



ViPNet Prime

Руководство администратора

Версия продукта: 1.9.14

© АО «ИнфоТеКС», 2026

ФРКЕ.00222-02 32 05

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.....	10
О документе.....	11
Соглашения документа.....	11
Комплект документации.....	12
Что нового в версии 1.9.14.....	13
Особенности и ограничения.....	16
Совместимые продукты ViPNet.....	18
Обратная связь.....	20
 Глава 1. Общие сведения	21
О защищенной сети	22
О ViPNet Prime	24
 Глава 2. Разграничение полномочий на основе ролей администраторов	27
Роли для управления ViPNet Prime	28
Суперадминистратор	29
Сервисный администратор.....	29
Оператор Prime	30
Роли для управления организацией	32
Владелец организации.....	32
Администратор организации	33
Сетевой администратор шлюза безопасности	34
Аудитор устройств.....	35
 Глава 3. Начало работы	36
Вход в ViPNet Prime	37
Защита канала управления.....	37
Вход по паролю	39
Изменение пароля своей учетной записи	39
Вход по сертификату.....	40
Вход через AD FS	41
Интерфейс ViPNet Prime	42
Главная консоль	42
Управление организацией.....	43
Модуль ViPNet VPN.....	44

Подключение модулей к ViPNet Prime	46
Глава 4. Управление лицензиями.....	47
Общая информация.....	48
Загрузка и обновление лицензии.....	51
Включение режима фиксированного распределения лицензий	54
Распределение лицензий для нескольких организаций	55
Распределение лицензий для отдельной организации.....	56
Выбор пакета лицензий для пользователей	57
Создание отчета об использовании лицензий	58
Освобождение лицензии ViPNet Connect	62
Глава 5. Настройка аутентификации	63
Способы аутентификации.....	64
Аутентификация администраторов в ViPNet Prime.....	65
Аутентификация по сертификату	67
Порядок действий	67
Требования к сертификату администратора	68
Установка сертификата УЦ и CRL.....	68
Загрузка сертификата администратора	69
Контроль за сроком действия сертификатов	69
Обновление сертификата администратора.....	70
Отключение аутентификации по паролю	71
Пример использования ViPNet PKI Client для аутентификации по сертификату.....	72
Аутентификация по паролю	74
Управление временем блокировки входа в учетную запись	74
Настройка длины и срока действия пароля.....	75
Доменная аутентификация.....	77
Установка и настройка AD FS на стороне AD	77
Настройка доменной аутентификации с помощью служб федераций AD FS	80
Глава 6. Управление организацией	83
Порядок создания организации	84
Управление учетными записями администраторов.....	85
Создание учетной записи администратора в главной консоли	85
Создание учетной записи администратора в организации	87
Назначение ролей учетной записи в организации.....	88
Управление организационной структурой	90
Создание организации	90

Создание подразделения	90
Выбор организации и подразделения	91
Удаление организации или подразделения	92
Управление пользователями	93
Добавление пользователей вручную	93
Импорт учетных записей пользователей из файла CSV	94
Настройка интеграции с Active Directory	96
Импорт учетных записей пользователей из Active Directory	98
Удаление пользователей	99
Перемещение пользователей и устройств подразделения	99
Управление устройствами	101
Создание устройств	101
Назначение пользователя на устройства	102
Изменение имени устройства	102
Просмотр и удаление устройств организации	103
Глава 7. Управление защищенной сетью	107
Порядок создания сети организации	108
Создание центра управления и его координатора	109
Инициализация ключевого центра организации	111
Переключение координаторов поколения ViPNet 5 на работу с новыми протоколами	112
Создание защищенных узлов	114
Создание координатора	114
Создание клиента	115
Создание ViPNet xFirewall	117
Создание узла ViPNet CSS Connect HW	117
Создание узлов L2	118
Защищенный смартфон ViPNet HardPhone	119
Создание узлов квантовой сети	121
Создание узлов	122
Создание групп пользователей или узлов	124
Настройка сложности паролей пользователей и администраторов узлов	125
Задание пароля администратора узла	126
Компрометация пароля	128
Настройка шлюзов безопасности	129
Подключение к внешней сети	129
Создание ресурсов	132
Включение функций VPN, DPI, IPS и других	136

Защищенный интернет-шлюз	140
Включение функции кластера.....	140
Настройка доступа к веб-интерфейсу координатора	141
Настройка применения ViPNet Coordinator IG в промышленной сети	143
Смена типа и лицензии координатора.....	144
Смена поколения координатора.....	146
Различия в доступности функций между поколениями координатора	148
Регистрация ключевых блокнотов.....	150
Скачивание резервной конфигурации координатора	152
Аутентификация с учетной записью ViPNet Prime на координаторах поколения ViPNet 5.....	154
Настройка клиентов.....	155
Изменение уровня полномочий на клиенте	155
Блокировка VPN без ViPNet EPP	156
Расширенные настройки ViPNet Client	157
Настройка профиля DNS.....	158
Создание профиля DNS	159
Выбор профиля DNS по умолчанию	160
Группы серверов соединений	161
Смена типа, поколения узла и лицензии клиента	165
Поведение функций и настроек при смене платформы узла	169
Управление связями.....	171
Рекомендации по созданию связей.....	173
Создание связей между объектами организации.....	173
Копирование связей пользователя	174
Копирование связей шлюза безопасности	175
Дистрибутивы ключей.....	176
Выдача паролей пользователей	176
Создание дистрибутива ключей	178
Массовое создание и скачивание дистрибутивов ключей	179
Назначение прикладного ПО ViPNet	181
Назначение серверного ПО ViPNet Connect	182
Назначение ViPNet Connect одному пользователю	184
Назначение ViPNet Connect нескольким пользователям.....	184
Назначение ViPNet Деловая почта	185
Мастер-ключи.....	186
Порядок смены мастер-ключей поколения ViPNet 5	189
Отключение автоматической отправки обновлений ключей	189
Смена мастер-ключей организации	190

Смена мастер-ключей сети	193
Порядок смены мастер-ключей	194
Подготовка к смене мастер-ключей	195
Проверка наличия РНПК на сетевых узлах	196
Смена мастер-ключей персональных ключей	197
Смена мастер-ключей ключей обмена и защиты	198
Смена мастер-ключа доверенных организаций	200
Смена межсетевого мастер-ключа	201
Взаимодействие между организациями и защищенными сетями	203
Создание взаимодействия между организациями одной сети	203
Порядок создания взаимодействия между сетями	205
Особенности взаимодействия с сетью под управлением ViPNet Administrator	206
Создание запроса на взаимодействие с сетью	207
Создание взаимодействия между сетями	207
На мастер-ключах ГОСТ 28147-89	208
На мастер-ключах ГОСТ 34.12-2018	212
Завершение установки взаимодействия с сетью	213
Обработка межсетевой информации	214
Отправка межсетевой информации	216
Изменение шлюзового координатора	217
Связи с доверенными объектами	219
Управление доступом к ресурсам при межсетевом взаимодействии	221
Управление совместным доступом к сервисным функциям	223
Прекращение совместного доступа к сервисным функциям	224
Прекращение взаимодействия	224
Отправка обновлений на узлы	226
Управление файлами обновления ПО ViPNet	226
Обновление ПО ViPNet на узлах	227
Просмотр журнала транспортных конвертов	230
Обновление справочников и ключей	232
Компрометация ключей	235
Компрометация узла	235
Компрометация узлов управления	235
Глава 8. Управление адресной книгой ViPNet Connect Book	236
Интерфейс модуля ViPNet Connect Book	237
Настройка SIP-сервера	238
Добавление контакта	239
Создание и назначение полномочий	240

Импорт дополнительных данных о контакте из Active Directory	241
Глава 9. Администрирование.....	242
Просмотр версии	243
Просмотр журнала событий.....	244
Интеграция с сервисами отправки уведомлений по электронной почте и СМС	246
Контроль целостности и работы ПО ViPNet Prime.....	248
Срок хранения записей в журнале транспортных конвертов	249
Приложение А. Ограничения в названиях объектов	250
Приложение В. Поддерживаемые лицензии в ViPNet Prime	251
Приложение С. Поддерживаемые функции сетевых узлов	256
Приложение D. Возможные неполадки	265
Не создаются дистрибутивы ключей для узлов поколения ViPNet 5	265
Сессия истекает слишком быстро	265
Не приходит подтверждение связей при межсетевом взаимодействии	266
Не удается создать мастер-ключи.....	266
Устройство устанавливает удаленное в ViPNet Prime обновление	267
Не сопоставились лицензии при загрузке файла.....	268
Не принимается межсетевая информация из доверенной сети	268
Отображаются неверные дата и время mftp-конвертов	269
Приложение Е. История версий	270
Что нового в версии 1.9.12	270
Что нового в версии 1.9.11.1	270
Что нового в версии 1.9.11	271
Что нового в версии 1.9.10	271
Что нового в версии 1.9.9.....	272
Что нового в версии 1.9.8.....	272
Что нового в версии 1.9.6.....	273
Что нового в версии 1.9.5.3	276
Что нового в версии 1.9.5.2	276
Что нового в версии 1.9.5.1	276
Что нового в версии 1.9.5.....	277
Что нового в версии 1.9.0.....	278
Что нового в версии 1.7.2 fix4	284
Что нового в версии 1.7.2 fix3	285

Что нового в версии 1.7.2 fix2	285
Что нового в версии 1.7.2 fix.....	285
Что нового в версии 1.7.2.....	285
Что нового в версии 1.8	285
Что нового в версии 1.7.1.....	287
Что нового в версии 1.7	287
Что нового в версии 1.6	287
Приложение F. Термины и сокращения.....	289



Введение

О документе	11
Комплект документации	12
Что нового в версии 1.9.14	13
Особенности и ограничения	16
Совместимые продукты ViPNet	18
Обратная связь	20

О документе

Документ предназначен для администраторов ViPNet Prime, содержит указания по работе и описание основных сценариев создания и администрирования [защищенной сети](#).

Информация о дополнительных модулях системы управления и рекомендации по их использованию содержатся в документации модулей.

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.

Комплект документации

В формате PDF:

- ViPNet Prime. Руководство по установке.
- ViPNet Prime. Руководство администратора.
- ViPNet Prime. Лицензионное соглашение с конечным пользователем на использование ПО.

Лицензионные соглашения на компоненты сторонних производителей, которые использовались при разработке ViPNet Prime, см. в ZIP-архиве «ViPNet Prime. Руководство администратора (Приложение)».

Связанные документы (не входят в комплект поставки ViPNet Prime):

- ViPNet Prime Policy Management. Руководство администратора.
- ViPNet Prime Network Visibility System. Руководство администратора.
- ViPNet Prime Network Visibility System. Параметры приложений.

Что нового в версии 1.9.14

- **Поддержка функций:**
 - Failover для ViPNet Coordinator HW10
 - IPS, обновление IPS и обновление баз Malware Detection для ViPNet Coordinator IG
- **Поддержка узлов:**
 - Учебных узлов квантовой сети ViPNet QCL Server Academic Edition и ViPNet QCL Client Academic Edition
Подробнее см. [Создание узлов сети квантового распределения ключей](#).
 - Шифратора ViPNet L2-10G, использующего ключевые блокноты
Подробнее см. [Создание узлов L2](#).

- **Поддержка лицензионного объекта GeoIP update для скачивания базы данных стран с сервера обновлений**

Теперь вы можете загружать в ViPNet Prime Policy Management базу данных стран и использовать ее в правилах фильтрации по странам. Вы можете скачать базу данных стран с сервера обновлений при наличии лицензионного объекта GeoIP update и данных для входа на сервер обновлений. Об использовании базы данных стран см. в документе «ViPNet Prime Policy Management. Руководство администратора».

- **Создание дистрибутива ключей в фоновом режиме**

Теперь вы можете создавать дистрибутивы ключей не поддерживая активным сеанс администратора или работая в другом модуле или другой организации. Подробнее см. [Создание дистрибутива ключей](#) и [Массовое создание и скачивание дистрибутивов ключей](#).

- **Возможность распечатать пароль от дистрибутива ключей в любой момент до удаления узла из модуля VPN**

Подробнее см. [Создание дистрибутива ключей](#) и [Массовое создание и скачивание дистрибутивов ключей](#).

- **Возможность отправлять на клиент индивидуальный файл с настройками custom.yaml**

Подробнее см. [Расширенные настройки ViPNet Client](#).

- **Новый механизм отправки обновлений ПО на устройства**

Это позволит снизить нагрузку на ViPNet Prime и избежать отправки неверного ПО на устройства, которые поддерживают обновление ПО с помощью этого механизма. Сценарий отправки обновлений остался прежним, ViPNet Prime автоматически определяет, как отправлять обновление на узел.

Подробнее см. [Отправка обновлений на узлы](#).

- **Объединение журнала транспортных конвертов MFTP с журналом транспортных конвертов UT**

Теперь вся информация о транспортных конвертах отображается в едином журнале транспортных конвертов с указанием транспорта в разделе **Управление организацией**. Транспортные конверты, полученные при межсетевом взаимодействии, находятся в разделе **Доверенное взаимодействие > Организации**.

- **Новые возможности отправки обновлений справочников и ключей**

Теперь вы можете отправить справочники и ключи на несколько выбранных устройств, независимо от поколения узла и наличия ранее отправленных на узел обновлений справочников и ключей. Подробнее см. [Обновление справочников и ключей](#).

- **Администратор ViPNet Prime может скачать файл обновления ПО, ранее загруженный в ViPNet Prime**

Подробнее см. [Управление файлами обновления ПО ViPNet](#).

- **Сохранение связи с узлами доверенной сети при изменении варианта ключей узла в ViPNet Administrator**

Теперь справочники и ключи автоматически отправляются на связанные узлы при приеме информации, в которой изменился вариант ключей узла в ViPNet Administrator. Это позволяет не терять связь между узлами своей и доверенной сети.

- **Поддержка нового типа ключевых блокнотов КУБИТ для сетей, в которых используются ViPNet Coordinator KB5**

Подробнее см. [Регистрация ключевых блокнотов](#).

- **Управление группами серверов соединений**

Теперь в ViPNet Prime вы можете централизованно создавать и назначать на клиентские узлы группы серверов соединений. Подробнее см. [Группы серверов соединений](#).

- **ViPNet Prime запрещает создавать цепочки серверов соединений, в которых сервер соединений с вершины цепочки недоступен напрямую из внешней сети, так как это может нарушить работу сети**
- **ViPNet Prime запрещает создавать дистрибутив ключей для всех узлов поколения ViPNet 4, кроме ViPNet Client, если не задан пароль администратора для узла или для всех узлов организации, так как без пароля администратора вы не сможете настроить узел**
- **Возможность выбирать лицензию при включении функции на узле или смене лицензии**
- **Отправка файлов обновлений ПО на ViPNet Client 5 с помощью custom.yaml**

Подробнее см. [Обновление ПО ViPNet на узлах](#).

- **Новые требования к паролям учетных записей ViPNet Prime:**
 - Проверка, что при смене собственного пароля изменилось минимум 3 символа.
 - Настройка количества последних использованных паролей, которые нельзя задать при смене собственного пароля.
 - Возможность задать обязательное требование к смене предустановленного пароля.

Подробнее см. [Настройка длины и срока действия пароля](#).

- **Возможность просмотреть версию ViPNet Prime и его модулей**

Подробнее см. [Просмотр версии](#).

- **Изменения в интерфейсе**

- **Лицензионный объект Failover для шлюзов безопасности поколения ViPNet 5 теперь называется Failover v.5**
- **Возможность скрыть истекшие лицензии в разделе Лицензии и при распределении лицензий в организации**
- **Отображение новых параметров лицензий**
Теперь вы можете по параметрам лицензии определить идентификатор лицензии, срок действия, максимальную версию и какой организации она выдана.
- **Теперь срок действия сертификата администратора проверяется сразу при загрузке и, если до истечения срока осталось менее 30 дней, появляется красный маркер**
- **Возможность искать узлы по их идентификатору VPN ID в списках**
Вы можете искать узлы в модуле VPN по их идентификатору во всех окнах, где есть списки узлов. Для этого в строке поиска введите VPN ID узла, который ищете.

Особенности и ограничения

- При установке ViPNet Prime на Astra Linux SE версии 1.7.5.16 не включайте режим замкнутой программной среды, так как это приведет к неработоспособности ViPNet Prime.
- Перед обновлением ViPNet Prime проверьте, что для всех дополнительных модулей, которые у вас установлены, есть обновление, совместимое с ViPNet Prime 1.9.14 (см. системные требования в документации модулей).



Внимание! Если для модуля ещё нет версии, совместимой с ViPNet Prime 1.9.14, не обновляйте ViPNet Prime. Иначе это приведёт к неработоспособности ViPNet Prime.

- В ViPNet Prime нет возможности вернуться к использованию версии ниже текущей.
- При обновлении Astra Linux с версии 1.7.5 до версии 1.8 вы потеряете все пользовательские данные в системных папках. Это приведет к тому, что ViPNet Prime будет удален с компьютера, и будет необходимо повторно установить ViPNet Prime после обновления ОС.
- Создавайте не более 40000 защищённых узлов в ViPNet Prime.
- Не создавайте полносвязную топологию более чем для 10000 защищённых узлов.
- Регистрируйте за ViPNet Coordinator IG 5:
 - не более 100 клиентов — для исполнений Coordinator IG1000,
 - не более 10 клиентов — для исполнений Coordinator IG100.
- Используйте в качестве узла центра управления клиент [поколения ViPNet 5](#) с ключами *.ds5 только если в защищённой сети не будет ни одного узла поколения ViPNet 4.
- Для поддержки шифрования на алгоритмах ГОСТ 34.12-2018 «Магма» и «Кузнечик» в защищенной сети организации используйте [узлы поколения ViPNet 5](#). В качестве сервера соединений назначьте координатор поколения ViPNet 5, который поддерживает маршрутизацию трафика на этих алгоритмах.
- Не поддерживается удаленное обновление ПО из ViPNet Prime ViPNet Coordinator KB 4.
- Сменить поколение клиента или координатора можно только для узлов поколения ViPNet 4.
- ViPNet Coordinator HW 5 версии 5.2.1 и ниже не поддерживает смену мастер-ключа ключей защиты обновлений без установки нового дистрибутива ключей. Чтобы сменить мастер-ключи организации, сначала обновите ПО ViPNet Coordinator HW 5 до версии 5.3.1 и выше.
- Если в защищенной сети установлен ViPNet Coordinator HW версии 5.2.1, включите для него [функцию VPN-шлюз](#) или обновите ПО до версии 5.3.1. Иначе на координаторе могут не применяться справочники и ключи.
- Если в ViPNet Prime одновременно вносят изменения более семи администраторов, может снижаться скорость обработки запросов.

- Не рекомендуется изменять один объект в ViPNet Prime одновременно несколькими администраторами, иначе изменения могут не сохраниться или будут не видны другому администратору.
- Информацию о версиях ViPNet Coordinator HW 5, в которых будет поддержана возможность удаленного подключения пользователя с ролью сетевой администратор шлюза безопасности из ViPNet Prime по ссылке к веб-интерфейсу ViPNet Coordinator HW 5 см. в документации ViPNet Coordinator HW 5.
- При обновлении ViPNet Prime на версию 1.9.14 из модуля VPN будут удалены все файлы обновления, загруженные администратором в предыдущих версиях. После обновления ViPNet Prime нужно будет снова загрузить эти файлы в модуль VPN.
- Если в вашей сети есть узлы ViPNet Coordinator KB 4 с номером комплекта больше 9999, вы не сможете:
 - обновить мастер-ключи сети;
 - ввести в действие мастер-ключ ключей обмена организации;
 - скачать дистрибутив, который был создан в ViPNet Prime версии ниже 1.9.14;
 - перейти с ключевых блокнотов КУБИТ на ДСДР;
 - для всех ViPNet Coordinator KB и ViPNet L2-10G создать дистрибутив и отправить обновление справочников и ключей.

Совместимые продукты ViPNet

Версии модулей см. в «ViPNet Prime. Руководство по установке», «Состав ViPNet Prime».

Ниже указаны версии продуктов, которые совместимы с ViPNet Prime версии 1.9.14. Полный список поддерживаемых типов узлов защищенной сети см. в разделе [Поддерживаемые лицензии в ViPNet Prime](#).

Поколение ViPNet 5

- ViPNet Coordinator HW версии 5.1.2 и выше.
- ViPNet Coordinator KB версии 5.0.0 и выше.
- ViPNet Coordinator IG версии 5.1.0 и выше.
- ViPNet Client 5 for Linux версии 5.0.0 и выше.
- ViPNet Client 5 for Windows версии 5.0.0 и выше.
- ViPNet Client 5 for Android версии 5.2.1 и выше.
- ViPNet Client 5 for macOS версии 5.0.2 и выше.
- ViPNet Client 5 for iOS версии 5.0.2 и выше.
- ViPNet Client 5 для ОС Аврора версии 5.1.0 и выше.

Поколение ViPNet 4

- ViPNet Coordinator HW версии 4.5.4 и выше.
- ViPNet Coordinator IG версии 4.5.1 и выше.
- ViPNet Coordinator KB версии 4.3.4 и выше.
- ViPNet xFirewall версии 5.6.2 и выше.
- ViPNet L2-10G версии 2.6.0 и выше.
- ViPNet Client 4U for Linux версии 4.15 и выше.
- ViPNet Client 4U for Windows версии 4.14 и выше.
- ViPNet Client 4U for Android версии 4.0.0 и выше.
- ViPNet Client 4U for iOS версии 4.4.0 и выше.
- ViPNet Client 4U for macOS версии 4.4.0 и выше.
- ViPNet Client for Windows версии 4.5.3 и выше.
- ViPNet Client для ОС Аврора версии 4.0.1 и выше.
- ViPNet CSS Connect HW версии 1.0.0 (содержит ViPNet Client for Android версии 4.2.1 и ViPNet CSS Connect версий 2.13.1) и ViPNet CSS Connect HW версии 1.1.1 (содержит ViPNet Client for Android версии 4.0.0 и ViPNet CSS Connect версий 2.12).

- ViPNet L2Q-10G версии 2.3.3 и выше.
- ViPNet QTS Lite версии 1.0 и выше:
 - ViPNet РУКС Лайт версии 1.0.1 и выше.
 - ViPNet КУКС Лайт версии 1.0.1 и выше.
- ViPNet QTS 1.0 и выше:
 - ViPNet РУКС версии 1.0.1 и выше.
 - ViPNet КУКС версии 1.0.1 и выше.
- ViPNet РУКС VA версии 1.0.3 и выше.
- ViPNet КУКС VA версии 1.0.3 и выше.
- ViPNet QCL Client Academic Edition версии 1.0 и выше.
- ViPNet QCL Server Academic Edition версии 1.0 и выше.

Прикладное ПО

- ViPNet Connect 2.0 и выше:
 - ViPNet ConServer и ViPNet CPNS версии 2.13.1 и выше.
 - ViPNet Connect PSIP Server версии 2.12.5 и выше.
 - ViPNet CSS Connect for Windows версии 2.13.1 и выше.
 - ViPNet CSS Connect for macOS версии 2.13 и выше.
 - ViPNet CSS Connect for Linux версии 2.13 и выше.
 - ViPNet CSS Connect for Android версии 2.13.1 и выше.
 - ViPNet CSS Connect for iOS версии 2.13 и выше.
- ViPNet CSS Connect 3.0 и выше:
 - ViPNet CSS ConServer версии 3.1 и выше.
 - ViPNet CSS Connect for Windows версии 3.1.1 и выше.
 - ViPNet CSS Connect for macOS версии 3.1.1 и выше.
 - ViPNet CSS Connect for Linux версии 3.1.1 и выше.
 - ViPNet CSS Connect for Android версии 3.1 и выше.
 - ViPNet CSS Connect for iOS версии 3.1 и выше.
 - ViPNet CSS Connect для ОС Аврора версии 3.2 и выше.
- Управление возможностью использования ViPNet Деловая почта на узле:
 - ViPNet Деловая Почта для Windows версии 4.5.3 и выше.
 - ViPNet Деловая Почта для Linux версии 1.4.0 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

О защищенной сети	22
О ViPNet Prime	24

О защищенной сети

Защищенная сеть — виртуальная частная сеть (VPN), построенная по технологии ViPNet, которая может быть развернута поверх локальных или глобальных сетей любой структуры. Трафик между узлами такой сети защищается с помощью шифрования на симметричных ключах. Ключи распределяются централизованно.

Защищенная сеть состоит из узлов, на которых установлено программное обеспечение (далее — ПО) ViPNet:

- Координаторы — шлюзы безопасности, которые маршрутизируют трафик, передают управляющую информацию между узлами защищенной сети, выполняют функции VPN-шлюза и межсетевого экрана.
- Конечные узлы, которые регистрируются на координаторе как на VPN-шлюзе:
 - ViPNet xFirewall — межсетевые экраны с расширенными функциями анализа и фильтрации трафика.
Могут быть в программном или программно-аппаратном исполнении.
 - Клиенты — компьютеры и мобильные устройства пользователей защищенной сети с ПО ViPNet Client или ViPNet HardPhone.
 - Узлы квантовой сети — узлы сети квантового распределения ключей, которые вырабатывают в паре с другими узлами квантовые или квантовозащищенные ключи.

В защищенной сети информация защищается с помощью ПО, которое выполняет две основные функции:

- Фильтрация трафика сетевых узлов.
- Шифрование соединений между сетевыми узлами.

Клиенты получают от своего координатора (сервер IP-адресов) информацию об узлах, параметрах доступа и их активности.

Координаторы могут туннелировать узлы локальной сети, на которых не установлено ПО ViPNet Client (открытые узлы). Такие устройства в защищенной сети называются [ресурсами](#). При передаче через публичные сети трафик ресурсов инкапсулируется и шифруется координаторами, за которыми расположены ресурсы. Трафик от ресурса до координатора передается в открытом виде, а от координатора — в зашифрованном. Поэтому при передаче через публичные сети трафик ресурсов защищен.

Узлы защищенной сети имеют:

- Идентификатор VPN ID — шестнадцатеричный идентификатор вида `xxxxxyyyy`, где `xxxx` — номер защищенной сети, `yyyy` — внутрисетевой идентификатор узла.
- ViPNet-адрес — сетевой адрес вида `xxxxxyyyzzzz`, состоящий из номера защищенной сети `xxxx`, номера координатора `yyyy` и номера клиента на координаторе `zzzz`.

При организации VPN на каждом узле защищенной сети каждому удаленному узлу и каждому ресурсу присваивается виртуальный IP-адрес, уникальный на данном компьютере. Виртуальные IP-адреса закрепляются не за IP-адресами, а за идентификаторами узлов. Каждому узлу выделяется столько виртуальных IP-адресов, сколько реальных адресов имеет этот узел в данный момент. Виртуальный IP-адрес ресурса, закрепленный за ним, существует до тех пор, пока существует этот реальный IP-адрес. За диапазоном IP-адресов ресурсов закрепляется диапазон виртуальных адресов. Диапазон виртуальных адресов существует, пока существует соответствующий диапазон реальных туннелируемых адресов координатора.

Узлы защищенной сети получают настройки из дистрибутива ключей. Он устанавливается на узлы и содержит сведения о лицензии на ПО ViPNet. После установки дистрибутива ключей информация о настройках передается на устройства защищенной сети по защищенным каналам VPN при автоматическом обновлении справочников и ключей. Максимальный интервал обновления справочников и ключей — 60 мин.

О ViPNet Prime

ViPNet Prime — это веб-приложение для централизованного управления ПО ViPNet на защищенных узлах.

В ViPNet Prime вы можете разделить защищенную сеть на логические части — организации. Каждая организация изолирована от другой организации и содержит свой набор пользователей и устройств. Для управления организациями вы можете предоставить доступ отдельным администраторам.

По умолчанию в ViPNet Prime создана организация с названием Core Network. В ней суперадминистратор создает минимальный набор устройств для работы защищенной сети:

- [центр управления](#);
- [центральный координатор](#).

Между организациями вы можете создать взаимодействие, чтобы предоставить объекты организации в совместное использование другим организациям, например, для регистрации клиентов доверенных организаций на общем координаторе или для использования общего DNS-сервера.

Вы можете использовать ViPNet Prime:

- в сервисной модели SaaS (Software as a service), инфраструктурой которой владеет поставщик услуг или крупное предприятие со сложной организационной структурой и предоставляет другим организациям или филиалам доступ к ViPNet Prime по подписке;
- в модели On-Premise в собственной корпоративной сети.

Далее поставщиком услуг будем называть компанию, которая устанавливает ViPNet Prime в своей инфраструктуре и предоставляет доступ к ViPNet Prime.

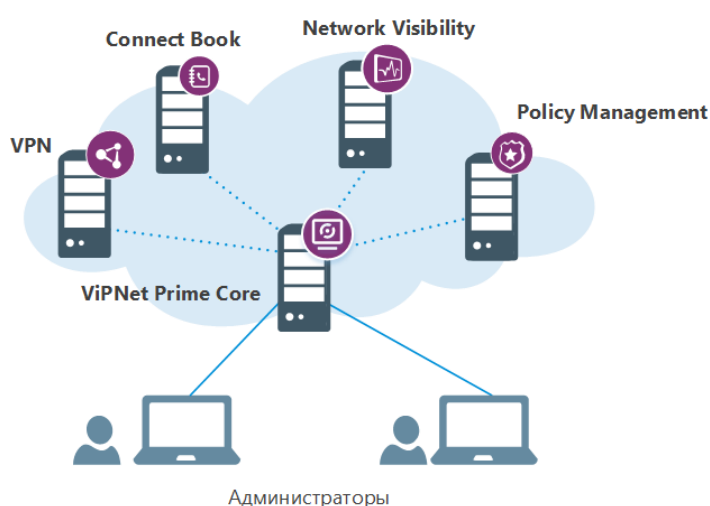


Рисунок 1. Состав системы управления ViPNet Prime

С помощью ViPNet Prime Core вы можете:

- управлять устройствами с ПО ViPNet в едином веб-интерфейсе;
- создавать [организации](#) — разделить [сеть ViPNet](#) на изолированные части с их пользователями, устройствами, администраторами;
- управлять доступом к администрированию организаций;
- настраивать доменную аутентификацию администраторов организаций через Active Directory Federation Services (AD FS);
- распределять лицензии на продукты ViPNet между организациями;
- вести учет использованных лицензий на продукты ViPNet;
- импортировать пользователей организации из Microsoft Active Directory или файла CSV;
- переходить в веб-интерфейс управления шлюзами безопасности поколения ViPNet 5.

К ViPNet Prime Core подключаются модули, которые отображаются в интерфейсе как разделы.

В модулях вы можете:

- в ViPNet Prime VPN:
 - создавать сеть VPN и управлять ее структурой:
 - создавать [клиенты](#), [координаторы](#), [ViPNet xFirewall](#), [узлы сети квантового распределения ключей](#);
 - задавать логическую структуру сети — создавать связи между узлами и пользователями;
 - настраивать доступ устройств к координаторам (IP-адреса, доменные имена) и способ подключения к внешней сети;
 - создавать защищенные каналы VPN между организациями или с другими сетями ViPNet;
 - совместно использовать сервисные функции сетевых узлов в доверенных организациях;
 - обновлять удаленно ПО ViPNet на узлах защищенной сети.

См. [Управление защищенной сетью](#).

В ключевом центре организации в модуле VPN создаются дистрибутивы ключей, с помощью которых передаются настройки на узлы защищенной сети — файлы с расширением *.dst или *.ds5.

- в ViPNet Prime Policy Management — централизованно управлять политиками безопасности на узлах.

См. «ViPNet Prime Policy Management. Руководство администратора».

- в ViPNet Prime Network Visibility System:
 - наблюдать за состоянием:
 - устройств, опрашиваемых по SNMP (координаторы, ViPNet xFirewall, квантовые узлы) — по протоколу SNMPv2 или SNMPv3;
 - клиентов — по защищенному каналу VPN или по TLS.

- просматривать сводную информацию о работе защищенных и открытых устройств.
См. «ViPNet Prime Network Visibility System. Руководство администратора».
- в ViPNet Connect Book — [управлять адресной книгой пользователей ViPNet CSS Connect](#).



2

Разграничение полномочий на основе ролей администраторов

Роли для управления ViPNet Prime	28
Роли для управления организацией	32

Роли для управления ViPNet Prime

Роли определяют полномочия администратора в веб-интерфейсе ViPNet Prime.

Если вы владеете серверной частью ViPNet Prime — компьютерами, на которых установлено ПО ViPNet Prime, то вы можете выступать как [поставщик услуг](#) для других организаций и предоставлять им доступ к ViPNet Prime по ссылке в интернете.



Примечание. Действия на компьютере, на котором установлен ViPNet Prime, выполняет администратор с учетной записью пользователя ОС, см. «ViPNet Prime. Руководство по установке».

Роли администраторов для поставщика услуг:

- [суперадминистратор](#);
- [сервисный администратор](#);
- [оператор Prime](#).

Роли администраторов для управления организацией:

- [владелец организации](#);
- [администратор организации](#);
- [сетевой администратор шлюза безопасности](#);
- [аудитор устройств](#).

Вы можете создать учетные записи администраторов с ролями:

- управления ViPNet Prime или поставщика услуг для администрирования и обслуживания ViPNet Prime;
- управления организациями, их подразделениями, устройствами и пользователями.

На уровне системы управления ViPNet Prime администратор имеет более высокие полномочия, чем на уровне управления организацией. Итоговые полномочия администратора — объединение полномочий ролей его учетной записи. Если вы создали учетную запись администратора в организации в разделе **Управление организацией > Учетные записи** и ей назначена роль в организации, то такому администратору вы не можете повысить полномочия до уровня системы управления.

Все действия администраторов в веб-интерфейсе фиксируются в [Журнале событий](#).

Суперадминистратор

- Обладает максимальными полномочиями управления и может быть только один.



Примечание. В документе роль суперадминистратора упоминается в сценариях, доступных только этой роли.

- Имеет встроенную учетную запись `admin`, ее нельзя удалить, и она не отображается в интерфейсе для остальных администраторов.
- Управляет лицензиями, учетными записями администраторов, предоставляет им права на управление организациями. Может управлять всеми организациями.
- Представляет организацию поставщика услуг (название организации по умолчанию — Core Network). При подключении модуля VPN в этой организации расположен центр управления защищенной сетью.
- Подключает функциональные модули к системе управления.
- Настраивает способ аутентификации администраторов (отключает аутентификацию по паролю).
- Включает режим фиксированного распределения лицензий.
- Загружает и удаляет файлы обновлений ПО ViPNet.
- Управляет автоматической отправкой справочников и ключей при регламентных процедурах.
- Проверяет целостность и работу ПО ViPNet Prime.
- Изменяет шлюзовой координатор.
- Обновляет мастер-ключи.
- Обновляет межсетевой мастер-ключ.
- Устанавливает межсетевое взаимодействие.
- Лицо с этой ролью может выполнять обязанности администратора безопасности, так как имеет доступ к инфраструктуре, на которой установлен ViPNet Prime.

Сервисный администратор

- Создает учетные записи сервисных администраторов, управляет личными сертификатами администраторов.
- Изменяет учетные записи администраторов (кроме суперадминистратора).
- Загружает файл лицензии и просматривает список всех лицензий на продукты ViPNet, но не распределяет их в организации.

- Настраивает сервисы для рассылки уведомлений по электронной почте и СМС.
- Не имеет доступа в функциональные модули.

Доступные разделы в **Главной консоли**:

- Сертификаты и CRL;
- Лицензии;
- Учетные записи;
- Журнал событий;
- Настройки.

Основные полномочия роли

- Создание и удаление учетных записей сервисного администратора.
- Загрузка личного сертификата для учетной записи сервисного администратора.
- Просмотр учетных записей администраторов в **Главной консоли**.
- Просмотр списка учетных записей администраторов, кроме суперадминистратора.
- Назначение роли сервисного администратора.
- Удаление организации.
- [Загрузка и обновление лицензии](#).
- Просмотр лицензий.
- Просмотр журнала событий (только действия в разделах **Главная консоль** и **Управление организацией**).
- Интеграция с сервисами отправки уведомлений по электронной почте и СМС.

Оператор Prime

- Создает организации и просматривает их параметры.
- Распределяет лицензии на ПО ViPNet в организации и создает отчет об использовании лицензий во всех организациях для передачи в ИнфоТеКС.
- Просматривает журнал событий.



Внимание! При создании организации администратору автоматически назначается роль владельца организации. Для безопасности суперадминистратор должен снять роль владельца организации с оператора Prime и назначить ее на себя или на другую учетную запись с ролями владельца организации или администратора организации.

Основные полномочия роли

- Создание организации (родительской, дочерней).
- Просмотр списка всех организаций.
- Просмотр лицензий.
- [Распределение лицензий для отдельной организации.](#)
- [Распределение лицензий для нескольких организаций.](#)
- Получение общего отчета для биллинга по всем организациям.
- [Просмотр журнала событий в Главной консоли.](#)

Роли для управления организацией

В модуле VPN:

- Владелец организации и администратор организации может выполнять все действия по работе с [объектами](#) (создание, изменение, просмотр, удаление).
- Аудитор устройств просматривает:
 - настройки шлюзов безопасности;
 - журнал транспортных конвертов;
 - настройки сложности паролей администраторов сетевых узлов ViPNet для локального входа в CLI шлюзов безопасности.

Все действия администраторов в веб-интерфейсе фиксируются в [Журнале событий](#).

Владелец организации

- Управляет пользователями и устройствами, а также настройками параметров организации (Microsoft Active Directory, Microsoft Active Directory Federation Services).
- Создает дочерние организации.
- Распределяет лицензии на продукты ViPNet в дочерние организации.
- Создает и просматривает учетные записи только в своих организациях, а также предоставляет им права на управление в организации.
- Удаляет организацию, изменяет ее название.

Если владелец организации назначен в родительскую организацию, то его полномочия не наследуются для дочерних организаций.

Основные полномочия роли

- Доступ в модули.
- Учетные записи:
 - [Создание и настройка учетной записи администратора в организации](#).
 - Изменение параметров своей учетной записи.
 - Просмотр учетных записей администраторов.
 - Просмотр списка всех учетных записей, кроме учетной записи суперадминистратора.
- Организации:

- Создание дочерних организаций.
- Удаление организаций, в которых он назначен владельцем организации.
- Изменение названия организации.
- Просмотр списка своих организаций.
- [Назначение полномочий на управление организацией.](#)
- [Настройка доменной аутентификации с помощью служб федераций AD FS.](#)
- [Настройка интеграции с Active Directory.](#)
- Создание, изменение, удаление пользователей организации.
- Создание, изменение, удаление, просмотр устройств в организации.
- Лицензии:
 - Создание, изменение, удаление устройств в организации.
 - Распределение лицензий в дочерние организации.
 - Создание отчета об использовании лицензий.
 - Просмотр доступных лицензий.
- Администрирование:
 - [Просмотр журнала событий уровня организации.](#)
 - [Интеграция с сервисами отправки уведомлений по электронной почте или SMS.](#)
- Работа с мастер-ключами:
 - [Создание мастер-ключей организации.](#)
 - Удаление мастер-ключей организации.
 - Создание взаимодействия между организациями одной защищенной сети.
 - Отправка запроса на взаимодействие с другой защищенной сетью.

Администратор организации

- Управляет пользователями, устройствами и настройками параметров организации (Microsoft Active Directory, Microsoft Active Directory Federation Services).
- Просматривает список доступных лицензий на ПО ViPNet для организаций, которыми управляет. Просмотр созданных учетных записей недоступен.
- Изменяет название организации. Удаление организации недоступно.

Основные полномочия роли

- Доступ в модули.
- Изменение параметров своей учетной записи.

