



ViPNet Coordinator IG 5

Подготовка к работе

Версия продукта: 5.2.0

ViPNet Coordinator IG10

ViPNet Coordinator IG100

ViPNet Coordinator IG1000

© АО «ИнфоТеКС», 2025

ФРКЕ.467759.003ИС1

Версия продукта 5.2.0

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.

Все условия эксплуатации и ограничения на использование ViPNet Coordinator IG приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet Coordinator IG.

АО «ИнфоТеКС»

125167, г. Москва, вн. тер. г. муниципальный округ Хорошевский, ул. Викторенко, д. 9, стр. 1, помещ. 47

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.....	5
О документе.....	6
Соглашения документа.....	6
Комплект поставки.....	7
Что нового в версии 5.2.0.....	8
Совместимость с продуктами ViPNet.....	15
Обратная связь.....	16
 Глава 1. Назначение ViPNet Coordinator IG.....	17
Общее описание.....	18
Функции.....	19
Межсетевой экран с контролем состояния соединений.....	19
Расширенная фильтрация промышленных протоколов	20
Криптографический шлюз	21
VPN-шлюз.....	22
Сервер IP-адресов.....	24
Сервер соединений.....	24
Маршрутизатор VPN-пакетов	25
Защищённый интернет-шлюз.....	26
Транспортный сервер MFTP	26
Коммутатор и маршрутизатор	26
Обработка сетевого трафика в соответствии с приоритетом	27
Оборудование радиодоступа	27
Абонентское устройство связи стандартов GSM	28
Промышленный шлюз	28
Дополнительные возможности	30
Кластер горячего резервирования.....	30
 Глава 2. Исполнения и лицензирование	31
Исполнения ViPNet Coordinator IG.....	32
Внешний вид аппаратных платформ.....	33
Основные отличия аппаратных платформ	34
Ограничение по регистрации клиентов за ViPNet Coordinator IG.....	35
Лицензирование.....	36
Функциональные ограничения по окончании срока действия лицензий.....	36

Глава 3. Режимы работы и управление	38
Режимы работы	39
Каналы управления.....	41
Ролевая модель доступа.....	42
Способы аутентификации.....	43
Способы управления.....	44
Управление с помощью ViPNet Prime.....	44
Управление с помощью веб-интерфейса	44
Управление с помощью командного интерпретатора.....	46
Одновременная работа пользователей.....	47
Глава 4. Ввод в эксплуатацию.....	49
Порядок действий.....	50
Способы подключения.....	51
Подключение через консоль.....	51
Подключение через канал Ethernet	53
Включение ViPNet Coordinator IG	55
Инициализация	57
Начало инициализации	57
Установка дистрибутива ключей	58
Настройка сети.....	59
Настройка проверки связи с узлом ViPNet.....	61
Выбор узла для проверки связи.....	62
Запуск драйверов и служб.....	63
Настройка после инициализации	64
Настройка подключения к ViPNet Prime	64
Настройка удалённого доступа.....	65
Перезагрузка и выключение ViPNet Coordinator IG	66
Приложение А. Термины и сокращения	68



Введение

О документе	6
Комплект поставки	7
Что нового в версии 5.2.0	8
Совместимость с продуктами ViPNet	15
Обратная связь	16

О документе

В документе описываются назначение и функции программно-аппаратного комплекса ViPNet Coordinator IG 5 (далее — ViPNet Coordinator IG), характеристики исполнений, лицензирование и возможности управления ViPNet Coordinator IG, приведен порядок действий по подготовке ViPNet Coordinator IG к использованию.

Соглашения документа

Обозначение	Описание
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская её, нажмите вторую
Меню > Команда	Последовательность элементов или действий
Код	Имя файла, путь, фрагмент кода или команда в командной строке

Комплект поставки

- Аппаратная платформа с предустановленным ПО ViPNet Coordinator IG.
- Документы в формате PDF:
 - «Подготовка к работе».
 - «Описание аппаратных платформ».
 - «Настройка с помощью командного интерпретатора».
 - «Настройка с помощью веб-интерфейса».
 - «Сценарии работы».
 - «Справочник команд и конфигурационных файлов».
 - «Лицензионные соглашения на компоненты сторонних производителей».

Что нового в версии 5.2.0

Новые возможности и другие изменения версии 5.2.0 по сравнению с версией 5.1.0:

- **Поддержка новых аппаратных платформ**

- IG100 I5 поддерживает технологию PoE (Power over Ethernet), которая позволяет ViPNet Coordinator IG:
 - подавать электропитание на подключённые к нему устройства по Ethernet-кабелю;
 - получать электропитание по Ethernet-кабелю и работать без подключения к электросети.
- IG1000 Q1 — серверная платформа высокой производительности; устанавливается в серверную стойку.

Подробнее о новых аппаратных платформах см. [Исполнения ViPNet Coordinator IG](#) и документ «Описание аппаратных платформ».

- **Несколько шлюзов Modbus**

Теперь интерфейсы RS-232 и RS-485 можно использовать одновременно. Для этого вы можете настроить на каждом интерфейсе отдельный независимый шлюз Modbus.

Команды для настройки шлюза Modbus теперь начинаются с ключевых слов `service mbgw` вместо `service modbus_gateway`.

Подробнее о настройке шлюзов Modbus см. в документах «Настройка с помощью командного интерпретатора» и «Настройка с помощью веб-интерфейса» в разделе «Настройка шлюза Modbus».

- **Поддержка протокола BGP**

В исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1 вы можете настроить использование протокола BGP для обмена маршрутами между автономными системами. При этом доступно:

- настройка собственного маршрутизатора;
- настройка соседей;
- анонсирование подсетей;
- настройка фильтров, префикс-листов и карт маршрутов (только в командном интерпретаторе);
- перераспределение подключённых и статических маршрутов с возможностью их фильтрации по карте маршрутов;
- настройка ECMP и UCMP (только в командном интерпретаторе);
- просмотр BGP-таблицы маршрутизации и BGP-сессий.

Подробнее о настройке использования протокола BGP см. в документах «Настройка с помощью командного интерпретатора» и «Настройка с помощью веб-интерфейса» в разделе «Настройка BGP».

- **Антивирусная проверка трафика, проходящего через прокси-сервер**

В исполнениях ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1 вы можете подключить внешнее средство антивирусной защиты по протоколу ICAP для проверки трафика, проходящего через прокси-сервер.

Подробнее о настройке антивирусной проверки трафика см. в документах «Настройка с помощью командного интерпретатора» и «Настройка с помощью веб-интерфейса» в разделе «Настройка антивирусной проверки трафика».

- **Расширение возможностей протокола IPLir 6**

- Поддержка сетей со сложной топологией;
- Оптимизация маршрутов служебного трафика и сокращения количества межузловых рассылок.

Данные возможности поддерживаются ViPNet Prime версии 1.9.5 и выше.

- **Новый способ регистрации IP-пакетов**

Раньше использовался способ регистрации IP-пакетов по интерфейсам. Все пропущенные и заблокированные IP-пакеты регистрировались в журнале IP-пакетов один раз — при прохождении сетевого интерфейса или блокировке. Все пропущенные транзитные IP-пакеты регистрировались два раза — на интерфейсах, через которые они прошли. Настройка регистрации выполнялась в конфигурационных файлах сетевых интерфейсов.

Теперь по умолчанию используется способ регистрации IP-пакетов по сетевым фильтрам. Каждый IP-пакет регистрируется в журнале IP-пакетов один раз — при срабатывании сетевого фильтра. При этом регистрировать IP-пакет или нет, настраивается для каждого сетевого фильтра отдельно. Это позволяет не записывать в журнал ненужную для вас информацию и снизить нагрузку на ViPNet Coordinator IG.

На каждом сетевом интерфейсе ViPNet Coordinator IG можно выбрать только один из этих способов. После обновления ПО ViPNet Coordinator IG до версии 5.2.0 продолжает действовать способ регистрации IP-пакетов по интерфейсам. Чтобы включить регистрацию IP-пакетов по сетевым фильтрам, см. документ «Настройка с помощью командного интерпретатора» или «Настройка с помощью веб-интерфейса», раздел «Журнал IP-пакетов».

- **Счётчики срабатывания правил межсетевого экрана**

Для исполнений ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1 добавлены счётчики срабатывания сетевых фильтров и правил трансляции адресов. На основе информации о количестве срабатываний каждого сетевого фильтра вы можете изменить их порядок в таблице сетевых фильтров, например передвинуть часто срабатывающие фильтры в начало таблицы, чтобы они применялись к IP-пакетам первыми. Это поможет оптимизировать производительность ViPNet Coordinator IG.

Просмотр счётчиков доступен только в веб-интерфейсе ViPNet Coordinator IG (см. документ «Настройка с помощью веб-интерфейса», раздел «Просмотр сетевых фильтров»). Значения

счётчиков автоматически передаются в ViPNet Prime, где используются для централизованного формирования политик безопасности.

- **Возможность отключения NTP-серверов по умолчанию**

В новой версии ViPNet Coordinator IG при добавлении дополнительных NTP-серверов вы можете исключить из процесса синхронизации времени публичные NTP-серверы, заданные по умолчанию. Подробнее см. в документах «Настройка с помощью командного интерпретатора» и «Настройка с помощью веб-интерфейса», в разделе «Настройка NTP-сервера».

- **Синхронизация таблицы открытых соединений в кластере**

Раньше при переключении узлов кластера все открытые соединения прерывались. Теперь вы можете включить синхронизацию таблицы открытых соединений, и соединения не будут прерываться при переключении узлов кластера. Это позволяет обеспечить бесперебойную работу приложений, трафик которых проходит через ViPNet Coordinator IG, в случае переключения узлов кластера.

Функция доступна во всех исполнениях ViPNet Coordinator IG100 и ViPNet Coordinator IG1000. Управление функцией выполняется с помощью параметров `syncconnections` и `syncalgtcp` в секции `[misc]` конфигурационного файла `failover.ini`. Подробнее см. в документе «Настройка с помощью командного интерпретатора» в разделе «Развёртывание кластера».

- **Отображение уровней сигналов GSM и Wi-Fi**

В исполнениях ViPNet Coordinator IG со встроенным модемом или модулем Wi-Fi вы можете проверить текущие уровни сигналов GSM и Wi-Fi. В командном интерпретаторе используйте команды `inet show usb-modem` и `inet show interface wlan0`. В веб-интерфейсе уровень сигнала отображается при наведении курсора на значки  и .

Также уровни сигналов периодически записываются в системный журнал: для GSM — по умолчанию, для Wi-Fi — после включения командой `inet wifi log signal` (см. документ «Настройка с помощью командного интерпретатора», раздел «Подключение к сети Wi-Fi»).

- **Отображение информации о состоянии оборудования**

В **промышленных исполнениях ViPNet Coordinator IG** вы можете просмотреть информацию о состоянии аппаратных модулей (температура процессора и модема, состояние дисковой памяти) через командный интерпретатор или веб-интерфейс. Это поможет оценить условия эксплуатации ViPNet Coordinator IG, выявить причины неполадок и предотвратить выход из строя оборудования. Подробнее см. в документе «Настройка с помощью командного интерпретатора» раздел «Просмотр состояния оборудования» и в документе «Настройка с помощью веб-интерфейса» раздел «Просмотр состояния».

- **Расширение состава универсальной конфигурации**

Теперь с помощью экспорта и импорта универсальной конфигурации (*.vbe) вы можете переносить следующие группы настроек с одного ViPNet Coordinator IG на другой:

- настройки шлюзов Modbus;
- правила фильтрации промышленных протоколов;
- настройки интерфейса GPIO.

Подробнее об использовании универсальной конфигурации см. в документах «Настройка с помощью командного интерпретатора» и «Настройка с помощью веб-интерфейса» в разделе «Управление универсальной конфигурацией».

- **Серийный номер аппаратной платформы**

Для более удобной инвентаризации оборудования теперь вы можете просмотреть серийный номер аппаратной платформы через командный интерпретатор или веб-интерфейс ViPNet Coordinator IG, а также получить его по SNMP. Если вы обновили ПО с версии, в которой не был задан серийный номер, вы можете вручную ввести его в память ViPNet Coordinator IG.

Подробнее о просмотре и задании серийного номера см. в документах «Настройка с помощью командного интерпретатора» и «Настройка с помощью веб-интерфейса» в разделе «Просмотр серийного номера».

- **Статистика правил межсетевого экрана**

Для исполнений ViPNet Coordinator IG100 I4 и ViPNet Coordinator IG1000 Q1 в разделе веб-интерфейса **Состояние системы** отображается информация о количестве сетевых фильтров и правил трансляции адресов: общее количество, количество активных, выключенных, а также правил, которые не срабатывали.

- **Новый порядок обработки исключений в группах объектов межсетевого экрана**

Изменена логика формирования действующего состава групп объектов межсетевого экрана при вложении групп друг в друга. Теперь обработка вложенных исключений происходит на каждом уровне вложенности, начиная с наиболее глубокого.

При обновлении ПО ViPNet Coordinator IG до версии 5.2.0 или импорте настроек межсетевого экрана с более старых версий убедитесь в корректности работы тех правил межсетевого экрана, которые используют группы объектов, содержащие другие группы в качестве состава или исключения.

- **Подключение к серверу TCP-туннелей**

Теперь ViPNet Coordinator IG может быть не только сервером TCP-туннелей, но и подключаться к своему серверу соединений в качестве клиента TCP-туннеля. Подробнее см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка TCP-туннеля».

