



ViPNet Prime

Руководство по установке

Версия продукта: 1.9.14

© АО «ИнфоТеКС», 2026

ФРКЕ.00222-02 32 03

Версия продукта: 1.9.14

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 Prime приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet Prime.

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.....	6
О документе.....	7
Соглашения документа.....	7
Комплект поставки.....	8
Системные требования.....	10
Системные требования к компьютеру с ViPNet Prime.....	10
Требования к компьютеру администратора.....	12
Системные требования для коннектора Active Directory.....	13
Требования к эксплуатации.....	13
Требования к безопасности.....	14
Требования к ПО ViPNet.....	14
Обратная связь.....	15
 Глава 1. Общие сведения.....	16
Схемы размещения модулей.....	17
Каналы передачи данных.....	20
Принцип работы ViPNet UT.....	20
 Глава 2. Предварительные действия.....	21
Общий порядок установки.....	22
Подготовка ОС.....	25
Выбор источника случайных чисел.....	28
Настройка DNS.....	29
Настройка DNS-сервера на примере Bind9.....	31
 Глава 3. Подготовка TLS-сертификатов сервера.....	33
О сертификате сервера.....	34
Требования к сертификату сервера.....	35
Конвертация сертификата сервера в формат PEM.....	37
Построение цепочки доверия сертификата сервера.....	38
Использование сертификата НУЦ Минцифры России.....	39
Издание самоподписанного сертификата сервера.....	40
Создание запроса на сертификат сервера ГОСТ.....	42
Обновление сертификата сервера.....	44
Обновление сертификатов сервера с помощью скрипта.....	44

Обновление сертификатов сервера ViPNet Prime NVS	45
Часто задаваемые вопросы	47
Глава 4. Установка ViPNet Prime	48
Установка базовых компонентов	49
Установка ViPNet Prime PMM	55
Установка ViPNet Prime NVS	58
Настройка окружения	59
Установка ViPNet Prime NVS Сборщик данных	60
Установка ViPNet Connect Book	61
Обновление ViPNet Prime	63
Глава 5. Администрирование и настройка	68
Установка, обновление и настройка коннектора Active Directory	69
Импорт учетных записей из одного домена Active Directory на несколько серверов с ViPNet Prime	74
Управление службами ViPNet Prime	78
Смена IP-адреса ViPNet Prime	81
Освобождение дискового пространства	84
Настройка журналов ViPNet Prime	85
Просмотр журналов ViPNet Prime	89
Пересечение подсетей Docker и LAN	92
Просмотр версии ViPNet Prime	94
Запрет входящих соединений к ViPNet Prime Key Center Nginx	95
Установка сертификатов TLS ГОСТ	97
Глава 6. Регламентные процедуры	98
Контроль целостности ViPNet Prime	99
Контроль целостности образов Docker-контейнеров и исполняемых файлов	101
Смена мастер-ПИН программного токена	102
Проверка ЭП файла обновления ПО ViPNet	103
Предварительные действия	103
Установка корневого сертификата и списка отозванных сертификатов	103
Проверка электронной подписи	105
Приложение А. Возможные неполадки	106
Недоступен веб-интерфейс	106
Не запускается ViPNet Prime	107
Ошибка при запуске модуля ViPNet Prime NVS	107

Недоступен веб-интерфейс по поддомену Active Directory Federation Services	107
При запуске ViPNet Prime не принимается мастер-ПИН.....	108
Недоступен веб-интерфейс модуля	108
Ошибка CSP correctness check failed	108
Пакет firewalld блокирует доступ к веб-интерфейсу.....	109
Ошибка при установке dpkg frontend lock	110
Установка сторонних пакетов нарушает зависимости	110
Дублирование окна ViPNet Prime VPN в веб-интерфейсе.....	110
Не приходит запрос на регистрацию модуля	110
Сбой времени при синхронизации с NTP-сервером	111
Ошибки после установки или обновления ViPNet Prime NVS	111
 Приложение В. Состав ViPNet Prime	 112
 Приложение С. Системные папки ViPNet Prime.....	 116
 Приложение D. Расчёт потребления ресурсов виртуальной машины	 118
 Приложение E. Сетевые соединения ViPNet Prime.....	 120
 Приложение F. Термины и сокращения	 123



Введение

О документе	7
Комплект поставки	8
Системные требования	10
Обратная связь	15

О документе

Документ предназначен для администратора, который устанавливает ViPNet Prime.

Предполагается, что читатель руководства обладает опытом администрирования Linux и имеет общее представление:

- о сетевых технологиях;
- принципах организации виртуальных частных сетей (VPN);
- об инфраструктуре открытых ключей (PKI);
- технологии контейнеризации Docker.

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



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

Обозначения при описании команд в документе:

- Команды, которые могут быть выполнены пользователем Unix-подобной операционной системы, содержат приглашение:
`$ команда`
- Команды, которые могут быть выполнены администратором Unix-подобной операционной системы, содержат приглашение:
`# команда`
- Параметры, которые должны быть заданы пользователем, заключены в угловые скобки:
`команда <параметр>`
- Необязательные параметры или ключевые слова заключены в квадратные скобки:
`команда <обязательный параметр> [необязательный параметр]`
- Допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой:
`команда {вариант-1 | вариант-2}`

Комплект поставки

Установочные файлы

- ViPNet Prime Management Services:
 - ViPNet Prime Core:
 - `extract-dist.sh`.
 - `core-ms.tgz`.
 - `prime-install.sh`.
 - ViPNet Prime VPN:
 - `extract-dist.sh`.
 - `vpn-ms.tgz`.
 - Транспортный сервер ViPNet Universal Transport (далее — ViPNet UT):
 - `extract-dist.sh`.
 - `transport.tgz`.
 - ViPNet Prime Network Visibility System (далее — ViPNet Prime NVS) — `nvs.tgz`.
 - ViPNet Prime NVS Сборщик данных (далее — Сборщик данных) — `nvs-rc.deb`.
 - ViPNet Prime Policy Management (далее — ViPNet Prime PMM) — `pmm.tgz`.
 - ViPNet Prime Connect Book (далее — ViPNet Connect Book):
 - `connect.tgz`.
 - `extract-dist.sh`.
- ViPNet Prime Key Center:
 - ViPNet Prime Core:
 - `extract-dist.sh`.
 - `core-kc.tgz`.
 - `install-certificates.sh`.
 - ViPNet Prime VPN:
 - `extract-dist.sh`.
 - `vpn-kc.tgz`.
- Конфигуратор:
 - `prime-deployment-configurator.tgz`.
 - `extract-dist.sh`.
 - `run.sh`.
- Файлы для проверки электронной подписи:

- корневой сертификат ключа проверки электронной подписи ИнфоТеКС в формате CER;
- список отозванных сертификатов в формате CRL.
- XML-файл для DPI — `ipoque_PACE2_dpuid.xml`.
- Утилита `Infotecs.ConfwizEnricher.exe` для адаптации правил из Check Point перед импортом в ViPNet Prime PMM.
- Скрипт для сбора диагностической информации ViPNet Prime — `diag<номер_версии>.sh`.
- Скрипт для сбора информации о текущем состоянии ViPNet Prime — `check<номер_версии>.sh`.

Полный состав комплекта см. в формуляре продукта.

Документация в формате PDF

- Руководство по установке.
- Руководство администратора.
- Лицензионные соглашения на компоненты сторонних производителей.
- Связанные документы модулей:
 - ViPNet Prime Policy Management. Руководство администратора.
 - ViPNet Prime Network Visibility System. Руководство администратора.
 - ViPNet Prime Network Visibility System. Параметры приложений.

Системные требования

Системные требования к компьютеру с ViPNet Prime

Системные требования приведены для гарантированной работы ViPNet Prime, без учёта дополнительного ПО, которое администратор может установить на компьютер. Перед установкой дополнительного ПО самостоятельно рассчитайте ресурсы для работы ViPNet Prime. В зависимости от количества модулей просуммируйте требования.

Установка стороннего ПО на компьютер с ViPNet Prime требует увеличения ресурсов компьютера. Если на компьютере с ViPNet Prime или на компьютере с ViPNet Prime NVS (если модуль расположен на отдельном компьютере) установлен Kaspersky Endpoint Security для Linux (далее — KESL):

- выделите для него дополнительные ресурсы компьютера — 8 Гбайт оперативной памяти, 8 ядер процессора;
- или установите ограничения ресурсов для конкретных задач KESL.

Общие системные требования

- Операционная система:
 - Операционная система специального назначения «Astra Linux Special Edition» (далее — Astra Linux SE) РУСБ.10015-01, очередное обновление 1.7 и 1.8. Гарантируется работа с версиями:
 - 1.7.5.9 (версии ядра Linux: 6.1.50-1-generic);
 - 1.8.3.8 (версии ядра Linux 6.1.141-1-generic и 6.12.34-1-generic).
 - 1.8.5.46 (версии ядра Linux 6.1.158-1-generic и 6.12.60-1-generic).



Внимание! При обновлении Astra Linux SE с версии 1.7 на 1.8 вы потеряете все пользовательские данные в системных папках. Это приведёт к тому, что ViPNet Prime будет удалён с компьютера и потребуются повторная установка ViPNet Prime. Подробнее см. на портале [справочного центра Astra Linux SE](#).

- Ubuntu 22.04.5 LTS (Desktop и Server, кроме Server (minimized)), (версии ядра Linux 5.15.0-generic и 6.8.0-generic).
- Ядро Linux версии generic. Работа с версиями hardened не поддерживается.
- Процессор с поддержкой AVX, выпущенный не ранее 2014 года, или процессоры уровня пятого поколения Intel и выше.
- Среда виртуализации:

- VMware ESXi 8.0.3.
- VMware Workstation Pro 16.x, 17.x.
- Proxmox 8.4, 9.
- ПК СВ «Брест» 3.3.3.
- zVirt Max 3.1.2.

Работа в других средах не гарантируется.

- Накопитель — SSD.

Таблица 1. Минимальные системные требования для установки ViPNet Prime Core, ViPNet Prime VPN и транспортного сервера ViPNet UT (базовая установка)

Процессор	8 ядер с тактовой частотой не ниже 3 ГГц
Оперативная память	16 Гбайт (рекомендуется от 32 Гбайт)
Свободное место на диске	500 Гбайт (рекомендуется 1 Тбайт)
Программное обеспечение	ViPNet Client 5 for Linux. Для передачи межсетевой информации по сети: • ViPNet Client 5 for Linux версии 5.0.0 или 5.1.3 и выше с лицензией Client for Linux (*.dst); • ViPNet Client 5 for Linux версии 5.1.3 и выше с лицензией Client for Linux v.5 (*.ds5)

Таблица 2. Минимальные системные требования для установки ViPNet Connect Book

Процессор	2 ядра
Оперативная память	2 Гбайт
Свободное место на диске	25 Гбайт

Таблица 3. Минимальные системные требования для установки ViPNet Prime PMM

Процессор	2 ядра
Оперативная память	5 Гбайт (при 20000 правил фильтрации и трансляции адресов увеличьте оперативную память на 1 Гбайт)
Свободное место на диске	30 Гбайт

Таблица 4. Минимальные системные требования для установки ViPNet Prime NVS

Процессор	8 ядер
Оперативная память	16 Гбайт
Свободное место на диске	55 Гбайт

Таблица 5. Минимальные системные требования для установки ViPNet Prime NVS Сборщик данных

Процессор	1 ядро
Оперативная память	400 Мбайт
Свободное место на диске	5 Гбайт
Программное обеспечение	ViPNet Client 5 for Linux версии 5.0.0 или выше

Установка на одном компьютере всех модулей

Ниже указаны системные требования для развёртывания защищённой сети, состоящей из 16 организаций по 650 узлов в каждой.

Таблица 6. Минимальные системные требования для установки ViPNet Prime (все модули)

Процессор	16 ядер
Оперативная память	32 Гбайт
Свободное место на диске	700 Гбайт (рекомендуется 2 Тбайт)
Тип накопителя	SSD
Программные требования	ViPNet Client 5 for Linux. Для передачи межсетевой информации по сети: • ViPNet Client 5 for Linux версии 5.0.0 или 5.1.3 и выше с лицензией Client for Linux (*.dst); • ViPNet Client 5 for Linux версии 5.1.3 и выше с лицензией Client for Linux v.5 (*.ds5)

Требования к компьютеру администратора

- Поддерживаемые браузеры:

- Google Chrome.
- Microsoft Edge.
- Mozilla Firefox.
- Яндекс Браузер.

Используйте только актуальные версии браузеров. В других браузерах работа не гарантирована.

- ViPNet PKI Client версии 1.6 и выше. Необходим для защиты канала управления при помощи двустороннего TLS по криптографическим алгоритмам ГОСТ.
- Минимальное разрешение экрана монитора: 1366 x 768.

- Синхронизируйте время между ViPNet Prime и компьютером администратора. Если время различается более чем на 1 минуту, вход в веб-интерфейс ViPNet Prime на компьютере администратора будет недоступен и отобразится сообщение *Время на сервере и устройстве отличаются. Установите одинаковое время.*

Это связано с тем, что сервер аутентификации генерирует токен доступа, проверяемый на компьютере администратора при входе в ViPNet Prime. Если время отличается более чем на 1 минуту на устройствах, то токен не проходит проверку. В качестве устройства или клиента аутентификации могут выступать компьютер администратора или координатор поколения ViPNet 5 с поддержкой перехода в веб-интерфейс координатора из ViPNet Prime.

Системные требования для коннектора Active Directory

- Операционная система — Windows Server 2016 или выше.
- [ASP.NET Core Runtime 3.1](#).
- Процессор — 64-разрядный с тактовой частотой 3 ГГц.
- Оперативная память — 8 Гбайт.
- Свободное место на жёстком диске — 32 Гбайт.

Требования к эксплуатации

- Для взаимодействия компьютера администратора с ViPNet Prime по HTTPS используйте [один TLS-сертификат, который подходит для всех доменных имён ViPNet Prime](#).
- Обеспечьте [доступ по доменному имени](#) к серверу ViPNet Prime.
- После установки и при обновлении ViPNet Prime не изменяйте порты и доменные имена модулей. Иначе вы не подключитесь к веб-интерфейсу ViPNet Prime.
- На границе сети разрешите внешние соединения WAN на портах по умолчанию:
 - Если администратору организации требуется подключаться из внешней сети к Prime, откройте порт TCP 443 для входящих соединений по HTTPS. В зависимости от конфигурации, откройте доступ к портам модулей ViPNet Prime.
 - Для работы транспортного сервера ViPNet UT откройте порты TCP 48080 и 48443 для входящих и исходящих соединений по HTTP и HTTPS соответственно.
 - Для связи ViPNet Prime NVS со сборщиками данных, расположенными за NAT-устройством в корпоративной сети организации или в WAN, откройте порт TCP 4222 для входящих и исходящих соединений.
- Закройте доступ к порту 5671 компьютера с ViPNet Prime.

- Отслеживайте свободное дисковое пространство. При увеличении нагрузки, например, при масштабировании сети, может потребоваться увеличить ресурсы компьютера с ViPNet Prime.

При удалённом обновлении ViPNet версии 5 на координаторах убедитесь, что на компьютере с ViPNet Prime есть свободное место для хранения обновлений. Например, для 100 координаторов с размером файла обновления 500 Мбайт потребуется 50 Гбайт свободного места.

- Регулярно создавайте резервные копии ViPNet Prime.

Рекомендуется создавать полную резервную копию один раз в неделю. Перед созданием резервной копии [остановите работу ViPNet Prime](#).



Совет. Вы можете хранить 1–2 последние полные резервные копии, если проверено восстановление из них.

Требования к безопасности

- Расположите рабочее место администратора в защищённом контуре.
- [Запретите все входящие соединения к HTTP-серверу ViPNet Prime KC Nginx, кроме необходимых для работы ViPNet Prime.](#)
- Для повышенной безопасности запретите интерфейсы удалённого управления (например, SSH, RDP) к компьютеру с ViPNet Prime.
- Для повышенной безопасности устанавливайте модуль ViPNet Prime NVS и сборщик данных на одном компьютере с другими модулями ViPNet Prime.

Требования к ПО ViPNet

Для установки ПО ViPNet на узлах, получите в ИнфоТеКСе файл лицензии *.itcslic. См. «ViPNet Prime. Руководство администратора» > «Управление лицензиями» и «ViPNet Prime. Руководство администратора» > «Совместимые продукты ViPNet».

В качестве координатора центра управления (Core Coordinator) выберите координатор с функцией регистрации клиентов, например:

- ViPNet Coordinator HW 4 исполнений VA, HW100 и выше.
- ViPNet Coordinator HW 5 исполнений VA, HW100 и выше с лицензией на VPN-функции.
- ViPNet Coordinator IG версии 4 или 5 исполнений IG100 и выше. Для повышения производительности Core Coordinator вместо ViPNet Coordinator IG100 используйте ViPNet Coordinator HW и уже за ним размещайте ViPNet Coordinator IG.
- ViPNet Coordinator KB 5 исполнений KB100 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.
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

Общие сведения

Схемы размещения модулей	17
Каналы передачи данных	20

Схемы размещения модулей

ViPNet Prime — веб-приложение. Его серверная часть состоит из двух частей:

- ViPNet Prime Management Services (далее — ViPNet Prime MS).
- ViPNet Prime Key Center (далее — ViPNet Prime KC).

Вы можете установить все модули ViPNet Prime на одном компьютере или модуль ViPNet Prime NVS на отдельном компьютере.

В базовую установку (обязательную) входят ViPNet Prime KC, MS (Core и VPN), транспортный сервер ViPNet UT. Остальные компоненты устанавливаются при необходимости.

Клиентская часть ViPNet Prime доступна на рабочем месте администратора через браузер.

Вы можете использовать ViPNet Prime:

- в сервисной модели предоставления услуг как платформу SaaS (software as a service) уровня поставщика услуг, где одна организация владеет и управляет инфраструктурой ViPNet Prime и предоставляет другим организациям шлюзы безопасности и управление сетью VPN как услугу;
- как платформу уровня предприятия, где одно предприятие владеет и управляет инфраструктурой ViPNet Prime.

Для использования базовых функций защищённой сети разверните два узла:

- Control Center — компьютер с ViPNet Prime и ViPNet Client 5 for Linux. Является центром управления сетью VPN.
- Core Coordinator — центральный координатор или координатор центра управления, за которым установлен ViPNet Prime. Является VPN-шлюзом.

Для компьютера с ViPNet Prime настройте DNS и правила межсетевого экрана в соответствии с конфигурацией вашей сети.

ViPNet Prime MS работает в контейнерах Docker. У каждого контейнера сетевой интерфейс с частной адресацией, которая не используется другими контейнерами или физическим компьютером. По умолчанию для работы стека контейнеров Docker выделяет свободную подсеть, начиная с подсети 172.18.0.0/16. При запуске или перезапуске стека контейнеров выделяется следующая, но не занятая другим стеком, подсеть, то есть 172.19.0.0/16, затем 172.20.0.0/16 и т.д. После подсети 172.31.0.0/16 Docker выделит в качестве следующей 192.168.0.0/20 подсеть. Если адрес подсети Docker пересекается с адресом подсети вашей локальной сети, смените сеть для Docker. Иначе это вызовет конфликт в сети.

ViPNet Prime KC работает как [службы](#) ОС.

Обратный прокси-сервер, встроенный в ViPNet Prime, перенаправляет сетевой трафик через ViPNet Prime Core KC Nginx к модулям. ViPNet Prime PMM и ViPNet Prime NVS обязательно должны иметь отдельный поддомен, так как назначить им другой порт невозможно. При установке модулей ViPNet Prime VPN и ViPNet Connect Book вы можете:

- Использовать разные поддомены для модулей. Например, ViPNet Prime имеет домен `example.ru`, модули могут иметь поддомены `vpn.example.ru` и `connectbook.example.ru`.
- Использовать разные порты. Например, ViPNet Prime имеет домен и порт `example.ru:443`, модули будут иметь домены и порты `example.ru:444` и `example.ru:445`.



Примечание. Использование поддоменов или разных портов для модулей не влияет на работу ViPNet Prime. Выбирайте любой удобный для вас способ.

Установка модулей на одном компьютере

В этой схеме установите все модули на одном компьютере. Рабочее место администратора и компьютер с ViPNet Prime подключите к локальной сети предприятия.

Администратор на рабочем месте использует:

- Браузер для подключения к ViPNet Prime с использованием TLS.
- ViPNet PKI Client для подключения к ViPNet Prime с использованием двустороннего TLS ГОСТ. Это опционально и настраивается:
 - при установке — добавляется сертификат сервера;
 - в веб-интерфейсе ViPNet Prime — добавляется личный сертификат администратора.

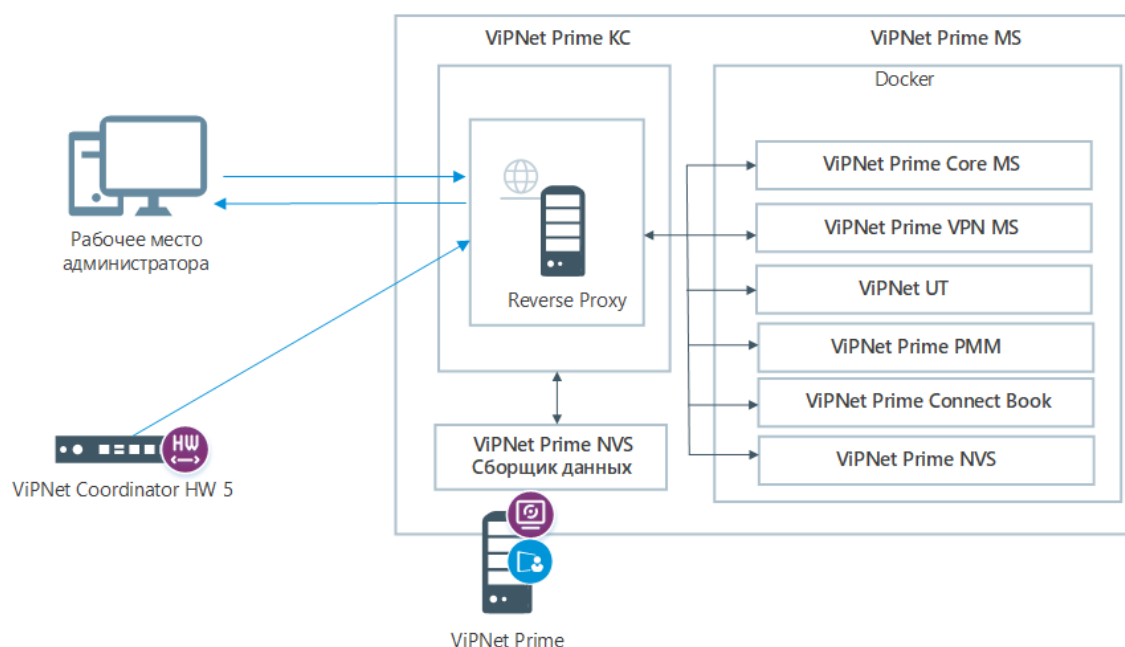


Рисунок 1. Размещение модулей на одном компьютере

Установка модулей на двух компьютерах (ViPNet Prime NVS отдельно)

Для обеспечения отказоустойчивости и снижения нагрузки на аппаратные ресурсы ViPNet Prime установите ViPNet Prime NVS на отдельном компьютере. ViPNet Prime NVS Сборщик данных установите на компьютере с остальными компонентами ViPNet Prime.

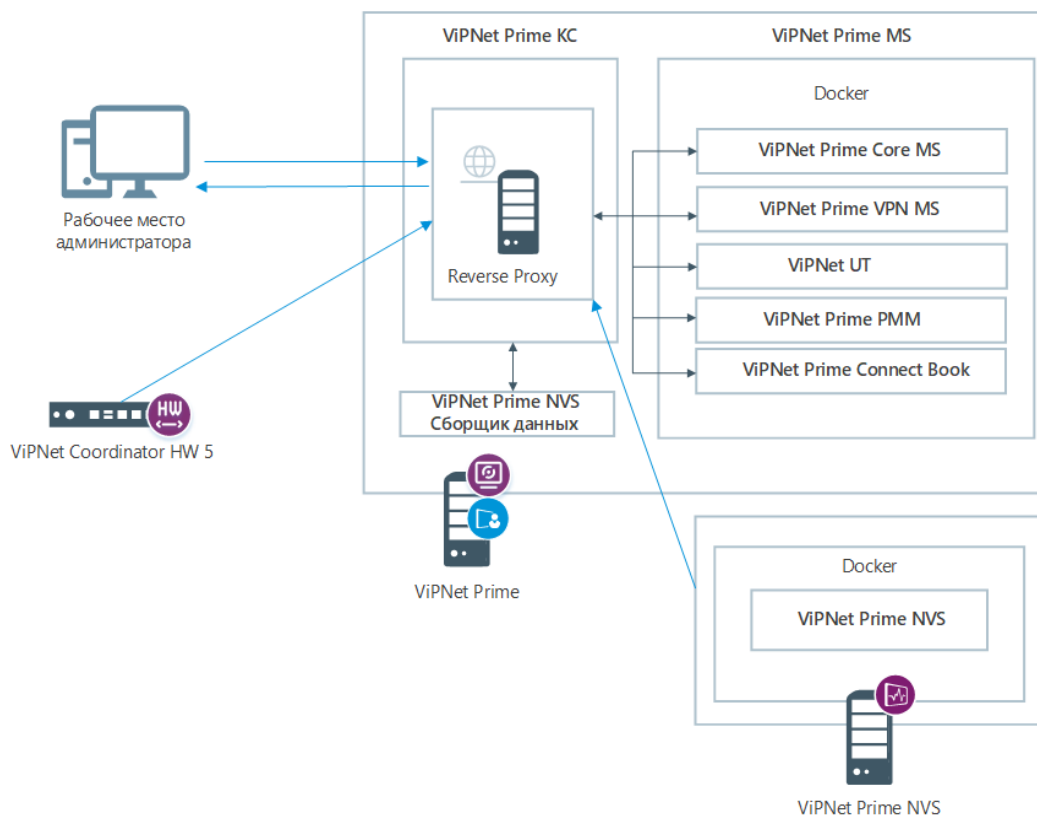


Рисунок 2. Размещение ViPNet Prime NVS на отдельном компьютере

В этой схеме:

- 1 Разрешите входящие соединения на локальном межсетевом экране:
 - на компьютере с ViPNet Prime по порту TCP 5671 для связи ViPNet Prime NVS и ViPNet Prime. Порт TCP 5671 используется по умолчанию для RabbitMQ.
 - на компьютере с ViPNet Prime NVS по портам:
 - TCP 28080 — для соединений по HTTP (VPN-трафик, приём данных телеметрии).
 - TCP 443 — для соединений по HTTPS (приём данных телеметрии).
- 2 Так как ViPNet Prime NVS Сборщик данных устанавливается на одну машину с ViPNet Prime, на компьютере с ViPNet Prime откройте порты:
 - TCP/UDP — 162 для работы SNMP-менеджера;
 - TCP/UDP — 161 для опроса координаторов сборщиком данных по протоколу SNMP.

