А, 50-60 Гц
Датчик вскрытия корпуса	Есть
Кнопка экстренного стирания ключевой информации	Есть
Сетевые интерфейсы	4 x Ethernet RJ45 10/100/1000 Мбит/с 2 x Ethernet SFP 1 Гбит/с (eth4, eth5)
Порты ввода-вывода	2 порта VGA 1 порт PS/2 4 порта USB 2.0 2 порта USB 3.0
Дополнительное оборудование	Кабель питания с литыми разъёмами VDE 10A, разъём евровилка Schuko C13 Салазки, комплект винтов и шайб для крепления в стойку

На передней панели KB1000 Q6 расположены 2 разъёма USB 2.0, порт VGA и кнопка экстренного стирания ключей.



Рисунок 12. Передняя панель KB1000 Q6

Остальные коммуникационные разъемы находятся на задней панели.

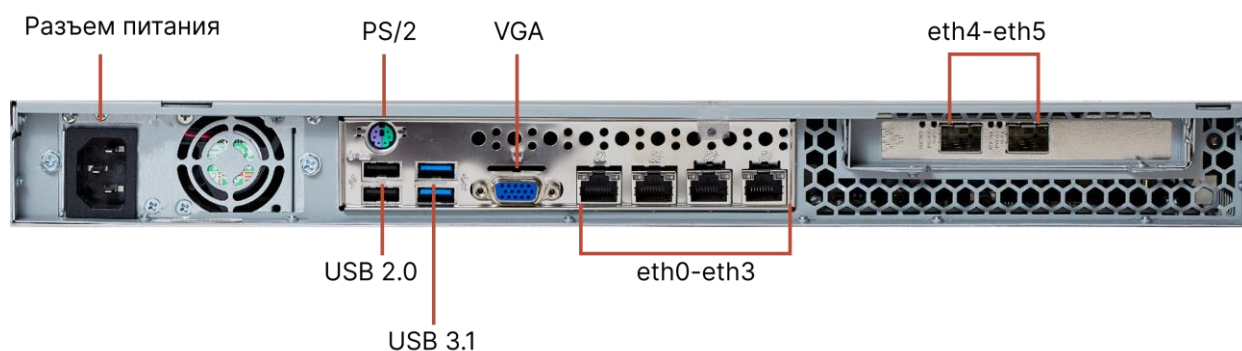


Рисунок 13. Задняя панель KB1000 Q6

Аппаратная платформа KB1000 Q8

Таблица 4. Характеристики KB1000 Q8

Характеристика	Описание
Форм-фактор	19" Rack 1U
Размеры (ШхВхГ)	430,0 x 44,0 x 476,0 мм
Масса	8 кг
Питание	Два встроенных блока питания выходной мощностью 300 Вт каждый, напряжением от 100 до 127 В, либо от 200 до 240 В, 5 А, 50-60 Гц
Датчик вскрытия корпуса	Есть
Кнопка экстренного стирания ключевой информации	Есть
Сетевые интерфейсы	4 x Ethernet RJ45 10/100/1000 Мбит/с 2 x Ethernet SFP 1 Гбит/с (eth4, eth5)
Порты ввода-вывода	1 порт VGA

Характеристика	Описание
	4 порта USB 3.1
Дополнительное оборудование	2 кабеля питания с литыми разъёмами VDE 10A, разъём евровилка Schuko C13 Самоклеющиеся наклейки «ножки» Салазки, комплект винтов и шайб для крепления в стойку

На передней панели платформы расположены: коммуникационные разъёмы и сетевые интерфейсы, порт VGA, кнопка питания и кнопка экстренного стирания ключей.

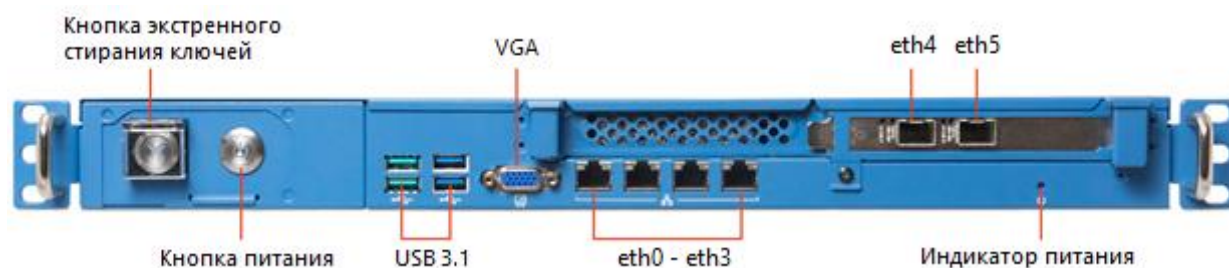


Рисунок 14. Передняя панель KB1000 Q8

На задней панели расположены разъёмы для адаптеров питания.



Рисунок 15. Задняя панель KB1000 Q8

Исполнения ViPNet Coordinator KB2000

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

Исполнение ViPNet Coordinator KB2000 распространяется на аппаратной платформе KB2000 Q4 и имеет двухпортовые сетевые адаптеры Intel Ethernet SPF+.



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

Аппаратная платформа KB2000 Q4

Таблица 5. Характеристики KB2000 Q4

Характеристика	Описание
Форм-фактор	19" Rack 1U
Размеры (ШхВхГ)	444,0 x 44,0 x 381,0 мм
Масса	8 кг
Питание	Встроенный блок питания выходной мощностью 500 Вт, напряжением от 100 до 120 В, либо от 200 до 240 В, 8 либо 4 А, 50-60 Гц
Датчик вскрытия корпуса	Есть
Кнопка экстренного стирания ключевой информации	Есть
Сетевые интерфейсы	4 x Ethernet RJ45 10/100/1000 Мбит/с 4 x Ethernet SFP+ 10 Гбит/с (eth2, eth3, eth6, eth7)
Порты ввода-вывода	1 порт VGA 1 порт PS/2 2 порта USB 3.0
Дополнительное оборудование	Кабель питания с литыми разъёмами VDE 10A, разъём евровилка Schuko C13

Характеристика	Описание
	Салазки, комплект винтов и шайб для крепления в стойку

На передней панели KB2000 Q4 находятся: сетевые интерфейсы Ethernet и Ethernet SFP+, дублирующий разъем адаптера питания, разъемы PS/2, USB 3.0 и VGA.

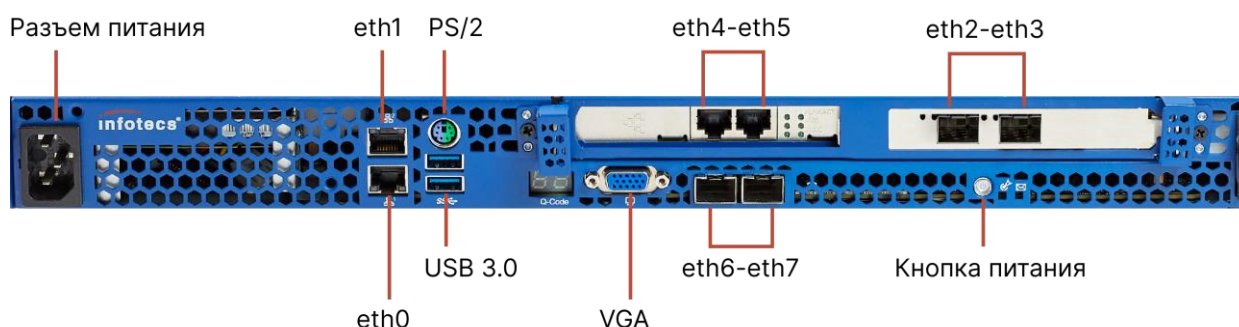


Рисунок 16. Передняя панель ViPNet Coordinator KB2000 Q4

На задней панели KB2000 Q4 расположены: разъем адаптера питания, COM-порт RS-232 и кнопка экстренного стирания ключевой информации.



Рисунок 17. Задняя панель ViPNet Coordinator KB2000 Q4

Аппаратная платформа KB2000 Q5

Таблица 6. Характеристики KB2000 Q5

Характеристика	Описание
Форм-фактор	19" Rack 1U
Размеры (Ш x В x Г)	430,0 x 44,0 x 476,0 мм
Масса	8 кг
Питание	Два встроенных блока питания выходной мощностью 300 Вт каждый, напряжением от 100 до 127 В, либо от 200 до 240 В, 5 А, 50-60 Гц
Датчик вскрытия корпуса	Есть

Характеристика	Описание
Кнопка экстренного стирания ключевой информации	Есть
Сетевые интерфейсы	4 x Ethernet RJ-45 10/100/1000 Мбит/с 4 x Ethernet SFP+ 10 Гбит/с (eth4, eth5, eth6, eth7)
Порты ввода-вывода	1 порт VGA 4 порта USB 3.1
Дополнительное оборудование	2 кабеля питания с литыми разъёмами VDE 10A, разъём евровилка Schuko C13 Самоклеющиеся наклейки «ножки» Салазки, комплект винтов и шайб для крепления в стойку

На передней панели платформы расположены: коммуникационные разъёмы и сетевые порты, порт VGA, кнопка питания и кнопка экстренного стирания ключевой информации.

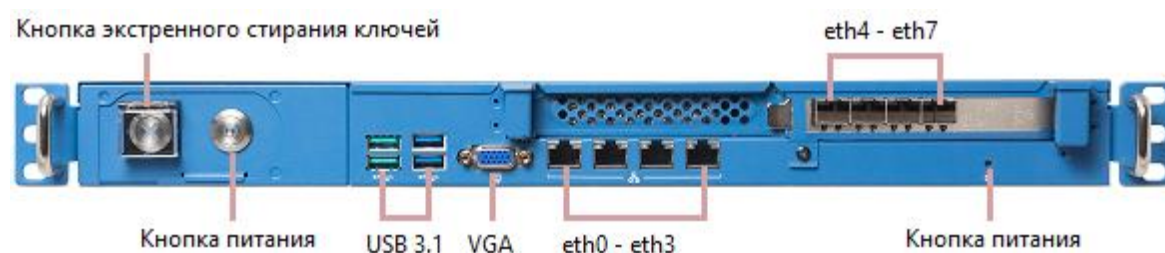


Рисунок 18: Передняя панель ViPNet Coordinator KB2000 Q5

На задней панели KB2000 Q5 расположены разъёмы адаптеров питания.



Рисунок 19: Задняя панель KB2000 Q5

Исполнения ViPNet Coordinator KB5000

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



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

Аппаратная платформа KB5000 Q1

Таблица 7. Характеристики KB5000 Q1

Характеристика	Описание
Форм-фактор	19" Rack 1U
Размеры (ШхВхГ)	444,0 x 44,0 x 381,0 мм
Масса	8 кг
Питание	Встроенный блок питания выходной мощностью 500 Вт, напряжением от 100 до 120 В, либо от 200 до 240 В, 8 либо 4 А, 50-60 Гц
Датчик вскрытия корпуса	Есть
Кнопка экстренного стирания ключевой информации	Есть
Сетевые интерфейсы	4 x Ethernet RJ45 10/100/1000 Мбит/с 4 x Ethernet SFP+ 10 Гбит/с (eth2, eth3, eth6, eth7)
Порты ввода-вывода	1 порт VGA 1 порт PS/2 2 порта USB 3.0 1 порт RS-232
Дополнительное оборудование	Кабель питания с литыми разъёмами VDE 10А, разъём евровилка Schuko C13 Салазки, комплект винтов и шайб для крепления в стойку

На передней панели KB5000 Q1 находятся: сетевые интерфейсы Ethernet и Ethernet SFP+, дублирующий разъем адаптера питания, разъемы PS/2, USB 3.0 и VGA.

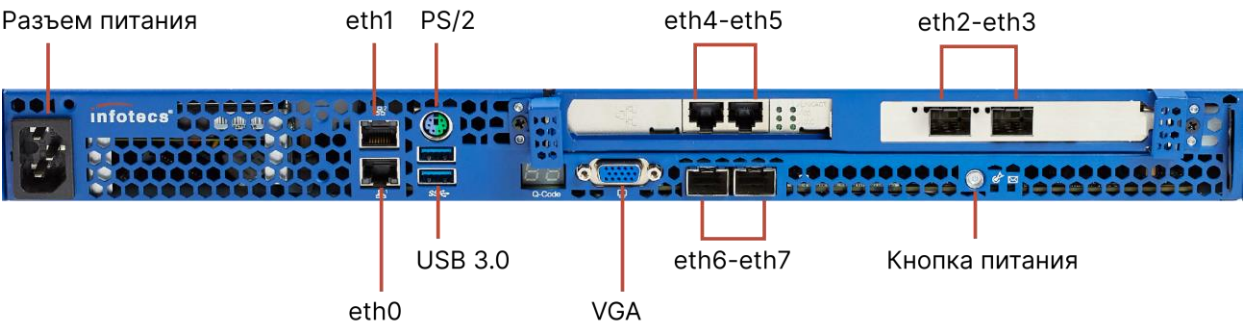


Рисунок 20. Передняя панель ViPNet Coordinator KB5000 Q1

На задней панели KB5000 Q1 расположены: разъем адаптера питания, COM-порт RS-232 и кнопка экстренного стирания ключевой информации.