- **Защищённый интернет-шлюз**

Исполнение ViPNet Coordinator IG1000 Q1 поддерживает функцию защищённого интернет-шлюза. При включении этой функции из ViPNet Prime, клиенты ViPNet Coordinator IG могут работать в одном из двух режимов:

- Работа в интернете. Корпоративные ресурсы недоступны.
- Работа в корпоративной сети. Доступ в интернет заблокирован.

Подробнее см. в документе «Сценарии работы», раздел «Использование ViPNet Coordinator IG в качестве защищённого интернет-шлюза».

- **Статистика обработанных IP-пакетов с учётом приоритета**

Теперь вы можете просмотреть статистику обработанных IP-пакетов с учётом приоритета в обслуживании (QoS) с помощью команды `machine show priority-stats`. Подробнее см. в «Справочнике команд и конфигурационных файлов».

- **Прекращение поддержки автоматического определения видимости узлов и сетей**

Для повышения стабильности работы защищённой сети больше не поддерживается автоматическое определение видимости узлов и сетей. Теперь во всех параметрах конфигурационного файла `iplir.conf`, отвечающих за настройку видимости, можно настроить видимость по реальным или виртуальным IP-адресам. Значения `auto` больше нет. После обновления ПО до версии 5.2.0 все настройки автоматического определения видимости будут преобразованы в видимость по реальным или виртуальным IP-адресам.

- **Изменение значений по умолчанию для параметров шлюза Modbus**

Интервал задержки, действующий после отправки посылки с последовательного интерфейса шлюза Modbus типа RS-485, теперь составляет 0 мс вместо 100 мс. Подробнее см. описание команды `service mbgw after-send-delay` в «Справочнике команд и конфигурационных файлов».

- **Команды по настройке журнала IP-пакетов**

- Настраивать параметры ведения журнала IP-пакетов теперь можно не только в конфигурационном файле, но и с помощью команд:

Параметр секции [db]	Команда
<code>maxsize</code>	<code>machine logs settings network-traffic maxsize</code>
<code>timedif</code>	<code>machine logs settings network-traffic timediff</code>
<code>omittcpclientport</code>	<code>machine logs settings network-traffic omit-client-port</code>
<code>registerbroadcast</code> <code>registerevents</code>	<code>machine logs settings network-traffic register</code>

- Просматривать значения параметров можно с помощью команды:

```
machine logs settings show.
```

- **Команды по настройке экспорта событий журнала IP-пакетов в формате CEF**

- Теперь часть настроек экспорта может быть выполнена как в конфигурационных файлах `iplir.conf`-<интерфейс или группа интерфейсов>, так и с помощью команд:

Параметр секции [cef]	Команда
<code>event</code>	<code>machine logs settings cef event-type</code>
<code>exclude</code>	<code>machine logs settings cef exclude</code> <code>machine logs settings cef include</code>

- В команду `machine logs settings show` добавлено отображение настроек экспорта.

- **Команды по настройке параметров VPN**

- Теперь часть параметров VPN собственного узла может быть настроена как в конфигурационном файле `iplir.conf`, так и с помощью команд:

Параметр секции [dynamic]	Команда
dynamic_proxy	iplir option mode
forward_id	
always_use_server	
timeout	iplir option keepalive-timeout
Параметр секции [misc]	Команда
be_dg_coordinator	iplir option be-default-gateway
client_pollinterval	iplir option ping-timeout
ifcheck_timeout	iplir option interface-timeout
ipforwarding	iplir option ip-forwarding
mssdecrease	iplir option mss-decrease
server_pollinterval	iplir option server-ping-timeout
timediff	iplir option maxtimediff
timesync	iplir option sync-time
udp_ports_count	iplir option udp-ports-count
Параметр секции [debug]	Команда
debuglevel	iplir option syslog-level

- Просмотр параметров работы службы `iplircfg` доступен по команде:
`iplir option show`
- Часть параметров VPN связанного узла может быть настроена как в конфигурационном файле `iplir.conf`, так и с помощью команд:

Параметр секции [id]	Команда
accessiplist	iplir node access-point add iplir node access-point delete
blockforward	iplir node blockforward
fqdn	iplir node add domain-name iplir node delete domain-name

- Просмотр списка связанных узлов:
`iplir node list`
- Просмотр настроек параметров VPN связанных узлов:
`iplir node show`
- Просмотр списка доменных имён связанного узла:
`iplir node show domain-names`
- Обновить DNS-кеш узла:
`iplir node update domain-name cache`

- **Изменения команд настройки и просмотра параметров межсетевого экрана**

Команды настройки параметров межсетевого экрана из группы `iplir` заменены на команды из группы `firewall`:

Команда в ПО версии 5.1.0	Команда в ПО версии 5.2.0
<code>iplir option set antispoofing</code>	<code>firewall setting antispoofing</code>
<code>iplir option set block-fragmented-packets</code>	<code>firewall setting block-fragmented-packets</code>
<code>iplir option set connection-ttl-ip</code>	<code>firewall setting connection-ttl-ip</code>
<code>iplir option set connection-ttl-tcp</code>	<code>firewall setting connection-ttl-tcp</code>
<code>iplir option set connection-ttl-udp</code>	<code>firewall setting connection-ttl-udp</code>
<code>iplir option set max-connections</code>	<code>firewall setting max-connections</code>
<code>iplir option get</code>	<code>firewall settings show</code>

- **Замена команд `vpn start\stop`**

Вместо команд `vpn start` и `vpn stop` теперь используется команда `firewall conntrack flush`. Она позволяет закрыть все открытые соединения без остановки служб.

Совместимость с продуктами ViPNet

Продукт	Версия
ViPNet Client 4 (Windows)	4.5.5 и выше
ViPNet Client 4U for Linux	4.15 и выше
ViPNet Client 4U for Android	4.0.0 и выше
ViPNet Client 4U for Windows	4.12.2 и выше
ViPNet Client 4U for iOS	4.1.0 и выше
ViPNet Client 4U for macOS	4.1.1 и выше
ViPNet Client 4U for Aurora	4.0.7 и выше
ViPNet Client 5 for Windows	5.0 и выше
ViPNet Client 5 for Linux	5.0.1 и выше
ViPNet Prime	1.9.6, 1.9.11 и выше
ViPNet Coordinator VA	4.3.3 и выше
ViPNet Coordinator HW 4	4.5.8 и выше
ViPNet Coordinator HW 5	5.1.2, 5.2.1 (алгоритм шифрования по ГОСТ 28147-89), 5.3 и выше
ViPNet Coordinator IG 4	4.3.3 и выше
ViPNet Coordinator IG 5	5.1.0
ViPNet xFirewall	5.6.3, 5.7.6 и выше
ViPNet PKI Client for Windows	2.0.1 и выше
ViPNet PKI Client for Linux	2.0.1 и выше

Обратная связь

Контактная информация

- 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.
Телеграм-канал поддержки: t.me/vhd21.
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

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

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



1

Назначение ViPNet Coordinator IG

Общее описание	18
Функции	19
Дополнительные возможности	30

Общее описание

ViPNet Coordinator IG — это индустриальный шлюз безопасности, который объединяет в одном устройстве следующие совместно работающие функции безопасности:

- межсетевой экран SPI (Stateful Packet Inspection) уровня сети или уровня промышленной сети;
- криптографический шлюз, обеспечивающий построение VPN на сетевом (L3) и канальном (L2) уровнях модели OSI;
- маршрутизатор и коммутатор;
- точка доступа Wi-Fi;
- абонентское устройство связи стандартов GSM;
- промышленный шлюз.

Перечень поддерживаемых функций зависит от [аппаратного исполнения](#) ViPNet Coordinator IG и приобретённой лицензии ([лицензируются отдельные модули](#)).

ViPNet Coordinator IG предназначен для использования:

- в государственных информационных системах до класса защищённости К1 включительно;
- в автоматизированных системах управления технологическим процессом (АСУ ТП) до класса защищённости К1 включительно;
- в информационных системах для обеспечения 1 и 2 уровня защищённости персональных данных;
- в информационных системах (ИС), информационно-телекоммуникационных системах (ИТС) и автоматизированных системах (АСУ) критической информационной инфраструктуры (КИИ) до 1 категории значимости.

Основные сценарии применения:

- защита периметра информационной и промышленной сети;
- сегментирование сети и защита доступа к сегменту;
- организация защищённого канала связи между сегментами сети, в том числе для распределённых систем;
- организация защищённого канала связи для последовательных сетей;
- организация удалённого защищённого доступа к сегменту сети, в том числе с использованием мобильных устройств;
- защита промышленных устройств от несанкционированного управления.

ViPNet Coordinator IG реализуется в исполнении программно-аппаратного комплекса на доверенной аппаратной платформе. Программно-аппаратный комплекс может поставляться в серверном и промышленном исполнении. Последние могут использоваться в промышленных помещениях при температурах от -40 до +60 °С и обеспечивают класс защиты IP30.

Функции



Примечание. Список доступных функций зависит от набора лицензий и аппаратного исполнения ViPNet Coordinator IG. Подробнее см. [Исполнения и лицензирование](#).

- **Межсетевой экран** с контролем состояния соединений. Выполняет фильтрацию IP-трафика и трансляцию IP-адресов (NAT).
- **Расширенная фильтрация промышленных протоколов.** Позволяет фильтровать трафик, относящийся к промышленным протоколам Modbus и МЭК 60870-5-104, на прикладном уровне.
- **Криптографический шлюз.** Позволяет организовывать защищённые соединения между узлами сети и между сегментами сетей с помощью защищённых каналов (туннелей).
- **Коммутатор и маршрутизатор.** Обеспечивает коммутацию сетевых узлов и маршрутизацию IP-трафика в сетях передачи данных.
- **Оборудование радиодоступа.** Обеспечивает взаимодействие с беспроводными сетями передачи данных по технологии Wi-Fi.
- **Абонентское устройство связи стандартов GSM.** Обеспечивает подключение к мобильной сети для организации беспроводного канала передачи данных.
- **Промышленный шлюз.** Обеспечивает взаимодействие с промышленной инфраструктурой с помощью интерфейса GPIO и объединяет последовательные линии связи и сеть Ethernet с помощью встроенного [шлюза Modbus](#).

Межсетевой экран с контролем состояния соединений

Фильтрация трафика

ViPNet Coordinator IG выполняет фильтрацию IP-пакетов на каждом сетевом интерфейсе по адресам, протоколам и портам в соответствии с настроенными сетевыми фильтрами. При этом поддерживается защита от спуфинга.

При использовании ViPNet Coordinator IG в качестве криптографического шлюза выполняется также фильтрация VPN-трафика (см. [Криптографический шлюз](#)).

Прокси-сервер

Для дополнительной обработки HTTP-трафика в ViPNet Coordinator IG реализован прокси-сервер, который позволяет кешировать данные и фильтровать содержимое HTTP-трафика.

Трансляция сетевых адресов (NAT)

ViPNet Coordinator IG может осуществлять трансляцию сетевых адресов для проходящего через него открытого трафика. Правила трансляции сетевых адресов используются 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 ViPNet Coordinator IG.
- 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.

Типы межсетевого экрана

ViPNet Coordinator IG удовлетворяет требованиям ФСТЭК к межсетевым экранам типов «А», «Б» и «Д» четвёртого класса защиты. В зависимости от применения в инфраструктуре вашей организации, ViPNet Coordinator IG может функционировать как межсетевой экран одного из типов:

- Тип «А» — межсетевой экран уровня сети, применяемый на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы;
- Тип «Б» — межсетевой экран уровня сети, применяемый на логической границе информационной системы или между логическими границами сегментов информационной системы;
- Тип «Д» — межсетевой экран, применяемый в автоматизированной системе управления технологическими или производственными процессами. Межсетевые экраны типа «Д» обеспечивают контроль и фильтрацию промышленных протоколов передачи данных. Кроме того, межсетевые экраны типа «Д» имеют расширенный набор режимов работы.

Расширенная фильтрация промышленных протоколов

Для трафика, относящегося к промышленным протоколам Modbus и МЭК 60870-5-104, ViPNet Coordinator IG выполняет фильтрацию на транспортном и прикладном уровнях модели OSI. Это позволяет защитить промышленные устройства от некорректных и запрещённых сигналов, которые могут быть отправлены с разрешённых устройств и сетевых узлов.

Криптографический шлюз

ViPNet Coordinator IG может выполнять роль шлюза в VPN-сеть, построенную по технологии ViPNet (далее — защищённая сеть). Это виртуальная частная сеть (VPN), организованная поверх локальных и глобальных IP-сетей с помощью ПО ViPNet. Трафик между узлами такой сети защищается с помощью шифрования на симметричных ключах. Ключи распределяются централизованно.

В минимальном варианте защищённая сеть может состоять из двух VPN-шлюзов, расположенных на границах локальных сетей и защищающих трафик между этими сетями.

Защищённая сеть (или сеть ViPNet) может состоять из узлов следующих типов:

- Клиенты — компьютеры или мобильные устройства с ПО ViPNet Client. Шифруют трафик при обмене данными с другими узлами защищённой сети.
- Координаторы — компьютеры или программно-аппаратные комплексы с ПО ViPNet Coordinator. Обеспечивают взаимодействие клиентов, маршрутизацию и фильтрацию защищённого трафика, а также другие функции.