- Организации:
 - Создание подразделений.
 - Просмотр списка своих организаций.
 - [Настройка доменной аутентификации с помощью служб федераций AD FS.](#)
 - [Настройка интеграции с Active Directory.](#)
- Создание, изменение, удаление пользователей организации.
- Создание, изменение, удаление, просмотр устройств в организации.
- Лицензии:
 - Создание отчета об использовании лицензий.
 - Просмотр доступных лицензий.
- Администрирование:
 - [Просмотр журнала событий уровня организации.](#)
 - [Интеграция с сервисами отправки уведомлений по электронной почте или SMS.](#)
- Работа с мастер-ключами:
 - Просмотр информации о мастер-ключах.
 - Отправка запроса на взаимодействие с другой защищенной сетью.

Сетевой администратор шлюза безопасности

Роль предназначена для удаленного подключения из ViPNet Prime по ссылке к веб-интерфейсу ViPNet Coordinator HW 5 версии 5.5 и выше и изменения его настроек, не связанных с фильтрацией трафика.

- Обладает доступом только к разделам **Главная консоль** и **Управление организацией**.
- Просматривает:
 - список устройств организации;
 - свойства координаторов в организации;
 - список доступных подразделений.
- Изменяет настройки в ViPNet Coordinator HW 5:
 - сетевых интерфейсов;
 - кластера;
 - взаимодействия с Active Directory и Captive Portal;
 - маршрутизации;
 - сетевых сервисов (DNS-сервера, DHCP-сервера, DHCP-relay, NTP-сервера);
 - SNMP-мониторинга;

- Управляет сертификатами координатора.

Аудитор устройств

- Имеет наименьшие полномочия.
- Просматривает настройки шлюзов безопасности, без возможности их изменения.
- Просматривает настройки координаторов поколения ViPNet 5.

Основные полномочия роли

- Доступ в модули.
- Изменение параметров своей учетной записи.
- Просмотр списка своих организаций.
- Просмотр устройств организации.
- [Просмотр журнала событий уровня организации.](#)

3

Начало работы

Вход в ViPNet Prime	37
Интерфейс ViPNet Prime	42
Подключение модулей к ViPNet Prime	46

Вход в ViPNet Prime

1 В браузере введите: `https://<доменное имя ViPNet Prime>:<порт>`.

2 При первом входе укажите:

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

Вы войдете с правами суперадминистратора. Ожидайте некоторое время загрузки интерфейса.

В дальнейшем вход зависит от типа аутентификации.



Внимание! После первого входа [измените пароль](#).

Защита канала управления

TLS с односторонней аутентификацией

При аутентификации по паролю или с доменной учетной записью для защиты канала управления ViPNet Prime через веб-интерфейс используется протокол TLS с аутентификацией сервера и шифрованием передаваемых данных.

В ViPNet Prime при установке был загружен сертификат сервера. Подробнее см. в Руководстве по установке. Чтобы обеспечить доверие к сертификату сервера, может потребоваться установить корневой сертификат в системное хранилище ОС на компьютере. Обычно это требуется только при использовании самоподписанных сертификатов.

Если в адресной строке браузера при подключении к Prime отображается значок в виде закрытого замка, канал защищен, и корневой сертификат и сертификаты промежуточных УЦ можно не устанавливать.

Если для TLS с односторонней аутентификацией вы используете сертификат сервера ГОСТ, на рабочем месте администратора вместо системного хранилища ОС установите корневой сертификат и сертификат сервера в ViPNet PKI Client. Подробнее см. в Руководстве по установке.

Чтобы установить сертификат:

- 1 Перед установкой корневого сертификата в системное хранилище на компьютере закройте браузер.
- 2 Скопируйте корневой сертификат на компьютер, с которого будете подключаться к веб-интерфейсу Prime.

- 3 Дважды щёлкните файл сертификата и выберите **Установить сертификат**.
- 4 Следуйте указаниям мастера (далее приведены только значимые шаги):
 - 4.1 На шаге **Хранилище сертификатов** выберите **Поместить все сертификаты в следующее хранилище** и нажмите **Обзор**.

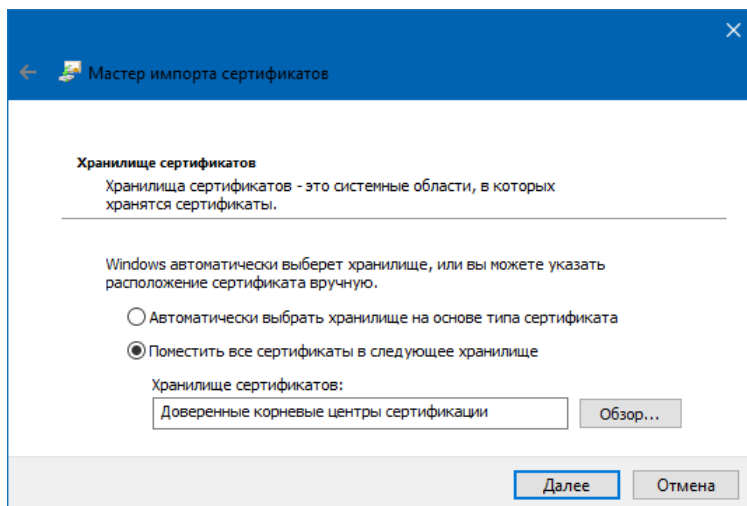


Рисунок 2. Хранилище для корневого сертификата выбрано

- 4.2 В списке выберите **Доверенные корневые центры сертификации** и нажмите **ОК**.

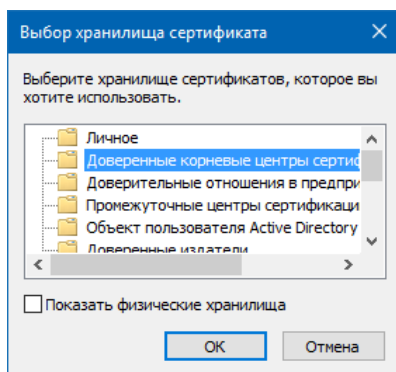


Рисунок 3. Выбор хранилища сертификатов

- 5 В окне подтверждения происхождения и подлинности сертификата нажмите **Да**.
- 6 В окне с информацией об успешной установке сертификата нажмите **ОК**.



Внимание! Чтобы защитить канал управления ViPNet Prime через веб-интерфейс, разрешите в настройках браузера использование корневых сертификатов из хранилища ОС. Например, в Mozilla Firefox в редакторе настроек установите параметру `security.enterprise_roots.enabled` значение `true`.

TLS с двусторонней аутентификацией

При аутентификации по сертификатам для защиты канала управления ViPNet Prime через веб-интерфейс используется протокол TLS с взаимной проверкой сертификатов администратора и сервера.

Для подключения пользователя к Prime по защищенному каналу с двусторонней аутентификацией на рабочем месте пользователя должны быть установлены личный сертификат администратора и соответствующий ему закрытый ключ. Подробнее о настройке TLS-канала с двусторонней аутентификации см. [Порядок действий](#) и в Руководстве по установке.

При подключении пользователя к Prime по защищенному каналу с двусторонней аутентификацией проверяются:

- Со стороны пользователя с помощью ViPNet PKI Client:
 - Сертификат сервера (ГОСТ) и доменное имя, прописанное в сертификате.
 - Действительность сертификата сервера — с помощью корневого сертификата удостоверяющего центра, установленного в ViPNet PKI Client.
- Со стороны Prime:
 - Действительность личного сертификата администратора.
 - Наличие учетной записи администратора в списке учетных записей Prime.

При успешной аутентификации и авторизации будет установлено защищенное подключение, и отобразится страница веб-интерфейса Prime.

Вход по паролю

Введите имя учетной записи администратора и пароль.

При первом входе в ViPNet Prime потребуется задать новый пароль, если суперадминистратор установил требование менять предустановленный пароль.



Примечание. Если вы забыли пароль или истек срок его действия, обратитесь к суперадминистратору.

Изменение пароля своей учетной записи

- 1 Войдите в ViPNet Prime.
- 2 Вверху справа нажмите на имя своей учетной записи.
- 3 Выберите **Изменить пароль**.

Если при входе появилось уведомление, что пароль не соответствует требованиям безопасности или скоро истечет срок его действия, в уведомлении нажмите **Изменить пароль**.

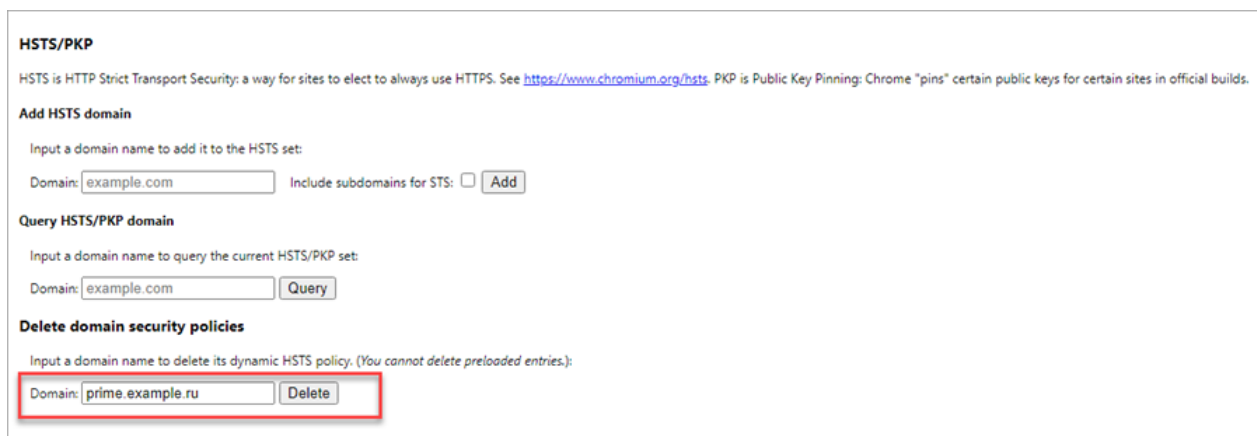
- 4 Задайте новый пароль и повторите его.

Требования к паролю

- Длина от 8 до 256 символов.
- Должен содержать хотя бы по одному символу из каждой категории:
 - Строчные и заглавные латинские буквы.
 - Цифры.
 - Специальные символы: ! " # \$ % & * () _ - + = @ ; : . , ^ ' ? { } [] / | \ > < ` ~
- Должен отличаться от предыдущего не менее, чем на 3 символа. Под отличием подразумевается добавление, удаление, замена и перестановка символов.

Вход по сертификату

- 1 Для входа администратора по сертификату [выполните предварительные действия](#).
- 2 Включите ViPNet PKI Client и ViPNet PKI Client TLS Unit.
- 3 Если на компьютере работают несколько администраторов, очистите кеш браузера.
- 4 При первом входе при подключении по TLS ГОСТ удалите информацию о доменном имени ViPNet Prime из политик HSTS браузера. Например, для Chrome:
 - 4.1 Перейдите на страницу `chrome://net-internals/#hsts`.



HSTS/PKP

HSTS is HTTP Strict Transport Security: a way for sites to elect to always use HTTPS. See <https://www.chromium.org/hsts>. PKP is Public Key Pinning: Chrome "pins" certain public keys for certain sites in official builds.

Add HSTS domain

Input a domain name to add it to the HSTS set:

Domain: Include subdomains for HSTS: ☐

Query HSTS/PKP domain

Input a domain name to query the current HSTS/PKP set:

Domain:

Delete domain security policies

Input a domain name to delete its dynamic HSTS policy. (You cannot delete preloaded entries.):

Domain:

Рисунок 4. Удаление политики HSTS

- 4.2 В группе **Delete domain security policies** введите доменное имя ViPNet Prime и нажмите **Delete**.
- 5 В браузере введите: `https://<доменное имя ViPNet Prime>:<порт>`.
- 6 В открывшемся окне выберите личный сертификат администратора.



Примечание. При переходе между разделами модулей выберите сертификат повторно. Это связано с тем, что модули имеют разные доменные имена.

7 Для входа по другому сертификату очистите кеш ViPNet PKI Client TLS Unit.

8 Введите пароль от хранилища ключей ViPNet PKI Client.

Чтобы просмотреть информацию о TLS-соединении, в области уведомлений щелкните правой кнопкой мыши значок TLS Unit и выберите **Информация о соединениях** (или **Последние соединения**). См. документацию на ViPNet PKI Client.



Примечание. Если выйти из TLS Unit и не очистить кеш, вход в ViPNet Prime будет возможен, пока не истечет токен авторизации (по умолчанию 15 минут). Чтобы избежать этого, закройте браузер и очистите кеш TLS Unit и браузера.

Вход через AD FS

Нажмите на кнопку для доменной аутентификации. Кнопка отображается, если [настроена доменная аутентификация](#).

Интерфейс ViPNet Prime

Главная консоль

Для управления учетными записями администраторов, создания организаций и просмотра отчетов об использовании лицензий выберите раздел **Главная консоль** .

Цифрами на рисунке обозначены:

1 Панель слева — состоит из двух частей:

- Панель переключения между разделами управления модулей. Для отображения раздела модуля [подключите его к ViPNet Prime](#).
- Панель переключения между подразделами.

Раздел **Главная консоль**  содержит:

- **Организации** — создание и удаление организаций, распределение лицензий на ПО ViPNet.
- **Сертификаты и CRL** — установка сертификатов УЦ и CRL для аутентификации администраторов по сертификату.
- **Лицензии** — просмотр доступных лицензий на ПО ViPNet, их распределение в организации, обновление файла лицензии.
- **Учетные записи** — создание и удаление учетных записей, назначение ролей на уровне системы управления.
- **Отчет для биллинга** — просмотр отчетов об использовании лицензий в организациях.
- **Регистрация модулей** — подключение модулей к системе управления. Модуль отображается в виде отдельного раздела на левой панели.
- **Журнал событий** — просмотр системных событий и действий администраторов в ViPNet Prime.
- **Настройки:**
 - общие настройки (отключение парольной аутентификации, срок хранения журнала транспортных конвертов УТ и другие);
 - интеграция с внешними сервисами рассылки уведомлений по электронной почте или СМС. Служит для отправки уведомлений на электронную почту при выявлении проблем в показателях здоровья модулем ViPNet NVS.
- **Контроль приложения** — [проверка работы и целостности ПО ViPNet Prime](#).

2 Панель просмотра. Отображает подраздел, выбранный на панели слева.

3 Панель справа. Отображает информацию об объекте, выбранном на панели просмотра.

Управление организацией

Для управления пользователями и устройствами выберите раздел **Управление организацией** . Раздел доступен администраторам с любой ролью, кроме сервисного администратора и оператора Prime, после подключения функционального модуля. Но, если сервисному администратору или оператору Prime назначена роль в организации, раздел будет доступен.

Цифрами на рисунке обозначены:

1 Панель слева. Содержит подразделы для настройки организации:

- **Пользователи** — для добавления пользователей в систему управления вручную или импорта учетных записей пользователей из Active Directory или файла CSV, обновления параметров существующих пользователей. Пользователи из этого раздела также отображаются в разделе **ViPNet VPN**  > **Пользователи**.
- **Устройства** — список всех управляемых сетевых объектов организации: компьютеры и мобильные устройства пользователей, координаторы, серверы и другие.
- **Подразделения** — для создания подразделений внутри организации.
- **Учетные записи** — для создания учетных записей на уровне организации. Такие учетные записи не отображаются в списке учетных записей уровня системы управления в разделе **Главная консоль** .
- **Импорт данных** — интеграция системы управления с каталогом Active Directory для импорта учетных записей пользователей.
- **Аутентификация** — подключение к службе AD FS для использования доменной аутентификации пользователей и администраторов при входе в ViPNet Prime. Раздел не доступен, если отключена аутентификация по паролю.
- **Журнал транспортных конвертов** — просмотр истории обмена транспортными конвертами между центром управления и сетевыми узлами с ПО ViPNet своей организации.

2 Список организаций, доступных для управления. Отображает название организации, для которой вы выполняете настройку. Суперадминистратору доступны все организации.

Если вы управляете несколькими организациями, в списке со значком  выберите название организации.

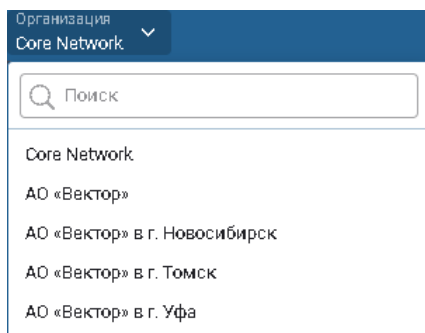


Рисунок 5. Выбор организации

- 3 Список подразделений выбранной организации.
- 4 Панель просмотра. Отображает подраздел, выбранный на панели навигации.
- 5 Панель свойств. Отображает информацию об объекте, выбранном на панели просмотра.
- 6  — меню с именем учетной записи администратора. Предназначено для выхода из ViPNet Prime, смены пароля своей учетной записи, установки личного сертификата для входа по сертификату. При входе по сертификату в меню отсутствует пункт **Выйти**. В этом случае чтобы выйти из ViPNet Prime, выключите ViPNet PKI Client TLS Unit.
- 7 Смена языка интерфейса: русский, английский.

Модуль ViPNet VPN



Примечание. Чтобы в интерфейсе отобразить раздел **ViPNet VPN** , [подключите модуль к ViPNet Prime](#).

Для управления структурой сети ViPNet организации выберите раздел **ViPNet VPN** .

Для администратора организации и владельца организации отображаются только доступные этим ролям разделы.

Цифрами на рисунке обозначены:

- 1 Панель слева. Содержит подразделы:
 - Группа **Управление защищенной сетью** — создание структуры сети ViPNet организации, связей между объектами сети ViPNet, [дистрибутивов ключей](#). Группа содержит подразделы:
 - **Пользователи** — для управления пользователями в модуле. Пользователи создаются в разделе **Управление организацией**.
 - **Клиенты** — для управления устройствами с клиентским ПО ViPNet (ViPNet Client).
 - **Координаторы** — для управления координаторами.
 - **Другие узлы** — для управления ViPNet xFirewall и узлами квантовой сети. Регистрируются на координаторе.

- **Ресурсы** — для управления устройствами, трафик которых **туннелируется** координаторами.
 - **Профили DNS** — для создания списка доменных зон, запросы на разрешение имен которых отправляются на защищенные корпоративные DNS-серверы.
 - **Группы серверов соединений** — для **создания групп серверов соединений** и назначения этих групп на клиенты.
 - **Доверенное взаимодействие**
 - **Организации** — создание взаимодействия с организациями и сетями, смена мастер-ключа обмена между доверенными организациями.
 - **Сети** — для установки взаимодействия с другими сетями ViPNet.
 - **Группы** предназначены для логического объединения объектов сети ViPNet и упрощения управления связями между ними. Содержит следующие подразделы:
 - **Группы пользователей** — можно использовать для быстрого создания связей между всеми пользователями группы.
 - **Группы узлов** — могут состоять из клиентов и шлюзов безопасности.
 - **Автоматические группы** — автоматически формируются для каждого координатора и состоят из клиентов и межсетевых экранов ViPNet xFirewall, зарегистрированных на определенном координаторе. Состав таких групп не может быть изменен администратором.
 - **Группа Сервис.** Содержит подразделы по обслуживанию и дополнительной настройке организации:
 - **Сервисные функции** — настройка серверного прикладного и управляющего ПО ViPNet (если предусмотрено лицензией), настройка сложности паролей узлов, задание паролей администраторов сетевых узлов, полномочий пользователей и другое.
 - **Обновление ПО** — загрузка обновлений ПО ViPNet и отправка их на узлы сети ViPNet.
 - **Мастер-ключи** — просмотр сроков действия мастер-ключей и смена мастер-ключей.
 - **Ключевые блокноты** — учет ключей для ViPNet Coordinator KB и ViPNet L2-10G (раздел отображается при наличии лицензии для ViPNet Coordinator KB или ViPNet L2-10G).
 - **Настройка модуля** — управление автоматической отправкой ключей при регламентных работах (смене мастер-ключей).
- 2 Панель просмотра. Чтобы отфильтровать список объектов, нажмите . Чтобы найти нужный объект, воспользуйтесь строкой поиска.
- 3 Панель справа. Отображает свойства или параметры выбранного на панели просмотра объекта.

Подключение модулей к ViPNet Prime

ViPNet Prime состоит из ViPNet Prime Core и модулей. После запуска модуля отправляется запрос ViPNet Prime Core на подключение этого модуля. Суперадминистратор регистрирует модуль. Модуль подключается к ViPNet Prime Core и отображается в интерфейсе как раздел.

Внимание! Модуль VPN нужно подключать обязательно. Зарегистрируйте модуль VPN в течение 60 минут после запуска, иначе для регистрации потребуются перезапустить его.

Чтобы перезапустить модуль VPN:



- 1 На компьютере с ViPNet Prime войдите в ОС с правами суперпользователя `root` или привилегированного пользователя для использования команды `sudo`.
- 2 Последовательно выполните команды:

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

Чтобы зарегистрировать модуль в ViPNet Prime:

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 Выберите Главная консоль  > Регистрация модулей.
- 3 Выберите модуль. Зарегистрируйте сначала модуль VPN, затем остальные модули.
- 4 Нажмите **Принять**.

После подключения модуль отобразится в виде раздела на панели слева, например **ViPNet VPN**



Если вы нажали **Отклонить** и хотите заново подтвердить подключение модуля, перезагрузите компьютер с установленным модулем. После перезагрузки ОС введите мастер-ПИН с помощью `sudo prime-control`.

4

Управление лицензиями

Общая информация	48
Загрузка и обновление лицензии	51
Включение режима фиксированного распределения лицензий	54
Распределение лицензий для нескольких организаций	55
Распределение лицензий для отдельной организации	56
Выбор пакета лицензий для пользователей	57
Создание отчета об использовании лицензий	58
Освобождение лицензии ViPNet Connect	62

Общая информация

Компания ИнфоТеКС выдает общий файл с лицензиями *.itcslic. Он содержит информацию о номере защищенной сети, лицензиях и сроках их действия, максимальную версию ПО ViPNet.

Общая лицензия *.itcslic может ограничивать:

- использование ViPNet Prime и модулей (ViPNet NVS, ViPNet PMM, Connect Book);
- количество устройств, которыми разрешено управлять в модуле (Policies nodes, Monitoring nodes);
- возможность создавать организации (лицензия Multitenancy mode).

Общая лицензия содержит обязательные лицензии на использование ViPNet Prime и модуля VPN.

По умолчанию в системе доступна только одна организация. Лицензия Multitenancy mode позволяет создавать новые организации. Для организаций вы можете настраивать отдельный доступ в ViPNet Prime. См. «ViPNet Prime. Руководство по установке».

Для работы счетчиков в ViPNet Prime Policy Management требуется лицензия на модуль ViPNet NVS и на устройства мониторинга, иначе в ViPNet Prime Policy Management количество срабатываний счетчиков не будет отображаться.

Лицензия на ПО ViPNet может быть:

- Базовой. Она разрешает создавать сетевые узлы — клиенты и шлюзы безопасности: координаторы, межсетевые экраны ViPNet xFirewall, узлы квантовой сети.
- Дополнительной. Она разрешает использовать:
 - функции на шлюзах (кластер горячего резервирования, DPI, IPS, инспекцию SSL/TLS-трафика и другие);
 - сервисные функции на клиентах (ViPNet ConServer и ViPNet CPNS и другие);
 - приложения ViPNet CSS Connect на устройствах пользователей.

Лицензия на ПО ViPNet и функции узла включается в [дистрибутив ключей](#) и передается в его составе на узел защищенной сети.

Лицензии могут назначаться или списываться двумя способами:

- по пользователям из пакетов лицензий;
- по устройствам или пользователям из свободных отдельных лицензий.

Пакеты лицензий ограничены по количеству пользователей, а лицензионные объекты из пакета — по количеству устройств пользователя. В списке лицензий они отображаются значком . Например, пакет лицензий ограничен 10 шт. и в каждом экземпляре пакета содержится: ViPNet Client — 3 шт., ViPNet CSS Connect — 3 шт. Это означает, что 10 пользователей могут использовать ПО ViPNet Client и ViPNet CSS Connect не более чем на трех устройствах. Один пакет лицензий

списывается на одного пользователя, если списывается хотя бы одна лицензия из пакета на этого пользователя.

Если истекает срок действия пакета лицензий, то истекает срок действия всех лицензий в пакете лицензий, даже если их срок действия больше, чем у пакета лицензий. За 30 дней до окончания срока действия лицензии отображается уведомление об этом.

Если срок действия лицензии из пакета истекает раньше, чем у пакета лицензий, это не влияет на срок действия пакета лицензий или других лицензий в нем.

Суперадминистратор или сервисный администратор загружает общий файл лицензии *.itcslic в ViPNet Prime. Для каждой корневой организации суперадминистратор или оператор Prime распределяет лицензии. В дочерних организациях лицензии могут распределять владельцы организаций. Администратор организации может только просмотреть список лицензий организации.

Вы можете выдать лицензии или пакеты лицензий в организациях двумя способами:

- Одновременно во всех организациях.
- В каждой организации по отдельности.

Лицензия освобождается при отключении функции или использования приложения в модуле VPN. Лицензии для координаторов, клиентов и функцию кластера с ПО ViPNet версии 5 отображаются с постфиксом v.5.

ViPNet Prime оповещает администраторов о приближении окончания срока действия лицензии или о его истечении. Если в разделе **Главная консоль > Лицензии** напротив даты окончания появляется:

- желтый индикатор — приближается окончание срока действия лицензии;
- красный индикатор — срок действия лицензии истек.

При включении функций к устройству привязывается лицензия с определенным идентификатором, который вы можете посмотреть в разделе **Главная консоль > Лицензии**. Там же отображается информация об организации, которой выдана лицензия. При обновлении лицензии, если вам продлили срок действия используемой лицензии, лицензия заменится автоматически. Если вам создали новую лицензию с другим идентификатором, вам придется обновить лицензию вручную: в настройках функции выберите новую лицензию.

Если истек срок действия лицензии на модуль, работа администратора в модуле ограничена, управление устройствами в модуле недоступно — отображается уведомление о работе в режиме ограниченной функциональности. Если администратор изменяет настройки, они сохраняются, но обновления на узлы не отправляются. При этом в модуле VPN блокируются:

- создание, скачивание дистрибутива ключей;
- отправка обновлений справочников и ключей вручную;
- отправка обновления ПО ViPNet;
- скачивание, отправка межсетевой информации;
- скачивание файла обновления *.cms;

- автоматическая отправка справочников и ключей.

При попытке администратора, например, создать дистрибутив ключей кнопка будет неактивна.

Вы можете просмотреть список лицензий, используемых на устройстве. Для этого в разделе **Устройства** выберите устройство и просмотрите список на панели справа в разделе **Лицензии**. Если у лицензии истек или истекает срок действия, вы можете нажать на нее и просмотреть параметры этой лицензии, чтобы запросить ее обновление.

Загрузка и обновление лицензии

Загрузка файла лицензии

- 1 Войдите в ViPNet Prime как сервисный администратор.
- 2 Выберите Главная консоль  > Лицензии.
- 3 Нажмите  Загрузить лицензию.
- 4 Выберите файл лицензии *.itcslic.
- 5 Нажмите Готово.

Обновление лицензии



Внимание! В ViPNet Prime версии 1.9.6 и выше лицензируются модули ViPNet NVS, ViPNet PMM, право на использование защищенной сети (модуль VPN), создание новых организаций, управление устройствами в модулях ViPNet NVS, ViPNet PMM. При обновлении ViPNet Prime с версии ниже 1.9.6 запросите в ИнфоТеКС новый файл лицензии *.itcslic, чтобы продолжить использовать ViPNet Prime.

Обратитесь в ИнфоТеКС за обновлением файла лицензии *.itcslic, чтобы:

- изменить лицензию на ПО ViPNet;
- увеличить количество лицензий;
- увеличить срок действия лицензий;
- расширить список лицензий.

Чтобы загрузить новый файл лицензии:

- 1 Войдите в ViPNet Prime как сервисный администратор.
- 2 Выберите Главная консоль  > Лицензии.
- 3 Нажмите  Загрузить лицензию.
- 4 Укажите путь к новому файлу лицензии *.itcslic.
- 5 Проверьте информацию о лицензии.

Загрузка лицензий

Шаг 1 из 2

lic_20665_26.07.2023_3327208-1.licslic **Обзор**

Для загрузки другой лицензии выберите файл.

Файл лицензии:

Название	lic_20665_26.07.2023_3327208-1.licslic
Номер сети	20665
Версия	5.9 и ниже
Срок действия	до 27.07.2024

Далее **Отмена**

Рисунок 6. Просмотр информации о лицензии

- 6 Если в файле не хватает некоторых используемых лицензий, вы можете просмотреть, какие лицензии отсутствуют в отчете. Для этого нажмите  **Скачать отчет**.
- 7 Просмотрите изменения в лицензии.
 - Если все лицензии сопоставились автоматически, закройте окно.
 - Если не все лицензии сопоставились автоматически, выберите новые вручную.

Загрузка лицензий

Шаг 3 из 3

Обновление лицензий на узлах. Установите соответствие между старыми и новыми лицензиями.

 **Connect (версия 5.9 и ниже)**
10 лицензий со сроком действия по 14.09.2024.

Заменить на:

Выберите подходящую лицензию

- #1 Connect (версия 5.9 и ниже)
50 лицензий со сроком действия по 30.05.2023.
- #2 Connect (версия 5.9 и ниже)
60 лицензий со сроком действия по 19.07.2024.

Назад **Загрузить** **Отмена**

Рисунок 7. Установка соответствия между старыми и новыми лицензиями при обновлении лицензии

- 8 Нажмите **Применить**.

Если после загрузки файла лицензии не удалось сопоставить новые и старые лицензии, см. [Не сопоставились лицензии при загрузке файла](#). Это может произойти, если вам создали новые лицензии, а не продлили истекшие, и истекшие лицензии остались в файле лицензии.

Включение режима фиксированного распределения лицензий

Чтобы ограничить количество лицензий, распределяемых в организацию, для контроля их перерасхода:

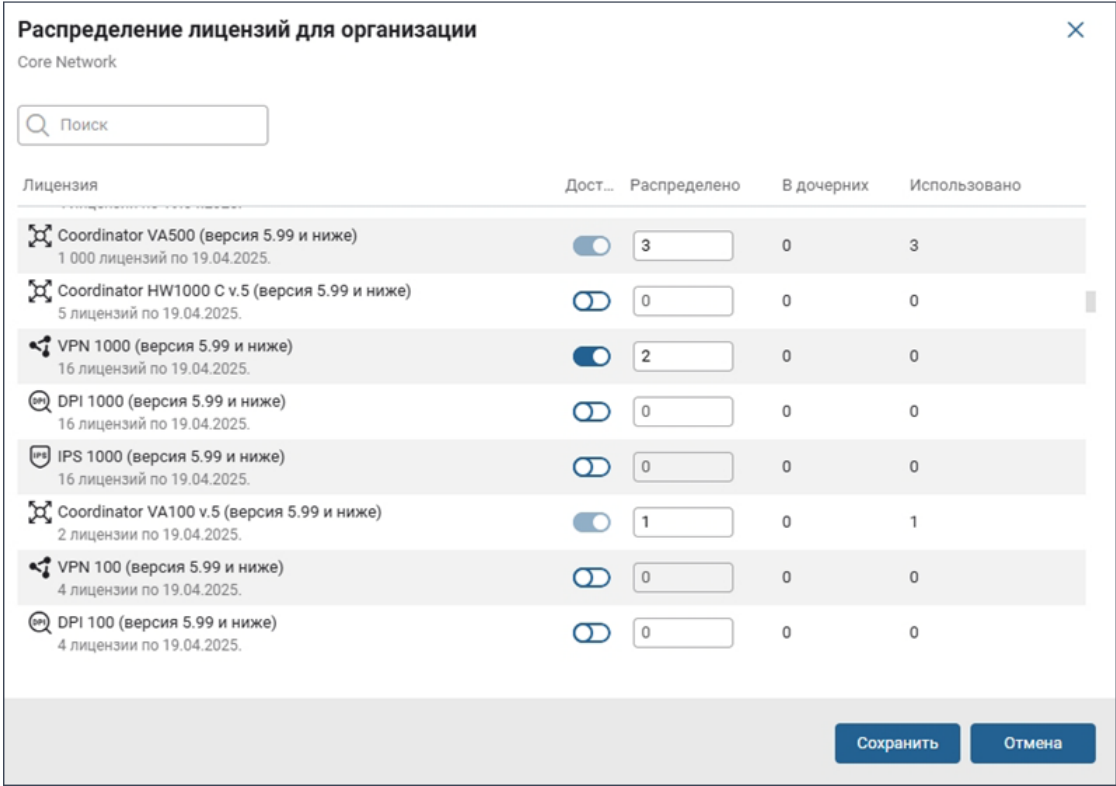
1 Войдите в ViPNet Prime как сервисный администратор.

2 Выберите Главная консоль  > Настройки > Общие.

3 Включите **Распределять организациям фиксированное количество лицензий**.

В результате настройки при распределении лицензий отобразится дополнительный столбец **Распределено**.

4 При распределении лицензий укажите их количество.



Лицензия	Дост...	Распределено	В дочерних	Использовано
 Coordinator VA500 (версия 5.99 и ниже) 1 000 лицензий по 19.04.2025.	☒	3	0	3
 Coordinator HW1000 C v.5 (версия 5.99 и ниже) 5 лицензий по 19.04.2025.	☐	0	0	0
 VPN 1000 (версия 5.99 и ниже) 16 лицензий по 19.04.2025.	☒	2	0	0
 DPI 1000 (версия 5.99 и ниже) 16 лицензий по 19.04.2025.	☐	0	0	0
 IPS 1000 (версия 5.99 и ниже) 16 лицензий по 19.04.2025.	☐	0	0	0
 Coordinator VA100 v.5 (версия 5.99 и ниже) 2 лицензии по 19.04.2025.	☒	1	0	1
 VPN 100 (версия 5.99 и ниже) 4 лицензии по 19.04.2025.	☐	0	0	0
 DPI 100 (версия 5.99 и ниже) 4 лицензии по 19.04.2025.	☐	0	0	0

Сохранить Отмена

Рисунок 8. Фиксированное распределение лицензий

Распределение лицензий для нескольких организаций

- 1 Войдите в ViPNet Prime как суперадминистратор или оператор Prime с ролью владельца организации.
- 2 Выберите Главная консоль  > Лицензии.
- 3 Чтобы скрыть истекшие лицензии, нажмите  > Скрывать истекшие лицензии.
- 4 Выберите лицензию на продукт ViPNet или пакет лицензий .
- 5 На панели справа нажмите  Распределить лицензию.
- 6 Напротив организаций включите  доступ. Для распределения лицензии для дочерних организаций включите  доступ для всех вышестоящих в иерархии организаций, начиная с корневой.
- 7 Нажмите Сохранить.

Распределение лицензии между организациями

Coordinator VA2000 v.5

Поиск

Организация	Доступ	Использовано
ОАО Вектор		2
▼ ООО Поставщик услуг		0
▼ ООО Дистрибьютер		0
ООО Партнер 1		0
ООО Партнер 2		0

Сохранить

Отмена

Рисунок 9. Распределение лицензии между организациями

Распределение лицензий для отдельной организации

- 1 Войдите в ViPNet Prime как суперадминистратор или оператор Prime с ролью владельца организации.
- 2 Чтобы ограничивать количество доступных лицензий в организациях, [включите режим фиксированного распределения лицензий](#).
- 3 Выберите Главная консоль  > Организации.
- 4 Выберите организацию.
- 5 На панели справа нажмите **Распределить лицензии**.
- 6 Вы можете скрыть истекшие лицензии, для этого нажмите   и выберите **Скрывать истекшие лицензии**.
- 7 Напротив названия продукта или пакета лицензий  включите  доступ к лицензиям.

Распределение лицензий для организации

Core Network

Лицензия	Доступ	Использовано
5 лицензий по 19.04.2025.		
 VPN 500 (версия 5.99 и ниже) 5 лицензий по 19.04.2025.		0
 DPI 500 (версия 5.99 и ниже) 5 лицензий по 19.04.2025.		0
 IPS 500 (версия 5.99 и ниже) 5 лицензий по 19.04.2025.		0
 Coordinator VA1000 v.5 (версия 5.99 и ниже) 4 лицензии по 19.04.2025.		1
 Coordinator VA2000 v.5 (версия 5.99 и ниже) 2 лицензии по 19.04.2025.		2
 VPN 2000 (версия 5.99 и ниже) 4 лицензии по 19.04.2025.		1
 DPI 2000 (версия 5.99 и ниже) 4 лицензии по 19.04.2025.		1
 IPS 2000 (версия 5.99 и ниже) 4 лицензии по 19.04.2025.		1

Сохранить

Отмена

Рисунок 10. Распределение лицензий для определенной организации

- 8 При фиксированном распределении лицензий укажите количество лицензий или пропустите этот шаг.
- 9 Нажмите **Сохранить**.

Выбор пакета лицензий для пользователей

Чтобы учитывать лицензии по количеству пользователей и назначать лицензии на устройства пользователей из пакета лицензий, выберите пакет лицензий для пользователей. Иначе лицензия будет списываться не из пакета лицензий, а из общего числа лицензий в организации.

Чтобы выбрать пакет лицензий для пользователя:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Распределите пакет лицензий в организацию.
- 4 Выберите **Управление организацией**  > **Пользователи**.
- 5 Чтобы назначить пакет лицензий на одного пользователя:
 - 5.1 Выберите пользователя.
 - 5.2 В разделе **Пакет лицензий** нажмите  **Выбрать пакет лицензий**.
- 6 Чтобы назначить пакет лицензий на несколько пользователей:
 - 6.1 Выберите пользователей.
 - 6.2 Нажмите **Выбрать пакет лицензий**.
- 7 Выберите пакет лицензий и нажмите **Сохранить**.

Чтобы просмотреть информацию о пакете, в свойствах пользователя выберите пакет лицензий и нажмите  > **Информация**.

Чтобы для пользователя выбрать другой пакет лицензий, в свойствах пользователя выберите пакет лицензий и нажмите  > **Изменить**.

Чтобы освободить пакет лицензий, в свойствах пользователя выберите пакет лицензий, нажмите  > **Отменить выбор пакета** и подтвердите отмену.

Создание отчета об использовании лицензий

Вы можете выгрузить отчеты об использовании лицензий на продукты ViPNet для расчёта с ИнфоТеКС в следующих вариантах:

- Отчет с детализацией для каждой организации за указанный период.
- Расход лицензий для каждой организации за указанный период.
- Общий отчет по всем организациям для предоставления в ИнфоТеКС.

В отчете учитываются только лицензии, которые использовались в течение всего отчетного периода. Лицензия считается использованной и учитывается в отчетах биллинга, если она была израсходована до начала указанного периода и освобождена после окончания периода.



Внимание! В отчете для биллинга не учитывается первый день списания лицензии. Чтобы отобразить лицензию в отчёте, выберите дату начала периода на один день позже.

Лицензия на прикладное ПО ViPNet, функции координатора или ViPNet xFirewall считается использованной, если в модуле VPN это ПО назначено на устройство.

Лицензия на продукт ViPNet не используется и возвращается обратно в список доступных лицензий, если:

- удалено устройство из защищенной сети (из модуля VPN);
- отключено [прикладное ПО ViPNet для пользователя](#);
- не задано устройство [в настройках сервисных функций](#).