Рисунок 21: Задняя панель ViPNet Coordinator KB5000 Q1

Аппаратная платформа KB5000 Q2

Таблица 8. Характеристики KB5000 Q2

Характеристика	Описание
Форм-фактор	19" Rack 1U
Размеры (Ш x В x Г)	430,0 x 44,0 x 476,0 мм
Масса	8 кг
Питание	Два встроенных блока питания выходной мощностью 300 Вт каждый, напряжением от 100 до 127, либо от 200 до 240 В, 5 А, 50-60 Гц
Датчик вскрытия корпуса	Есть
Кнопка экстренного стирания ключевой информации	Есть

Характеристика	Описание
Сетевые интерфейсы	4 x Ethernet RJ-45 10/100/1000 Мбит/с 4 x Ethernet SFP+ 10 Гбит/с (eth4, eth5, eth6, eth7)
Порты ввода-вывода	1 порт VGA 4 порта USB 3.1
Дополнительное оборудование	2 кабеля питания с литыми разъёмами VDE 10A, разъём евровилка Schuko C13 Самоклеющиеся наклейки «ножки» Салазки, комплект винтов и шайб для крепления в стойку

На передней панели платформы расположены: коммуникационные разъёмы и сетевые интерфейсы, порт VGA, кнопка питания и кнопка экстренного стирания ключевой информации.



Рисунок 22: Передняя панель ViPNet Coordinator KB5000 Q2

На задней панели KB5000 Q2 расположены разъёмы адаптеров питания.



Рисунок 23: Задняя панель KB5000 Q2

Коммутация сетевых портов SFP+

Аппаратные платформы KB2000 Q4, Q5 и KB5000 Q1, Q2 имеют 10-гигабитные сетевые адаптеры Intel Ethernet SFP+ и Broadcom Ethernet SFP+.

Для подключения всех перечисленных адаптеров к сети можно использовать как трансиверы SFP+, так и кабели, напрямую подключаемые к адаптерам. Подключаемый кабель должен удовлетворять следующим требованиям:

- Любой SFP+ пассивный медный кабель, соответствующий требованиям спецификаций SFF-8431 v4.1 и SFF-8472 v10.4.
- Идентификатор по спецификации SFF-8472 должен иметь значение 03h (SFP или SFP Plus). Вы можете проверить это значение у изготовителя кабеля.
- Максимальная длина кабеля — 7 метров.



Примечание. Нельзя использовать кабель прямого подключения для соединения с гигабитным коммутатором, к которому можно подключать SFP-модули.

Корпорация Intel производит пассивные медные кабели прямого подключения различной длины, которые полностью совместимы с 10-гигабитными сетевыми адаптерами, используемыми в исполнениях ViPNet Coordinator KB2000 и ViPNet Coordinator KB5000. В таблице ниже приведена информация, которая поможет вам приобрести нужный кабель.

Таблица 9. Коды продукции для заказа кабелей прямого подключения

Название продукции	Код продукции
Intel Ethernet SFP+ твинаксиальный кабель, 1 метр	XDACBL1M
Intel Ethernet SFP+ твинаксиальный кабель, 3 метра	XDACBL3M
Intel Ethernet SFP+ твинаксиальный кабель, 5 метров	XDACBL5M

Поддерживаемое дополнительное оборудование

При эксплуатации ViPNet Coordinator KB используется дополнительное оборудование:

- Внешние DVD/CD приводы — для считывания информации с ключевых блокнотов.
- Токены — для аутентификации с использованием типа аутентификации «Устройство».
- Трансиверы SFP и SFP+ — для подключения исполнений ViPNet Coordinator KB, имеющих соответствующие сетевые порты, к оптическим линиям связи.

Дополнительное оборудование, поддерживаемое ViPNet Coordinator KB, приведено ниже.

Таблица 10. Оптические приводы

Наименование	KB100		KB1000		KB2000		KB5000	
	N1	Q1/Q2	Q6	Q8	Q4	Q5	Q1	Q2
Liteon eBAU108-Ultra Slender	✓	✓	✓	✓	✓	✓	✓	✓
ASUS SDRW-08D2S-U LITE	✓	✓	—	✓	—	✓	—	✓
ASUS ZenDrive U7M (SDRW-08U7M-U)	✓	✓	—	✓	—	✓	—	✓
ASUS ZenDrive U9M (SDRW-08U9M-U)	✓	✓	—	✓	—	✓	—	✓
Hitachi-LG Slim Portable DVD Writer GP60NB60	✓	✓	—	✓	—	✓	—	✓

Таблица 11. Трансиверы SFP

Наименование	KB100		KB1000		KB2000		KB5000	
	N1	Q1/Q2	Q6	Q8	Q4	Q5	Q1	Q2
Avago AFBR 5710PZ	✓	✓	✓	✓	—	—	—	—
FINISAR FTLF8519P3BNL	✓	✓	—	✓	—	—	—	—
Neoros NR-SFP-1G-SX-LC2	✓	✓	—	✓	—	—	—	—
SNR SNR-SFP-SX	✓	✓	—	✓	—	—	—	—

Таблица 12. Трансиверы SFP+

Наименование	KB100		KB1000		KB2000		KB5000	
	N1	Q1/Q2	Q6	Q8	Q4	Q5	Q1	Q2
Avago AFBR 709SMZ	—	—	—	—	✓	✓	✓	✓
Avago AFBR 710SMZ	—	—	—	—	—	✓	—	✓
Intel E10GSFPSR	—	—	—	—	—	✓	—	✓

FiberTrade FT-SFP+SR-0,5-D	—	—	—	—	—	✓	—	✓
FIBO FT-S10-X312LD	—	—	—	—	—	✓	—	✓
FIBO FT-S10-M8503LD	—	—	—	—	—	✓	—	✓
FINISAR FTLX8574D3BCV	—	—	—	—	—	✓	—	✓
MikroTik S+85DLC03D	✓	✓	—	✓	—	✓	—	✓
Neoros NR-SFP-10G-SR-LC2	—	—	—	—	—	✓	—	✓

Таблица 13. Токены

Наименование	KB100		KB1000		KB2000		KB5000	
	N1	Q1/Q2	Q6	Q8	Q4	Q5	Q1	Q2
Рутокен Lite модификации: 64КБ, micro 64КБ	✓	✓	✓	✓	✓	✓	✓	✓
Рутокен Lite 1010	✓	✓	—	✓	—	✓	—	✓
Рутокен ЭЦП 2.0 модификации: 2000 64КБ, 2000 micro, 2100, 2100 micro, 3000, 3000 micro, 2200 64КБ, 3000 128КБ, 4500 128КБ Flash 32ГБ, 4500 128КБ Flash 64ГБ	✓	✓	✓	✓	✓	✓	✓	✓
Рутокен ЭЦП 3.0 модификации: 3100, 3220, 3220 micro, 3220 metal	✓	✓	—	✓	—	✓	—	✓
Jacarta ГОСТ	✓	✓	✓	✓	✓	✓	✓	✓
JaCarta-2 PRO/ГОСТ модификации: JC006-2.F27, JC206-2.F27, JC007-2.F27, JC207-2.F27, JC034-2.F27, JC234-2.F27	✓	✓	✓	✓	✓	✓	✓	✓

Меры безопасности и предосторожности

При эксплуатации ViPNet Coordinator KB соблюдайте следующие меры предосторожности и безопасности:

Меры безопасности

- 1 Перед обслуживанием извлеките ViPNet Coordinator KB из стойки, а также отключите кабели электропитания, чтобы полностью обесточить оборудование во избежание поражения электрическим током.
- 2 После отключения ViPNet Coordinator KB от электропитания дождитесь пока он остынет, перед началом технического обслуживания.
- 3 Во избежание травм не прикасайтесь к движущимся частям вентиляторов.
- 4 Во избежание повреждения ViPNet Coordinator KB электростатическим разрядом применяйте меры по предотвращению накопления статического заряда: используйте антистатический браслет, подключённый к земле, если у вас нет антистатического браслета, держите руки сухими и сначала прикоснитесь к металлическому предмету, чтобы устранить статическое электричество.
- 5 Запрещено эксплуатировать ViPNet Coordinator KB с открытой крышкой корпуса или без установленного воздуховода (при наличии). Открытие крышки приведет к срабатыванию датчика несанкционированного доступа и блокировке ViPNet Coordinator KB. При этом в консоли выводится соответствующее сообщение * TAMPERING DETECTED! Keys will be removed, system will be halted and locked! *.
- 6 Не загромождайте и не накрывайте вентиляционные отверстия на передней и задней панелях ViPNet Coordinator KB. Не размещайте ViPNet Coordinator KB рядом с радиаторами или вентиляторами отопления. Несоблюдение данных правил может привести к перегреву и снижению надёжности ViPNet Coordinator KB, а также к аннулированию гарантии.
- 7 Для обеспечения надлежащей вентиляции необходимо обеспечить зазор не менее 15 см до передней и задней стороны корпуса. Зазоры для обеспечения вентиляции не требуются со стороны боковых, верхней и нижней частей ViPNet Coordinator KB.
- 8 Для подключения ViPNet Coordinator KB к электросети используйте кабели, входящие в комплект поставки. Подключение допускается только с использованием предназначенных для этого разъёмов.
- 9 Не подключайте ViPNet Coordinator KB к розеткам питания с напряжением, не соответствующим характеристикам используемой аппаратной платформы.
- 10 Не размещайте соединительные кабели рядом с электродвигателями и другими источниками магнитных или радиочастотных помех.
- 11 ViPNet Coordinator KB должен быть заземлен. Не используйте для подключения незаземлённые электрические розетки.

- 12 При эксплуатации ViPNet Coordinator KB запрещается вносить изменения в его состав, конструкцию, электрическую и монтажную схему.
- 13 Все работы по техническому обслуживанию должны выполняться только квалифицированным персоналом.
- 14 Не допускайте контакта с поверхностью сильных растворителей (разбавителей, бензола и других веществ).

Меры предосторожности

- 1 Исполнения ViPNet Coordinator KB в форм-факторе 1U предназначены для установки в телекоммуникационные 19" стойки. Во избежание повреждения ViPNet Coordinator KB используйте для монтажа в стойку специальные направляющие, входящие в комплект поставки.
- 2 Не допускайте установки ViPNet Coordinator KB на неровную или неустойчивую поверхность.
- 3 Не кладите и не роняйте предметы на крышку ViPNet Coordinator KB, не допускайте попадания внутрь посторонних предметов.
- 4 Не допускайте воздействия на ViPNet Coordinator KB сильных магнитных полей.
- 5 Избегайте воздействия на ViPNet Coordinator KB жидкостей, дождя.
- 6 Не допускайте воздействия на ViPNet Coordinator KB температур свыше 50° С и прямого солнечного света.
- 7 При подключении электропитания к ViPNet Coordinator KB сначала подключайте кабели к оборудованию, затем к электрической сети.
- 8 После транспортировки, хранения в условиях холода или в условиях повышенной влажности необходимо выдержать оборудование в сухом помещении при нормальных климатических условиях в оригинальной упаковке для предотвращения запотевания не менее 12 часов.
- 9 Перед транспортировкой ViPNet Coordinator KB выключите его и отсоедините все внешние устройства, а также удалите носители из накопителя на оптических дисках.
- 10 При транспортировке ViPNet Coordinator KB используйте оригинальную упаковку для защиты от грязи, воды, ударов и царапин.

З

Ввод в эксплуатацию

Порядок действий	44
Установка справочников и ключей	45
Использование ключевого блокнота ДСДР	61
Просмотр информации об установленных ключах	66
Обновление справочников и ключей	67

Порядок действий

Для ввода в эксплуатацию ViPNet Coordinator KB, выполните следующие действия:

- 1 Установите справочники и ключи сетевого узла ViPNet (см. [Установка справочников и ключей](#) на стр. 45).

Установку справочников и ключей требуется выполнить в следующих случаях:

- При первоначальной инициализации справочников и ключей с помощью [дистрибутива ключей](#) сетевого узла (файла *.dst).

Для этого вам понадобятся USB-носитель с файлом *.dst для ViPNet Coordinator KB и токен с персональным ключом пользователя.

USB-носитель с файлом *.dst и пароль администратора ViPNet Coordinator KB вы можете получить у [администратора сети ViPNet](#). Вместе с этим вы получите токен, на котором будет сохранен [персональный ключ пользователя](#), и PIN-код доступа к этому токenu.



Внимание! Вы можете пройти аутентификацию на ViPNet Coordinator KB только с помощью персонального ключа пользователя на токене, поэтому [администратор сети ViPNet](#) в процессе создания файла *.dst должен настроить способ аутентификации «**Устройство (персональный ключ)**». Подробное описание приведено в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора» в разделе «Задание способа аутентификации пользователя».

Персональный ключ рекомендуется сохранить на токен, не содержащий другой информации. При необходимости отформатируйте токен. Информацию о поддерживаемых токенах см. в разделе «[Перечень поддерживаемых токенов](#)» (на стр. 39).