Чтобы обнаруживать открытые устройства, на которых не установлено ПО ViPNet с функцией шифрования трафика на сетевом уровне, откройте исходящий порт 161 не только в защищённой, но и открытой сети. После этого в ViPNet Prime NVS укажите диапазон сканируемых IP-адресов и маску подсети. В результате сборщик данных будет отправлять на них SNMP-запросы с порта 161. См. «ViPNet Prime Network Visibility System. Руководство администратора», раздел «Обнаружение новых устройств в сети».
- 3 Разрешите исходящие соединения на компьютере с ViPNet Prime NVS по портам TCP 5671 и 443 для связи ViPNet Prime NVS и ViPNet Prime.

Каналы передачи данных

В сети ViPNet Prime есть два вида каналов связи:

- Канал связи между устройствами сети ViPNet — по нему передаются данные между устройствами. Канал защищён симметричным шифрованием по алгоритмам:
 - ГОСТ 34.12-2018 «Мagma» и «Кузнечик».
 - ГОСТ 28147–89.
- Канал управления, по которому передаётся служебная информация от ViPNet Prime к управляемым устройствам по протоколам:
 - HTTP/HTTPS — за передачу данных отвечает ViPNet UT.
 - ViPNet MFTP из состава ПО ViPNet поколения 4 с шифрованием по ГОСТ 28147–89.

По умолчанию порт TCP 48080 (HTTP) используется транспортом для взаимодействия с координаторами, порт TCP 48443 (HTTPS) используется для взаимодействия с ViPNet Client 5.

Принцип работы ViPNet UT

ViPNet UT состоит из двух компонентов:

- транспортный сервер;
- транспортный клиент.

Транспортный сервер устанавливается на компьютере с ViPNet Prime. Транспортный клиент входит в продукты поколения ViPNet 5 (кроме ViPNet xFirewall). Настройки транспортного клиента передаются на устройство в дистрибутиве ключей *.ds5.

Транспортный сервер доставляет на управляемое устройство:

- лицензию на продукт ViPNet;
- обновления справочников и ключей;
- обновление ПО;
- политики безопасности.

Транспортный клиент устройства передаёт в ViPNet Prime уведомления о доставке и применении обновлений.

2

Предварительные действия

Общий порядок установки	22
Подготовка ОС	25
Выбор источника случайных чисел	28
Настройка DNS	29
Настройка DNS-сервера на примере Bind9	31

Общий порядок установки

- 1 Выберите [схему размещения модулей](#).
- 2 Создайте папку `/infotecs/1.9.14/`:

```
$ sudo mkdir -p /infotecs/1.9.14/
```
- 3 В зависимости от схемы размещения:
 - 3.1 При установке на один компьютер скопируйте все файлы с ПО в папку `/infotecs/1.9.14/` и проверьте, что скопировано все ПО из комплекта поставки.
 - 3.2 При установке на два компьютера (компьютеры А и Б):
 - 3.2.1 На компьютер А скопируйте все файлы с ПО в папку `/infotecs/1.9.14`, кроме папки с архивом для установки ViPNet Prime NVS.
 - 3.2.2 На компьютере Б в папку `/infotecs/1.9.14` скопируйте папку с архивом для установки ViPNet Prime NVS.
- 4 Для работы ViPNet Prime и подключения по адресу `https://<ViPNet Prime DNS name>:<ViPNet Prime port>` назначьте [доменные имена модулям](#).
Доменные имена и порты ViPNet Prime укажите при установке.
- 5 Для доменных имён ViPNet Prime задайте [записи на DNS-сервере](#).
- 6 Для доменных имён ViPNet Prime получите в удостоверяющем центре один SSL/TLS-сертификат для веб-сервера (далее — сертификат сервера). Проверьте, что сертификат сервера соответствует [требованиям](#). Для использования частных доменных имён ViPNet Prime [создайте самоподписанный сертификат](#).
- 7 [Подготовьте к установке сертификаты сервера](#) (четыре файла) для подключения по TLS/HTTPS по алгоритмам TLS RSA в формате PEM. Если по правилам безопасности вашей организации требуется подключаться к ViPNet Prime с использованием двустороннего TLS ГОСТ, подготовьте сертификаты сервера (восемь файлов) по алгоритмам TLS ГОСТ в формате PEM.
Скопируйте их на сервер ViPNet Prime.
- 8 [Подготовьте ОС](#) к установке ViPNet Prime.
- 9 Убедитесь, что имя компьютера `hostname` или полное имя компьютера в домене `hostname.domainname` не совпадает с доменными именами ViPNet Prime Core и модулей. Если они совпадают, измените имя компьютера в файлах `/etc/hostname` и `/etc/hosts`, добавьте запись `127.0.1.1 <hostname>`. Отсутствие записи в `/etc/hosts` может привести к сетевым задержкам при использовании команд, требующих разрешения имени компьютера. Это негативно скажется на работоспособности ViPNet Prime.
- 10 Установите [базовые компоненты ViPNet Prime](#) с опцией `--no-start`.
Если правилами безопасности вашей организации требуется использовать двусторонний TLS ГОСТ:

10.1 На шаге **Do you want to install certificates set** введите **n** и следуйте дальнейшим шагам установки.



Внимание! На этом шаге не устанавливайте TLS ГОСТ-сертификат. Вы укажете TLS ГОСТ-сертификат позднее, когда запустите скрипт `install-certificates.sh`.

10.2 Аналогично сертификатам сервера для TLS RSA подготовьте к установке сертификаты сервера для TLS ГОСТ. Создайте запрос на сертификат сервера для TLS ГОСТ с помощью скрипта из комплекта поставки.



Примечание. В запросе на сертификат сервера для TLS ГОСТ `create-gost-tls-key.sh` не указываются такие поля как город, организация, ИНН. Поэтому он может не приниматься некоторыми российскими УЦ.

10.3 Перейдите в папку `/usr/share/infotecs/prime/deployment/core-ke:`

```
$ cd /usr/share/infotecs/prime/deployment/core-ke
```

10.4 Запустите скрипт `install-certificates.sh`:

```
$ sudo ./install-certificates.sh
```

10.5 На шаге **Do you want to install another certificates set** введите **y** и следуйте дальнейшим шагам установки.

11 Установите [остальные модули ViPNet Prime](#) (необязательно).



Внимание! После установки ViPNet Prime обязательно [запустите все модули](#), иначе стартовый контроль завершится ошибкой.

12 [Сконфигурируйте сеть для контейнеров Docker](#) и закройте доступ к порту 5671 (порт RabbitMQ).

13 Убедитесь, что на сетевой интерфейс компьютера с ViPNet Prime назначен только один адрес, он задан статически и совпадает:

- с адресом, который вы указали для компьютера с ViPNet Prime:

```
$ grep allow /etc/nginx/sites-enabled/nsms.conf | grep -v "127.0.0.1" | uniq
```
- с адресом, который сопоставляется с доменным именем ViPNet Prime и который указан в `/etc/hosts`.

14 Выполните [стартовую проверку целостности ViPNet Prime](#).

15 Если при установке ViPNet Prime вы указывали сертификат сервера ГОСТ:

15.1 Для одностороннего TLS ГОСТ на рабочем месте администратора:

15.1.1 Установите ViPNet PKI Client. См. документацию на ViPNet PKI Client.

15.1.2 В ViPNet PKI Client импортируйте сертификат сервера ГОСТ и корневой сертификат УЦ.



Внимание! При подключении к ViPNet Prime может всплывать окно с запросом на сертификат. Закройте его. Это не влияет на работу ViPNet Prime.

15.2 Для двустороннего TLS ГОСТ на рабочем месте администратора:

15.2.1 Установите ViPNet PKI Client. См. документацию на ViPNet PKI Client.

15.2.2 В ViPNet PKI Client импортируйте личный сертификат администратора и корневой сертификат УЦ, который выпустил сертификат на доменные имена ViPNet Prime.

15.2.3 Загрузите личный сертификат администратора, корневой сертификат УЦ, CRL в ViPNet Prime. См. «ViPNet Prime. Руководство администратора», раздел «Настройка аутентификации администраторов по сертификату».

16 Между ViPNet Prime и компьютером администратора синхронизируйте время. При рассинхронизации времени более чем на минуту нельзя подключиться к ViPNet Prime.

17 В веб-интерфейсе ViPNet Prime:

17.1 Подключите установленные модули. См. «ViPNet Prime. Руководство администратора», раздел «Подключение модулей к ViPNet Prime».



Внимание! Если вы переносите данные из ViPNet Administrator с помощью утилиты миграции сети ViPNet Prime Migration Tool, не создавайте узлы управления в ViPNet Prime VPN и не инициализируйте ключевой центр организации Core Network — центр управления и его координатор, иначе утилита миграции сети остановится с ошибкой и не перенесёт данные в ViPNet Prime.

17.2 Для работы с сетью VPN загрузите лицензию для ViPNet Prime и распределите лицензии для устройств Control Center и Core Coordinator, см. «ViPNet Prime. Руководство администратора», «Загрузка и обновление лицензии» и «Создание центра управления и его координатора».

17.3 Инициализируйте ключевой центр организации. См. «ViPNet Prime. Руководство администратора», раздел «Инициализация организации».

17.4 Создайте дистрибутивы ключей для узлов управления. См. «ViPNet Prime. Руководство администратора», раздел «Создание центра управления и его координатора».

18 На компьютере с ViPNet Prime установите ViPNet Client 5 for Linux и дистрибутив ключей узла центра управления Control Center. См. документацию на ViPNet Client.

19 На координаторе центра управления установите дистрибутив ключей узла Core Coordinator. См. документацию на координатор.

20 Для добавления пользователей из Active Directory в ViPNet Prime [установите коннектор](#). О настройке интеграции см. «ViPNet Prime. Руководство администратора», раздел «Настройка интеграции с Active Directory».

Подготовка ОС

Перед установкой ViPNet Prime подготовьте ОС:

- Штатными средствами ОС задайте сетевому интерфейсу статический IP-адрес. Он необходим для работы ViPNet Prime.
- Установите пакеты для работы ViPNet Prime.
- На Astra Linux SE настройте замкнутую программную среду (см. ниже) и отключите режимы:
 - Блокировка интерпретаторов.
 - Уровни конфиденциальности.
 - Блокировка установки бита исполнения.

Установка пакетов для ОС

Таблица 7. Установка пакетов для ОС

ОС	Команды	Примечание
Astra Linux SE 1.7.5.9	<pre>\$ sudo apt update && sudo apt install dpkg ca-certificates ufw docker.io docker-compose libseccomp2 libpcap0.8 -y</pre>	Используйте установочный диск из комплекта поставки ОС.
Astra Linux SE 1.8.3.8 и 1.8.5.46	<pre>\$ sudo apt-get update && sudo apt install dpkg ca-certificates systemd-resolved ufw docker.io docker-compose-v2 libseccomp2 libpcap0.8 -y</pre>	Используйте установочный диск из комплекта поставки ОС
Ubuntu 22.04.5	<pre>\$ sudo apt update && sudo apt install dpkg ca-certificates ufw docker.io docker-compose libseccomp2 libpcap0.8 -y</pre>	Используйте сетевой репозиторий (требуется подключение к интернету)



Внимание! Если ViPNet Prime NVS будет установлен на отдельном компьютере, установите пакеты на нём.

Настройка замкнутой программной среды Astra Linux SE

Работа ViPNet Prime в ОС с включённым режимом замкнутой программной среды (далее — режим ЗПС) возможна только в Astra Linux Special Edition. Если версия и сборка вашей ОС отличается от указанной в [требованиях](#), ViPNet Prime не будет работать с включённым в ОС режимом ЗПС.

Чтобы настроить режим ЗПС:

- 1 Перед входом в ОС выберите атрибут безопасности **Уровень целостности — Высокий**.

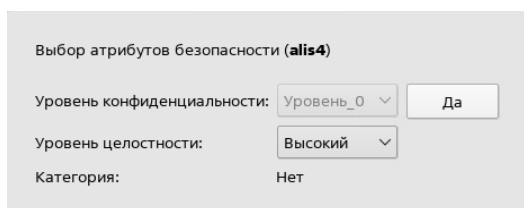


Рисунок 3. Выбор уровня целостности

Если в ОС не установлен графический интерфейс, то при входе в ОС на запрос **Integrity level** введите 63 (высокий уровень целостности).

```
Astra Linux 1.7.5 astra tty3
astra login: secadmin
Password:
Integrity level: 63
```

Рисунок 4. Вход в ОС без графического интерфейса

- 2 Войдите в ОС под учётной записью ОС с правами суперпользователя `root` или администратора для использования команды `sudo`.
- 3 Импортируйте ключ проверки электронной подписи ИнфоТеКСа:

- 3.1 Перейдите в папку с архивом дистрибутива ViPNet Prime Core KC:

```
$ cd /infotecs/1.9.14/core-kc.prime_cert.<номер_версии>/
```

- 3.2 Выдайте права на исполнение скрипту `extract-dist.sh`:

```
$ sudo chmod +x extract-dist.sh
```

- 3.3 Распакуйте архив `core-kc.tgz`:

```
$ sudo ./extract-dist.sh -c
```

- 3.4 Запустите скрипт `install-signature-keys.sh`:

```
$ sudo /usr/share/infotecs/prime/deployment/core-kc/install-signature-keys.sh
```

Скрипт установит пакет `astra-digsig-oldkeys` и разместит ключ `infotecs_pub_key.gpg` в папке `/etc/digsig/keys/infotecs/`.

- 3.5 На запрос **Reboot now (y/n)?** согласитесь на перезагрузку ОС, введите **Y** и нажмите **Enter**.

```
To run Core Installer required signature verification keys have been imported.
To apply settings need reboot system. Without reboot Core Installer may not start.
Reboot now (y/n)? y
```

Рисунок 5. Запрос на перезагрузку ОС

- 4 Войдите в ОС под учётной записью ОС с правами суперпользователя `root` или администратора для использования команды `sudo`.
- 5 Чтобы включить режим ЗПС в графическом интерфейсе:
 - 5.1 На Astra Linux SE 1.7 выберите **Панель управления > Безопасность > Политика безопасности > Замкнутая программная среда > Контроль исполняемых файлов > Включить**.

5.2 На Astra Linux SE 1.8 выберите **Параметры > Параметры системы > Ограничения программной среды > Замкнутая программная среда > Контроль исполняемых файлов > Включить**.

5.3 Сохраните изменения и перезагрузите компьютер.

6 Чтобы включить режим ЗПС в терминале:

6.1 Откройте файл `/etc/digsig/digsig_initramfs.conf` и укажите `DIGSIG_ELF_MODE=1`.

6.2 Выполните:

```
$ sudo update-initramfs -uk all
```

6.3 Перезагрузите компьютер.

Чтобы выключить режим ЗПС:

1 Через графический интерфейс:

1.1 На Astra Linux SE 1.7 выберите **Панель управления > Безопасность > Политика безопасности > Замкнутая программная среда > Контроль исполняемых файлов > Выключить**.

1.2 На Astra Linux SE 1.8 выберите **Параметры > Параметры системы > Ограничения программной среды > Замкнутая программная среда > Контроль исполняемых файлов > Выключить**.

1.3 Сохраните изменения и перезагрузите компьютер.

2 В терминале:

2.1 Откройте файл `/etc/digsig/digsig_initramfs.conf` и укажите `DIGSIG_ELF_MODE=0`.

2.2 После изменения выполните:

```
$ sudo update-initramfs -uk all
```

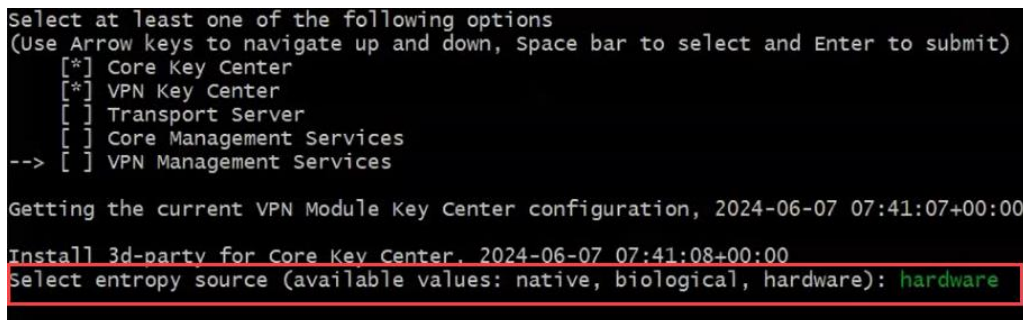
2.3 Перезагрузите компьютер.

Выбор источника случайных чисел

В ViPNet Prime для выполнения криптографических операций используется последовательность случайных чисел. Перед установкой ViPNet Prime определите, какой источник случайных чисел планируете использовать по требованиям безопасности. При установке базовых компонентов выберите источник случайных чисел.

ViPNet Prime поддерживает:

- **hardware** — физический датчик случайных чисел (ФДСЧ), например, АПМДЗ «Соболь» или «Аккорд-АПМДЗ». Настройте заранее, см. документацию на АПМДЗ, и подключите к серверу ViPNet Prime. Иначе появится сообщение `Entropy source not available or insufficient entropy. Installation cannot be continued. Please configure entropy source and retry`. ФДСЧ нельзя использовать при установке ViPNet Prime на виртуальную машину.
- **biological** — биологический датчик случайных чисел (электронная рулетка). Требуется запуск один раз в месяц.
- **native** — программный датчик, который для выработки случайной последовательности использует встроенный генератор случайных чисел UNIX-системы.



```
Select at least one of the following options
(Use Arrow keys to navigate up and down, Space bar to select and Enter to submit)
[*] Core Key Center
[*] VPN Key Center
[ ] Transport Server
[ ] Core Management Services
--> [ ] VPN Management Services

Getting the current VPN Module Key Center configuration, 2024-06-07 07:41:07+00:00
Install 3d-party for Core Key Center. 2024-06-07 07:41:08+00:00
Select entropy source (available values: native, biological, hardware): hardware
```

Рисунок 6. Выбор источника случайных чисел при установке

Чтобы сменить источник случайных чисел:

- 1 Выполните команду:
`$ sudo deployment-configurator install --no-start`
- 2 Выберите компонент **Core Key Center**.
- 3 Нажмите **Enter**.
- 4 Укажите источник случайных чисел и нажмите **Enter**.
- 5 В ходе работы мастера установки согласитесь с предложенными ответами на вопросы. Не изменяйте порты модулей и доменные имена. Иначе вы не сможете подключиться к веб-интерфейсу ViPNet Prime.
- 6 Выполните команду:
`$ sudo deployment-configurator start --all`

Настройка DNS



Примечание. Для сетевой связности компонентов ViPNet Prime MS и ViPNet Prime NVS используется внутренняя сеть Docker. Для разрешения доменных имен между модулями в этой внутренней сети используется служба `systemd-resolved`. После установки ViPNet Prime отключаются другие службы DNS. Поэтому при использовании других служб DNS (`networking/resolvconf`, `NetworkManager`) их настройки не применяются.

Чтобы подключаться к веб-интерфейсу ViPNet Prime за пределами локальной сети организации, используйте публичные доменные имена (приобретите или арендуйте у хостинг-провайдера), для локального подключения — частные доменные имена.

Подключение к веб-интерфейсу ViPNet Prime из локальной сети организации аналогично подключению к сайту в интернете. Между сервером и веб-интерфейсом используется защищённое HTTPS-соединение.

Чтобы подключиться к веб-интерфейсу ViPNet Prime, получите сертификат сервера и укажите в нём доменные имена модулей. Например, пусть модули имеют доменные имена веб-серверов:

- ViPNet Prime Core — `prime.example.ru`.
- ViPNet Prime VPN — `vpn.example.ru`.
- ViPNet Prime PMM — `pmm.example.ru`.
- ViPNet Prime NVS — `nvs.example.ru`.

Пусть веб-интерфейс ViPNet Prime будет доступен по IP-адресу `10.0.0.11`, а ViPNet Prime NVS имеет IP-адрес `10.0.0.12`.

Независимо от схемы размещения ViPNet Prime NVS, на DNS-сервере укажите для ViPNet Prime NVS IP-адрес `10.0.0.11` `nvs.example.ru`.

Настройка на DNS-сервере необходима для других компьютеров, которые подключаются к ViPNet Prime, например, компьютеру администратора.

Если ViPNet Prime NVS установлен на одном компьютере с ViPNet Prime, убедитесь, что в файле `/etc/hosts` есть запись `10.0.0.11 nvs.example.ru`. Если ViPNet Prime NVS установлен на отдельном компьютере:

- на компьютере с ViPNet Prime в файле `/etc/hosts` проверьте наличие записи для ViPNet Prime NVS `10.0.0.11 nvs.example.ru`;
- на компьютере с ViPNet Prime NVS в файле `/etc/hosts` проверьте наличие записи для ViPNet Prime NVS `10.0.0.12 nvs.example.ru`.

С рабочего места администратора обеспечьте доступ к IP-адресам компьютеров, на которых установлен ViPNet Prime, и используемым портам.

Для реализации [сервисной модели предоставления услуг](#) в ViPNet Prime используются поддомены для деления пространства между организациями. Для этого на DNS-сервер добавьте записи:

- для основного домена (ViPNet Prime Core);
- для доменов модулей;
- для поддоменов организаций (перенаправление должно быть на IP-адрес ViPNet Prime Core).

После этого для поддоменов организаций вы можете настроить аутентификацию через Microsoft Active Directory (см. «ViPNet Prime. Руководство администратора», «Настройка аутентификации с помощью служб федераций AD FS»). Примеры доменных имён для сервисной модели предоставления услуг смотрите в разделе [О сертификате сервера](#).

Таблица 8. Пример DNS-записей для домена *example.ru*

Тип записи	Имя записи	Целевое значение
CNAME-запись	*.Prime	Prime.example.ru.
A-запись	Prime	10.0.0.11
A-запись	vpn	10.0.0.11
A-запись	nvs	10.0.0.11
CNAME-запись	*.nvs	nvs.example.ru.

Настройка DNS-сервера на примере Bind9

1 Установите bind9 и dnsutils:

```
$ sudo apt install bind9 -y && sudo apt install dnsutils -y
```

2 Настройте forward-зоны. Для этого добавьте в файл /etc/bind/named.conf.local следующую запись:

```
zone "example.com" {
    type master;
    file "/etc/bind/db.example.com";
};

zone "153.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.182.168.153";
};
```

где:

- o example.com — зона прямого просмотра;
- o 153.168.192.in-addr.arpa — зона обратного просмотра.

3 Создайте зону обратного просмотра:

3.1 Выполните команду:

```
$ sudo nano /etc/bind/db.example.com
```

3.2 Добавьте в файл следующую запись:

```
$TTL 604800
@      IN      SOA      ns1.example.com. admin.example.com. (
    1          ; Serial
    604800     ; Refresh
    86400      ; Retry
    2419200    ; Expire
    604800)    ; Negative Cache TTL
@      IN      NS       ns1.example.com.
ns1     IN      A        192.168.153.146
@      IN      A        192.168.153.146
mycomputer  IN    A      192.168.153.1
```

4 Создайте зону обратного просмотра:

4.1 Выполните команду:

```
$ sudo nano /etc/bind/db.192.168.153
```

4.2 Добавьте в файл следующую запись:

```
$TTL 604800
@      IN      SOA      ns1.example.com. admin.example.com. (
        2      ; Serial
        604800 ; Refresh
        86400  ; Retry
        2419200 ; Expire
        604800) ; Negative Cache TTL
@      IN      NS       ns1.example.com.
146    IN      PTR      example.com.
1      IN      PTR      mycomputer.example.com.
```

5 Проверьте конфигурацию сервера и зон прямого и обратного просмотра:

```
$ sudo named-checkconf
```

```
$ sudo named-checkzone example.com /etc/bind/db.example.com
```

```
$ sudo named-checkzone 153.168.192.in-addr.arpa /etc/bind/db.192.168.153
```

6 На компьютере с ViPNet Prime откройте для редактирования конфигурационный файл /etc/systemd/resolved.conf.

7 Раскомментируйте строку DNS= и укажите адрес DNS-сервера, например 192.168.153.146:

```
DNS=192.168.153.146
```

8 Раскомментируйте строку Domains= и через пробел без запятых запишите vipnet и доменные имена защищённых ресурсов, которые были заданы администратором сети.