Координаторы могут туннелировать узлы локальной сети, на которых не установлено ПО ViPNet Client (открытые узлы). Трафик от таких узлов шифруется на координаторе и передаётся на клиенты или узлы, туннелируемые другим координатором (см. функцию [VPN-шлюз](#)).

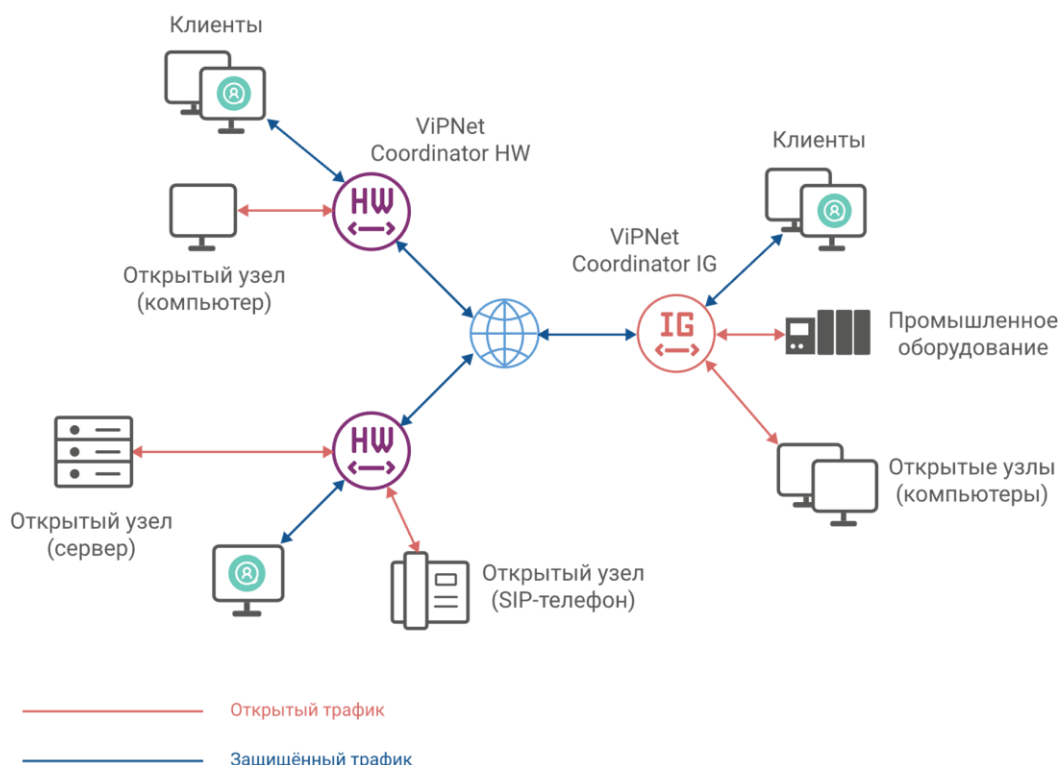


Рисунок 1. Типы узлов сети ViPNet

Управление защищённой сетью

Для настройки и управления защищённой сетью используется [ViPNet Prime](#), который обеспечивает создание узлов защищённой сети и связей между ними, а также:

- настройку параметров доступа к узлам;
- создание [дистрибутивов ключей](#) для узлов;
- обновление справочников и ключей на узлах;
- обновление ПО ViPNet на узлах;
- управление политиками безопасности узлов;
- мониторинг состояния узлов.

Функции координатора

ViPNet Coordinator IG выполняет следующие функции в защищённой сети:

- [VPN-шлюз](#);
- [сервер IP-адресов](#);
- [сервер соединений](#);
- [маршрутизатор VPN-пакетов](#);
- [транспортный сервер MFTP](#).

VPN-шлюз

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

Туннелирование на сетевом уровне

Туннелирование на сетевом уровне позволяет организовать защищённое соединение между удалёнными друг от друга открытыми узлами, которые туннелируются разными координаторами, а также между открытыми узлами и узлами [защищённой сети](#).

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 узлы назначения в защищённой сети;
 - или на другой координатор, если узел назначения — открытый узел, туннелируемый этим координатором.
- 3 На другом координаторе из зашифрованных IP-пакетов извлекаются исходные IP-пакеты, расшифровываются, обрабатываются сетевыми фильтрами и передаются на открытые узлы назначения.

Для фильтрации туннелируемого трафика в межсетевом экране координатора используется отдельный набор сетевых фильтров.

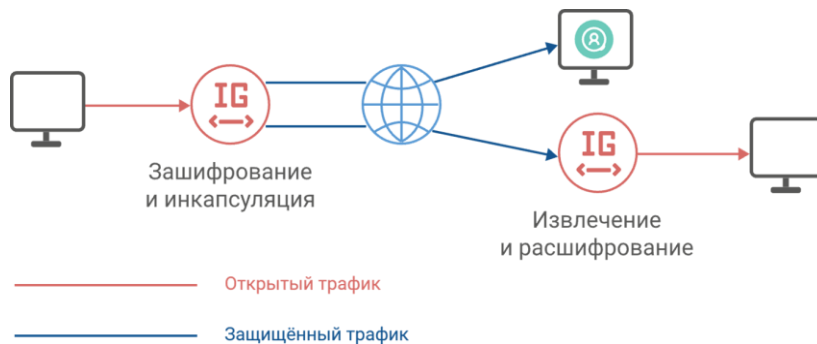


Рисунок 2. Защита соединения на сетевом уровне модели OSI

Туннелирование на канальном уровне

Туннелирование на канальном уровне, или L2OverIP, позволяет организовать защищённое соединение между узлами удалённых 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 упаковываются в IP-пакеты специального формата и передаются по защищённому каналу.
- 3 Из полученных IP-пакетов на координаторах извлекаются исходные кадры и передаются узлам сегмента назначения.

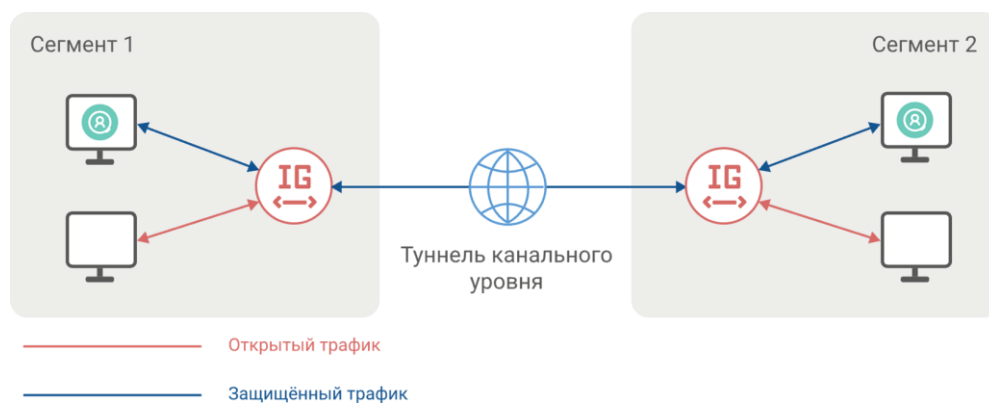


Рисунок 3. Защита соединения на канальном уровне модели OSI

Сервер IP-адресов

Клиенту для взаимодействия с другими защищёнными узлами требуется информация об адресах и параметрах доступа. Данную информацию клиент получает автоматически от координатора, который выполняет для него 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 эту информацию 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.
- Чтобы подтвердить свое присутствие в сети, координатор периодически (по умолчанию — каждые 15 минут) отправляет 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 Prime. Сервер IP-адресов можно сменить, выбрав другой координатор, с которым у данного клиента есть связь.

Примечание. Использование ViPNet Coordinator IG в качестве шлюзового координатора в другие сети ViPNet возможно:



- для [исполнений](#) ViPNet Coordinator IG100 и ViPNet Coordinator IG1000 — в сетях под управлением ViPNet Prime версии 1.9.11 или выше;
 - только для исполнения ViPNet Coordinator IG1000 Q1 — в сетях под управлением ViPNet Prime версии ниже 1.9.11.
-

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](#).



Рисунок 4. Организация соединений между сетевыми узлами ViPNet

Когда удалённый 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 5. Доступ удалённого клиента к сети ViPNet через TCP-туннель

Для каждого узла защищённой сети можно назначить свой сервер соединений. Для клиентов — это координатор, выполняющий функцию **сервера IP-адресов**.

Маршрутизатор VPN-пакетов

Клиенты, находящиеся в разных подсетях, связываются друг с другом через координаторы. Координатор при этом выполняет маршрутизацию защищённого трафика в сети ViPNet.

Защищённый трафик маршрутизируется на основе идентификаторов (ViPNet ID), которые присваиваются каждому узлу сети ViPNet и не меняются при смене IP-адреса узла. Это позволяет узлам защищённой сети взаимодействовать между собой независимо от изменений параметров и конфигурации физической сети.

Порядок взаимодействия клиентов через координатор:

- Клиент вставляет в открытую часть IP-пакета идентификатор узла назначения и отправляет IP-пакет координатору (идентификатор защищён от подмены).
- Координатор на основе идентификатора определяет маршрут доставки IP-пакета и отправляет его адресату или другому координатору, указав свой IP-адрес в качестве адреса источника (параметры трансляции адресов для защищённого трафика изменить нельзя).

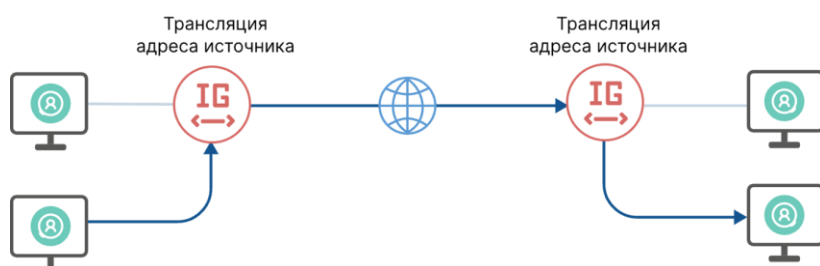


Рисунок 6. Функция маршрутизации защищённого трафика в сети ViPNet

Трафик маршрутизируется как внутри одной сети ViPNet, так и при взаимодействии с другими сетями ViPNet.

Защищённый интернет-шлюз

Защищённый интернет-шлюз позволяет разделить доступ узлов защищённой сети в интернет и к корпоративным ресурсам.

Клиенты, связанные с защищённым интернет-шлюзом, могут работать в одном из двух режимов:

- Работа в интернете. Корпоративные ресурсы недоступны.
- Работа в корпоративной сети. Доступ в интернет заблокирован.

Такое разделение обеспечивает доступ в интернет с максимальным уровнем безопасности, возможным без физического отключения компьютера от корпоративной сети.

Транспортный сервер MFTP

Клиенты и координаторы версий ниже 5.x обмениваются с ViPNet Prime [транспортными конвертами MFTP](#). Если такой клиент зарегистрирован за ViPNet Coordinator IG, то для передачи конвертов используется [транспортный сервер MFTP](#) на ViPNet Coordinator IG.

Внимание!



- Функция транспортного сервера MFTP поддерживается только в исполнениях ViPNet Coordinator IG100 и ViPNet Coordinator IG1000. Подробнее см. [Ограничение по регистрации клиентов за ViPNet Coordinator IG](#).
 - ViPNet Coordinator IG не поддерживает передачу транспортных конвертов MFTP другим координаторам и расположенным за ними клиентам. Для этого используйте ViPNet Coordinator HW.
-

Коммутатор и маршрутизатор

ViPNet Coordinator IG выполняет маршрутизацию транзитного IP-трафика на основе политик и таблиц маршрутизации. При этом поддерживается статическая маршрутизация и маршрутизация по протоколам DHCP/PPP, OSPF и BGP. Доступна настройка балансировки трафика.

В ViPNet Coordinator IG реализована функция MultiWAN, которая позволяет настроить резервирование канала доступа в интернет.

Для расширения возможностей по обработке трафика и взаимодействия со сторонним сетевым оборудованием ViPNet Coordinator IG поддерживает функции:

- работа с виртуальными локальными сетями VLAN IEEE 802.1Q;
- агрегирование сетевых интерфейсов IEEE 802.3ad;

- обработка сетевого трафика в соответствии с приоритетом.

В качестве сетевых служб в ViPNet Coordinator IG реализованы функции DHCP-, DNS- и NTP-сервера, а также агента DHCP-relay.

Обработка сетевого трафика в соответствии с приоритетом

В ViPNet Coordinator IG реализована поддержка протокола классификации сетевого трафика DiffServ. Использование этого протокола предполагает, что в заголовок каждого IP-пакета может быть добавлена DSCP-метка, задающая приоритет обработки пакета.

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

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

ViPNet Coordinator IG поддерживает следующие политики обработки трафика с учётом приоритета в соответствии с [RFC 2474](#) и [RFC 2475](#):

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

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

Оборудование радиодоступа

ViPNet Coordinator IG позволяет:

- подключиться к внешней сети передачи данных по беспроводному каналу с использованием точки доступа Wi-Fi этой сети;
- подключить внешние устройства к локальной сети по беспроводному каналу Wi-Fi.



Примечание. Возможность подключения к сети Wi-Fi зависит от наличия встроенного модуля Wi-Fi в вашем [исполнении ViPNet Coordinator IG](#).