- При восстановлении справочников, ключей и настроек на ViPNet Coordinator KB после некорректного обновления ПО или их переноса с другого ViPNet Coordinator KB того же исполнения (например, при замене аппаратной платформы). Для выполнения данных операций требуется файл экспорта *.vbe, в который были экспортированы справочники, ключи и настройки с другого действующего ViPNet Coordinator KB. Подробнее см. в документе «Настройка с помощью командного интерпретатора». в главе Резервное копирование и восстановление настроек.
- 2 Установите ключевой блокнот ДСДР (см. [Установка ключевого блокнота ДСДР](#) на стр. 62).

Для установки ключей из [ключевого блокнота ДСДР](#) вам потребуется внешний привод для компакт-дисков.

Установка справочников и ключей

Для установки справочников и ключей в ViPNet Coordinator KB, выполните следующую последовательность действий:

Таблица 14. Последовательность установки справочников и ключей

Действие	Ссылка
☐ Иницилируйте установку справочников и ключей на ViPNet Coordinator KB	Начало установки (на стр. 45)
☐ Укажите часовой пояс, дату и время	Настройка часового пояса, даты и времени (на стр. 46)
☐ Выберите нужный дистрибутив ключей	Установка дистрибутива ключей на ViPNet Coordinator KB (на стр. 48)
☐ Настройте параметры всех сетевых интерфейсов ViPNet Coordinator KB	Настройка сетевых интерфейсов (на стр. 50)
☐ Настройте параметры DNS-сервера	Настройка DNS-сервера (на стр. 51)
☐ Настройте параметры NTP-сервера	Настройка NTP-сервера (на стр. 52)
☐ При необходимости измените имя ViPNet Coordinator KB и диапазон виртуальных адресов	Настройка имени ViPNet Coordinator KB и диапазона виртуальных адресов (на стр. 53)
☐ Выберите режим подключения ViPNet Coordinator KB к внешней сети через межсетевой экран	Настройка подключения к внешней сети через межсетевой экран (на стр. 54)
☐ Проверьте связь с одним или несколькими узлами сети ViPNet	Проверка связи с другим сетевым узлом (на стр. 57)
☐ Завершите установку справочников и ключей	Завершение установки (на стр. 59)

Начало установки

Установка справочников и ключей производится с помощью мастера установки, который запускается автоматически после первичной авторизации на ViPNet Coordinator KB. После установки справочников и ключей для работы с ViPNet Coordinator KB вместо первичной авторизации выполняется процедура аутентификации пользователя.

Мастер установки может работать в одном из двух режимов:

- 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 сочетания клавиш.

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.
- **Space** «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 Выполните первичную авторизацию на ViPNet Coordinator KB, для этого введите имя пользователя `user` и пароль `user`. После авторизации в системе автоматически будет запущен мастер установки.
- 2 Выберите режим работы мастера установки в ответ на сообщение `Please select setup wizard operating mode:`
 - 1 — консольный;
 - 2 — полноэкранный.
- 3 После выбора режима работы мастера вам будет предложено ознакомиться с лицензионным соглашением ViPNet Coordinator KB. В консольном режиме введите `y`. В полноэкранном режиме выберите **Yes**.
- 4 Введите `y` и нажмите **Enter** в ответ на предложение начать установку в консольном режиме `Would you like to start installing keys or restoring configuration? [y/n]`. В полноэкранном режиме нажмите **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 KB. 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 KB 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 KB 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**.

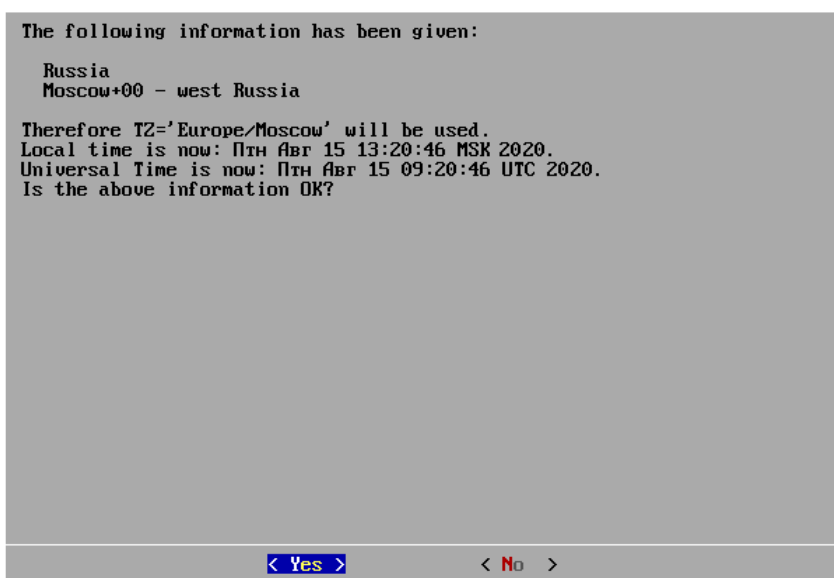


Рисунок 24. Запрос на установку часового пояса в полноэкранном режиме

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

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

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

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

Установка дистрибутива ключей на ViPNet Coordinator KB

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

- 1 В ответ на сообщение `Insert USB storage device with DST or VBE file and press <Enter>` подключите USB-носитель к одному из USB-разъемов ViPNet Coordinator KB и нажмите **Enter**.

В полноэкранном режиме в ответ на сообщение `Insert USB storage device with DST or VBE file and press [Next]` подключите USB-носитель к одному из USB-разъемов ViPNet Coordinator KB и нажмите **Next**.

- 2 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 **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 **Next**.

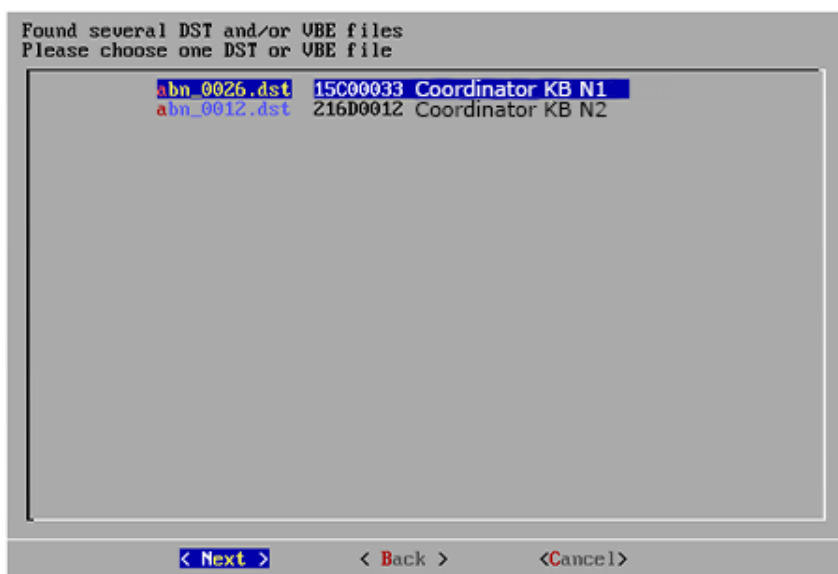


Рисунок 25. Выбор файла для установки справочников и ключей

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 вернитесь к предыдущему шагу, для этого в окне сообщения нажмите **Back**.

- В ответ на сообщение `Enter password` введите пароль к дистрибутиву ключей или пароль доступа к файлу экспорта и нажмите **Enter**. В полноэкранном режиме в ответ на сообщение **Enter password for selected DST file** введите пароль и нажмите **Next**.

Начнется установка справочников и ключей из выбранного файла.

- В ответ на сообщение `Insert token and enter PIN Code` подключите к одному из USB-разъемов ViPNet Coordinator KB токен, на котором сохранен **персональный ключ пользователя**, и введите PIN-код доступа к токenu.

После ввода PIN-кода установка справочников и ключей из выбранного файла будет продолжена.

По завершении установки справочников и ключей из дистрибутива ключей появится информация об узле, и мастер установки перейдет к следующему шагу.

В случае установки справочников и ключей из файла экспорта мастер установки перейдет к завершающему шагу (см. [Завершение установки](#) на стр. 59).

Настройка сетевых интерфейсов

При импорте справочников и ключей из файла экспорта *.vbe следующие шаги вплоть до завершения установки пропускаются, так как все настройки импортируются из файла экспорта. В результате успешного импорта и перезагрузки ViPNet Coordinator KB будут установлены те настройки, которые были на момент выполнения экспорта (см. [Завершение установки](#) на стр. 59).

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

Для настройки сетевых интерфейсов ViPNet Coordinator KB выполните следующие действия:

- 1 Включите интерфейс, если это необходимо. Для этого в консоли в ответ на сообщение `Configure interface eth<номер>? [y/n]` введите **y** и нажмите **Enter**. В полноэкранном режиме установите переключатель в положение **UP** с помощью клавиши «пробел» и нажмите **Next**.



Примечание. Должен быть настроен хотя бы один сетевой интерфейс для настройки подключения к внешней сети через межсетевой экран.

После включения интерфейса мастер установки перейдет к следующему шагу.

Если сетевой интерфейс включать не надо, введите **n** и нажмите **Enter**. В полноэкранном режиме установите переключатель в положение **DOWN** и нажмите **Next**. Мастер установки предложит настроить следующий сетевой интерфейс. В случае отказа от конфигурации последнего сетевого интерфейса, мастер установки перейдет к настройке имени ViPNet Coordinator KB и диапазонов виртуальных адресов (см. [Настройка имени ViPNet Coordinator KB и диапазона виртуальных адресов](#)).

- 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 **y** и нажмите **Enter**. В полноэкранном режиме установите переключатель в положение **DHCP** и нажмите **Next**.

Если для интерфейса нужно задать статические параметры, введите **n** и нажмите **Enter**. В полноэкранном режиме установите переключатель в положение **StaticIP** и нажмите **Next**.
- 3 Если для интерфейса не был выбран режим DHCP, введите последовательно IP-адрес и маску подсети, после чего нажмите **Enter**. В полноэкранном режиме введите параметры интерфейса в соответствующие поля, используя для перехода между полями ввода клавишу «стрелка вниз», после чего нажмите **Next**.

Если сконфигурированный на данном шаге сетевой интерфейс не последний, то мастер перейдет к конфигурированию следующего сетевого интерфейса.
- 4 Если ни для одного включенного сетевого интерфейса не был задан режим DHCP, введите IP-адрес шлюза по умолчанию и нажмите **Enter**. В полноэкранном режиме после ввода IP-адреса нажмите **Next**.

Настройка DNS-сервера

Для настройки DNS-сервера выполните следующие действия:

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

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

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

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

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

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

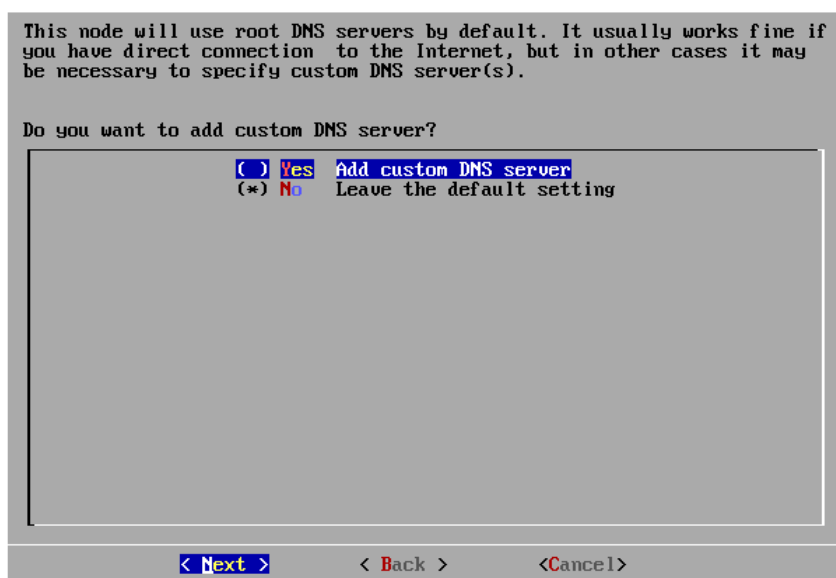


Рисунок 26. Запрос на добавление IP-адреса DNS-сервера в полноэкранном режиме

Настройка NTP-сервера



Внимание! Для корректной работы службы NTP-сервера ViPNet Coordinator KB необходимо обеспечить доступность NTP-сервера.

Для синхронизации системного времени ViPNet Coordinator KB с использованием серверов точного времени выполните следующие действия:

- 1 Включите автоматический запуск сервиса NTP при загрузке ViPNet Coordinator KB, если это необходимо. Для этого в ответ на сообщение `Do you want to use NTP daemon to synchronize the time? [y/n]` введите `y` и нажмите **Enter**. В полноэкранном режиме установите переключатель в положение **ON (Enable starting the NTP server at boot)** и нажмите **Next**.

После включения автоматического запуска сервиса NTP мастер установки перейдет к следующему шагу.

Если сервис NTP запускать не нужно, введите `n` и нажмите **Enter**. В полноэкранном режиме установите переключатель в положение **OFF (Disable starting the NTP server at boot)** и нажмите **Next**. В этом случае мастер перейдет к настройке имени ViPNet Coordinator KB (см. [Настройка имени ViPNet Coordinator KB и диапазона виртуальных адресов](#) на стр. 53).