9 Перезапустите systemd-resolved:

```
root@host:~# systemctl restart systemd-resolved
```

10 Очистите DNS-кеш:

```
root@host:~# systemd-resolve --flush-caches
```

или

```
root@host:~# resolvectl flush-caches
```

11 Проверьте доступность DNS-сервера по доменному имени:

```
$ ping example.com
```

3

Подготовка TLS-сертификатов сервера

О сертификате сервера	34
Требования к сертификату сервера	35
Конвертация сертификата сервера в формат PEM	37
Построение цепочки доверия сертификата сервера	38
Использование сертификата НУЦ Минцифры России	39
Издание самоподписанного сертификата сервера	40
Создание запроса на сертификат сервера ГОСТ	42
Обновление сертификата сервера	44
Часто задаваемые вопросы	47

О сертификате сервера

Вы можете подключаться к веб-интерфейсу ViPNet Prime с компьютеров, находящихся в интернете или локальной сети. Для этого требуется установить защищённое TLS-соединение:

- с односторонней аутентификацией, предполагающей только проверку подлинности сертификата сервера. В этом случае потребуются:
 - сертификат сервера, созданный по алгоритму RSA (далее — сертификат RSA), и соответствующий ключ ЭП;
 - корневой сертификат УЦ, издавшего сертификат сервера, и соответствующий CRL;
 - при наличии сертификаты всех УЦ из цепочки и соответствующие CRL;
 - если требуется правилами вашей организации, сертификат сервера, созданный по алгоритму ГОСТ Р 34.10-2012(далее — ГОСТ) и соответствующий ключ ЭП, корневой сертификат УЦ, а также, при наличии, сертификаты всех УЦ из цепочки и соответствующий CRL.
- с двусторонней аутентификацией, предполагающей проверку подлинности сертификата сервера и вашего сертификата администратора. Для этого потребуются:
 - сертификат сервера и ключи по алгоритму RSA;
 - сертификат сервера и ключи по алгоритму ГОСТ для сервера ViPNet Prime:
 - корневой сертификат УЦ (*.crt);
 - CRL для корневого сертификата УЦ (*.crl) — не требуется для установки, необходим для аутентификации по сертификату;
 - сертификат сервера с полной цепочкой доверия (*.crt);
 - сертификат сервера с закрытым ключом в контейнере PFX (*.pfx).
 - Для компьютера администратора:
 - личный сертификат администратора (*.pem, *.crt или *.cer) по алгоритму ГОСТ (далее — сертификат ГОСТ);
 - сертификат корневого УЦ и промежуточного (если УЦ не головной);
 - CRL для корневого сертификата УЦ (*.crl).

Требования к сертификату сервера

- Сертификат с проверкой подлинности домена (Domain Validation, DV-сертификат).
- Длина ключа проверки ЭП:
 - для сертификата RSA: 2048 бит или более.
 - для сертификата ГОСТ: 256 бит.
- Формат файла ключа проверки ЭП: PEM, PKCS#1.
- Формат файла сертификата: PEM. Файл должен начинаться с -----BEGIN CERTIFICATE----- и заканчиваться -----END CERTIFICATE----- . Если формат сертификата не соответствует PEM, [конвертируйте его](#) для установки в ViPNet Prime.
- Поле Subject Alternative Name содержит:
 - список доменных имён ViPNet Prime и модулей (если список имён всех подключаемых организаций заранее известен);
 - или маску доменных имён ViPNet Prime и модулей (если список имён подключаемых организаций может изменяться).
- Поле ExtendedKeyUsage со значением ServerAuthentication.
- При использовании самоподписанных сертификатов заполните поле Common Name (CN).



Примечание. Требования к сертификатам и срокам действия могут изменяться со временем, уточняйте актуальные требования у издателей сертификатов и производителей браузеров.

Примеры доменных имён

Рассмотрим сеть, которая состоит из двух организаций:

- prime.example.ru доменное имя ViPNet Prime для входа поставщика услуг;
- доменные имена модулей:
 - vpn.example.ru
 - pmm.example.ru
 - nvs.example.ru
 - connect.example.ru
- доменные имена организаций:
 - org1.prime.example.ru
 - org2.prime.example.ru

В запросе на сертификат сервера:

- В поле Common Name (CN) — укажите доменное имя ViPNet Prime Core.

- В поле `SAN` — доменные имена ViPNet Prime Core, модулей и организаций. Если количество организаций заранее неизвестно, укажите `*.example.ru` и получите wildcard-сертификат.

В ViPNet Prime в сценарии **поставщика услуг** и организаций-потребителей настройте доменную аутентификацию:

- настройте интеграцию с Active Directory Federation Service для нескольких организаций;
- подключите домены для **организаций** для отдельного доступа к веб-интерфейсу ViPNet Prime по своим доменным именам как к облачному сервису.

См. «ViPNet Prime. Руководство администратора» > «Доменная аутентификация».

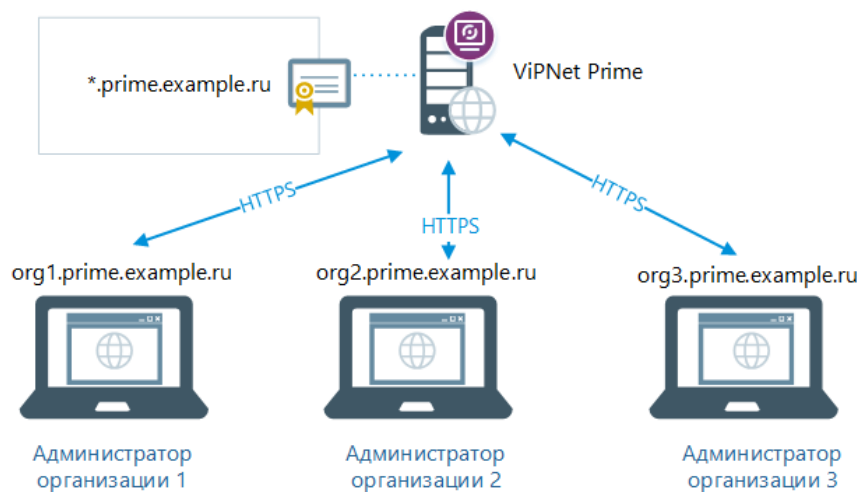


Рисунок 7. Подключение к веб-интерфейсу ViPNet Prime в сценарии поставщика услуг

Конвертация сертификата сервера в формат PEM

Если формат сертификата не соответствует PEM, конвертируйте его. Для сертификата RSA преобразуйте сертификат, CRL и закрытый ключ. Для сертификатов на алгоритмах ГОСТ преобразуйте сертификат и CRL.

- Чтобы сконвертировать сертификат из DER в PEM:

```
$ sudo openssl x509 -in <имя_файла>.der -inform DER -out <имя_файла>.crt
```

- Чтобы сконвертировать CRL из DER в PEM:

```
$ sudo openssl crl -in <имя_файла>.crl -inform DER -out <имя_файла>.crl
```

- Убедитесь, что получен закрытый ключ в формате PEM. Файл должен начинаться с -----BEGIN RSA PRIVATE KEY----- и заканчиваться -----END RSA PRIVATE KEY-----.

- Если файл закрытого ключа имеет заголовок -----BEGIN PRIVATE KEY-----, сконвертируйте его в файл PEM:

```
$ sudo openssl rsa -in <имя_файла>.key -out <имя_файла>.key
```

Где <имя_файла>.key — файл ключа с заголовком -----BEGIN PRIVATE KEY-----.

- Если ключ в контейнере PFX, сконвертируйте его в файл PEM:

```
$ sudo openssl pkcs12 -in <имя_файла>.pfx -out <имя_файла>.pem -nodes -nocerts
```

Построение цепочки доверия сертификата сервера

Цепочка доверия сертификатов необходима для проверки подлинности сертификат. Если сертификат сервера подписан промежуточным УЦ, постройте цепочку доверия для сертификата сервера.

Например, получены:

- `root.crt` — сертификат головного УЦ;
- `intermediate_1.crt` — сертификат промежуточного УЦ;
- `intermediate_2.crt` — сертификат УЦ, который издал сертификат сервера;
- `prime.example.ru.crt` — сертификат сервера, содержащий все доменные имена для подключения к ViPNet Prime, его модулям и организациям.

Чтобы восстановить цепочку доверия:

- 1 Последовательно (начиная с сертификата сервера) запишите сертификаты в новый файл:

```
echo $'\r' | tee -a prime.example.ru.crt intermediate_2.crt intermediate_1.crt &&  
cat prime.example.ru.crt intermediate_2.crt intermediate_1.crt  
> prime.example.ru.fullchain.crt
```

- 2 Чтобы проверить цепочку доверия:

```
$ sudo openssl verify -CAfile root.crt -untrusted intermediate-2.crt -untrusted  
intermediate-1.crt prime.example.ru.fullchain.crt
```

- 3 Убедитесь, что ключ соответствует сертификату и запросу на сертификат. Для этого сравните хэш-суммы:

```
$ openssl x509 -noout -modulus -in prime.example.ru.crt | openssl md5  
$ openssl rsa -noout -modulus -in example.ru.key | openssl md5  
$ openssl req -noout -modulus -in example.ru.csr | openssl md5  
$ openssl req -noout -modulus -in example.ru.csr > req_name-mod.txt && openssl  
x509 -noout -modulus -in prime.example.ru.crt > certificate_name-mod.txt && openssl  
rsa -noout -modulus -in example.ru.key > privatekey_name-mod.txt && diff3 req_name-  
mod.txt certificate_name-mod.txt privatekey_name-mod.txt
```

Если все три файла идентичны, утилита `diff3` ничего не отобразит.

Использование сертификата НУЦ Минцифры России

- 1 Получите сертификат сервера для ViPNet Prime. См. <https://www.gosuslugi.ru/tls>.
- 2 На компьютере с ViPNet Prime и на компьютере администратора установите корневой и промежуточный сертификаты НУЦ Минцифры России в хранилище ОС.
См. <https://www.gosuslugi.ru/crt>.

Издание самоподписанного сертификата сервера

Вы можете использовать самоподписанные сертификаты по алгоритмам RSA для ViPNet Prime, если нет необходимости подключаться к ViPNet Prime из глобальной сети.

Издание сертификата в корпоративном УЦ

1 Создайте закрытый ключ:

```
$ sudo openssl genrsa -out key.pem 2048
```

2 Создайте файл `req.cnf` со структурой по шаблону:

```
[ req ]
default_bits          = 2048
distinguished_name    = req_distinguished_name
req_extensions        = req_ext
[ req_distinguished_name ]
countryName           = Country Name (2 letter code)
stateOrProvinceName   = State or Province Name (full name)
localityName          = Locality Name (eg, city)
organizationName      = Organization Name (eg, company)
commonName            = Common Name (e.g. server FQDN or YOUR name)
[ req_ext ]
subjectAltName        = @alt_names
keyUsage              = keyEncipherment, dataEncipherment
extendedKeyUsage      = serverAuth
[alt_names]
DNS.1                = example.com
DNS.2                = *.example.com
DNS.3                = prime.example.com
```

В разделе `[alt_names]` укажите доменное имя модуля. Страну, город и организацию вы введёте позже при создании запроса на сертификат, поэтому все остальные поля, кроме раздела `[alt_names]`, оставьте без изменений.

3 Создайте запрос на сертификат:

```
$ sudo openssl req -config req.cnf -new -key key.pem -out req.csr
```

Укажите значения, запрашиваемые в шагах работы команды.

4 В корпоративном УЦ издайте сертификат по запросу.

Издание TLS-сертификата с помощью OpenSSL

Если в вашей организации нет корпоративного УЦ, создайте самоподписанный сертификат с помощью OpenSSL на компьютере Linux.

1 Создайте закрытый ключ УЦ:

```
$ sudo openssl genrsa -out ca.key 2048
```

2 Создайте сертификат УЦ на 365 дней:

```
$ sudo openssl req -x509 -new -key ca.key -days 365 -out ca.crt
```

3 Создайте закрытый ключ для сертификата сервера:

```
$ sudo openssl genrsa -out nginx.key 2048
```

4 Создайте запрос на сертификат и укажите доменные имена:

```
$ sudo openssl req -new -key nginx.key -subj  
"/CN=<доменное_имя_1>/CN=<доменное_имя_2>" -out nginx.csr
```

5 Создайте текстовый файл (например, `openssl.cnf`) и укажите список SAN (Subject Alternative Name), идентичный списку в запросе на сертификат:

```
[SAN]  
subjectAltName = @alt_names  
[alt_names]  
DNS.1 = <доменное.имя.1>  
DNS.2 = <*.доменное.имя.1>  
DNS.3 = <доменное.имя.2>
```

6 Издайте сертификат сервера:

```
$ sudo openssl x509 -req -in nginx.csr -CA ca.crt -CAkey ca.key -CAcreateserial -  
out nginx.crt -days 365 -extensions SAN -extfile openssl.cnf
```

Создание запроса на сертификат сервера ГОСТ

С помощью скрипта



Примечание. В запросе на сертификат сервера для TLS ГОСТ `create-gost-tls-key.sh` не указываются такие поля как город, организация, ИНН. Поэтому он может не приниматься некоторыми российскими УЦ.

Если правилами безопасности вашей организации требуется подключаться к ViPNet Prime с использованием TLS ГОСТ, создайте закрытый ключ `*.pfx` и запрос на сертификат сервера `*.req` с помощью скрипта `create-gost-tls-key.sh` из комплекта поставки:

1 Установите базовые компоненты ViPNet Prime.

2 Перейдите в папку:

```
$ cd /usr/share/infotecs/prime/deployment/core-kc/
```

3 Выполните команду:

```
$ sudo ./create-gost-tls-key.sh
```

4 Следуйте вопросам:

4.1 Введите имя домена без имени хоста, которое будет использоваться при подключении к веб-интерфейсу ViPNet Prime.

Например, если вы планируете подключаться по адресу `core.example.ru`, в ответ на запрос введите `example.ru`. В результате в запросе на сертификат ГОСТ в поле SAN будут указаны имена `example.ru` и `*.example.ru`.

4.2 Задайте пароль к контейнеру с закрытым ключом и подтвердите его.

В папке `/usr/share/infotecs/prime/deployment/core-kc` будут созданы файлы запроса и закрытого ключа.



Примечание. Чтобы подключаться к ViPNet Prime с помощью сертификата сервера ГОСТ, установите ViPNet PKI Client версии 2.0.

С использованием ViPNet PKI Client

1 На компьютер администратора установите ViPNet PKI Client версии 2.0.

2 Создайте запрос на сертификат сервера. Выберите шаблон сертификата **Специальный** и включите  **Расширенный режим**.

3 Заполните атрибуты:

- **Общее имя** — доменное имя ViPNet Prime, по которому вы будет подключаться к серверу ViPNet Prime через HTTPS, например, `core.example.ru`;
- **Использование ключа (Критичное)** — Цифровая подпись, Шифрование ключей и Согласование ключей;
- **Расширенное использование ключа (Критичное)** — Проверка подлинности сервера;
- **Альтернативное имя владельца (Критичное)** — доменные имена модулей ViPNet Prime (`prime.example.ru`, `vpn.example.ru`, `pmm.example.ru`, `nvs.example.ru`, `cb.example.com`). В качестве типа выберите **Доменное имя**.

Обновление сертификата сервера

Срок действия сертификата сервера ограничен. Чтобы сохранить работоспособность ViPNet Prime и не потерять доступ к его веб-интерфейсу, заранее, например, за 14 дней до окончания срока действия сертификата получите новые сертификаты и обновите их. Чтобы просмотреть срок действия сертификата сервера:

- В браузере:
 - Откройте веб-интерфейс ViPNet Prime.
 - Нажмите значок сведений о сайте.
 - Просмотрите сведения об используемом сертификате.

- В командной строке:

```
$ openssl x509 -in <путь к файлу сертификата> -text -noout
```

Срок действия сертификата указан в поле **Validity**.

- В ViPNet Prime NVS выберите **Система > Состояние системы > Здоровье > TLS-сертификаты**. За 30 дней администратору придёт уведомление о скором истечении срока действия сертификатов. См. «ViPNet Prime Network Visibility System. Руководство администратора».

Обновление сертификатов сервера с помощью скрипта



Внимание! Обновить сертификаты ViPNet Prime NVS можно только вручную (см. ниже).

- 1 В УЦ закажите сертификаты, удовлетворяющие [требованиям](#).
- 2 На компьютере с ViPNet Prime войдите в ОС под учётной записью ОС с правами суперпользователя `root` или администратора для использования команды `sudo`.
- 3 [Завершите работу ViPNet Prime](#).
- 4 Получите в УЦ файлы:
 - сертификат RSA и соответствующий ключ ЭП;
 - корневой сертификат УЦ, издавшего сертификат сервера, и соответствующий CRL;
 - при наличии сертификаты всех УЦ из цепочки и соответствующие CRL;
 - если требуется правилами вашей организации, сертификат ГОСТ и соответствующий ключ ЭП, корневой сертификат УЦ, а также, при наличии, сертификаты всех УЦ из цепочки и соответствующий CRL.
- 5 Перейдите в папку `/usr/share/infotecs/prime/deployment/core-kc:`

```
$ cd /usr/share/infotecs/prime/deployment/core-kc
```

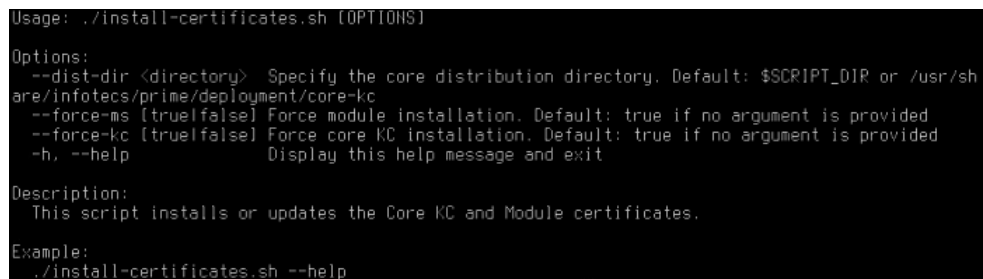
6 Выполните команду:

```
$ sudo ./install-certificates.sh
```

7 Установите новые сертификаты на компьютере, с которого вы подключаетесь к ViPNet Prime.

Чтобы вызвать справку для скрипта `install-certificates.sh`, выполните

```
$ sudo ./install-certificates.sh --help
```



```
Usage: ./install-certificates.sh [OPTIONS]

Options:
  --dist-dir <directory> Specify the core distribution directory. Default: $SCRIPT_DIR or /usr/share/infotecs/prime/deployment/core-kc
  --force-ms [true|false] Force module installation. Default: true if no argument is provided
  --force-kc [true|false] Force core KC installation. Default: true if no argument is provided
  -h, --help              Display this help message and exit

Description:
  This script installs or updates the Core KC and Module certificates.

Example:
  ./install-certificates.sh --help
```

Рисунок 8. Вывод справочной информации

Обновление сертификатов сервера ViPNet Prime NVS

- 1 Обратитесь в УЦ для получения сертификатов, удовлетворяющих [требованиям](#).
- 2 На компьютере с Prime войдите в ОС под учётной записью ОС с правами суперпользователя `root` или администратора для использования команды `sudo`.
- 3 [Завершите работу ViPNet Prime](#).
- 4 Получите в УЦ файлы:
 - сертификат RSA и соответствующий ключ ЭП;
 - корневой сертификат УЦ, издавшего сертификат сервера, и соответствующий CRL;
 - при наличии сертификаты всех УЦ из цепочки и соответствующие CRL.
- 5 Скопируйте полученные в УЦ файлы на компьютер с установленным ViPNet Prime NVS в папку `/infotecs/certs`.
- 6 Выполните команду:

```
$ sudo deployment-configurator stop
```
- 7 Выберите **Monitoring module**.
- 8 Запустите установку ViPNet Prime NVS:
 - 8.1 Выполните команду:

```
$ sudo deployment-configurator install
```
 - 8.2 Выберите **Monitoring module**.

- 9 Укажите пути к новым сертификатам и ключу.
- 10 Завершите установку, не изменяя остальные параметры.
- 11 Запустите ViPNet Prime NVS:
 - 11.1 Выполните команду:

```
$ sudo deployment-configurator start
```
 - 11.2 Выберите **Monitoring module**.
- 12 Установите новые сертификаты на компьютере, с которого вы подключаетесь к ViPNet Prime.



Примечание. Обновление сертификата администратора см. в «ViPNet Prime. Руководство администратора» > «Обновление сертификата администратора».

Часто задаваемые вопросы

- **Какие доменные имена использовать для ViPNet Prime?**
 - Публичные доменные имена, если нужно подключаться к ViPNet Prime из глобальной сети. На такие имена получите сертификат сервера, имеющий публичное доверие.
 - Частные доменные имена, если не нужно подключаться к ViPNet Prime из глобальной сети. На такие имена создайте самоподписанный SSL/TLS-сертификат. В этом случае ViPNet Prime будет иметь [ограничения](#).
- **УЦ предоставляет для сайтов несколько типов SSL/TLS-сертификатов сервера: DV (Domain Validation), OV (Organization Validation), EV (Extended Validation). Что выбрать?**

Достаточно сертификата с подтверждением владения доменом (DV, Domain Validation).
- **Всегда нужен wildcard-сертификат?**

Нет, не всегда. Он нужен, если вы как поставщик услуг планируете предоставлять доступ к веб-интерфейсу ViPNet Prime нескольким организациям-потребителям.
- **Обязательно ли использовать только А-записи при настройке DNS?**

Нет, не обязательно. Можно использовать CNAME-записи для всех модулей, которые будут ссылаться на единственную А-запись.

4

Установка ViPNet Prime

Установка базовых компонентов	49
Установка ViPNet Prime PMM	55
Установка ViPNet Prime NVS	58
Установка ViPNet Prime NVS Сборщик данных	60
Установка ViPNet Connect Book	61
Обновление ViPNet Prime	63

Установка базовых компонентов

В состав базовых компонентов ViPNet Prime входят:

- ViPNet Prime Core KC;
- ViPNet Prime Core MS;
- ViPNet Prime VPN KC;
- ViPNet Prime VPN MS;
- транспортный сервер ViPNet UT.

Особенности установки

- Если сертификат сервера содержит wildcard-домены, то для ViPNet Prime VPN вы сможете назначить отличное от ViPNet Prime Core (**Prime DNS name**) доменное имя.
- Если сертификат не предусматривает нескольких wildcard-доменов или развёртывание не предусматривает другой конфигурации, то при установке ViPNet Prime VPN вы можете указать доменное имя ViPNet Prime Core (**Prime DNS name**).
- Для ViPNet Prime VPN укажите порт, отличный от того, что указали для ViPNet Prime Core (**ViPNet Prime port**).

Установка

Ниже рассматривается вариант установки ViPNet Prime и его модулей с использованием разных доменных имён и одного порта.

- 1 Войдите в ОС под учётной записью ОС с правами суперпользователя `root` или администратора для использования команды `sudo`.
- 2 При входе в Astra Linux SE:
 - В графическом интерфейсе выберите атрибут безопасности **Уровень целостности** — **Высокий**.

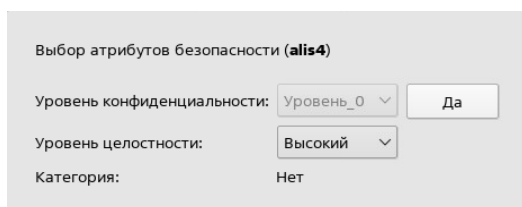


Рисунок 9. Выбор уровня целостности

- В командной строке на запрос **Integrity level** введите 63 (высокий уровень целостности).

```
Astra Linux 1.7.5 astra tty3
astra login: secadmin
Password:
Integrity level: 63
```

Рисунок 10. Вход в ОС без графического интерфейса

3 Подготовьте ОС к установке ViPNet Prime.

4 Разместите сертификаты в папке /infotecs/certs.

5 Если вы используете kesl, добавьте в исключения kesl цепочку сертификатов:

```
$ sudo kesl-control --add-certificate /infotecs/certs/nginx.crt
$ sudo systemctl restart kesl
```

6 Разместите содержимое папки с ПО в папке /infotecs/1.9.14. Если вы устанавливаете ViPNet Prime NVS на отдельном компьютере, разместите ПО ViPNet Prime NVS на него.

7 Перейдите в папку /infotecs/1.9.14/:

```
$ cd /infotecs/1.9.14/
```

8 Посмотрите содержимое папки /infotecs/1.9.14:

```
$ tree -L 3
```

Убедитесь, что структура файлов и папок соответствует структуре из комплекта поставки.

9 Распакуйте архив с ПО:

```
$ sudo find . -name "extract-dist.sh" -exec chmod +x {} \; -exec {} -c \;
```

Компоненты ViPNet Prime Core KC, ViPNet Prime Core MS, ViPNet Prime VPN KC, ViPNet Prime VPN MS, ViPNet Prime NVS, ViPNet Connect Book, ViPNet UT и deployment-configurator распакуются по умолчанию в папки:

- o /usr/lib/infotecs/prime-deployment-configurator
- o /usr/share/infotecs/prime/deployment/core-ms
- o /usr/share/infotecs/prime/deployment/vpn-ms
- o /usr/share/infotecs/prime/deployment/core-kc
- o /usr/share/infotecs/prime/deployment/vpn-kc
- o /usr/share/infotecs/prime/deployment/connect
- o /usr/share/infotecs/prime/deployment/transport

Также вы можете распаковать каждый архив по отдельности. Например, чтобы распаковать архив core-ms.tgz, выполните:

```
$ cd /infotecs/1.9.14/core-ms.prime.<номер_версии>/
$ sudo chmod +x ./extract-dist.sh
$ sudo ./extract-dist.sh -c
```

10 Если вы устанавливаете ViPNet Prime на Astra Linux SE 1.7.5.9, выполните команду:

```
$ sudo systemctl enable --now systemd-resolved.service
```

11 Запустите configurator:

```
$ sudo deployment-configurator install --no-start
```

12 Выберите компоненты:

- Core Key Center.
- Transport Server.
- VPN Key Center.
- Core Management Services.
- VPN Management Services.