Для этого модуль Wi-Fi поддерживает два режима работы:

- режим клиента — для подключения ViPNet Coordinator IG к сторонней точке доступа Wi-Fi;
- режим точки доступа — для подключения внешних устройств Wi-Fi к ViPNet Coordinator IG.

Абонентское устройство связи стандартов GSM

ViPNet Coordinator IG может подключаться к мобильным сетям стандартов GSM, UMTS, LTE. Это позволяет организовать беспроводной канал передачи данных из любого места, которое входит в зону покрытия сети вашего оператора мобильной связи.



Примечание. Возможность подключения к сети 3G/4G зависит от наличия встроенного модема в вашем исполнении ViPNet Coordinator IG.

Промышленный шлюз

ViPNet Coordinator IG позволяет подключать устройства, взаимодействующие по промышленному протоколу Modbus RTU, к сетям Ethernet или к беспроводным сетям. Для этого в ViPNet Coordinator IG реализован шлюз Modbus, который преобразует сигналы из протокола Modbus RTU в Modbus TCP и наоборот. В результате обеспечивается взаимодействие устройств, работающих по данным протоколам.

Устройства Modbus RTU подключаются к ViPNet Coordinator IG по последовательным линиям связи, использующих стандарты RS-232 и RS-485.

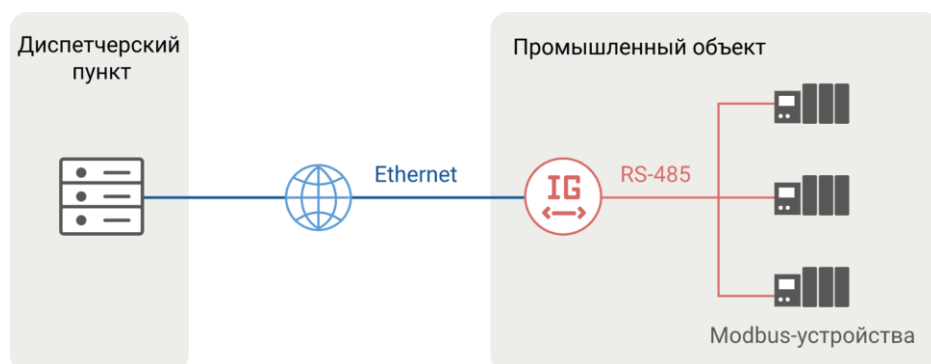


Рисунок 7. Организация взаимодействия Modbus-устройств и диспетчерского пункта

Возможности ViPNet Coordinator IG расширяет интерфейс GPIO, который вы можете применять для решения следующих задач безопасности АСУ ТП:

- Подключение датчика вскрытия внешнего шкафа.
- Подключение внешней кнопки для перевода ViPNet Coordinator IG в [специальный режим работы](#).

- Сигнализация о событиях, отслеживаемых ViPNet Coordinator IG.
- Отправка сигналов о режиме работы ViPNet Coordinator IG в [кластере](#).

Подробнее об использовании шлюза Modbus в промышленных сетях см. в документе «Сценарии работы».

Дополнительные возможности

Кластер горячего резервирования

ViPNet Coordinator IG поддерживает работу в составе кластера горячего резервирования, который состоит из двух синхронизированных между собой ViPNet Coordinator IG. При сбое в работе одного узла кластера, его функции выполняет второй узел.

Работа в кластере обеспечивает непрерывность выполнения функций шлюза безопасности, что важно для работы АСУ ТП и других АС.

Особенности функционирования кластера:

- Узлы кластера переключаются без перезагрузки.
- Настройки ViPNet Coordinator IG синхронизируются между узлами кластера.
- Для быстрого восстановления связи с сетевым оборудованием после переключения узлов кластера поддерживаются технологии:
 - Виртуальные MAC-адреса сетевых интерфейсов;
 - Синхронизация таблицы открытых соединений.

Подробнее см. документ «Настройка с помощью командного интерпретатора», раздел «Развёртывание кластера».

2

Исполнения и лицензирование

Исполнения ViPNet Coordinator IG	32
Лицензирование	36

Исполнения ViPNet Coordinator IG

ViPNet Coordinator IG может поставляться в различных исполнениях, которые отличаются аппаратной платформой, а также наличием или отсутствием беспроводных модулей Wi-Fi и 3G/4G.

Таблица 1. Исполнения и аппаратные платформы

Исполнение	Аппаратная платформа	Описание
ViPNet Coordinator IG10 I1	IG10 I1	Промышленное исполнение
ViPNet Coordinator IG10 I2	IG10 I2	Промышленное исполнение
ViPNet Coordinator IG100 I1	IG100 I1	Промышленное исполнение
ViPNet Coordinator IG100 I4	IG100 I4	Промышленное исполнение
ViPNet Coordinator IG100 I5	IG100 I5	Промышленное исполнение
ViPNet Coordinator IG1000 Q1	IG1000 Q1	Серверное исполнение

Особенности промышленных исполнений:

- Компактный корпус с возможностью установки на DIN-рейку.
- Работа от источника питания с постоянным током и напряжением 12–24 В.
- Пониженное энергопотребление и тепловыделение.
- Расширенный диапазон рабочих температур (см. [Основные отличия аппаратных платформ](#)).
- Возможность встраивания беспроводных модулей.
- Функция [промышленного шлюза](#).
- Соответствие стандартам электромагнитной совместимости по ГОСТ 30804.6.4 – 2013, ГОСТ 30805.22-2013 (CISPR 22:2006) для устройств класса А или Б.
- Соответствие стандартам устойчивости к электромагнитным помехам по ГОСТ CISPR 24-2013, ГОСТ 30804.6.2-2013 (IEC 61000-6-2:2005).
- Класс защиты IP30 в соответствии с ГОСТ 14254-2015.

Особенности серверных исполнений:

- Повышенная производительность.
- Размещение в серверной стойке.
- Соответствие стандартам электромагнитной совместимости по ГОСТ 30805.22-2013 (CISPR 22:2006).
- Соответствие стандартам устойчивости к электромагнитным помехам по ГОСТ CISPR 24-2013.
- Класс защиты IP20 в соответствии с ГОСТ 14254-2015.

Внешний вид аппаратных платформ



IG10 I1

IG10 I2

Рисунок 8. Исполнения ViPNet Coordinator IG10



IG100 I1

IG100 I4

IG100 I5

Рисунок 9. Исполнения ViPNet Coordinator IG100



IG1000 Q1

Рисунок 10. Исполнения ViPNet Coordinator IG1000

Основные отличия аппаратных платформ

Таблица 2. Производительность аппаратных платформ

Платформа	Суммарная производительность всех задействованных сетевых интерфейсов, Мбит/с	Максимальное количество одновременных соединений	Максимальное количество сетевых фильтров	Максимальное количество правил фильтрации промышленных протоколов
IG10 I1	9	1000	50	50
IG10 I2	9	1000	50	50
IG100 I1	55	15000	200	100
IG100 I4	250	1000000	400	400
IG100 I5	55	15000	200	100
IG1000 Q1	900	2500000	1000	500

Таблица 3. Сетевые порты и порты ввода-вывода

Платформа	Ethernet RJ45	Ethernet SFP	RS-232/RS-485	GPIO	USB	Консольный
IG10 I1	1x WAN / 2x LAN	—	Совмещённый	1x In / 1x Out	2x	RS-232 (RJ45)
IG10 I2	2x WAN / 3x LAN	—	Раздельный	1x In / 1x Out	2x	RS-232 (RJ45)
IG100 I1	1x WAN / 2x LAN	—	Совмещённый	1x In / 1x Out	2x	RS-232 (RJ45)
IG100 I4	2x WAN / 3x LAN	2x WAN	Раздельный	2x In / 2x Out	2x	RS-232 (RJ45)
IG100 I5	1x WAN (PoE PD) / 2x LAN (PoE PS)	—	Совмещённый	1x In / 1x Out	2x	RS-232 (RJ45)
IG1000 Q1	4x WAN/LAN	4x WAN/LAN	—	16x In / 8x Out	6x	RS-232 (DB9-M), VGA+USB

Возможность установки беспроводных модулей Wi-Fi и 3G/4G доступна только для промышленных исполнений ViPNet Coordinator IG.



Внимание! Модуль Wi-Fi и модем 3G/4G устанавливаются в ViPNet Coordinator IG только на этапе производства. Установка данных модулей в готовое изделие невозможна.

Таблица 4. Эксплуатационные отличия аппаратных платформ

Платформа	Эксплуатация при температуре	Резервное питание	Управление
IG10 I1	от -20 до +60°C от -40°C без модуля Wi-Fi	—	Командный интерпретатор
IG10 I2	от -40 до +60°C	Резервный порт питания	Командный интерпретатор
IG100 I1	от -40 до +60°C	—	Веб-интерфейс, командный интерпретатор
IG100 I4	от -40 до +60°C	Резервный порт питания	Веб-интерфейс, командный интерпретатор
IG100 I5	от -40 до +60°C	Питание по PoE	Веб-интерфейс, командный интерпретатор
IG1000 Q1	от +10 до +35°C	Резервный блок питания	Веб-интерфейс, командный интерпретатор

Аппаратные платформы IG10 I2 и IG100 I4 могут размещаться на электрических подстанциях.



Примечание. Подробное описание аппаратных платформ см. в документе «Описание аппаратных платформ».

Ограничение по регистрации клиентов за ViPNet Coordinator IG

Администратор ViPNet Prime при добавлении клиентов в защищённую сеть регистрирует их за координатором. ViPNet Coordinator IG в зависимости от исполнения имеет ограничения:

Таблица 5. Функциональные ограничения по регистрации клиентов за ViPNet Coordinator IG

Исполнения	Регистрация клиентов
ViPNet Coordinator IG10	Не поддерживается
ViPNet Coordinator IG100	Не более 10 клиентов за ViPNet Coordinator IG На клиентах не будут поддерживаться: • деловая почта • файловый обмен • ViPNet Connect Обновление ПО ViPNet 4.x для клиентов должно производиться последовательно, по одному
ViPNet Coordinator IG1000	Не более 100 клиентов за ViPNet Coordinator IG

Лицензирование

Функции и возможности ViPNet Coordinator IG определяются лицензией, которая назначается в ViPNet Prime. Для этого необходимо получить файл лицензии и загрузить его в ViPNet Prime.

Лицензионный файл может содержать следующие лицензии:

- Основная
Разрешает использование ViPNet Coordinator IG в качестве межсетевого экрана типа «А/Б».
- VPN
Разрешает:
 - установку туннелируемых соединений на сетевом и канальном уровнях;
 - регистрацию ViPNet-клиентов за ViPNet Coordinator IG (только для исполнений ViPNet Coordinator IG100 и ViPNet Coordinator IG1000);
 - настройку фильтрации защищённого трафика;
 - смену типа межсетевого экрана («А/Б» и «Д»).
- IPF
Разрешает фильтрацию промышленных протоколов Modbus и МЭК 60870-5-104 на прикладном уровне.
- Modbus Gateway
Разрешает использование промышленного шлюза Modbus.
- Failover
Разрешает работу ViPNet Coordinator IG в составе кластера.

В ViPNet Prime можно включить или выключить функции, для которых есть отдельные лицензии.

Функциональные ограничения по окончании срока действия лицензий

Лицензии имеют срок действия, по окончании которого ViPNet Coordinator IG будет работать с ограничениями. Подробнее об ограничениях см. таблицу ниже.

Таблица 6. Функциональные ограничения в работе ViPNet Coordinator IG по окончании срока действия лицензий

Лицензия	Функциональные ограничения
Основная	• Блокируется транзитный открытый трафик. • Запрещается создание и изменение транзитных фильтров открытой сети. • Запрещается настройка интерфейса GPIO, кроме возможности отключения отслеживания пользовательских событий (<code>service piomonitor reset</code>). Интерфейс продолжает работать. • Сохраняется связь с ViPNet Prime для обновления лицензий. • Прекращается действие лицензии VPN — см. ниже.
VPN	• Закрываются туннелируемые соединения сетевого и канального уровней; установка новых соединений запрещается. • Прекращается обслуживание зарегистрированных ViPNet-клиентов и регистрация новых. • Блокируется защищённый трафик, кроме служебного трафика между координаторами. • Запрещается создание и изменение сетевых фильтров туннелируемых узлов и защищённой сети. • Запрещается смена типа межсетевого экрана («А/Б» и «Д»). • Сохраняется связь с ViPNet Prime.
IPF	• Фильтрация промышленных протоколов отключается. • Запрещается создание и изменение правил фильтрации промышленных протоколов. • При обновлении ПО ViPNet Coordinator IG правила фильтрации не переносятся, а фильтрация промышленных протоколов отключается.
Modbus Gateway	• Шлюзы Modbus выключаются. • Запрещается изменение параметров шлюзов Modbus.
Failover	• Сохраняется работоспособность узлов кластера и синхронизация настроек, кроме автоматического переключения. • Сохраняется возможность ручного переключения узлов кластера через командный интерпретатор.