Примечание. Максимальная разница между значением системного времени ViPNet Coordinator KB с другими узлами сети определяется параметром `timediff` в конфигурационном файле `iplir.conf` и по умолчанию составляет 6 секунд. Для синхронизации системного времени необходимо использовать сервер точного времени для всех узлов сети, иначе для обеспечения связи с другими узлами сети необходимо будет точно настраивать системное время всех узлов вручную.

- 2 Появится сообщение, что для синхронизации системного времени по умолчанию будут использоваться общедоступные 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]`.
 - Если необходимо добавить определенный NTP-сервер, введите `y` и нажмите **Enter**. В полноэкранном режиме установите переключатель в положение **Yes (Add custom NTP server)** и нажмите **Next**.

После этого введите IP-адрес или DNS-имя NTP-сервера и нажмите **Enter**. В полноэкранном режиме после ввода нажмите **Next**.
 - Если NTP-сервер добавлять не нужно, введите `n` и нажмите **Enter**. В полноэкранном режиме установите переключатель в положение **No (Leave the default setting)** и нажмите **Next**. В этом случае будут использоваться либо настройки по умолчанию, либо текущие настройки (если это не первая установка справочников и ключей).

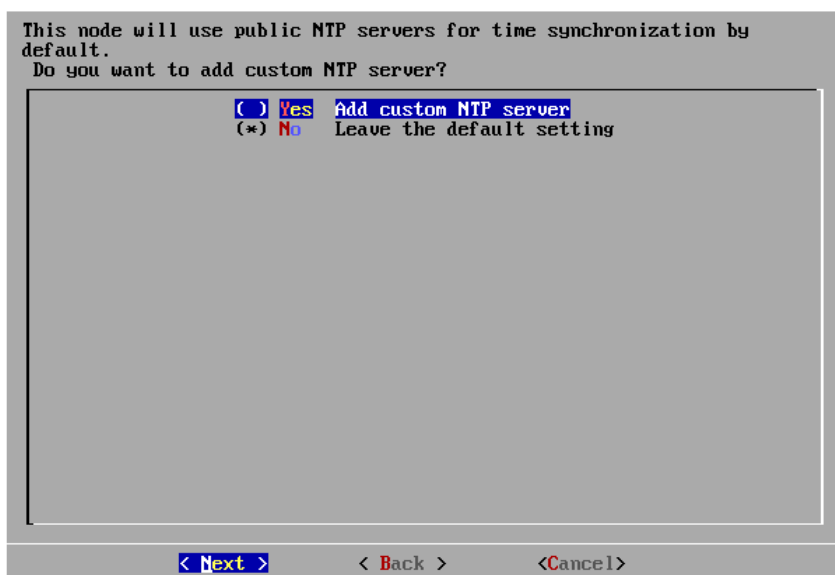


Рисунок 27. Запрос на добавление NTP-сервера в полноэкранном режиме

После отказа от добавления NTP-сервера мастер установки перейдет к настройке имени ViPNet Coordinator KB.

Настройка имени ViPNet Coordinator KB и диапазона виртуальных адресов

Для настройки имени ViPNet Coordinator KB и диапазона виртуальных адресов выполните следующие действия:

- 1 Введите имя ViPNet Coordinator KB, если вы хотите изменить имя, заданное по умолчанию, и нажмите **Enter**. В полноэкранном режиме введите нужное имя и нажмите **Next**.

По умолчанию предлагается имя, сформированное по шаблону <исполнение ViPNet Coordinator KB>-<идентификатор узла>. Например: KB1000-270E033A.

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

Виртуальные адреса из указанного диапазона будут назначаться одиночным туннелируемым адресам. Для диапазонов туннелируемых узлов IP-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 настройке виртуальных адресов для туннелируемых узлов см. в документе «Настройка с помощью командного интерпретатора» в разделе «Настройка туннелируемых адресов».

Выполните одно из действий:

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

После этого введите начальный и конечный IP-адреса нового диапазона виртуальных адресов и нажмите **Enter**. Например: `11.0.0.1-11.0.254.254`. В полноэкранном режиме после ввода нажмите **Next**.

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

- 3 Если на предыдущем этапе вы настроили хотя бы один сетевой интерфейс, мастер установки предложит проверить соединение с узлом сети ViPNet (см. [Проверка связи с другим узлом сети ViPNet](#) на стр. 57) и при необходимости настроить подключение к внешней сети через межсетевой экран.



Примечание. Должно быть дано согласие проверить соединение с одним из сетевых узлов сети ViPNet для настройки подключения к внешней сети через межсетевой экран.

Настройка подключения к внешней сети через межсетевой экран

Вы можете настроить подключение ViPNet Coordinator KB к внешней сети через межсетевой экран 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. 50).
- 2 Дано согласие проверить соединение с одним из сетевых узлов ViPNet (см. [Настройка имени ViPNet Coordinator KB и диапазона виртуальных адресов](#) на стр. 53).

Чтобы настроить подключение ViPNet Coordinator KB к внешней сети через межсетевой экран, выполните следующие действия:

- 1 После согласия выполнить проверку соединения с узлом ViPNet, появится сообщение с предложением задать режим подключения ViPNet Coordinator KB 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 KB 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 KB к сети через межсетевой экран появляется сообщение с предложением выбрать сетевой интерфейс, через который необходимо проверить соединение с другим узлом - Choose the VPN host, which you are going to use for testing the VPN connection.

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

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

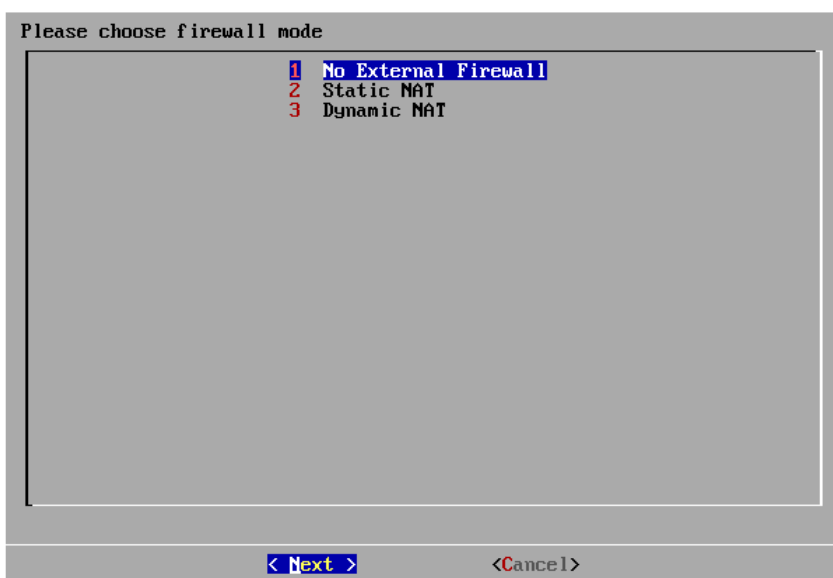


Рисунок 28. Выбор режима работы ViPNet Coordinator KB через межсетевой экран

- 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 «Со статической трансляцией адресов», введите цифру 2 и нажмите клавишу **Enter**. В полноэкранном режиме выберите режим 2 (**Static NAT**) и нажмите кнопку **Next**.
- Чтобы выбрать режим «С динамической трансляцией адресов», введите цифру 3 и нажмите клавишу **Enter**. В полноэкранном режиме выберите режим 3 (**Dynamic NAT**) и нажмите кнопку **Next**.

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

- 3** Если был выбран режим **Без использования межсетевого экрана**, то перейдите к проверке связи с другим сетевым узлом ViPNet (см. [Проверка связи с другим узлом сети ViPNet](#) на стр. 57).
- 4** Если был выбран режим **Со статической трансляцией адресов**, выполните следующие действия:

- 4.1 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 KB. По умолчанию используется порт 55777.



Примечание. Изменять номер порта нужно в том случае, если в локальной сети через один межсетевой экран (или NAT-устройство) работает несколько сетевых 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**.

- 4.2 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 IP-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 сети ViPNet (см. [Проверка связи с другим узлом сети ViPNet](#) на стр. 57).

- 4.3 Если вы задали фиксированный IP-адрес внешнего межсетевого экрана, вам будет предложено выбрать сетевой интерфейс, который будет использоваться для внешних подключений. Выберите сетевой интерфейс (аналогично п. 4.1). После этого перейдите к проверке связи с другим узлом ViPNet.
- 5 Если был выбран режим **С динамической трансляцией адресов**, выполните следующие действия:
- 5.1 Выберите координатор, через который ViPNet Coordinator KB будет подключаться к сети (аналогично п. 4.2).
- 5.2 Если в установленных справочниках не указан IP-адрес выбранного координатора, через который будет производиться подключение, задайте его (аналогично п. 4.3).
- 5.3 После этого перейдите к проверке связи с другим узлом сети ViPNet.

Проверка связи с другим узлом сети ViPNet

Вы можете проверить связь с другим узлом сети ViPNet только в том случае, если на предыдущем этапе был настроен хотя бы один сетевой интерфейс (см. [Настройка сетевых интерфейсов](#) на стр. 50).

Для проверки связи с узлом сети ViPNet выполните следующие действия:

- 1 Если в процессе установки ключей вы изменяли параметры сетевых интерфейсов, то после настройки диапазона виртуальных адресов (см. [Настройка имени ViPNet Coordinator KB и диапазона виртуальных адресов](#) на стр. 53) 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 узлами сети ViPNet выполнять не нужно, введите `n` и нажмите **Enter**. В полноэкранном режиме нажмите **No**. В этом случае установка справочников и ключей будет завершена.
 - Если необходимо выполнить проверку связи с другим узлом сети ViPNet, введите `y` и нажмите **Enter**. В полноэкранном режиме нажмите **Yes**.



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

В этом случае мастер предложит настроить подключение ViPNet Coordinator KB к внешней сети. В противном случае настройки подключения к сети будут скопированы из дистрибутива ключей без изменения.

- 2 Появится список узлов сети ViPNet, с которыми ViPNet Coordinator KB имеет связь. Информация о связях содержится в справочниках, установленных на ViPNet Coordinator KB.

Выберите узел сети ViPNet, 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 узлу в списке, и нажмите **Enter**.

В полноэкранном режиме выберите нужный узел и нажмите **Next**.



Примечание. На данном этапе ввода в эксплуатацию связь с другим ViPNet Coordinator KB не может быть установлена, поэтому для проверки связи с другими узлами сети ViPNet необходимо выбрать такой узел, с которым у вводимого в эксплуатацию ViPNet Coordinator KB установлено прямое подключение по сети и который не является аналогичным ViPNet Coordinator KB.

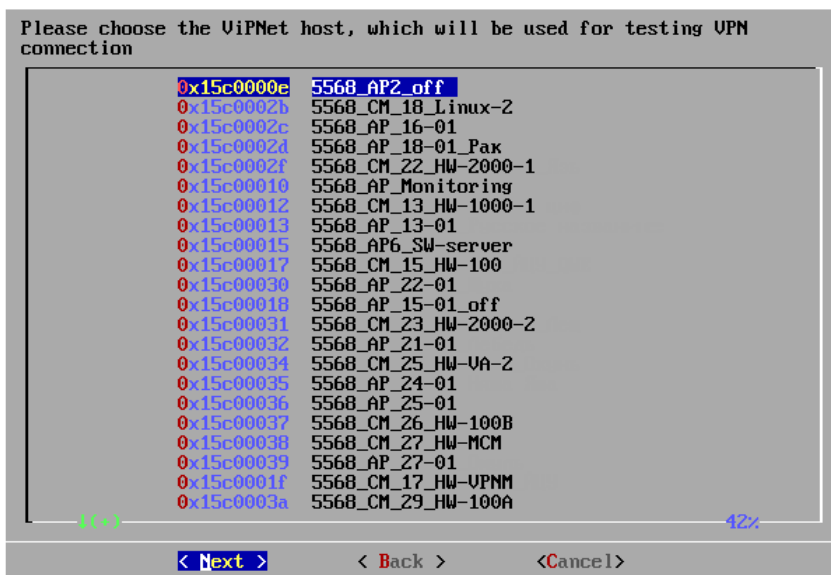


Рисунок 29. Выбор узла сети ViPNet для проверки связи в полноэкранном режиме

- 3 Если в справочниках не указан IP-адрес для выбранного сетевого узла ViPNet, мастер установки предложит задать его вручную: The IP address of the ViPNet host has not been found. Do you want to specify one? [y/n].

Чтобы задать IP-адрес для узла сети ViPNet, введите **y** и нажмите **Enter**. Затем введите IP-адрес и нажмите **Enter**.

В полноэкранном режиме нажмите **Yes**. Затем введите IP-адрес и нажмите **Next**.

Начнется проверка связи с выбранным узлом ViPNet.



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

- 4 По окончании появляется сообщение о результатах проверки связи с выбранным узлом.
 - Если связь с узлом сети ViPNet была установлена, все выполненные настройки сохраняются в конфигурационный файл `iplir.conf`.
нажмите **Enter**. В полноэкранном режиме нажмите **OK**.
Перейдите к следующему шагу (см. [Завершение установки](#) на стр. 59).
 - Если установить связь с узлом сети ViPNet не удалось, появится 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 **y**. На экране появится окно журнала регистрации IP-пакетов.
 - Для отказа от просмотра журнала введите **n**.