13 Нажмите Enter.

14 Начнётся установка. В ходе установки ответьте на вопросы:



Внимание! Порядок вопросов при установке ViPNet Prime может отличаться от описанного в документе.

14.1 Do you want to install the Key Center and the Management Services on the same computer — введите `y`, так как ViPNet Prime KC и MS необходимо устанавливать на один компьютер согласно [схемам размещения модулей](#).

14.2 Select entropy source (available values: native, biological, hardware) — выберите источник случайных чисел. Подробнее см. в [Выбор источника случайных чисел](#).

14.3 Path to the trusted CA certificate — введите путь к сертификату корневого УЦ, который выдал TLS-сертификат сервера ViPNet Prime, например, `/infotecs/certs/ca.crt`. По умолчанию система ожидает сертификат по пути `/ca.crt`.

14.4 Path to the TLS server certificate — введите путь к TLS-сертификату сервера, например, `/infotecs/certs/nginx.crt`. Если сертификат не содержит wildcard-записей в поле `Subject Alternative Name`, после сообщения продолжайте установку, это не ошибка.

14.5 Path to the private key associated with the TLS server certificate — введите путь к закрытому ключу TLS-сертификата сервера, например `/infotecst/certs/nginx.key`.

14.6 Do you want to install another certificates set — задайте использование TLS ГОСТ при подключении к веб-интерфейсу ViPNet Prime:



Внимание! Укажите **н** даже если вам требуется TLS ГОСТ. Вы укажете TLS ГОСТ-сертификат позднее, когда запустите скрипт `install-certificates.sh`. См. [Общий порядок установки](#).

14.7 Type the Core DNS name — введите доменное имя ViPNet Prime Core. По нему вы будете подключаться к веб-интерфейсу ViPNet Prime.

14.8 Type the Core port — введите порт ViPNet Prime Core. По нему вы будете подключаться к веб-интерфейсу ViPNet Prime. По умолчанию — 443.

14.9 Type the Core IP address for <доменное имя ViPNet Prime> (will be added to /etc/hosts), or leave it empty if you use external DNS server — введите статический IP-адрес компьютера с ViPNet Prime (запись будет добавлена в `/etc/hosts`) при отсутствии DNS-сервера или оставьте значение пустым при использовании корпоративного DNS-сервера.

14.10 Type PostgreSQL password — введите пароль для подключения к базе данных PostgreSQL. Длина пароля — от 10 до 32 символов с использованием строчных и заглавных букв латинского алфавита, цифр и специальных символов ! # \$ % ^ & _ = + -.

14.11 Type the Universal Transport client ID or keep the generated value — введите идентификатор устройства Control Center с функцией транспортного клиента:

- При первой установке ViPNet Prime оставьте предложенное значение. Пример идентификатора: a5d953cd-91cd-54d1-ced3-0889f0325cd3.
- Если ViPNet Prime уже установлен и запускался, укажите идентификатор, который создан при первой установке. Чтобы посмотреть идентификатор, откройте другое окно терминала и выполните:

```
$ sudo docker exec -it -u postgres smp_smp-postgresql_1 psql -P pager=off  
-U postgres -p 5433 -d security_management -c "select value from  
smp_config where key='prime-transport-client-id';"
```

14.12 Path to the trusted CA certificate — введите путь к сертификату корневого УЦ, который выдал TLS-сертификат сервера ViPNet Prime.

14.13 Allow adding child organizations — включите, если при построении вашей сети будете создавать дочерние организации от корневых:



Внимание! После установки и при обновлении ViPNet Prime вы не сможете отключить этот параметр.

- **y** — включить;
- **n** — отключить.

14.14 Do you want to install the Key Center and the Management Services on the same computer — введите y, так как установка ViPNet Prime выполняется на один компьютер.

14.15 Type the Core DNS name — введите доменное имя ViPNet Prime Core.

14.16 Type the Core port — введите порт ViPNet Prime Core.

14.17 Type the VPN module DNS name — введите доменное имя ViPNet Prime VPN.

14.18 Type the VPN module port — введите порт ViPNet Prime VPN.

14.19 Type the host's external interface IP address — введите IP-адрес внешнего сетевого интерфейса компьютера с ViPNet Prime.

14.20 Do you want to install the Key Center and the Management Services on the same computer — введите y, так как установка ViPNet Prime выполняется на один компьютер.

14.21 Path to the VPN module's trusted CA certificate — введите путь к сертификату корневого УЦ, который выдал сертификат сервера ViPNet Prime, например, /infotecs/certs/ca.crt.

14.22 Type the Core DNS name — введите доменное имя ViPNet Prime Core.

14.23 Type the Core port — введите порт ViPNet Prime Core.

14.24 Type the VPN module DNS name — введите доменное имя ViPNet Prime VPN.

14.25 Type the VPN module IP address to resolve the <доменное имя ViPNet Prime VPN> to — введите IP-адрес, который соответствует доменному имени ViPNet Prime VPN.

14.26 Type the VPN module port — задайте порт ViPNet Prime VPN.

14.27 При необходимости включите совместимость со сторонними модулями.

15 Установка базовых компонентов продолжится. В результате мастер установки выведет запись об успешном конфигурировании базовых компонентов ViPNet Prime `Prime was successfully configured`.

16 [Сконфигурируйте сеть для контейнеров Docker](#).



Внимание! Сконфигурируйте сеть для контейнеров Docker. Если сеть не сконфигурировать, это приведёт к пересечению подсетей Docker и LAN и потери работоспособности ViPNet Prime.

17 Запустите ViPNet Prime:

```
$ sudo deployment-configurator start
```

18 Выберите ранее установленные компоненты и нажмите **Enter**.

```
Select at least one of the following options
(Use Arrow keys to navigate up and down, Space bar to select and Enter to submit)
[*] Core Key Center
[*] Transport Server
[*] VPN Key Center
[*] Core Management Services
[ ] Connect Module
--> [*] VPN Management Services
```

Рисунок 11. Выбор компонентов для запуска ViPNet Prime

19 На запрос **Enter master PIN** — задайте мастер-ПИН для слота программного токена для хранения закрытого ключа подписи токенов аутентификации. Затем подтвердите его. Рекомендуемая длина — от 10 до 20 символов с использованием букв, цифр и специальных символов — ! @ # \$ % ^ & _ = +.



Внимание! Запомните мастер-ПИН. Он необходим для доступа к ViPNet Prime. Восстановить его невозможно.

```
Creating nsm automatic-update-service_1 ... done
Creating nsm software-update-service_1 ... done
Creating nsm automatic-update-service_1 ... done
Creating nsm action-log-service_1 ... done
Creating nsm ncc-service_1 ... done
Creating nsm configuration-service_1 ... done
Creating nsm smp-gateway-service_1 ... done
Started component. ComponentId=vpn-ms
Connecting to prime-control daemon...
Master PIN is not initialized, creating
Enter master PIN: *****
Confirm master PIN: *****
```

Рисунок 12. Задание мастер-ПИНа

Первое подключение к ViPNet Prime

1 В браузере введите:

`https://<доменное имя ViPNet Prime>:<порт>.`

2 При первом входе укажите:

- имя учётной записи — `admin`;
- пароль — `P@ssw0rd`.

Вы войдёте с правами суперадминистратора. Ожидайте загрузки интерфейса. При запуске ViPNet Prime проводит стартовый контроль целостности своих компонентов, и в браузере может отображаться сообщение, что приложение работает в режиме ограниченной функциональности.

- ### 3
- Для работы с сетью VPN загрузите лицензию для ViPNet Prime и распределите лицензии для устройств Control Center и Core Coordinator, см. «ViPNet Prime. Руководство администратора», «Загрузка и обновление лицензии» и «Создание центра управления и его координатора».
- ### 4
- Зарегистрируйте ViPNet Prime VPN, см. «ViPNet Prime. Руководство администратора», «Подключение модулей к ViPNet Prime».

При переходе в ViPNet Prime VPN могут не отображаться алгоритмы шифрования. Это связано с тем, что инициализация ещё не завершена. Дождитесь завершения инициализации.

Установка ViPNet Prime PMM

Ограничения

- устанавливается на один компьютер с базовыми компонентами ViPNet Prime;
- не поддерживает работу с конфигуратором deployment-configurator.

Предварительные действия

1 Установите [базовые компоненты ViPNet Prime](#).

2 В ViPNet Prime VPN создайте:

- сеть организации;
- устройства — центр управления и его координатор.

См. «ViPNet Prime. Руководство администратора», раздел «Создание центра управления и его координатора».

3 Выясните ViPNet-адрес и [идентификатор узла](#) центра управления Control Center в ViPNet Prime VPN.

- ViPNet-идентификатор — шестнадцатеричный идентификатор вида XXXXYYYY, где XXXX — номер защищённой сети, YYYY — идентификатор сетевого узла.
- ViPNet-адрес — шестнадцатеричный сетевой адрес вида XXXXYYYYZZZZ, где XXXX — номер защищённой сети, YYYY — номер координатора, ZZZZ — номер клиента, зарегистрированного за координатором.

Например, на рисунке ниже ViPNet-идентификатор сетевого узла — 41680002. Первые четыре цифры 4168 — это шестнадцатеричный номер защищённой сети, на которую выдан файл лицензии, вторая часть идентификатора 0002 — это порядковый шестнадцатеричный номер сетевого узла. ViPNet-адрес — 416800010001. Номер сетевого узла (0002) необходимо указать при установке ViPNet Prime PMM. Номер присваивается узлу при его создании автоматически. Значение ViPNet-адреса (416800010001) вводится при установке ViPNet Prime PMM полностью.

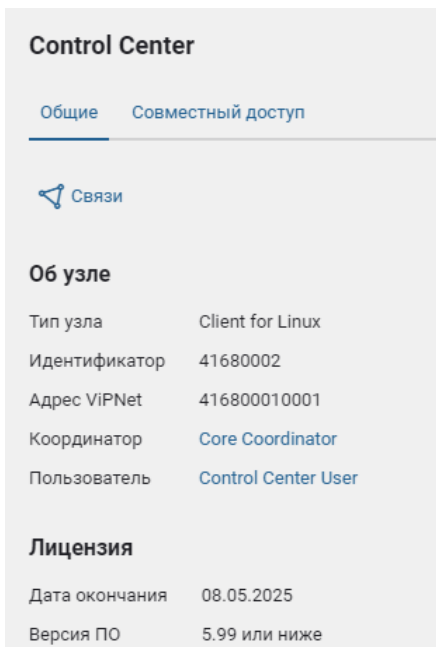


Рисунок 13. Просмотр информации о сетевом узле

Установка

- 1 На компьютере с ViPNet Prime перейдите в папку с архивом ПО ViPNet Prime PMM:

```
$ cd /infotecs/1.9.14/pmm.prime.<номер_версии>
```

- 2 Распакуйте архив с ПО:

```
$ sudo tar -xvzf pmm.tgz
```

- 3 Сконфигурируйте ViPNet Prime PMM:

```
$ sudo ./installer/configure
```

Следуйте указаниям установщика. Установщик автоматически задаёт некоторые параметры. В этом случае подтвердите значение или измените его:

- **Type the Policy Management module DNS name** — введите доменное имя ViPNet Prime PMM.
- **Type the Policy Management module internal port** — введите внутренний порт ViPNet Prime PMM.



Внимание! Не используйте номера портов, которые ранее были заданы в ViPNet Prime (ViPNet Prime Core) и номер порта ViPNet Prime VPN, иначе ViPNet Prime PMM не запустится. Запретите доступ из внешней сети к порту ViPNet Prime PMM.

- **Ready to install. Would you like to load docker images and apply the settings? (y/n)?** — запрос на подтверждение настроек, запись и загрузку образов в Docker. Введите **y**, чтобы согласиться.

- 4 Запустите ViPNet Prime PMM:

```
$ sudo ./up.sh
```

Если в вашей сети есть узлы поколения ViPNet 4, после установки модуля назначьте функцию управления политиками безопасности этому узлу. См. «ViPNet Prime Policy Management. Руководство администратора», раздел «Назначение функции управления политиками безопасности».

Установка ViPNet Prime NVS

Ограничения

- При повторной установке ViPNet Prime NVS не вносит изменения в файл `/etc/hosts/`. При необходимости внесите изменения в файл вручную.
- Используйте один сертификат сервера для ViPNet Prime и модулей, который подходит под все доменные имена модулей (в поле SAN должны быть указаны доменные имена ViPNet Prime и модулей).

Установка ViPNet Prime NVS

В зависимости от того, где вы устанавливаете ViPNet Prime NVS (на одном компьютере с ViPNet Prime или на отдельном), выполняйте нижеописанные действия там.

- 1 Если вы устанавливаете ViPNet Prime NVS на отдельный компьютер, [подготовьте ОС](#) для установки.
- 2 Если в ОС включен режим ЗПС, выполните команду:

```
$ sudo export COMPOSE_HTTP_TIMEOUT=300
```
- 3 Запустите установку ViPNet Prime NVS:
 - 3.1 Запустите конфигуратор:

```
$ sudo deployment-configurator install
```
 - 3.2 Выберите компонент **Monitoring module**.
- 4 Следуйте шагам установки:
 - 4.1 **Type the path to the monitoring module's trusted CA certificate (ca.crt)** — введите путь к сертификату корневого УЦ, например, `/infotecs/certs/ca.crt`.
 - 4.2 **Type the path to the monitoring module certificate (nginx.crt)** — введите путь к сертификату сервера ViPNet Prime NVS, например, `/infotecs/certs/nginx.crt`.
 - 4.3 **Type the path to the private key associated with the monitoring module certificate (nginx.key)** — введите путь к закрытому ключу сертификата сервера ViPNet Prime NVS, например, `/infotecs/certs/nginx.key`.
 - 4.4 **Do you want to install monitoring module on the same computer as ViPNet Prime? (y/n)** — введите `y`, если установка ViPNet Prime NVS происходит на один компьютер с базовыми компонентами ViPNet Prime, `n` — если на отдельном компьютере.
 - 4.5 **Type the Core IP address** — укажите IP-адрес ViPNet Prime Core. Укажите значение, которое задали на аналогичном шаге в разделе [Установка базовых компонентов](#).
 - 4.6 **Type the Core DNS name** — укажите доменное имя ViPNet Prime Core. Укажите значение, которое задали на аналогичном шаге в разделе [Установка базовых компонентов](#).
 - 4.7 **Type the Core port** — порт доступа к ViPNet Prime Core. Укажите значение, которое задали на аналогичном шаге в разделе [Установка базовых компонентов](#).

- 4.8 Type the monitoring module IP address** — укажите IP-адрес, на котором будет развёрнут модуль NVS. Если модуль устанавливается на одном компьютере с ViPNet Prime, данный шаг не появляется.
- 4.9 Type the monitoring module DNS name** — укажите доменное имя ViPNet Prime NVS.
- 4.10 Type the monitoring module port** — укажите порт доступа к ViPNet Prime NVS.
- 4.11 Type the monitoring module NATS broker port** — порт брокера сообщений NATS. Используется для подключения сборщиков данных и шлюзов, передающих счетчики срабатывания правил. По умолчанию — 4222.
- 4.12 Type the monitoring module Public Sink URL** — публичный URL конечной точки приёма данных по протоколу HTTPS для устройств открытой сети. Должен заканчиваться на `/sink`. Например, `https://nvs.domain/sink`, где `nvs.domain` — доменное имя сервера ViPNet Prime NVS.
- 4.13 Type the monitoring module public NATS URL** — публичный URL точки подключения NATS (адрес ViPNet Prime). Например, `nats://prime.example.ru:4222`, где `prime.example.ru` — доменное имя ViPNet Prime, 4222 — порт брокера сообщений NATS.
- 4.14 Do you want to preform NVS MongoDB migration to a new version? (y/n)** – введите `n`, если вы устанавливаете ViPNet Prime NVS впервые. При обновлении ViPNet Prime NVS введите `y`.

Настройка окружения

- 1** Перейдите в папку с ПО ViPNet Prime NVS:

```
$ cd /infotecs/1.9.14/nvs.prime.<номер_версии>/nvs
```

- 2** С учетом вычислительных ресурсов компьютера задайте ограничения в файле `docker-compose.limit.yml`.

По умолчанию используются значения, удовлетворяющие минимальным требованиям.

- 3** Перезагрузите ViPNet Prime NVS, чтобы применить настройки окружения:

- 3.1** Выполните команду:

```
$ sudo deployment-configurator stop
```

- 3.2** Выберите **Monitoring module**.

- 3.3** Выполните команду:

```
$ sudo deployment-configurator start
```

- 3.4** Выберите **Monitoring module**.

Установка ViPNet Prime NVS

Сборщик данных

- 1 Если на сервере, где устанавливается сборщик данных используется самоподписанный сертификат, добавьте его в список доверенных сертификатов. Для этого скопируйте его в папку `/usr/local/share/ca-certificates` и примените изменения с помощью команды:

```
$ sudo update-ca-certificates
```

- 2 Перейдите в папку со сборщиком данных:

```
$ cd /infotecs/1.9.14/nvs-rc-<номер_версии>/
```

- 3 Установите DEB-пакет:

```
$ sudo dpkg -i ./nvs-rc.deb
```

- 4 Если вы устанавливаете сборщик данных на Ubuntu, может появиться запрос на перезагрузку служб. Отклоните его, нажмите **<Cancel>**.

- 5 На запрос **Which user vipnetclient is installed/run under?** — введите имя пользователя, от имени которого установлены ключи в ViPNet Client 5 for Linux.

- 6 Остановите работу сборщика данных:

```
$ sudo systemctl stop nvs-rc
```

- 7 В ViPNet Prime отправьте справочники и ключи на узлы защищённой сети вручную.

- 8 Проверьте соединение узла Control Center с любым узлом в домене .vipnet:

```
$ ping -n <ViPNet-идентификатор_узла>.vipnet
```

Если соединение отсутствует, убедитесь, что выполнены рекомендации по настройке работы с DNS для ViPNet Client, см. «ViPNet Client 5 for Linux. Руководство администратора», раздел «Рекомендации по настройке работы с DNS».

- 9 Запустите сборщик данных:

```
$ sudo systemctl start nvs-rc
```

Установка ViPNet Connect Book

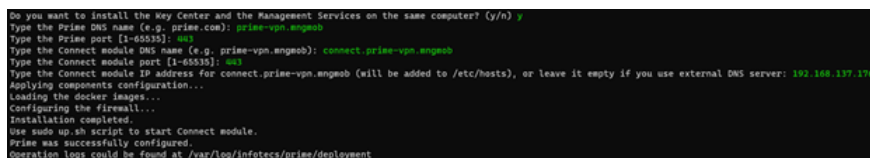
Ограничение

Установка ViPNet Connect Book возможна только на компьютере с ViPNet Prime.

Установка

- 1 **Установите базовые компоненты.**
- 2 Для настройки ViPNet Connect Book выполните команду с параметром `--no-start`, чтобы после установки модуль автоматически не запустился:

```
$ sudo deployment-configurator install --no-start
```
- 3 Выберите **Connect Module** как на рисунке ниже и нажмите **Enter**.
- 4 Следуйте шагам установки:
 - 4.1 **Do you want to install the Key Center and the Management Services on the same computer** — введите `y`, так как компоненты ViPNet Prime MS и ViPNet Prime KC установлены на одном компьютере.
 - 4.2 **Type the Prime DNS name** — введите доменное имя ViPNet Prime Core.
 - 4.3 **Type the Prime port** — введите порт ViPNet Prime Core.
 - 4.4 **Type the Connect module DNS name** — введите имя ViPNet Connect Book.
 - 4.5 **Type the Connect module port** — введите внешний порт ViPNet Connect Book. По умолчанию 443.
 - 4.6 **Type the Connect module IP address for <доменное имя модуля ViPNet Connect Book> (will be added to /etc hosts), or leave it empty if you use external DNS server** — введите IP-адрес ViPNet Connect Book для подключения к доменному имени ViPNet Connect Book (будет добавлен в `/etc/hosts`). Если вы используете внешний DNS-сервер, пропустите шаг.



```
Do you want to install the Key Center and the Management Services on the same computer? (y/n) y
Type the Prime DNS name (e.g. prime.com): prime-vpn.angelsb
Type the Prime port [1-65535]: 443
Type the Connect module DNS name (e.g. prime-vpn.angelsb): connect.prime-vpn.angelsb
Type the Connect module port [1-65535]: 443
Type the Connect module IP address for connect.prime-vpn.angelsb (will be added to /etc/hosts), or leave it empty if you use external DNS server: 192.168.137.170
Applying components configuration...
Loading the docker images...
Configuring the firewall...
Installation completed.
Use made up .sh script to start Connect module.
Prime was successfully configured.
Operation logs could be found at /var/log/infotecs/prime/deployment
```

Рисунок 14. Установка ViPNet Connect Book

- 5 Чтобы запустить ViPNet Connect Book:
 - 5.1 Выполните команду:

```
$ sudo deployment-configurator start
```
 - 5.2 Выберите **Connect Module** и нажмите **Enter**.

```

(Use Arrow keys to navigate up and down, Space bar to select and Enter to submit)
[ ] Core Key Center
[ ] Transport Server
[ ] VPN Key Center
[ ] Core Management Services
--> [*] Connect Module
[ ] VPN Management Services
Starting components...

Up Connect module, 2024-05-24 12:20:05+03:00

-----
      Connect module
-----
Creating network "connect_module_connect-module-net" with the default driver
Creating connect_module_postgresql_1 ...
Creating connect_module_nginx_1      ...
Creating connect_module_nginx_1      ... done
Creating connect_module_postgresql_1 ... done
Creating connect_module_core_1       ...
Creating connect_module_core_1       ... done
Started component. ComponentId=connect
Prime was successfully configured.
Operation logs could be found at /var/log/infotecs/prime/deployment

```

Рисунок 15. Запуск ViPNet Connect Book

Обновление ViPNet Prime

Особенности и ограничения

- При обновлении компонентов ViPNet Prime не изменяйте порты и доменные имена модулей, иначе придётся повторно установить ПО и указать предыдущие значения доменных имён и портов, затем подключить модули заново.
- Перед обновлением на версию 1.9.14 уточните совместимость модулей и ViPNet Prime (см. документацию к модулям).
- После обновления ViPNet Prime VPN и ViPNet Prime PMM повторно примите его регистрацию (см. «ViPNet Prime. Руководство администратора», «Подключение модулей к ViPNet Prime»).
- В ViPNet Prime версии 1.9.14 изменились поддерживаемые версии ОС. Перед обновлением ViPNet Prime обновите ОС до поддерживаемой версии.

Последовательность обновлений

Обновляйте ViPNet Prime, как показано на рисунке ниже.



Внимание! Возврат к более ранней версии приведёт к нарушению работоспособности ViPNet Prime.

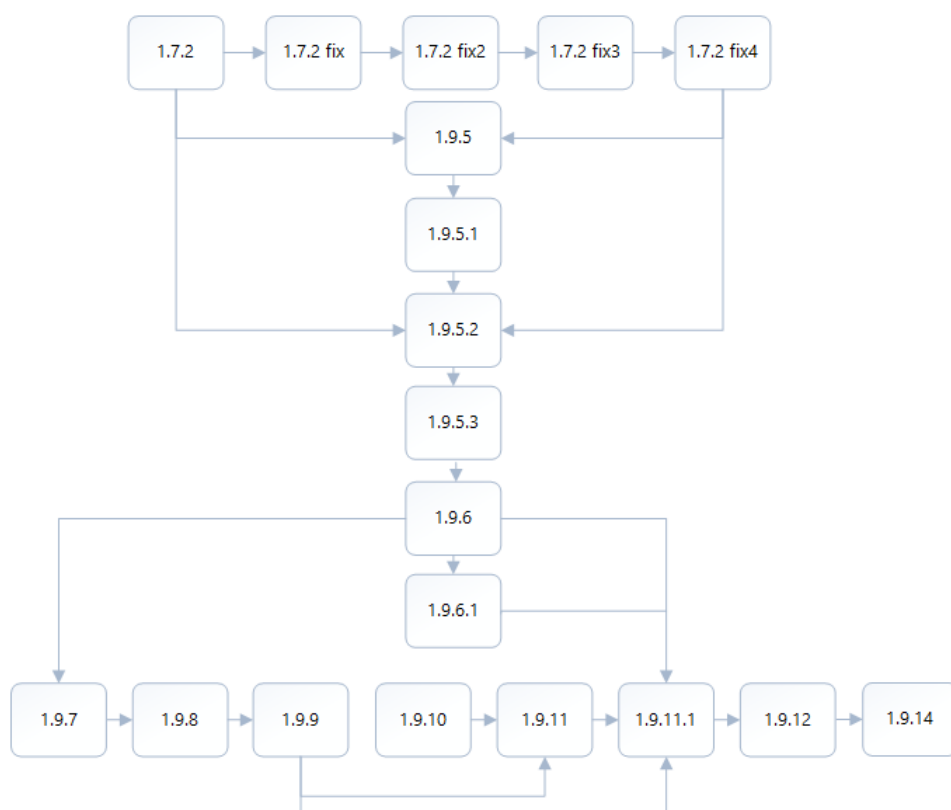


Рисунок 16. Обновление ViPNet Prime

Ниже описано обновление всех модулей ViPNet Prime.

Предварительные действия

Перед обновлением ViPNet Prime обновите ОС до поддерживаемой версии.

Обновление



Внимание! После обновления ViPNet Prime запустите все модули, иначе стартовый контроль завершится ошибкой.