3

Режимы работы и управление

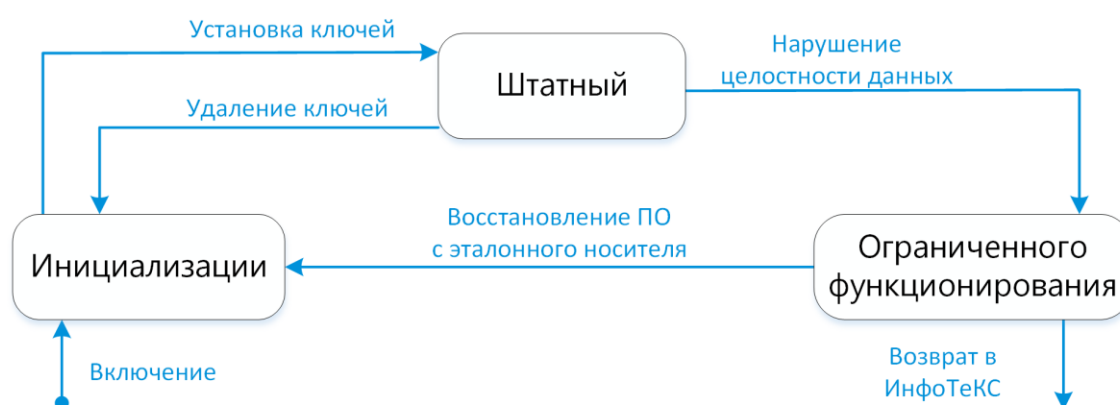
Режимы работы	39
Каналы управления	41
Ролевая модель доступа	42
Способы аутентификации	43
Способы управления	44
Одновременная работа пользователей	47

Режимы работы

ViPNet Coordinator IG в зависимости от состояния может находиться в одном из режимов работы: инициализации, штатном, ограниченного функционирования. Переключение между этими режимами выполняется автоматически.

Если ViPNet Coordinator IG используется как межсетевой экран типа «Д», к штатному режиму добавляются: специальный режим и режим регламентного обслуживания. Переключение между ними выполняется вручную.

ViPNet Coordinator IG как
межсетевой экран типа «А/Б»



ViPNet Coordinator IG как
межсетевой экран типа «Д»

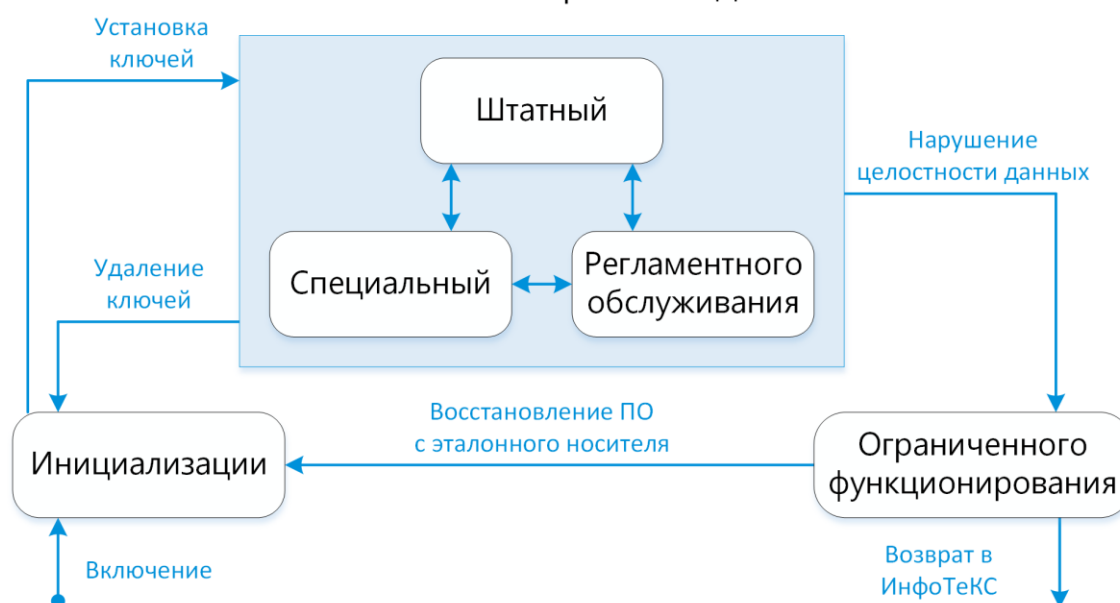


Рисунок 11. Режимы работы ViPNet Coordinator IG

До установки дистрибутива ключей ViPNet Coordinator IG находится в режиме инициализации. После установки дистрибутива ключей он переходит в штатный режим.

В случае возникновения ошибок при загрузке ViPNet Coordinator IG или нарушения целостности конфигурационных файлов ViPNet Coordinator IG переходит в режим ограниченного функционирования, в котором блокируется работа всех сетевых интерфейсов.

Режимы межсетевого экрана типа «Д»

Помимо режима инициализации и ограниченного функционирования ViPNet Coordinator IG может находиться в одном из режимов:

- Штатный. Работают все функции ViPNet Coordinator IG. Недоступно: обновление справочников и ключей, обновление ПО, управление копиями конфигураций VPN, импорт настроек.
- Регламентного обслуживания. Предназначен для обновления справочников и ключей, обновления ПО, управления копиями конфигураций VPN, импорта настроек, а также регламентного обслуживания защищаемых узлов.
- Специальный. Предназначен для чрезвычайных ситуаций в работе системы. Межсетевой экран по умолчанию настроен пропускать любой сетевой трафик. Обновление справочников и ключей, обновление ПО, управление копиями конфигураций VPN, импорт настроек недоступны.

Для каждого из этих режимов задан свой набор сетевых фильтров, которые можно изменить. Любые действия с сетевыми фильтрами (создание, изменение, удаление) применяются только для текущего режима работы межсетевого экрана.

Переключение режимов для межсетевого экрана типа «Д»

Переключить режим работы можно любым из доступных [способов управления](#).



Внимание! Не переключайте режим работы ViPNet Coordinator IG одновременно несколькими способами. Иначе, это может нарушить работоспособность ViPNet Coordinator IG.

Также можно переключить ViPNet Coordinator IG в специальный режим и обратно с помощью внешнего устройства типа «кнопка» или «переключатель», подключённого к интерфейсу GPIO. (см. документ «Сценарии работы», раздел «Подключение внешнего устройства для перехода в специальный режим»).

Каналы управления

Управление возможно с помощью компьютера, подключённого к ViPNet Coordinator IG:

- Локально — через консольный порт (RS-232) или с помощью монитора и клавиатуры (только для исполнения ViPNet Coordinator IG1000 Q1).
- Удалённо — по сети Ethernet с использованием протоколов:
 - SSH;
 - HTTP/HTTPS — доступно для исполнений ViPNet Coordinator IG100 и ViPNet Coordinator IG1000.

Удалённое подключение разрешено только с узлов защищённой сети и возможно после инициализации ViPNet Coordinator IG (см. [Ввод в эксплуатацию](#)).

При локальном подключении и удалённом подключении по SSH доступно [управление с помощью командного интерпретатора](#). При удалённом подключении по HTTP/HTTPS — [управление с помощью веб-интерфейса](#).

Наиболее критичные для безопасности и работоспособности ViPNet Coordinator IG настройки доступны только локально.

Ролевая модель доступа

Роли

Для разграничения прав доступа к ViPNet Coordinator IG используются роли:

- Администратор — обладает полными правами доступа: может изменять настройки, обновлять ПО, выполнять резервное копирование, восстановление, просматривать журналы событий.
- Аудитор — может просматривать настройки и журналы событий.

Учётные записи

Для управления и аудита ViPNet Coordinator IG используются учётные записи двух типов:

- Локальные — учётные записи пользователей ViPNet Coordinator IG, созданные на ViPNet Coordinator IG:
 - Учётная запись `user` с ролью аудитора. Используется при вводе ViPNet Coordinator IG в эксплуатацию, после чего блокируется с возможностью последующей разблокировки.
 - Учётная запись `admin` с ролью администратора.

Изменить или удалить локальные учётные записи, а также добавить новые учётные записи невозможно.

- Централизованные — учётные записи пользователей ViPNet Prime, созданные в ViPNet Prime.

При использовании централизованной учётной записи пользователь будет иметь права администратора или аудитора в ViPNet Coordinator IG в зависимости от роли его учётной записи в ViPNet Prime.

Использование централизованных учётных записей возможно при наличии соединения ViPNet Coordinator IG с ViPNet Prime.

Способы аутентификации

ViPNet Coordinator IG поддерживает два способа аутентификации пользователей:

- по паролю;
- по сертификату.

Способ аутентификации устанавливается в ViPNet Prime и применяется для всей защищённой сети.

Аутентификация по паролю

Пароль применяется для аутентификации при использовании любого [канала управления](#) и [типа учётной записи](#).

Таблица 7. Аутентификация в зависимости от канала управления

Канал управления	Пользователь с локальной учётной записью	Пользователь с централизованной учётной записью
Локальный доступ	По паролю	По паролю
SSH	По паролю	По паролю
HTTP/HTTPS	По паролю	По паролю

Аутентификация по сертификату

Для аутентификации используется USB-токен, на котором хранятся закрытый ключ и сертификат пользователя. Поддерживаются следующие USB-токены:

- Рутокен ЭЦП 2.0 (2000, 2100, 2200, 3000, 4500);
- Рутокен ЭЦП 3.0 (3100).

При локальном доступе необходимо подключить USB-токен к ViPNet Coordinator IG. При удалённом доступе вместо сертификата локального пользователя используется его пароль и [ключ обмена](#), установленный на узле.

Таблица 8. Аутентификация в зависимости от канала управления

Канал управления	Пользователь с локальной учётной записью	Пользователь с централизованной учётной записью
Локальный доступ	По сертификату	По сертификату
SSH	По паролю и ключу обмена	Аутентификация запрещена
HTTP/HTTPS	По паролю и ключу обмена	По сертификату

Способы управления

Управление с помощью ViPNet Prime

ViPNet Prime используется для управления продуктами ViPNet, формирования структуры защищённой сети, централизованной рассылки справочников, ключей и обновлений ПО.

С помощью ViPNet Prime можно задать настройки и передать их на ViPNet Coordinator IG:

- [тип межсетевого экрана](#) «А/Б» или «Д»;



Внимание! При изменении типа межсетевого экрана с «А/Б» на «Д» все настройки сетевых фильтров удаляются. Подробнее см. документ «Настройка с помощью командного интерпретатора», раздел «Смена типа межсетевого экрана с сохранением сетевых фильтров».

- параметры подключения к ViPNet Coordinator IG:
 - параметры доступа к веб-интерфейсу;
 - режим подключения к внешней сети (Подробнее см. в документе «Настройка с помощью командного интерпретатора», раздел «Настройка подключения к внешней сети»);
 - параметры доступа к ViPNet Coordinator IG для других узлов сети.
- адреса туннелируемых узлов;
- политики безопасности.

С помощью модуля ViPNet Prime Policy Management можно передать на ViPNet Coordinator IG:

- сетевые фильтры и правила трансляции адресов;
- команду по переключению [режима работы](#) для межсетевого экрана типа «Д».

Управление с помощью веб-интерфейса



Внимание! Веб-интерфейс доступен только в [исполнениях ViPNet Coordinator IG100 и ViPNet Coordinator IG1000](#). Для управления ViPNet Coordinator IG10 используйте [командный интерпретатор](#).

В веб-интерфейсе ViPNet Coordinator IG доступно:

- Настройка сетевых интерфейсов и параметров подключения к сетям Ethernet, 3G/4G, Wi-Fi.
- Настройка подачи питания по технологии PoE.
- Настройка сетевых фильтров и правил трансляции адресов.

- Настройка фильтрации промышленных протоколов на прикладном уровне.
- Настройка туннелирования узлов.
- Настройка сетевых служб: встроенного DHCP-, DNS-, NTP- и прокси-сервера, DHCP-relay.
- Настройка обработки прикладных протоколов DNS, FTP, H.323, SCCP, SIP.
- Настройка шлюза Modbus.
- Настройка интерфейса GPIO.
- Настройка защиты соединения по технологии L2OverIP.
- Настройка маршрутизации.
- Настройка MultiWAN.
- Просмотр списка сетевых узлов ViPNet.
- Настройка даты и времени.
- Переключение режимов работы при функционировании ViPNet Coordinator IG как межсетевого экрана типа «Д».
- Управление ключами локального SSH-сервера.
- Управление локальными учётными записями администратора (`admin`) и аудитора (`user`).
- Создание резервных копий.
- Настройка расписания резервного копирования на ViPNet Prime.
- Восстановление из резервной копии.
- Экспорт и импорт настроек.
- Настройка параметров удалённого мониторинга по протоколу SNMP.
- Мониторинг состояния ViPNet Coordinator IG, настройка параметров регистрации событий, просмотр журналов:
 - системного журнала;
 - журнала IP-пакетов;
 - журнала пакетов промышленных протоколов;
 - журнала аудита и журнала СКЗИ;
 - журнала DNS-запросов;
 - журнала MFTP.
- Настройка перезагрузки ViPNet Coordinator IG по расписанию.

Режимы просмотра и настройки

Пользователь с ролью аудитора может работать только в режиме просмотра. Пользователь с ролью администратора может работать в режиме настройки сразу после аутентификации.

Для настройки параметров, которые нельзя изменять несколькими пользователями одновременно, необходимо отдельно включать режим настройки. Чтобы изменить настройки таких параметров, нажмите , внесите изменения и нажмите .

Управление с помощью командного интерпретатора

В командном интерпретаторе доступны все настройки, которые вы можете сделать с помощью веб-интерфейса, а также:

- Настройка режимов подключения ViPNet Coordinator IG к внешней сети.
- Настройка системы защиты от сбоев.
- Управление сертификатами пользователей ViPNet Coordinator IG.
- Управление конфигурациями VPN.
- Настройка транспортного сервера MFTP.
- Обновление и восстановление ПО ViPNet Coordinator IG.