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

Завершение установки

Для завершения установки справочников и ключей выполните следующие действия:

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

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

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



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

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

Если драйверы и службы запускать не нужно, введите `n` и нажмите **Enter**. В полноэкранном режиме нажмите **No**. В этом случае после установки ключей необходимо вручную запустить службы и драйверы:

```
hostname# iplir start
hostname# failover start
hostname# mftp start
```

- 3 Появится сообщение об успешном завершении установки, и мастер запустит командный интерпретатор.
- 4 Чтобы продолжить настройку ViPNet Coordinator KB в командном интерпретаторе, выполните аутентификацию. Для этого подключите токен и введите PIN-код.
- 5 Если при установке ключей были настроены DNS- и NTP-серверы, запустите их:

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

Теперь вы можете выполнить необходимую настройку ViPNet Coordinator KB с помощью командного интерпретатора или веб-интерфейса в соответствии с требуемыми сценариями использования. Подробнее см. документы «Настройка с помощью командного интерпретатора» и «Настройка с помощью веб-интерфейса».

Если при настройке сетевых интерфейсов хотя бы для одного из них был задан режим DHCP, проверьте, что от DHCP-сервера получен маршрут по умолчанию. Для этого выполните одно из действий:

- В командном интерпретаторе выполните команду:

```
hostname> inet show routing
```

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

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

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



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

Использование ключевого блокнота ДСДР

Назначение ключевых блокнотов ДСДР

Каждому узлу ViPNet Coordinator KB в сети ViPNet назначается **ключевой блокнот ДСДР**. Он содержит информацию, необходимую для выработки ключей шифрования при сетевом обмене между узлами ViPNet Coordinator KB.

Ключевые блокноты устанавливаются на ViPNet Coordinator KB до начала его эксплуатации (после установки справочников и ключей), а также в случае плановой смены или компрометации ключей. ViPNet Coordinator KB проверяет серию и номер ключевого блокнота чтобы исключить его повторное использование. Подробнее см. в документе «Правила пользования», разделы «Плановая смена и обновление ключевой информации», «Компрометация ключевой информации, смена ключей при компрометации».



Примечание. При работе ViPNet Coordinator KB в кластере горячего резервирования, на оба узла кластера должны быть установлены одинаковые ключевые блокноты ДСДР.

Процедура получения ключевых блокнотов описана в документе «ViPNet Coordinator KB. Правила пользования». Носителем является оптический диск, на который записывают ключевой блокнот ДСДР для конкретного узла ViPNet Coordinator KB. Серия и номер ключевого блокнота наносятся на поверхность диска и используются при регистрации ключевого блокнота ДСДР администратором в ПО ViPNet Удостоверяющий и ключевой центр.

На лицевой стороне оптического диска ДСДР нанесена следующая информация:

- гриф;
- тип ключевого блокнота ДСДР;
- восьмизначный порядковый номер серии;
- четырехзначный номер ключевого блокнота ДСДР;
- номер комплекта ключей;
- тип упаковки.

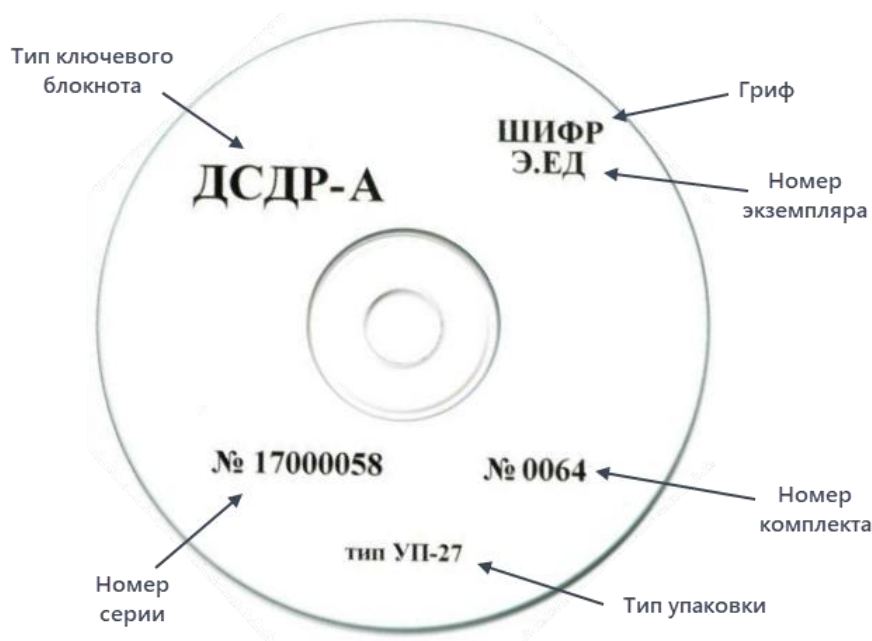


Рисунок 30. Компакт-диск ключевого блокнота ДСДР

Установка ключевого блокнота ДСДР

Чтобы установить ключевой блокнот ДСДР:

- 1 Войдите в режим администратора.
- 2 Подключите к ViPNet Coordinator KB внешний привод для компакт-дисков.
- 3 Установите диск ДСДР в привод для компакт-дисков.
- 4 Выполните команду `hostname# admin update-dsdr`.
- 5 В ответ на сообщение `DSDR will be updated. IPLIR and MFTP will be stopped` введите **Yes** и нажмите **Enter**.

Если серия и номер ключевого блокнота ДСДР на диске совпадают с ключевой информацией ViPNet Coordinator KB, то с диска ДСДР будет считана необходимая информация.



Примечание. Чтобы обеспечить автоматическую смену серии блокнота ДСДР, последовательно установите все серии, предназначенные для текущего ViPNet Coordinator KB (см. «[Настройка автоматической смены ключевого блокнота](#)»).

Смена ключевого блокнота ДСДР

Срок действия ключевых блокнотов ДСДР — 15 месяцев с момента ввода в действие. По истечении срока действия связь между узлами ViPNet Coordinator KB будет прервана, поэтому ключевые

блокноты необходимо своевременно заменять. Вы можете сменить ключевой блокнот вручную или настроить его автоматическую смену.

Подготовка к смене ключевых блокнотов

Смена серии ДСДР — ответственный этап, поскольку неправильные действия могут привести к потере связи между узлами и нарушению работы сети ViPNet. Перед сменой ДСДР выполните резервное копирование текущей конфигурации ViPNet Administrator и ViPNet Coordinator KB чтобы иметь возможность восстановить конфигурацию в случае неудачи.

- Для ViPNet Coordinator KB — резервная копия конфигурации создается в командном интерпретаторе при подключении к локальной консоли. Подробнее см. в документе «Настройка с помощью командного интерпретатора» в разделе «Резервное копирование и восстановление настроек» .
- Для ViPNet Administrator — резервная копия конфигурации создается штатными средствами ViPNet Administrator. Подробнее см. в документе «ViPNet Удостоверяющий и ключевой центр 4. Руководство администратора» в разделе «Создание резервной копии текущей конфигурации» .

Рекомендуем дополнительно создать резервную копию альтернативными средствами.

Смена ключевого блокнота

- 1 Администратор сети ViPNet регистрирует в ПО ViPNet Administrator ключевой блокнот из новой серии. Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр 4. Руководство администратора» раздел «Учет ключей ДСДР».
- 2 Администратор сети ViPNet выпускает обновление справочников и ключей, которое отправляется на ViPNet Coordinator KB из ПО ViPNet Administrator или устанавливается вручную из дистрибутива ключей. Подробнее см. документ «ViPNet Центр управления сетью 4. Руководство администратора», раздел «Обновление справочников и ключей»:
 - Если обновление справочников и ключей отправлено администратором сети ViPNet из ПО ViPNet Administrator, убедитесь в их успешной доставке и применении. Для этого выполните на ViPNet Coordinator KB:

```
Hostname# admin show dsdrnet
```

Если вывод команды содержит номер новой серии ДСДР, значит обновление выполнено успешно.
 - Если вы обновляете справочники и ключи вручную, то получите USB-накопитель с дистрибутивом ключей у администратора сети ViPNet. Затем подключите USB-накопитель к ViPNet Coordinator KB и выполните обновление (см. «[Обновление справочников и ключей](#)»).
- 3 После обновления справочников и ключей установите ключевой блокнот из зарегистрированной серии (см. «[Установка ключевого блокнота ДСДР](#)»).

Настройка автоматической смены ключевого блокнота

Вы можете установить на ViPNet Coordinator KB два ключевых блокнота — текущий, который используется для выработки симметричных ключей и следующий, который задействуется после окончания срока действия текущего. Чтобы настроить автоматическую смену ключевого блокнота:

- 1 Администратор сети ViPNet регистрирует в ПО ViPNet Administrator серии обоих ключевых блокнотов — текущего и следующего, и задает даты их ввода в действие. Чтобы смена серии происходила автоматически, в ПО ViPNet Administrator должны быть включены следующие настройки:
 - контроль срока действия ключей;
 - использование новой серии ключей с указанной даты.

Подробнее см. в документе «ViPNet Удостоверяющий и ключевой центр 4. Руководство администратора» в разделе «Учет ключей ДСДР».

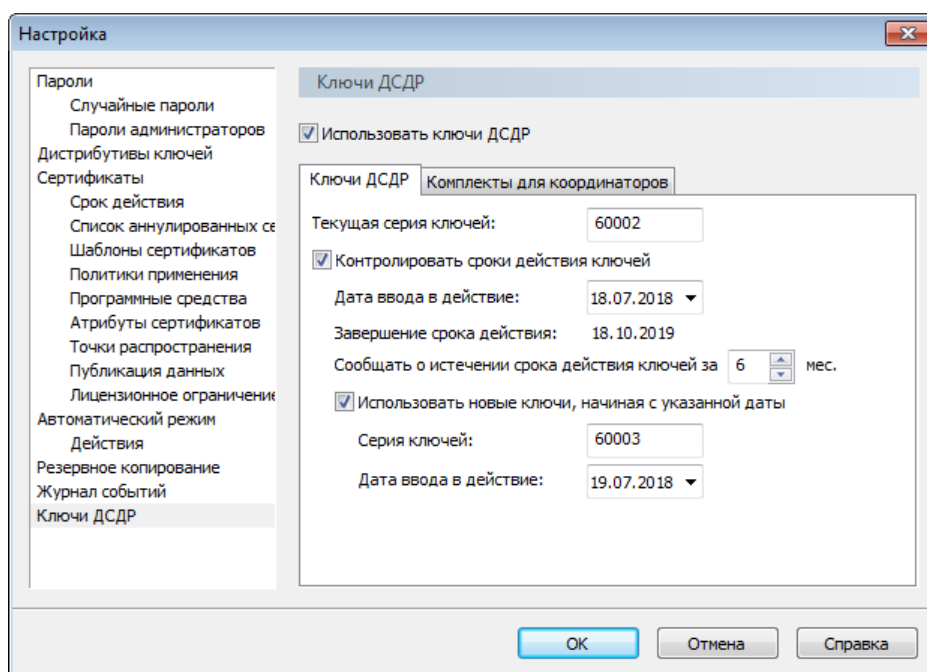


Рисунок 31: Настройка контроля срока действия ключей ДСДР в ПО ViPNet Administrator



Примечание. Если вы регистрируете следующий ключевой блокнот в дополнение к уже установленному, то номера комплектов ключей переназначать не требуется.

- 2 Администратор сети ViPNet выпускает обновление справочников и ключей, которое отправляется на ViPNet Coordinator KB из ПО ViPNet Administrator или устанавливается вручную из дистрибутива ключей. Подробнее см. документ «ViPNet Центр управления сетью 4. Руководство администратора», раздел «Обновление справочников и ключей»:
 - Если обновление справочников и ключей отправлено администратором сети ViPNet из ПО ViPNet Administrator, убедитесь в их успешной доставке и применении. Для этого выполните на ViPNet Coordinator KB:

```
Hostname# admin show dsdrnet
```

Если вывод команды содержит номер новой серии ДСДР, значит обновление выполнено успешно.

- Если вы обновляете справочники и ключи вручную, то получите USB-накопитель с дистрибутивом ключей у администратора сети ViPNet. Затем подключите USB-накопитель к ViPNet Coordinator KB и выполните обновление (см. «[Обновление справочников и ключей](#)»).

- 3 После обновления справочников и ключей установите оба ключевых блокнота из зарегистрированных серий (см. «[Установка ключевого блокнота ДСДР](#)»). Если текущий ключевой блокнот был установлен ранее, то установите только следующий.

Следующий ключевой блокнот необходимо установить на ViPNet Coordinator KB до наступления даты ввода в действие новой серии.

При наступлении даты ввода в действие новых ключей смена ДСДР будет произведена автоматически в 00:00 UTC.



Внимание! При настройке автоматической смены серии ДСДР убедитесь, что все ViPNet Coordinator KB в вашей сети ViPNet имеют версию ПО не ниже 4.3.0 и при необходимости обновите их. Иначе после смены серии ДСДР связь между ними прервется.

Вы можете контролировать статус и время действия установленного ключевого блокнота удаленно по протоколу SNMP. Для этого используется специальная база управляющей информации (MIB), включающая текущий статус ДСДР. Подробнее о настройке мониторинга с помощью SNMP см. в документе «Настройка с помощью командного интерпретатора» в разделе «Мониторинг по протоколу SNMP».