- 1 Создайте резервную копию ViPNet Prime. Она пригодится, если работоспособность ViPNet Prime после обновления будет нарушена.
- 2 Отключите автоматическую отправку СКИ.
- 3 При необходимости обновите Astra Linux SE до поддерживаемой в ViPNet Prime версии 1.9.14.
- 4 Если вы обновляли Astra Linux SE с версии 1.8.1.16 на 1.8.3.8 или 1.8.5.46, удалите пакет `docker compose`:

```
$ sudo apt remove docker-compose
```

- 5 [Установите пакеты](#) для работы ViPNet Prime.
- 6 [Проверьте ЭП файлов](#) обновления ViPNet Prime.

- 7 Если вы используете `kesl`, добавьте в исключения `kesl` цепочку сертификатов:

```
$ sudo kesl-control --add-certificate /infotecs/certs/nginx.crt  
$ sudo systemctl restart kesl
```

Проверьте наличие свободного места в разделе, на котором установлен ViPNet Prime:

```
$ df -h /dev/<имя раздела, например, sda1>
```

Размер свободного пространства должен быть минимум в три раза больше занятого. Это потребуется при обновлении ViPNet Prime NVS и ViPNet Prime PMM. После обновления место освободится.

- 8 Создайте папку для установочных файлов ViPNet Prime версии 1.9.14, например, `/infotecs/1.9.14`:

```
$ sudo mkdir -p /infotecs/1.9.14
```
- 9 Разместите содержимое папки с ПО в папке `/infotecs/1.9.14`.
- 10 Остановите работу ViPNet Prime и модулей:

- 10.1 Чтобы остановить базовые компоненты и ViPNet Connect Book:

```
$ sudo deployment-configurator stop --all
```

- 10.2 Остановите работу ViPNet Prime NVS (если ViPNet Prime NVS установлен на отдельном компьютере, выполните команду на нём):

```
$ cd /infotecs/1.9.12/nvs.prime.<номер_версии>/nvs
```

```
$ sudo ./down.sh
```

10.3 Остановите работу ViPNet Prime PMM:

```
$ sudo /usr/share/infotecs/prime/deployment/pmm/down.sh
```

11 Обновите базовые компоненты ViPNet Prime, ViPNet Prime NVS и ViPNet Connect Book:

11.1 Перейдите в папку /infotecs/1.9.14:

```
$ cd /infotecs/1.9.14
```

11.2 Распакуйте архив с ПО:

```
$ sudo find . -name "extract-dist.sh" -exec chmod +x {} \; -exec {} -c \;
```

11.3 Если вы обновляете ViPNet Prime на Astra Linux SE, запустите скрипт `install-signature-keys.sh`:

```
$ sudo /usr/share/infotecs/prime/deployment/core-kc/install-signature-keys.sh
```

11.4 Запустите конфигуратор для обновления базовых компонентов, ViPNet Prime NVS и ViPNet Connect Book (если ViPNet Prime NVS установлен на отдельном компьютере, также выполните команду на нём):

```
$ sudo deployment-configurator install --no-start
```



Внимание! При обновлении ViPNet Prime на Ubuntu на вопрос **There are some problems with installing PostgreSQL. Want to proceed** введите **Y**.

11.5 Установите базовые компоненты новой версии — выполните пункты 11-15 из раздела [Установка базовых компонентов](#). Установщик будет автоматически подставлять значения, которые вы указывали при первой установке. Не изменяйте значения доменных имён модулей и портов. Вы можете:

- изменить источник случайных чисел;
- указать новый сертификат сервера и ключ;
- добавить или указать новый TLS ГОСТ-сертификат.



Внимание! Во время установки базовых компонентов ViPNet Prime 1.9.14 появится новый шаг **Type PostgreSQL password**. Введите пароль для базы данных PostgreSQL.

11.6 Если при установке базовых компонентов появится предупреждение `NetworkManger is unavailable. This may cause the software to malfunction. For the software to function correctly, make sure that NetworkManger is on. You can turn on NetworkManger after the installation is complete`, завершите установку ViPNet Prime и запустите NetworkManager:

```
$ sudo apt install network-manager  
$ sudo systemctl unmask NetworkManager  
$ sudo systemctl enable NetworkManager  
$ sudo systemctl start NetworkManager
```

12 Обновите ViPNet Prime PMM:

12.1 Перейдите в папку с архивом новой версии ViPNet Prime PMM:

```
$ cd /infotecs/1.9.14/pmm.prime.<номер_версии>
```

12.2 Распакуйте архив `pmm.tgz`:

```
$ sudo tar -xvzf pmm.tgz
```

12.3 Настройте ViPNet Prime PMM:

```
$ sudo ./installer/configure
```

12.4 Установщик будет автоматически подставлять значения, которые вы указывали при первой установке. Вы можете принять заданные значения или изменить их.

12.5 В ответ на вопрос **Setup is completed. Would you like to load docker images, migrate database and write configuration? (y/n)** введите **y**, чтобы согласиться с результатом конфигурирования, загрузкой образов в Docker и переносом базы данных.

13 Обновите сборщик данных:

13.1 Остановите сборщик данных:

```
$ sudo systemctl stop nvs-rc
```

13.2 Установите пакет `libcurl4`:

```
$ sudo apt install libcurl4
```

13.3 Перейдите в папку с новой версией сборщика данных:

```
$ cd /infotecs/1.9.14/nvs-rc-<номер_версии>
```

13.4 Установите сборщик данных:

```
$ sudo dpkg -i ./nvs-rc.deb
```

14 [Сконфигурируйте сеть для контейнеров Docker.](#)



Внимание! Сконфигурируйте сеть для контейнеров Docker. Если сеть не сконфигурировать, это приведёт к пересечению подсетей Docker и LAN и потери работоспособности ViPNet Prime.

15 [Запустите базовые компоненты ViPNet Prime.](#)

16 Введите мастер-ПИН.

17 [Запустите остальные модули ViPNet Prime.](#)

18 Проверьте работоспособность модулей в веб-браузере. Если есть запросы на подключение модулей, подключите их к ViPNet Prime (см. «ViPNet Prime. Руководство администратора», раздел «Подключение модулей к ViPNet Prime»).

19 Удалите Docker-образы предыдущей версии:

19.1 Выполните команду:

```
$ docker ps -a
```

Убедитесь, что контейнеры имеют статус `up` или `up (healthy)`.

19.2 Выполните команду:

```
$ docker image prune -a
```

19.3 В ответ на вопрос **WARNING! This will remove all image without at least one container associated to them. Are you sure you want to continue? [y/N]** введите **y**.

5

Администрирование и настройка

Установка, обновление и настройка коннектора Active Directory	69
Управление службами ViPNet Prime	78
Смена IP-адреса ViPNet Prime	81
Освобождение дискового пространства	84
Настройка журналов ViPNet Prime	85
Просмотр журналов ViPNet Prime	89
Пересечение подсетей Docker и LAN	92
Просмотр версии ViPNet Prime	94
Запрет входящих соединений к ViPNet Prime Key Center Nginx	95
Установка сертификатов TLS ГОСТ	97

Установка, обновление и настройка коннектора Active Directory

Если в организации используется служба каталогов Active Directory (далее — AD), учётные записи пользователей можно импортировать в ViPNet Prime.

Если организация предоставляет поставщику услуг доступ к компьютеру с установленным Active Directory, импорт записей может выполнить суперадминистратор. В остальных случаях импорт записей в ViPNet Prime выполняют владелец организации или администратор организации.

Коннектор AD — это веб-служба Pear, которая выгружает учётные записи пользователей из AD и передает их в ViPNet Prime. Коннектор AD входит в поставку ViPNet Prime и устанавливается как сайт веб-сервера Microsoft IIS на компьютере домена. У него должен быть сетевой доступ до контроллера домена.

Для безопасной передачи данных между компьютером с AD и компьютером с Prime по TLS/HTTPS скрипт коннектора AD устанавливает сертификат для сайта Pear. В закрытой сетевой инфраструктуре вы можете не устанавливать TLS-сертификат, но тогда данные из AD будут передаваться в ViPNet Prime по HTTP.

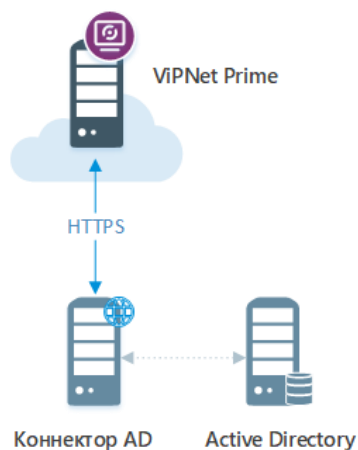


Рисунок 17. Соединения между коннектором AD и ViPNet Prime

Для импорта учётных записей пользователей в ViPNet Prime:

- 1 Установите и настройте коннектор AD.
- 2 В ViPNet Prime настройте параметры импорта из AD и параметры подключения к AD. См. «ViPNet Prime. Руководство администратора», раздел «Настройка интеграции с Active Directory».

- 3 В ViPNet Prime импортируйте учётные записи пользователей из AD. См. «ViPNet Prime. Руководство администратора», раздел «Импорт учетных записей пользователей из Active Directory».

Предварительные действия

- 1 На компьютере с AD установите:
 - Microsoft Internet Information Services (IIS) и включите роль веб-сервера IIS.
 - [ASP.NET Core Hosting Bundle](#).
 - 2 Если компьютер с Prime и коннектор AD располагаются в сети одной организации, для доменного имени коннектора AD вы можете использовать собственный сертификат вашего корпоративного УЦ. В этом случае обеспечьте доверие к такому сертификату. Для этого установите корневой сертификат вашего УЦ на обоих компьютерах.
 - 3 Если компьютер с ViPNet Prime расположен в сети поставщика услуг, а коннектор AD располагается в сети организации-потребителя, используйте сертификат с публичным доверием и проверкой подлинности доменного имени коннектора Active Directory.
 - 4 В поле сертификата Subject Alternative Name укажите доменное имя для веб-сервера коннектора Active Directory (сайта в IIS).
- Экспортируйте файл сертификата и связанный файл закрытого ключа в формате PFX (PKCS#12).
- Установите сертификат на компьютере с AD с помощью скрипта установки `install-pear.ps1` из комплекта поставки.

Установка и обновление коннектора AD

- 1 Сохраните копию файла `appsettings.json`, если вы обновляете коннектор AD.
- 2 Удалите установочные файлы коннектора AD предыдущей версии.
- 3 Создайте папку, которая будет соответствовать корню сайта. Например, `C:\pear`.
- 4 В папку `C:\install\` скопируйте:
 - папку `script`;
 - установочный скрипт — `install-pear.ps1`;
 - установочный файл коннектора AD — `Pear.Service.<номер версии>.zip`;
 - файл `*.pfx`.
- 5 Перейдите в папку `C:\install\` и запустите скрипт установки от имени администратора через PowerShell:

```
.\install-pear.ps1 -installDir <путь к папке установки> -port <номер порта коннектора AD> -updateCertificate true -certificate <путь к сертификату *.pfx> -certificatePassword <пароль от *.pfx> -webAppName <имя сайта IIS>
```

Например:

```
.\install-pear.ps1 -installDir C:\pear -port 8095 -siteHost https://<адрес Prime Core>:<порт>/auth -updateCertificate true -certificate C:\install\certificate.pfx -certificatePassword <пароль> -webAppName pear
```

Где:

- `-installDir` — папка установки. Если параметр не указан, коннектор AD будет установлен в папку по умолчанию `C:\pear`.
- `-port` — номер порта, по которому будет доступен коннектор AD (служба `PearServices`). Если параметр не указан, будет использоваться порт по умолчанию `8095`.
- `-silsoHost` — URL службы аутентификации `Silso` в составе `ViPNet Prime`.
- `-updateCertificate {true | false}` — параметр установки или обновления информации о сертификате. Указывается при установке и обновлении сертификата:
 - `true` — установить или обновить информацию о сертификате;
 - `false` — не устанавливать сертификат или не обновлять информацию о нём.
- `-certificate` — путь к файлу в формате `PFX`. Используется только при заданном параметре `updateCertificate`. По умолчанию `.\certificate.pfx`.
- `-certificatePassword` — пароль, на котором зашифрован сертификат при издании в УЦ. Используется только при заданном параметре `updateCertificate`.
- `-webAppName` — имя сайта IIS. По умолчанию `pear`.

Скрипт создаст и настроит сайт в IIS, а также установит сертификат в хранилище сертификатов.

По умолчанию в IIS для сайта будет создана привязка (site bindings) HTTPS с портом `8095`.

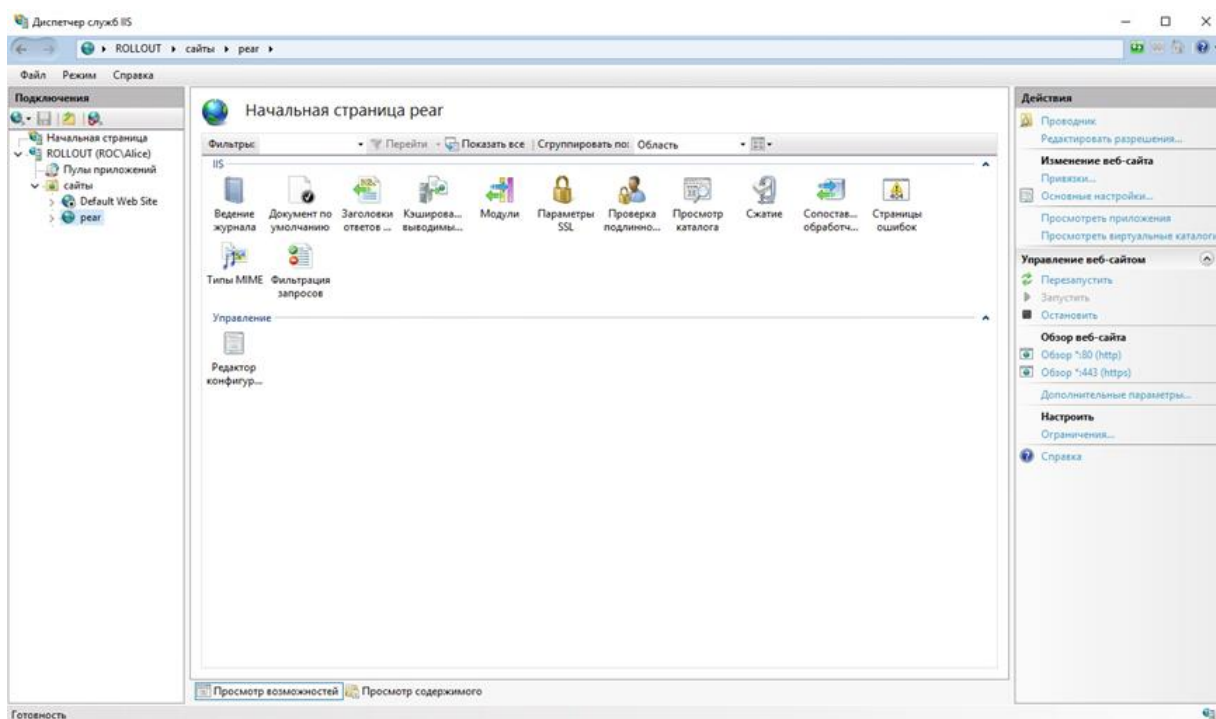


Рисунок 18. Сайт Pear в диспетчере служб IIS

Настройка коннектора AD

- 1 Откройте **Панель управления > Администрирование > Диспетчер служб IIS**.
- 2 В окне **Диспетчер служб IIS** на панели **Подключения** выберите сайт pear.
- 3 На панели **Действия** нажмите **Проводник**. Откроется папка с файлами службы.
- 4 Откройте файл конфигурации службы `appsettings.json` в текстовом редакторе от имени администратора.
- 5 Укажите параметры конфигурации и сохраните изменения в файле.

Таблица 9. Параметры `appsettings.json`

Название	Описание
AuthenticationConfiguration (служба аутентификации)	
<code>AuthenticationConfiguration.Authority</code>	URL службы аутентификации ViPNet Prime <code>https://<доменное имя Prime>:<порт>/auth</code>
ActiveDirectory	
<code>ActiveDirectory.LdapUsername</code>	Имя учётной записи пользователя LDAP
<code>ActiveDirectory.LdapPassword</code>	Пароль пользователя LDAP
<code>ActiveDirectory.LdapDirectoryPath</code>	Путь к каталогу LDAP. Не используйте русские буквы
<code>ActiveDirectory.LdapMaxPageSize</code>	Значение политики <code>MaxPageSize</code> для LDAP-сервера. По умолчанию параметр отсутствует в файле.
<code>ActiveDirectory.OrganizationId</code>	Уникальный идентификатор для организации. Генерируется в ViPNet Prime в окне настроек импорта пользователей из Active Directory. Пример: <code>pear-d0d7280c-d629-40e3-9f7b-aaf100c62b5f</code> См. «ViPNet Prime. Руководство администратора», раздел «Настройка интеграции с Active Directory»

Пример конфигурации:

```
{
  "AuthenticationConfiguration": {
    "Authority": "https://<адрес Prime>:<порт>/auth"
  },
  "ActiveDirectory": {
    "LdapUsername": "example.ad\\Alind1988",
    "LdapPassword": "Ct162@G1G%378rS",
    "LdapDirectoryPath": "LDAP://ads-01.example.ru/CN=Users;DC=example;DC=ad",
```

```
"LdapMaxPageSize": 1000,  
  
"OrganizationId": "pear-a0adbac0-93d2-45c2-b872-aa0800891518"  
}
```



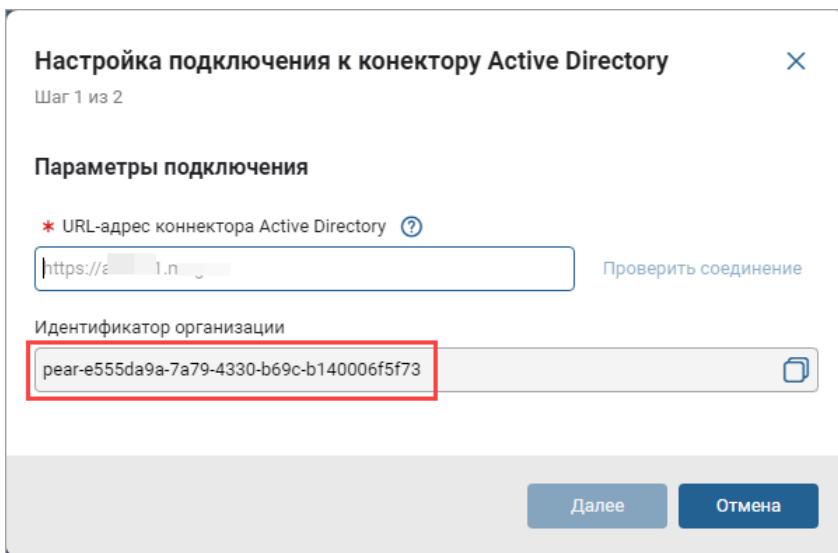
Примечание. В файле конфигурации JSON экранируйте специальные символы. Например, символ «\» замените на «\\», «"» — на «\"». См. [RFC JSON](#).

6 Идентификатор организации скопируйте из настроек импорта пользователей из Active Directory и укажите в качестве параметра `ActiveDirectory.OrganizationId`. Для этого:

6.1 В Prime выберите **Управление организацией > Импорт данных**.

6.2 Нажмите **Настроить**.

6.3 Нажмите , чтобы скопировать идентификатор организации в буфер обмена.



Настройка подключения к конектору Active Directory

Шаг 1 из 2

Параметры подключения

* URL-адрес конектора Active Directory ?

https://... .n

Проверить соединение

Идентификатор организации

pear-e555da9a-7a79-4330-b69c-b140006f5f73

Далее Отмена

Рисунок 19. Просмотр идентификатора организации

7 Чтобы использовать HTTP для конектора AD, в настройках сайта IIS измените тип привязки сайта с HTTPS на HTTP.

8 Для применения настроек конектора к AD перезапустите сайт IIS.

9 Чтобы узнать версию конектора AD обратитесь к нему по адресу. В зависимости от типа привязки сайта, введите:

- o `http://localhost:<порт>/hc`
- o `https://localhost:<порт>/hc`

Порт вы можете посмотреть в диспетчере служб IIS в свойствах привязок (site bindings) веб-сайта.

Импорт учетных записей из одного домена Active Directory на несколько серверов с ViPNet Prime

При необходимости вы можете импортировать данные из одного домена Active Directory на несколько серверов с ViPNet Prime. Для этого установите на компьютер с Active Directory несколько экземпляров коннектора (свой для каждого сервера с ViPNet Prime).

Ниже описан вариант настройки импорта данных с одного домена Active Directory на два сервера с ViPNet Prime.

Предварительные действия

- 1 На компьютере с AD установите:
 - Microsoft Internet Information Services (IIS) и включите роль веб-сервера IIS.
 - [ASP.NET Core Hosting Bundle](#).
- 2 Если компьютер с ViPNet Prime и коннектор AD располагаются в сети одной организации, для доменного имени коннектора AD вы можете использовать собственный сертификат вашего корпоративного УЦ. В этом случае обеспечьте доверие к такому сертификату. Для этого установите корневой сертификат вашего УЦ на обоих компьютерах.
- 3 Если компьютер с ViPNet Prime расположен в сети поставщика услуг, а коннектор AD располагается в сети организации-потребителя, используйте сертификат с публичным доверием и проверкой подлинности доменного имени коннектора Active Directory.
- 4 В поле сертификата `Subject Alternative Name` укажите доменное имя для веб-сервера коннектора Active Directory (сайта в IIS).

Экспортируйте файл сертификата и связанный файл закрытого ключа в формате PFX (PKCS#12).

Установите сертификат на компьютере с AD с помощью скрипта установки `install-pear.ps1` из комплекта поставки.

Установка коннектора AD

- 1 Установите корневые сертификаты на компьютер с Active Directory.
- 2 Создайте папки, которые будут соответствовать корню для каждого сайта. Например, `C:\FirstPear` для первого и `C:\SecondPear` для второго.
- 3 Создайте папку `C:\install\` скопируйте в неё:
 - папку `script`;
 - установочный скрипт — `install-pear.ps1`;
 - установочный файл коннектора AD — `Pear.Service.<номер версии>.zip`;
 - файлы сертификатов `*.pfx` с обоих серверов с ViPNet Prime.

4 Перейдите в папку C:\install\ и запустите скрипты для установки от имени администратора через PowerShell:

```
.\install-pear.ps1 -installDir <путь к папке установки> -port <номер порта  
коннектора AD> -updateCertificate true -certificate <путь к сертификату *.pfx> -  
certificatePassword <пароль от *.pfx> -webAppName <имя сайта IIS>
```

Например:

```
.\install-pear.ps1 -installDir C:\FirstPear -port 8095 -updateCertificate true -  
certificate cert.pfx -certificatePassword <пароль> -webAppName firstPear  
.\install-pear.ps1 -installDir C:\SecondPear -port 8098 -updateCertificate true -  
certificate cert2.pfx -certificatePassword <пароль> -webAppName secondPear
```

Где:

- o -installDir — папка установки. Если параметр не указан, коннектор AD будет установлен в папку по умолчанию C:\pear.
- o -port — номер порта, по которому будет доступен коннектор AD (служба PearServices). Для каждого коннектора укажите свой порт. Если параметр не указан, будет использоваться порт по умолчанию 8095.
- o -updateCertificate {true | false} — параметр установки или обновления информации о сертификате. Указывается при установке и обновлении сертификата:
 - true — установить или обновить информацию о сертификате;
 - false — не устанавливать сертификат или не обновлять информацию о нём.
- o -certificate — путь к файлу в формате PFX. Используется только при заданном параметре updateCertificate. По умолчанию .\certificate.pfx.
- o -certificatePassword — пароль, на котором зашифрован сертификат при издании в УЦ. Используется только при заданном параметре updateCertificate.
- o -webAppName — имя сайта IIS. По умолчанию pear.

Скрипт создаст и настроит сайт в IIS, а также установит сертификат в хранилище сертификатов.

По умолчанию в IIS для сайта будет создана привязка (site bindings) HTTPS с портом 8095.

5 Настройте коннектор AD:

- 5.1 Откройте **Панель управления > Администрирование > Диспетчер служб IIS**.
- 5.2 В окне **Диспетчер служб IIS** на панели **Подключения** выберите сайт pear.
- 5.3 На панели **Действия** нажмите **Проводник**. Откроется папка с файлами службы.
- 5.4 Откройте файл конфигурации службы appsettings.json в текстовом редакторе от имени администратора.
- 5.5 Укажите параметры конфигурации и сохраните изменения в файле.