Командный интерпретатор запускается автоматически после аутентификации:

- при локальном подключении;
- при удалённом подключении по протоколу SSH.

Режимы просмотра и настройки

Пользователь с ролью аудитора может работать только в режиме просмотра. Пользователь с ролью администратора может работать в режиме просмотра и в режиме настройки. Для перехода в режим настройки необходимо выполнить команду:

```
hostname> enable
```

```
hostname#
```

Чтобы вернуться в режим просмотра:

```
hostname# exit
```

```
hostname>
```

Одновременная работа пользователей

ViPNet Coordinator IG поддерживает одновременную работу до пяти пользователей в командном интерпретаторе и работу одного пользователя в веб-интерфейсе независимо от [типов учётных записей](#). При этом определённые настройки не могут одновременно редактировать несколько пользователей. Для этого настройки распределены по группам. Если пользователь редактирует настройки группы, то вся группа настроек недоступна для редактирования другими пользователями, пока первый пользователь не сохранит изменения.

Таблица 9. Распределение команд ViPNet Coordinator IG по группам настроек

Группа настроек	Команды
Системные	• Настройка даты и времени • Настройка сетевых интерфейсов • Перезагрузка ViPNet Coordinator IG • Резервное копирование конфигурации • Настройка системы защиты от сбоев • Настройка транспортного сервера MFTP • Другие системные настройки
VPN	Настройка параметров работы в защищённой сети ViPNet
Firewall	Настройка сетевых фильтров и правил трансляции адресов
IPF	Настройка правил фильтрации промышленных протоколов
Modbus	Настройка шлюза Modbus
GPIO	Настройка интерфейса GPIO
Modem	Настройка модема

Например, если администратор с учётной записью `admin` начал вносить изменения в сетевые фильтры, то настройка сетевых фильтров и правил трансляции адресов (группа настроек Firewall) будет заблокирована от изменения другими администраторами до тех пор, пока `admin` не применит изменения. При этом второй администратор может снять блокировку `admin` для изменения настроек межсетевого экрана. В этом случае `admin` получит уведомление и несохранённые изменения будут потеряны.

Отдельные команды, связанные с системными процессами, устанавливают глобальную блокировку, на время которой:

- блокируются команды всех групп настроек, в том числе команды просмотра настроек;
- на сессии пользователей накладываются ограничения.

Таблица 10. Команды, устанавливающие глобальную блокировку

Команда	Ограничения
<code>admin remove keys</code> — удаление ключей	Завершение сессий всех пользователей
<code>admin system erase</code> — удаление ПО	Завершение сессий всех пользователей, новые сессии не открываются
<code>admin upgrade software</code> — обновление ПО	Завершение сессий всех пользователей, новые сессии не открываются
<code>machine backup export</code> — экспорт конфигурации	Текущие сессии пользователей сохраняются, новые сессии не открываются
<code>machine reboot</code> — перезагрузка	Завершение сессий всех пользователей
<code>machine self-test</code> — проверка целостности ПО	Текущие сессии пользователей сохраняются, новые сессии не открываются

Примечание.



- Блокировки не синхронизируются в режиме кластера. Блокировка, установленная на активном узле, после переключения кластера остаётся действующей.
- Глобальная блокировка не всегда проверяется до начала выполнения интерактивных команд. В некоторых случаях это приводит к завершению команды после окончания интерактивного ввода.

4

Ввод в эксплуатацию

Порядок действий	50
Способы подключения	51
Включение ViPNet Coordinator IG	55
Инициализация	57
Настройка после инициализации	64
Перезагрузка и выключение ViPNet Coordinator IG	66

Порядок действий



Примечание. Для ввода в эксплуатацию двух ViPNet Coordinator IG в составе кластера см. документ «Настройка с помощью командного интерпретатора», раздел «Развёртывание кластера».

1 У администратора защищённой сети:

- Получите дистрибутив ключей (файл *.ds5) и пароль к нему.



Внимание! После первого подключения ViPNet Coordinator IG к ViPNet Prime дистрибутив ключей, использованный для ввода в эксплуатацию, становится недействительным. Если необходимо удалить ключи и выполнить повторную инициализацию, запросите новый дистрибутив ключей.

При организации кластера из двух ViPNet Coordinator IG используйте один и тот же дистрибутив ключей для каждого узла кластера.

- Узнайте доменное имя и идентификатор узла ViPNet Prime.
- Если в защищённой сети используется аутентификация по сертификату, получите USB-токен (список поддерживаемых USB-токенов см. в разделе [Способы аутентификации](#)). В ходе инициализации на USB-токен будут сохранены сертификат и закрытый ключ администратора, которые будут использоваться для локальной аутентификации на ViPNet Coordinator IG.

Если вы организуете кластер из двух ViPNet Coordinator IG, вам потребуется два USB-токена — по одному для каждого узла кластера.

- 2 Если в вашем ViPNet Coordinator IG есть модем или Wi-Fi, то, чтобы их использовать, установите SIM-карту (для модема) и внешние антенны. Подробнее см. документ «Описание аппаратных платформ», разделы «Установка SIM-карты» и «Беспроводные модули».
- 3 Если у вас промышленное исполнение ViPNet Coordinator IG, разместите его на DIN-рейке, если серверное исполнение — в серверной стойке (см. документ «Описание аппаратных платформ»).
- 4 Во время инициализации вы сможете проверить связь с каким-либо из связанных узлов сети ViPNet. Для этого подключите ViPNet Coordinator IG к коммутационному оборудованию сети.
- 5 Подключитесь к ViPNet Coordinator IG одним из способов (см. [Способы подключения](#)).
- 6 Выполните инициализацию ViPNet Coordinator IG (см. [Инициализация](#)).
- 7 С помощью командного интерпретатора выполните настройки для завершения ввода в эксплуатацию (см. [Настройка после инициализации](#)).

Способы подключения

В ходе инициализации ViPNet Coordinator IG необходимо установить дистрибутив ключей, в котором содержатся справочники, ключи и лицензия ViPNet Coordinator IG. Есть несколько способов подключения к ViPNet Coordinator IG для выполнения инициализации. В каждом из них используется свой способ установки дистрибутива ключей:

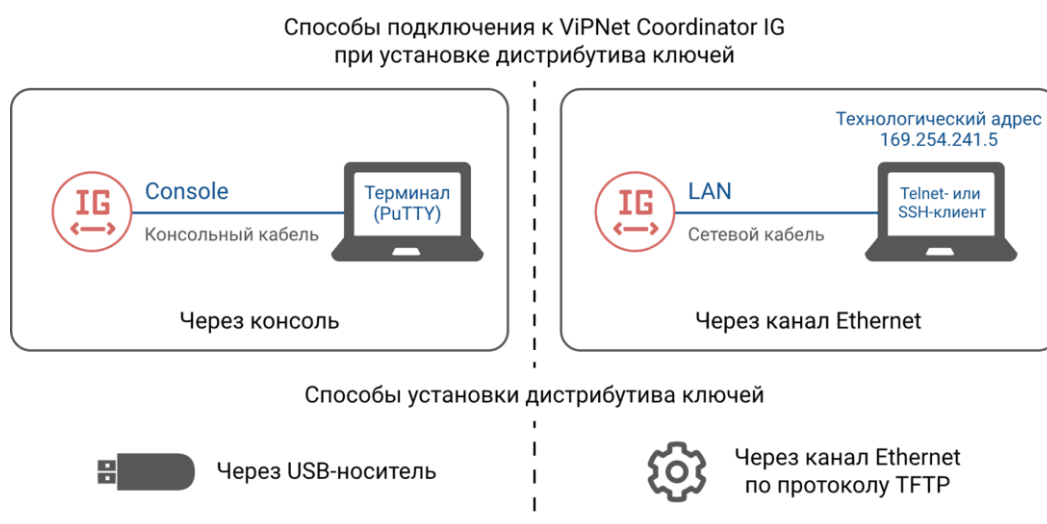


Рисунок 12. Способы подключения и установки справочников и ключей на ViPNet Coordinator IG

Вы можете выбрать один из способов подключения:

- Через консоль. Компьютер необходимо подключить к консольному порту ViPNet Coordinator IG, а дистрибутив ключей записать на USB-носитель.

Для исполнения ViPNet Coordinator IG1000 Q1 вы можете отдельно подключить монитор и клавиатуру вместо использования консольного порта.

- Через канал Ethernet. Компьютер необходимо подключить к сетевому интерфейсу ViPNet Coordinator IG, а дистрибутив ключей записать в папку на этом компьютере.

Подключение через консоль

Для этого способа вам понадобятся:

- Для промышленных исполнений:
 - консоль — компьютер с Windows или Linux любых версий;
 - консольный кабель RS-232 с разъёмами DB9 и RJ45 (например, Cisco CAB-CONSOLE-RJ45);
 - переходник USB-DB9 — при отсутствии порта RS-232 на компьютере;
 - USB-носитель;
 - программа для терминального подключения (например, PuTTY, minicom, picocom).

- Для серверных исполнений:
 - один из вариантов консоли:
 - компьютер с Windows или Linux любых версий; консольный кабель RS-232 с разъёмами DB9 на обоих концах кабеля; переходник USB-DB9 — при отсутствии порта RS-232 на компьютере;
 - монитор (VGA) и клавиатура (USB).
 - USB-носитель;
 - программа для терминального подключения (например, PuTTY, minicom, picocom).

Подготовьте дистрибутив ключей

- 1 Отформатируйте USB-носитель в одну из файловых систем: FAT32, ext2, ext3 или ext4.
- 2 Перенесите на USB-носитель дистрибутив ключей (файл *.ds5).

Подключитесь к ViPNet Coordinator IG

- 1 Подключите консоль одним из способов:
 - Подключите компьютер к консольному порту ViPNet Coordinator IG с помощью консольного кабеля.
 - Подключите монитор и клавиатуру к портам **VGA** и **USB** соответственно — доступно только для ViPNet Coordinator IG1000 Q1.
- 2 Если вы подключились к консольному порту, запустите на компьютере программу для терминального подключения и задайте в ней параметры (приведены настройки PuTTY):
 - Тип терминала — VT100 (**Terminal > Keyboard > VT100+**).
 - Кодировка символов — KOI8-R (**Window > Translation**, в списке **Remote character set** выберите **KOI8-R**).
 - Параметры подключения через последовательный порт (**Connection > Serial**):
 - Скорость обмена данными:

Для аппаратной платформы IG100 I4 — 115200 (в поле **Speed** введите **115200**).

Для других платформ — 38400 (в поле **Speed** введите **38400**).
 - Размер данных — 8 (в поле **Data bits** введите **8**).
 - Стоповые биты — 1 (в поле **Stop bits** введите **1**).
 - Чётность — None (в поле **Parity** выберите **None**).
 - Контроль потока — None (в поле **Flow control** выберите **None**).
- 3 Включите ViPNet Coordinator IG (см. [Включение ViPNet Coordinator IG](#)).

Подключение через канал Ethernet

Для этого способа вам понадобятся:

- Компьютер с сетевой картой Ethernet и Windows или Linux любых версий.
- Сетевой кабель RJ45 Cat. 5 для подключения компьютера к ViPNet Coordinator IG.
- Программа для подключения к ViPNet Coordinator IG (Telnet- или SSH-клиент).

Подготовьте компьютер и дистрибутив ключей

- 1 Перенесите на компьютер дистрибутив ключей (файл *.ds5).
- 2 На компьютере с Windows включите службы TFTP и SSH (или Telnet):
 - 2.1 В меню **Пуск** начните вводить «компоненты» и выберите **Включение или отключение компонентов Windows (Turn Windows features on or off)**.
 - 2.2 Выберите **Клиент TFTP (TFTP Client)** и **Простые службы TCPIP (Simple TCPIP services)**.
 - 2.3 Нажмите **ОК**.
- 3 На время установки дистрибутива ключей:
 - 3.1 Отключите компьютер от внешней сети.
 - 3.2 Если на компьютере установлен ViPNet Client, отключите защиту ViPNet. Для этого в основном меню ViPNet Client выберите **Файл > Конфигурации > Отключить защиту**.
 - 3.3 На компьютере с Windows отключите службы безопасности и обновления:
 - Брандмауэр Windows (Windows Firewall);
 - Защитник Windows (Windows Defender);
 - Центр обновления Windows (Windows Update).
 - 3.4 На компьютере с Windows в меню **Пуск** начните вводить «свойства» и выберите **Свойства браузера (Manage browser add-ons) > Безопасность (Security) > Интернет (Internet) > Другой (Custom level)**. Измените уровень для сброса особых параметров на **Средний**. Нажмите **Сбросить**, затем нажмите **Применить** и **ОК**.

Подключитесь к ViPNet Coordinator IG

- 1 Подключите компьютер с помощью сетевого кабеля:
 - к порту **LAN 1** — для всех промышленных исполнений ViPNet Coordinator IG, кроме ViPNet Coordinator IG100 I4;
 - к порту **LAN 3** — для ViPNet Coordinator IG100 I4;
 - к порту с сетевым интерфейсом **eth1** — для ViPNet Coordinator IG1000 Q1 (соответствие физических портов и сетевых интерфейсов см. в документе «Описание аппаратных платформ», раздел «IG1000 Q1»).
- 2 Установите на сетевом интерфейсе компьютера IP-адрес 169.254.241.5.