Просмотр информации об установленных ключах

При необходимости вы можете просмотреть информацию о следующих ключах, установленных на ViPNet Coordinator KB:

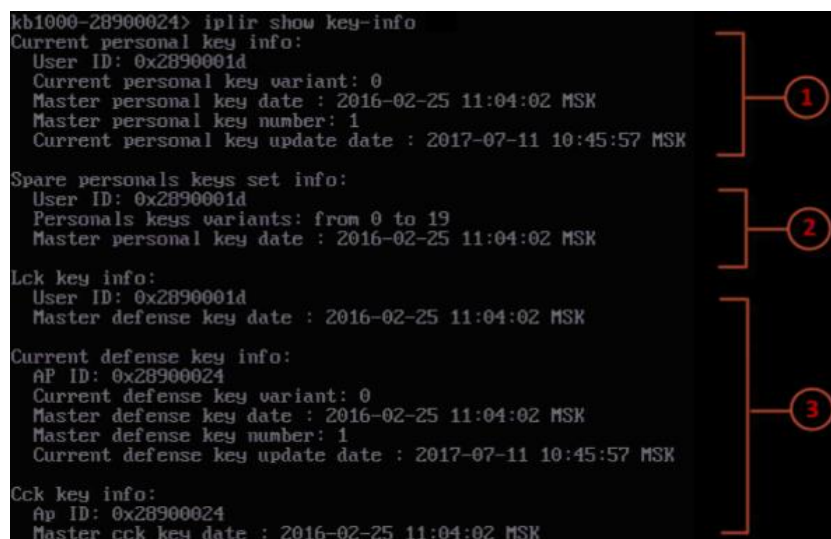
- персональный ключ пользователя;
- резервный набор персональных ключей (РНПК);
- ключи узла ViPNet.

Информация об установленных ключах может быть востребована сотрудниками технического сопровождения при возникновении проблем с ключевой системой ViPNet Coordinator KB (например, после некорректного обновления справочников и ключей или в других случаях).

Для просмотра информации о ключах выполните:

```
hostname> iplir show key-info
```

В результате отобразятся списки с информацией по типам ключей. Пример выводимой информации о ключах представлен на рисунке ниже.



```
kb1000-28900024> iplir show key-info
Current personal key info:
  User ID: 0x2890001d
  Current personal key variant: 0
  Master personal key date : 2016-02-25 11:04:02 MSK
  Master personal key number: 1
  Current personal key update date : 2017-07-11 10:45:57 MSK

Spare personals keys set info:
  User ID: 0x2890001d
  Personals keys variants: from 0 to 19
  Master personal key date : 2016-02-25 11:04:02 MSK

Lck key info:
  User ID: 0x2890001d
  Master defense key date : 2016-02-25 11:04:02 MSK

Current defense key info:
  AP ID: 0x28900024
  Current defense key variant: 0
  Master defense key date : 2016-02-25 11:04:02 MSK
  Master defense key number: 1
  Current defense key update date : 2017-07-11 10:45:57 MSK

Cck key info:
  Ap ID: 0x28900024
  Master cck key date : 2016-02-25 11:04:02 MSK
```

Рисунок 32: Просмотр информации о ключах

Цифрами на рисунке обозначены:

- 1 Информация о текущем персональном ключе пользователя.
- 2 Информация о РНПК.
- 3 Информация о ключах узла ViPNet Coordinator KB.

Обновление справочников и ключей

Обновление справочников и ключей выполняется в следующих случаях:

- изменение топологии сети ViPNet;
- выпуск нового токена для аутентификации пользователя;
- смена ключевого блокнота ДСДР;
- добавление или изменение связей между узлами сети ViPNet;
- смена мастер-ключей в сети.

Обновление справочников и ключей на ViPNet Coordinator KB выполняется в автоматическом режиме, либо вручную.



Внимание! В случае компрометации ключей обновлять справочники и ключи запрещено. В этом случае удалите ключи командой `admin keys remove` и заново выполните [первичную инициализацию](#).

Автоматическое обновление не требует каких-либо действий на ViPNet Coordinator KB, для этого администратор сети ViPNet отправляет обновление справочников и ключей из ПО [ViPNet Центр управления сетью](#). Такое обновление возможно только в случае, когда не требуется обновлений персонального ключа пользователя.

В случае если меняется персональный ключ пользователя, например, если произошла смена мастер-ключей в сети, то обновление справочников и ключей необходимо провести в ручном режиме.

Для обновления справочников и ключей вручную вам понадобится USB-носитель с актуальными файлами *.dst и abn_XXXX.XPS для ViPNet Coordinator KB, который вы можете получить у [администратора сети ViPNet](#).

Чтобы обновить справочники и ключи вручную:

- 1 На ViPNet Coordinator KB запустите локальное обновление справочников и ключей:

```
hostname# admin keys update
```

В ответ на запрос `Insert USB drive with application initialization file...` подключите полученный USB-накопитель и нажмите **Enter**. Будет выведен список файлов с дистрибутивами ключей.

- 2 Введите номер файла с обновленным дистрибутивом ключей, затем пароль к нему.
- 3 После запроса `Extract the current token and insert token with new personal key` отключите текущий токен и подключите новый.
- 4 Введите PIN-код от нового токена и дождитесь завершения обновления справочников и ключей.

4

Возможности управления

Способы управления ViPNet Coordinator KB	69
Управление с помощью административного ПО ViPNet	70
Управление с помощью командного интерпретатора	71
Управление с помощью веб-интерфейса	73
Режимы работы	74
Экстренное стирание ключевой информации	75

Способы управления ViPNet Coordinator KB

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

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

Выполнение настройки ViPNet Coordinator KB в ЦУСе облегчает управление и позволяет оповестить об изменении параметров сетевые узлы ViPNet, связанные с ViPNet Coordinator KB, путем отправки на эти узлы справочников и ключей. Программа ViPNet Policy Manager позволяет централизованно управлять встроенными сетевыми экранами узлов, в том числе координаторов ViPNet Coordinator KB (см. [Управление с помощью административного ПО ViPNet](#) на стр. 70).

- Веб-интерфейс ViPNet Coordinator KB.

Наглядный и интуитивно понятный веб-интерфейс позволяет упростить и сделать более удобными просмотр и выполнение некоторых настроек ViPNet Coordinator KB (см. [Управление с помощью веб-интерфейса](#) на стр. 73).

- Командный интерпретатор ViPNet Coordinator KB.

Вы можете использовать командную оболочку ViPNet при подключении с помощью локальной консоли или через SSH-клиент. Командный интерпретатор предоставляет наиболее полные возможности по администрированию ViPNet Coordinator KB.

Управление с помощью административного ПО ViPNet

Для удаленной настройки ViPNet Coordinator KB вы можете использовать административное ПО ViPNet:

- Формирование структуры сети ViPNet, задание основных параметров сетевых узлов, централизованная отправка справочников и ключей на сетевые узлы ViPNet выполняется с помощью ViPNet Administrator. Администратор сети ViPNet также может настроить адреса доступа к ViPNet Coordinator KB, параметры подключения узла ViPNet Coordinator KB к внешней сети через межсетевой экран, адреса туннелируемых узлов. Настройки, выполненные в ViPNet Administrator, применяются на узле ViPNet Coordinator KB после установки файла *.dst, либо после обновления справочников и ключей на этом узле по сети ViPNet.
- Для формирования политик безопасности и их рассылки на узлы по сети ViPNet используется ViPNet Policy Manager. Политики безопасности могут включать в себя сетевые фильтры и правила трансляции IP-адресов. Фильтры и правила трансляции, полученные из программы ViPNet Policy Manager, недоступны для редактирования на узлах. Подробнее о политиках безопасности см. в документе «ViPNet Policy Manager. Руководство администратора».
- Для удаленного мониторинга состояния ViPNet Coordinator KB вы можете использовать ПО [ViPNet StateWatcher](#). Подробнее см. в документе «ViPNet StateWatcher. Руководство администратора».

Управление с помощью командного интерпретатора

В командном интерпретаторе доступны все настройки ViPNet Coordinator KB:

- Настройка системных функций ViPNet Coordinator KB: настройка даты и времени, создание копий конфигурации и другое.
- Настройка подключения ViPNet Coordinator KB к сети, настройка сетевых интерфейсов, параметров подключения к сетям.
- Настройка режимов подключения ViPNet Coordinator KB к сети через межсетевой экран.
- Управление межсетевым экраном путем настройки сетевых фильтров и правил трансляции адресов.
- Управление обработкой прикладных протоколов.
- Настройка VPN: настройка видимости узлов, туннелирования адресов, работа со списком сетевых узлов ViPNet и другие.
- Объединение удаленных сегментов сети по технологии L2OverIP.
- Настройка транспортного модуля: выбор канала передачи конвертов между узлами, настройка протоколирования событий транспортного модуля и другое.
- Настройка сетевых служб: встроенного DHCP-, DNS-, NTP- и прокси-сервера, DHCP-relay.
- Настройка статической и динамической маршрутизации.
- Настройка системы защиты от сбоев.
- Настройка функции MultiWAN.
- Резервирование и восстановление настроек ViPNet Coordinator KB, обновление ViPNet Coordinator KB.
- Настройка параметров протоколирования событий, просмотр системного журнала, журналов регистрации IP-пакетов, транспортных конвертов и журнала СКЗИ.
- Настройка взаимодействия ViPNet Coordinator KB с источником бесперебойного питания.
- Настройка параметров удаленного мониторинга по протоколу SNMP и другое.

Командный интерпретатор запускается автоматически после аутентификации пользователя ViPNet Coordinator KB. При этом он может быть запущен как локально с помощью обычной консоли, так и удаленно при подключении с других узлов сети ViPNet, связанных с ViPNet Coordinator KB, по протоколу SSH.

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

Работа с учетной записью пользователя ViPNet Coordinator KB

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

```
hostname# admin remove keys
```



Примечание. Вы можете выполнить эту команду только при подключении к ViPNet Coordinator KB через локальную консоль. Выполнение команды в удаленной SSH-сессии невозможно.

Чтобы сменить пароль пользователя ViPNet Coordinator KB, выполните команду:

```
hostname# admin passwd
```



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

Управление с помощью веб-интерфейса

Вы можете подключиться к веб-интерфейсу ViPNet Coordinator KB с удаленного компьютера и работать в браузере. В веб-интерфейсе вы можете настроить:

- Дату и время.
- Подключение ViPNet Coordinator KB к сети, сетевые интерфейсы.
- Сетевые фильтры и правила трансляции адресов.
- Туннелирование адресов.
- Сетевые службы: встроенный DHCP-, DNS-, NTP- и прокси-сервер, DHCP-relay.
- L2OverIP, MultiWAN.
- Статическую и динамическую маршрутизацию.
- Удаленный мониторинг по протоколу SNMP.
- Мониторинг состояния ViPNet Coordinator KB.
- Посмотреть системный журнал, журнал регистрации IP-пакетов, транспортных конвертов, переключений режимов кластера (в режиме кластера).
- Посмотреть список сетевых узлов ViPNet.

В веб-интерфейсе доступны не все настройки ViPNet Coordinator KB, полный набор настроек есть только в командном интерпретаторе.

Чтобы подключение к ViPNet Coordinator KB через веб-интерфейс было безопасным, подключайтесь с защищенного узла ViPNet. Между этим узлом и ViPNet Coordinator KB должна быть создана связь в ViPNet Administrator.

К ViPNet Coordinator KB могут подключиться одновременно до 5 (исполнение KB100) или до 30 (остальные исполнения) пользователей, но только один из них может работать в режиме администратора.

Режимы работы

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

- Режим пользователя — активируется по умолчанию после аутентификации на ViPNet Coordinator KB. В нем доступен только просмотр настроек ViPNet Coordinator KB. В командном интерпретаторе в строке приглашения отображается символ «>».
- Режим администратора — доступен после авторизации с паролем администратора сетевого узла. В нем можно настраивать ViPNet Coordinator KB. В командном интерпретаторе в строке приглашения отображается символ «#».

На ViPNet Coordinator KB могут авторизоваться три типа администраторов:

- администратор узла ViPNet Coordinator KB;
- администратор группы сетевых узлов ViPNet;
- администратор сети ViPNet.

Экстренное стирание ключевой информации

В некоторых ситуациях возникает необходимость экстренного стирания ключевой информации. Такими ситуациями могут быть:

- Компрометация ключей.
- Действия при подозрении на компрометацию ключей в целях ее предотвращения.
- Подготовка ViPNet Coordinator KB к транспортировке при отключенном питании или неисправности.
- Необходимость блокировки ViPNet Coordinator KB при нештатной ситуации.
- Вывод из эксплуатации при неисправности ViPNet Coordinator KB.

Для выполнения данной операции исполнения ViPNet Coordinator KB оборудованы кнопкой экстренного стирания ключей. После нажатия данной кнопки будут удалены все ключи и справочники, установленные в ViPNet Coordinator KB, независимо от состояния устройства и наличия электропитания, а его функции будут заблокированы.



Примечание. При срабатывании датчика несанкционированного доступа (например, при вскрытии корпуса ViPNet Coordinator KB) также происходит экстренное стирание ключевой информации.