Таблица 10. Параметры *appsettings.json*

Название	Описание
AuthenticationConfiguration (служба аутентификации)	
AuthenticationConfiguration.Authority	URL службы аутентификации ViPNet Prime https://<доменное имя ViPNet Prime>:<порт>/auth
ActiveDirectory	
ActiveDirectory.LdapUsername	Имя учётной записи пользователя LDAP
ActiveDirectory.LdapPassword	Пароль пользователя LDAP
ActiveDirectory.LdapDirectoryPath	Путь к каталогу LDAP. Не используйте русские буквы
ActiveDirectory.LdapMaxPageSize	Значение политики MaxPageSize для LDAP-сервера. По умолчанию параметр отсутствует в файле.
ActiveDirectory.OrganizationId	Уникальный идентификатор для организации. Генерируется в Prime в окне настроек импорта пользователей из Active Directory. Пример: pear-d0d7280c-d629-40e3-9f7b-aaf100c62b5f См. «ViPNet Prime. Руководство администратора», раздел «Настройка интеграции с Active Directory»

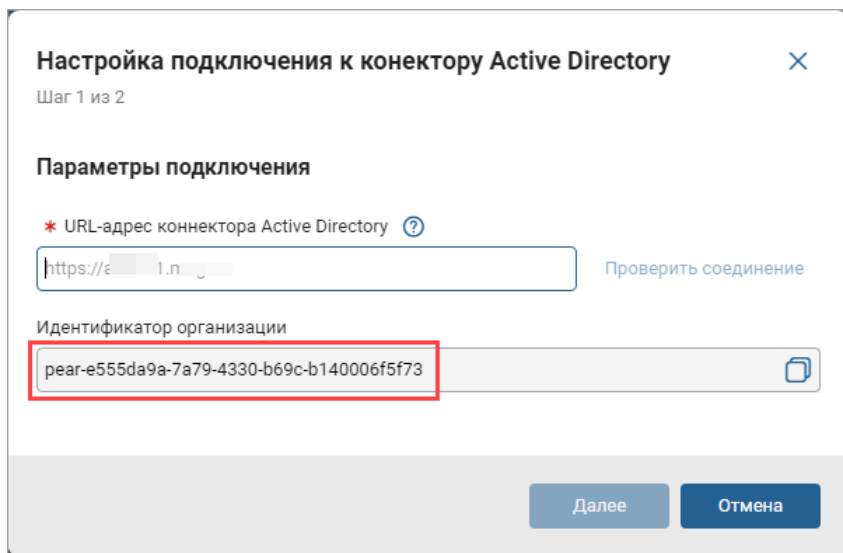
Пример конфигурации:

```
{
  "AuthenticationConfiguration": {
    "Authority": "https://<адрес ViPNet Prime>:<порт>/auth"
  },
  "ActiveDirectory": {
    "LdapUsername": "example.ad\\Alind1988",
    "LdapPassword": "Ct162@G1G%378rS",
    "LdapDirectoryPath": "LDAP://ads-01.example.ru/CN=Users;DC=example;DC=ad",
    "LdapMaxPageSize": 1000,
    "OrganizationId": "pear-a0adbac0-93d2-45c2-b872-aa0800891518"
  }
}
```



Примечание. В файле конфигурации JSON экранируйте специальные символы. Например, символ «\» замените на «\\», «"» — на «\"». См. [RFC JSON](#).

- 5.6 Скопируйте файл `appsettings.json` в папку второго коннектора и измените параметры для соединения со вторым сервером ViPNet Prime.
- 6 Идентификатор организации скопируйте из настроек импорта пользователей из Active Directory и укажите в качестве параметра `ActiveDirectory.OrganizationId`. Для этого:
- 6.1 В Prime выберите **Управление организацией > Импорт данных**.
- 6.2 Нажмите **Настроить**.
- 6.3 Чтобы скопировать идентификатор организации в буфер обмена нажмите .



Настройка подключения к коннектору Active Directory

Шаг 1 из 2

Параметры подключения

* URL-адрес коннектора Active Directory ?

https://... .n

Проверить соединение

Идентификатор организации

pear-e555da9a-7a79-4330-b69c-b140006f5f73

Далее Отмена

Рисунок 20. Просмотр идентификатора организации

Повторите эти действия на втором компьютере с ViPNet Prime.

- 7 Для применения настроек коннектора к AD перезапустите сайт IIS.

Управление службами ViPNet Prime

ViPNet Prime автоматически запускается при перезагрузке ОС вне зависимости от того, был ли он запущен или нет до перезагрузки ОС.

Имена служб и контейнеров см. в [Состав ViPNet Prime](#).

Скрипты:

- `up.sh`:
 - создаёт контейнеры Docker, если их нет;
 - запускает контейнеры, если они есть;
 - если настройки и версии контейнеров изменились, останавливает, удаляет, затем создаёт новые и запускает.
- `down.sh` — останавливает контейнеры Docker, затем удаляет их.

Команды `deployment-configurator start` и `deployment-configurator stop` запускают скрипты `up.sh` и `down.sh` выбранных модулей.

При каждой перезагрузке компьютера с ViPNet Prime:

- 1 Остановите работу ViPNet Prime и модулей.
- 2 Убедитесь, что Docker-контейнеры отсутствуют:

```
$ sudo docker ps -a
```
- 3 Запустите ViPNet Prime и модули.
- 4 Введите мастер-ПИН.

Одновременный запуск ViPNet Prime Core, ViPNet Prime VPN, ViPNet Prime NVS, ViPNet Connect Book, ViPNet UT

```
$ sudo deployment-configurator start --all
```

Одновременная остановка ViPNet Prime Core, ViPNet Prime VPN, ViPNet Prime NVS, ViPNet Connect Book, ViPNet UT

```
$ sudo deployment-configurator stop --all
```

ViPNet Prime KC

Для перезапуска служб ViPNet Prime KC:

```
$ sudo service <имя_службы> restart
```

Чтобы посмотреть имена служб:

```
$ ls /etc/systemd/system | grep '\.service$' | sed 's/\.service$//'  
$ systemctl list-units --type service --state running,failed
```

Перезапускайте ViPNet Prime Core и ViPNet Prime VPN части Key Center вместе:

- С помощью конфигуратора:

```
$ sudo deployment-configurator stop
```

Выберите **Core Key Center** и **VPN Key Center**.

```
$ sudo deployment-configurator start
```

- Если используете скрипты `down.sh` и `up.sh`, запускайте их в указанном порядке:

```
$ sudo /usr/share/infotecs/prime/deployment/vpn-kc/down.sh
```

```
$ sudo /usr/share/infotecs/prime/deployment/core-kc/down.sh
```

```
$ sudo /usr/share/infotecs/prime/deployment/vpn-kc/up.sh
```

```
$ sudo /usr/share/infotecs/prime/deployment/core-kc/up.sh
```

ViPNet Prime MS

Чтобы остановить, запустить или перезапустить ViPNet Prime Core и ViPNet Prime VPN части Management Services:

- С помощью конфигуратора:

```
$ sudo deployment-configurator stop
```

Выберите **Core Management Services** и **VPN Management Services**.

```
$ sudo deployment-configurator start
```

- Или если используете скрипты `down.sh` и `up.sh`:

```
$ sudo /usr/share/infotecs/prime/deployment/vpn-ms/down.sh
```

```
$ sudo /usr/share/infotecs/prime/deployment/core-ms/down.sh
```

```
$ sudo /usr/share/infotecs/prime/deployment/vpn-ms/up.sh
```

```
$ sudo /usr/share/infotecs/prime/deployment/core-ms/up.sh
```

ViPNet Prime NVS

- С помощью `deployment-configurator`:

```
$ sudo deployment-configurator stop
```

Выберите **Monitoring module**.

```
$ sudo deployment-configurator start
```

- С помощью скриптов:

```
$ cd /infotecs/1.9.14/nvs.prime.<номер_версии>
```

```
$ sudo ./down.sh
```

```
$ sudo ./up.sh
```

Для управления сборщиком данных используйте команды:

- Запуск:
`# sudo systemctl start nvs-rc`
- Остановка:
`# sudo systemctl stop nvs-rc`
- Перезапуск:
`# sudo systemctl restart nvs-rc`
- Просмотр статуса службы:
`# sudo systemctl status nvs-rc`

ViPNet Prime PMM

Чтобы перезапустить:

```
$ sudo /usr/share/infotecs/prime/deployment/pmm/down.sh  
$ sudo /usr/share/infotecs/prime/deployment/pmm/up.sh
```

ViPNet Connect Book

Чтобы перезапустить модуль:

- С помощью конфигуратора:
`$ sudo deployment-configurator stop`
Выберите **Connect Module**.
`$ sudo deployment-configurator start`
- Или с помощью скриптов:
`$ sudo /usr/share/infotecs/prime/deployment/connect/down.sh`
`$ sudo /usr/share/infotecs/prime/deployment/connect/up.sh`

Смена IP-адреса ViPNet Prime



Внимание! Перед сменой IP-адреса ViPNet Prime [создайте резервную копию](#) ViPNet Prime.

Если ViPNet Prime установлен на одном компьютере, то достаточно сменить только один адрес. Если ViPNet Prime установлен на двух компьютерах, вы можете сменить IP-адрес на обоих или только на одном из них.

ViPNet Prime установлен на одном компьютере

- 1 [Остановите работу](#) ViPNet Prime, модулей и сборщика данных.
- 2 Смените IP-адрес на сетевом интерфейсе компьютера штатными средствами ОС. Убедитесь, что интерфейсу назначен верный адрес.
- 3 В файле `/etc/hosts` измените IP-адреса, связанные с доменными именами модулей ViPNet Prime на новый адрес.
- 4 Запустите установку ViPNet Prime и модулей:

```
$ sudo deployment-configurator install --no-start
```
- 5 При запросе IP-адреса для каждого модуля укажите новый IP-адрес. Остальные параметры оставьте без изменения.
- 6 Укажите новый IP-адрес в файле `nvs.conf` в строке `allow <IP-адрес>` конфигурации Nginx для ViPNet Prime NVS:

```
$ sudo nano /etc/nginx/dynamic-routes/http/nvs/nvs.conf
```
- 7 [Запустите базовые компоненты ViPNet Prime.](#)
- 8 [Запустите остальные модули ViPNet Prime.](#)

ViPNet Prime NVS установлен на отдельном компьютере

- На компьютере А установлено:
 - ViPNet Prime Core;
 - ViPNet Prime VPN;
 - [транспортный сервер ViPNet UT](#);
 - ViPNet Prime PMM;
 - ViPNet Connect Book;
 - Сборщик данных.
- На компьютере Б установлен ViPNet Prime NVS.

Смена IP-адреса на компьютере А

Чтобы сменить IP-адрес на компьютере А, последовательно выполните действия сначала на компьютере А, затем на компьютере Б:

1 На компьютере А:

- 1.1 **Остановите работу** ViPNet Prime, модулей и сборщика данных.
- 1.2 Смените IP-адрес на сетевом интерфейсе компьютера штатными средствами ОС. Убедитесь, что интерфейсу назначен верный адрес.
- 1.3 В файле `/etc/hosts` измените IP-адреса, связанные с доменными именами модулей ViPNet Prime, на новый. Для доменного имени ViPNet Prime NVS укажите новый IP-адрес ViPNet Prime.
- 1.4 Выполните команду и выберите установленные модули:

```
$ sudo deployment-configurator install --no-start
```
- 1.5 При запросе IP-адресов модулей укажите новый IP-адрес. Остальные параметры оставьте без изменения.
- 1.6 Укажите новый IP-адрес в файлах конфигурации Nginx для ViPNet Prime NVS:
 - 1.6.1 Измените IP-адрес в файле `nvs.conf` в строке `allow <IP-адрес>`:

```
$ sudo nano /etc/nginx/dynamic-routes/http/nvs/nvs.conf
```
 - 1.6.2 Если при установке ViPNet Prime NVS был выбран защищённый канал VPN для получения данных мониторинга, в файле `nvs_sink.conf` в строке `allow <IP-адрес>` укажите верный IP-адрес:

```
$ sudo nano /etc/nginx/dynamic-routes/http/nvs_sink/nvs_sink.conf
```

2 На компьютере Б:

- 2.1 **Остановите работу** ViPNet Prime NVS.
- 2.2 В файле `/etc/hosts` измените IP-адреса, связанные с доменными именами модулей ViPNet Prime, на новый. Для доменного имени ViPNet Prime NVS укажите IP-адрес компьютера с ViPNet Prime NVS.
- 2.3 Перейдите в папку с распакованным установщиком ViPNet Prime NVS.
- 2.4 Выполните команду:

```
$ sudo ./install.sh
```
- 2.5 На шаге **Type the Core IP address** укажите новый IP-адрес компьютера А.
- 2.6 На компьютере А **запустите** ViPNet Prime и модули.
- 2.7 **Запустите** сборщик данных на компьютере А.
- 2.8 **Запустите** ViPNet Prime NVS на компьютере Б.

Смена IP-адреса на компьютере Б

Чтобы сменить IP-адрес на компьютере Б, выполните действия сначала на компьютере А, затем на компьютере Б:

1 На компьютере А:

1.1 **Остановите работу** ViPNet Prime, модулей и сборщика данных.

1.2 Укажите новый IP-адрес в файле `nvs.conf` в строке `allow <IP-адрес>` конфигурации Nginx для ViPNet Prime NVS:

```
$ sudo nano /etc/nginx/dynamic-routes/http/nvs/nvs.conf
```

2 На компьютере Б:

2.1 **Остановите работу** ViPNet Prime NVS.

2.2 Смените IP-адрес на сетевом интерфейсе компьютера штатными средствами ОС. Убедитесь, что интерфейсу назначен верный адрес.

2.3 В файле `/etc/hosts` измените IP-адрес компьютера с ViPNet Prime NVS.

2.4 Перейдите в папку с распакованным установщиком ViPNet Prime NVS.

2.5 Выполните команду:

```
$ sudo ./install.sh
```

2.6 На шаге **Type the monitoring module IP address** укажите новый IP-адрес компьютера с ViPNet Prime NVS.

2.7 На компьютере А **запустите** ViPNet Prime и модули.

2.8 **Запустите** сборщик данных на компьютере А.

2.9 **Запустите** ViPNet Prime NVS на компьютере Б.

Освобождение дискового пространства

Контейнеры Docker изолируют в себе файловую систему. Внутри них скапливаются ненужные данные, которые увеличивают размер контейнера. Это приводит к заполнению дискового пространства. На компьютере данные контейнеров Docker хранятся в `/var/lib/docker`. Данные ViPNet Prime не хранятся в контейнерах Docker, поэтому пересоздание контейнеров не приведет к потере данных. Чтобы избавиться от ненужных данных и освободить дисковое пространство, пересоздайте контейнеры:

- 1 Выполните команду:

```
$ sudo deployment-configurator stop
```

- 2 Выберите ViPNet Prime Core KC, ViPNet Prime Core MS, ViPNet Prime VPN KC, ViPNet Prime VPN MS, транспортный сервер ViPNet UT, ViPNet Prime NVS и ViPNet Connect Book и нажмите **Enter**.

- 3 Выполните команду:

```
$ sudo deployment-configurator start
```

- 4 Выберите ViPNet Prime Core KC, ViPNet Prime Core MS, ViPNet Prime VPN KC, ViPNet Prime VPN MS, транспортный сервер ViPNet UT, ViPNet Prime NVS и ViPNet Connect Book и нажмите **Enter**.

- 5 Чтобы перезапустить ViPNet Prime PMM выполните:

```
$ sudo /usr/share/infotecs/prime/deployment/pmm/down.sh
```

```
$ sudo /usr/share/infotecs/prime/deployment/pmm/up.sh
```

Настройка журналов ViPNet Prime

Для записи журналов используется служба `journald`, которая собирает сообщения, опубликованные в `stdout` службами на хосте и службами, работающими в Docker.

Файл конфигурации `/etc/systemd/journald.conf` оставьте в качестве справочника значений по умолчанию системы. Добавляйте настройки в дополнение к этому файлу, как фрагменты конфигурации в папках:

- `/usr/lib/systemd/*.conf.d`
- `/usr/local/lib/systemd/*.conf.d`
- `/etc/systemd/*.conf.d`

Конфигурации в этих папках имеют более высокий приоритет и переопределяют основной файл конфигурации. Файлы в подпапках конфигурации `/*.conf.d/` сортируются по имени файла в лексикографическом порядке, независимо от того, в какой из подпапок находятся. Когда в нескольких файлах указана одинаковая опция, для опций, которые принимают только одно значение, наибольший приоритет имеет запись в последнем файле в порядке сортировки, а для опций, которые принимают список значений, записи обрабатываются по мере их появления в отсортированных файлах.

Файлы в `/etc/` зарезервированы для локального администратора, папки `/usr/` — для размещения фрагментов конфигурации пакетов ОС.

Учитывайте логику файлов конфигурации для переопределения настроек (в том числе установленных сторонними пакетами), так как основной файл конфигурации `/etc/systemd/journald` имеет самый низкий приоритет.



Совет. Указывайте перед именами файлов в этих подкаталогах двузначное число и тире, чтобы упростить упорядочение файлов.

Настройка `journald`

1 Создайте файл, например, `/etc/systemd/journald.conf.d/overrides.conf`.

2 В этом файле в разделе `[Journal]` укажите:

- o `Storage=persistent`

Журналы будут размещаться в папке `/var/log/journal/`. Папка создается автоматически после удаления пользователем ОС.

- o `Seal=yes`

Используется для защиты долговременных (persistent) файлов журнала от незаметного изменения.

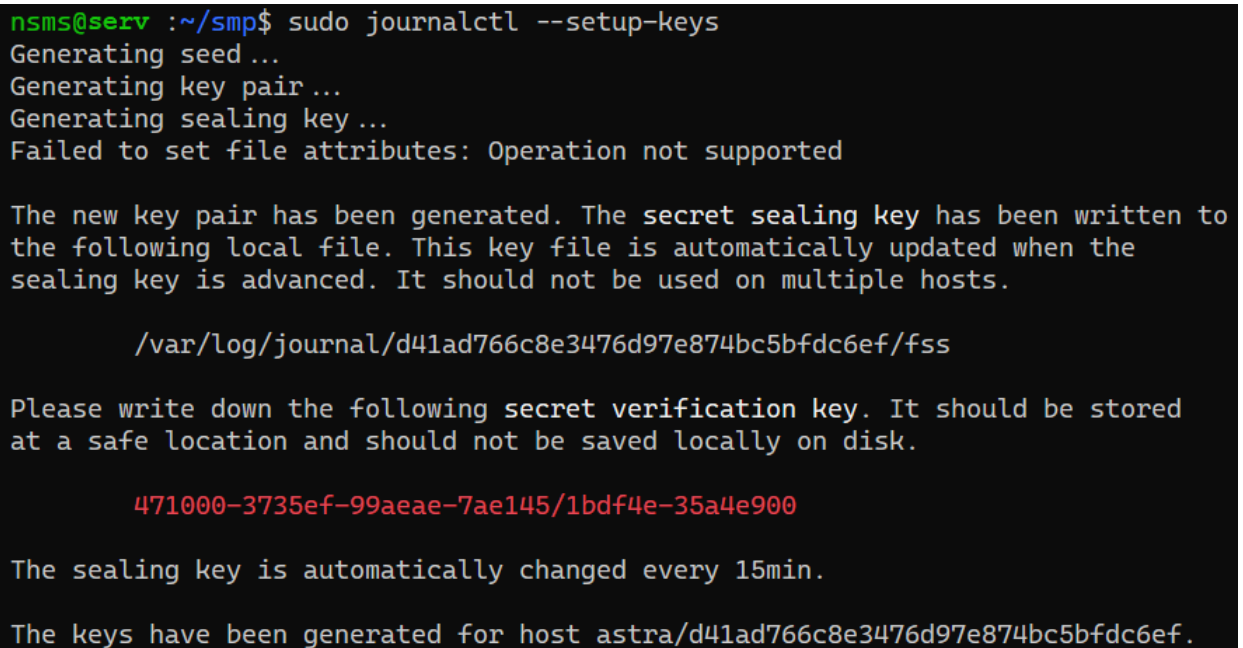
- o `SplitMode=uid`

Физически разделяет журнал, хранящийся на диске, и позволяет организовать непривилегированным учетным записям ОС доступ только для чтения к части журнала (с помощью команды `setfacl`).

- 3 Создайте ключи для проверки целостности журнала:

```
$ sudo journalctl --setup-keys --interval=10s
```

- 4 Скопируйте или перепишите из вывода предыдущей команды ключ `secret verification key` в надежное и секретное место (выводится красным цветом).



```
nsms@serv :~/smp$ sudo journalctl --setup-keys
Generating seed ...
Generating key pair ...
Generating sealing key ...
Failed to set file attributes: Operation not supported

The new key pair has been generated. The secret sealing key has been written to
the following local file. This key file is automatically updated when the
sealing key is advanced. It should not be used on multiple hosts.

/var/log/journal/d41ad766c8e3476d97e874bc5bfdc6ef/fss

Please write down the following secret verification key. It should be stored
at a safe location and should not be saved locally on disk.

471000-3735ef-99aeae-7ae145/1bdf4e-35a4e900

The sealing key is automatically changed every 15min.

The keys have been generated for host astra/d41ad766c8e3476d97e874bc5bfdc6ef.
```

Рисунок 21. Ключ для проверки целостности журнала

- 5 Перезапустите службу:

```
$ sudo systemctl restart systemd-journald
```

Проверка целостности журнала

Пример команды:

```
$ sudo journalctl --verify --verify-key <secret verification key>
```

Размер журналов

```
$ sudo journalctl --disk-usage
```

Очистка журналов

Чтобы очистить журналы и оставить на диске занятым объем, например, 100 Мбайт:

```
$ sudo journalctl --vacuum-size=100M
```

Чтобы очистить журналы и оставить на диске только данные за последний указанный период времени, например, две недели:

```
$ sudo journalctl --vacuum-time=2weeks
```

Автоматическая очистка журналов

По умолчанию размер журналов ограничен значением в 10% от объёма раздела, на котором он сохраняется. Это значение вы можете контролировать параметром `SystemMaxUse`.

Другие параметры: `SystemMaxUse`, `SystemKeepFree`, `SystemMaxFileSize`, `SystemMaxFiles`, `RuntimeMaxUse`, `RuntimeKeepFree`, `RuntimeMaxFileSize`, `RuntimeMaxFiles`.

Журналы хранятся в нескольких файлах: один файл — текущий, другие — архивные (максимум 7 файлов). Размер файла равен одной восьмой отведённого объёма. Когда текущий файл заполняется, файлы ротируются. Количество файлов определяются параметрами `SystemMaxFiles` и `RuntimeMaxFiles`, либо рассчитываются, если задать параметры `SystemMaxFileSize` и `RuntimeMaxFileSize` определяющие максимальный размер файла журнала.

В конфигурационном файле в секции `[Journal]` укажите, например:

```
SystemMaxUse=100G
SystemKeepFree=100G
SystemMaxFileSize=1G
SystemMaxFile=100
```

Чтобы просмотреть разрешенные ограничения для журналов:

```
$ sudo systemctl status systemd-journald
$ sudo journalctl -t systemd-journald
```

Транспортный сервер ViPNet UT

По умолчанию системные журналы очищаются автоматически, если на компьютере установлена утилита `Logrotate`. Настройки автоматической очистки помещаются в папку `/etc/logrotate.d/` при установке транспортного сервера.

По умолчанию ротация настроена таким образом, что журналы ежедневно архивируются. Журналы хранятся один день, архивы с журналами — пять дней.

Настройки ротации транспортного сервера ViPNet UT вы можете изменять с помощью `Logrotate`. Системные журналы хранятся в папке `/var/log/transport/`.

```

secadmin@astra:~$ sudo ls -laR /var/log/transport/
/var/log/transport/:
итого 16
drwx----- 4 root root 4096 мая 14 13:59 .
drwxr-xr-x 16 root root 4096 мая 14 16:07 ..
drwx----- 3 root root 4096 мая 14 13:59 common
drwxr-xr-x 2 root root 4096 мая 14 13:59 journal

/var/log/transport/common:
итого 12
drwx----- 3 root root 4096 мая 14 13:59 .
drwx----- 4 root root 4096 мая 14 13:59 ..
drwx----- 3 root root 4096 мая 14 13:59 2024

/var/log/transport/common/2024:
итого 12
drwx----- 3 root root 4096 мая 14 13:59 .
drwx----- 3 root root 4096 мая 14 13:59 ..
drwx----- 2 root root 4096 мая 14 13:59 05

/var/log/transport/common/2024/05:
итого 72
drwx----- 2 root root 4096 мая 14 13:59 .
drwx----- 3 root root 4096 мая 14 13:59 ..
-rw-r--r-- 1 root root 18802 мая 14 16:14 14_all.log
-rw-r--r-- 1 root root 4303 мая 14 16:14 14_auth_server_all.log
-rw-r--r-- 1 root root 2782 мая 14 16:14 14_heartbeat_service_all.log
-rw-r--r-- 1 root root 871 мая 14 16:14 14_pubsub_server_all.log
-rw-r--r-- 1 root root 8680 мая 14 16:14 14_redis_all.log
-rw-r--r-- 1 root root 6294 мая 14 16:14 14_syslog.log
-rw-r--r-- 1 root root 2166 мая 14 14:05 14_upload_server_all.log

/var/log/transport/journal:
итого 8
drwxr-xr-x 2 root root 4096 мая 14 13:59 .
drwx----- 4 root root 4096 мая 14 13:59 ..
secadmin@astra:~$

```

Рисунок 22. Журналы транспортного сервера ViPNet UT

Просмотр журналов ViPNet Prime

Просмотр журнала службы из состава ViPNet Prime KC

- Для просмотра журнала службы:

```
$ sudo journalctl -u <имя_службы>
```

Имена служб см. в [Состав ViPNet Prime](#).

- Для просмотра журнала службы:

```
$ sudo journalctl -u <имя_службы> -n <количество последних сообщений>
```

- Для просмотра журналов syslog:

```
$ sudo tail /var/log/syslog -n <число_строк>
```

Просмотр журнала контейнера Docker из состава ViPNet Prime MS

- Для просмотра журналов у конкретного контейнера Docker:

```
$ sudo journalctl CONTAINER_NAME=<имя_контейнера>
```

- Чтобы посмотреть имена контейнеров:

```
$ sudo docker ps -a --format "{{.Names}}"
```

Просмотр журнала сборщика данных

Информация о событиях, происходящих в процессе работы сборщика данных, сохраняется в файле журнала `/var/log/infotecs/nvs/remote-collector-YYYYMMDD.json`. Также в файл `/var/log/infotecs/nvs/error-YYYYMMDD.log` сохраняется информация об ошибках ViPNet Prime NVS. Просмотреть события сборщика данных вы можете с помощью команды:

```
# sudo journalctl -u nvs-rc
```

Просмотр журнала аудита

В журнале аудита вы можете просмотреть события в случае нарушения работоспособности. Журнал аудита использует службу `journald`.