Чтобы сформировать отчет об использовании лицензий на ПО ViPNet за текущий месяц по всем организациям в конце календарного месяца:

- 1 Войдите в ViPNet Prime как оператор Prime.
- 2 Выберите Главная консоль  > Отчет для биллинга.
- 3 Выберите Отчет для биллинга перед поставщиком услуг.
- 4 Укажите отчетный период с помощью календаря .
- 5 Сохраните отчет об использовании лицензий за месяц во всех организациях и передайте его [представителю ИнфоТеКС](#). Чтобы сохранить отчет об использовании лицензий, нажмите  **Скачать отчет** и в списке выберите формат отчета XML или XLSX. Файл будет сохранен на вашем компьютере. См. Примеры XML-отчетов для биллинга.
- 6 Чтобы просмотреть статистику использования лицензий на графике, в таблице выберите лицензию.

Отчет для биллинга		
Статистика использования	Отчет для биллинга	Отчет для биллинга перед поставщиком услуг
04.2026	↓ Скачать отчет	5 записей
Функциональность	На начало периода	На конец периода
Client for Linux	0	3
Client for Windows	0	1
Coordinator KB1000 v5	0	4
Coordinator VA500 v.5	0	1
VPN 500	0	1

Рисунок 11. Просмотр отчета об использовании лицензий за месяц

Чтобы просмотреть статистику использования лицензий на продукты ViPNet за отчетный период с детализацией по организациям:

- 1 Войдите в ViPNet Prime как владелец организации.
- 2 Выберите Главная консоль  > Отчет для биллинга.
- 3 Выберите одну из вкладок:
 - **Отчет для биллинга** — для просмотра лицензий, использованных полностью или частично. Для задания отчетного периода и выбора организации нажмите **Построить отчет**.
 - **Статистика использования** — для просмотра лицензий, использованных полностью в течение указанного периода. Для задания отчетного периода и выбора организации нажмите **Выбрать**.
- 4 Задайте отчетный период с помощью календаря  и выберите организации.

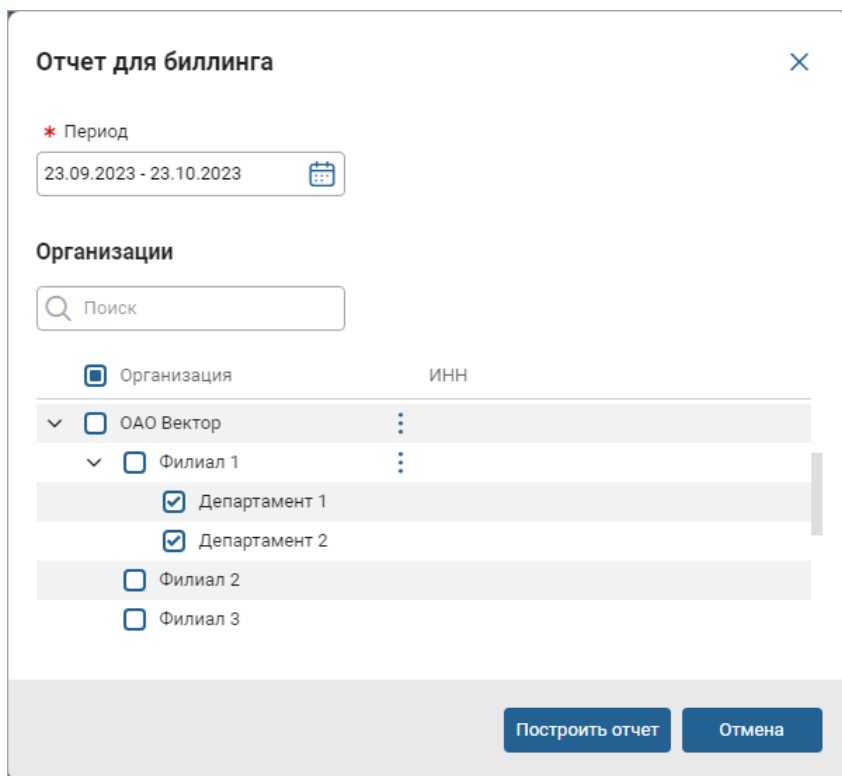


Рисунок 12. Выбор параметров для построения детального отчета для биллинга

Информация об использованных лицензиях по каждой организации будет отображена в таблице со следующими столбцами:

- **Организация** — названия организаций со списком лицензионных объектов ViPNet.
 - ИНН организации.
 -  — отображение на графике использования лицензий. По умолчанию для всех лицензий отображение использования лицензий на графике выключено и имеет значок .
 - **Расход лицензий за период** — количество лицензий на продукты ViPNet, которые были израсходованы в течение указанного периода. Лицензии, используемые частично в указанном периоде, не учитываются в биллинге.
- 5 Чтобы просмотреть список лицензий для определенной организации, в столбце **Организация** напротив организации нажмите значок .
 - 6 Для просмотра использования лицензий продуктов ViPNet в течение указанного периода на графике нажмите название продукта ViPNet.
 - 7 Чтобы задать новые параметры для отчета, нажмите **Изменить организации**.
 - 8 Чтобы сохранить отчет об использовании лицензий, нажмите **Скачать отчет** и в списке выберите формат отчета XML или XLSX. Файл будет сохранен на вашем компьютере.

Отчет для биллинга

Отчет для биллинга

Статистика использования

Отчет для биллинга перед ИнфоТекС

Отчет за период 13.10.2022 - 17.10.2022

Записей: 3

Изменить данные

Скачать отчет

Организация	ИНН	На начало периода
Core Network		
Coordinator KB2000 v5		3
Client for Linux		2
Failover KB2000 v5		2

Рисунок 13. Просмотр отчета об использовании лицензий с детализацией по каждой организации за указанный период

Освобождение лицензии ViPNet Connect

Чтобы освободить лицензию на использование ViPNet Connect на всех устройствах пользователя, например, при удалении устройства:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN**  > **Пользователи**.
- 3 Выберите пользователей.
- 4 Нажмите .
- 5 Выберите **Запретить использование приложения ViPNet Connect**.

5

Настройка аутентификации

Способы аутентификации	64
Аутентификация администраторов в ViPNet Prime	65
Аутентификация по сертификату	67
Аутентификация по паролю	74
Доменная аутентификация	77

Способы аутентификации

Администратор может входить в ViPNet Prime:

- по паролю,
- сертификату,
- с использованием доменной аутентификации (запрещено для сертифицированной версии ViPNet Prime).

После первого входа в ViPNet Prime [с паролем по умолчанию](#) суперадминистратор выполняет одно из следующих действий:

- [изменяет пароль учетной записи](#);
- [настраивает аутентификацию по сертификату](#) для других учетных записей и отключает аутентификацию по паролю.

Аутентификация администраторов в ViPNet Prime

За аутентификацию в ViPNet Prime отвечает специальный сервис. Различают:

- аутентификацию администраторов в ViPNet Prime;
- аутентификацию администраторов на ViPNet Coordinator HW 5 или ViPNet Coordinator IG 5 с учетной записью ViPNet Prime.

Аутентификация администратора в ViPNet Prime:

- 1 Администратор вводит в браузере: `https://<доменное имя ViPNet Prime>:<порт>`.
- 2 ViPNet Prime проверяет:
 - наличие токена доступа для входа;
 - время действия токена доступа;
 - соответствие времени на устройстве аутентификации и в ViPNet Prime.
- 3 Если токен доступа найден:
 - и действителен — открывается ViPNet Prime;
 - время на устройстве аутентификации и в ViPNet Prime отличается более чем на 1 минуту — токен доступа не проходит проверку, появится сообщение об ошибке. Это ограничение защищает от использования недействительных токенов путем изменения времени на устройстве аутентификации.

В качестве устройства аутентификации могут выступать компьютер администратора или координатор поколения ViPNet 5 с поддержкой перехода в веб-интерфейс координатора из ViPNet Prime.
- 4 Если токена доступа нет или он недействителен, открывается страница аутентификации.
- 5 Пользователь вводит [учетные данные](#).
- 6 Сервис аутентификации сверяет данные: имя учетной записи и хэш пароля или сертификат, цепочку сертификатов удостоверяющего центра, который выдал личный сертификат, CRL.
- 7 Если данные корректные, создается токен доступа и открывается ViPNet Prime.

Токен доступа используется далее для аутентификации последующих управляющих запросов.
- 8 Если данные неверные, появляется сообщение об ошибке.
- 9 После аутентификации токен доступа позволяет поддерживать активным сеанс администратора в течение заданного срока действия токена доступа. Срок действия токена (бездействия пользователя) ограничено, но его можно изменить:
 - 9.1 На компьютере ViPNet Prime запустите терминал с правами суперпользователя
 - 9.2 Остановите ViPNet Prime:

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

- 9.3** Измените в конфигурационном файле `/usr/share/infotecs/smp-kc/config.env` значение `SILSO_CookieAuthenticationOptions__ExpireTimeSpan=00:15:00`.



Внимание! В синтаксисе параметра

`SILSO_CookieAuthenticationOptions__ExpireTimeSpan` используются одинарный `( )` и двойной `( )` символы нижнего подчеркивания.

По умолчанию установлено 15 минут, вы можете задать от 15 минут до 8 часов. Если такого параметра нет в конфигурационном файле, добавьте его.

- 9.4** Запустите ViPNet Prime:

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

Установленное время бездействия распространяется на всех пользователей и все модули.

Срок действия токена доступа автоматически продлевается при каждом нажатии мыши или на клавишу администратором ViPNet Prime, даже если не происходит взаимодействия с сервером. Если запущен фоновый процесс, который не требует участия администратора, например выгрузка файла `*.dst`, сеанс администратора завершится по истечении установленного времени бездействия. При этом процесс не прервется.

Аутентификация по сертификату

Порядок действий

- 1 При установке ViPNet Prime должны быть загружены сертификаты сервера, см. Руководство по установке. При необходимости [обеспечьте доверие к сертификату сервера](#).
- 2 Ознакомьтесь с [требованиями к личному сертификату администратора](#).
- 3 При выборе УЦ обратите внимание на срок обновления CRL. Так как администратор загружает CRL вручную, выберите УЦ, в которых CRL обновляются не чаще одного раза в месяц.
- 4 Получите в УЦ:
 - Личный сертификат (подтверждает личность администратора, далее — сертификат администратора).
 - Сертификат УЦ.
 - Сертификаты корневого и промежуточных УЦ (если УЦ не головной).
 - CRL (список серийных номеров сертификатов, которые были аннулированы, отозваны или действие которых было прекращено).
- 5 На компьютере, с которого подключаетесь к веб-интерфейсу ViPNet Prime, установите ViPNet PKI Client. Подробнее см. документацию на ViPNet PKI Client.
- 6 В ViPNet PKI Client загрузите сертификат администратора, сертификат УЦ, CRL и сертификаты головного и промежуточных УЦ, если УЦ не головной. Подробнее см. документацию на ViPNet PKI Client.
- 7 Для проверки подлинности сертификата администратора:
 - 7.1 В ViPNet Prime [загрузите сертификат УЦ и его CRL](#). Если УЦ не является головным, загрузите сертификаты промежуточных УЦ.
 - 7.2 [Загрузите сертификат администратора](#).
- 8 Убедитесь, что аутентификация по сертификату работает.
- 9 Для безопасности [отключите аутентификацию по паролю](#). После отключения аутентификации по паролю вы не сможете включить ее. Если у вас есть проблемы с аутентификацией по сертификатам, вы можете потерять доступ к ViPNet Prime.

В результате будет доступен [вход по сертификату в ViPNet Prime](#) и, например, на ViPNet Coordinator HW 5:

- в CLI — по имени учетной записи администратора ViPNet Prime и токену;
- в веб-интерфейсе — по сертификату администратора ViPNet Prime.

Требования к сертификату администратора

- Расширение файла — *.pem, *.crt, *.cer.
- Алгоритм ключа проверки электронной подписи:
 - ГОСТ Р 34.10-2012 для ключей длины 256 бит (OID 1.2.643.7.1.1.1.1).
 - ГОСТ Р 34.10-2012 для ключей длины 512 бит (OID 1.2.643.7.1.1.1.2).
- Сертификат должен быть действительным.
- Должны быть установлены все сертификаты, необходимые для проверки подлинности сертификата администратора (далее — цепочка сертификатов).
- Все сертификаты в цепочке сертификатов должны быть действительными.
- Должен быть установлен актуальный CRL.

Максимальное количество загруженных корневых и промежуточных сертификатов УЦ или CRL — 100.

Установка сертификата УЦ и CRL

Перед установкой сертификата администратора установите корневой и промежуточные сертификаты УЦ и CRL:

- в хранилище системы управления — для учетных записей, созданных в **Главная консоль**  > **Учетные записи**. Предназначаются для поставщика услуг.
- в хранилище организации — для учетных записей, созданных в **Управление организацией**  > **Учетные записи**. Предназначаются для организации.

Так как организации изолированы друг от друга, то корневой сертификат и CRL загружаются для каждой организации.

Таблица 1. Полномочия администраторов

Действие	Роль учетной записи администратора
Установка сертификатов корневых и промежуточных УЦ и CRL в хранилище системы управления	Сервисный администратор
Установка сертификатов корневых и промежуточных УЦ и CRL в хранилище организации	Владелец организации

Загрузка сертификатов корневых и промежуточных УЦ и CRL

- 1 Войдите в ViPNet Prime как сервисный администратор или владелец организации.
- 2 Выберите **Главная консоль**  > **Сертификаты и CRL**.

3 Для установки сертификатов корневого и промежуточных УЦ:

3.1 Выберите **Корневые сертификаты**.

3.2 Нажмите **Установить корневой сертификат** и выберите хранилище:

- **В платформу** — чтобы установить сертификат в хранилище сертификатов для учетных записей администраторов, созданных в **Главная консоль**  > **Учетные записи**.
- **В организацию** — чтобы установить сертификат в хранилище сертификатов для учетных записей администраторов, созданных в **Управление организацией**  > **Учетные записи**.

4 Для установки CRL:

4.1 Выберите **CRL**.

4.2 Нажмите **Установить CRL** и выберите хранилище.

Загрузка сертификата администратора

1 Войдите в ViPNet Prime как сервисный администратор или владелец организации.

2 Выберите:

- **Главная консоль**  > **Учетные записи**. Раздел доступен сервисному администратору.
- **Управление организацией**  > **Учетные записи**. Раздел доступен владельцу организации.

3 Выберите учетную запись администратора.

4 Справа в группе **Личные сертификаты** нажмите **Установить сертификат**.

5 Выберите сертификат администратора.

6 Просмотрите информацию о сертификате и нажмите **Установить**.

Чтобы обновить истекающий сертификат:

1 Выберите учетную запись администратора. В разделе **Личные сертификаты** нажмите .

Чтобы обновить свой личный сертификат на панели сверху нажмите на имя пользователя и выберите **Личные сертификаты**.

2 Нажмите **Установить сертификат**. Выберите сертификат администратора и нажмите **Установить**.

Контроль за сроком действия сертификатов

Периодически обновляйте все установленные сертификаты и CRL для аутентификации администраторов.

Вы можете следить за приближением окончания срока действия сертификата или CRL с помощью:

- Уведомлений по электронной почте — если настроен почтовый сервер и указан адрес электронной почты.

Уведомление отправляется:

- о личном сертификате — учётной записи администратора, которому принадлежит сертификат;
- CRL или корневом сертификате организации — учётным записям владельца организации и суперадминистратору;
- CRL или корневом сертификате платформы — суперадминистратору.
- Индикаторов в веб-интерфейсе — отображаются, если срок действия истекает или истек:
 - в разделе **Сертификаты и CRL**, на вкладках **Корневые сертификаты** или **CRL** и напротив сертификата или CRL,
 - в разделе **Учетные записи** и напротив личного сертификата.

Если ViPNet Prime обнаружил сертификаты или CRL с уже истекшим сроком действия, в веб-интерфейсе появляется красный индикатор.

Если при проверке срока действия обнаружены сертификаты или CRL, до истечения срока действия которых осталось менее 30 дней, появляется желтый индикатор, и на следующий день администратор, который отвечает за обновление этого сертификата или CRL, получает уведомление на электронную почту.

Если срок действия сертификата или CRL приближается к окончанию, [обновите его](#).

Если вы обновили сертификат, и сразу появился индикатор, значит до окончания действия сертификата осталось менее 30 дней.

Обновление сертификата администратора

Если срок действия сертификатов и CRL еще не истёк, как обновить их см. в разделах [Установка сертификата УЦ и CRL](#) и [Загрузка сертификата администратора](#).

Обновить истекший сертификат администратора, CRL, корневой сертификат или другие сертификаты из цепочки доверия может только суперадминистратор. Администраторам ViPNet Prime с другой ролью для обновления истекшего личного сертификата следует обратиться к суперадминистратору с помощью любого доступного канала связи и передать ему новый личный сертификат.

Если истек сертификат суперадминистратора, он может обновить его в консоли на компьютере ViPNet Prime:

- 1 На компьютере с ViPNet Prime войдите в ОС с правами суперпользователя `root` или привилегированного пользователя для использования команды `sudo`.
- 2 Подготовьте сертификаты и CRL, которые будете обновлять.

3 Поместите файлы новых сертификатов в папки для импорта. Для этого выполните команду:

```
$ sudo cp ~/<папка с сертификатами>/<сертификат.cer>  
/var/lib/infotecs/smp-kc/admin_certs/personal — чтобы обновить личный сертификат.  
  
$ sudo cp ~/<папка с сертификатами>/<корневой сертификат.der>  
/var/lib/infotecs/smp-kc/admin_certs/root — чтобы обновить корневой сертификат.  
  
$ sudo cp ~/<папка с сертификатами>/<CRL.crl>  
/var/lib/infotecs/smp-kc/admin_certs/crl — чтобы обновить CRL.
```

4 Перезапустите сервис аутентификации silso. Для этого последовательно выполните команды:

```
$ sudo systemctl restart silso  
  
$ sudo systemctl restart prime-control  
  
$ sudo prime-control
```

5 Чтобы убедиться, что сертификаты успешно обновились, вы можете просмотреть информацию об этом в журнале аудита:

```
$ sudo journalctl -u silso | grep -i importing
```

6 После обновления сертификатов и CRL в ViPNet Prime файлы удаляются из папок для импорта.

Отключение аутентификации по паролю

При повышенных требованиях к безопасности вы можете отключить аутентификацию по паролю. Вход администраторов будет возможен только по личному сертификату администратора. Аутентификация по паролю отключается для всех организаций, то есть для всей сети ViPNet.

При отключении аутентификации по паролю также отключается аутентификация администраторов через Active Directory Federation Services (AD FS).



Внимание! До отключения аутентификации по паролю даже при наличии загруженных сертификатов разрешен вход в ViPNet Prime по паролю или через Active Directory Federation Services (AD FS).

Чтобы отключить аутентификацию администраторов по паролю:

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 Убедитесь, что на координаторе инициализированы токены локальных учетных записей (см. документацию на координатор).
- 3 Выберите Главная консоль  > Настройки.
- 4 Выберите Способ аутентификации > Аутентификация администраторов по паролю.
- 5 Нажмите Отключить.



Внимание! После отключения аутентификации по паролю включить её обратно невозможно.

Пример использования ViPNet PKI Client для аутентификации по сертификату

На рабочем месте администратора установите ViPNet PKI Client и ViPNet PKI Client TLS Unit.

При использовании аутентификации по сертификату по требованиям безопасности должны быть установлены сертификаты сервера ViPNet Prime с криптографическими алгоритмами ГОСТ. См. «ViPNet Prime. Руководство по установке».

Создание запроса на личный сертификат

- 1 В ViPNet PKI Client выберите **Сертификаты**.
- 2 Нажмите **Создать запрос**.
- 3 Заполните поля запроса на сертификат.

Создание запроса на сертификат - ViPNet PKI Client

Заполнить данными из сертификата Очистить форму

Источник шаблонов: Предустановленный

Алгоритм открытого ключа: ГОСТ Р 34.10-2012/512

Параметры открытого ключа: Набор параметров А (ТК 26)

Шаблон: Физическое лицо

* Фамилия: Иванов

* Имя Отчество: Иван Иванович

* Фамилия Имя Отчество: Иванов Иван Иванович

* Страна: Российская Федерация (RU)

Субъект РФ по адресу регистрации:

Наименование населенного пункта:

Название улицы, номер дома:

Создать запрос Отмена

Рисунок 14. Создание запроса на сертификат

- 4 Сохраните запрос.
- 5 В зависимости от версии ViPNet PKI Client укажите место хранения контейнера ключей:
 - 1.x — откроется окно криптопровайдера, выберите папку на диске.
 - 2.x — откроется окно ViPNet PKI Client, выберите **Хранилище ViPNet PKI Client**.
- 6 Задайте пароль от контейнера ключей. Подробнее см. в документации ViPNet PKI Client.

Создание личного сертификата в УЦ

Ниже приведен пример с использованием тестового УЦ ИнфоТеКС <http://testcert.infotecs.ru/>.

- 1 Прочитайте **Условия применения**. Если согласны, продолжите действие на странице.
- 2 Выберите файл запроса на личный сертификат.
- 3 Нажмите **Отправить запрос**. Создастся сертификат.
- 4 Скачайте сертификат. Он сохранится в загрузки браузера.
- 5 Скачайте корневой сертификат УЦ и CRL.
- 6 В ViPNet PKI Client загрузите файлы от УЦ: личный сертификат, корневой сертификат, CRL.
- 7 Если ViPNet PKI Client версии 1.x и личный сертификат и закрытый ключ хранятся не на токене, импортируйте их в Infotecs Software Token. Для этого выберите сертификат, затем выберите **Скопировать ключ в Infotecs Software Token**.

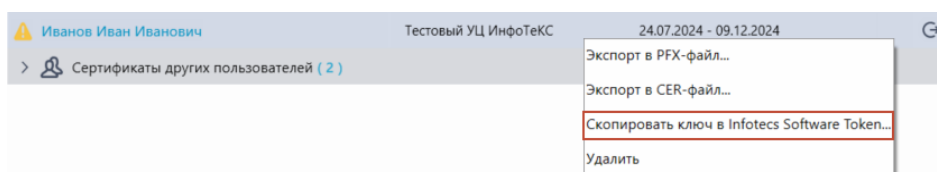


Рисунок 15. Копирование ключа в программный токен

- 8 Выгрузите личный сертификат. Для этого выберите сертификат, затем выберите **Экспорт в CER-файл**. Этот файл загрузите для учетной записи администратора в ViPNet Prime.

Аутентификация по паролю

Управление временем блокировки входа в учетную запись

При аутентификации по паролю учетная запись защищена от подбора пароля. После четырех неудачных попыток ввода пароля вход в учетную запись временно блокируется. По умолчанию время блокировки — 10 минут.

В случае превышения попыток ввода:

- вход для учетной записи блокируется на время, установленное в конфигурационном файле;
- в веб-интерфейсе появляется информация о временной блокировке входа для учетной записи и отображается время, оставшееся до разблокировки;
- вход для учетной записи блокируется в ViPNet Prime и в ViPNet Coordinator HW 5;
- в журнале аудита фиксируется каждая попытка входа и событие блокировки учетной записи.

Чтобы изменить время блокировки учетной записи:

- 1 Войдите в ОС с правами суперпользователя root или привилегированного пользователя для использования команды `sudo`.
- 2 Остановите ViPNet Prime:

```
$ sudo deployment-configurator stop --all
```
- 3 Откройте файл `/usr/share/infotecs/smp-kc/config.env`.
- 4 Для параметра `SILSO_IdentityLockoutOptions__LockoutDurationInMin` установите значение от 10 до 1440 минут.



Внимание! В синтаксисе параметра

`SILSO_IdentityLockoutOptions__LockoutDurationInMin` используются одинарный (`_`) и двойной (`__`) символы нижнего подчеркивания.

Если значение не входит в указанный диапазон, для значения меньше 10 минут система устанавливает время блокировки 10 минут, для значения больше 1440 минут — 1440 минут.

- 5 Запустите ViPNet Prime:

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

Настройка длины и срока действия пароля

Если не отключена аутентификация по паролю, вы можете настроить:

- минимальную длину пароля,
- срок действия пароля,
- количество сохраняемых паролей,
- необходимость смены предустановленного пароля.

Чтобы задать настройки:

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 Выберите **Главная консоль**  > **Настройки**.
- 3 В разделе **Настройка паролей учетных записей** нажмите .
- 4 Укажите максимальный срок действия пароля от 1 до 365 дней. По умолчанию установлен срок 180 дней. Рекомендуется устанавливать срок действия пароля от 1 до 184 дней. Срок действия считается в днях с учетом текущего и истекает в 00:00 по UTC. Например, если срок действия пароля установлен 1 день, то в 00:00 следующего дня пароль перестанет действовать.
- 5 Укажите минимальную длину пароля от 6 до 31 символа. По умолчанию длина пароля 8 символов. Рекомендуется устанавливать минимальную длину пароля от 8 до 31 символа.
- 6 Укажите количество сохраняемых паролей. По умолчанию установлено 5, вы можете установить от 5 до 15. ViPNet Prime будет хранить хэш-суммы паролей, а не сами пароли. При смене пароля будет сверяться хэш-сумма нового пароля с сохраненными. Если новый пароль совпадет с хранимой хэш-суммой, ViPNet Prime не даст установить этот пароль.
- 7 Выберите **Требовать сменить предустановленный пароль**, чтобы при входе в ViPNet Prime требовалось сменить пароль, если он был задан не владельцем учетной записи.
- 8 Нажмите **Сохранить**.



Примечание. Настройки не распространяются на пароли администраторов и пользователей узлов.

При обновлении ViPNet Prime с версии, где не было настроек, настройки устанавливаются по умолчанию.

Если длина пароля после обновления не соответствует требованиям, при каждом входе будет отображаться предупреждение.

Срок действия пароля отсчитывается с момента:

- создания учетной записи;
- обновления ViPNet Prime;

- изменения пароля.

После истечения срока действия пароля при входе в ViPNet Prime администратору потребуется сменить пароль, иначе вход в ViPNet Prime будет запрещен.

За 7 дней до истечения срока действия пароля администратор оповещается с помощью уведомления:

- в веб-интерфейсе;
- по электронной почте, если настроен почтовый сервер и получение уведомлений.

Доменная аутентификация

Для использования доменной аутентификации пользователей и администраторов организации:



Внимание! В сертификате сервера, в поле SAN должен быть указан домен организации. Подробнее см. в Руководстве по установке в разделе «Подготовка TLS-сертификатов».

- 1 [Настройте службу федерации AD FS на стороне AD.](#)
- 2 Настройте подключение к AD FS организации на стороне ViPNet Prime.

Это позволит администраторам в организации входить в ViPNet Prime с учетной записью каталога AD.

Установка и настройка AD FS на стороне AD

Для взаимодействия с Active Directory в ViPNet Prime встроен сервис аутентификации. Он работает по протоколу OpenID Connect и выступает в качестве клиента. К нему нужно настроить доверие сервера AD FS. Для этого:

- 1 Установите службу федерации AD FS.
- 2 Добавьте группу приложений (Application Groups). Консоль управления AD FS генерирует идентификатор клиента для новой программы. Идентификатор клиента понадобится вам для настройки интеграции в ViPNet Prime.
- 3 Добавьте правила преобразования утверждения. Это необходимо для отправки адреса электронной почты из Active Directory в качестве утверждения клиентскому приложению.

ViPNet Prime и AD FS в одном домене

Установка AD FS

- 1 На компьютере с AD установите роль **Службы федерации Active Directory**.
- 2 Настройте службу AD FS:
 - 2.1 Укажите TLS-сертификат для установления доверительных отношений между ViPNet Prime и AD FS.



Внимание! Для установления доверия между AD FS и ViPNet Prime необходим TLS-сертификат с двумя wildcard-записями. Например, если ViPNet Prime доступен по адресу `https://Prime.example.ru`, а AD FS — `https://adfs.Prime.example.ru`, сертификат должен иметь записи `*.example.ru` и `*.Prime.example.ru`.

- 2.2 Задайте **Отображаемое имя службы**.

2.3 Укажите учетную запись пользователя домена или групповую учетную запись, для запуска службы.

2.4 Создайте новую базу данных или укажите расположение уже созданной.

Проверьте выбранные параметры, убедитесь, что все предварительные требования соблюдены и нажмите **Настроить**.

Добавление группы приложений

- 1 На компьютере AD запустите **Диспетчер серверов**.
- 2 Перейдите в **Сервис > Управление AD FS**.
- 3 Выберите **Группы приложений > Добавить группы приложений**.
- 4 Задайте **Имя**, например Prime, и выберите тип **Серверное приложение, подключающееся к веб-API**.

Сохраните на компьютере автоматически сгенерированный **Идентификатор клиента (Client ID)**. Он потребуется при [настройке доменной аутентификации с помощью AD FS](#).

- 5 В поле **Перенаправить URI** укажите:
 - адрес обработки результатов входа, например
`https://Prime.example.ru/auth/signin-<поддомен>;`
 - адрес обработки результатов выхода, например
`https://Prime.example.ru/auth/signout-callback-oidc.`

При первой настройке AD FS вручную задайте параметр **<поддомен>**. Это псевдоним для аутентификации организации. Его значение будет ставиться перед доменным именем ViPNet Prime. Укажите такое же значение [при настройке аутентификации в ViPNet Prime](#) в параметре **Поддомен**.

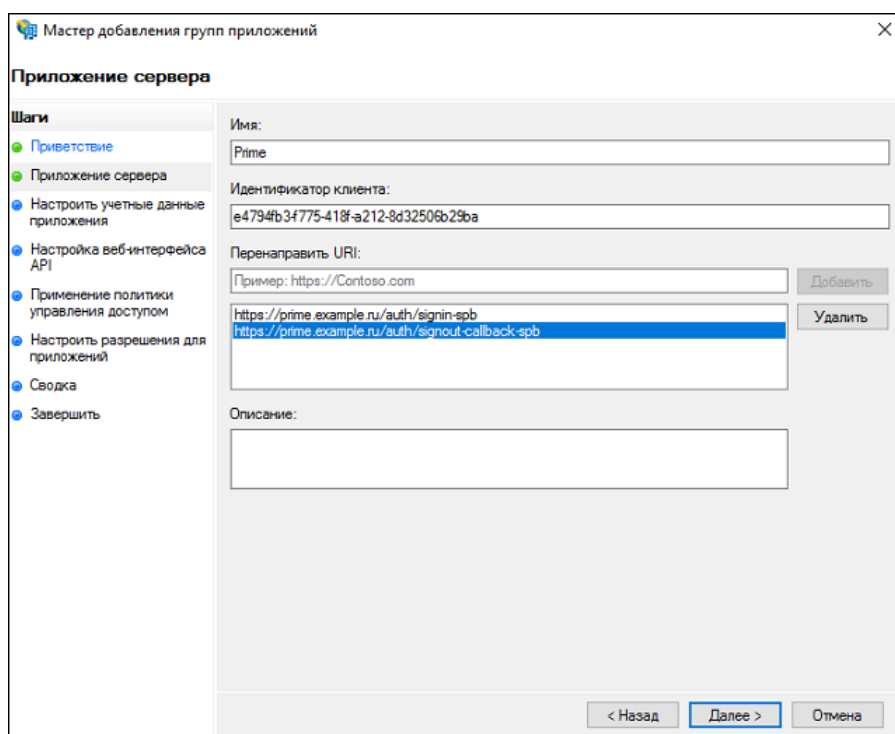


Рисунок 16. Создание приложения сервера

- 6 Выберите **Создать общий секрет (Client secret)** и сохраните на компьютере. Он потребуется при [настройке доменной аутентификации с помощью AD FS](#).
- 7 Добавьте сохраненный ранее идентификатор клиента.
- 8 Укажите политику управления доступом. По умолчанию выбрана **Разрешение для каждого**.
- 9 В поле **Разрешенные области** выберите **allatclaims**, **openid** и **profile**.
- 10 В следующем окне проверьте указанные параметры и нажмите **Далее**.
- 11 Нажмите **Заккрыть**.

Добавление правила преобразования утверждения

Для работы доменной аутентификации ViPNet Prime с использованием AD FS создайте правило и добавьте утверждение с адресом почтового ящика пользователя. Для этого:

- 1 Откройте свойства группы приложений.
- 2 В разделе **Веб-интерфейс API** выберите созданное ранее приложение.
- 3 Перейдите на вкладку **Правила преобразования выдачи** и нажмите **Добавить правило**.
- 4 В выпадающем списке выберите **Отправка атрибутов LDAP как утверждений**.
- 5 Задайте **Имя правила утверждения**.
- 6 В качестве хранилища атрибутов укажите **Active Directory**.
- 7 Настройте сопоставление атрибутов LDAP и типов исходящего утверждения:
 - В столбце **Атрибут LDAP** выберите **E-Mail-Addresses**.

- В столбце **Тип исходящего утверждения** выберите **Адрес электронной почты**.

Мастер добавления правила преобразования утверждения

Настройка правила

Шаги

- Выберите тип правила
- Настройте правило утверждения

Это правило можно настроить для отправки значений атрибутов LDAP как утверждений. Выберите хранилище атрибутов, из которого следует извлекать атрибуты LDAP. Укажите, как атрибуты будут сопоставляться с типами исходящих утверждений, которые будут выпускаться с помощью этого правила.

Имя правила утверждения:

email

Шаблон правила. Отправка атрибутов LDAP как утверждений

Хранилище атрибутов:

Active Directory

Сопоставление атрибутов LDAP типам исходящих утверждений:

Атрибут LDAP (выберите или введите, чтобы добавить больше)	Тип исходящего утверждения (выберите или введите, чтобы добавить больше)
E-Mail-Addresses	Адрес электронной почты
*	

< Назад Готово Отмена

Рисунок 17. Настройка правила утверждения

Настройка доменной аутентификации с помощью служб федераций AD FS

Чтобы задать параметры подключения к AD FS организации:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Если вы администрируете несколько организаций, **выберите организацию**.
- 3 Выберите **Управление организацией**  > **Аутентификация**.
- 4 Нажмите **Настроить**.
- 5 Задайте параметры:
 - **URL-адрес службы AD FS**. Поддерживается только HTTPS. Например: `https://adfs.server.com/adfs`.
 - **Идентификатор приложения (Client ID)** — параметр, полученный при настройке приложения ViPNet Prime в AD FS. Например: `f5d1fe59-7cb2-4c64-be91-e1a48e9dbee7`.
 - **Секрет приложения (Client Secret)** — параметр, полученный при настройке приложения ViPNet Prime в AD FS. Например: `Ug737Fmp1NHmSrxAUqW9NY3KErOizREfwltGtWlO`.
 - **Поддомен** — доменное имя (псевдоним) для аутентификации организации в системе управления с использованием AD FS. Например, введите имя `org1`, если прямая ссылка

организации `org1.Prime.example.ru`. Настройте разрешение заданного доменного имени, см. руководство по установке, раздел «Настройка DNS».

При первой настройке AD FS задайте такое же значение, как в параметре `<поддомен>` [при настройке группы приложений](#).

- **URL-адрес страницы входа в приложение ViPNet Prime** — ссылка организации для подключения к веб-интерфейсу ViPNet Prime через AD. Формируется автоматически на основе параметра **Поддомен**.
- **Название кнопки для доменной аутентификации** — отображается при подключении к веб-интерфейсу ViPNet Prime.
- **Сервис аутентификации приложения в ViPNet Prime** — адреса обработки результатов входа и выхода. Формируются автоматически на основе параметра **Поддомен**. Значения в ViPNet Prime должны совпадать со значениями в параметре **URI перенаправления** в свойствах группы приложений.

При настройке первой организации проверьте, чтобы параметры совпадали.

Если вы уже настроили AD FS и настраиваете доменную аутентификацию для других организаций, добавьте адреса из параметра **Сервис аутентификации приложения в ViPNet Prime** в AD FS:

- Скопируйте адреса из параметра **Сервис аутентификации приложения**.
- На компьютере AD откройте **Диспетчер серверов > Сервис > Управление AD FS > Группы приложений**.
- Откройте свойства группы, добавленной для ViPNet Prime.
- В параметр **URI перенаправления** добавьте скопированные адреса из ViPNet Prime.
- Сохраните изменения.

6 Нажмите **Создать**.

7 Если вы изменяете уже существующие настройки, перезагрузите ViPNet Prime.

Аутентификация AD FS

×

dfdfa315-8056-4708-9998-7deb9ccb681d

Секрет приложения (Client Secret)

Страница входа в приложение ViPNet Prime

* Поддомен ?

provider1

URL-адрес страницы входа в приложение ViPNet Prime

https://provider1.tst143.dev.spb.mngmob

* Название кнопки для доменной аутентификации ?

Доменная аутентификация

Не более 30 символов с пробелами.

Сервис аутентификации приложения ViPNet Prime

Это URL-адреса, на которые служба AD FS будет перенаправлять пользователя после аутентификации или отказа в аутентификации. Используйте их в AD FS для Redirect URI.

https://tst143.dev.spb.mngmob/auth/signin-provider1

https://tst143.dev.spb.mngmob/auth/signout-callback-oidc

Сохранить

Отмена

Рисунок 18. Настройка федеративного доступа для организации

Примечание. Пользователям, которые будут использовать доменную аутентификацию, задайте одинаковый адрес электронной почты в ViPNet Prime и в Active Directory.

Чтобы администраторы ViPNet Prime могли использовать доменную аутентификацию, при создании учетной записи укажите адрес электронной почты пользователя, импортированного из Active Directory.

ViPNet Prime. Руководство администратора | 82

6

Управление организацией

Порядок создания организации	84
Управление учетными записями администраторов	85
Управление организационной структурой	90
Управление пользователями	93
Управление устройствами	101

Порядок создания организации

Действие	Роль
☐ Для разграничения прав управления организациями создайте учетные записи администраторов и назначьте им роли	• Владелец организации
☐ По требованиям безопасности настройте аутентификацию администраторов по сертификатам	• Сервисный администратор • Владелец организации
☐ Создайте корневые организации	• Оператор Prime
☐ Создайте дочерние организации	• Владелец организации
☐ Создайте подразделения	• Владелец организации • Администратор организации

Затем распределите лицензии на ПО ViPNet в организации, чтобы администратор смог создать защищенную сеть организации:

Действие	Роль
☐ Распределите лицензии на продукты ViPNet	• Оператор Prime
☐ Создайте структуру сети организации	• Владелец организации • Администратор организации

Управление учетными записями администраторов

После первого входа в ViPNet Prime для передачи управления другим администраторам создайте учетные записи и назначьте им роли. Роли могут быть назначены учетной записи администратора в разделах:

- в разделе **Главная консоль** — для управления лицензиями и администрирования на уровне поставщика услуг:
 - сервисный администратор;
 - оператор Prime.
- в разделе **Управление организацией** — [на уровне организации](#):
 - владелец организации;
 - администратор организации;
 - сетевой администратор шлюза безопасности;
 - аудитор устройств.

Если ViPNet Prime установлен и используется одним предприятием, создайте учетные записи в организации в разделе **Главная консоль** .

Создание учетной записи администратора в главной консоли

- 1 Войдите в ViPNet Prime как сервисный администратор.
- 2 Выберите **Главная консоль**  > **Учетные записи**.
- 3 Нажмите  **Добавить**.
- 4 На шаге 1 укажите:
 - Имя учетной записи администратора.
Не используйте символ / в имени учетной записи. Имя не должно начинаться и заканчиваться специальным символом.
 - Пароль для учетной записи. Чтобы автоматически создать надежный пароль, нажмите **Сгенерировать**.
Длина пароля не более 256 символов. [Минимальную длину задает](#) суперадминистратор.
Пароль должен содержать не менее одного символа из каждой категории:

- заглавные латинские буквы;
- строчные латинские буквы;
- цифры;
- специальные символы: ! " # \$ % & * () _ - + = @ ; : . , ^ ' ? { } [] / | \ > < ` ~

- **Имя пользователя** — текстовое описание имени администратора.
- **Почта** — адрес электронной почты администратора для доменной аутентификации и получения уведомлений из ViPNet Prime и других модулей.