Для дальнейшей работы потребуется повторно ввести ViPNet Coordinator KB в эксплуатацию. Подробнее см. в разделе «Ввод в эксплуатацию» (на стр. 43).

Особенности экстренного стирания ключевой информации

- Не нажимайте кнопку экстренного стирания ключей во время следующих операций:
 - установка ключевого блокнота ДСДР;
 - установка справочников и ключей;
 - процедура регламентного контроля;
 - обновление ПО ViPNet Coordinator KB;
 - программное удаление ключей.

Нажатие кнопки прервет нормальное выполнение этих операций и может вызвать неработоспособность ViPNet Coordinator KB.

- На некоторых модификациях исполнения ViPNet Coordinator KB100 кнопка экстренного стирания ключей фиксируется после нажатия. Перед последующим вводом ViPNet Coordinator KB100 в эксплуатацию снимите кнопку с фиксации (нажмите ее еще раз).

5

Лицензирование и функциональные ограничения

Лицензирование ViPNet Coordinator KB	77
Ограничения на количество связей с ViPNet-узлами	78
Ограничения при использовании ViPNet Coordinator KB в защищенной сети ViPNet	79

Лицензирование ViPNet Coordinator KB

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

Таблица 15. Исполнения ViPNet Coordinator KB и их аппаратные платформы

Исполнения ViPNet Coordinator KB	Аппаратные платформы	Название роли
ViPNet Coordinator KB100	KB100 N1, Q1, Q2	Coordinator KB100
ViPNet Coordinator KB1000	KB1000 Q6, Q8	Coordinator KB1000
ViPNet Coordinator KB2000	KB2000 Q4, Q5	Coordinator KB2000
ViPNet Coordinator KB5000	KB5000 Q1, Q2	Coordinator KB5000

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

Таблица 16. Лицензионные ограничения, накладываемые ролями

Название роли	Использование в кластере горячего резервирования
Coordinator KB100	Да (с установленной дополнительной ролью Failover KB100)
Coordinator KB1000	Да
Coordinator KB2000	Да
Coordinator KB5000	Да



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

Ограничения на количество связей с ViPNet-узлами

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

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

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

Таблица 17. Максимальное количество ViPNet-клиентов, связанных с ViPNet Coordinator KB

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

Ограничения при использовании ViPNet Coordinator KB в защищенной сети ViPNet

Использование ViPNet Coordinator KB имеет ряд ограничений, связанных с особенностями технологии ViPNet либо с реализацией отдельных схем включения. Внимательно ознакомьтесь с данными ограничениями при проектировании вашей сети ViPNet.

Каскадная схема включения

ViPNet Coordinator KB не поддерживает работу при включении каскадом трех и более ViPNet Coordinator KB. Пример такой схемы включения приведен на рисунке ниже.

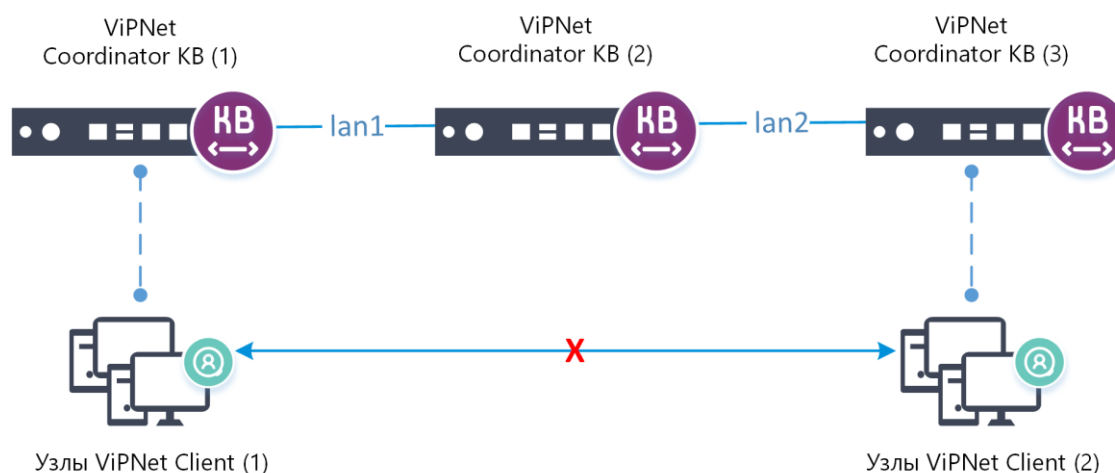


Рисунок 33: Включение ViPNet Coordinator KB каскадом

В приведенном примере координаторы ViPNet Coordinator KB (1) и ViPNet Coordinator KB (3) расположены в сетях lan1 и lan2, для которых шлюзом является координатор ViPNet Coordinator KB (2). При таком включении, даже если в административном ПО заданы связи между всеми координаторами, IP-пакеты между координаторами ViPNet Coordinator KB (1) и ViPNet Coordinator KB (3) будут блокироваться.

Также будут блокироваться IP-пакеты между сетевыми узлами, подключенными к данным координаторам.

Подключение через промежуточный ViPNet Coordinator KB

При проектировании защищенной сети ViPNet может возникнуть ситуация, когда координаторы разных сегментов защищенной сети связаны друг с другом не напрямую, а через промежуточный координатор. Пример такой схемы включения приведен на рисунке ниже, в качестве промежуточного координатора используется Coordinator ViPNet KB (1).

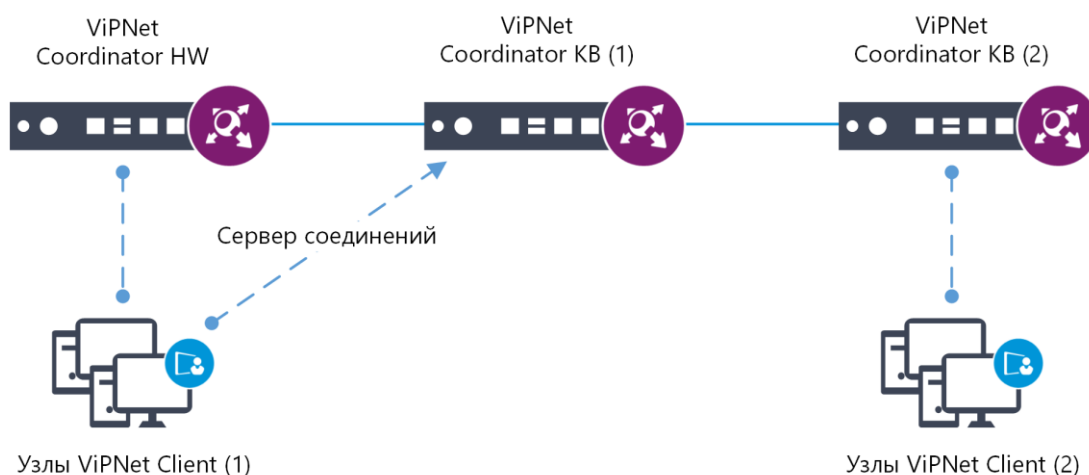


Рисунок 34: Подключение через промежуточный ViPNet Coordinator KB

В приведенном примере защищенный обмен информацией между узлами ViPNet Client (1) и ViPNet Client (2) возможен только, если:

- 5 Для узла ViPNet Client (1) в качестве сервера соединений выбран промежуточный координатор ViPNet Coordinator KB (1).
- 6 Пограничный координатор для ViPNet Client (1) не является координатором класса KB.

Иначе IP-пакеты между сетевыми узлами будут блокироваться.

Прочие ограничения при использовании в сети ViPNet

Ограничения при эксплуатации ViPNet Coordinator KB связанные с особенностями аппаратных платформ, лицензирования и режимами работы:

- Если роль Failover KB100 была добавлена на ViPNet Coordinator KB100 не при первичной установке дистрибутива ключей, а при обновлении ключей, то команды для работы с кластером могут не появиться в текущем сеансе работы командного интерпретатора. В таком случае необходимо завершить сеанс работы командного интерпретатора, после чего отключить токен и заново выполнить процедуру аутентификации.

- ViPNet Coordinator KB не поддерживает функции межсетевого взаимодействия. Учитывайте это при проектировании вашей сети ViPNet и при настройке ViPNet Coordinator KB с помощью управляющего ПО ViPNet Administrator.
- В ViPNet Coordinator KB работа с парольными ключами не поддерживается, поэтому при настройке устройства с помощью управляющего ПО ViPNet Administrator используйте только вариант аутентификации через персональный токен-ключ. В противном случае после обновления ключевой информации связь с ViPNet Coordinator KB в защищенной сети ViPNet будет нарушена.
- Доступ к веб-интерфейсу ViPNet Coordinator KB по умолчанию заблокирован встроенным межсетевым экраном. Для управления ViPNet Coordinator KB с использованием веб-интерфейса необходимо добавить пользовательское правило межсетевого экрана, разрешающее входящие соединения по протоколу TCP на порт 8080.
- Максимальное количество IP-адресов, используемых сетевыми интерфейсами ViPNet Coordinator KB (как физическими, так и логическими), не может превышать 128.
- После смены варианта ключей ViPNet Coordinator KB необходимо выполнить обновление справочников и ключей вручную (см. раздел Обновление справочников и ключей в документе «Настройка с помощью командного интерпретатора»). В противном случае отправка обновлений ключевой информации узла через ЦУС приведет к потере связи ViPNet Coordinator KB с узлами сети ViPNet.
- Функция локального обновления ПО ДНСД поддерживается только для ViPNet Coordinator KB с версией ПО ДНСД не ниже 2.0.0. Для обновления ПО ДНСД версии ниже чем 2.0.0 обратитесь в службу поддержки ИнфоТеКС (чтобы узнать версию ПО ДНСД используйте команду version).
- Для ViPNet Coordinator KB возможно только локальное обновление программного обеспечения. При этом он поддерживает роль транспортного сервера и может доставлять обновления программного обеспечения из ЦУС на другие сетевые узлы ViPNet.

6

История версий ViPNet Coordinator KB

Что нового в версии 4.3.2	83
Что нового в версии 4.3.1	85
Что нового в версии 4.3.0	88
Что нового в версии 4.2.1	89
Что нового в версии 4.2.1	89

Что нового в версии 4.3.2

- **Поддержка новой аппаратной платформы**

Добавлена поддержка аппаратной платформы KB2000 Q5. Платформа производится в формате 1U. Технические характеристики KB2000 Q5 приведены в разделе «[Описание исполнений](#)» (на стр. 33).

- **Поддержка токенов Jakarta-2 ГОСТ**

Добавлена поддержка токенов Jakarta-2 ГОСТ, Jakarta-2 PKI/ГОСТ и Jakarta-2 PRO/ГОСТ.

- **Увеличено максимальное количество поддерживаемых соединений МЭ**

В новой версии ViPNet Coordinator KB увеличено максимальное количество поддерживаемых соединений межсетевого экрана для аппаратных платформ KB1000 Q8 и KB5000 Q2. Подробнее об ограничениях для разных исполнений см. в документе «Справочник команд и конфигурационных файлов».

- **Добавлены новые параметры мониторинга SNMP**

Добавлена поддержка новых параметров мониторинга:

- сведения о версии ПО ДНСД;
- сведения о текущих значениях напряжения, полученных с элемента питания ДНСД;
- сведения о состоянии и параметрах работы службы, отвечающей за контроль событий ДНСД.

- **Повышение отказоустойчивости агента SNMP**

В целях повышения отказоустойчивости работоспособность SNMP-агента контролируется системой. Это увеличивает надежность работы системы мониторинга ViPNet Coordinator KB в нештатных ситуациях.

- **Обновление версии ПО ДНСД**

В новой версии ПО ДНСД увеличено хранилище ключевой информации для последующих версий ViPNet Coordinator KB.

- **Исправление ошибок**

Исправлены ошибки, выявленные в ходе эксплуатации предыдущих версий ViPNet Coordinator KB, повышена стабильность работы.

Что нового в версии 4.3.1

- **Поддержка новых аппаратных платформ**

Добавлена поддержка новой аппаратной платформы KB5000 Q2. Платформа обладает высокой производительностью и предназначена для установки в стандартные 19" телекоммуникационные стойки.

- **Обновленная система мониторинга**

Добавлена поддержка новых параметров мониторинга, получаемых с физических сенсоров:

- сведения о датчиках температуры и их текущих значениях;
- сведения о датчиках скорости вращения вентиляторов и их текущих значениях;
- сведения о датчиках напряжения и их текущих значениях.

- **Исправление ошибок**

Исправлены ошибки, выявленные в ходе эксплуатации предыдущих версий ViPNet Coordinator KB, повышена стабильность работы.

Что нового в версии 4.3.0

- **Поддержка новой аппаратной платформы**

Добавлено новое исполнение ViPNet Coordinator KB1000 на базе аппаратной платформы KB1000 Q8, предназначенной для установки в стандартные 19" телекоммуникационные стойки.