- 3 Подключитесь к ViPNet Coordinator IG с помощью Telnet- или SSH-клиента по IP-адресу 169.254.241.1. В параметрах подключения укажите (приведены настройки PuTTY):
 - Тип терминала VT100 (**Terminal > Keyboard > VT100+**).
 - Кодировка символов KOI8-R (**Window > Translation**, в списке **Remote character set** выберите **KOI8-R**).
 - Метод ввода linux (**Connection > Data > Terminal type string**, введите **linux**).
 - Ширина окна по умолчанию 120 символов (**Windows > Columns**, введите **120**).
- 4 Включите ViPNet Coordinator IG (см. [Включение ViPNet Coordinator IG](#)).

Включение ViPNet Coordinator IG



Внимание! Перед включением ViPNet Coordinator IG ознакомьтесь с разделами «Требования к подключению внешних устройств» и «Меры безопасности» документа «Описание аппаратных платформ».

Промышленные исполнения

Промышленные исполнения ViPNet Coordinator IG включаются автоматически после подачи электропитания одним из способов:

- от блока питания;
- от коммутатора по технологии PoE — только для исполнения ViPNet Coordinator IG100 I5.

При использовании обоих способов одновременно ViPNet Coordinator IG будет работать от блока питания, а питание от коммутатора будет резервным.

Перед включением промышленного исполнения ViPNet Coordinator IG:

- 1 Заземлите корпус аппаратной платформы, закрепив кабель заземления с помощью болта или винта на нижней панели.
- 2 Убедитесь, что источник питания отвечает следующим требованиям:
 - Блок питания обеспечивает постоянный ток с напряжением от 12 до 24 В $\pm 10\%$.
Если вы планируете подавать питание с ViPNet Coordinator IG на внешние устройства по технологии PoE, блок питания должен обеспечивать напряжение 24 В $\pm 10\%$.
 - Коммутатор с PoE выделяет мощность по Ethernet-каналу не менее 30 Вт.

Чтобы включить ViPNet Coordinator IG, выполните одно из действий в зависимости от способа подачи питания:

- Подключите к разъёму питания ViPNet Coordinator IG кабель питания, соблюдая полярность. Индикатор **PWR** на передней панели загорится зелёным.
- Подключите к порту **WAN** Ethernet-кабель от коммутатора, подающего питание по технологии PoE. Индикатор **PWR** на передней панели загорится зелёным. Спустя некоторое время, когда загрузится служба питания по PoE, индикатор **PD** также загорится зелёным.



Примечание. Спецификацию портов питания, а также описание световой индикации состояний ViPNet Coordinator IG в процессе загрузки см. в документе «Описание аппаратных платформ».

Серверные исполнения

Чтобы включить ViPNet Coordinator IG серверного исполнения:

- 1 Подключите кабель питания к блоку питания. При подключении обоих блоков питания, один из них будет работать как основной, второй — как резервный.
- 2 Нажмите кнопку питания на передней панели ViPNet Coordinator IG.



Примечание. Если в предыдущий раз кабель питания был отключён, когда ViPNet Coordinator IG находился во включённом состоянии, то ViPNet Coordinator IG включится автоматически при подключении питания.

Инициализация

При инициализации ViPNet Coordinator IG устанавливается дистрибутив ключей, а также выполняется базовая настройка для работы в сети ViPNet.

Начало инициализации

1 В строке приглашения введите:

- имя пользователя — `user`;
- пароль — `user`.



Примечание. Пароль `user` используется только при инициализации — когда на ViPNet Coordinator IG не установлен дистрибутив ключей.

При вводе пароля на экране не отображаются вводимые символы, а курсор остается неподвижным.

Мастер в консоли будет выводить текстовые сообщения, на которые вам потребуется вводить `y` (да), `n` (нет) или нужные значения. После ввода ответа нажимайте **Enter**.

2 Примите условия лицензионного соглашения — введите `y`.

Если текст отображается неправильно, в настройках консоли или Telnet-, SSH-клиента выбрана неверная кодировка. Чтобы просмотреть лицензионное соглашение, введите `n` (ViPNet Coordinator IG будет перезагружен) и повторно подключитесь, выбрав кодировку KOI8-R.

3 В строке `Would you like to start installing keys/restoring configuration` введите `y`.

4 Последовательно выберите континент, страну и часовой пояс.

Для этого вводите номер из списка.

5 Подтвердите установку часового пояса — в строке `Is the above information OK` введите `1`.

6 Если требуется изменить дату и время, введите их в формате `YYYY-MM-DD hh:mm:ss`. Иначе нажимайте **Enter**.



Внимание! Если системные дата и время заданы неверно, защищённые соединения с другими узлами ViPNet могут блокироваться.

7 Мастер перейдет к [Установке дистрибутива ключей](#).

Установка дистрибутива ключей

1 Выберите способ установки дистрибутива ключей:

В строке `Would you like to install appliance initialization file from TFTP, USB storage device` введите:

- `t` — для установки с компьютера по протоколу TFTP;
- `u` — для установки с USB-носителя.



Внимание! Не отключайте питание ViPNet Coordinator IG до завершения установки дистрибутива ключей. Иначе это может привести к неработоспособности ViPNet Coordinator IG.

2 Если вы выбрали установку по протоколу TFTP, запустите командную строку на компьютере (cmd.exe в Windows) и выполните команду:

```
tftp -i 169.254.241.1 put <имя файла *.ds5>
```

Затем в Telnet- или SSH-клиенте нажмите **Enter** (см. [Подключение через канал Ethernet](#)).

3 Если вы выбрали установку с USB-носителя, подключите его к ViPNet Coordinator IG и нажмите **Enter**.

- Если на носителе только один файл `*.ds5`, он будет выбран для установки автоматически.
- Если файлов несколько, выберите нужный из списка `Found several appliance initialization files`.
Если файлов больше 20, список выводится постранично.
- Если файлов `*.ds5` не обнаружено, мастер предложит заново выбрать способ установки.

4 В строке `Enter password` введите пароль к дистрибутиву ключей, который вы получили от администратора защищённой сети.

При вводе пароля на экране не отображаются вводимые символы, а курсор остаётся неподвижным.

Расшифрование дистрибутива ключей может занять несколько минут.

5 После строки `Select the setup method` выберите ручной способ настройки — введите `1`.



Примечание. Вы можете импортировать настройки из файла индивидуальной или универсальной конфигурации. Подробнее см. документ «Настройка с помощью командного интерпретатора», разделы «Управление индивидуальной конфигурацией» и «Управление универсальной конфигурацией».

6 В строке `Enter new admin password` задайте пароль для локальной учётной записи администратора `admin` на ViPNet Coordinator IG.

В строке `Confirm new admin password` введите пароль ещё раз.

- 7 Если дистрибутив ключей содержит информацию о том, что используется способ аутентификации по сертификату, мастер перейдёт к шагу 7.1. Если используется способ аутентификации по паролю, мастер перейдёт к [настройке сети](#).
- 7.1 При появлении сообщения `Insert token and press Enter` подключите USB-токен, на который будет записан сертификат администратора для аутентификации на ViPNet Coordinator IG под локальной учётной записью `admin`.
- 7.2 В строке `Do you want to initialize token? [Yes/No]` введите `y` — для инициализации USB-токена и записи сертификата.



Внимание! В ходе инициализации USB-токена все данные на нём будут удалены.

- 7.3 В строке `Enter admin-token pincode` введите PIN-код администратора USB-токена (см. документацию на USB-токен).
-



Внимание! Если вы введёте некорректный PIN-код администратора USB-токена несколько раз подряд, он будет заблокирован (максимальное количество попыток ввода см. в документации на USB-токен). После этого вы больше не сможете записать сертификат на этот USB-токен.

- 7.4 В строке `Enter new user-token pincode` задайте PIN-код пользователя USB-токена и подтвердите его. Этот PIN-код будет использоваться при аутентификации администратора на ViPNet Coordinator IG.
- 8 Мастер перейдет к [настройке сети](#).

Настройка сети

- 1 Последовательно настройте сетевые интерфейсы, начиная с `eth0`:

Для этого в строке `Configure interface eth<номер>` введите:

- `y` — включить и настроить интерфейс;
- `n` — пропустить интерфейс и перейти к следующему.

Когда интерфейсы закончатся, мастер перейдет к настройке DNS-сервера.

- 1.1 В строке `Use dhcp on the interface eth<номер>` введите:

- `y` — установить для интерфейса режим DHCP;
- `n` — установить режим статической адресации.

- 1.1 Если выбран режим статической адресации, задайте IP-адрес для интерфейса. В следующей строке задайте маску интерфейса.

Внимание! При задании IP-адреса нельзя использовать:



- IP-адрес — 0.0.0.0.
 - Маски подсети — 0.0.0.0, 255.255.255.254 и 255.255.255.255.
 - IP-адреса одной подсети для разных сетевых интерфейсов.
-

- 2 Если ни для одного интерфейса не был задан режим DHCP, в строке `Enter ip-address of the default gateway` задайте IP-адрес шлюза по умолчанию.
- 3 В строке `Do you want to enable DNS server` задайте начальное состояние DNS-сервера при загрузке ViPNet Coordinator IG:
 - `y` — включать DNS-сервер при загрузке;
 - `n` — не включать DNS-сервер при загрузке.
- 4 Если вы включили автозапуск DNS-сервера, в строке `Do you want to add custom DNS server` введите:
 - `n` — использовать корневые DNS-серверы;
 - `y` — добавить DNS-сервер. Затем укажите его IP-адрес.
- 5 В строке `Do you want to enable NTP server` задайте начальное состояние NTP-сервера при загрузке ViPNet Coordinator IG:
 - `y` — включать NTP-сервер при загрузке;
 - `n` — не включать NTP-сервер при загрузке.
- 6 Если вы включили автозапуск NTP-сервера, в строке `Do you want to add custom NTP server` введите:
 - `n` — синхронизировать системное время с публичными NTP-серверами;
 - `y` — добавить NTP-сервер. Затем укажите IP-адрес или доменное имя NTP-сервера.
- 7 По умолчанию для ViPNet Coordinator IG назначается сетевое имя вида: `<исполнение ViPNet Coordinator IG>-<идентификатор узла>`, например, `ig100-5b980005`.
Чтобы оставить предложенное имя, нажмите **Enter**, или введите другое имя.
- 8 По умолчанию ViPNet Coordinator IG назначает **виртуальные IP-адреса** из диапазонов:
 - 11.0.0.1–11.255.255.254 (CIDR 11.0.0.1/8) — для узлов ViPNet и одиночных туннелируемых узлов;
 - 12.0.0.1–12.255.255.254 — для диапазонов туннелируемых узлов.

Если диапазон IP-адресов в вашей сети пересекается хотя бы с одним из этих диапазонов, измените диапазон виртуальных IP-адресов:

- Чтобы изменить диапазон виртуальных IP-адресов, в строке `Do you want to specify custom virtual IP address range` введите `y`. Затем укажите начальный и конечный IP-адреса нового диапазона, например, `13.0.0.1-13.0.254.254` или `11.0.0.1/16`. Этот диапазон будет использоваться для узлов ViPNet и одиночных туннелируемых узлов. Для диапазонов туннелируемых узлов будет использоваться диапазон виртуальных IP-адресов:

<x+1>.0.0.1-<x+1>.255.255.254, где x — первый октет заданного диапазона виртуальных IP-адресов.

- Чтобы оставить диапазон виртуальных IP-адресов без изменений, введите n.

Подробнее о виртуальных IP-адресах см. документ «Настройка с помощью командного интерпретатора», разделы «Настройка виртуальных IP-адресов» и «Настройка видимости узлов».

- 9 Мастер перейдет к [настройке проверки связи с узлом ViPNet](#).

Настройка проверки связи с узлом ViPNet



Внимание! Если вы подключились к ViPNet Coordinator IG с помощью Telnet- или SSH-клиента, откажитесь от проверки связи с узлом сети ViPNet. В момент проверки связи к сетевым интерфейсам будут применены настройки, заданные на предыдущем этапе, и соединение по технологическому адресу будет прервано.

- 1 Если был настроен хотя бы один сетевой интерфейс, вы можете проверить связь ViPNet Coordinator IG с любым узлом сети ViPNet, с которым у ViPNet Coordinator IG заданы связи в справочниках дистрибутива ключей. Для этого в строке `Do you want to probe VPN-connection with some host in order to verify the configuration you've just made` введите y.

Чтобы отказаться от проверки, введите n. Мастер перейдет к [запуску драйверов и служб](#).

- 2 Перед проверкой связи необходимо задать режим подключения ViPNet Coordinator IG к внешней сети. Для этого в строке `Do you want to configure firewall mode` введите:
- n — для использования настроек режима подключения из дистрибутива ключей. Мастер перейдет к [выбору узла для проверки связи](#);
 - y — для задания режима подключения вручную.

- 3 Во втором случае выберите режим:

- 1 — **Со статической трансляцией адресов** — если ViPNet Coordinator IG доступен из внешней сети (имеет публичный IP-адрес или доступен через устройство со статическим NAT).
- 2 — **С динамической трансляцией адресов** — если ViPNet Coordinator IG доступен из внешней сети с использованием [сервера соединений](#).

Подробнее см. в документе «Настройка с помощью командного интерпретатора», раздел «Настройка подключения к внешней сети».