Изменить эти параметры могут суперадминистратор, сервисный администратор или владелец организации.

5 На шаге 2 в разделе **Роли в системе управления** выберите роли.

6 Чтобы ознакомиться с полномочиями ролей, нажмите **Показать полномочия ролей** ⓘ.

Рисунок 19. Назначение ролей учетной записи администратора в главной консоли

7 Чтобы назначить роль учетной записи администратора в организации:

7.1 В разделе **Роли в организациях** нажмите ⓘ **Добавить**.

7.2 Выберите организации и нажмите **Сохранить**.

7.3 Выберите организацию и роли в ней.

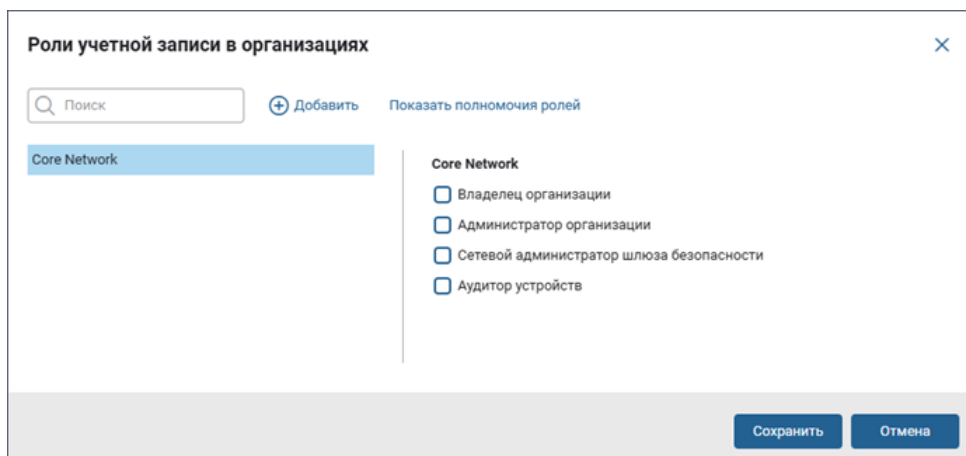


Рисунок 20. Назначение ролей учетной записи в организациях

7.4 Нажмите **Сохранить**.

8 Нажмите **Готово**.

Чтобы изменить пароль или другие параметры учетной записи администратора, нажмите .

Создание учетной записи администратора в организации

1 Войдите в ViPNet Prime как владелец организации.

2 Выберите **Управление организацией**  > **Учетные записи**.

3 Нажмите  **Добавить**.

4 Задайте следующие параметры:

- Имя учетной записи администратора.

Не используйте символ / в имени учетной записи. Имя не должно начинаться и заканчиваться специальным символом.

- Пароль учетной записи. Чтобы автоматически создать надежный пароль, нажмите **Сгенерировать**.

Длина пароля не более 256 символов. [Минимальную длину задает](#) суперадминистратор.

Пароль должен содержать не менее одного символа из каждой категории:

- заглавные латинские буквы;
- строчные латинские буквы;
- цифры;
- специальные символы: ! " # \$ % & * () _ - + = @ ; : . , ^ ' ? { } [] / | \ > < ` ~

- Имя пользователя.
- Адрес электронной почты администратора для доменной аутентификации и получения уведомлений из ViPNet Prime.

5 В группе **Роли в организации** выберите роли учетной записи.

6 Нажмите **Готово**.

Чтобы изменить пароль или другие параметры учетной записи администратора:

- 1 Войдите в ViPNet Prime как владелец организации.
- 2 Выберите **Управление организацией**  > **Учетные записи**.
- 3 Выберите учетную запись и нажмите .

При смене пароля чужой учетной записи требование к количеству измененных символов не предъявляется.

Назначение ролей учетной записи в организации

- 1 Войдите в ViPNet Prime как владелец организации.
- 2 Выберите **Главная консоль**  > **Организации**.
- 3 Выберите организацию.
- 4 На панели справа в группе **Администраторы** нажмите .
- 5 Нажмите  **Добавить**.
- 6 В окне **Добавление администраторов** выберите учетные записи и нажмите **Сохранить**.
- 7 Выберите учетную запись администратора и роли для него.
- 8 Чтобы ознакомиться с полномочиями ролей администраторов, нажмите **Показать полномочия ролей**.

Администраторы в организации

Поиск

+

Добавить

Показать полномочия ролей

auditor

auditor

☐ Владелец организации

☒ Администратор организации

☐ Сетевой администратор шлюза безопасности

☐ Аудитор устройств

Сохранить

Отмена

Рисунок 21. Назначение роли учетной записи администратора в организации

9 Нажмите **Сохранить**.

Управление организационной структурой

Создание организации

Защищенную сеть разделите на изолированные части — организации, чтобы предоставить к ним доступ для управления. Организациями могут быть потребители **поставщика услуг**, подразделения или филиалы крупного предприятия и так далее.

Когда администратор создает организацию, то его учетной записи назначается роль владельца организации. Для создания корневой организации администратор должен обладать полномочием создания родительских и дочерних организаций, то есть быть суперадминистратором или оператором Prime. Корневые организации отображаются в разделе **Главная консоль**  > **Организации** в списке первого уровня. Максимальное количество корневых организаций — 100.

Чтобы создать организацию (корневую, дочернюю):

- 1 Войдите в ViPNet Prime как оператор Prime или владелец организации.
- 2 Выберите **Главная консоль**  > **Организации**.
- 3 Нажмите  **Добавить**.
- 4 Введите название организации и ИНН (при необходимости).
- 5 Чтобы различать организации в отчетах для биллинга и статистике использования, введите произвольное название типа организации (например, поставщик услуг, организация-потребитель, дилер, реселлер, партнер и тому подобное).
ИНН и тип организации используются в отчетах для биллинга.
- 6 Чтобы создать дочернюю организацию, в поле **Родительская организация** выберите вышестоящую организацию.
- 7 Нажмите **Добавить**.

Если организацию создает оператор Prime, то для безопасности суперадминистратор должен снять роль владельца организации с оператора Prime и назначить ее на себя или на другую учетную запись с ролями владельца организации или администратора организации.

Создание подразделения

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **Управление организацией**  > **Подразделения**.

- 3 Если вы администрируете несколько организаций, [выберите организацию](#).
- 4 Нажмите  **Добавить**.
- 5 Введите название подразделения.
- 6 Для создания подчиненного подразделения выберите вышестоящее подразделение. Максимальный уровень вложенности подразделений — 10.
- 7 Нажмите **Добавить**.

Выбор организации и подразделения

Если вы управляете несколькими организациями:

- 1 Вверху нажмите  и выберите организацию.

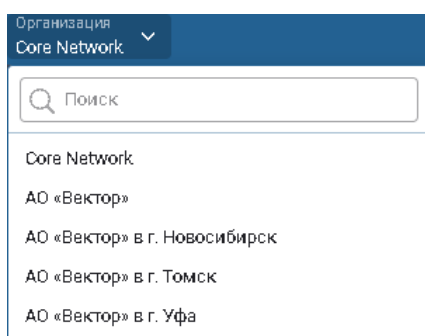


Рисунок 22. Выбор организации

- 2 Вверху нажмите  и выберите подразделение. Если в организации не созданы подразделения, список не отображается.

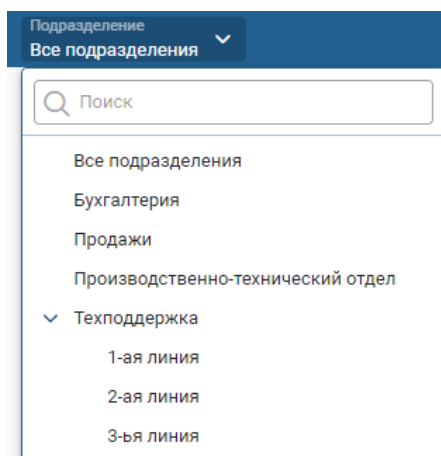


Рисунок 23. Выбор подразделения

- 3 Чтобы просмотреть пользователей и устройства всех подразделений организации, выберите **Все подразделения**.

Удаление организации или подразделения

Вы можете удалить организацию или подразделение, если они не содержат дочерние организации или подразделения с критически важными для работоспособности сети устройствами.

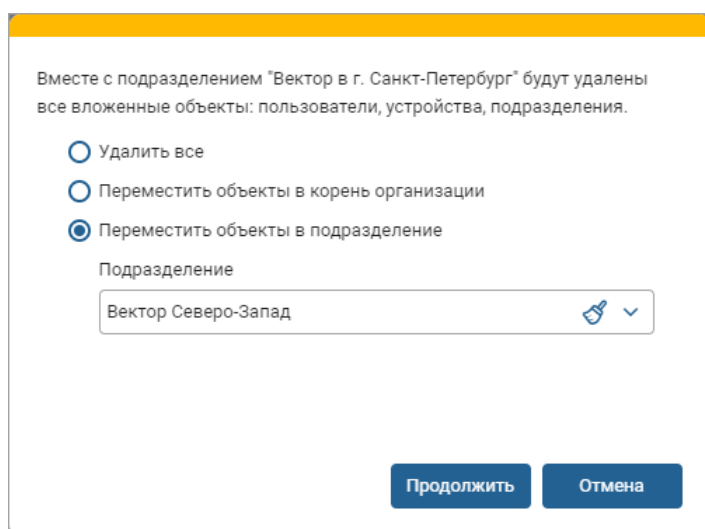
При удалении подразделения вы можете переместить входящие в него дочерние подразделения, пользователей и устройства в другое подразделение или в корень родительской организации.

Чтобы удалить организацию:

- 1 Войдите в ViPNet Prime как сервисный администратор или владелец организации.
- 2 Выберите **Главная консоль**  > **Организации**.
- 3 Выберите организацию.
- 4 Нажмите .

Чтобы удалить подразделение:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию.
- 3 Выберите **Управление организацией**  > **Подразделения**.
- 4 Выберите подразделение.
- 5 Нажмите .
- 6 Если в подразделении созданы дочерние подразделения, то выберите, следует ли перемещать объекты из удаляемого подразделения в другое.



Вместе с подразделением "Вектор в г. Санкт-Петербург" будут удалены все вложенные объекты: пользователи, устройства, подразделения.

☐ Удалить все

☐ Переместить объекты в корень организации

☒ Переместить объекты в подразделение

Подразделение

Вектор Северо-Запад

Продолжить Отмена

Рисунок 24. Удаление подразделения

- 7 Нажмите **Продолжить**.

Управление пользователями

Вы можете создать пользователей несколькими способами:

- [добавить пользователей вручную](#);
- [импортировать учетные записи пользователей из Active Directory](#);
- [импортировать учетные записи пользователей из файла CSV](#).

Чтобы пользователи использовали прикладное ПО ViPNet на своих устройствах, [выдайте организации лицензии на ПО](#).

Чтобы обновить данные о пользователях из AD или CSV, вы можете импортировать данные только для пользователей, учетные записи которых были изменены.

Чтобы импортировать учетные записи пользователей из AD:

- 1 Установите и настройте коннектор AD. См. «ViPNet Prime. Руководство по установке».
- 2 В ViPNet Prime [настройте параметры импорта из AD и параметры подключения к AD](#).
- 3 В ViPNet Prime [импортируйте учетные записи пользователей из AD](#).

Формат данных пользователей

- Максимальная длина имени пользователя — 128 символов.
- Номер телефона указывается в международном формате:
 - максимальная длина номера — 15 символов;
 - допустимы только цифры и знак +.

Добавление пользователей вручную

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 [Выберите организацию и подразделение](#).
- 3 Выберите **Управление организацией**  > **Пользователи**.
- 4 Нажмите **Добавить**.
- 5 Введите имя пользователя, его описание (например, департамент или должность) и контактные данные — адрес электронной почты и [номер телефона](#).
- 6 Выберите подразделение, в котором следует создать пользователя.
- 7 Нажмите **Создать**.

Импорт учетных записей пользователей из файла CSV

- 1 Подготовьте файл CSV к импорту. Файл выгрузите из внешней системы (например, Active Directory). В качестве разделителя значений используйте запятую или точку с запятой.

Пример содержания файла:

NAME,EMAIL,PHONE,DESCRIPTION

Иванов Иван,ivanov@example.ru,+1234567891,Отдел закупок

Сидоров Дмитрий,sidorov@example.ru,,Отдел закупок

Петров Андрей,petrov@example.ru,+1234567890,Отдел закупок

- 2 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 3 Выберите **Управление организацией**  > **Пользователи**.
- 4 Нажмите  **Импортировать**. Следуйте указаниям мастера.
- 5 В качестве источника для импорта выберите **Из файла CSV**.
- 6 Нажмите **Обзор файлов** и выберите файл CSV.
- 7 В списке **Разделитель** выберите символ, который разделяет значения в строках, и нажмите **Далее**.

Примечание. Убедитесь, что в файле CSV:



- используется кодировка UTF-8;
- в полях с описанием пользователя символ, выбранный в качестве разделителя, встречается только как разделитель.

-
- 8 Проверьте, что заголовки столбцов из файла CSV соответствуют названиям параметров пользователя. Если соответствия в названиях столбцов не определены автоматически, в списках выберите соответствия вручную.

Импорт пользователей ✕

Шаг 2 из 4

Проверьте, что заголовки столбцов из файла CSV соответствуют названиям параметров пользователя. Если соответствия в названиях столбцов не определены автоматически, в списках выберите соответствия вручную.

* Имя пользователя

NAME 🔍 ▼

Почта

EMAIL 🔍 ▼

Телефон

PHONE 🔍 ▼

Описание

DESCRIPTION 🔍 ▼

Назад Далее Отмена

Рисунок 25. Проверка соответствия заголовков столбцов из файла CSV и названий параметров пользователя

- 9 На странице **Параметры импорта** выберите, какие учетные записи пользователей импортировать:
- **Только новых пользователей** — чтобы импортировать только новые учетные записи пользователей.
 - **Все доступные для импорта** — чтобы импортировать все учетные записи пользователей.
 - **Только обновления для существующих пользователей** — чтобы обновить информацию о пользователях с измененными адресом электронной почты, телефоном, описанием.

Флажок **Выбор импортируемых записей вручную** выбран по умолчанию.

- 10 Чтобы импортировать все учетные записи пользователей из файла CSV без предварительного просмотра, снимите флажок **Выбор импортируемых записей вручную**.
- 11 Чтобы сохранить исключенные из импорта учетные записи пользователей с некорректными данными в файл CSV, нажмите **Скачать исключенные записи**. Вы сможете изменить эти учетные записи и импортировать их позже.

Некорректными данными считаются:

- некорректный формат адреса электронной почты (Ivanov@ вместо Ivanov@example.ru);
- слишком короткий номер телефона;
- не указано имя пользователя (обязательное поле).

Рисунок 26. Выбор импортируемых записей пользователей из файла CSV

- 12 Выберите пользователей и нажмите **Импортировать**.
- 13 На странице с информацией об успешном импорте пользователей нажмите **Заккрыть**.

Настройка интеграции с Active Directory

Интеграция с AD позволит **добавить доменные учетные записи пользователей в защищенную сеть**. Из каталога AD загружаются имя пользователя, адрес электронной почты, номер телефона.

Максимальное количество импортируемых учетных записей пользователей — 65534.

Для интеграции с AD:

- 1 Установите коннектор AD с помощью скрипта из комплекта поставки на компьютере с AD. См. «ViPNet Prime. Руководство по установке», раздел «Установка, обновление и настройка коннектора Active Directory».
- 2 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 3 Выберите **Управление организацией**  > **Импорт данных**.
- 4 Нажмите **Настроить**.
- 5 На шаге 1 введите:
 - URL-адрес коннектора AD с указанием протокола подключения:
`https://<IP-адрес или доменное имя коннектора AD>:<порт>/`
 - Параметр в поле **Идентификатор организации** задается автоматически.

Таймаут ожидания ответа от AD при проверке соединения — 15 секунд.

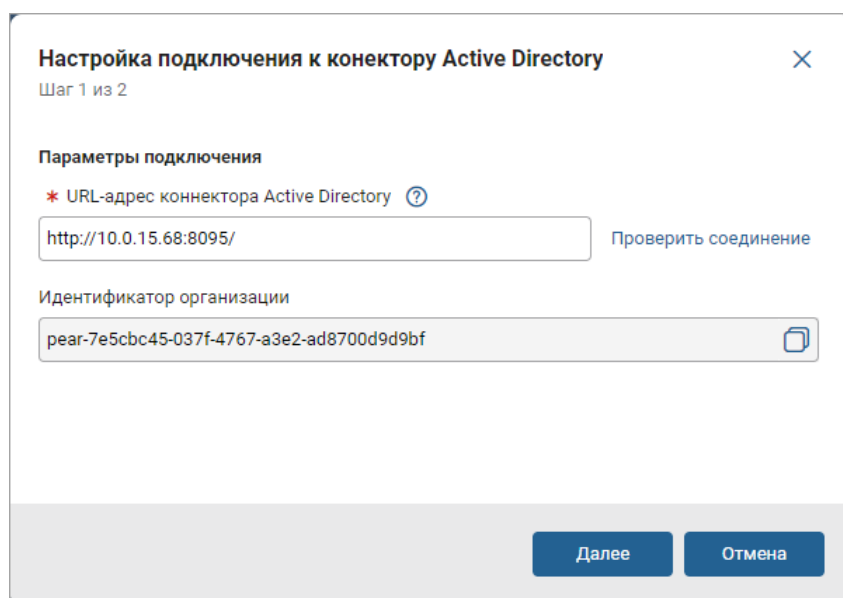


Рисунок 27. Ввод URL-адреса коннектора AD

- 6 На шаге 2 с учетом синтаксиса LDAP-запроса задайте названия атрибутов импорта:
- **LDAP-запрос для импорта пользователей из Active Directory.** По умолчанию запрос `objectCategory=person` импортирует все учетные записи из AD.
 - **Внешний идентификатор.** Например, `objectGUID`.
 - **Имя пользователя** — имя пользователя Active Directory или LDAP-сервера. Например, `cn`.
 - **Email** — адрес электронной почты. Например, `mail`.
 - **Телефон** — номер телефона пользователей. Например, `mobile`.
Номер телефона должен быть задан [в международном формате](#).
 - **Описание** — информация о пользователях. Например, `description`.
 - **Фотография** — атрибут `thumbnailPhoto`. Ограничение на размер файла — 100 Кбайт.

Настройка подключения к конектору Active Directory

Шаг 2 из 2

*** Внешний идентификатор**

Например: objectGUID

*** Имя пользователя**

Например: cn, userPrincipalName, adminDisplayName.

Почта

Например: mail, mailAddress, otherMailbox.

Телефон

Например: mobile, otherMobile, telephoneNumber.

Описание

Например: description, adminDescription.

Фотография

Например: thumbnailPhoto

Рисунок 28. Настройка параметров выгрузки пользователей из AD

Импорт учетных записей пользователей из Active Directory

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **Управление организацией**  > **Пользователи**.
- 3 Нажмите  **Импортировать**.
- 4 На шаге 1 выберите **Из Active Directory**.
- 5 Нажмите **Далее**.
- 6 На шаге 2 выберите:
 - **Все доступные для импорта** — чтобы импортировать все учетные записи пользователей Active Directory.
 - **Только новых пользователей** — чтобы импортировать только новые учетные записи пользователей Active Directory.

- **Только обновления для существующих пользователей** — чтобы заменить информацию о пользователях, учетные записи которых были обновлены в Active Directory.

Флажок **Выбор импортируемых записей вручную** выбран по умолчанию.

- 7 Чтобы импортировать все учетные записи пользователей из Active Directory без предварительного просмотра, снимите флажок **Выбор импортируемых записей вручную**.
- 8 Чтобы учетные записи пользователей Active Directory с некорректными данными изменить и импортировать из файла CSV позже, нажмите **Скачать исключенные записи**.
- 9 Нажмите **Далее**.
- 10 На странице **Выбор импортируемых записей** выберите учетные записи пользователей Active Directory.
- 11 Нажмите **Импортировать**.
- 12 Чтобы закрыть мастер импорта пользователей и продолжить выполнение операции в фоновом режиме, нажмите **Заккрыть**.

Удаление пользователей

При удалении пользователей удалите сначала их устройства. Пользователи удаляются из всех модулей.

Чтобы удалить пользователя:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Если устройства пользователя задействованы в модуле VPN, удалите устройства из модуля VPN:
 - 2.1 Выберите **ViPNet VPN**  > **Клиенты**.
 - 2.2 Выберите устройства пользователя и нажмите .
- 3 **Удалите устройства пользователя из системы управления.**
- 4 Выберите **Управление организацией**  > **Пользователи**.
- 5 Выберите пользователей и нажмите .

Перемещение пользователей и устройств подразделения

Вы можете перемещать пользователей и устройства между подразделениями внутри одной организации. Вместе с пользователями перемещаются их устройства.

Чтобы переместить пользователей вместе с их устройствами (или только устройства):

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Если вы администрируете несколько организаций, [выберите организацию и подразделение](#).
- 3 Выберите **Управление организацией**  > **Пользователи** (или **Устройства**).
- 4 Выберите пользователей или устройства и нажмите  **Переместить**.
- 5 Выберите **Переместить в корень организации** или **Переместить в подразделение** и выберите подразделение.
- 6 Нажмите **Переместить**.

Управление устройствами

Чтобы централизованно контролировать работу устройств и управлять ими из ViPNet Prime, создайте устройства.

Вы можете создать устройства двумя способами:

- Сначала [создать устройство](#), затем в модуле VPN выбрать его в качестве координатора, межсетевого экрана ViPNet xFirewall, клиента или ресурса.
- Создать новое устройство в модуле VPN — [координатор](#), [межсетевой экран ViPNet xFirewall](#), [клиент](#) или [ресурс с несколькими IP-адресами](#).

В этом случае созданные в модуле VPN координаторы, клиенты или межсетевые экраны ViPNet xFirewall отобразятся в списке всех устройств организации со значком выполнения функций в модуле VPN .

Создание устройств

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 [Выберите организацию и подразделение](#).
- 3 Выберите **Управление организацией**  > **Устройства**.
- 4 Чтобы создать пользовательское устройство с владельцем (мобильное устройство или рабочий компьютер сотрудника):
 - 4.1 Нажмите  **Новое устройство**.
 - 4.2 В списке выберите **Для пользователя**.
 - 4.3 Укажите параметры устройства:
 - Имя и описание устройства. Максимальная длина имени устройства — 50 символов.
 - Пользователя устройства.



Внимание! После добавления устройства в модуль VPN смена пользователя на устройстве невозможна.

- 5 Чтобы создать серверное устройство для организации (шлюз безопасности, ресурс с одним IP-адресом, серверы ConServer и CPNS):
 - 5.1 Нажмите  **Новое устройство**.
 - 5.2 Укажите имя и описание устройства. Максимальная длина имени устройства — 50 символов.
 - 5.3 Выберите **В организацию**.

6 Нажмите **Сохранить**.

7 Далее в модуле VPN при создании устройства защищенной сети выберите созданное устройство.

Назначение пользователя на устройства

Вы можете назначить пользователя на устройство несколькими способами:

- при создании нового устройства выбрать пользователя этого устройства;
- для выбранного пользователя добавить одно или несколько устройств;
- при создании нового устройства — клиента в модуле VPN.

Чтобы создать устройство для пользователя:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите **Управление организацией**  > **Пользователи**.
- 4 Выберите пользователя.
- 5 Нажмите  **Добавить устройство** и выберите один из пунктов:
 - Чтобы назначить пользователя на созданные устройства, выберите **Добавить из существующих**. Выберите устройство и нажмите **Добавить**.
 - Чтобы назначить пользователя и создать новое устройство в организации, выберите **Создать новое** и введите имя устройства и его описание, затем нажмите **Создать**.

Если было создано устройство без пользователя и задействовано в модуле VPN в качестве клиента, то назначить пользователя на такое устройство нельзя. Удалите клиент из модуля VPN и назначьте пользователя на его устройство.

Чтобы назначить пользователя на созданное устройство, которое не задействовано в модуле:

- 1 Выберите **Управление организацией**  > **Устройства**.
- 2 Выберите устройство и на панели справа нажмите .
- 3 В поле **Пользователь устройства** выберите пользователя и нажмите **Сохранить**.

Изменение имени устройства

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.

- 3 Выберите **Управление организацией**  > **Устройства**. Будет отображен список всех устройств организации.
- 4 Выберите устройство и на панели справа нажмите .
- 5 В поле **Имя устройства** укажите новое имя и нажмите **Сохранить**.

Просмотр и удаление устройств организации

Для каждого устройства вы можете просмотреть, в каком модуле задействовано устройство. Если устройство выполняет важные функции в модулях, то ему назначается уровень важности — высокий или средний. Устройства с высоким уровнем важности нельзя удалить из системы

управления в разделе **Управление организацией**  > **Устройства**, так как удаление может привести к нарушению работы сети организации. Их следует удалять сначала из модуля VPN. Устройства со средним уровнем важности можно сразу удалить в этом разделе, но не рекомендуется.

Устройства, у которых отсутствует уровень важности функций, вы можете удалить из системы управления в разделе **Управление организацией**  > **Устройства**.

При удалении устройства из модуля VPN или в разделе **Управление организацией**  > **Устройства** убедитесь, что устройство не используется в модуле РММ или NVS. Удаление устройства может повлиять на работоспособность политик безопасности и правил мониторинга.

Таблица 2. Важные для работоспособности сети функции устройств в модуле VPN

Важность функций	Название функции в модуле VPN	Устройство в защищенной сети
 Высокая	Центр управления (Control Center)	Клиент
	Шлюз в доверенную сеть	Координатор
	Совместный доступ к узлу в доверенных организациях для создания связей	Координатор
	Совместный доступ к функциям узла в доверенных организациях	Координатор, клиент, ресурс
 Средняя	Туннелирование	Координатор
	Сервер соединений	Координатор
	Регистрация узлов (клиентов)	Координатор
	DNS-сервер	Координатор, клиент, ресурс
	Центр управления политиками безопасности в сети ViPNet VPN	Клиент
	Сервер мониторинга в модуле VPN	Клиент

Важность функций	Название функции в модуле VPN	Устройство в защищенной сети
Функции устройства, которые не влияют на работоспособность защищенной сети организации	Сервер групповых чатов Conserver	Клиент
	Сервер push-уведомлений CPNS	Клиент
	Транспортный сервер Connect Hub	Клиент
	Сервер хранения файлов Connect File Exchange	Клиент
	Защищенный интернет-шлюз	Координатор
	ViPNet CSS Connect для различных платформ	Клиент
	Кластер (Failover)	Координатор
	Совместный доступ к объекту в доверенных организациях для создания связей	Клиент, ресурс, ViPNet xFirewall, ViPNet РУКС, ViPNet КУКС, ViPNet РУКС VA, ViPNet КУКС VA, ViPNet РУКС Лайт, ViPNet QCL Server Academic Edition, ViPNet QCL Client Academic Edition, ViPNet КУКС Лайт, ViPNet CSS Connect HW
	Инспекция SSL/TLS-трафика	Координатор, ViPNet xFirewall
	IPF IG	Координатор (ViPNet Coordinator IG 5)
	Modbus Gateway	Координатор (ViPNet Coordinator IG 5)
	IEC101-IEC104 Converter	Координатор (ViPNet Coordinator IG 5)
	SSL	Координатор (ViPNet xFirewall)
	Обновление базы вредоносного ПО	Координатор (ViPNet Coordinator HW 5)
	Обновление базы URL-категорий	Координатор (ViPNet Coordinator HW 5)
	SSL-инспекции	Координатор (ViPNet Coordinator HW 5)
	Подключение СКЗИ-потребителей	Координатор (ViPNet КУКС Лайт)

Чтобы просмотреть список всех устройств в организации:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.

- 3 Выберите **Управление организацией**  > **Устройства**. Будет отображен список всех устройств организации.

В столбце **Модуль** отображается, в каких модулях задействовано устройство. Значок  показывает, что устройство используется в модуле VPN.

В столбце **Важность для сети** отображено, выполняет ли устройство важные функции в каком-либо модуле.

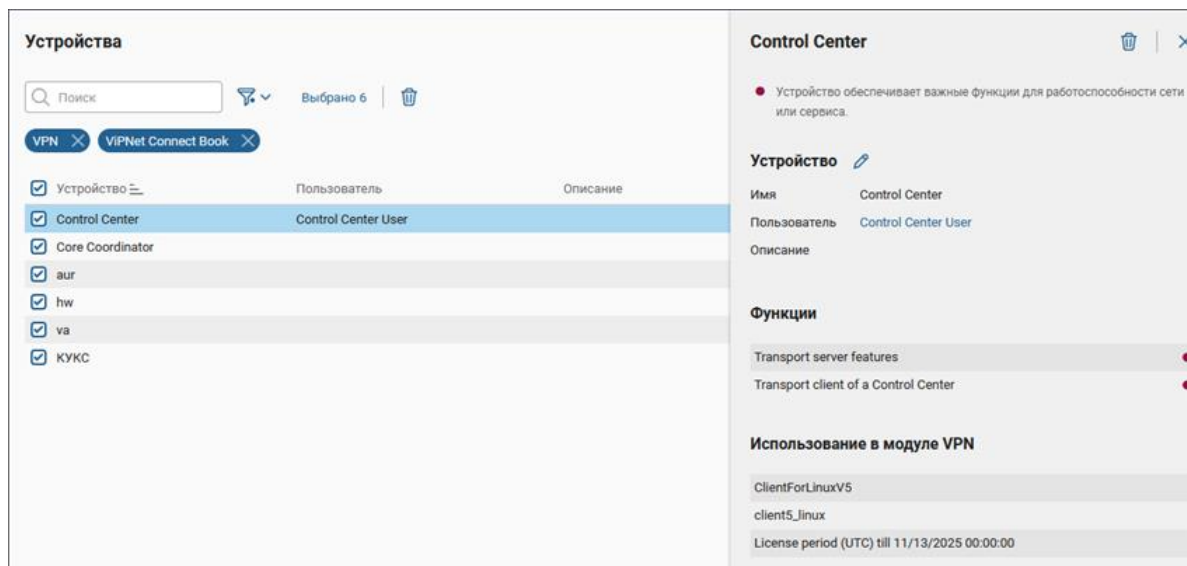


Рисунок 29. Просмотр всех устройств в организации

- 4 В меню  в группе **Использование в модуле** выберите:
-  **ViPNet VPN** — чтобы просмотреть устройства, которые задействованы в модуле VPN;
 - **Нераспределенное устройство** — чтобы найти удаленные из модулей и не используемые в модулях устройства.

ИСПОЛЬЗОВАНИЕ В МОДУЛЕ

☐ Нераспределенное устройство

☐  VPN

ПРИНАДЛЕЖНОСТЬ ПОЛЬЗОВАТЕЛЮ

☒ Все

☐ Без пользователя

☐ С пользователем

ВАЖНОСТЬ ДЛЯ СЕТИ

☒ Все

☐ Не влияют на работу сети

☐  Средняя

☐  Высокая

Рисунок 30. Настройка отображения устройств

- 5 В меню  в группе **Принадлежность пользователю** выберите:

- **С пользователем** — чтобы найти в модуле VPN-клиенты;
 - **Без пользователя** — чтобы найти в модуле VPN-координаторы, ресурсы и межсетевые экраны ViPNet xFirewall.
- 6 Чтобы просмотреть устройства, выполняющие важные функции в защищенной сети, в меню  в группе **Важность для сети** выберите **Средняя** или **Высокая**.

Удаление устройств

Вы можете удалить устройство на двух уровнях:

- из системы управления — устройство удаляется из всех функциональных модулей;
- только из функционального модуля.

Вы можете удалить устройство из системы управления, если оно не выполняет важные для сети функции. Если устройство выполняет важные функции в модулях, назначьте его функции на другое устройство. Например, при выполнении устройством функций DNS-сервера, в модуле VPN в настройках профиля DNS выберите другое устройство в качестве DNS-сервера.

При замене шлюзового координатора со старого снимается признак выполнения функции шлюзового координатора, когда он получит обновление справочников и ключей. Если шлюзовой координатор вышел из строя и не может принять обновление справочников и ключей, удалите его из модуля VPN, чтобы снять с него признак выполнения важных функций в защищенной сети.

На действующем шлюзовом координаторе нельзя отключить функцию VPN-шлюз, сначала замените его на новый шлюзовой координатор.

Чтобы удалить устройства из системы управления:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите **Управление организацией**  > **Устройства**.
- 4 Выберите устройства, нажмите  и подтвердите удаление.

7

Управление защищенной сетью

Порядок создания сети организации	108
Создание центра управления и его координатора	109
Инициализация ключевого центра организации	111
Создание защищенных узлов	114
Настройка шлюзов безопасности	129
Настройка клиентов	155
Управление связями	171
Дистрибутивы ключей	176
Назначение прикладного ПО ViPNet	181
Мастер-ключи	186
Взаимодействие между организациями и защищенными сетями	203
Отправка обновлений на узлы	226
Компрометация ключей	235

Порядок создания сети организации

Действие

- ☐ Войдите в ViPNet Prime как владелец организации и (или) администратор организации
- ☐ Убедитесь, что организации выданы лицензии на продукты и их функции
- ☐ Выберите организацию или подразделение
- ☐ Создайте пользователей
- ☐ Инициализируйте ключевой центр организации
- ☐ Создайте координаторы
- ☐ Создайте клиенты
- ☐ Создайте устройства, на которых не требуется или невозможно установить ViPNet Client, но которые должны быть доступны в сети организации. См. [Создание ресурсов](#)
- ☐ Настройте параметры для доступа клиентов и ресурсов к координаторам
- ☐ Создайте связи между объектами сети ViPNet. Для удобства создания связей, объедините пользователей или узлы в группы
- ☐ Чтобы клиенты отправляли запросы на разрешение доменных имен заданным защищенным DNS-серверам, [создайте профили DNS](#)
- ☐ Назначьте прикладное ПО ViPNet на клиенты
- ☐ Задайте пароль администратора для узлов
- ☐ Создайте дистрибутивы ключей для узлов
- ☐ На компьютере ViPNet Prime установите ViPNet Client 5 for Linux и дистрибутив ключей [центра управления](#).

Разверните шлюзы безопасности, на мобильные устройства и компьютеры пользователей установите ViPNet Client. Установите дистрибутивы ключей на узлах.

См. документацию на ViPNet Client

Создание центра управления и его координатора

Защищенная сеть содержит два обязательных узла:

- [центр управления](#);
- [координатор, за которым зарегистрирован узел центра управления](#).

На компьютер с ViPNet Prime администратор устанавливает ViPNet Client 5 for Linux. Это обеспечивает передачу и защиту трафика между центром управления и управляемыми узлами.

При установке ViPNet Prime создается автоматически устройство с именем Control Center по умолчанию. При первом входе в модуль VPN выберите это устройство в качестве центра управления и создайте для него координатор.

В качестве координатора центра управления (имя по умолчанию — 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 4 или 5 исполнений KB100 и выше.

Выбор поколения для узла центра управления влияет на выбор алгоритма шифрования межсетевого взаимодействия:

- Если центр управления — клиент поколения ViPNet 5 (дистрибутив ключей *.ds5), вы можете создавать межсетевое взаимодействие с шифрованием по ГОСТ 28147-89 или ГОСТ 34.12-2018 «Магма» и «Кузнечик».
- Если центр управления — клиент поколения ViPNet 4 (дистрибутив ключей *.dst), вы можете создавать межсетевое взаимодействие только с шифрованием по ГОСТ 28147-89.

Для шифрования трафика по алгоритмам ГОСТ 34.12-2018 «Магма» и «Кузнечик» между узлами внутри одной сети или при взаимодействии нескольких защищенных сетей под управлением ViPNet Prime выберите:

- в качестве узлов управления — центра управления Control Center и его координатора — [узлы поколения ViPNet 5](#);
- [создайте организацию с мастер-ключами ключей обмена на алгоритмах ГОСТ 34.12-2018 «Магма» и «Кузнечик»](#).

Если на узле центра управления используется лицензия «Client for Linux v.5» (дистрибутив ключей *.ds5), с узлами на *.dst пропадет связность в защищенной сети.

Если в организации должны присутствовать узлы поколения ViPNet 4 (такие как ViPNet xFirewall, Coordinator HW 4 или ViPNet Client 5 с дистрибутивом ключей *.dst):

- для узла центра управления используйте лицензию «Client for Linux» (дистрибутив ключей *.dst);
- при инициализации организации для мастер-ключей обмена выберите ГОСТ 28147-89 для совместимости.

При первом запуске модуля VPN:

- 1 Распределите лицензии в организацию Core Network на Linux-клиент и координатор. Для координатора [распределите лицензию на функции VPN-шлюза](#).
- 2 Войдите в ViPNet Prime как владелец организации и администратор организации.
- 3 Выберите **ViPNet VPN** .
- 4 Нажмите **Создать узлы управления**.
- 5 На шаге 1 выберите устройство центра управления и лицензию для него.
- 6 На шаге 2 создайте координатор центра управления:
 - 6.1 Введите имя координатора.
 - 6.2 Выберите лицензию.
- 7 Создайте мастер-ключи. Подробнее см. [Инициализация ключевого центра организации](#).
- 8 Для координатора центра управления [задайте IP-адрес и другие параметры доступа](#).
- 9 На узле центра управления установите ViPNet Client и дистрибутив ключей.
- 10 Разверните координатор центра управления и установите на нем дистрибутив ключей.

Инициализация ключевого центра организации

При инициализации ключевого центра ViPNet Prime всегда создаются мастер-ключи сети по ГОСТ 28147-89. Они используются для взаимодействия между узлами с *.dst.

При инициализации ключевого центра организации создаются мастер-ключи для взаимодействия между узлами с *.ds5 и другими узлами (с *.dst и *.ds5). От выбора алгоритма мастер-ключей организации будет зависеть, смогут ли взаимодействовать узлы с *.dst и *.ds5 между собой.

При взаимодействии между узлами центра управления и организаций, находящихся под управлением ViPNet Prime, используются разные мастер-ключи в зависимости от поколения узлов:

- Если узлы центра управления на *.ds5, в вашей организации нет узлов с *.dst, связь с узлами в другой организации на *.dst не требуется, при инициализации организации выберите алгоритм ГОСТ 34.12-2018.
- Если в сети требуется взаимодействие узлов с *.dst и *.ds5, при инициализации организации выберите алгоритм ГОСТ 28147-89.



Внимание! Для поддержки шифрования на алгоритмах ГОСТ 34.12-2018 «Магма» и «Кузнечик» в защищенной сети организации требуются [узлы поколения ViPNet 5](#).

Инициализация ключевого центра организации

- 1 Войдите в ViPNet Prime как владелец организации.
- 2 Выберите **ViPNet VPN** .
- 3 [Выберите организацию](#).
- 4 Нажмите **Создать мастер-ключи**.
- 5 Укажите сроки действия мастер-ключей.
- 6 Выберите алгоритм мастер-ключа ключей защиты обновлений: **Магма, Кузнечик**.

О поддержке алгоритмов шифрования «Магма» или «Кузнечик» смотрите в документации поддерживаемых продуктов.

- 7 Выберите алгоритм мастер-ключей обмена:
 - **ГОСТ 28147-89** — в организации с узлами [поколения ViPNet 4](#) (или поколения ViPNet 4 и ViPNet 5).
 - **Магма или Кузнечик** — в организации с узлами только [поколения ViPNet 5](#).

При инициализации организации Core Network вы задаете алгоритм только для двух мастер-ключей: мастер-ключа ключей защиты обновлений и мастер-ключа ключей обмена.