- **Политики маршрутизации и проверка состояния шлюзов (Dead Gateway Detection, DGD)**

В новой версии ViPNet Coordinator KB реализованы механизмы, позволяющие распределить нагрузку на сеть или настроить резервные каналы доступа в Интернет для сетей, в инфраструктуре которых используется несколько шлюзов (провайдеров):

- Пользовательские таблицы маршрутизации. С их помощью вы можете задать маршруты для различных ситуаций. Например, основную таблицу маршрутизации и дополнительную таблицу на случай, если шлюз основного провайдера станет недоступен и потребуются перенаправить трафик через шлюз альтернативного провайдера.
- Политики маршрутизации (Routing policy). С их помощью вы можете задать условия, при которых трафик будет перенаправляться по тем или иным маршрутам.
- Проверка состояния шлюзов (Dead Gateway Detection, DGD). С помощью этой функции вы можете задавать выполнение политики маршрутизации в зависимости от доступности или недоступности шлюза.

Подробную информацию о работе и настройке пользовательских таблиц маршрутизации, политик маршрутизации и DGD см. в документах «Настройка с помощью командного интерпретатора» и «Настройка с помощью веб-интерфейса», в разделе «Настройка функции MultiWAN».

- **Возможность создания агрегированных интерфейсов**

В новой версии ViPNet Coordinator KB появилась возможность объединять несколько физических сетевых интерфейсов ViPNet Coordinator KB в один агрегированный. Эта функция может понадобиться, если пропускной способности отдельных сетевых интерфейсов недостаточно для решения ваших задач. Также вы можете использовать агрегированные интерфейсы для повышения надежности и резервирования каналов связи. При соответствующей настройке агрегированного интерфейса передача данных будет продолжаться, даже если какой-либо входящий в него физический интерфейс выйдет из строя.

- **Управление MTU и поддержка Jumbo frame**

В новой версии ViPNet Coordinator KB вы можете изменить размер MTU на значение из диапазона 1280–9000 байт, чтобы оптимизировать передачу данных и снизить нагрузку на центральный процессор (задав значение MTU более 1500 байт) или для согласования размера MTU (в том случае, если на связанном оконечном сетевом оборудовании задан размер MTU меньше стандартного (менее 1500 байт)). Подробнее о настройке MTU см. в документах «Настройка с помощью командного интерпретатора» и «Настройка с помощью веб-интерфейса».

- **Веб-интерфейс для удаленного управления ViPNet Coordinator KB**

В дополнение к командному интерпретатору в состав новой версии ViPNet Coordinator KB включен веб-интерфейс, предназначенный для мониторинга и управления основными параметрами настройки ViPNet Coordinator KB по протоколу http. Работа с веб-интерфейсом поддерживается всеми современными браузерами и доступна с защищенных узлов сети ViPNet, связанных с координатором. Подробное описание работы с веб-интерфейсом изложено в документе «Настройка с помощью веб-интерфейса»

- **Удаленное управление с помощью протокола SSH**

Для расширения возможностей по управлению в ViPNet Coordinator KB реализованы функции удаленного управления по протоколу SSH. Удаленное управление допускается только с другого ViPNet Coordinator KB, для этого в командный интерпретатор ViPNet Coordinator KB встроен SSH-клиент.

- **Автоматическая смена серии ДСДР**

Для новой версии ViPNet Coordinator KB в программе ЦУС возможно одновременно назначить два ключевых блокнота ДСДР и настроить автоматическую смену текущей серии ДСДР при истечении ее срока действия. Данная функция доступна при использовании ЦУС версии не ниже 4.6.7.

- **Усовершенствованный механизм работы кластера горячего резервирования**

В предыдущих версиях ViPNet Coordinator KB в кластере горячего резервирования необходимо было назначать дополнительные IP-адреса сетевым интерфейсам пассивного узла. Такие IP-адреса указывались в значении параметра `passiveip` в секциях `[channel]` конфигурационного файла `failover.ini`. В ViPNet Coordinator KB версии 4.3.0 сетевым интерфейсам пассивного узла не назначаются IP-адреса, поэтому больше данный параметр не используется. При этом проверка доступности интерфейсов активного узла кластера горячего резервирования пассивным происходит с помощью отправки ARP-запросов в режиме проверки наличия дублирующего IP-адреса (Duplicate address detection).

- **Добавлен режим кластера горячего резервирования для исполнения KB100**

Для повышения отказоустойчивости обеспечена работа системы защиты от сбоев ViPNet Coordinator KB в режиме кластера горячего резервирования для исполнения ViPNet Coordinator KB100. Для активации режима кластера горячего резервирования используется дополнительная роль **Failover KB100**, назначаемая в программе ЦУС.

- **Синхронизация времени между узлами кластера горячего резервирования**

Теперь при функционировании ViPNet Coordinator KB в составе кластера горячего резервирования на пассивном узле кластера выполняется синхронизация системного времени при расхождении времени более чем на 1 секунду, либо при отличающихся настройках временных зон узлов.

- **Обновление встроенного SNMP-агента**

Для взаимодействия с последними версиями программного обеспечения сетевого менеджмента (NMS) в ViPNet Coordinator KB версии 4.3.0 добавлена поддержка новых параметров баз управляющей информации SNMP. Также повышена стабильность работы и изменен уровень журналирования событий SNMP-агента по умолчанию.

- **Расширенная функциональность DHCP-сервера и агента DHCP-relay**

В ViPNet Coordinator KB версии 4.3.0 были реализованы следующие новые функции DHCP-сервера:

- работа в кластере горячего резервирования;
- передача DHCP-клиентам дополнительных параметров сети, таких как: широковещательный IP-адрес, адреса DNS- и NTP-серверов, доменное имя и другие опции DHCP-сервера в соответствии с [RFC 2132](#);
- передача параметров сети DHCP-клиентам, находящимся в удаленной подсети;
- работа с несколькими сетевыми интерфейсами. DHCP-сервер может работать на разных сетевых интерфейсах одновременно, и для каждого интерфейса можно задать свой набор параметров;
- одновременное использование DHCP-сервера и DHCP-relay;
- запуск нескольких процессов DHCP-relay для нескольких сетевых интерфейсов;
- возможность указать запасной DHCP-сервер;
- возможность указать туннелируемый DHCP-сервер.

Подробнее о работе и настройке DHCP-сервера и DHCP-relay см. в документах «Настройка с помощью командного интерпретатора» и «Настройка с помощью веб-интерфейса», в разделах «Настройка параметров DHCP-сервера» и «Настройка DHCP-relay».

- **Локальное обновление ПО ДНСД**

В процессе локального обновления ПО ViPNet Coordinator KB при необходимости может быть обновлено ПО ДНСД. При этом файлы обновления ПО ДНСД включаются в состав пакета обновления и разворачиваются автоматически.

- **Возможность пропускать любые защищенные IP-пакеты**

В новой версии ViPNet Coordinator KB появилась возможность пропускать защищенные IP-пакеты для узлов ViPNet, даже если связь с ними не была задана в ЦУСе.

- **Поддержка RuToken Lite**

Теперь для аутентификации на ViPNet Coordinator KB вы можете использовать новый тип токена – Rutoken Lite производства компании «Актив».

Что нового в версии 4.2.1

- **Исправление ошибок**

Исправлены ошибки, выявленные в ходе эксплуатации предыдущих версий ViPNet Coordinator KB, повышена стабильность работы продукта.

Что нового в версии 4.2.0

- **Поддержка новых исполнений**

Теперь ViPNet Coordinator KB поставляется в одном из пяти исполнений (см. [Описание исполнений](#) на стр. 25):

- ViPNet Coordinator KB100 — на базе аппаратной платформы KB100 N1.
- ViPNet Coordinator KB1000 — на базе аппаратной платформы KB1000 Q6 и KB1000 Q7.
- ViPNet Coordinator KB2000 — на базе аппаратной платформы KB2000 Q4.
- ViPNet Coordinator KB5000 — на базе аппаратной платформы KB5000 Q1.

- **Добавлен режим кластера горячего резервирования**

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

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

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

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

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

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

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

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

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

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

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

Для поддержки механизма обеспечения качества обслуживания (QoS) в новой версии ViPNet Coordinator KB реализована возможность обрабатывать трафик в соответствии с заданными приоритетом.

- **Новые функции маршрутизации IP-трафика**

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

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

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

- **Появилась возможность экстренного удаления ключевой информации**

Теперь ViPNet Coordinator KB может стереть всю ключевую информацию по нажатию специальной кнопки, которая расположена на передней панели аппаратной платформы.

Данная функция не поддерживается в исполнении ViPNet Coordinator KB1000 (KB1000 Q7).

- **Датчик несанкционированного доступа**

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

В исполнении ViPNet Coordinator KB1000 (KB1000 Q7) ДНСД не применяется.

- **Прекращение поддержки устаревших исполнений**

Больше не поддерживаются следующие исполнения:

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



Термины и сокращения

DHCP (Dynamic Host Configuration Protocol)

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

DiffServ (Differentiated Service)

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

DSCP-метка

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

L2OverIP

Технология, которая позволяет организовать защиту удаленных сегментов сети, использующих одно и то же адресное пространство, на канальном уровне модели OSI. В результате узлы из разных сегментов сети смогут взаимодействовать друг с другом в одном широковещательном домене. В основе технологии лежит перехват на канальном уровне модели OSI Ethernet-кадров, отправленных из одного сегмента сети в другой.

OSPF (Open Shortest Path First)

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

ViPNet Administrator

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

ViPNet Policy Manager

Программа для централизованного управления политиками безопасности узлов защищенной сети ViPNet.

ViPNet StateWatcher

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

ViPNet Центр управления сетью (ЦУС)

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

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

изменение конфигурации сети;

формирование и рассылка справочников;

рассылка ключей узлов и ключей пользователей;

формирование информации о связях пользователей для Удостоверяющего и ключевого центра;

задание полномочий пользователей сетевых узлов ViPNet.

Администратор сети ViPNet

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

Виртуальная защищенная сеть

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

Датчик несанкционированного доступа (ДНСД)

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

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.

Кластер горячего резервирования

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

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

Клиент (ViPNet-клиент)

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

Ключевой блокнот ДСДР

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

Ключи узла ViPNet

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

Координатор (ViPNet-координатор)

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

Маршрутизация

Процесс выбора пути для передачи информации в сети.

Межсетевой экран

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

Обычная консоль

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

Пароль администратора ViPNet Coordinator KB

Пароль для включения режима администратора ViPNet Coordinator KB. Создается администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр.

Персональный ключ пользователя

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

PIN-код

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

Политики безопасности

Набор параметров — сетевых фильтров и правил трансляции сетевых адресов, регулирующих безопасность сетевого узла.

Резервный набор персональных ключей (РНПК)

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

Роль

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

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

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

Сервер IP-адресов

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

Сервер соединений

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

Сетевой узел ViPNet

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

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищенных узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Симметричный ключ

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

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

Токен

Компактное устройство аутентификации, предназначенное для обеспечения информационной безопасности пользователя.

Трансляция сетевых адресов (NAT)

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

Транспортный конверт

Зашифрованная информация служб или приложений, доставляемая на защищенные узлы ViPNet транспортным сервером MFTP.

Транспортный сервер MFTP

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

Транспортный сервер MFTP

Компонент координатора, обеспечивающий маршрутизацию транспортных конвертов MFTP между узлами сети ViPNet.

Туннелирование

Технология, позволяющая защитить соединения между узлами локальных сетей, которые обмениваются информацией через интернет или другие публичные сети, путем инкапсуляции и шифрования трафика этих узлов не самими узлами, а координаторами, которые установлены на границе их локальных сетей.



Изменения в документации

- **21.04.2023 — обновлены документы:**
 - «Подготовка к работе»
Обновлен раздел «Перечень поддерживаемых токенов».
- **06.07.2023 — обновлены документы:**
 - «Подготовка к работе»
Обновлены разделы: «Защищенная сеть ViPNet», «Подключение через промежуточный ViPNet Coordinator KB».
- **12.03.2024 — обновлены документы:**
 - «Подготовка к работе»:
Обновлен раздел: «Смена ключевого блокнота ДСДР».
Уточнен список совместимых продуктов ViPNet.
Уточнены характеристики аппаратных платформ KB100 Q1/Q2.
Уточнена максимальная разница системного времени между ViPNet Coordinator KB 4 и другими узлами сети (изменения по итогам сертификации).
Уточнен и дополнен раздел «Использование ключевого блокнота».
Уточнен сценарий обновления справочников и ключей
Дополнен раздел «Подключение через промежуточный ViPNet Coordinator KB».
 - «Настройка с помощью командного интерпретатора»:
Добавлен раздел «Смена мастер-ключей».
Обновлен список NTP-серверов по умолчанию.
База управляющей информации для протокола SNMP VIPNETDNSD-MIB дополнена значениями низкого и критического заряда батареи.

- «Настройка с помощью веб-интерфейса»:
Обновлен список NTP-серверов по умолчанию.
База управляющей информации для протокола SNMP VIPNETDNSD-MIB дополнена значениями низкого и критического заряда батареи.
- «Справочное руководство по командному интерпретатору и конфигурационным файлам»:
Уточнена максимальная разница системного времени между ViPNet Coordinator KB 4 и другими узлами сети (изменения по итогам сертификации).
Добавлено описание команды `admin keys update`
- **17.05.2024 — обновлены документы:**
 - «Подготовка к работе»
Обновлены спецификации аппаратных платформ.
Добавлен раздел «Поддерживаемое дополнительное оборудование»