- 4 Если вы выбрали режим **Со статической трансляцией адресов**, вы можете изменить порт для отправки и получения UDP-пакетов. В строке `Do you want to specify custom UDP port` введите:
- n — оставить порт по умолчанию 55777.
 - y — задать номер порта.



Примечание. Если через одно устройство с NAT к внешней сети подключены несколько координаторов, у них должны быть разные UDP-порты.

Мастер перейдет к [выбору узла для проверки связи](#).

5 Если вы выбрали режим [С динамической трансляцией адресов](#):

5.1 В строке `Specify the sequence number of the VPN Coordinator` введите номер координатора, через который ViPNet Coordinator IG будет подключаться к сети.

В списке выводятся только те координаторы, с которыми у ViPNet Coordinator IG заданы связи в справочниках установленного дистрибутива ключей.



Примечание. Если в дистрибутиве ключей нет связей с другими координаторами, появится сообщение `Your VPN host has no links with VPN coordinators`. В этом случае вы можете отменить настройку режима подключения или настроить другой режим.

5.2 Если для выбранного координатора не указан IP-адрес, появится сообщение `The IP address of the VPN Coordinator has not been found. Do you want to specify one?` В этом случае введите `y` и задайте его вручную.

6 Мастер перейдет к [выбору узла для проверки связи](#).

Выбор узла для проверки связи

1 В строке `Specify the sequence number of the VPN host` введите номер узла из списка для проверки связи.



Примечание. В списке выводятся узлы ViPNet, с которыми заданы связи для ViPNet Coordinator IG. Информация о связях содержится в дистрибутиве ключей.

2 Если в справочниках установленного дистрибутива ключей не указан IP-адрес выбранного узла, появится сообщение `The IP address of the VPN host has not been found. Do you want to specify one?`. В этом случае введите `y` и задайте его вручную.

3 Нажмите **Enter** для сохранения настроек подключения к сети и начала проверки. Проверка связи с узлом может занять несколько минут. Дождитесь сообщения о результатах проверки.

4 Если проверка завершилась успешно, мастер перейдет к [запуску драйверов и служб](#).

5 Если связь с узлом установить не удалось, то для выяснения причины вы можете просмотреть журнал IP-пакетов. Для этого в строке `Do you want to view IP packet log in order to investigate the issue` введите `y`.

Подробнее о работе с журналом IP-пакетов см. в документе «Настройка с помощью командного интерпретатора», в разделе «Журнал IP-пакетов».

6 Для выполнения повторной проверки связи с узлом после просмотра журнала нажмите **Enter**.



Примечание. Если необходимо прекратить инициализацию, нажмите **Ctrl+C**.

Запуск драйверов и служб

1 Запустите драйверы и службы ViPNet Coordinator IG:

В строке `Do you want to start VPN services before leaving the installation wizard` введите **Y**.

Инициализация завершена.

- Если вы подключены к ViPNet Coordinator IG с помощью Telnet- или SSH-клиента по технологическому адресу, то текущее соединение будет завершено после нажатия на любую клавишу.

Для дальнейшей настройки подключитесь к ViPNet Coordinator IG локально через консоль. Доступ по SSH и HTTP/HTTPS после инициализации запрещён.

- Если вы подключены к ViPNet Coordinator IG через консоль, дождитесь сообщений:

```
ViPNet Coordinator IG successfully deployed!
```

```
Press Enter to proceed to authentication form.
```

После чего нажмите **Enter** для запуска командного интерпретатора.

2 Отсоедините USB-носитель.

3 Для завершения настройки системных служб необходимо перезагрузить ViPNet Coordinator IG:

3.1 Войдите под локальной учётной записью администратора:

- имя пользователя — `admin`;
- для аутентификации по паролю — введите пароль администратора, который вы задали в ходе инициализации ViPNet Coordinator IG;
- для аутентификации по сертификату — подключите USB-токен и введите PIN-код.

3.2 Войдите в режим настройки:

```
hostname> enable
```

3.3 Выполните команду перезагрузки:

```
hostname# machine reboot
```

4 Для завершения ввода в эксплуатацию ViPNet Coordinator IG выполните действия из раздела [Настройка после инициализации](#).

Настройка после инициализации

Настройка подключения к ViPNet Prime

1 Войдите под локальной учётной записью администратора:

- имя пользователя — `admin`;
- для аутентификации по паролю — введите пароль администратора;
- для аутентификации по сертификату — подключите USB-токен и введите PIN-код.

2 Перейдите в режим настройки:

```
hostname> enable
```

3 Определите IP-адрес доступа к ViPNet Prime. Для этого откройте конфигурационный файл `iplir.conf`:

```
hostname# iplir show config
```

IP-адрес доступа указан в секции `[id]` узла `Control Center` в параметре `accessip`.

Например:

```
[id]
id=0x2c670002
name= Control Center
accessip= 11.0.0.2
```

Чтобы закрыть файл, нажмите клавишу **Q**.

4 Добавьте в файл `hosts` запись о соответствии IP-адреса и доменного имени ViPNet Prime:

```
hostname# machine hosts add <IP-адрес доступа к ViPNet Prime> <доменное имя ViPNet Prime>
```

Например: `machine hosts add 11.0.0.2 prime.company`



Примечание. Файл `hosts` не синхронизируется между узлами кластера. Если вы инициализируете ViPNet Coordinator IG в составе кластера, внесите изменения в файл `hosts` на обоих узлах кластера.

5 Проверьте маршрут по умолчанию в таблице маршрутизации:

```
hostname# inet show routing
```

Если маршрут по умолчанию отсутствует, задайте статический маршрут по умолчанию (см. документ «Настройка с помощью командного интерпретатора», раздел «Настройка маршрутизации»). Убедитесь, что заданный в маршруте шлюз по умолчанию доступен для ViPNet Coordinator IG.

Настройка удалённого доступа

По умолчанию удалённый доступ к ViPNet Coordinator IG заблокирован.

- Чтобы управлять ViPNet Coordinator IG с помощью веб-интерфейса, создайте разрешающий фильтр защищённой сети:

```
hostname# firewall vpn add rule "Allow ViPNet WebGUI" src <идентификатор узла | группа узлов> dst @local tcp dport 8080 pass
```

- Чтобы подключаться к ViPNet Coordinator IG по SSH, создайте разрешающий фильтр защищённой сети:

```
hostname# firewall vpn add rule "Allow SSH Server" src <идентификатор узла | группа узлов> dst @local service @ssh pass
```

В качестве параметра `<идентификатор узла>` укажите идентификатор узла в защищённой сети, с которого вы хотите подключиться. Подключайтесь к ViPNet Coordinator IG только с узлов защищённой сети.

ViPNet Coordinator IG готов к эксплуатации. Для настройки и управления вы можете использовать командный интерпретатор и веб-интерфейс. Подробнее см. документы «Настройка с помощью командного интерпретатора» и «Настройка с помощью веб-интерфейса». Веб-интерфейс доступен во всех исполнениях ViPNet Coordinator IG100 и ViPNet Coordinator IG1000.



Примечание. Если вы предполагаете использовать локальную учётную запись `user` для аудита ViPNet Coordinator IG, разблокируйте её. Подробнее см. документ «Настройка с помощью командного интерпретатора», раздел «Управление локальными учётными записями».

Перезагрузка и выключение ViPNet Coordinator IG



Внимание! Перед тем как перезагрузить или выключить ViPNet Coordinator IG, убедитесь, что выключение ViPNet Coordinator IG не повлечёт за собой нарушение работы связанных компьютеров и устройств.

Перезагрузка

Таблица 11. Способы перезагрузки ViPNet Coordinator IG

Исполнение	Командный интерпретатор	Веб-интерфейс	Кнопка Reset
ViPNet Coordinator IG10 I1	+	-	+
ViPNet Coordinator IG10 I2	+	-	+
ViPNet Coordinator IG100 I1	+	+	+
ViPNet Coordinator IG100 I4	+	+	+
ViPNet Coordinator IG100 I5	+	+	+
ViPNet Coordinator IG1000 Q1	+	+	-

Чтобы перезагрузить ViPNet Coordinator IG:

- через командный интерпретатор — выполните команду:
`hostname# machine reboot`
- через веб-интерфейс — см. документ «Настройка с помощью веб-интерфейса», раздел «Перезагрузка ViPNet Coordinator IG»;
- кнопкой **Reset** на корпусе ViPNet Coordinator IG — нажмите и удерживайте её нажатой несколько секунд, пока индикаторы на ViPNet Coordinator IG не начнут мигать жёлтым.

Выключение

Таблица 12. Способы выключения ViPNet Coordinator IG

Исполнение	Отключение от источника питания	Кнопка Power	Кнопка Reset	Командный интерпретатор
ViPNet Coordinator IG10 I1	+	-	-	-
ViPNet Coordinator IG10 I2	+	-	+	-
ViPNet Coordinator IG100 I1	+	-	-	-

Исполнение	Отключение от источника питания	Кнопка Power	Кнопка Reset	Командный интерпретатор
ViPNet Coordinator IG100 I4	+	+	-	-
ViPNet Coordinator IG100 I5	+	-	-	-
ViPNet Coordinator IG1000 Q1	Не рекомендуется	+	-	+

Выключение промышленных исполнений ViPNet Coordinator IG:

- кнопкой **Power** — нажмите и удерживайте её нажатой более 4-х секунд пока не погаснут индикаторы;
- кнопкой **Reset** — нажмите и удерживайте её нажатой около 20–30 секунд пока не погаснут индикаторы.



Внимание! Кнопка **Reset** также используется для удаления ПО ViPNet Coordinator IG (см. документ «Настройка с помощью командного интерпретатора», раздел «Восстановление ПО»). Чтобы случайно не запустить процедуру удаления ПО, не отпускайте и не нажимайте повторно кнопку **Reset**, если индикаторы горят красным или мигают красным. В этом случае дождитесь, когда индикаторы снова будут мигать жёлтым, и отпускайте кнопку, — запустится перезагрузка.

Выключение серверных исполнений ViPNet Coordinator IG:

- через командный интерпретатор — выполните команду:

```
hostname# machine halt
```
- кнопкой **Power** — нажмите её. Чтобы выключить ViPNet Coordinator IG, не дожидаясь завершения работы служб, нажмите кнопку и удерживайте её нажатой несколько секунд.

После выключения ViPNet Coordinator IG с помощью кнопки, вы сможете включить его, нажав на ту же кнопку при подключённом источнике питания:

- для включения ViPNet Coordinator IG1000 Q1 нажмите кнопку **Power**.
- для включения ViPNet Coordinator IG100 I4 нажмите и удерживайте кнопку **Power** до 4-х секунд;
- для включения ViPNet Coordinator IG10 I2 нажмите кнопку **Reset**.

Описание световой индикации состояний ViPNet Coordinator IG в процессе загрузки см. в документе «Описание аппаратных платформ».



Термины и сокращения

TCP-туннель

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

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

ViPNet Client

Программное обеспечение, которое выполняет функции VPN-клиента в сети ViPNet и обеспечивает защиту компьютера от несанкционированного доступа при работе в локальных или глобальных сетях.

ViPNet Prime

ПО для централизованного управления решениями ViPNet. Позволяет управлять конфигурацией сети (включая устройства, пользователей и лицензии), централизованно обновлять ПО ViPNet и выполнять мониторинг состояния сети ViPNet.

Включает в себя основные функциональные модули:

- ViPNet VPN — модуль управления топологией сети, регистрирует защищаемые устройства и задает связи между ними.
- ViPNet Network Visibility System — модуль мониторинга состояния сети ViPNet и входящих в нее устройств.
- ViPNet Policy Management — модуль централизованного управления политиками безопасности узлов сети 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.

Виртуальный IP-адрес

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

Дистрибутив ключей

Набор, содержащий:

- [ключи обмена](#);
- [ключ защиты обновлений](#);
- справочники с информацией об узлах защищенной сети;
- лицензия.

Формируется в ViPNet Prime на основе заданных связей между узлами. Необходим для инициализации и работы ViPNet Coordinator IG.

Для узлов защищенной сети поколения 5 используется дистрибутив ключей `ds5`, для узлов поколения 4 — `dst`.

Защищенный узел

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

Клиент (ViPNet-клиент)

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

Ключи защиты обновлений

Ключи защиты обновлений обеспечивают безопасное удаленное обновление ключей обмена из ключевого центра ViPNet Prime и их хранение в ViPNet Coordinator IG.

Ключи обмена

На ключах обмена защищается канал передачи данных между двумя связанными узлами сети ViPNet.

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.

Открытый узел

Узел без ПО ViPNet с функцией шифрования трафика на сетевом уровне, расположенный в сети «за координатором».

Политики безопасности

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

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 функцию сервера соединений выполняет координатор, назначенный сервером IP-адресов.

Сетевой узел ViPNet

Сетевой узел с ПО ViPNet, зарегистрированный в ViPNet Prime VPN.

Сеть ViPNet

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

Транспортный конверт

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

Транспортный сервер MFTP

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

Туннелирование

Технология для защиты соединений между устройствами локальных сетей, которые связаны через интернет или другие публичные сети. Шифрование трафика устройств выполняется координаторами, установленными на границах локальных сетей.

Шлюз Modbus

Программно-аппаратная функциональность, выполняющая преобразование трафика интерфейса Ethernet в интерфейсы RS-232 и RS-485 и обратно для обеспечения взаимодействия Ethernet- и Modbus-устройств.

Шлюзовой координатор

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