При инициализации любой другой организации вы задаете алгоритм:

- мастер-ключа ключей защиты обновлений,
- мастер-ключа ключей обмена,
- мастер-ключа ключей обмена для технической связи,
- мастер-ключа ключей обмена между организациями и поставщиком услуг.

После инициализации организации вы не можете изменить алгоритмы мастер-ключей.

8 Нажмите Сохранить.

Инициализация ключевого центра

Для завершения инициализации организации укажите сроки действия мастер-ключей и алгоритмы ключей.

Мастер-ключ ключей защиты обновлений

Срок действия: 06.05.2023 | Алгоритм: Магма

Мастер-ключ ключей обмена

Срок действия: 06.05.2023 | Алгоритм: ГОСТ 28147-89

Мастер-ключ ключей обмена для технической связи

Срок действия: 06.05.2023 | Алгоритм: ГОСТ 28147-89

Мастер-ключ ключей обмена между узлами организации и поставщиком услуг

Срок действия: 06.05.2023 | Алгоритм: ГОСТ 28147-89

Сохранить | Отмена

Рисунок 31. Инициализация организации, кроме Core Network

Переключение координаторов поколения ViPNet 5 на работу с новыми протоколами

При инициализации организации создаются мастер-ключи для организации. Мастер-ключи формируют ключи для шифрования трафика между узлами. На стороне узлов зашифровывает и расшифровывает данные драйвер протокола IPlir.

Для взаимодействия узлов с использованием новых алгоритмов шифрования требуется, чтобы все узлы в организации перешли с протокола IPlir4 на IPlir6. Для этого выполните одно из действий:

- Дождитесь, когда координаторы поколения ViPNet 5 [сообщат о своей конфигурации в ViPNet Prime](#) и автоматически включится использование IP1r6. В этом случае в журнале транспортных конвертов будет принят конверт с обновлением **Индивидуальная конфигурация**.
- Принудительно переключите все координаторы сети на использование новых алгоритмов (подходит для сетей только с [узлами поколения ViPNet 5](#)).

Если защищенная сеть содержит узлы только поколения ViPNet 5, такие как ViPNet Coordinator HW 5.3.1 и выше, ViPNet Coordinator IG 5.2 и выше, принудительно включите признак работы по протоколу IP1r6 для всех координаторов сети (по умолчанию отключен):

1 Остановите ViPNet Prime:

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

2 Откройте файл /usr/share/infotecs/vpn-ms/config.env для изменения.

3 Добавьте в файл параметр NSMS_DefaultIL6SEnabled со значением true.

```
NSMS_DefaultIL6SEnabled=true
```

4 Запустите ViPNet Prime:

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

Создание защищенных узлов

Вы можете создать устройства в модуле VPN двумя способами:

- Сначала [создать устройство](#) в разделе **Управление организацией**  > **Устройства** и затем в модуле VPN выбрать его в качестве координатора, межсетевого экрана ViPNet xFirewall, клиента или ресурса.
- Создать сразу устройство в модуле VPN: [координатор](#), [межсетевой экран ViPNet xFirewall](#), [клиент](#) или ресурс. В этом случае устройство отобразится в списке устройств организации в разделе **Управление организацией**  > **Устройства** со значком функций в модуле VPN . Этот способ описан далее в документе при создании устройств в модуле VPN.

В результате создания устройства в модуле VPN списывается базовая лицензия на тип устройства.

Создание координатора

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 [Выберите организацию и подразделение](#).
- 3 Выберите **ViPNet VPN**  > **Координаторы**.
- 4 Нажмите  **Добавить**.
- 5 На шаге 1 нажмите  **Создать**.
- 6 На шаге 2 укажите:
 - имя устройства;
 - лицензию.



Примечание. Если в сети используются ключевые блокноты КУБИТ вы не сможете выбрать лицензию для ViPNet Coordinator KB 4 и ViPNet L2-10G, так как они поддерживают работу только с ключевыми блокнотами ДСДР.

- 7 Нажмите **Добавить**.
- 8 [Включите функцию VPN-шлюз](#), если координатор должен выполнять VPN-функции.
- 9 Для шлюзов безопасности поколения ViPNet 4 [задайте пароль администратора узла](#). Без пароля администратора вы не сможете выпустить дистрибутив ключей.
- 10 Если в защищенной сети используются ViPNet Coordinator KB или ViPNet L2, [зарегистрируйте серию ключевых блокнотов](#). Иначе вы не сможете создать дистрибутив ключей для узлов.



Примечание. Для каждого координатора автоматически создается группа, в которую будут автоматически добавляться узлы, зарегистрированные на координаторе. Такие группы находятся в разделе **Автоматические группы** и помогают быстро создавать связи со всеми узлами одного координатора.

На панели справа в разделе **Об узле** вы можете посмотреть идентификатор узла VPN ID, по которому можете найти узел в списках узлов в модуле VPN.

Создание клиента

Вы можете создать клиента:

- С пользователем — для использования на клиенте приложений ViPNet CSS Connect, ViPNet Деловая Почта и для работы серверного ПО ViPNet CSS версии 3 (CPNS, FileExchange, Connect Hub).
- Без пользователя — для использования на клиенте серверного ПО ViPNet CSS версии 2 (CPNS, ConServer) или если на клиенте не используются приложения ViPNet CSS Connect и ViPNet Деловая Почта.

Связи между пользователями позволяют общаться пользователям в приложениях ViPNet CSS Connect и ViPNet Деловая Почта.

Чтобы создать клиент:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите **ViPNet VPN**  > **Клиенты**.
- 4 Нажмите  **Добавить**.
- 5 Нажмите  **Создать**, если отсутствуют устройства из раздела **Управление организацией**.
- 6 Введите имя нового устройства и описание.
- 7 Выберите, куда добавить устройство:
 - **В организацию** или **В подразделение** — чтобы создать устройства с серверным ПО ViPNet без пользователя.
 - **Пользователю** — чтобы выбрать пользователя устройства.

По умолчанию клиент добавляется в корень организации без привязки к пользователю.



Внимание! После добавления клиента в защищенную сеть на нем нельзя сменить пользователя.

- 8 В группе **Параметры** в списке **Координатор** выберите VPN-сервер для регистрации клиента. Вы не сможете сменить координатор для устройства после создания дистрибутива ключей.



Примечание. Регистрируйте на ViPNet Coordinator IG 5:

- не более 100 клиентов — на Coordinator IG1000, Coordinator IG-VA1000,
- не более 10 клиентов — на Coordinator IG100.

- 9 Чтобы передавать VPN-трафик от клиента к другим узлам защищенной сети через координатор клиента, выберите **Передавать VPN-трафик через сервер соединений**.

Трафик клиента будет направлен через координатор, на котором он зарегистрирован, даже если некоторые узлы доступны напрямую. Если настройка включена, оптимизация маршрутов не будет использоваться. Это повысит надежность, но может уменьшить скорость обмена данными.

Если сервер соединений клиента — ViPNet Coordinator KB 4 или ViPNet Coordinator KB 5 с поддержкой ГОСТ 28147-89, то для работы клиента выберите **Передавать VPN-трафик через сервер соединений**. Иначе ViPNet Coordinator KB отбросит трафик не от своего клиента, если после оптимизации маршрута трафик пойдет не через сервер соединений клиента.

- 10 В списке **Тип узла** выберите ОС, для которой предназначено ПО ViPNet Client.

- 11 Нажмите **Добавить**.

- 12 Чтобы настроить клиент сразу, нажмите **Настройки клиента**:

12.1 Если для клиента доступны разные лицензии, выберите нужную в списке **Лицензия**.

12.2 Выберите группу серверов соединений. Подробнее см. [Группы серверов соединений](#).

12.3 Выберите **Передавать VPN-трафик через сервер соединений**, чтобы маршрут VPN-трафика не оптимизировался и шел всегда через сервер соединений.

12.4 Чтобы клиенты отправляли запросы на разрешение имен на защищенные DNS-серверы, [добавьте клиенты в профиль DNS](#).

12.5 Если необходимо, включите функции, добавьте клиент в группу, задайте расширенные настройки.

- 13 [Задайте связи с другими объектами](#), например ресурсами, которые должны быть доступны для клиента.

- 14 Создайте для нового клиента [дистрибутив ключей](#) и передайте его пользователю для установки на устройстве.

Для узла Client for Aurora поколения ViPNet 4 не доступны никакие функции и прикладное ПО, кроме ViPNet Connect.

На панели справа в разделе **Об узле** вы можете посмотреть идентификатор узла VPN ID, по которому можете найти узел в списках узлов в модуле VPN.

Создание ViPNet xFirewall

Для работы ViPNet xFirewall в защищенной сети зарегистрируйте его на координаторе — устройстве с функциями VPN-шлюза.

Чтобы создать устройство ViPNet xFirewall:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Определите координатор, на котором будет зарегистрирован сетевой узел ViPNet xFirewall. Это может быть координатор из своей организации (или подразделения) или координатор доверенной организации, [предоставленный в совместный доступ](#).
- 4 Выберите **ViPNet VPN**  > **Другие узлы**.
- 5 Нажмите  **Добавить**.
- 6 На шаге 1 нажмите  **Создать**.
- 7 На шаге 2 укажите:
 - имя устройства и его описание;
 - лицензию;
 - координатор, на котором будет зарегистрирован новый узел.
- 8 Нажмите **Добавить**.
- 9 [Задайте пароль администратора узла](#). Без пароля администратора вы не сможете выпустить дистрибутив ключей.

Для включения IPS, анализа трафика SSL/TLS и других функций [разрешите дополнительные функции](#).

Создание узла ViPNet CSS Connect HW

Аппаратный телефон ViPNet CSS Connect HW работает как СКЗИ-потребитель квантовой сети.

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 [Распределите лицензию на узел](#) или убедитесь, что лицензия распределена.
- 4 Выберите **ViPNet VPN**  > **Клиенты**.
- 5 Нажмите  **Добавить**.
- 6 На шаге 1 нажмите  **Создать**.
- 7 На шаге 2 укажите:

- имя устройства;
- описание;
- организацию, подразделение или пользователя.

8 На шаге 3 укажите:

- координатор;
- платформу клиента CSS Connect HW.

9 Нажмите **Добавить**.

10 [Задайте пароль администратора узла](#).

11 [Создайте дистрибутив ключей](#).

При необходимости [обновите ПО](#) на узле [ViPNet CSS Connect HW](#).

Создание узлов L2

ViPNet L2 — универсальный канальный шифратор уровня L2 модели OSI топологии «точка-точка». Может использовать один из источников ключей в зависимости от того, какая лицензия на него распределена:

- L2-10G — использует ключевые блокноты ДСДР;
- L2Q-10G — использует ключи ViPNet QTS.

Особенности ViPNet L2Q

- Узел ViPNet L2Q относится к поколению ViPNet 4.
- Вы можете создать только связь «точка-точка» между двумя L2Q-10G.
- Вы можете разрешить создание связи с узлом ViPNet L2Q из доверенной организации и затем создавать связи с этим узлом при взаимодействии между организациями только внутри одной защищенной сети.
- Нельзя создать связь с узлами из доверенной сети.
- Узел не поддерживает VPN-функции.
- Нельзя сменить лицензию ViPNet L2Q на другой тип узла. При этом вы можете изменить тип узла на ViPNet L2Q. Об особенностях смены типа узла см. в разделе [Смена типа и лицензии координатора](#).

Особенности ViPNet L2-10G

- Вы можете создать связь только по принципу «точка-точка» между узлами ViPNet L2-10G.
- Связь между узлом ViPNet L2-10G и узлами ViPNet L2-10G, ViPNet Coordinator KB 4 и ViPNet Coordinator KB 5 строится на ключах ДСДР, с остальными узлами — на ключах обмена из дистрибутива ключей *.dst.

- Узел не поддерживает VPN-функции.
- Вы можете разрешить создание связи с узлом ViPNet L2-10G из доверенной организации только внутри одной защищенной сети и затем создавать связи с этим узлом при взаимодействии между организациями.
- Нельзя изменять лицензию ViPNet L2-10G на другой тип или другое поколение. При этом вы можете изменить другой тип узла на ViPNet L2-10G. Об особенностях смены типа узла см. в разделе [Смена типа и лицензии координатора](#).
- Нельзя добавить узел в группу.
- Нельзя создать узел ViPNet L2-10G, если указан тип ключевых блокнотов КУБИТ. Так как ViPNet L2 — узел поколения ViPNet 4 и не поддерживает ключи КУБИТ, предназначенные для поколения ViPNet 5.

Порядок действий

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 [Создайте координатор](#).
- 4 Для доступа администратора к режиму настройки (вход в `enable`) [задайте пароль администратора узла](#). Без пароля администратора вы не сможете выпустить дистрибутив ключей.
- 5 [Создайте связи](#).
- 6 Для ViPNet L2-10G [зарегистрируйте ключи ДСДР](#). Иначе вы не сможете создать дистрибутив ключей для узла.
- 7 [Создайте дистрибутив ключей](#).

Защищенный смартфон ViPNet HardPhone

Для работы ViPNet HardPhone при инициализации устройства необходимо установить дистрибутив ключей. Начиная с ViPNet Prime версии 1.9.12, изменился порядок лицензирования ViPNet HardPhone. Ранее для использования ViPNet HardPhone требовалась только лицензия Client for Android или Client for Android v.5. Теперь, кроме этого, вам потребуется включить функцию **Защищенный смартфон HardPhone**. Лицензия на использование этой функции приобретается отдельно и не входит в пакет лицензий. Без этой лицензии вы не сможете инициализировать устройство.

Функция **Защищенный смартфон HardPhone** доступна только для узлов Client for Android. Если вы по ошибке назначили функцию на другое устройство Client for Android, которое не является HardPhone, эта функция назначится на узел в ViPNet Prime, но не применится на устройстве и не будет использоваться. При этом в ViPNet Prime предупреждение не отобразится.

Чтобы создать узел ViPNet HardPhone в ViPNet Prime, [создайте клиент](#).

Чтобы включить функцию **Защищенный смартфон HardPhone**:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Распределите лицензию HardPhone в организацию.
- 3 Выберите организацию и подразделение.
- 4 Выберите ViPNet VPN  > Клиенты.
- 5 Выберите клиент и нажмите .
- 6 Выберите **Общие**.
- 7 Включите **Защищенный смартфон HardPhone**.
- 8 Выберите лицензию и нажмите **Применить**.
- 9 Чтобы изменить выбранную лицензию, нажмите , выберите новую лицензию и нажмите **Применить**.
- 10 Нажмите **Сохранить**.

Дождитесь отправки на узел обновлений справочников и ключей или отправьте их вручную.

Чтобы включить функцию **Защищенный смартфон HardPhone** на нескольких узлах:

- 1 Выберите клиенты.
- 2 На панели сверху нажмите  > **Защищенный смартфон HardPhone** > **Включить**.

Операция проходит в фоновом режиме. После завершения появится оповещение, в котором вы можете нажать **Подробнее**, чтобы ознакомиться со списком узлов, на которых включены функции и распределены лицензии. Вы можете найти важные узлы с помощью поиска по идентификатору VPN ID. Чтобы скачать отчет с информацией о назначении функции на узлы, на панели сверху окна с отчетом нажмите **Скачать файлом**. Отчет сохранится в файл `change_report_DD-MM-YYYY_HH-MM-SS.csv`.

Если вы закрыли вкладку браузера, вы можете узнать результат включения функции на устройствах в **Журнале событий**, расположенном в **Главной консоли**.

Если на узле уже установлен дистрибутив ключей, дождитесь отправки обновлений справочников и ключей.

В результате в свойствах клиента на панели справа на вкладке **Общие** в разделе **Особенности клиента** отобразится название функции.

Чтобы отключить функцию **Защищенный смартфон HardPhone** на нескольких узлах:

- 1 Выберите клиенты.
- 2 На панели сверху нажмите  > **Защищенный смартфон HardPhone** > **Отключить**.
- 3 Подтвердите операцию.

Создание узлов квантовой сети

Оборудование ViPNet QTS, ViPNet QTS Lite или ViPNet QCL разворачивается на базе [защищенной сети](#).

В одной защищенной сети вы можете развернуть одну сеть квантового распределения ключей (далее — квантовая сеть). Чтобы организовать взаимодействие между двумя квантовыми сетями, создайте межсетевое взаимодействие. Межсетевое взаимодействие будет работать между защищенными сетями, квантовые и квантовозащищенные ключи выработать не получится.

Квантовая сеть ViPNet QTS состоит из узлов:

- ViPNet КУКС — клиентский узел квантовой сети с возможностью создания только одной оптической связи.
- ViPNet РУКС — распределительный узел квантовой сети с возможностью создания двух оптических связей.
- ViPNet МУКС — магистральный узел квантовой сети.
- ViPNet QSS Switch — оптический коммутатор.

Квантовая сеть ViPNet QTS Lite состоит из узлов:

- ViPNet КУКС Лайт.
- ViPNet РУКС Лайт.
- ViPNet QSS Switch.

Виртуальная сеть квантового распределения ключей состоит из узлов:

- ViPNet РУКС VA.
- ViPNet КУКС VA.

Квантовая сеть ViPNet QCL состоит из учебных узлов:

- ViPNet QCL Client academic edition — клиентский узел квантовой сети.
- ViPNet QCL Server academic edition — центральный узел квантовой сети.

Подробнее о квантовых сетях см. «ViPNet QTS. Руководство по эксплуатации», «ViPNet QTS Lite. Руководство по эксплуатации», «ViPNet РУКС VA. Руководство по эксплуатации», «ViPNet QCL. Руководство по эксплуатации».

ViPNet Prime версии 1.9.14 поддерживает узлы РУКС, КУКС, РУКС VA, КУКС VA, РУКС Лайт, КУКС Лайт, Server academic edition, Client academic edition и СКЗИ-потребителей квантовозащищённых ключей — CSS Connect HW, L2Q-10G.

Особенности

- В ViPNet QTS Lite и одной защищенной сети может быть только один узел ViPNet РУКС Лайт.
- В ViPNet QTS Lite нельзя добавить узел РУКС или КУКС.

- В ViPNet QTS может быть несколько узлов ViPNet КУКС и ViPNet РУКС, между которыми автоматически создается полносвязная топология.
- В виртуальной сети квантового распределения ключей может быть несколько узлов ViPNet РУКС VA и ViPNet КУКС VA.
- Узлы ViPNet CSS Connect HW, ViPNet L2Q-10G получают и используют квантовозащищенные ключи. Они являются СКЗИ-потребителями.
- ViPNet QTS может включать не более 1000 узлов квантовой сети, между которыми создана полносвязная топология.
- В одной защищенной сети может быть только один узел ViPNet QCL Server Academic Edition.

Общий порядок действий

- 1 Администратор ViPNet Prime создает узлы для каждого устройства квантовой сети и связи между узлами.
- 2 Администратор ViPNet Prime создает дистрибутивы ключей защищенной сети и пароли к ним для устройств квантовой сети.
- 3 Администратор защищенной сети развертывает защищенную сеть на узлах квантовой сети, устанавливает дистрибутивы ключей защищенной сети.
- 4 Администратор QTS настраивает управляющий узел квантовой сети и создаёт дистрибутивы ключей квантовой сети для остальных узлов.
- 5 Администратор QTS устанавливает дистрибутивы ключей квантовой сети на всех узлах.
- 6 Администратор QTS настраивает оптические связи между узлами.

Создание узлов

Узлы ViPNet QTS, ViPNet QTS Lite и виртуальной сети квантового распределения ключей относятся к поколению ViPNet 4 и работают на ключах из дистрибутива *.dst.

В ViPNet Prime автоматически создаются связи:

- между узлами ViPNet QTS:
 - всеми узлами РУКС в одной сети;
 - всеми узлами КУКС в одной сети;
 - каждым узлом КУКС и каждым узлом РУКС в одной сети;
- между узлами ViPNet QTS Lite:
 - узлом РУКС Лайт и каждым узлом КУКС Лайт в одной сети;
 - всеми узлами КУКС Лайт в одной сети;
- между узлами виртуальной сети квантового распределения ключей:
 - всеми узлами РУКС VA в одной сети;

- всеми узлами КУКС VA в одной сети;
- каждым узлом КУКС VA и каждым узлом РУКС VA в одной сети;
- между узлами ViPNet QCL:
 - узлом Server Academic Edition (QCL) и всеми узлами Client Academic Edition (QCL) в одной сети;
 - между всеми узлами Client Academic Edition (QCL) в одной сети.

Чтобы создать узел квантовой сети:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 [Распределите лицензию на узел](#) или убедитесь, что лицензия распределена.
- 4 Выберите **ViPNet VPN**  > **Другие узлы**.
- 5 Нажмите  **Добавить**.
 - 5.1 На шаге 1 нажмите  **Создать**.
 - 5.2 На шаге 2 укажите:
 - имя устройства и его описание;
 - лицензию;



Примечание. В одной защищенной сети ViPNet QTS Lite может быть только один узел РУКС Лайт. Если РУКС Лайт создан, другие лицензии на РУКС Лайт не отображаются для выбора.

- координатор, на котором будет зарегистрирован новый узел.
- 5.3 Нажмите **Добавить**.
 - 6 Чтобы включить возможность подключить к узлам квантовой сети ViPNet QTS Lite СКЗИ-потребителя квантовых ключей:
 - 6.1 Выберите узел КУКС Лайт.
 - 6.2 Нажмите , перейдите на вкладку **Функции** и включите  **Подключение СКЗИ-потребителей**.
 - 6.3 Нажмите **Сохранить**.
 - 7 [Задайте пароль администратора узла](#). Без пароля администратора вы не сможете выпустить дистрибутив ключей защищенной сети.
 - 8 [Создайте и скачайте дистрибутив ключей](#).
 - 9 Передайте дистрибутив ключей администратору защищенной сети для установки на узлы.

Создание групп пользователей или узлов

Группы предназначены для объединения объектов для управления связями между ними. Группы удобно использовать при работе с большим количеством устройств или пользователей.

Группы могут быть созданы администратором вручную или автоматически. Вы можете создать группы двух видов:

- группы пользователей;
- группы узлов.

В группы узлов вы можете добавить только клиенты, координаторы и межсетевые экраны ViPNet xFirewall. Ресурсы не входят в состав групп узлов.

Клиенты или межсетевые экраны ViPNet xFirewall, которые зарегистрированы на одном координаторе, добавляются в автоматически создаваемую группу. Все узлы, в том числе новые, зарегистрированные на этом координаторе, автоматически добавляются в группу. Используйте такие группы, например, для создания связей между клиентами одного координатора и сетевыми ресурсами.

Каждая группа объектов должна иметь уникальное имя в организации. По умолчанию объекты внутри группы не связаны между собой. Вы можете установить связь сразу между всеми объектами группы.

Создание связи пользователя или устройства с группой эквивалентно созданию связей пользователя или устройства с каждым участником или устройством группы.

Чтобы создать группу пользователей или узлов:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN**  > **Группы пользователей** (или **Группы узлов**).
- 3 Нажмите  **Добавить**.
- 4 На шаге 1 введите имя группы и ее описание. Группа должна иметь уникальное название в организации (нельзя создать группу узлов и группу пользователей с одинаковым названием).
- 5 При необходимости выберите **Создавать связи между всеми пользователями группы** (или **Создавать связи между всеми узлами группы**).
- 6 На шаге 2 нажмите  **Добавить**.
- 7 В окне **Добавление в группу** выберите пользователей (или устройства) и нажмите **Добавить**. Вы можете найти узел или пользователя по идентификатору узла VPN ID.

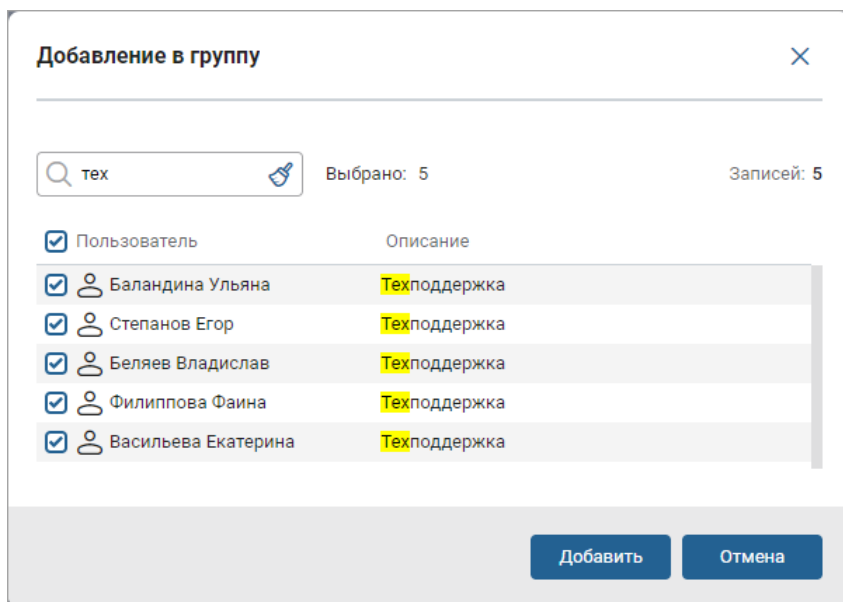


Рисунок 32. Выбор пользователей и добавление их в группу

- 8 Чтобы завершить создание группы, нажмите **Создать**.
- 9 Настройте связи группы объектов с другими сетевыми объектами организации: группами, пользователями, клиентами, сетевыми ресурсами, координаторами, межсетевыми экранами ViPNet xFirewall. См. [Создание связей между объектами организации](#).

Настройка сложности паролей пользователей и администраторов узлов

Пароль администратора сетевого узла предназначен для входа в режим администратора на узле. Вы можете задать этот пароль отдельно на каждом узле либо задать общий пароль администратора всех сетевых узлов.

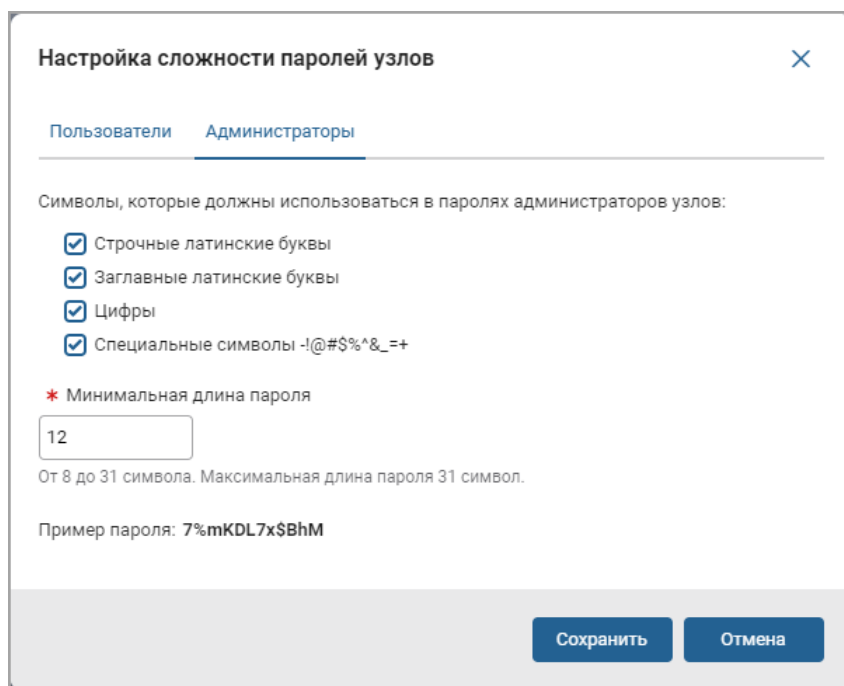
По умолчанию пароли пользователей и администраторов узлов (клиентов, координаторов и межсетевых экранов ViPNet xFirewall) состоят из 10 символов и содержат строчные и заглавные латинские буквы, цифры и специальные символы.

Настройки сложности паролей действуют для сетевых узлов с [ПО поколения ViPNet 4](#). Для сетевых узлов с [ПО поколения ViPNet 5](#) автоматически создается пароль, в котором присутствует хотя бы один символ из строчных и заглавных латинских букв, цифр, специальных символов.

Чтобы задать сложность паролей пользователей и администраторов узлов:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 [Выберите организацию и подразделение](#).
- 3 Выберите **ViPNet VPN**  > **Сервис** > **Сервисные функции**.
- 4 Выберите **Настройка сложности паролей узлов** и нажмите .

- 5 Выберите **Пользователи** или **Администраторы**.
- 6 Задайте требования к паролю (использование строчных и заглавных латинских букв, цифр, специальных символов). По умолчанию заданы требования максимальной сложности паролей.
- 7 Задайте минимальную длину пароля от 8 до 31 символа. Рекомендуемая безопасная длина пароля — 12 символов.
- 8 Нажмите **Сохранить**.



Настройка сложности паролей узлов

Пользователи Администраторы

Символы, которые должны использоваться в паролях администраторов узлов:

- ☒ Строчные латинские буквы
- ☒ Заглавные латинские буквы
- ☒ Цифры
- ☒ Специальные символы -!@#\$\$%^&_+=

* Минимальная длина пароля

12

От 8 до 31 символа. Максимальная длина пароля 31 символ.

Пример пароля: 7%mkDL7x\$BhM

Сохранить Отмена

Рисунок 33. Настройка сложности паролей узлов

Задание пароля администратора узла

Пароль администратора узла или всех узлов организации позволяет использовать возможности администратора локально на узле. Этот режим позволяет получить доступ к расширенным настройкам узла. Вход в режим администратора доступен только после ввода пароля пользователя на узле.

Вы можете задать пароль администратора для каждого узла индивидуально в свойствах объекта или задать общий пароль администратора для всех узлов организации централизованно. В обоих случаях вы можете задать 3 таких пароля, например, для нескольких администраторов.

Для новых узлов действуют пароли администратора всех узлов, которые заданы централизованно.

При удалении пароля в ViPNet Prime администратор не сможет получить доступ к расширенным настройкам.

Если пароль администратора узла не задан, вы не сможете создать дистрибутив ключей для шлюза безопасности поколения ViPNet 4, так как вы не сможете настроить его без пароля.



Внимание! Пароль администратора узла или всех узлов организации недоступен для просмотра после его создания. Если вы забыли пароль, задайте новый пароль и удалите действующий.

Чтобы задать пароль администратора для всех узлов организации:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию.
- 3 Выберите ViPNet VPN  > Сервисные функции.
- 4 Выберите Пароли администраторов всех узлов организации и нажмите .
- 5 Задайте пароль. Чтобы задать пароль автоматически, нажмите **Сгенерировать**. При генерации пароля действуют настройки сложности паролей (см. [Настройка сложности паролей пользователей и администраторов узлов](#)). Для безопасности используйте длину пароля не менее 12 символов.
- 6 Укажите срок действия пароля. По умолчанию 365 дней.
- 7 Введите описание для пароля, например имя администратора, который будет использовать этот пароль.
- 8 Чтобы удалить один из паролей, выберите строку со сроком действия пароля и нажмите .

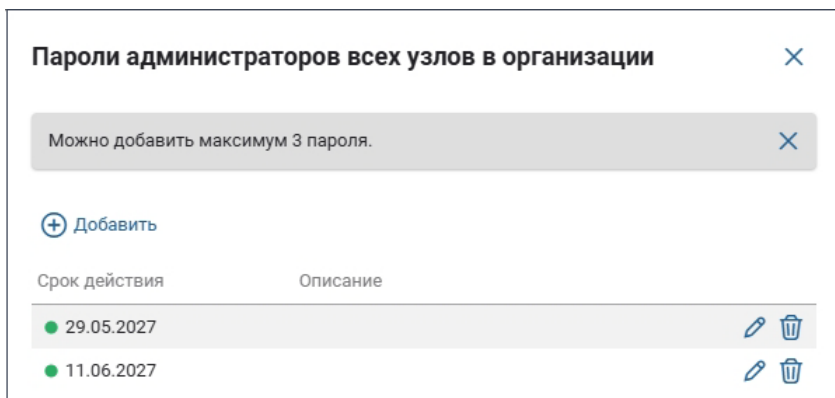


Рисунок 34. Удаление пароля администратора всех узлов

Чтобы задать пароль администраторов для узла индивидуально:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите ViPNet VPN  > Клиенты (или Координаторы, или Другие узлы).
- 4 Выберите объект.
- 5 Для устройств поколения ViPNet 4 в группе Пароли администраторов узла нажмите  **Добавить**.
- 6 Укажите пароль и срок его действия.

7 Нажмите **Добавить**.

Компрометация пароля

При компрометации пароля администратора узла или группы узлов ключи узла не считаются скомпрометированными. В этом случае достаточно сменить пароль:

- 1 Администратор или пользователь узла информирует администратора ViPNet Prime о компрометации пароля.
- 2 Администратор в ViPNet Prime удаляет скомпрометированный пароль для узла и задает новый пароль. На узел отправятся справочники и ключи с новым паролем.

При компрометации пароля пользователя смените пароль пользователя. См. документацию продукта.

Настройка шлюзов безопасности

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN**  > **Координаторы** (или в разделе **Другие узлы** выберите узел ViPNet xFirewall).
- 3 Настройте [параметры подключения шлюза безопасности к внешней сети](#).
- 4 Чтобы упростить создание связей, [создайте группу узлов](#).
- 5 [Задайте связи шлюза безопасности с другими объектами](#).
- 6 [Активируйте режим кластера](#).

Подключение к внешней сети

Чтобы устройства сети ViPNet устанавливали соединения с внешними сетями (например, интернетом), укажите параметры для доступа устройств к координаторам, а также к межсетевым экранам ViPNet xFirewall.

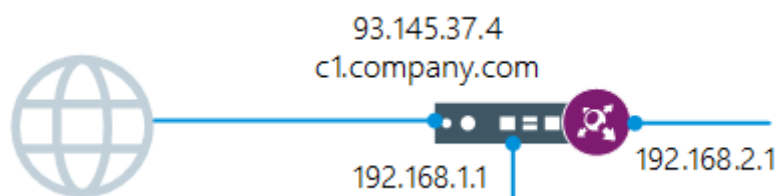


Рисунок 35. IP-адреса координатора

В сети организации, работающей на алгоритмах шифрования Магма или Кузнечик, в качестве сервера соединений вы можете назначить координатор поколения ViPNet 5. Тогда в сети будет возможна маршрутизация трафика с помощью этих координаторов, так как они поддерживают маршрутизацию трафика, зашифрованного на алгоритмах шифрования Магма или Кузнечик.

Если для координатора, который доступен напрямую из внешней сети:

- Заданы адреса — его адреса автоматически получают координаторы, которые используют его как сервер соединений. Поэтому в ViPNet Prime можно не задавать адреса координатора при выборе **Координатор доступен с использованием сервера соединений**.
- Не заданы адреса — узлы, которые используют его в качестве сервера соединений и сервера IP-адресов, не смогут подключиться к защищенной сети. На ViPNet Client 4U и Client 5 не установится дистрибутив ключей. Также если вы задавали адрес, а потом его удалили, клиенты не примут новые справочники из-за отсутствия адреса своего координатора.

Чтобы настроить подключение координатора или межсетевого экрана ViPNet xFirewall к сети:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.

- 2 Выберите **ViPNet VPN**  > **Координаторы** (или **Другие узлы**).
- 3 Выберите узел.
- 4 На панели справа нажмите .
- 5 На вкладке **Параметры подключения** выберите, как узел подключен к внешней сети (интернету):
 - **Координатор доступен напрямую** — шлюз безопасности имеет адрес из внешней сети или на внешнем маршрутизаторе заданы параметры для пропуска пакетов из внешней сети.
 - **Координатор доступен с использованием сервера соединений** — на внешнем маршрутизаторе не заданы параметры для пропуска пакетов из внешней сети:
 - Выберите сервер соединений.
 - Если требуется весь входящий и исходящий VPN-трафик направлять через сервер соединений для контроля передаваемого трафика, выберите **Передавать VPN-трафик через сервер соединений**.

В ViPNet-сетях есть механизм оптимизации маршрута передачи трафика между ViPNet-узлами. Если между узлами есть возможность установить прямой канал связи, трафик будет передаваться напрямую. Если прямой канал связи не установить, трафик будет передаваться через сервер соединений. Если выбрано **Передавать VPN-трафик через сервер соединений**, маршруты передачи трафика между узлами не будут оптимизироваться, трафик всегда будет передаваться только через его сервер соединений.

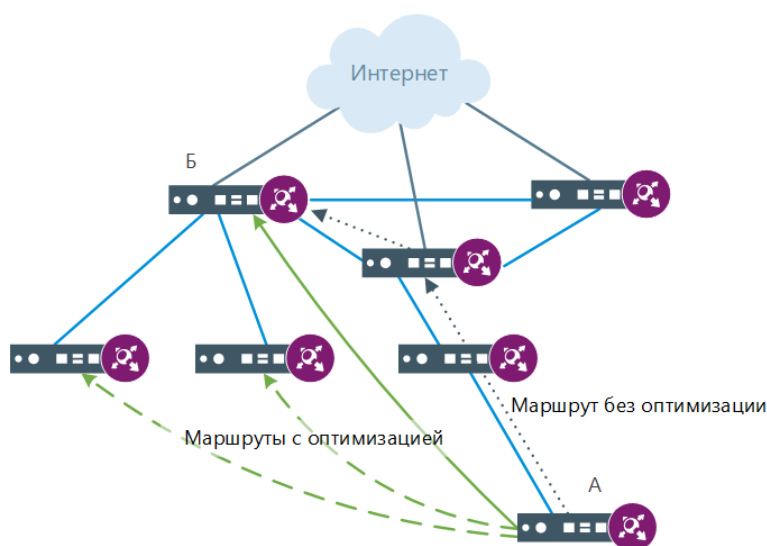


Рисунок 36. Оптимизация маршрутов

Примечание. На шлюзах безопасности для подключения к внешней сети используются режимы VPN:



- «со статической трансляцией адресов» — соответствует **Координатор доступен напрямую**;
- «с динамической трансляцией адресов» — соответствует **Координатор доступен с использованием сервера соединений**.

Если вы подключаете узлы к внешней сети через сервер соединений, у вас может образоваться цепочка серверов соединений, то есть последовательность серверов соединений, которая используется узлом для доступа к внешней сети. При создании цепочки серверов соединений необходимо, чтобы хотя бы один сервер соединений был доступен напрямую. Если вы пытаетесь создать цепочку подключений, в которой ни один сервер соединений не доступен напрямую, появится уведомление, что это запрещено.



Примечание. Чтобы изменить способ подключения координатора поколения ViPNet 4 с режима **доступен с использованием сервера соединений** на режим **доступен напрямую**, создайте связь между этим координатором и координатором, который является для него сервером соединений.

Рисунок 37. Настройка параметров координатора

6 Если Координатор доступен напрямую, в IP-адреса или доменные имена координатора введите все адреса, по которым координатор может быть доступен для других устройств организации:

- IP-адреса внешних и внутренних сетевых интерфейсов координатора;
- доменные имена координатора.

Например, для координатора с тремя сетевыми интерфейсами, изображенного на рисунке, укажите следующие адреса:

- IP-адреса 93.145.37.4, 192.168.1.1, 192.168.2.1.
- доменное имя c1.company.com.

7 Задайте другие параметры доступа узлов к координатору:

7.1 Порт TCP-туннеля (координатора). По умолчанию задан порт 80. Используется внешними узлами, если нет доступа по протоколу UDP.

7.2 UDP-порт. Значение по умолчанию 55777. Измените номер порта, если несколько координаторов подключены через один межсетевой экран. Каждый из них должен иметь собственный порт. UDP-порт возможно задать после добавления IP-адреса или DNS-имени.

Если используется внешний маршрутизатор, то укажите порт, заданный на маршрутизаторе.

При подключении через сервер соединений пакеты будут передаваться с координатора с использованием этого порта.