События журнала имеют вид: {дата} {время} {имя компьютера} {служба} [AUDIT] {статус события INF | ERR} {учетная запись администратора ViPNet ViPNet Prime | SYSTEM} {название события} {дополнительные параметры события}.

Статус события:

- [INF] — успешно;
- [ERR] — ошибка.

Чтобы просмотреть журнал:

- 1 Авторизуйтесь на компьютере с Prime:

1.1 Включите контроль исполняемых файлов. Для этого выберите атрибут безопасности **Уровень целостности — Высокий**.

1.2 Войдите в ОС под учётной записью ОС с правами суперпользователя `root` или администратора для использования команды `sudo`.

2 Чтобы просмотреть записи журнала:

- о за сегодня:

```
$ sudo journalctl --utc -o short-precise --since "today" | grep '\[AUDIT\]'
```

- о за последние трое суток:

```
$ sudo journalctl --utc -o short-precise --since "3 days ago" | grep '\[AUDIT\]'
```

- о за период времени:

```
$ sudo journalctl --utc -o short-precise --since "2022-02-07" --until "2022-08-08 03:00" | grep '\[AUDIT\]'
```

- о события аудита с учётной записью администратора `admin`:

```
$ sudo journalctl --utc -o short-precise | grep '\[AUDIT\]' | grep 'admin'
```

- о ошибки в журнале:

```
$ sudo journalctl --utc -o short-precise | grep '\[AUDIT\]' | grep '\[ERR\]'
```

- о события службы аутентификации:

```
$ sudo journalctl --utc -o short-precise -t 'silso' | grep '\[AUDIT\]'
```

- о события службы авторизации:

```
$ sudo journalctl --utc -o short-precise -t 'auth-service' | grep '\[AUDIT\]'
```

Удаление событий журнала

1 Чтобы сохранить в файл все события аудита старше трех дней:

```
$ sudo journalctl --utc -o short-precise --until "3 days ago" | grep '\[AUDIT\]' > audit.log
```

2 Чтобы удалить события аудита старше трех дней:

```
$ sudo journalctl --vacuum-time=3d
```



Внимание! Перед удалением журнала сохраняйте копию журнала и оставляйте события за последние три дня.

Пример событий аудита:

```
Apr 21 10:48:38.916106 hostname silso[6858]: [AUDIT] [INF] admin Началось создание учетной записи. {"UserAccountId": null, "UserAccountName": "user", "UserAccountOrganizationId": null, "SubjectId": "399bad82-b879-40ae-8123-afb000c1594b", "Process": "Silso"}
```

```
Apr 21 10:48:39.111122 hostname auth-service[7080]: [AUDIT] [INF] admin Назначение роли учетной записи. {"SubjectId": "399bad82-b879-40ae-8123-afb000c1594b", "Role": "service-administrator", "TargetSubjectId": "7e46e068-7b4d-4abc-9ad2-afeb00e3985e"}
```

```
Apr 21 10:48:39.111583 hostname auth-service[7080]: [AUDIT] [INF] admin Назначение
роли учетной записи. {"SubjectId": "399bad82-b879-40ae-8123-afb000c1594b", "Role":
"platform-operator", "TargetSubjectId": "7e46e068-7b4d-4abc-9ad2-afeb00e3985e"}

Apr 21 10:48:39.111853 hostname auth-service[7080]: [AUDIT] [INF] admin Назначение
роли учетной записи. {"SubjectId": "399bad82-b879-40ae-8123-afb000c1594b", "Role":
"organization-owner", "TargetSubjectId": "7e46e068-7b4d-4abc-9ad2-afeb00e3985e"}

Apr 21 10:48:39.112116 hostname auth-service[7080]: [AUDIT] [INF] admin Назначение
роли учетной записи. {"SubjectId": "399bad82-b879-40ae-8123-afb000c1594b", "Role":
"utm-auditor", "TargetSubjectId": "7e46e068-7b4d-4abc-9ad2-afeb00e3985e"}

Apr 21 10:48:39.112367 hostname auth-service[7080]: [AUDIT] [INF] admin Назначение
роли учетной записи. {"SubjectId": "399bad82-b879-40ae-8123-afb000c1594b", "Role":
"organization-administrator", "TargetSubjectId": "7e46e068-7b4d-4abc-9ad2-
afeb00e3985e"}

Apr 21 10:48:38.929610 hostname silso[6858]: [AUDIT] [INF] admin Создание учетной
записи. {"UserAccountId": "7e46e068-7b4d-4abc-9ad2-afeb00e3985e", "UserAccountName":
"NameUser", "UserAccountOrganizationId": null, "SubjectId": "399bad82-b879-40ae-8123-
afb000c1594b", "Process": "Silso"}
```

Выгрузка журналов

Для удобства чтения журналов используйте параметры для `journalctl`:

- `-o short-iso` — дата события будет выводиться в формате ГГГГ-ММ-ДД ЧЧ:ММ:СС.
- `--no-hostname` — удаляет упоминание имени хостовой машины в каждой записи журнала.

Для удобства выгрузки журналов по всем контейнерам и службам ViPNet Prime используйте скрипт `diag.sh` из комплекта поставки. В структуре архива журналы будут располагаться по пути `/var/log/infotecs`.

Пересечение подсетей Docker и LAN

ViPNet Prime MS состоит из служб, которые работают в виртуальных контейнерах Docker. Для каждого контейнера создается виртуальный сетевой интерфейс. См. на сайте [Docker](#).

Сконфигурируйте сеть:



Примечание. Если ViPNet Prime NVS установлен на отдельном компьютере, запустите скрипт и на нём.

- 1 [Завершите работу ViPNet Prime.](#)
- 2 Перейдите в папку со скриптом `docker_network_configurator.<версия>.py` и выдайте права на исполнение:

```
$ sudo chmod +x docker_network_configurator.<версия>.py
```
- 3 Запустите скрипт `docker_network_configurator.<версия>.py`:

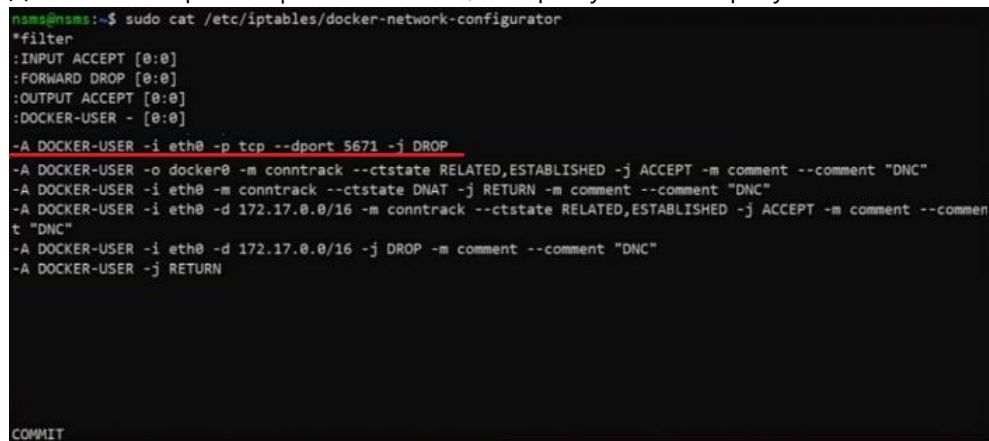
```
$ sudo ./docker_network_configurator.<версия>.py
```
- 4 Укажите IP-адрес для виртуального сетевого интерфейса `docker0`, который будет выступать в роли сетевого моста между контейнерами.
- 5 Укажите диапазон адресов, который будет использоваться для контейнеров.
- 6 Укажите внешний сетевой интерфейс.
- 7 Закройте доступ к порту 5671 (порт RabbitMQ):
 - 7.1 Если ViPNet NVS установлен на одном компьютере с ViPNet Prime — добавьте в файл правило, запрещающее весь трафик для внешнего сетевого интерфейса:

```
-A DOCKER-USER -i <имя внешнего сетевого интерфейса> -p tcp --dport 5671 -j DROP
```
 - 7.2 Если ViPNet NVS установлен на отдельном компьютере, то на компьютере с ViPNet Prime добавьте правила в указанном ниже порядке:
 - Разрешающее трафик от компьютера с ViPNet NVS на компьютер с ViPNet Prime:

```
-A DOCKER-USER -i <имя внешнего сетевого интерфейса> -p tcp --dport 5671 -s <IP-адрес компьютера с ViPNet NVS> -j ACCEPT
```
 - Запрещающее весь трафик для внешнего интерфейса:

```
-A DOCKER-USER -i <имя внешнего сетевого интерфейса> -p tcp --dport 5671 -j DROP
```

Добавляйте строки в файл в то место, которое указано на рисунке.



```
nsms@nsms:~$ sudo cat /etc/iptables/docker-network-configurator
*filter
:INPUT ACCEPT [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
:DOCKER-USER - [0:0]
-A DOCKER-USER -i eth0 -p tcp --dport 5671 -j DROP
-A DOCKER-USER -o docker0 -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT -m comment --comment "DNC"
-A DOCKER-USER -i eth0 -m conntrack --ctstate DNAT -j RETURN -m comment --comment "DNC"
-A DOCKER-USER -i eth0 -d 172.17.0.0/16 -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT -m comment --comment "DNC"
-A DOCKER-USER -i eth0 -d 172.17.0.0/16 -j DROP -m comment --comment "DNC"
-A DOCKER-USER -j RETURN
COMMIT
```

Рисунок 23. Пример добавления строк

- 8 Перезагрузите компьютер с ViPNet Prime.
- 9 Запустите ViPNet Prime.

Просмотр версии ViPNet Prime

- 1 Войдите в ViPNet Prime.
- 2 В верхнем правом углу нажмите .
- 3 Перейдите на вкладку **Модули**.

Запрет входящих соединений к ViPNet Prime Key Center Nginx

Запретите все входящие соединения с ViPNet Prime Key Center Nginx, кроме:

- соединений с рабочих мест администраторов ViPNet Prime;
- адреса 127.0.0.1;
- IP-адреса сетевого интерфейса компьютера ViPNet Prime Key Center;
- диапазона адресов контейнеров Docker — ограничьте адреса в конфигурации Docker в файле `/etc/docker/daemon.json` и укажите эти адреса в списке разрешенных;
- виртуальных адресов всех узлов, которыми управляете через ViPNet Prime, например `7.0.0.0/8`,
- адреса ViPNet Prime NVS, если он развернут на отдельном компьютере.

Порядок действий:

- 1 Создайте файл `access_list.conf` в папке `/etc/nginx/`, укажите разрешённые IP-адреса.
- 2 Все остальные IP-адреса запретите.

```
#Prime
allow 127.0.0.1;
allow 192.168.30.214;

#Docker
allow 10.66.0.0/16;
allow 172.17.0.0/16;

#ViPNet
allow 7.0.0.2;

#Блокировка остального трафика
deny all;
```

Рисунок 24. Пример добавления разрешенных адресов в файл

- 3 Укажите этот файл в `/etc/nginx/nginx.conf` в секциях `http { }` и `stream { }`.

```
include ./sites-enabled/*;
include ./dynamic-routes/http/*/*.conf;
include ./sites/*.conf;
## Пользовательские правила
include ./access_list.conf;
}

stream {
    include ./dynamic-routes/stream/*/*.conf;
    ## Пользовательские правила
    include ./access_list.conf;
}
```

Рисунок 25. Пример добавления файла с разрешенными IP-адресами



Внимание! После обновления ViPNet Prime или переустановки ViPNet Prime Core заново укажите файл `access_list.conf` в `/etc/nginx/nginx.conf` в секциях `http { }` и `stream { }`. Файл `access_list.conf` повторно создавать не требуется.

Если необходим сетевой доступ сервису, обслуживающему ViPNet Prime, проверьте наличие этого адреса в списке разрешенных входящих соединений.

Установка сертификатов TLS ГОСТ

Если правилами безопасности вашей организации требуется использовать двусторонний TLS ГОСТ:

Подготовьте к установке сертификаты сервера для TLS ГОСТ. Создайте запрос на сертификат сервера для TLS ГОСТ с помощью скрипта из комплекта поставки.



Примечание. В запросе на сертификат сервера для TLS ГОСТ `create-gost-tls-key.sh` не указываются такие поля как город, организация, ИНН. Поэтому он может не приниматься некоторыми российскими УЦ.

- 1 **Перейдите в папку** `/usr/share/infotecs/prime/deployment/core-kc:`
`$ cd /usr/share/infotecs/prime/deployment/core-kc`
- 2 **Запустите скрипт** `install-certificates.sh`:
`$ sudo ./install-certificates.sh`
- 3 На шаге **Do you want to install another certificates set** введите `y`.
- 4 **Path to the trusted CA certificate** — введите путь к сертификату корневого УЦ для TLS ГОСТ, например `/infotecs/certs/ca-gost.crt`.
- 5 **Path to the TLS server certificate** — введите путь к сертификату сервера для TLS ГОСТ, например `/infotecs/certs/nginx-gost.crt`.
- 6 **Path to the private key associated with the TLS server certificate (.pfx)** — введите путь к PFX-контейнеру с закрытым ключом сертификата сервера для TLS ГОСТ, например, `/infotecs/certs/nginx-gost.pfx`.
- 7 **Type the private key password** — введите пароль от PFX-контейнера с ключом ЭП сертификата сервера для TLS ГОСТ.

6

Регламентные процедуры

Контроль целостности ViPNet Prime	99
Контроль целостности образов Docker-контейнеров и исполняемых файлов	101
Смена мастер-ПИН программного токена	102
Проверка ЭП файла обновления ПО ViPNet	103

Контроль целостности ViPNet Prime

В ViPNet Prime проверяется целостность для критичных и некритичных служб. Нарушение целостности некритичных служб приведёт к переходу работы ViPNet Prime в режим ограниченной функциональности. Нарушение целостности критичной службы заблокирует работу в ViPNet Prime.

Целостность проверяется для всех служб:

- автоматически:
 - после установки и при каждом запуске ViPNet Prime (стартовый контроль);
 - по таймеру — один раз в час (динамический контроль).
- вручную при регламентном контроле. См. «ViPNet Prime. Руководство администратора», раздел «Контроль целостности ПО». Рекомендуемый срок регламентного контроля — не реже одного раза в месяц.

Проверка целостности может завершиться с результатом:

- Нарушения целостности не выявлены — целостность служб не нарушена. Для всех служб в журнале аудита отображается событие успешной проверки целостности.
- Выявлены нарушения целостности некритичных служб — служба повреждена или не отвечает. Администратору недоступны действия в ViPNet Prime. В журнале аудита для службы, которая не прошла проверку целостности или не отвечает, отображается событие **Блокировка в результате контроля целостности или работоспособности** и событие о нарушении контроля целостности [AUDIT] [ERR] SYSTEM. В ViPNet Prime отображается сообщение о работе приложения в режиме ограниченной функциональности.
- Выявлены нарушения целостности — целостность хотя бы одной из критичных служб нарушена. Это приведёт к блокировке:
 - веб-интерфейса ViPNet Prime;
 - службы создания ключей из состава ViPNet Prime KC;
 - ViPNet Prime VPN.

Чтобы восстановить работоспособность ПО:

- 1 На компьютере с ViPNet Prime в журнале аудита найдите запись о заблокированной службе:

```
$ sudo journalctl -f --utc -o short-precise --since "today" | grep '\[AUDIT\]'
```

- 2 [Перезапустите ViPNet Prime и модули.](#)

- 3 Убедитесь в успешном завершении стартового контроля всего приложения. Для этого на компьютере с ViPNet Prime в журнале аудита найдите сообщение:

```
[AUDIT] [INF] SYSTEM Стартовый контроль целостности и работоспособности ViPNet Prime.
```

- 4 Если работа в интерфейсе заблокирована, стартовый контроль целостности не пройден, контрольные суммы служб не соответствуют эталонным значениям — восстановите эталонные значения служб. Для этого повторно установите ViPNet Prime:

```
$ sudo deployment-configurator install
```

При повторной установке не изменяйте порты и доменные имена модулей. Иначе вы не сможете подключиться к веб-интерфейсу ViPNet Prime.

Контроль целостности образов Docker-контейнеров и исполняемых файлов

Контроль целостности образов Docker-контейнеров происходит автоматически при запуске ViPNet Prime и его модулей с помощью скриптов `up.sh` и через `deployment-configurator`. Чтобы проверить целостность образов Docker-контейнеров вручную:

- 1 Перейдите в папку с распакованным модулем.
- 2 Выполните команду для проверки целостности:

```
$ sudo ./check-integrity.sh
```
- 3 Дождитесь завершения проверки. В случае успешного прохождения контроля целостности образов Docker-контейнеров появится сообщение `Integrity check passed successfully`.

Целостность исполняемых файлов, содержащихся в образах Docker-контейнеров, проверяется вручную с периодичностью, которая принята в вашей организации. Для этого:

- 1 Перейдите в папку с распакованным модулем.
- 2 Выполните команду для проверки целостности:

```
$ sudo ./check-container-integrity.sh
```
- 3 Дождитесь завершения проверки. После прохождения контроля целостности исполняемых файлов, содержащихся в Docker-контейнерах, появится сообщение о проверке целостности файла с контрольными суммами и для каждого Docker-контейнера, например:

```
Total:
1 PRG files processed, 1 checks passed, 0 checks failed, 0 checks skipped
1787 files checked, 1787 checks passed, 0 files corrupted, 0 checks failed
```

В случае успешного прохождения контроля целостности значение параметров `files corrupted` и `checks failed` должно быть равно 0.

При нарушении целостности образов Docker-контейнеров или исполняемых файлов, содержащихся в них:

- Выполните восстановление ViPNet Prime из резервной копии.
- Переустановите ViPNet Prime с помощью ПО из комплекта поставки.

Смена мастер-ПИН программного токена

Ключи хранятся в программном токене, доступ к которому защищён с помощью мастер-ПИНа. Для безопасности меняйте мастер-ПИН раз в шесть месяцев. Перед сменой мастер-ПИНа убедитесь:

- ViPNet Prime запущен;
- пройден стартовый контроль целостности;
- введён действующий мастер-ПИН;
- доступно окно аутентификации в веб-интерфейсе;
- при переходе между вкладками отсутствует предупреждение о работе ViPNet Prime в режиме ограниченной функциональности.

Чтобы сменить мастер-ПИН программного токена:

- 1 При входе в Astra Linux SE выберите атрибут безопасности **Уровень целостности — Высокий**.
- 2 Войдите в ОС под учётной записью ОС с правами суперпользователя `root` или администратора для использования команды `sudo`.
- 3 Смените мастер-ПИН:

```
$ sudo prime-control change-pin
```

- 4 Укажите текущий мастер-ПИН.
- 5 Укажите новый мастер-ПИН и подтвердите его.
- 6 Для просмотра событий операции откройте журнал аудита в отдельном окне терминала:

```
$ sudo journalctl -t prime-control -t silso -f --since '5 minutes ago' | grep '[AUDIT\\]\\|SoftToken'
```



Внимание! После смены мастер-ПИНа, ViPNet Prime будет не доступен минуту. Мастер-ПИН нельзя восстановить. Если вы потеряете мастер-ПИН, вы потеряете доступ к ViPNet Prime.

Проверка ЭП файла обновления ПО ViPNet

Перед обновлением ViPNet Prime или перед отправкой обновления ПО ViPNet через ViPNet Prime на узлы (файлы *.lzh) проверьте ЭП этих файлов. Для проверки ЭП файлов не используйте компьютер с ViPNet Prime. Это приведёт к нарушению работоспособности ViPNet Prime.

Предварительные действия

- 1 Получите доверенным способом от представителей ИнфоТеКС следующие файлы (либо используйте те файлы, которые находятся в комплекте поставки в папке `signature check`):
 - о корневой сертификат ключа проверки ЭП ИнфоТеКС (*.cer);
 - о список отозванных сертификатов (*.crl);
 - о файлы обновления ПО ViPNet;
 - о ЭП файлов обновления в форматах SIG (для ViPNet PKI Client версии ниже 2.0) и DETACHED.SIG (для ViPNet PKI Client версии 2.0 и выше).
- 2 Скачайте с официального сайта ИнфоТеКС [программу ViPNet PKI Client](#) и установите.

Установка корневого сертификата и списка отозванных сертификатов

- 1 Запустите ViPNet PKI Client (File Unit) и нажмите  **Настройки**:

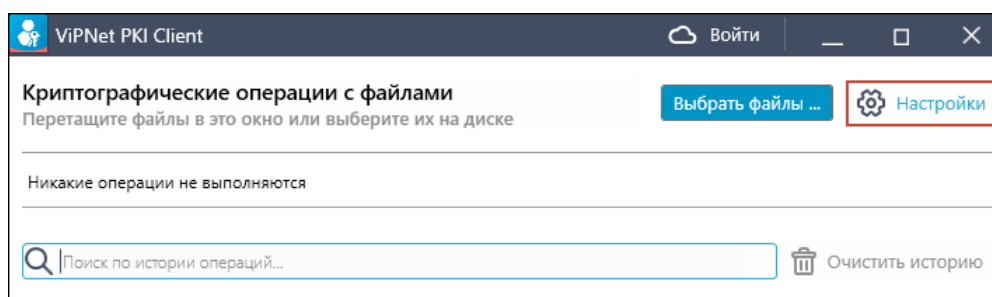


Рисунок 26. Настройка ViPNet PKI Client

- 2 Перейдите в раздел **Сертификаты** и нажмите  **Добавить сертификаты или CRL**:

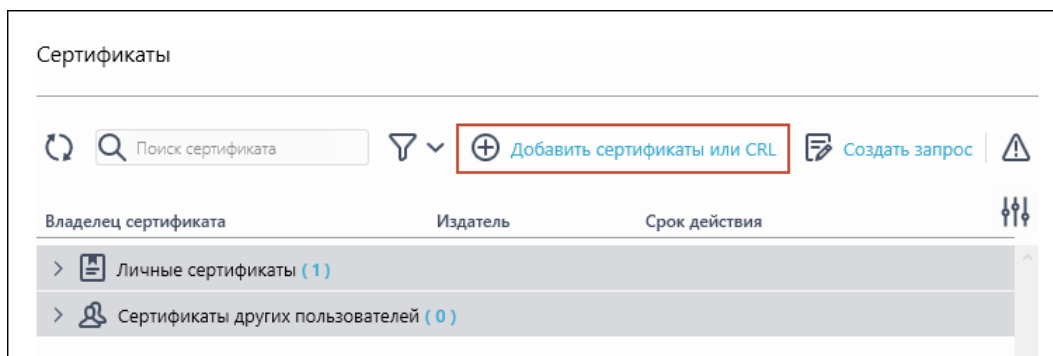


Рисунок 27. Импорт корневого сертификата и списка отозванных сертификатов

- 3 Выберите файл корневого сертификата (*.crt или *.cer) и файл списка отозванных сертификатов (*.crl):

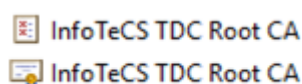


Рисунок 28. Корневой сертификат и список отозванных сертификатов

Внимание! Если ранее вы уже устанавливали корневой сертификат с именем InfoTeCS TDC Root CA, удостоверьтесь, что он отсутствует в хранилище «Промежуточные центры сертификации». Для этого:



- 1 Запустите диспетчер сертификатов с помощью команды `/opt/itcs/bin/certmgr-gui` в Astra Linux SE.
- 2 Откройте папку «Промежуточные центры сертификации» («Intermediate Certification Authorities»), а в ней — папку «Сертификаты» («Certificates»).
- 3 Если найдете сертификат с указанным именем, удалите его.

- 4 Нажмите **Добавить**:

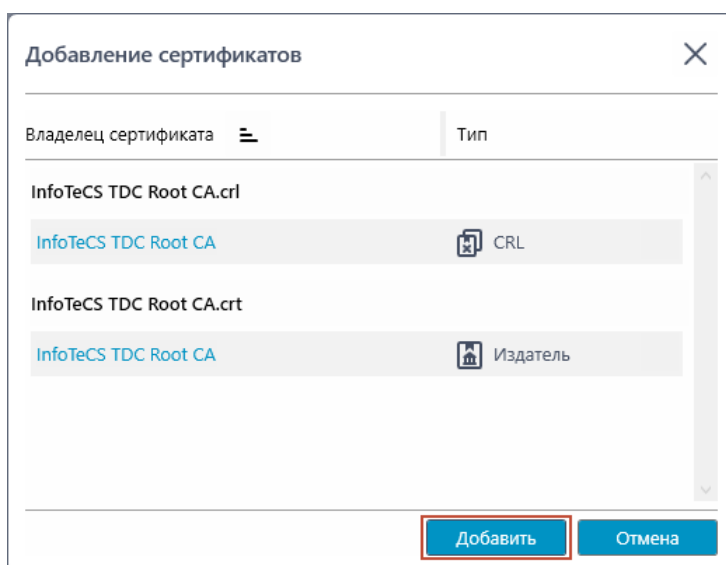


Рисунок 29. Подтверждение импорта корневого сертификата и списка отозванных сертификатов

4.1 В окне **Предупреждение системы безопасности** подтвердите установку корневого сертификата.

4.2 В окне **Добавление сертификатов** нажмите кнопку **Заккрыть**.

Установка корневого сертификата и списка отозванных сертификатов завершена.

Проверка электронной подписи

1 В главном окне программы ViPNet PKI Client выполните одно из действий:

- Нажмите **Выбрать файлы** и выберите файл обновления ПО и файл *.sig (*.detached.sig).
- Перетащите файл обновления ПО и файл *.sig (*.detached.sig) в главное окно программы.

2 Щелкните значок  напротив имени файла *.sig (*.detached.sig).