Внимание! Не изменяйте UDP-порт доступа для координатора центра управления Core Coordinator, если в защищенной сети узлы разных поколений: и ViPNet 4, и ViPNet 5. Иначе станет недоступно соединение между координатором и узлами поколения ViPNet 5.

Если вы уже сменили UDP-порт, установите новые дистрибутивы ключей на всех узлах защищенной сети.

Настроить TCP- и UDP-порты для доступа к координатору можно как в ViPNet Prime, так и на координаторе. Будут использоваться последние настройки, заданные на координаторе или в ViPNet Prime.

8 Нажмите **Сохранить**.

9 Если координатор подключен к внешней сети с использованием сервера соединений, [создайте связи](#) между сервером соединений и клиентами координатора.

Создание ресурсов

Координаторы выполняют функции шлюза в защищенной сети для устройств, на которых не установлено ПО ViPNet с функцией шифрования трафика на сетевом уровне. Такие устройства называются ресурсами (например, сетевые принтеры, сетевые хранилища данных). Кроме

подключения отдельных устройств вы можете подключить к защищенной сети в качестве ресурса подсеть с диапазоном IP-адресов.

Вы можете добавить 65535 ресурсов в одну организацию в разделе **ViPNet VPN > Ресурсы**. Однако для стабильной работы сети в организацию рекомендуется добавлять не более 1000 ресурсов. При этом один ресурс может содержать до 1000 записей, в том числе записей с исключениями. Количество IP-адресов в диапазоне не ограничено. Общее количество туннелируемых IP-адресов в связях клиента не должно превышать 3000, иначе вы не сможете установить дистрибутив ключей на узле ViPNet Client 4U или ViPNet Client 5.

Для создания ресурса в организации:

- [создайте координатор в организации](#);
- расположите координатор и его ресурсы в одной маршрутизируемой сети.

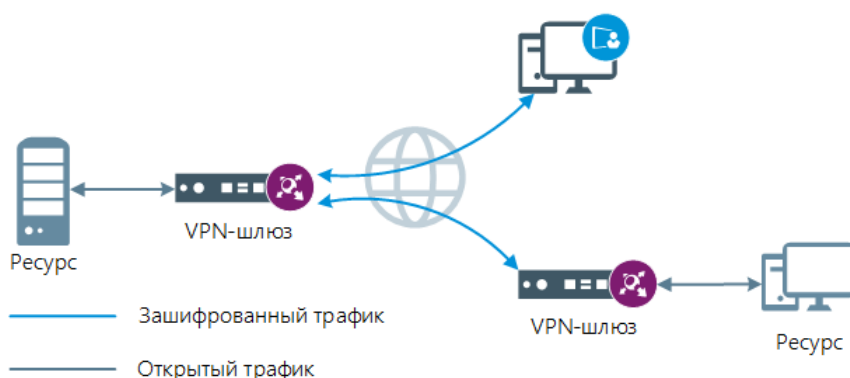


Рисунок 38. Защита соединения на сетевом уровне модели OSI при передаче данных через публичные сети

Вы можете создать ресурс двумя способами:

- для туннелируемого координатором диапазона IP-адресов в модуле VPN создать новое устройство — ресурс (отображается только в модуле VPN);
- для единичного туннелируемого координатором IP-адреса создать устройство (см. [Создание устройств](#)), затем в модуле VPN выбрать его в качестве ресурса.

Чтобы создать ресурс:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите **ViPNet VPN**  **> Ресурсы**.
- 4 Нажмите  **Добавить** и в меню выберите один из пунктов:
 - **Создать новый ресурс** — чтобы создать новое устройство ресурса для туннелирования координатором нескольких IP-адресов, в том числе диапазона IP-адресов. Откроется мастер создания нового ресурса, следуйте его указаниям.

Введите имя ресурса и укажите координатор, который будет выполнять туннелирование IP-адресов.

Добавление ресурса ✕

Шаг 1 из 2

* Имя ресурса

Voice Server

Описание

* Координатор

VA2000 🔍 ▼

Далее
Отмена

Рисунок 39. Создание нового ресурса

- **Добавить существующий ресурс** — чтобы выбрать созданное ранее устройство в качестве ресурса для туннелирования его IP-адреса.

Выберите устройство и туннелирующий координатор. В списке для выбора ресурса отображаются все устройства организации, которые не задействованы в модуле VPN.

Добавление ресурса ✕

Шаг 1 из 2

🔍 Поиск Записей: 9

Устройство	Описание
IG100-I4 A0	
Mail Server	
SIP-Server-MSK	
Сервер приложений	

* Координатор

VA2000 🔍 ▼

Далее
Отмена

Рисунок 40. Выбор устройства при добавлении ресурса

- 5 В поле **Добавление IP-адресов ресурса** введите IP-адрес или диапазон IP-адресов ресурса для туннелирования и нажмите **Добавить**.

Диапазон IP-адресов задайте интервалом (например, 192.168.1.0–192.168.1.255) или с использованием маски в префиксном формате (например, 192.168.1.0/28).

Не задавайте для туннелирования IP-адреса, которые могут пересекаться с адресами действующей сети, чтобы избежать некорректной работы сети. Иначе отобразится сообщение «Диапазон IP-адресов, охватывающий несколько подсетей, может стать причиной некорректной работы сети».

- 6 Чтобы исключить IP-адрес или диапазон IP-адресов из записи заданных IP-адресов, в поле **Добавление IP-адресов ресурса** введите IP-адрес или диапазон IP-адресов ресурса и нажмите **Исключить**.



Внимание! Если вы случайно исключите все адреса из ресурса, то ресурс будет недоступен в защищенной сети.

Запись с IP-адресом или диапазоном IP-адресов будет отображена в списке ниже.

Рисунок 41. Добавление ресурса

- 7 Нажмите **Сохранить**.

Чтобы удалить заданные IP-адреса или диапазон IP-адресов для ресурса:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN**  > **Ресурсы**.
- 3 Чтобы найти ресурс, в поле поиска начните вводить имя ресурса или его IP-адрес.
- 4 Выберите ресурс.
- 5 Напротив **IP-адреса для туннелирования** нажмите .
- 6 Наведите указатель мыши на запись и нажмите .
- 7 Нажмите **Сохранить**.

Включение функций VPN, DPI, IPS и других

Вы можете разрешить использование функций:

- ViPNet Coordinator HW 5:
 - VPN-шлюз;
 - Failover;
 - DPI;
 - IPS;
 - обновление DPI;
 - обновление IPS;
 - обновление базы вредоносного ПО;
 - обновление базы URL-категорий;
- ViPNet Coordinator IG 5:
 - VPN-шлюз;
 - Failover;
 - IPF;
 - Modbus Gateway;
 - IEC101-IEC-104 Converter;
 - IPS;
 - обновление IPS;
 - обновление базы вредоносного ПО;
- ViPNet xFirewall:
 - IPS;
 - Failover (для ViPNet xFirewall xF100);
 - SSL-инспекции;
- ViPNet Coordinator KB 4 и KB 5:
 - Failover;

Каждая функция лицензируется и по умолчанию отключена.

Для координаторов поколения ViPNet 4 и ViPNet Coordinator KB 5 всегда включена функция VPN-шлюза, её нельзя отключить и она не отображается в интерфейсе.

Примечание. Ограничения:



- за ViPNet Coordinator IG10 и ViPNet Coordinator HW10 нельзя регистрировать клиенты;
- за ViPNet Coordinator IG100 зарегистрируйте не более 10 клиентов (ограничение ViPNet Coordinator IG100).

Функции координатора, которые зависят от работы функций VPN-шлюза:

- сервер соединений,
- защищенный интернет-шлюз,
- регистрация клиентов и устройств ViPNet xFirewall,
- туннелирование ресурсов,
- защищенный DNS-сервер,
- межсетевой шлюз,
- режим работы межсетевого экрана.

Чтобы использовать координатор ViPNet Coordinator HW 5 или ViPNet Coordinator IG 5 для этих функций, включите **VPN-шлюз**. При отключении функции **VPN-шлюз** на координатор не отправляются справочники и ключи, но он сохраняет свои настройки и продолжает выполнять функции в сети, назначение VPN-функций на узел недоступно.



Примечание. Функцию **VPN-шлюз** для координаторов с ПО ViPNet 5 можно включить при наличии лицензии на функции VPN.

Чтобы разрешить использование дополнительных функций:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN** .
- 3 Выберите **Координаторы** (или **Другие узлы**).
- 4 Выберите устройство.
- 5 Нажмите .
- 6 Включите дополнительные функции. Разрешить использование функций VPN-шлюза можно только на координаторе. Для этого на вкладке **Общие** включите  **VPN-шлюз**.

Настройки координатора

Core Coordinator

ОбщиеФункцииПараметры подключенияГруппы

* Тип координатора

Coordinator VA1000 v.5

* Лицензия

Coordinator VA1000 v.5 (версия 5.99 и ниже)
Срок действия по 06.12.2024

Профиль DNS

Профили DNS не созданы.

☒ VPN-шлюз

Поддерживаемые функции ?

Регистрация узлов

Сервер соединений

DNS-сервер

Межсетевой шлюз

Туннелирование

Failover

Защищенный интернет-шлюз

DPI

Обновление DPI

Сохранить

Отмена

Рисунок 42. Включение функций VPN-шлюза на координаторе

- 7 На вкладке **Функции** включите  дополнительные функции. Функции отображаются, если организации выданы лицензии на них.



Примечание. Если в организации нет лицензий на функции, вкладка **Функции** не отображается.

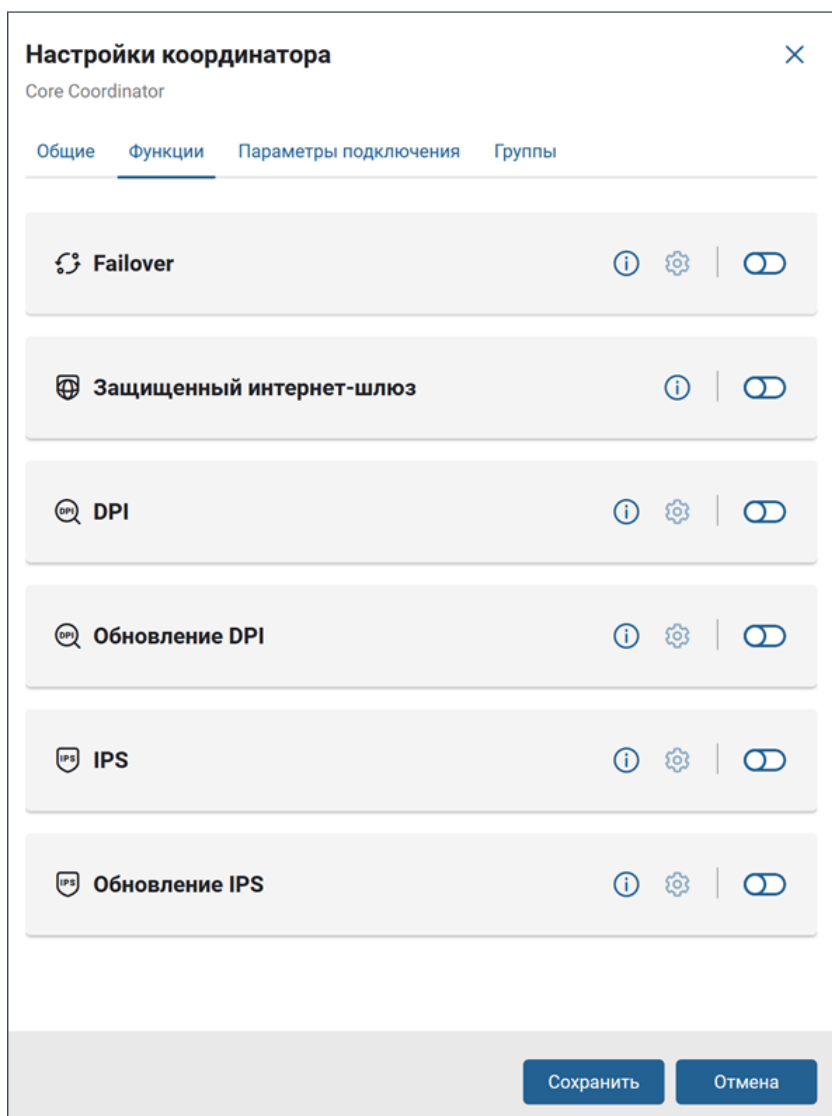


Рисунок 43. Разрешение использования дополнительных функций

- 8 Выберите лицензию на функцию и нажмите **Применить**.
- 9 Чтобы изменить выбранную лицензию, нажмите , выберите новую лицензию и нажмите **Применить**.
- 10 Нажмите **Сохранить**.

Чтобы посмотреть, какие функции включены для координатора, выберите координатор на панели справа в разделе **Функции координатора** посмотрите список.

Если у вас истекла лицензия на функцию и при загрузке файла с новой лицензией не продлился срок ее действия, порядок действий см. в разделе [Не сопоставились лицензии при загрузке файла](#).

Защищенный интернет-шлюз

Защищенный интернет-шлюз разделяет доступ клиентов в интернет и к корпоративным ресурсам сети VPN.

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

- Работа в интернете — запрещены соединения с узлами сети VPN, кроме защищенного интернет-шлюза.
- Работа в корпоративной сети — заблокирован доступ в интернет.

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

Чтобы включить функцию защищенного интернет-шлюза:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN**  > **Координаторы**.
- 3 Выберите координатор.
- 4 Нажмите .
- 5 Для поколения ViPNet 5 и выше на вкладке **Общие** включите **VPN-шлюз**.
- 6 На вкладке **Функции** включите  **Защищенный интернет-шлюз**.
- 7 Нажмите **Сохранить**.
- 8 Чтобы на клиентах, не зарегистрированных на координаторе, доступ в интернет был организован через защищенный интернет-шлюз, [создайте связи между клиентами и координатором с функцией защищенного интернет-шлюза](#). Связи между координатором и зарегистрированными на нем клиентами создаются автоматически. Об управлении настройкой на клиенте см. «ViPNet Client. Руководство пользователя», «Управление конфигурациями программы».

Включение функции кластера

Чтобы использовать шлюз безопасности в [кластере](#):

- 1 [Выдайте лицензии на Failover соответствующие исполнению шлюза](#).
- 2 В модуле VPN включите **Failover** для устройства и создайте для него дистрибутив ключей.

В кластер горячего резервирования можно включить только шлюзы безопасности с одинаковым типом ПО и исполнением. В защищенной сети кластер — единое устройство, поэтому на обоих устройствах установите один и тот же дистрибутив ключей.

Ниже приведена настройка кластера на основе координаторов. Кластер на основе ViPNet xFirewall создается аналогично.

Чтобы создать кластер, например, на основе ViPNet Coordinator HW1000:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN**  > **Координаторы**.
- 3 Выберите координатор.
- 4 Нажмите .
- 5 На вкладке **Функции** включите  **Failover**. Настройка доступна при наличии лицензии Failover1000 в организации.
- 6 Нажмите **Сохранить**.
- 7 Создайте дистрибутив ключей для выбранного координатора и установите его на обоих устройствах кластера.

О развертывании кластера см. в документации шлюза безопасности.

Настройка доступа к веб-интерфейсу координатора

Вы можете перейти из ViPNet Prime в веб-интерфейс управления координаторов поколения ViPNet 5.

Для защиты передачи данных с ViPNet Coordinator HW и ViPNet Coordinator IG используется защищенный канал ViPNet и протокол TLS с односторонней аутентификацией.

Модуль VPN перенаправляет запрос к веб-интерфейсу координатора. Обращение к узлу осуществляется по неизменяемому в рамках сети ViPNet доменному имени, сформированному на основе ViPNet-идентификатора узла. Это помогает избежать ситуаций, когда ViPNet-узел становится недоступным для других узлов по IP-адресу или доменному имени.

Ссылка для доступа к веб-интерфейсу формируется только для узлов, которым сформирован дистрибутив ключей.

Предварительные действия

Для открытия локальной консоли управления из ViPNet Prime на узле Control Center настройте разрешение доменных имен `.vipnet`.

- 1 Войдите на сервер ViPNet Prime с правами суперпользователя `root` или привилегированного пользователя для использования команды `sudo`.
- 2 Перейдите в `/etc/systemd/resolved.conf`.
- 3 Укажите адрес DNS-сервера — 11.254.254.254.

4 На узле Control Center выполните рекомендации по настройке работы с DNS для ViPNet Client, см. «ViPNet Client 5 for Linux. Руководство администратора», раздел «Рекомендации по настройке работы с DNS».

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

```
ping -n <VPN-идентификатор_узла>.vipnet
```

Например: `ping -n 536E0001.vipnet`

Настройка доступа к веб-интерфейсу координатора

1 Войдите в ViPNet Prime как владелец организации или администратор организации.

2 Выберите **ViPNet VPN**  > **Координаторы**.

3 Выберите координатор.

4 Нажмите .

5 На вкладке **Параметры подключения** в группе **Параметры доступа к веб-интерфейсу** укажите:

- Протокол доступа:
 - **http** — когда нет TLS-сертификата для соединения по протоколу HTTPS.
 - **https** (по умолчанию) — когда TLS-сертификат установлен на координаторе.
- Порт доступа для подключения. По умолчанию 8080.

6 Нажмите **Сохранить**.

7 При изменении порта доступа или протокола синхронизируйте это с настройками координатора.

См. «ViPNet Coordinator HW 5. Настройка с помощью командного интерпретатора», раздел «Настройка подключения с помощью веб-интерфейса».

Для перехода в веб-интерфейс координатора:

1 Войдите в ViPNet Prime как владелец организации, администратор организации или аудитор устройств, или сетевой администратор шлюза безопасности.

2 Выберите **Управление организацией**  > **Устройства**.

3 Выберите координатор.

4 Нажмите ссылку для перехода в веб-интерфейс координатора.

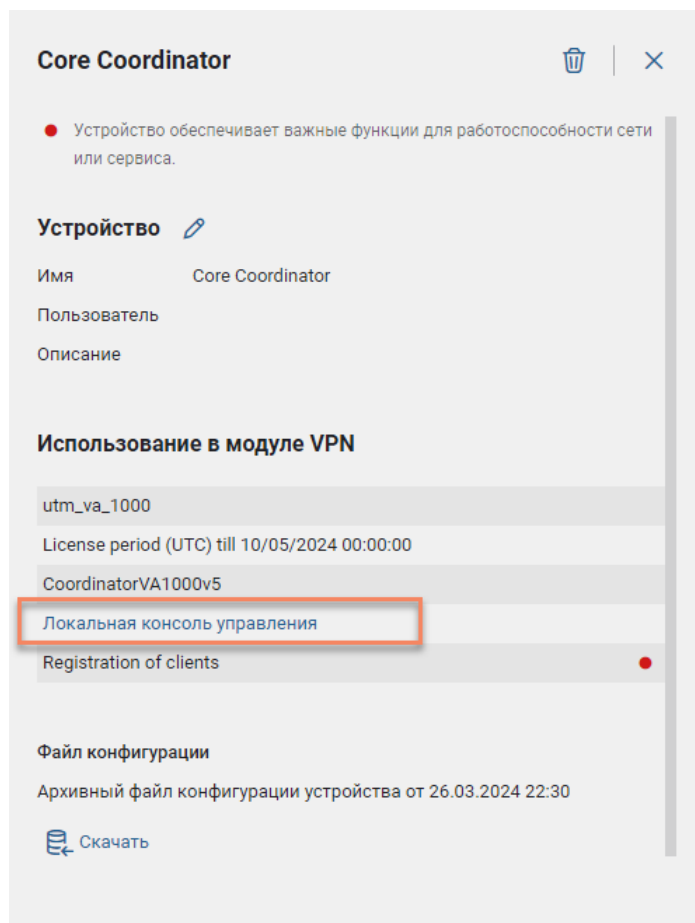


Рисунок 44. Переход в веб-интерфейс координатора

Настройка применения ViPNet Coordinator IG в промышленной сети

ФСТЭК России устанавливает требования к межсетевым экранам, которые бывают нескольких типов. В зависимости от назначения сети, в которую устанавливается ViPNet Coordinator IG, вы можете выбрать для него [тип межсетевого экрана](#):

- тип «А», тип «Б» (по умолчанию) — межсетевой экран уровня сети;
- тип «Д» — межсетевой экран уровня промышленной сети.

Межсетевой экран типа «Д» поддерживает дополнительные режимы работы. Подробнее см. в документации ViPNet Coordinator IG.

Чтобы использовать ViPNet Coordinator IG в качестве межсетевого экрана промышленной сети:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите ViPNet VPN  > Координаторы.
- 3 Выберите координатор.

- 4 Нажмите .
- 5 Включите **VPN-шлюз**.
- 6 На вкладке **Функции** в группе **Режим работы межсетевого экрана** нажмите .
- 7 Выберите тип «Д» межсетевого экрана и нажмите **Сохранить**.
- 8 Нажмите **Сохранить**.



Примечание. Чтобы изменить режим работы ViPNet Coordinator IG 5, включите **VPN-шлюз**.

ViPNet Coordinator IG поддерживает функцию межсетевого шлюза:

- исполнения Coordinator IG100, Coordinator IG100-I4 и Coordinator IG100-A1 v.5 — при включении функции **VPN-шлюз**.
- исполнения Coordinator IG100 A0, Coordinator IG100 B0, Coordinator IG100 A1, Coordinator IG100 B1 — отдельно не лицензируется, функция доступна по умолчанию.

Включение дополнительных функций на координаторе

- 1 Убедитесь, что организации выданы лицензии на функцию **IPF IG, Modbus IG, IEC101-IEC104 Converter**.
- 2 На вкладке **Функции** включите:
 - **IPF** — фильтрация промышленных протоколов;
 - **Modbus Gateway** — использование шлюза промышленного протокола Modbus RTU-TCP.
 - **IEC101-IEC104 Converter** — использование преобразователя (конвертера) протоколов IEC 60870-5-101 и IEC 60870-5-104.
- 3 Нажмите **Сохранить**.

Смена типа и лицензии координатора

Вы можете изменить тип координатора поколения ViPNet 4 и ViPNet 5 на новый без создания нового координатора, например при замене аппаратной платформы координатора на более производительную, виртуальной платформы на аппаратную или замене ViPNet Coordinator HW на ViPNet Coordinator IG или ViPNet Coordinator KB того же поколения.

Перед сменой типа или лицензии распределите в организацию действующую лицензию.

Особенности и ограничения

- При смене типа координатора автоматически освобождается лицензия на старую платформу и на все лицензируемые функции, которые недоступны или не лицензируются для нового типа.

- Если для старого типа функция не лицензировалась, а для нового — лицензируется, и в организацию распределена лицензия на эту функцию, лицензия спишется, и функция будет включена.
- Если лицензия координатора просрочена или вам требуется сменить лицензию на новую с другими лицензионными ограничениями для этого координатора, вы можете изменить лицензию в свойствах координатора.
- При смене типа Coordinator KB 5 на другой тип освобождается номер комплекта ДСДР и создается ссылка на веб-интерфейс координатора. При обратной смене типа номер комплекта ДСДР назначается автоматически, и удаляется ссылка на веб-интерфейс координатора.
- Нельзя сменить тип координатора ViPNet L2-10G на другой тип.
- При смене любого типа координатора на ViPNet L2-10G и ViPNet Coordinator KB 4 для узла устанавливается номер комплекта ДСДР.
- Нельзя сменить тип координатора на ViPNet L2 или ViPNet Coordinator KB 4, если в сети выбран тип ключевого блокнота КУБИТ.
- При смене типа Coordinator KB 4 на другой тип освобождается номер комплекта ДСДР.

Смена типа или лицензии координатора

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN**  > **Координаторы**.
- 3 Выберите координатор.
- 4 Убедитесь, что новый тип координатора поддерживает все необходимые функции. Отключите неиспользуемые или неподдерживаемые функции.
- 5 Нажмите .
- 6 Чтобы сменить тип:
 - 6.1 В окне **Настройки координатора** > **Общие** в списке **Тип координатора** выберите тип. Тип координатора отображается в списке, если на него выдана лицензия.

Если лицензий несколько (с разными ограничениями), выберите лицензию вручную. Если лицензия одна, она выбирается автоматически.
 - 6.2 В группе **Поддерживаемые функции** просмотрите список функций старого типа координатора, которые будут недоступны для нового типа или которые требуется отключить, так как новый тип координатора эти функции не поддерживает или нет свободной действующей лицензии на эту функцию. Чтобы отключить функцию, не поддерживаемую новым типом координатора, перейдите на вкладку **Функции** и отключите функцию .
- 7 Чтобы сменить только лицензию, в окне **Настройки координатора** > **Общие** в списке **Лицензия** выберите новую лицензию.
- 8 Нажмите **Сохранить**.

- 9 Чтобы завершить изменение типа или лицензии координатора, создайте и установите новый дистрибутив ключей на новом координаторе (см. [Создание дистрибутива ключей](#)).

Не требуется создавать новый дистрибутив ключей при смене:

- платформ виртуальных исполнений;
- лицензии.

В этих случаях на координаторы автоматически отправляется обновление справочников и ключей.

Настройки координатора VA 1000 ПАК

Общие | Функции | Параметры подключения | Группы

* Тип координатора
Coordinator VA2000

* Лицензия
Coordinator VA2000 – версия 9.0 и ниже
Срок действия по 25.03.2030

Поддерживаемые функции ?

- ✓ Регистрация клиентов
- ✓ Сервер соединений
- ✓ Защищенный интернет-шлюз
- ✓ HW 5.0 (UTM)
- ✓ DNS-сервер
- ✓ Межсетевой шлюз
- ✓ Туннелирование
- ✗ ViPNet Failover 1000 Будет недоступна
- ViPNet Failover 2000

Сохранить Отмена

Рисунок 45. Смена типа координатора Coordinator VA1000 на Coordinator VA2000

Смена поколения координатора

Если необходимо перевести узел на поколение ViPNet 5, вы можете изменить тип уже существующего узла, при этом будут сохранены все его связи и настройки. Вы можете сменить поколение:

- ViPNet Coordinator HW 4 на ViPNet Coordinator HW 5;



Внимание! Вы можете сменить поколение ViPNet Coordinator HW на версию 5.3.2 и выше.

- ViPNet Coordinator IG 4 на ViPNet Coordinator IG 5;
- ViPNet Coordinator KB 4 на ViPNet Coordinator KB 5.

Чтобы сменить поколение координатора:

- Распределите в организацию лицензию на нужный тип координатора.
- Лицензия на нужный тип координатора должна быть свободна и действительна.
- Меняйте поколение только с ViPNet 4 на ViPNet 5. Смена поколения с ViPNet 5 на ViPNet 4 запрещена.
- Перед сменой поколения отключите все лицензируемые функции на координаторе.
- Не отправляйте политики безопасности в ViPNet Prime Policy Management на устройства в процессе смены поколения до выпуска и установки нового дистрибутива ключей. Иначе на координатор может не отправиться политика или отправится неактуальная политика.

Нельзя поменять поколение координатора, который выполняет VPN-функции, если эти функции не поддерживает новый тип координатора или в организацию не распределены лицензии на VPN-функции. Отключите такие функции на координаторе, затем измените его тип.

При смене поколения:

- Освобождается лицензия на старый тип координатора и списывается лицензия на новый тип.
- Включаются VPN-функции, если новый тип координатора поддерживает и фактически выполняет их, списывается лицензия.
- Для координатора поколения ViPNet 5 создается ссылка на веб-интерфейс, если поддерживается для нового типа координатора.
- Сохраняются настройки координатора.

Порядок действий

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Убедитесь, что в организацию распределены лицензии на поколение узлов ViPNet 5.
- 4 Выберите **ViPNet VPN**  > **Координаторы**.
- 5 Выберите координатор поколения ViPNet 4, который требуется обновить.
- 6 Отключите неиспользуемые или неподдерживаемые функции.
- 7 Задайте настройки, соответствующие узлу поколения ViPNet 5:
 - выберите **новый тип координатора**,
 - выберите лицензию для поколения ViPNet 5.

- 8 Сохраните изменения.
- 9 [Создайте дистрибутив ключей](#) в формате *.ds5.
- 10 Сохраните на USB-носитель дистрибутив ключей в формате *.ds5 и с паролем от дистрибутива ключей передайте его администратору координатора доверенным способом.
- 11 Администратор координатора выполняет действия:
 - 11.1 Сохраняет резервную копию координатора.
 - 11.2 Устанавливает на координатор обновление ПО.
 - 11.3 Устанавливает дистрибутив ключей в формате *.ds5.

После смены типа узла ViPNet Prime автоматически отправляет обновление справочников и ключей на узлы, связанные с координатором, тип которого изменился.

После смены типа координатора:

- ViPNet Prime не будет взаимодействовать с координатором до установки на нем нового дистрибутива ключей. При этом сам координатор будет работать.
- При наличии политик безопасности для узла отправьте результирующие политики на устройство, это не произойдет автоматически.
- Справочники и ключи отправятся автоматически на узлы, связанные с координатором, тип которого изменился.

Различия в доступности функций между поколениями координатора

Функция	Узел ViPNet 4	Узел ViPNet 5
DNS-сервер	Доступна при создании узла	Доступна на узле, поддерживающем функцию DNS-сервера, включается при включении функции VPN. Для ViPNet Coordinator KB доступна, не нужно дополнительно включать функцию VPN
Туннелирование	Доступна при создании узла	Доступна, включается при включении функции VPN. Для ViPNet Coordinator KB доступна, не нужно дополнительно включать функцию VPN
Регистрация узлов	Доступна при создании узла	Доступна, включается при включении функции VPN. Для ViPNet Coordinator KB доступна, не нужно дополнительно включать функцию VPN

Функция	Узел ViPNet 4	Узел ViPNet 5
Сервер соединений для координатора	Доступна при создании узла	Доступна, включается при включении функции VPN. Для ViPNet Coordinator KB доступна, не нужно дополнительно включать функцию VPN
Межсетевой шлюз	Доступна при создании узла	Доступна, включается при включении функции VPN. Для ViPNet Coordinator KB доступна, не нужно дополнительно включать функцию VPN
Защищенный интернет-шлюз	Доступна при создании узла	Доступна, включается при включении функции VPN. Для ViPNet Coordinator KB не доступна
Failover	Доступна при наличии лицензии	Доступна при наличии лицензии
DPI	Недоступна для узлов поколения ViPNet 4	Выключена. Доступна при наличии лицензии
IPS	Доступна только для ViPNet xFirewall	Выключена. Доступно для ViPNet Coordinator HW и ViPNet Coordinator IG при наличии лицензии
Обновление DPI	Недоступна	Выключена. Доступна при наличии лицензии
Обновление IPS	Недоступна	Выключена. Доступна при наличии лицензии
Обновление базы вредоносного ПО	Недоступна	Выключена. Доступна при наличии лицензии
Обновление базы URL-категорий	Недоступна	Выключена. Доступна при наличии лицензии
IPF	Недоступна	Выключена. Доступна при наличии лицензии
Modbus Gateway	Недоступна	Выключена. Доступна при наличии лицензии
IEC101-IEC104 Converter	Недоступна	Выключена. Доступна при наличии лицензии
Режимы работы межсетевого экрана (А и Д)	Доступна, без лицензии на функцию	Доступна, без лицензии на функцию. Сохраняет установленное значение
Ссылка на веб-интерфейс координатора	Недоступна	Доступно только ViPNet Coordinator HW, VA или IG

Функция	Узел ViPNet 4	Узел ViPNet 5
Пароли администраторов узла	Доступна всем узлам	Недоступна

Регистрация ключевых блокнотов

Если в защищенной сети используются ViPNet Coordinator KB или ViPNet L2-10G, для выработки ключей шифрования IP-трафика, передаваемого между координаторами, используются ключевые блокноты ДСДР (Документ Сети Доверенного Распространения) или КУБИТ (Ключевой Универсальный Блокнот ИнфоТеКС). Ключевые блокноты содержат ключевую информацию, которая используется для шифрования конфиденциальной информации. Ключевые блокноты используются для средств криптографической защиты данных, не содержащих сведений, составляющих государственную тайну.

Ключевые блокноты ДСДР или КУБИТ необходимо зарегистрировать в ViPNet Prime. Для этого укажите номера серий и номера комплектов ключей. Информация о номерах указана на диске ДСДР или КУБИТ, который выдается сторонней уполномоченной организацией. Номера серий ключей действуют для всех координаторов ViPNet Coordinator KB и ViPNet L2-10G одной защищенной сети.

За полгода, а также за 3 месяца до даты окончания действия текущей серии ключей ДСДР или КУБИТ отображается оповещение для владельца организации, администратора организации и аудитора устройств. Проверьте номер следующей серии ключей на диске и зарегистрируйте ее в ViPNet Prime.

По умолчанию срок действия серии ключей ДСДР или КУБИТ 1 год и 3 месяца. Датой ввода в действие серий ключей считается указанная дата по локальному времени ViPNet Prime в 00:00 UTC, даже для сегодняшней даты. Настройка поддерживается только в положительном часовом поясе.

После регистрации ключевого блокнота текущая серия ключей сменится на следующую автоматически в дату, указанную в качестве даты ввода в действие.

Связь между узлами ViPNet L2-10G или ViPNet Coordinator KB 4 и узлами ViPNet L2-10G, ViPNet Coordinator KB 4 или ViPNet Coordinator KB 5 строится на ключах ДСДР, с остальными узлами — на ключах обмена из дистрибутива ключей *.dst.

Связь между узлами ViPNet Coordinator KB 5 строится на ключах ДСДР или КУБИТ.

Для регистрации ключей:

- 1 Задайте параметры ключевых блокнотов для сети.
- 2 Задайте номера комплектов ключевых блокнотов для всех ViPNet Coordinator KB или ViPNet L2-10G в организациях.

Чтобы задать параметры ключевых блокнотов:

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 Выберите **ViPNet VPN**  > **Ключевые блокноты**.

3 В разделе **Серии ключей** нажмите .

4 Укажите текущую серию ключей:

4.1 В разделе **Текущая серия ключей** выберите тип ключевого блокнота.

Вы можете выбрать тип КУБИТ только если в сети нет ViPNet Coordinator KB 4 и ViPNet L2-10G.

Если в вашей сети есть ViPNet Coordinator KB 4, вы можете обновить их до ViPNet Coordinator KB 5, чтобы использовать ключевые блокноты КУБИТ. Если в сети есть ViPNet L2, вы можете использовать только ключевые блокноты ДСДР.

4.2 Выберите алгоритм ключа:

- **Магма** или **Кузнечик** — в защищенной сети, состоящей только из узлов **поколения ViPNet 5**. Можно выбрать для ключевых блокнотов ДСДР или КУБИТ.
- **ГОСТ 28147-89** — в защищенной сети, состоящей из узлов поколения ViPNet 5 и **поколения ViPNet 4**. Нельзя выбрать для ключевых блокнотов КУБИТ.

Если в вашей сети используются только ViPNet Coordinator KB 5, вы можете выбрать алгоритм ГОСТ 28147-89 или ГОСТ 34.12-2018 «Магма» и «Кузнечик». Если в вашей сети используются ViPNet L2, ViPNet Coordinator KB 4 и KB 5, выбирайте алгоритм ГОСТ 28147-89.

4.3 Укажите номер серии.

4.4 Укажите дату ввода в действие (по умолчанию — текущая дата).

4.5 Нажмите **Сохранить**.



Внимание! Указанные параметры невозможно изменить, если до ввода в действие осталось меньше 24 часов.

5 Чтобы указать следующую серию ключей:

5.1 В разделе **Серии ключей** нажмите .

5.2 В разделе **Следующая серия ключей** укажите тип ключевого блокнота следующей серии.

5.3 Выберите алгоритм ключа.

5.4 Введите номер серии и дату ввода в действие (по умолчанию — через 1 год и 3 месяца после ввода в действие текущей серии ключей).

Номер текущей и следующей серии ключевых блокнотов для одного типа ключевых блокнотов не может совпадать.

6 Нажмите **Сохранить**.



Внимание! Изменить алгоритм шифрования без смены серии ключей невозможно.

Чтобы задать номер комплекта ключевого блокнота:

1 Войдите в ViPNet Prime как суперадминистратор, владелец или администратор организации.

2 Выберите **ViPNet VPN**  > **Ключевые блокноты**.

3 В разделе **Комплекты для координаторов** напротив координатора нажмите .

Для ключевых блокнотов ДСДР вы можете указать номер комплекта до 9999. Для ключевых блокнотов КУБИТ вы можете указать номер комплекта до 50000. Если ранее вы использовали ключи ДСДР и номер комплекта был выше 9999, номер комплекта будет считаться некорректным. Измените номер комплекта.

4 Введите номер комплекта ключей и нажмите **Сохранить**.

Убедитесь, что в сети нет узлов с некорректным номером комплекта ключевого блокнота. Иначе вы не сможете создать дистрибутивы ключей или отправить обновление справочников и ключей на эти узлы. Узлы с некорректным номером комплекта подсвечиваются красным индикатором.

В списке комплектов вы можете посмотреть идентификатор координатора VPN ID, чтобы по этому идентификатору найти координатор в списках узлов в модуле VPN.

При обновлении ViPNet Prime номера комплектов сохраняются и, если были некорректные, вам будут запрещены некоторые действия пока вы не измените номера комплектов.

Если в сети есть координаторы с некорректными номерами комплектов ключевых блокнотов

- Не обновляйте ViPNet Prime, если создан новый мастер-ключ сети, но ещё не задана дата отложенной установки новых ключей обмена и ключей защиты. Иначе после смены ключей такие узлы потеряют связь со всеми узлами сети и вам придётся устанавливать дистрибутивы ключей на этих узлах вручную.
- Не вводите в действие мастер-ключ ключей обмена организации.
- Не обновляйте мастер-ключи сети.

Скачивание резервной конфигурации координатора

Для восстановления конфигурации координатора после сбоев или переноса на другую платформу в ViPNet Prime вы можете скачать последнюю его конфигурацию. В нее входит полная копия конфигурации координатора, в том числе ключи. Гарантируется хранение конфигурации до 600 Мбайт.

Поддерживается одновременная отправка резервных конфигураций с 20 координаторов. При большем количестве координаторов отправляйте резервные конфигурации в разное время.

Координатор отправляет свою конфигурацию один раз в сутки в ViPNet Prime. Периодичность отправки резервной конфигурации задается на координаторе.

Файл резервной конфигурации координаторов поколения ViPNet 5 скачивается в формате ECF.

Чтобы скачать конфигурацию координатора:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите **Управление организацией**  > **Устройства**.
- 4 Выберите устройство.
- 5 Справа на панели выберите **Файл конфигурации**.
- 6 Нажмите **Скачать**.

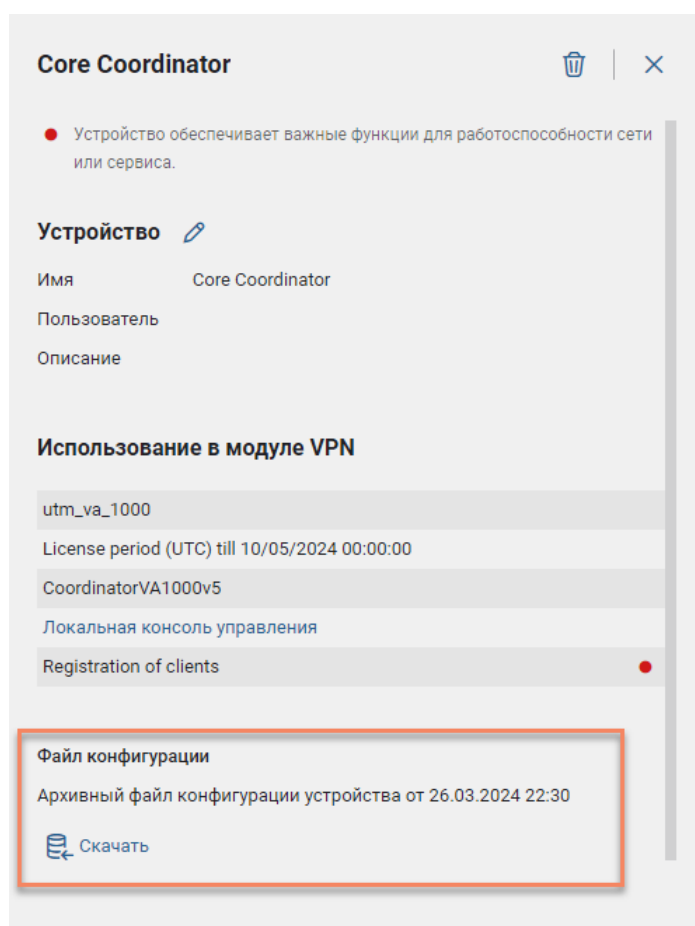


Рисунок 46. Скачивание резервной копии конфигурации координатора

В ViPNet Prime 1.9.8 и выше события скачивания конфигурации шлюза безопасности (события «Выгрузка конфигурации ПАК» и «Сохранение конфигурации ПАК») доступны для просмотра для ролей уровня организации: администратор организации, владелец организации, аудитор устройств. Чтобы отображались новые события для уже развернутых устройств, измените имя или описание устройства. События, которые были в журнале до обновления на версию 1.9.8, останутся недоступными для просмотра для этих ролей.

Аутентификация с учетной записью ViPNet Prime на координаторах поколения ViPNet 5

Вы можете использовать учетную запись ViPNet Prime (централизованная учетная запись) для аутентификации на координаторах ViPNet Coordinator HW 5 и ViPNet Coordinator IG 5.

Способы аутентификации в веб-интерфейсе:

- по имени учетной записи ViPNet Prime и паролю;
- по сертификату.



Внимание! Для ViPNet Coordinator HW 5 не работает аутентификация по паролю с использованием учетной записи ViPNet Prime в локальной консоли.

Способы аутентификации в CLI:

- Локально по сертификату на токене.

Аутентификация в CLI при локальном подключении к координатору с использованием учетной записи ViPNet Prime возможна только по [сертификату на токене](#). Токен должен быть подключен к аппаратной платформе координатора в процессе всего сеанса работы в CLI.

- Удаленно по паролю.

Аутентификация в CLI при удаленном подключении по SSH разрешена только по имени учетной записи ViPNet Prime и паролю. Необходимо, чтобы такое подключение было не запрещено на координаторе.

Для ViPNet Coordinator HW 5 версии 5.4.0 и выше и ViPNet Coordinator IG 5 версии 5.3.0 и выше при аутентификации в CLI с учетной записью ViPNet Prime имя учетной записи вводите с префиксом `prime/`, например `prime/User`.

Настройка клиентов

Изменение уровня полномочий на клиенте

Уровень полномочий пользователя разрешает изменять настройки в клиентском приложении ViPNet и имеет следующие значения по умолчанию:

- Windows-клиент: ViPNet Client for Windows, ViPNet Client 4U for Windows, ViPNet Client 5 for Windows — специальные полномочия;
- Android-клиент: ViPNet Client 4U for Android, ViPNet Client 5 for Android — максимальные полномочия;
- Аврора-клиент: ViPNet Client 4U для ОС Аврора, ViPNet Client 5 для ОС Аврора — максимальные полномочия;
- iOS-клиент: ViPNet Client 4U for iOS, ViPNet Client 5 for iOS — максимальные полномочия;
- Linux-клиент: ViPNet Client 4U for Linux, ViPNet Client 5 for Linux — максимальные полномочия;
- клиенты ViPNet CSS Connect HW — максимальные полномочия.

Ограничения функциональных возможностей ПО ViPNet, которые зависят от уровня полномочий пользователя, заданных в ViPNet Prime, см. в документации соответствующих продуктов.

Уровень полномочий задается для клиентов. Особенности полномочий пользователя ViPNet Client for Windows см. в документе «Классификация полномочий. Приложение к документации ViPNet».

Таблица 3. Обзор полномочий пользователя ViPNet Client 4U и ViPNet Client 5.

Лицензия	Уровень полномочий пользователя			
	Максимальный	Средний	Минимальный	Специальный
Client for Android v.4, v.5		Ввод пароля при включении VPN-соединения		
Client for Aurora v.4, v.5	не требуется	требуется всегда, кроме случаев, когда установлена блокировка экрана устройства с использованием графического ключа, PIN-кода, пароля или отпечатка пальца	требуется всегда	(уровень отсутствует, применяется максимальный)
Client for iOS v.4, v.5 Client for macOS v.4, v.5	не требуется	не требуется	требуется всегда	(уровень отсутствует, применяется максимальный)
Client for Windows v.4,		Автозапуск после входа в ОС		

Лицензия	Уровень полномочий пользователя			
	Максимальный	Средний	Минимальный	Специальный
v.5 Client for Linux Client for Linux v.5	да*	да*	нет	(уровень отсутствует, применяется максимальный)
Client for KasperskyOS v.5	Ввод пароля при включении VPN-соединения			
	не требуется	не требуется	требуется	(уровень отсутствует, применяется максимальный)

*кроме клиентов из Microsoft Store.

Чтобы изменить уровень полномочий:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию.
- 3 Выберите ViPNet VPN  > Сервисные функции.
- 4 Выберите группу Полномочия пользователей в ПО ViPNet и нажмите .
- 5 Для типа узла в списке выберите один из уровней полномочий: Минимальные, Средние, Максимальные, Специальные (только для Windows).
- 6 Нажмите Сохранить.

При изменении уровня полномочий на минимальные, резервный набор персональных ключей удаляется с узла и из дистрибутива ключей .dst. На устройстве с ViPNet Client for Linux при этом выключается VPN, включить который можно будет только с помощью пароля от последнего установленного .dst.

Если вы изменяете полномочия пользователей с минимального на любое другое, рекомендуется установить на узле новый дистрибутив ключей, чтобы обеспечить обновление ключей при смене мастер-ключей.

Блокировка VPN без ViPNet EPP

Если на клиенте не установлено приложение ViPNet EPP (EPP) Агент, вы можете блокировать на узле пользовательский защищенный трафик VPN. При этом не блокируются DNS-трафик и служебный трафик.

Для разблокировки пользовательского защищенного трафика VPN установите на узле EPP Агент.

Чтобы блокировать пользовательский защищенный трафик VPN на клиенте:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.

- 2 Выберите организацию и подразделение.
- 3 Выберите ViPNet VPN  > Клиенты.
- 4 Чтобы включить функцию на одном клиенте:
 - 4.1 Выберите клиент и нажмите .
 - 4.2 Выберите **Общие**.
 - 4.3 Включите  **Блокировка VPN без EPP**.
- 5 Чтобы включить функцию на нескольких клиентах, выберите клиенты и нажмите  > **Блокировка VPN без EPP** > **Включить**.

Расширенные настройки ViPNet Client

Вы можете централизованно задать настройки из режима отладки клиента в формате YAML. Поддерживаемые настройки см. в документации клиента. Например, см. «ViPNet Client 4U for Linux. Руководство администратора», раздел «Управление настройками ViPNet Client 4U».

Администратор задает настройки в виде параметров и их значений. Настройки передаются на клиенты всей сети ViPNet:

- в обновлениях справочников и ключей при изменении структуры сети;
- в дистрибутиве ключей.

При формировании обновления справочников и ключей или дистрибутива ключей для узла ViPNet Prime проверяет, включена ли отправка индивидуальных расширенных настроек:

- Если отправка индивидуальных настроек включена, на узел отправляется индивидуальный файл `custom.yaml`.
- Если отправка индивидуальных настроек отключена и создан общий файл `custom.yaml`, на узел отправляется общий файл `custom.yaml`.

Массовая отправка общих настроек на узлы

Чтобы задать расширенные настройки YAML:

- 1 Создайте файл `custom.yaml` и укажите в нем настройки.
- 2 На компьютере ViPNet Prime в папке `/var/lib/infotecs/vpn-kc/data/dst-service/custom-yaml/` сохраните файл `custom.yaml`.
- 3 Чтобы применить настройки на узлах, создайте дистрибутивы ключей и установите их на клиентах.

Чтобы отключить настройки YAML:

- 1 В файле `custom.yaml` удалите все содержимое.
- 2 Добавьте в файл строку:

```
# custom.yaml\n
```

- 3 Сохраните изменения в файле.
- 4 Чтобы отправить изменения справочников и ключей, измените структуру сети, например, создайте связи между узлами.

Чтобы удалить настройки YAML, отправленные на клиенты:

- 1 Удалите файл `/var/lib/infotecs/vpn-kc/data/dst-service/custom-yaml/custom.yaml`.
- 2 Чтобы отправить изменения справочников и ключей, измените структуру сети, например, создайте связи между узлами.

Отправка индивидуальных настроек

Чтобы настроить отправку индивидуальных настроек на клиент:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите **ViPNet VPN**  > **Клиенты**.
- 4 Выберите клиент и нажмите .
- 5 Выберите **Расширенные настройки**.
- 6 Включите  **Отправлять расширенные настройки**.
- 7 В поле укажите настройки.

Вы можете использовать любые символы. Максимальный объем сохраняемого файла — 1 Мбайт.

- 8 Нажмите **Сохранить**.

В настройках клиента на панели справа в разделе **Особенности клиента** появится запись **Включены расширенные настройки**.

При отключении отправки расширенных настроек содержимое файла сохранится и отобразится в поле при повторном включении.

Настройка профиля DNS

При удаленном подключении к корпоративным ресурсам, расположенным в защищенной сети, мобильные устройства пользователей получают сетевые настройки из разных локальных сетей и сетей передачи данных. Для пользователя список доступных DNS-серверов может содержать публичные DNS-серверы. При подключении из публичной сети к ресурсам защищенной сети DNS-запрос может быть отправлен на публичные DNS-серверы. Это создает возможность атаки с подменой ресурса, при которой клиент в ответ на DNS-запрос получит IP-адрес сайта, контролируемого злоумышленником, и перейдет на него. Рекомендуется запросы на разрешение

имен корпоративных ресурсов отправлять на выделенные защищенные DNS-серверы. Для этого создайте [профиль DNS](#) и укажите в нем доменные зоны для списка защищенных DNS-серверов.



Внимание! В качестве DNS-сервера нельзя использовать клиент поколения ViPNet 4 на ОС Аврора.

В случае если в защищенной сети присутствуют не взаимодействующие между собой DNS-серверы, обслуживающие отдельные корпоративные ресурсы, добавьте такие DNS-серверы в разные профили DNS и задайте для каждого профиля защищенные DNS-серверы и доменные зоны.

Чтобы мобильные устройства пользователей имели доступ к защищенным корпоративным доменным зонам и отправляли запросы на разрешение доменных имен корпоративных ресурсов на защищенные DNS-серверы, создайте [профиль DNS](#).

Создание профиля DNS

Чтобы клиенты отправляли запросы на разрешение имен на защищенные DNS-серверы и доменные зоны:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите ViPNet VPN  > Профили DNS.
- 4 Нажмите  **Добавить**.
- 5 На шаге 1:
 - 5.1 Введите имя для профиля DNS и описание.

По умолчанию все DNS-запросы публичных ресурсов отправляются на защищенные DNS-серверы (выбрано **Обрабатывать обращения к публичным ресурсам только на корпоративных DNS-серверах**).
 - 5.2 Нажмите **Далее**.
- 6 На шаге 2 для выбора защищенных DNS-серверов:
 - 6.1 Нажмите  **Добавить**.
 - 6.2 Выберите объекты, которые будут выполнять функции DNS-серверов. Вы можете найти их по идентификатору узла VPN ID.



Примечание. Если для ресурса задан только диапазон IP-адресов, то такой ресурс нельзя выбрать в качестве DNS-сервера. Задайте для такого ресурса хотя бы одну запись с одним IP-адресом.

- 6.3 Нажмите **Добавить**.

Примечание. Для корректной работы с профилем DNS на клиентах под управлением iOS или macOS создайте профиль DNS, в котором:



- Общее количество устройств и IP-адресов ресурсов, используемых в качестве DNS-серверов: не более 5.
- Количество DNS-зон: не более 125.

Чтобы найти профили DNS, для которых это не выполняется, в меню  выберите **Содержат некорректные параметры**.

6.4 Нажмите **Далее**.

7 На шаге 3 для добавления доменных зон:

7.1 Нажмите **Добавить**.

7.2 В поле **Доменное имя** введите доменное имя, которое необходимо обрабатывать на указанных DNS-серверах, и нажмите **Добавить**.

7.3 Нажмите **Далее**.

8 На шаге 4 для выбора узлов, которые должны отправлять запросы на разрешение имен на указанные DNS-серверы:

8.1 Нажмите **Добавить**.

8.2 В окне **Добавление узлов** выберите узлы, для которых нужно применить профиль DNS. Вы можете найти их по идентификатору узла VPN ID.

8.3 Нажмите **Добавить**.



Внимание! Профиль DNS не применяется к координаторам и ViPNet xFirewall.

9 Чтобы завершить добавление профиля DNS, нажмите **Создать**.

Выбор профиля DNS по умолчанию

Чтобы профиль DNS автоматически назначался на новые клиенты:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию.
- 3 Выберите **ViPNet VPN**  > **Сервисные функции**.
- 4 Выберите группу **Профиль DNS для новых узлов** и нажмите .
- 5 Выберите один из ранее созданных профилей DNS.
- 6 Выберите лицензию и нажмите **Применить**.

7 Чтобы изменить выбранную лицензию, нажмите , выберите новую лицензию и нажмите **Применить**.

8 Нажмите **Сохранить**.

Чтобы отменить выбор профиля DNS по умолчанию, нажмите **Сбросить настройки**. Профиль DNS по умолчанию отмечается в списке профилей символом .

Группы серверов соединений

Группа серверов соединений объединяет несколько координаторов с функцией сервера соединений и позволяет клиенту, на который назначена группа, переключаться на другой сервер соединений из группы, если используемый стал недоступен. Информация о назначении группы серверов соединений передается на клиенты в составе обновления справочников и ключей.

Использование группы серверов соединений:

- обеспечивает резервирование серверов соединений,
- позволяет управлять нагрузкой на координаторы в сети,
- упрощает перемещение клиентов между локальными сетями.

Это особенно актуально для мобильных устройств, которые смогут выбирать разные серверы соединений в зависимости от своего местоположения.

В группу серверов соединений могут входить координаторы поколения ViPNet 4 и ViPNet 5, которые могут выполнять функцию сервера соединений.

Добавление координатора в группу серверов соединений — критичная функция, то есть, чтобы удалить такой координатор из модуля VPN или ViPNet Prime, вам потребуется с начала удалить его из группы серверов соединений.

Вы можете просмотреть, в каких группах серверов соединений используется координатор, для этого в его свойствах в разделе **Особенности координатора** нажмите **Входит в группу серверов соединений**. Просмотрите список групп, в которые входит координатор.

На клиент может быть назначена только одна группа серверов соединений.

Группу серверов соединений можно назначить только на клиенты.

В одной организации вы можете создать до 100 групп серверов соединений.



Внимание! Работу с группой серверов соединений поддерживают только ViPNet Client 5. Версии ViPNet Client 5, которые поддерживают работу с группами серверов соединений, смотрите в документации ViPNet Client 5.

Особенности

- Чтобы добавить координатор в группу серверов соединений, у него должна быть включена функция VPN-шлюз. Если функцию отключили или на нее истекла лицензия, координатор продолжит работать как сервер соединений для узлов, которые уже используют его. Но вы не сможете добавить его в группу серверов соединений, назначить группу с таким координатором на новый узел или изменить группу серверов соединений. Удалите такой узел из группы серверов соединений или включите функцию VPN-шлюз.
- Для клиента, на который назначена группа серверов соединений, создаются автоматические связи со всеми координаторами из группы, даже если этот клиент не поддерживает работу с группой серверов соединений.
- Если администратор изменяет схему подключения к защищенной сети координатора, который входит в группу серверов соединений, группа серверов соединений изменяется: добавляется или удаляется координатор с вершины цепочки серверов соединений.
- Не рекомендуется добавлять координатор центра управления в группу серверов соединений. Иначе у него может снизиться производительность, что может привести к частичной потере работоспособности сети.
- Не назначайте группу серверов соединений на клиент центра управления.
- Не рекомендуется в одну группу серверов соединений объединять координаторы с разными платформами, например HW 1000 и HW 5000, иначе смена сервера соединений большим количеством узлов на менее производительный координатор может привести к неполадкам и выходу из строя серверов соединений.
- У координатора, который используется в группе серверов соединений, или у его сервера соединений должны быть заданы IP-адреса или доменные имена, по которым координатор будет доступен для клиентов из локальных или внешних сетей.
- Если назначить группу серверов соединений на клиент, отличный от ViPNet Client 5, он продолжит использовать как сервер соединений координатор, за которым зарегистрирован.
- При включении координаторов в группу серверов соединений обеспечьте равнозначный доступ и сетевую связность этих координаторов до транспортного сервера (центра управления — для UT или координатора, за которым зарегистрирован клиент — для MFTP) и координатора центра управления для узлов, работающих по MFTP.
- Если координатор, за которым расположены клиенты, расположен за сервером соединений, то все координаторы из группы серверов соединений, назначенной на клиенты, должны иметь сетевую связность с этим сервером соединений.

Создание группы серверов соединений

- 1 Войдите в ViPNet Prime как владелец или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите ViPNet VPN  > Группы серверов соединений.
- 4 Нажмите **Добавить**.
- 5 Укажите имя группы и добавьте описание, нажмите **Далее**.

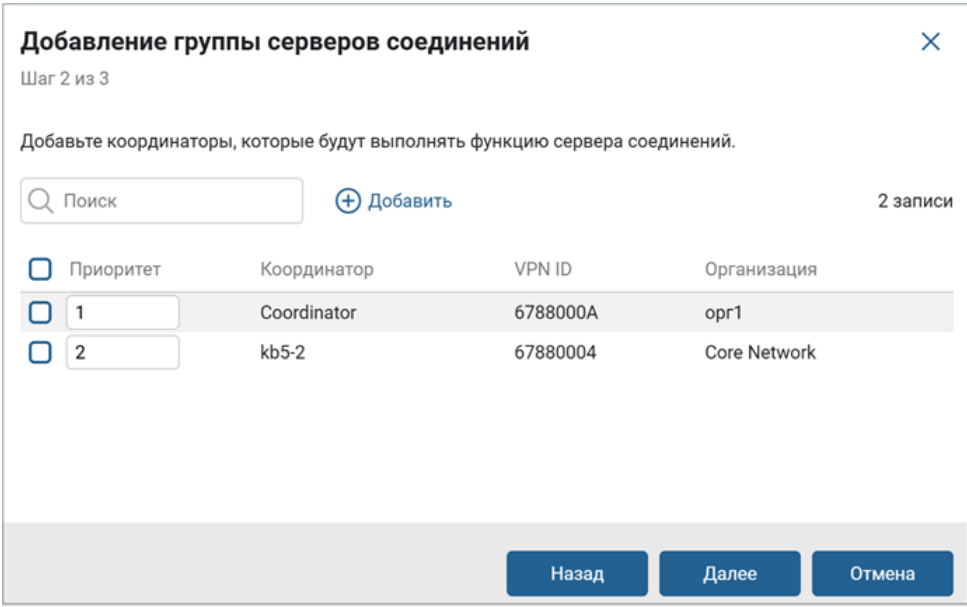
- 6 Нажмите  **Добавить**, чтобы добавить координаторы, которые будут выполнять функции сервера соединений. Вы можете найти координатор по идентификатору узла VPN ID.

- 6.1 Выберите от 1 до 5 координаторов и нажмите **Добавить**.

Вы можете отфильтровать организации, координаторы из которых показывать в списке.

- 6.2 Вы можете указать приоритет для каждого координатора. Приоритет может принимать значения от 1 до 255. Где 1 — максимальный приоритет, 255 — минимальный приоритет. Нажмите **Далее**.

Если вы добавляете в группу сервер соединений, который при подключении к защищенной сети использует другой сервер соединений, сервер соединений с вершины цепочки серверов соединений также автоматически добавляется в группу. Приоритеты для таких координаторов рассчитываются автоматически. Координаторы, которые добавляются автоматически, не отображаются в списке группы.



Добавление группы серверов соединений ✕

Шаг 2 из 3

Добавьте координаторы, которые будут выполнять функцию сервера соединений.

 **Добавить** 2 записи

☐ Приоритет	Координатор	VPN ID	Организация
☐ 1	Coordinator	6788000A	opr1
☐ 2	kb5-2	67880004	Core Network

Назад Далее Отмена

Рисунок 47. Добавление серверов соединений

- 7 Вы можете добавить клиенты, которые будут использовать эту группу серверов соединений. Вы можете найти их по идентификатору узла VPN ID.

- 7.1 Нажмите  **Добавить**, чтобы добавить узлы, которые будут подключаться с помощью группы серверов соединений.

Группу серверов соединений можно назначать только на клиенты. Вы можете отфильтровать клиентские узлы по типу узла. Координатор, за которым расположен клиент, не влияет на то, какую группу серверов соединений можно назначить на узел.

- 7.2 Выберите узлы и нажмите **Добавить**.

Вы можете назначить узлам созданную группу серверов соединений позже.

- 8 Нажмите **Готово**.

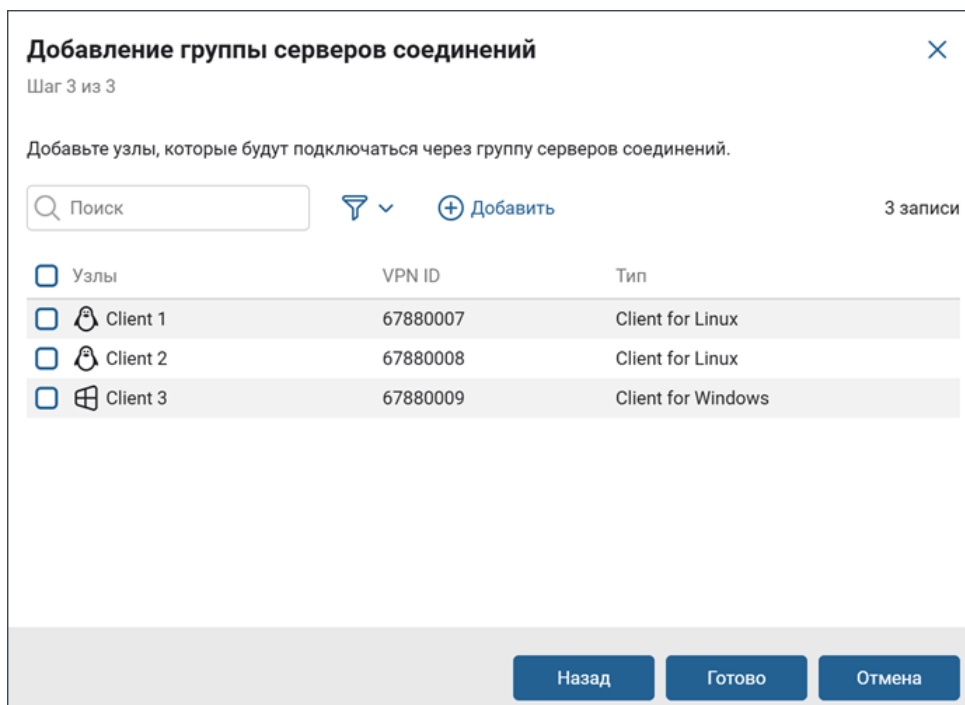


Рисунок 48. Выбор клиентов, которые будут подключаться через группу серверов соединений

- 9 Добавьте еще одну группу или нажмите **Заккрыть**.

Просмотр группы серверов соединений

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите **ViPNet VPN** > **Группы серверов соединений**.
- 4 Выберите группу.
- 5 На панели справа на вкладке **Общие** вы можете просмотреть состав группы серверов соединений.

Изменение группы серверов соединений

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите **ViPNet VPN** > **Группы серверов соединений**.
- 4 Выберите группу и нажмите .
- 5 Вы можете изменить:
 - Название и описание группы.
 - Список координаторов — добавьте или удалите координаторы. Нельзя удалить все серверы соединений из группы, пока она назначена на узел.
 - Список узлов — добавьте или удалите узлы.

6 Нажмите **Сохранить**.

Удаление группы серверов соединений

- 1 Выберите группу.
- 2 На панели справа нажмите  и подтвердите удаление.

Нельзя удалить группу серверов соединений, если она назначена на узлы.

Назначение группы серверов соединений узлу

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите **ViPNet VPN**  > **Клиенты**.
- 4 Выберите клиент и нажмите .
- 5 В списке **Группа серверов соединений** выберите группу.
- 6 Сохраните изменения.

При обновлении клиентов на версию 5 группа серверов соединений формируется автоматически на основании координатора, указанного в качестве сервера соединений для узла. После обновления узла вы можете изменить такую группу на одну из созданных в ViPNet Prime.

Смена типа, поколения узла и лицензии клиента

При переносе узла на другой компьютер или другое мобильное устройство может потребоваться сменить тип клиента на узле. При переходе к работе на алгоритмах ГОСТ 34.12-2018 необходимо сменить лицензию на новую с постфиксом v.5. Вы можете сделать это, не создавая новый узел в ViPNet Prime. Для уже существующего клиента вы можете сменить:

- тип узла и лицензию в рамках поколения;
- поколение узла (ViPNet 4 на ViPNet 5), в том числе с одновременной сменой типа узла, например, Client for Windows сменить на Client for Linux v.5.

Создавать новый узел не потребуется. Все связи, функции и настройки узла сохраняются, идентификатор ViPNet не изменится.



Внимание! Перед сменой поколения клиента сначала обновите все координаторы. Клиент на узле центра управления обновляйте в последнюю очередь.

Особенности:

- Если узел использует лицензию из пакета лицензий, тип узла можно сменить только на тот тип, на который в пакете есть свободная действующая лицензия.
- Вы можете сменить тип клиента, если в организации есть свободные лицензии на клиент или свободные лицензии в пакете лицензий.
- Если на узел назначено:
 - прикладное ПО:
 - сервер push-уведомлений CPNS;
 - сервер групповых чатов ConServer;
 - транспортный сервер Connect Hub;
 - сервер хранения файлов Connect File Exchange;
 - функция **Защищенный смартфон HardPhone**;
 - функция **Блокировка VPN без EPP**;
 - нелицензируемая функция DNS-сервер или Центр управления политиками безопасности,
 чтобы сменить тип, отключите функцию на узле. Остальные функции останутся включенными, если распределена свободная непросроченная лицензия. Если такой лицензии нет, отключите функцию перед сменой типа клиента.
- После смены типа узла, если узел участвует в межсетевом взаимодействии, отправьте межсетевую информацию в доверенную сеть или организацию. Если межсетевое взаимодействие создано на мастер-ключах ГОСТ 34.12-2018, скачайте межсетевую информацию и передайте ее администратору доверенной сети. Рядом с сетями, которым нужно передать межсетевую информацию, появятся индикаторы.
- После смены типа узла сохраняется принадлежность к группам и доступ к узлу из доверенных организаций.
- Сменить лицензию без смены типа клиентского узла нельзя при массовом выборе узлов. Смените лицензии на каждом узле отдельно.
- Для клиента центра управления ViPNet Prime можно сменить только поколение.
- При смене платформы узла с Windows или Linux станет недоступна ViPNet Деловая почта, если ранее была установлена на узле.
- Если пользователь сменил компьютер или мобильное устройство, его сообщения в ViPNet CSS Connect и ViPNet Деловая почта не переносятся на новое устройство.

Чтобы сменить тип или лицензию узла:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите **ViPNet VPN**  > **Клиенты**.
- 4 Чтобы сменить тип, поколение узла или лицензию на одном клиенте:
 - 4.1 Выберите клиент и нажмите .

- 4.2 Отключите неиспользуемые или неподдерживаемые функции на узле.
- 4.3 Выберите **Общие**.
- 4.4 Чтобы сменить тип или поколение узла, в списке **Тип узла** выберите новый тип. Вы можете одновременно сменить тип и поколение узла. Новая лицензия назначается автоматически, но вы можете ее заменить. Для этого в списке **Лицензия** выберите новую лицензию.
- 4.5 Чтобы сменить только лицензию, в списке **Лицензия** выберите новую лицензию.
- 4.6 Ознакомьтесь с предупреждением и подтвердите смену.
- 5 Чтобы сменить тип узла нескольких клиентов:
- 5.1 Выберите клиенты. Вы можете одновременно изменить тип узлов для поколения ViPNet 4 и ViPNet 5, но только в рамках поколения. В списке отображаются все типы, для которых в организацию распределено хотя бы по одной лицензии.
- Вы не сможете сменить поколение клиента сразу для нескольких узлов.
- 5.2 На панели сверху нажмите  > **Изменить платформу на** и выберите новую платформу.

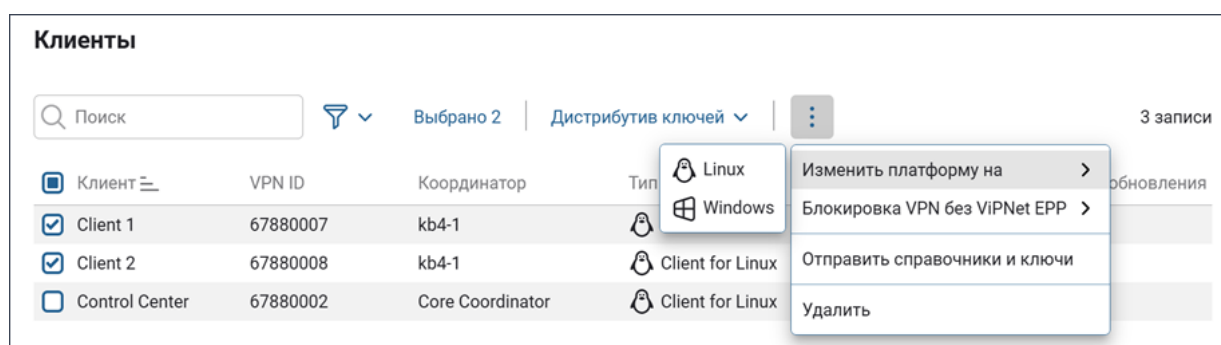


Рисунок 49. Смена типа клиента на нескольких узлах

- 5.3 Просмотрите список лицензий, которые будут назначены на узлы. Лицензии выбираются автоматически.

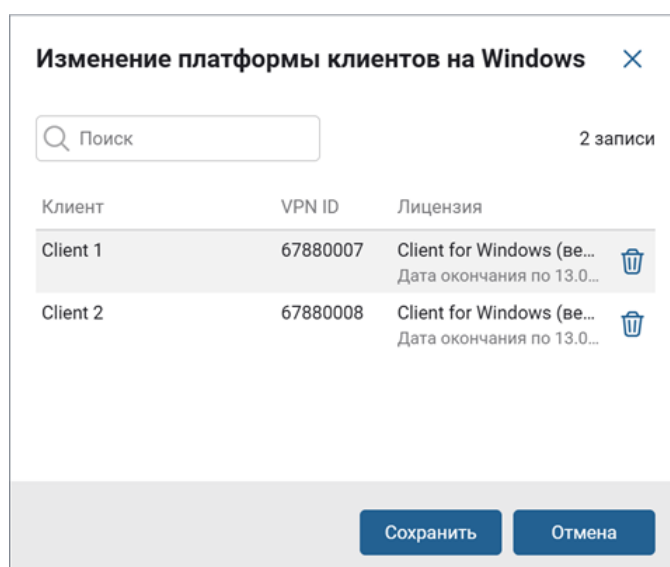


Рисунок 50. Просмотр информации о назначаемых на узлы лицензиях

Вы можете найти интересующие вас узлы по идентификатору VPN ID. Чтобы удалить узлы из списка, нажмите  напротив узла. Если узлу не удастся сменить платформу, в списке вы можете ознакомиться с причиной.

Если Prime не смог сменить лицензию на узле, вы можете посмотреть информацию об этом в отчете. Чтобы скачать отчет с информацией об изменяемых лицензиях на узлах, на панели сверху нажмите **Скачать отчет**. Отчет сохранится в файл

platform_report_<platform>_DD-MM-YYYY_HH-mm-ss.csv.

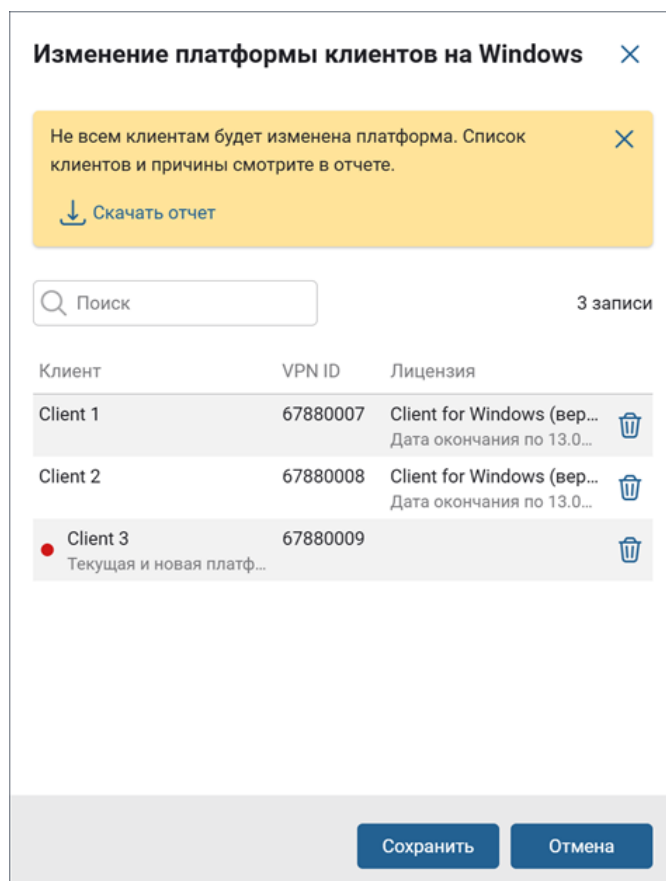


Рисунок 51. Информация о назначаемых на клиенты лицензиях

5.4 Нажмите **Сохранить**, ознакомьтесь с предупреждением и подтвердите смену.

- 6 Если вы сменили тип или поколение узла, создайте и установите новый дистрибутив ключей на узел. При смене поколения клиента перед установкой на узел дистрибутива ключей *.ds5 обновите ПО на узле.



Внимание! При смене только лицензии дистрибутив ключей создавать не нужно, дождитесь отправки обновлений справочников и ключей.

После создания нового дистрибутива ключей и до момента его установки на узел рекомендуется отключить VPN на узле, чтобы избежать некорректной работы.

После смены типа или поколения узла отправьте политики безопасности на устройство из модуля ViPNet Prime Policy Management. Это не произойдет автоматически.

Поведение функций и настроек при смене платформы узла

Функция/ Настройка	Поколение ViPNet 4 (с *.dst)	Поколение ViPNet 5 (с *.ds5)	Поведение функции при смене платформы
Connect	Доступно всем узлам при наличии лицензии	Доступно всем узлам при наличии лицензии	Останется в том же состоянии
Business Mail	Доступно только для Client for Windows и Client for Linux при включенной переменной окружения	Доступно только для Client for Windows v.5 и Client for Linux v.5 при включенной переменной окружения	При смене на тип узла Client for Windows, Client for Windows v.5 или Client for Linux, Client for Linux v.5 остается в том же состоянии. При смене на другой тип узла станет недоступна
DNS-сервер	Доступно всем узлам, кроме Client for Aurora и CSS Connect HW	Доступно всем узлам	Для узлов поколения ViPNet 4 — при смене на тип узла Client for Aurora, CSS Connect HW удалите функцию с узла. Для узлов поколения ViPNet 5 — остается в том же состоянии
CPNS	Доступно только для Client for Linux	Доступно только для Client for Linux v.5	При смене на тип узла Client for Linux или Client for Linux v.5 остается в том же состоянии. При смене на другой тип узла станет недоступна, отключите функцию
ConServer	Доступно только для Client for Linux	Доступно только для Client for Linux v.5	При смене на тип узла Client for Linux или Client for Linux v.5 остается в том же состоянии. При смене на другой тип узла станет недоступна, отключите функцию
Connect Hub	Доступно только для Client for Linux	Доступно только для Client for Linux v.5	При смене на тип узла Client for Linux или Client for Linux v.5 остается в том же состоянии. При смене на другой тип узла станет недоступна, отключите функцию
Connect File Exchange	Доступно только для Client for Linux	Доступно только для Client for Linux v.5	При смене на тип узла Client for Linux или Client for Linux v.5 остается в том же состоянии. При смене на другой тип узла станет недоступна, отключите функцию

Функция/ Настройка	Поколение ViPNet 4 (с *.dst)	Поколение ViPNet 5 (с *.ds5)	Поведение функции при смене платформы
Блокировка VPN без ViPNet EPP	Доступно только для Client for Windows и Client for Linux	Доступно только для Client for Windows v.5 и Client for Linux v.5	При смене на тип узла Client for Linux, Client for Linux v.5 или Client for Windows, Client for Windows v.5 остается в том же состоянии. При смене на другой тип узла станет недоступна, отключите функцию
HardPhone	Доступно только для Client for Android	Доступно только для Client for Android v.5	При смене на другой тип узла станет недоступна, отключите функцию
Центр управления политиками безопасности	Доступно только для Client for Linux и Client for Windows в организации Core Network при наличии лицензии	Доступно только для Client for Linux v.5 и Client for Windows v.5 в организации Core Network	При смене на тип узла Client for Linux v.5 или Client for Windows v.5 функция остается в том же состоянии. При смене на другой тип узла станет недоступна, отключите функцию
StateWatcher	Доступно только для Client for Windows	Доступно только для Client for Windows v.5	При смене на тип узла Client for Windows v.5 функция остается в том же состоянии. При смене на другой тип узла станет запрещена, отключите функцию
Узел Control Center	Только для Client for Linux	Только для Client for Linux v.5	Можно сменить только на Client for Linux
Полномочия			Меняются в соответствии с полномочиями, выставленными для типа узла

Управление связями

Связь между узлами защищенной сети позволяет одному узлу устанавливать VPN-соединения с другими сетевыми узлами. Существует несколько видов связей между объектами защищенной сети, отличающихся между собой характером установления связи:

- Связи, которые задает администратор.
- Обязательные связи — связи, установленные по умолчанию, они не зависят от действий администратора.
- Производные связи — связи, которые создаются автоматически при создании другой связи или каких-либо действиях администратора.

В защищенной сети возможно установить связи между следующими объектами в любых возможных комбинациях:

- любыми узлами;
- пользователями;
- группами;
- сетевыми ресурсами.

Связь между пользователями позволяет им звонить и обмениваться сообщениями друг с другом по защищенному VPN-каналу с помощью ViPNet CSS Connect версии 3 или писать письма в ViPNet Деловая почта.

Связь между узлами позволяет их пользователям звонить и обмениваться сообщениями друг с другом по защищенному VPN-каналу с помощью ViPNet Connect версии 2.

Вы можете использовать группы, чтобы упростить создание и изменение связей между большим количеством узлов и пользователей. По умолчанию узлы или пользователи, входящие в группу, не связаны между собой. Вы можете настроить автоматическое создание связей между всеми объектами внутри одной группы. При добавлении нового объекта в группу он будет получать связь со всеми объектами группы.

Производные и обязательные технологические связи отображаются в свойствах объекта, их нельзя изменить вручную, и они удаляются автоматически после прекращения причины их возникновения.