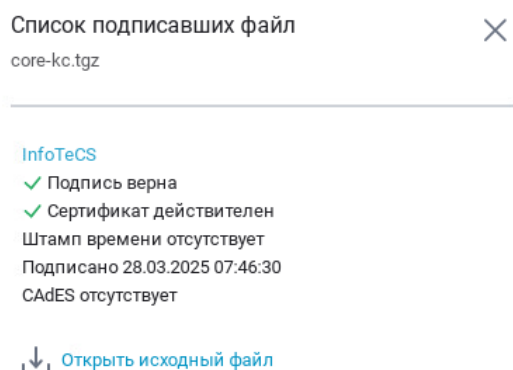


Рисунок 30. Результат проверки ЭП файла

3 Повторите процедуру проверки для других файлов обновления.



Возможные неполадки

Недоступен веб-интерфейс

При перезапуске ViPNet Prime скриптами `down.sh` и `up.sh` невозможно открыть веб-интерфейс ViPNet Prime.

При просмотре `docker ps` обнаружен контейнер `smp-service` в состоянии `unhealthy`.

Возможные причины

Установлен антивирус Касперского, который блокирует работу ViPNet Prime.

Устранение проблемы

- 1 Получите идентификаторы имени интерфейсов для стеков `smp` и `nsms`:

```
# sudo docker network ls -q -f'name=smp_smp-net'
# sudo docker network ls -q -f'name=nsms_nsms-net'
```

- 2 Добавьте в исключения межсетевого экрана в таблицу `mangle` следующие записи:

```
# sudo iptables -t mangle -A OUTPUT -o br-<идентификатор smp-интерфейса> -m mark --mark 0x89f337f1 -j MARK --set-xmark 0x0/0xffffffff
# sudo iptables -t mangle -A OUTPUT -o br-<идентификатор nsms-интерфейса> -m mark --mark 0x89f337f1 -j MARK --set-xmark 0x0/0xffffffff
```

После запуска скриптов `down.sh` или `up.sh` ID docker-сетей будут сгенерированы заново, потребуется обновить правила. При перезапуске операционной системы ID docker-сетей не меняются.

Не запускается ViPNet Prime

При перезагрузке компьютера и после ввода мастер-ПИН невозможно открыть веб-интерфейс ViPNet Prime.

Возможные причины

На Astra Linux SE включен режим ЗПС. Службы ViPNet Prime не успели запуститься.

Устранение проблемы

Повторно [запустите ViPNet Prime](#).

Ошибка при запуске модуля ViPNet Prime NVS

Не запускается ViPNet Prime NVS. В окне терминала имеется ошибка, что один или несколько Docker-контейнеров не запустились.

Возможные причины

Количество ядер процессора на компьютере с ViPNet Prime NVS больше 16.

Устранение проблемы

- 1 [Завершите работу ViPNet Prime NVS](#).
- 2 Откройте для редактирования файл `docker-compose.limit.yml`.
- 3 Для контейнеров, которые не запускаются, измените значение параметра `DOTNET_GCHeapHardLimit` на `0x18000000`.

Недоступен веб-интерфейс по поддомену Active Directory Federation Services

Невозможно открыть веб-интерфейс ViPNet Prime.

Возможные причины

В wildcard сертификатах отсутствуют доменные имена, по которым вы обращаетесь к ViPNet Prime.

Устранение проблемы

Перевыпустите wildcard-сертификаты с корректными доменными именами и [обновите их](#) с помощью скриптов.

При запуске ViPNet Prime не принимается мастер-ПИН

ViPNet Prime развернут в среде виртуализации VMware vSphere. При запуске ViPNet Prime мастер-ПИН не принимается.

Устранение проблемы

Служба `prime-control` не запускается. Чтобы запустить его, в VMware vSphere в настройках конфигурации включите EVC (Enhanced vMotion Compatibility): выберите **Settings > Configure > VMware EVC > Enabled**.

Недоступен веб-интерфейс модуля

В ViPNet Prime при переключении между разделами, окно модуля может не открыться.

Устранение проблемы

Откройте страницу модуля в отдельной вкладке браузера и разрешите подключение.

Ошибка CSP correctness check failed

После перезапуска ViPNet Prime и прохождения стартового контроля целостности "prime-control" и ввода мастер-ПИНа:

- веб-интерфейс не загружается;
- отображается бесконечная загрузка страницы.

В качестве источника энтропии случайных чисел используется БДСЧ (электронная рулетка). ViPNet Prime VPN подключен к ViPNet Prime.

В журнале `ks4-service` присутствует ошибка «CSP correctness check failed»:

```
$ sudo journalctl -u ks4-service  
  
$ sudo journalctl -u ks4-service | grep '\[ERR\]'
```

Возможные причины

Израсходована энтропия для криптографических операций. Размер файла `dsdr.bin` меньше чем 64 байт.

Чтобы посмотреть размер файла:

```
$ ls -l /var/lib/infotecs/smp-kc/data/prime-control/dsdr.bin
```

```
root@astraKC:/home/adminkc# ls -l /var/lib/infotecs/smp-kc/data/prime-control/dsdr.bin
-rw-rw---- 1 smp smp 31 июл 25 12:40 /var/lib/infotecs/smp-kc/data/prime-control/dsdr.bin
```

Рисунок 31. Просмотр размера файла

Устранение проблемы

1 Выполните команды:

```
$ sudo apt install xxd
```

```
$ sudo /opt/itcs/bin/uprngctl rnd -l 1000 | grep -oP "(?<=.{4}):).*" | xxd -r -p > /var/lib/infotecs/smp-kc/data/prime-control/dsdr.bin
```

2 Перезапустите ViPNet Prime:

```
$ sudo deployment-configurator stop --all
```

```
$ sudo deployment-configurator start --all
```

Пакет `firewalld` блокирует доступ к веб-интерфейсу

Возможные причины

Пакет `firewalld` может блокировать работу по протоколу HTTPS.

Устранение проблемы

Разрешите работу протоколу HTTPS. Для этого:

1 Завершите работу ViPNet Prime.

2 Выполните команду:

```
$ sudo firewall-cmd --permanent --zone=public --add-service=https
```

3 Проверьте внесенные изменения:

```
$ sudo firewall-cmd --list-all-zones
```

4 Перезапустите `firewalld`:

```
$ sudo firewall-cmd --reload
```

5 Проверьте, что внесенные изменения применены:

```
$ sudo firewall-cmd --list-all-zones
```

6 Запустите ViPNet Prime.

Ошибка при установке dpkg frontend lock

Для устранения проблемы выполните команду `dpkg-reconfigure unattended-upgrades` и повторно запустите установку.

Установка сторонних пакетов нарушает зависимости

Возможные причины

Скрипт `install-3d-party.sh` понижает версии некоторых пакетов в ОС. Это нарушает зависимости при установке пакетов, не относящихся к ViPNet Prime.

Устранение проблемы

Выполните команду:

```
$ sudo apt --fix-broken install
```

Дублирование окна ViPNet Prime VPN в веб-интерфейсе

Возможные причины

Доменное имя или порт ViPNet Prime VPN совпадает с ViPNet Prime Core.

Устранение проблемы

Переустановите ViPNet Prime VPN. Задайте доменное имя и (или) порт для ViPNet Prime VPN отличное от ViPNet Prime Core.

Не приходит запрос на регистрацию модуля

Возможные причины

Нет доверия к промежуточным сертификатам.

Устранение проблемы

Обеспечьте доверие к промежуточным сертификатам.

Сбой времени при синхронизации с NTP-сервером

Если на компьютере с ViPNet Prime не удаётся синхронизировать время с NTP-сервером, например из-за проблем с доступом к NTP-серверу, [перезапустите ViPNet Prime](#). Иначе работоспособность ViPNet Prime нарушится.

Ошибки после установки или обновления ViPNet Prime NVS

После установки и принятия запроса на регистрацию ViPNet Prime NVS, веб-интерфейс ViPNet Prime NVS не открывается. После обновления ViPNet Prime NVS не открывается веб-интерфейс ViPNet Prime.

Возможные причины

Отсутствует ключ ЭП сертификата сервера.

Устранение проблемы

- 1 Запустите терминал.
- 2 Узнайте номер Docker-контейнера, журнал которого необходимо посмотреть.

```
$ sudo docker ps | grep nvs_nats
```
- 3 Проверьте журнал NATS ViPNet Prime NVS.

```
$ sudo docker logs -f nvs_nats_<номер контейнера из предыдущего шага>
```
- 4 Убедитесь, что в журнале присутствует запись `nats-server: /nats/conf/nats-server.conf:16:1: error parsing X509 certificate/key pair: tls: failed to find PEM block with type ending in "PRIVATE KEY" in key input after skipping PEM blocks of the following types: [CERTIFICATE CERTIFICATE]`.
- 5 Повторно установите ViPNet Prime NVS.



Состав ViPNet Prime

В ViPNet Prime версии 1.9.14 входят:

- ViPNet Prime Core — 1.17.
- Транспортный сервер ViPNet UT — 2.2.
- Коннектор Active Directory — Pear 1.5.99.
- Модули:
 - ViPNet Prime VPN — 1.15.
 - ViPNet Prime NVS — 1.11.
 - ViPNet Prime PMM — 1.11.
 - ViPNet Connect Book — 1.7.

ViPNet Prime KC

Службы ViPNet Prime Core:

- prime-control — контроль целостности и исправности ViPNet Prime, управление паролями мастер-ПИНа программного токена;
- silso — служба аутентификации и идентификации на базе протокола OpenID Connect;
- settings-service — служба настроек;
- auth-service — служба авторизации;
- nginx (pin_source_proxy) — обратный прокси-сервер и отдача статического контента веб-приложения;
- uprng — криптографический компонент, который отвечает за генерацию последовательности случайных чисел;
- postgresql — система управления базами данных PostgreSQL.

Службы ViPNet Prime VPN:

- ks4-service — служба управления мастер-ключами, шифрованием, созданием ключей узла и пользователя для узлов поколения ПО ViPNet 4;
- ks5-service — служба управления мастер-ключами, шифрованием, созданием ключей защиты обновлений и ключей обмена для узлов поколения ПО ViPNet 5;
- kc-web-api-service — шлюз API ключевого центра для авторизации запросов;
- dst-service — служба создания дистрибутивов ключей и справочников;
- hw-service — служба управления настройками шлюзов безопасности поколения ПО ViPNet 5;
- mftp-service — служба создания и отправки транспортных MFTP-конвертов и получения обратных квитанций;
- uprng — криптографический компонент, который отвечает за генерацию последовательности случайных чисел;
- vipnet_custom_key_generation_service — криптографический компонент, который отвечает за генерацию ключей для поколения ПО ViPNet 5.

ViPNet Prime MS

Docker-контейнеры ViPNet Prime Core:

- smp_smp-service_1 — служба объектов общей предметной области;
- smp_smp-billing_1 — служба биллинга;
- smp_smp-import_1 — служба импорта;
- smp_smp-log_1 — служба журналов;
- smp_smp-license_1 — служба лицензий;
- smp_smp-messaging_1 — служба рассылок;
- smp_smp-backup_1 — служба резервного копирования;
- smp_smp-transport_1 — служба транспорта UT;
- smp_smp-postgresql_1 — система управления базами данных PostgreSQL;
- smp_smp-rabbitmq_1 — брокер сообщений;
- smp_smp-nginx_1 — обратный прокси-сервер.

Docker-контейнеры ViPNet Prime VPN:

- nsms_nginx_1 — обратный прокси-сервер;
- nsms_web-api_1 — шлюз для входящих запросов пользователей;
- nsms_action-log-service_1 — служба журнала действий пользователя;
- nsms_automatic-update-service_1 — служба для автоматической отправки справочников и ключей на узлы сети ViPNet;
- nsms_configuration-service_1 — служба настроек;

- nsms_smp-gateway-service_1 — служба для взаимодействия с ViPNet Prime Core;
- nsms_ncc-service_1 — служба управления структурой защищённой сети;
- nsms_workflow-service_1 — служба для координации работ других служб;
- nsms_software-update-service_1 — служба для работы с обновлениями ПО;
- nsms_postgresql_1 — система управления базами данных PostgreSQL;
- nsms_pgouncer_1 — список соединений к PostgreSQL;
- nsms_kafka_1 — распределённый журнал сообщений;
- nsms_rabbitmq_1 — брокер сообщений.

Docker-контейнеры транспортного сервера ViPNet Universal Transport:

- nginx_base — веб-сервер для остальных служб транспортного сервера (кеш, перенаправление запросов к службе аутентификации);
- d_upload_server — принимает запросы на публикацию и удаление сообщений (HTTP-сервер);
- d_pubsub_server — служба подписки на обновления (WebSocket-сервер);
- d_auth_server — служба аутентификации, авторизует клиентов, подтверждает выданные им токены (HTTP-сервер);
- d_redis — база данных Redis;
- logging_transport — служба журналирования.

ViPNet Prime NVS

- nvs_core_1 — функциональная служба модуля;
- nvs_telemetry_1 — служба обработки данных телеметрии;
- nvs_file-storage_1 — служба файлового хранилища;
- nvs_sink_1 — служба приема данных;
- nvs_mongo_1 — система управления базами данных MongoDB;
- nvs_kafka_1 — распределённый журнал сообщений;
- nvs_nginx_1 — обратный прокси-сервер;
- nvs_elasticsearch_1 — поисковый движок;
- nvs_zookeeper_1 — консистентное ядро;
- nvs_nats_1 — брокер сообщений;
- nvs_redis_1 — кеш;
- nvs_reports_1 — служба отчетов.

ViPNet Prime NVS Сборщик данных

nvs-rc — служба сбора данных с snmp-устройств.

ViPNet Prime PMM

- `pmm_pmm-edge-server_1` — клиентское приложение, которое встраивается в веб-интерфейс ViPNet Prime, проксирует HTTP-запросы к серверу и уведомления на основе WebSocket;
- `pmm_pmm-core_1` — функциональная служба модуля;
- `pmm_pmm-mftp_1` — создание конвертов с политиками безопасности для отправки транспортом MFTP;
- `pmm_pmm-worker_1` — исполнение ресурсоемких длительных задач, например, проверок политик безопасности на согласованность правил;
- `pmm_pmm-mongo_1` — система управления базами данных MongoDB.

ViPNet Connect Book

- `connect_module_core_1` — функциональная служба модуля;
- `connect_module_postgresql_1` — система управления базами данных PostgreSQL;
- `connect_module_nginx_1` — обратный прокси-сервер.



Системные папки ViPNet Prime

При управлении дисковым пространством компьютеров, на которых установлен ViPNet Prime, учитывайте размер основных папок. При значительном росте размера сети, объем папок может расти на 30% и более от указанного в столбце «Рекомендуемый объем» в таблице ниже.

При управлении дисковым пространством компьютеров, на которых установлен ViPNet Prime, учитывайте:

- размер основных папок — при значительном росте размера сети, объем папок может расти на 30% и более от указанного в столбце «Типовой объем» в таблице ниже;
- процент свободного места раздела, где расположена папка `/var/lib/infotecs` — не менее 30% или 20 Гбайт.

Чтобы посмотреть размер свободного и процент использованного места раздела с папкой `/var/lib/infotecs` выполните команду:

```
$ df -h /var/lib/infotecs
```

Таблица 11. Системные папки ViPNet Prime

Модуль	Путь	Описание	Типовой объем
ViPNet Prime Core	<code>/var/lib/infotecs/smp-ms/data</code>	база данных	6 Гбайт
транспортный сервер ViPNet UT	<code>/var/lib/infotecs/transport</code>	файловое хранилище для пакетов перед их отправкой	27 Гбайт
ViPNet Prime VPN	<code>/var/lib/infotecs/vpn-kc/data</code>	база данных служб	60 Гбайт
	<code>/var/lib/infotecs/vpn-ms/data</code>	база данных служб	8 Гбайт

Модуль	Путь	Описание	Типовой объём
	/var/lib/infotecs/vpn-kc/data/dst-service/export	файлы дистрибутивов ключей	40 Гбайт
ViPNet Connect Book	/var/lib/infotecs/connect_module/data	база данных	1 Гбайт
ViPNet Prime PMM	/var/lib/infotecs/pmm/data	база данных	40 Гбайт
ViPNet Prime NVS	/var/lib/infotecs/nvs/data	база данных	5 Гбайт
		данные мониторинга	80 Гбайт в месяц
Сборщик данных	/var/lib/infotecs/nvs-rc/db	база данных	5 Гбайт
Журналы модулей	/var/log/infotecs	журналы	52 Гбайт
Раздел для установки и обновления ПО ViPNet Prime	/usr/share/infotecs	папка, в которую распаковывается ПО ViPNet при установке	13 Гбайт
Раздел для хранения контейнеров Docker	/var/lib/docker	папка, в которой хранятся контейнеры Docker и файлы для их работы	45 Гбайт
Раздел для хранения данных PostgreSQL	/var/lib/postgresql	база данных	



D

Расчёт потребления ресурсов виртуальной машины

В таблице представлена зависимость потребления ресурсов процессора (далее — ЦП) и оперативной памяти (далее — ОЗУ) от количества узлов и связей в сети. Расчёт приведён для базовой установки ViPNet Prime (ViPNet Prime Core, ViPNet Prime VPN, ViPNet UT):

- Процессор: 12 ядер.
- Оперативная память: 32 Гбайт.

Сценарий/Количество узлов	500		1000		6000		10000		15000	
	ЦП	ОЗУ	ЦП	ОЗУ	ЦП	ОЗУ	ЦП	ОЗУ	ЦП	ОЗУ
Созданы узлы	40%	9,8 ГБ	40%	10 ГБ	40%	13,3 ГБ	40%	14,3 ГБ	40%	15 ГБ
Выпущены дистрибутивы ключей	70%	11,3 ГБ	70%	11,6 ГБ	80%	15,2 ГБ	80%	16,4 ГБ	80%	18 ГБ
Созданы связи и разослана справочно-ключевая информация	65%	12,5 ГБ	70%	13,4 ГБ	70%	19 ГБ	80%	21,5 ГБ	100 %	25 ГБ
Суммарное количество связей	250000		1000000		6000000		10000000		15000000	

С увеличением узлов и связей в сети увеличивается потребление ресурсов виртуальной машины при выполнении ресурсоёмких операций. [Минимальные системные требования](#) подходят для сетей размером до 6000 устройств.



Сетевые соединения ViPNet Prime



Примечание. Ниже указаны порты, которые по умолчанию используются ViPNet Prime и модулями. Если при установке ViPNet Prime вы меняли порты, установленные по умолчанию, учитывайте это при построении сетевых соединений.

№	Протокол, порт	Источник — Назначение	Требуется ли открывать порт	Описание
1	TCP 443 (HTTPS)	- Компьютер администратора — ViPNet Prime - ViPNet-узлы — ViPNet Prime - Модули — ViPNet Prime Core	Да	Трафик от веб-интерфейса, команды, запросы, данные модулей
2	TCP 48080 (HTTP)	ViPNet-узлы — ViPNet Prime	Да, только для интерфейса tun0	Справочники, обновления ПО ViPNet, ответные квитанции устройств
3	TCP 48443 (HTTPS)	ViPNet-узлы — ViPNet Prime	Да	Справочники, обновления ПО ViPNet, ответные квитанции устройств

№	Протокол, порт	Источник — Назначение	Требуется ли открывать порт	Описание
4	TCP 447 (HTTPS)	Компьютер администратора — ViPNet Prime (ViPNet Connect Book)	Да	Команды, запросы, данные модулей
5	TCP 8811 (HTTPS)	- Модули — ViPNet Prime Core - Компьютер администратора — ViPNet Prime - Между внутренними компонентами ViPNet Prime Core - ViPNet Coordinator HW5 — ViPNet Prime	Нет	Аутентификация пользователей и служб
6	TCP 80 (HTTP)	Между внутренними компонентами ViPNet Prime Core	Нет	Команды, запросы, данные модулей
7	TCP 5671 (HTTPS)	- Модули — ViPNet Prime Core - Между внутренними компонентами ViPNet Prime Core	- Да, только для машин Prime KC и MS; - Для схемы с установкой ViPNet Prime NVS на отдельной машине открыть для машины ViPNet Prime NVS	Данные брокера сообщений RabbitMQ
8	TCP 5673 (HTTPS)	Модуль ViPNet Prime VPN — ViPNet Prime Core (Rabbit MQ)	Нет	Данные брокера сообщений RabbitMQ
9	TCP 15672 (HTTPS)	Модуль ViPNet Prime VPN — ViPNet Prime Core (Rabbit MQ)	Нет	Данные брокера сообщений RabbitMQ
10	TCP 48081 (HTTP)	Между транспортным сервером в составе ViPNet Prime и внутренними компонентами ViPNet Prime Core	Нет	Взаимодействие транспортного сервера и транспортного клиента через интерфейс защищённой сети tun0. Шифрование TLS не используется
11	TCP 514 (HTTPS)	Между внутренними компонентами транспортного сервера	Нет	Логи

№	Протокол, порт	Источник — Назначение	Требуется ли открывать порт	Описание
12	TCP 5201 (HTTPS)	ViPNet Prime — ViPNet Connect Book	Нет	Команды, запросы, данные модулей
13	TCP 28090 (HTTP)	ViPNet Prime — ViPNet Prime NVS (Nginx)	На машине ViPNet Prime NVS открыть доступ только для машины ViPNet Prime KC (для схемы с установкой ViPNet Prime NVS на отдельной машине)	Пользовательские данные, данные мониторинга
14	TCP 4222 (NATS)	ViPNet Prime — ViPNet Prime NVS	Да	Приём и отправка данных по протоколу TLS на сборщики данных, расположенные в корпоративной сети
15	TCP 28080	ViPNet Prime — ViPNet Prime NVS (внешние агенты, сервер)	Да	Данные мониторинга
16	TCP 26022 (HTTPS)	ViPNet Prime — ViPNet Prime NVS (Nginx)	Нет	Нотификации, данные модулей
17	TCP 9092 (HTTPS)	ViPNet Prime — ViPNet Prime NVS (Kafka)	Нет	Нотификации, данные модулей
18	TCP порт ViPNet Prime PMM (администратор задает при установке)	ViPNet Prime — сервер ViPNet Prime PMM (Nginx)	Нет	Команды, запросы, данные модулей
19	TCP/UDP 162	ViPNet Prime NVS (сборщик)	Да, на сборщике	Подключение устройств, опрашиваемых по SNMP, обнаружение устройств
20	TCP/UDP 161	ViPNet Prime NVS (сборщик)	Да, на сборщике	Опрос SNMP-агента SNMP-менеджером



Термины и сокращения

TLS-сертификат

Сертификат X.509, который удостоверяет подлинность доменного имени сайта (конечной системы или субъекта, в более широком смысле) и позволяет зашифровывать соединение между веб-сервером и браузером. Для шифрования передаваемых данных используется протокол TLS.

ViPNet-идентификатор

Уникальный 4-байтовый идентификатор сетевого узла ViPNet, который состоит из номера сети ViPNet и порядкового номера узла. Идентификатор представлен в шестнадцатеричном виде, например, 2F400002.

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 удалённых узлов в приложениях ViPNet.

Защищённое устройство

Узел [защищённой сети](#), на котором установлено программное обеспечение ViPNet с функцией шифрования трафика.

Модуль ViPNet Network Visibility System

Модуль системы управления ViPNet Prime для мониторинга состояния устройств.

Модуль ViPNet Prime PMM

Модуль системы ViPNet Prime для управления политиками безопасности устройств [защищённой сети](#).

Модуль ViPNet Prime VPN

Модуль ViPNet Prime для управления [защищённой сетью](#).

Организация (ViPNet-организация)

Объект управления, подчинённые объекты которого логически изолированы от объектов других организаций. Представляет собой часть сети ViPNet, к управлению которой может быть предоставлен отдельный доступ в веб-интерфейсе ViPNet Prime.

Поколение ViPNet 4

Поколение продуктов ViPNet с централизованным управлением из ViPNet Administrator или ViPNet Prime и передачей транспортных конвертов по MFTP. Использует дистрибутивы ключей *.dst.

Поколение ViPNet 5

Поколение продуктов ViPNet с централизованным управлением из ViPNet Prime и передачей транспортных сообщений по HTTP/HTTPS. Использует дистрибутивы ключей *.ds5.

Поставщик услуг

Компания, которая владеет серверной частью системы управления ViPNet Prime и лицензиями на продукты ViPNet и предоставляет доступ к ViPNet Prime по ссылке другим компаниям.

Сеть ViPNet

Защищённая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов. Узлы обмениваются информацией с помощью наложенной маршрутизации. Каждая сеть имеет свой уникальный номер.

Транспортный сервер UT

Серверная часть транспортного компонента UT ViPNet Prime. Обеспечивает передачу транспортных сообщений по протоколу HTTP от ViPNet Prime к транспортному клиенту UT устройств сети ViPNet, поддерживающих работу с дистрибутивом ключей *.ds5.

Файл лицензии

Разрешение на пользование определённым набором продуктовой линейки ViPNet. Определяет номер защищённой сети, максимальное количество лицензий того или иного программного обеспечения ViPNet, максимальную разрешённую версию программного обеспечения ViPNet, срок действия лицензии и другие параметры.

Файл лицензии выдает ИнфоТекС в файле *.itcslic.

Формат PEM

Формат текстового файла с сертификатом в кодировке Base64. Отличается тегами:

- с которого начинается: -----BEGIN CERTIFICATE-----
- и которым заканчивается: -----END CERTIFICATE-----

Файл в формате PEM может иметь расширение PEM, CER, CRT или KEY.

Центр управления

Обязательное устройство сети ViPNet, связанное с устройствами всех организаций. Обеспечивает отправку обновлений об изменении свойств объектов, связей между объектами, лицензионных ограничений, ключей на защищённые устройства ViPNet. Это устройство функционирует как ViPNet-клиент. Имя по умолчанию — Control Center.