К производным связям относятся:

- Связь между координаторами связанных сетевых ресурсов или клиентов.
- Связь между серверами соединений связанных координаторов или клиентов, если их трафик по правилам маршрутизации проходит через два и более координаторов.
- Связь узла с узлами связанной группы.
- Связи между узлами (или пользователями) внутри одной группы, если в свойствах группы выбрано **Создавать связь между всеми узлами (или пользователями) группы**.

- Связи между узлами двух связанных групп.
- Связь между клиентами, принадлежащими одному пользователю.
- Связь между устройством и назначенным ему DNS-сервером.
- Связь между сервером групповых чатов и сервером пуш-уведомлений (устройством с ПО ViPNet ConServer и ViPNet CPNS) и устройствами пользователей с ПО ViPNet Connect.
- Связь между координаторами, выполняющими роль шлюза между доверенными сетями.
- Связь между серверами соединений, которые подключены к внешней сети напрямую и являются последними в цепочке серверов соединений связанных узлов. В группе серверов соединений связи создадутся со всеми координаторами, подключенными к сети напрямую.
- Связи между координатором и зарегистрированными на нем клиентами.
- Связи между координаторами, когда один из координаторов — [сервер соединений](#) для другого координатора.
- Связь между шлюзовым координатором и координатором узла, который использует DNS-сервер из доверенной сети.
- Связь между шлюзовым координатором в доверенную сеть и сервером соединений, последним в цепочке серверов соединений, если связаны координатор, подключенный к внешней сети через сервер соединений, и узел из доверенной сети. В группе серверов соединений связи создадутся со всеми координаторами, подключенными к сети напрямую.

К обязательным связям относятся:

- Технологические связи узлов и ресурсов с центром управления.

Такие связи позволяют устройствам принимать информацию об изменении свойств объектов, связей между ними, лицензионных ограничений, ключей. Например, если в защищенной сети было добавлено или удалено устройство, связанное с другими устройствами защищенной сети, информация об этом будет автоматически отправлена на устройства.

Примечание. Технологические связи шлюзов поколения ViPNet 4 с центром управления не отображаются в конфигурационном файле узла `iplir.conf`.

Чтобы убедиться в наличии связи между узлом и центром управления, отправьте на узел обновление справочников и ключей. Просмотрите в журнале транспортных конвертов, принял ли их узел. Если принял — значит техническая связь есть и работает.



Отсутствие связи с центром управления в `iplir.conf` не влияет на получение узлом обновлений от центра управления, но при этом не работает команда `iplir ping`.

Чтобы команда `iplir ping` работала, отображалась связь узла в `iplir.conf`, или если узел не принял справочники и ключи, создайте явную связь между узлом и центром управления.

- Технологические связи координаторов сети с координатором центра управления — межсерверные каналы.

Рекомендации по созданию связей

Чтобы два клиента могли устанавливать соединения между собой, клиенты должны обладать информацией о параметрах доступа друг к другу. Такую информацию каждый клиент получает от своего сервера IP-адресов. Клиент также сообщает серверу IP-адресов информацию о собственных параметрах доступа. По умолчанию функции сервера IP-адресов и маршрутизации выполняет координатор, на котором зарегистрирован клиент в ViPNet Prime.

Координаторы обмениваются информацией о клиентах, для которых они являются серверами IP-адресов, с учетом связей, установленных между клиентами. Для обеспечения этого обмена в управляющем ПО установите связи между координаторами, выполняющими функции сервера IP-адресов. Вы можете связать каждый координатор со всеми координаторами, но в больших сетях это приведет к загрузке каналов служебной информацией, а координаторы будут загружены ее обработкой.

Рекомендации:

- Клиенты, зарегистрированные на одном координаторе, по умолчанию не связаны друг с другом. Вы можете создать такую связь.
- Чтобы создать резервный сервер IP-адресов для группы клиентов, свяжите эти клиенты с некоторым координатором. Клиенты выберут этот координатор в качестве резервного сервера IP-адресов. Для такого координатора задайте такие же связи, как и для резервируемого координатора.
- Если координатор — сервер соединений для другого координатора, создайте связи между его клиентами и координатором, являющимся сервером соединений.
- Администратор организации должен убедиться, что в организации клиенты с ViPNet Connect связаны только с [одним сервером групповых чатов ConServer](#) и [одним сервером push-уведомлений CPNS](#).
- Для узлов проверьте топологию серверов соединений. Она должна включать в себя координатор, подключенный к внешней сети напрямую. Иначе при топологии «кольцо» нарушается маршрутизация трафика и узлы не получают обновления. В этом случае для восстановления работоспособности узлов создайте и установите новый дистрибутив ключей на таких узлах.

Особенности связей также см. в разделе [Назначение прикладного ПО ViPNet](#).

Создание связей между объектами организации

Для защищенного соединения по каналу VPN между двумя устройствами установите связи между ними. Связь между двумя пользователями устанавливает связь между всеми их устройствами. Вы можете установить связи с объектами внутри одной организации и с объектами доверенных организаций, если они разрешены для создания связей (см. [Связи с доверенными объектами](#)).

Связи отображаются на вкладках:

- **Добавленные** — добавленные администратором вручную связи.
- **Все** — автоматические, обязательные связи и добавленные вручную связи.

Чтобы создать связь между объектами:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN** .
- 3 Выберите объект или группу объектов для добавления связи.
- 4 На панели справа нажмите  **Связи**.

В окне добавления связей вы можете отфильтровать узлы по их идентификатору VPN ID.

- 5 Нажмите  **Добавить связь**.
- 6 Нажмите   и выберите свою организацию.

Вы можете отфильтровать узлы по их идентификатору VPN ID.

- 7 Выберите объекты, с которыми хотите установить связь.
 - Чтобы у пользователей была связь в ViPNet Connect 2.x, создайте связи между их узлами.
 - Чтобы у пользователей была связь в ViPNet CSS Connect 3.x, создайте связи между их пользователями.
 - Чтобы у пользователей была связь в ViPNet Деловая Почта, создайте связи между их пользователями.
- 8 Чтобы отфильтровать список объектов, нажмите   и выберите тип объекта.
- 9 Нажмите **Добавить**.
- 10 Нажмите **Сохранить**.

Копирование связей пользователя

Если для пользователя добавлены связи, вы можете скопировать их и применить для другого пользователя или группы пользователей. В списке связей пользователя скопированные связи отображаются как связи, добавленные вручную.

Чтобы для пользователя или группы пользователей скопировать связи другого пользователя:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN**  > **Пользователи** (или **Группы пользователей**).
- 3 Выберите пользователя (или группу пользователей), для которого копируете связи.
- 4 На панели справа нажмите  **Связи**.
- 5 Нажмите **Скопировать связи**.

- 6 Выберите пользователя, с которого хотите скопировать связи.
- 7 Нажмите **Копировать**.

Копирование связей шлюза безопасности

Если для шлюза безопасности вы ранее создавали связи, вы можете скопировать их и применить для другого шлюза безопасности. Под шлюзом безопасности в этом разделе будем понимать координаторы, узлы ViPNet xFirewall и узлы квантовой сети.

Копируются все связи из своей и доверенных сетей, которые созданы администратором вручную. В списке связей узла скопированные связи отображаются как связи, добавленные вручную.

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN**  > **Координаторы** (или **Другие узлы**).
- 3 Выберите узел, для которого копируете связи.
- 4 На панели справа нажмите  **Связи**.
- 5 Нажмите **Скопировать связи**.
- 6 Выберите узел, с которого хотите скопировать связи. Узел, с которого копируются связи, не добавляется в связи по умолчанию.
- 7 При необходимости выберите **Добавить выбранный узел в связи**.
- 8 Нажмите **Копировать**.
- 9 Просмотрите список связей, которые будут добавлены. Чтобы удалить связь из списка, выберите узел и нажмите .
- 10 Нажмите **Сохранить**.

Если скопированы связи из доверенной сети, отправьте межсетевую информацию в доверенную сеть.

Дистрибутивы ключей

Дистрибутивы ключей содержат служебную информацию о связях, лицензию и ключи для шифрования сетевого трафика. Для работы ПО ViPNet установите дистрибутив ключей на клиенты, координаторы, межсетевые экраны ViPNet xFirewall, узлы квантовой сети.

Чаще всего дистрибутив ключей вам требуется создавать при добавлении пользователя в защищенную сеть (для развертывания его узла). Создайте дистрибутив ключей повторно в следующих случаях:

- Проблемы при функционировании устройства пользователя в сети ViPNet, например, если произошла поломка компьютера и информация, хранившаяся на нем, была повреждена, и восстановить ее невозможно (в том числе справочники и ключи).
- Состояние устройства пользователя не позволяет отправлять и принимать зашифрованные письма, зашифровывать трафик, при этом удаленное обновление справочников и ключей по каким-либо причинам невозможно.
- При смене лицензии или платформы координатора (кроме смены исполнений VA на более производительные).

Чтобы получить актуальный дистрибутив ключей:

- 1 Создайте дистрибутив ключей. Распечатается [пароль пользователя](#). Скачивается последний созданный дистрибутив ключей.
- 2 Скачайте дистрибутив ключей. Он загрузится на компьютер через браузер в формате *.dst или *.ds5.

Если вы создали и не установили новый дистрибутив ключей на координаторах [поколения ViPNet 5](#), отправьте обновления справочников и ключей, иначе на координаторе вы не сможете отправлять в ViPNet Prime резервные копии *.ecf и проходить единую аутентификацию через ViPNet Prime. Это связано с тем, что при новом создании дистрибутива ключей изменяются секреты для аутентификации.

Кроме этого, установка нового дистрибутива ключей на координаторах приведет к потере локальных настроек и правил фильтрации и трансляции на координаторе. Чтобы получить актуальные справочники и ключи, дождитесь автоматического обновления справочников и ключей на координаторе.

Выдача паролей пользователей

Пароль пользователя выдается отдельно от дистрибутива ключей в распечатанном виде и хранится в системе управления до удаления узла из модуля VPN. Пароль печатается в ПИН-конверте на принтере.

По требованиям безопасности на рабочем месте администратора для браузера отключите предварительный просмотр документов, отправляемых на печать, и выберите принтер для печати по умолчанию.

Для печати используйте ПИН-конверты с двумя областями — закрытой (пароль) и открытой (название организации, имя пользователя и имя сетевого узла).

Таблица 4. Параметры ПИН-конверта (по умолчанию)

Параметр	Переменная в конфигурации	Значение
Высота конверта, мм	• NSMS_DstService_PinEnvelop__Size__Height	100
Ширина конверта, мм	• NSMS_DstService_PinEnvelop__Size__Width	210
Высота закрытой области печати, мм	• NSMS_DstService_PinEnvelop__ClosedPrintArea__Size__Height	18
Ширина закрытой области печати, мм	• NSMS_DstService_PinEnvelop__ClosedPrintArea__Size__Width	57
Координаты левого нижнего угла закрытой области (x, y)	• NSMS_DstService_PinEnvelop__ClosedPrintArea__XCoordinate	(118, 40)
	• NSMS_DstService_PinEnvelop__ClosedPrintArea__YCoordinate	
Размер шрифта в закрытой области печати	• NSMS_DstService_PinEnvelop__ClosedPrintArea__FontSize	18
Размер шрифта в открытой области печати	• NSMS_DstService_PinEnvelop__OpenPrintArea__FontSize	18
Высота открытой области печати, мм	• NSMS_DstService_PinEnvelop__OpenPrintArea__Size__Height	40
Ширина открытой области печати, мм	• NSMS_DstService_PinEnvelop__OpenPrintArea__Size__Width	82
Координаты левого нижнего угла открытой области (x, y)	• NSMS_DstService_PinEnvelop__OpenPrintArea__XCoordinate	(35, 40)
	• NSMS_DstService_PinEnvelop__OpenPrintArea__YCoordinate	



Внимание! Перед печатью паролей в ПИН-конвертах убедитесь, что все символы пароля помещаются в закрытой области. Если вы используете пароли длиннее 10 символов, измените размер шрифта в переменной конфигурации NSMS_DstService_PinEnvelop__ClosedPrintArea__FontSize на 10. Если в открытую область печати не помещается вся информация, измените размер шрифта в переменной конфигурации NSMS_DstService_PinEnvelop__OpenPrintArea__FontSize на 10.

Если приобретены ПИН-конверты другого формата, измените параметры печати:

- 1 На компьютере ViPNet Prime Key Center войдите в ОС с правами суперпользователя `root` или привилегированного пользователя для использования команды `sudo`.

2 Откройте конфигурационный файл `/usr/share/infotecs/vpn-kc/config.env` и измените значения параметров ПИН-конверта.

3 Перезапустите сервис выдачи ключей:

```
user@host:~$ sudo systemctl restart dst-service
```

Настройка применяется ко всем организациям ViPNet Prime.

Создание дистрибутива ключей



Внимание! Если скачать дистрибутив ключей, не создавая новый, скачается последний созданный дистрибутив ключей с возможно неактуальной информацией. Чтобы скачать актуальный дистрибутив ключей, заново создайте дистрибутив ключей и скачайте его. Дистрибутив ключей с большим количеством связей может создаваться продолжительное время, процесс не зависит от активности сессии администратора.

Чтобы создать и скачать дистрибутив ключей:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите ViPNet VPN  > Клиенты (или Координаторы, или Другие узлы).
- 4 Выберите узел.
 - Чтобы впервые создать дистрибутив ключей, на панели справа нажмите **Создать сейчас**.
 - Чтобы создать дистрибутив ключей повторно, на панели справа нажмите  > **Создать**.
- 5 Справа внизу появится оповещение, что дистрибутив создан. Чтобы скачать дистрибутив сразу, на оповещении нажмите **Скачать дистрибутив**.

Браузер загрузит на ваш компьютер дистрибутив ключей — файл с расширением `*.dst` или `*.ds5`.

- 6 Чтобы скачать дистрибутив ключей позднее:
 - 6.1 Выберите узел.
 - 6.2 На панели справа нажмите  > **Скачать**. Если дистрибутив ключей еще не создавался, то **Скачать** будет недоступно.
 - 6.3 Передайте доверенным способом дистрибутивы ключей и пароли от них администраторам или пользователям устройств для установки на узлах.
- 7 Чтобы распечатать ПИН-конверт с паролем пользователя, нажмите  > **Распечатать пароль**.

Вы можете распечатать пароль как сразу после создания дистрибутива ключей, так и в любой другой момент до удаления узла из модуля VPN.

Массовое создание и скачивание дистрибутивов ключей



Внимание! Перед массовым созданием дистрибутивов ключей для координаторов убедитесь, что на компьютере с ViPNet Prime достаточно свободного места. Один дистрибутив ключей для координатора может занимать более 20 Мбайт.

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите ViPNet VPN  > Клиенты (или Координаторы, или Другие узлы).
- 3 Чтобы в списке отобразить нужные типы объектов, в меню  выберите:
 - тип узла;
 - **Дистрибутив ключей > Не создан** — чтобы найти сетевые узлы, для которых дистрибутив ключей еще не создан;
 - **Дистрибутив ключей > Создан** — чтобы найти сетевые узлы, которым выдан дистрибутив ключей.
- 4 Выберите сетевые узлы. В больших сетях выбирайте не более 20 узлов за один раз, иначе загрузка архива с дистрибутивами ключей займет продолжительное время.
- 5 Нажмите **Дистрибутив ключей** и выберите **Создать**.

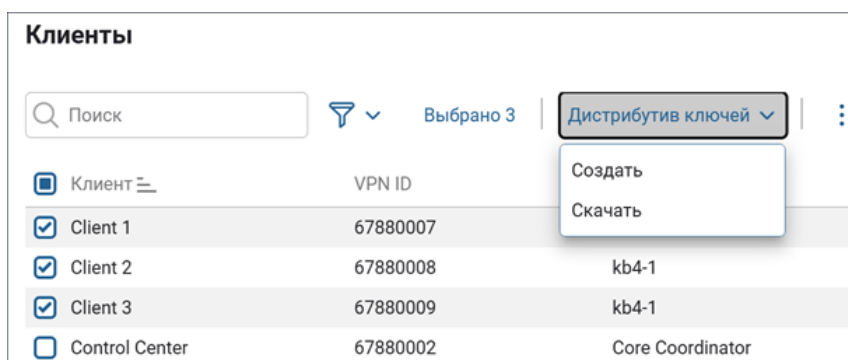


Рисунок 52. Создание дистрибутива ключей для нескольких узлов

- 6 Если при создании дистрибутивов ключей вы продолжили работу в модуле VPN в той же организации, в которой создаются дистрибутивы ключей, вам будет предложено распечатать все пароли от дистрибутивов ключей. Подтвердите печать ПИН-конвертов с паролями.
- 7 Нажмите **Скачать дистрибутивы**, подтвердите скачивание.

Дистрибутивы для выбранных узлов будут помещены в архив `distributives.zip`.



Внимание! Если не удалось скачать дистрибутивы ключей и оперативная память браузера перегружена, обновите браузер до последней версии или повторите операцию с меньшим количеством дистрибутивов ключей.

- 8 Если при создании дистрибутивов ключей вы перешли в другую организацию, в другой модуль ViPNet Prime или закрыли окно с ViPNet Prime, после возвращения к работе с дистрибутивами ключей распечатайте пароли отдельно для каждого дистрибутива:

8.1 Выберите узел.

8.2 Нажмите  > **Распечатать пароль**.

- 9 Передайте дистрибутивы ключей и пароли от них доверенным способом администраторам и пользователям для установки на узлы.

Чтобы скачать несколько дистрибутивов ключей позже:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите ViPNet VPN  > **Клиенты** (или **Координаторы**, или **Другие узлы**).
- 3 Выберите узлы.
- 4 Нажмите **Дистрибутив ключей** и выберите **Скачать**.

Назначение прикладного ПО

ViPNet

Чтобы пользователь мог использовать приложение ViPNet Connect на всех своих устройствах с ViPNet Client, в модуле VPN разрешите пользователю использовать это приложение.

Лицензии на приложение ViPNet Connect списываются по количеству пользователей. При назначении ПО ViPNet Connect нескольким пользователям будет занято количество лицензий на приложение ViPNet Connect, равное количеству пользователей, которым разрешено использовать приложение.

В одной организации вы можете использовать либо ViPNet Connect версии 2, либо ViPNet CSS Connect версии 3. Для этого в организации назначьте узлу с серверным ПО Connect при использовании:

- ViPNet Connect версии 2 — функции сервера push-уведомлений CPNS и сервера групповых чатов ConServer.
- ViPNet CSS Connect версии 3 — функции транспортного сервера Connect Hub, сервера хранения файлов Connect File Exchange и сервера push-уведомлений CPNS.

Чтобы использовать одновременно ViPNet Connect версии 2 и ViPNet CSS Connect версии 3:

- 1 [Создайте две организации.](#)
- 2 Настройте между ними взаимодействие.
- 3 В первой организации с ViPNet Connect версии 2:
 - 3.1 Создайте координатор и [предоставьте его в совместное использование во вторую организацию.](#)
 - 3.2 За этим координатором создайте один или два клиента на платформе Linux с пользователем для ViPNet CPNS и ViPNet ConServer.
 - 3.3 Настройте функции сервера push-уведомлений CPNS и сервера групповых чатов ConServer.
- 4 Во второй организации с ViPNet CSS Connect версии 3:
 - 4.1 Для транспортного сервера Connect Hub создайте узел на платформе Linux с пользователем. В качестве координатора используйте координатор из первой организации, на котором зарегистрирован узел с CPNS.
 - 4.2 Настройте функции транспортного сервера Connect Hub, сервера хранения файлов Connect File Exchange и сервера push-уведомлений CPNS.
 - 4.3 Создайте связи между пользователями с ViPNet CSS Connect версии 3 и узлами Connect Hub и Connect File Exchange.
- 5 Создайте связи между узлами CPNS и ConServer из первой организации и узлами Connect Hub и Connect File Exchange из второй организации.

- 6 Создайте связи между пользователем узла CPNS из первой организации и пользователем узла Connect Hub из второй организации.
- 7 [Создайте дистрибутивы ключей и установите их на узлах.](#)

Назначение серверного ПО ViPNet Connect

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 [Выберите организацию.](#)
- 3 Проверьте, что организации [выданы лицензии на серверное ПО ViPNet Connect](#):
 - при использовании ViPNet Connect версии 2:
 - **CPNS** — сервер push-уведомлений.
 - **ConServer** — сервер групповых чатов.
 - при использовании ViPNet CSS Connect версии 3:
 - **Connect Hub** — транспортный сервер.
 - **Connect File Exchange** — сервер хранения файлов.
 - **ConServer** — сервер групповых чатов.
- 4 Выберите ViPNet VPN  > **Сервисные функции.**
- 5 Выберите функцию и нажмите .

Функции отображаются при наличии лицензий.

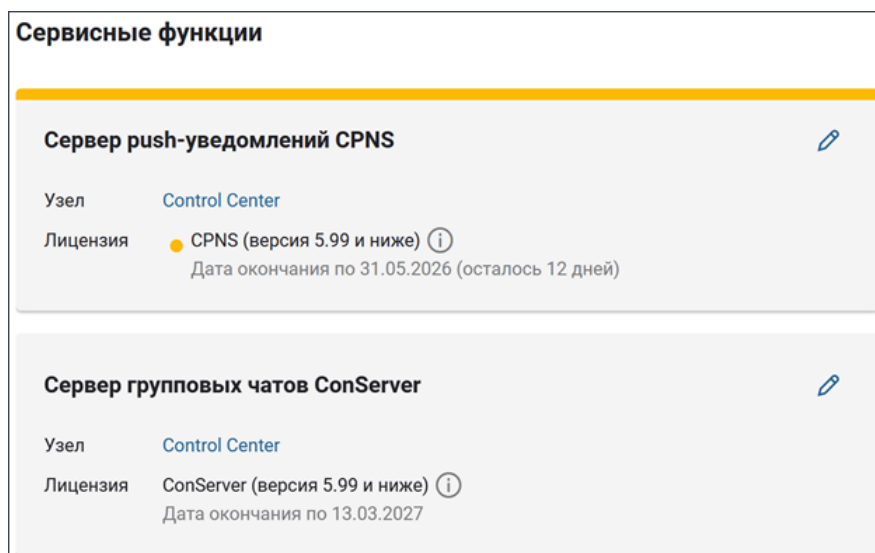


Рисунок 53. Назначение узла сервером групповых чатов и сервером push-уведомлений

- 6 Выберите узел, на котором будет развернуто серверное ПО ViPNet Connect. В списке отображены только узлы с лицензией на Linux-клиент.
- 7 Нажмите .

- 8 Выберите лицензию и нажмите **Применить**.
- 9 Чтобы изменить выбранную лицензию, нажмите , выберите новую лицензию и нажмите **Применить**.
- 10 Нажмите **Сохранить**.
- 11 Чтобы назначить несколько транспортных серверов Connect Hub:
 - 11.1 Выберите **Транспортные серверы Connect Hub**.
 - 11.2 Нажмите .
 - 11.3 Выберите узел, выберите лицензию и нажмите **Применить**.
 - 11.4 Чтобы изменить выбранную лицензию, нажмите  > **Редактировать**, выберите новую лицензию и нажмите **Применить**.
 - 11.5 Нажмите **Сохранить**.
- 12 При наличии узлов Connect Hub и Connect File Exchange создайте связи:
 - между узлами Connect Hub и Connect File Exchange;
 - между узлами Connect Hub и CPNS;
 - между клиентами с ViPNet CSS Connect и Connect File Exchange;
 - между пользователями, зарегистрированными на узлах Connect Hub;
 - между пользователями Connect Hub и пользователями ViPNet CSS Connect;
 - между пользователями Connect File Exchange и пользователями ViPNet CSS Connect;
 - между пользователями Connect File Exchange и Connect File Exchange.

Чтобы в доверенных организациях использовать серверное ПО ViPNet Connect без развертывания собственных серверов, разрешите использовать доверенным организациям сервисные функции узла (см. [Управление совместным доступом к сервисным функциям](#)).

О том, как развернуть серверное ПО ViPNet Connect, см. «ViPNet ConServer и ViPNet CPNS. Руководство администратора» или «ViPNet CSS ConServer. Руководство администратора».

Примечание. Убедитесь, что сервер групповых чатов и сервер push-уведомлений:



- принадлежат одной и той же организации;
- в случае разделенного сервера — серверы связаны между собой.

Иначе корректная работа ViPNet ConServer и ViPNet CPNS будет невозможна.

Назначение ViPNet Connect одному пользователю

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN**  > **Пользователи**.
- 3 Выберите пользователя.
- 4 На панели справа на вкладке **Общие** в группе **Приложения** нажмите .
- 5 В окне **Приложения пользователя** включите  **ViPNet Connect**. Будет израсходована одна лицензия на приложение.
Чтобы освободить лицензии на приложение или отключить возможность использовать приложение, отключите  **ViPNet Connect**.
- 6 Выберите лицензию и нажмите **Применить**.
- 7 Чтобы изменить выбранную лицензию, нажмите , выберите новую лицензию и нажмите **Применить**.
- 8 Нажмите **Сохранить**.

Чтобы просмотреть устройства пользователей с ViPNet Connect:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN**  > **Клиенты**.
- 3 Нажмите  и выберите **ViPNet Connect**.

Назначение ViPNet Connect нескольким пользователям

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN**  > **Пользователи**.
- 3 Выберите пользователей.
- 4 Нажмите .
- 5 Выберите **Разрешить использование ViPNet Connect**.

Назначение ViPNet Деловая почта

- 1 Войдите на сервер ViPNet Prime с правами суперпользователя `root` или привилегированного пользователя для использования команды `sudo`.

- 2 Остановите ViPNet Prime:

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

- 3 Откройте настройки модуля VPN `/usr/share/infotecs/vpn-ms/config.env`.

- 4 Добавьте параметр `NSMS_Directory__BusinessMailEnabled` и задайте ему значение `true`:

```
NSMS_Directory__BusinessMailEnabled=true
```



Внимание! В синтаксисе параметра `NSMS_Directory__BusinessMailEnabled` используются одинарный (`_`) и двойной (`__`) символы нижнего подчеркивания.

- 5 Запустите ViPNet Prime:

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

- 6 Между пользователями, которые будут использовать приложение ViPNet Деловая Почта, создайте связи.

Мастер-ключи

Для создания защищенных VPN-соединений между узлами ключевой центр организации создает:

- Внутрисетевые мастер-ключи:
 - **мастер-ключи организации** — создает администратор при инициализации ключевого центра или новой организации, можно выбрать алгоритм каждого ключа;
 - **мастер-ключи сети** — создается для каждой сети по умолчанию, всегда по алгоритму ГОСТ 28147-89;
 - **мастер-ключи обмена между доверенными организациями** — создает администратор при создании межорганизационного взаимодействия, можно выбрать алгоритм.
- **Межсетевые мастер-ключи для взаимодействия с доверенными сетями** — создает суперадминистратор при создании межсетевого взаимодействия, можно выбрать алгоритм.

При инициализации ключевого центра владелец организации создает мастер-ключи организации Core Network:

- **Мастер-ключ ключей защиты обновлений** — для защиты обновлений справочников и ключей, обновлений ПО ViPNet.
- **Мастер-ключ ключей обмена** — для защиты данных, передаваемых между узлами внутри организации.

При создании организации, кроме Core Network, владелец организации дополнительно создает:

- **Мастер-ключ ключей для технической связи** — для защиты связей:
 - между узлами организаций и **центром управления Control Center**;
 - между координаторами организаций и **координатором центра управления**.
- **Мастер-ключ ключей обмена между узлами организации и поставщиком услуг** (организацией Core Network) — для защиты VPN-канала между узлами доверенных организаций с узлами Core Network в одной защищенной сети.

При взаимодействии между организациями (кроме Core Network) используется **мастер-ключ ключей обмена между доверенными организациями**.

На мастер-ключах формируются ключи, которые входят в состав ключей сетевых узлов организации. По умолчанию срок действия мастер-ключей — 1 год и 3 месяца. За 14 дней до окончания срока действия мастер-ключей отображается уведомление **о смене мастер-ключей**. Оно доступно к просмотру для ролей:

- сервисного администратора;
- владельца организации;
- администратора организации.

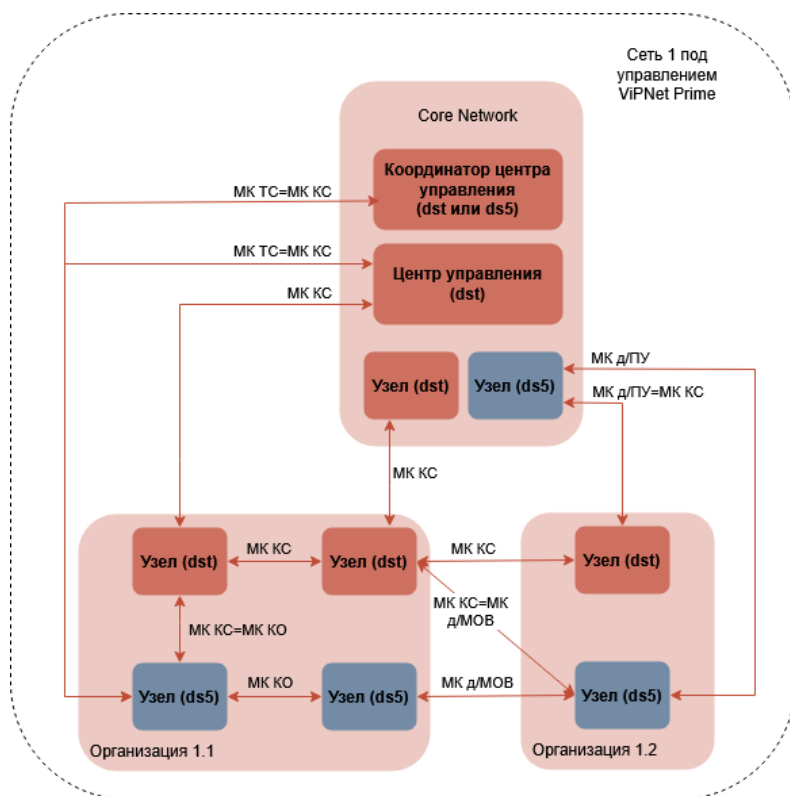
При компрометации мастер-ключей их смена выполняется внепланово.

Использование мастер-ключей

При взаимодействии между узлами центра управления и организаций, находящихся под управлением ViPNet Prime, используются разные мастер-ключи в зависимости от поколения узлов.

Если узлы центра управления на *.ds5, в вашей организации нет узлов с *.dst, связь с узлами в другой организации на *.dst не требуется, при создании мастер-ключей организации выбирайте алгоритм ГОСТ 34.12-2018 (см. Сеть 2 под управлением ViPNet Prime).

Если в сети требуется взаимодействие узлов с *.dst и *.ds5, при создании мастер-ключей организации выбирайте алгоритм ГОСТ 28147-89 (см. Сеть 1 под управлением ViPNet Prime).



МК КС - мастер-ключ ключей обмена сети
 МК КО - мастер-ключ ключей обмена (мастер-ключ организации)
 МК ТС - мастер-ключ ключей обмена для технической связи между узлами организации и центром управления (мастер-ключ организации)
 МК д/ПУ - мастер-ключ ключей обмена между узлами организации и поставщиком услуг (мастер-ключ организации)
 МК д/МОВ - мастер-ключ ключей обмена для межорганизационного взаимодействия (для взаимодействия между организациями кроме поставщика услуг)

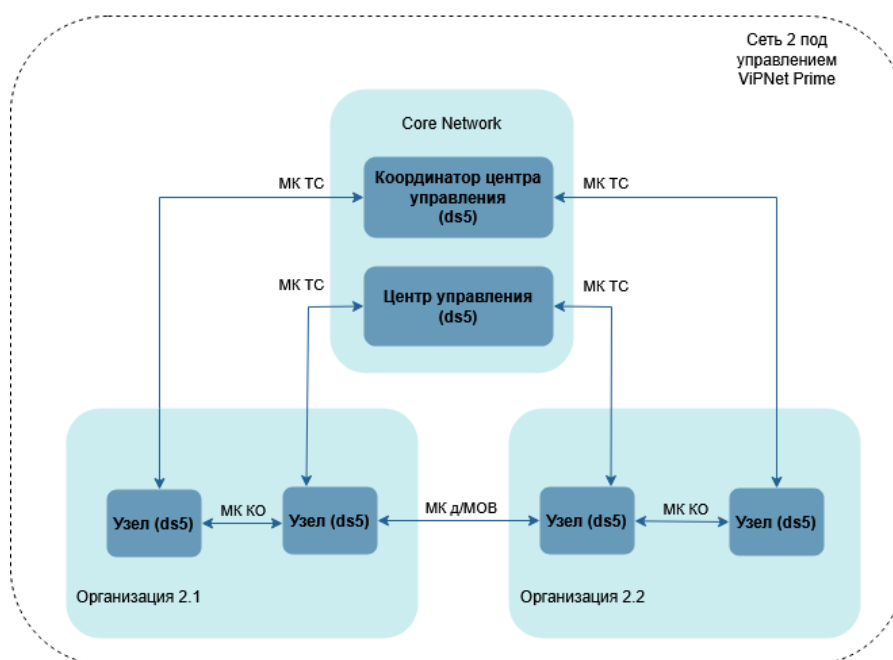
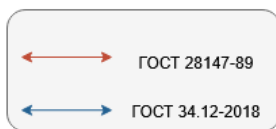


Рисунок 54. Принцип взаимодействия на мастер-ключах

Особенности взаимодействия:

- При инициализации ключевого центра всегда создаются мастер-ключи сети по ГОСТ 28147-89.
- При создании мастер-ключей организации по ГОСТ 28147-89 мастер-ключ ключей обмена сети импортируется в мастер-ключи организации. То есть мастер-ключ ключей обмена сети импортируется:
 - в мастер-ключ ключей обмена,
 - мастер-ключ ключей для технической связи,
 - мастер-ключ ключей обмена между узлами организации и поставщиком услуг,
 - мастер-ключ ключей обмена между доверенными организациями.

Узлы поколения ViPNet 5 (*.ds5) при взаимодействии с узлами поколения ViPNet 4 (*.dst) используют мастер-ключ ключей обмена (ViPNet 5), который равен мастер-ключу ключей обмена сети (ViPNet 4), если мастер-ключ организации по ГОСТ 28147-89. Узлы поколения ViPNet 4 и ViPNet 5 могут взаимодействовать только если эти ключи совпадают.

Порядок смены мастер-ключей поколения ViPNet 5

- 1 Отключите автоматическую отправку обновлений ключей.
- 2 Смените мастер-ключ ключей защиты обновлений.
- 3 Включите автоматическую отправку обновлений ключей.
- 4 Смените мастер-ключ ключей обмена.
- 5 При взаимодействии организации с организацией Core Network [смените мастер-ключ обмена между их узлами](#).

Отключение автоматической отправки обновлений ключей

Автоматическую отправку обновлений ключей необходимо отключать перед сменой:

- мастер-ключей сети;
- [мастер-ключа ключей защиты обновлений](#).

При проведении работ, требующих контроля за отправкой обновлений справочников и ключей, например [при смене лицензий для функции](#), вы можете отключить автоматическую отправку.

Если не отключить автоматическую отправку ключей, после применения нового мастер-ключа защиты обновлений на узел отправятся обновления справочников и ключей на старом мастер-ключе и узел станет неработоспособным.

Для отключения автоматической отправки ключей:

- 1 Войдите в ViPNet Prime как суперадминистратор или обратитесь к поставщику услуг.
- 2 Выберите **ViPNet VPN**  > **Настройка модуля**.
- 3 Выберите **Автоматическая отправка обновлений ключей**.
- 4 Нажмите **Отключить**. Во всех разделах интерфейса отобразится уведомление об отключении для владельца организации, администратора организации и аудитора устройств.

Чтобы после окончания регламентных работ включить автоматическую отправку ключей, нажмите **Включить**.

Смена мастер-ключей организации

Смене мастер-ключей организации подлежат:

- мастер-ключ ключей защиты обновлений;
- мастер-ключ ключей обмена;
- мастер-ключ ключей обмена для технической связи.



Внимание! ViPNet Coordinator HW 5 версии 5.2.1 и ниже не поддерживает смену мастер-ключа ключей защиты обновлений. Чтобы сменить мастер-ключи организации, сначала обновите ПО ViPNet Coordinator HW 5 до версии 5.3.1 и выше. Иначе не будут приниматься справочники и ключи, обновления ПО.

Для смены мастер-ключей организации:

- 1 Войдите в ViPNet Prime как владелец организации.
- 2 Выберите **ViPNet VPN**  > **Мастер-ключи**.
- 3 Выберите **Мастер-ключи организации**.
- 4 Перед сменой мастер-ключей удалите неиспользуемые мастер-ключи:
 - 4.1 Выберите мастер-ключ со статусом **Не используется**.
 - 4.2 Нажмите .
 - 4.3 Выберите **Удалить**.
- 5 Выберите тип мастер-ключа.

Смена мастер-ключа ключей защиты обновлений

Перед сменой мастер-ключа ключей защиты обновлений суперадминистратору необходимо [отключить автоматическую отправку обновлений ключей](#), после этого кнопка  **Создать новый мастер-ключ** станет активной.

- 1 Нажмите  **Создать новый мастер-ключ**.
- 2 Установите срок действия мастер-ключа.
По умолчанию — 1 год и 3 месяца. Датой начала действия мастер-ключей обмена устанавливается текущая дата и ее нельзя изменить.
- 3 Нажмите **Сохранить**. Новый мастер-ключ примет статус **Не используется**.
- 4 Назначьте новый мастер-ключ текущим:
 - 4.1 Выберите мастер-ключ.
 - 4.2 Нажмите  и выберите **Сделать текущим**.
 - 4.3 Нажмите **Сделать текущим**.
- 5 Новый мастер-ключ примет статус **Текущий**. Текущая дата будет установлена как дата ввода в эксплуатацию.



Примечание. Сетевые узлы, которым нужно отправить новые ключи защиты обновлений, будут отмечены . До получения новых ключей защиты на узлах еще используются ключи на основе старого мастер-ключа.

- 6 Для завершения смены мастер-ключа ключей защиты обновлений обновите ключи защиты на узлах, отмеченных значком 
 - удаленно:
 - на все сетевые узлы поколения ViPNet 5 — выберите **Мастер-ключ ключей защиты обновлений** и справа нажмите **Отправить**.

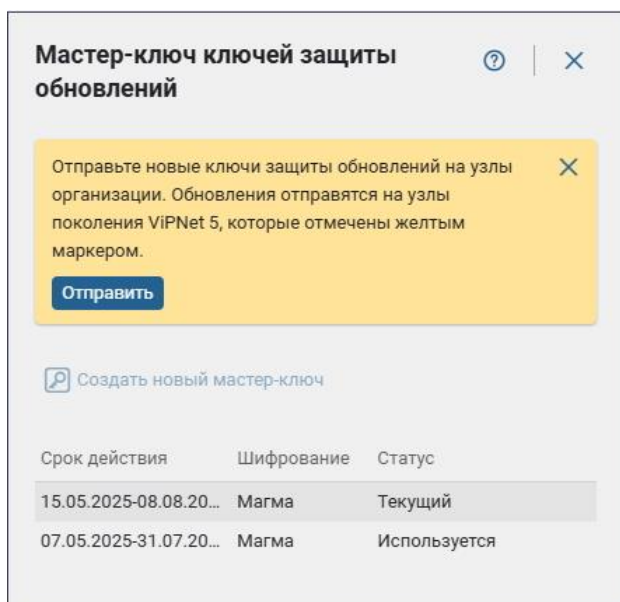


Рисунок 55. Обновление ключей узлов поколения 5

- на выбранный сетевой узел — выберите узел и справа нажмите **Обновить**.

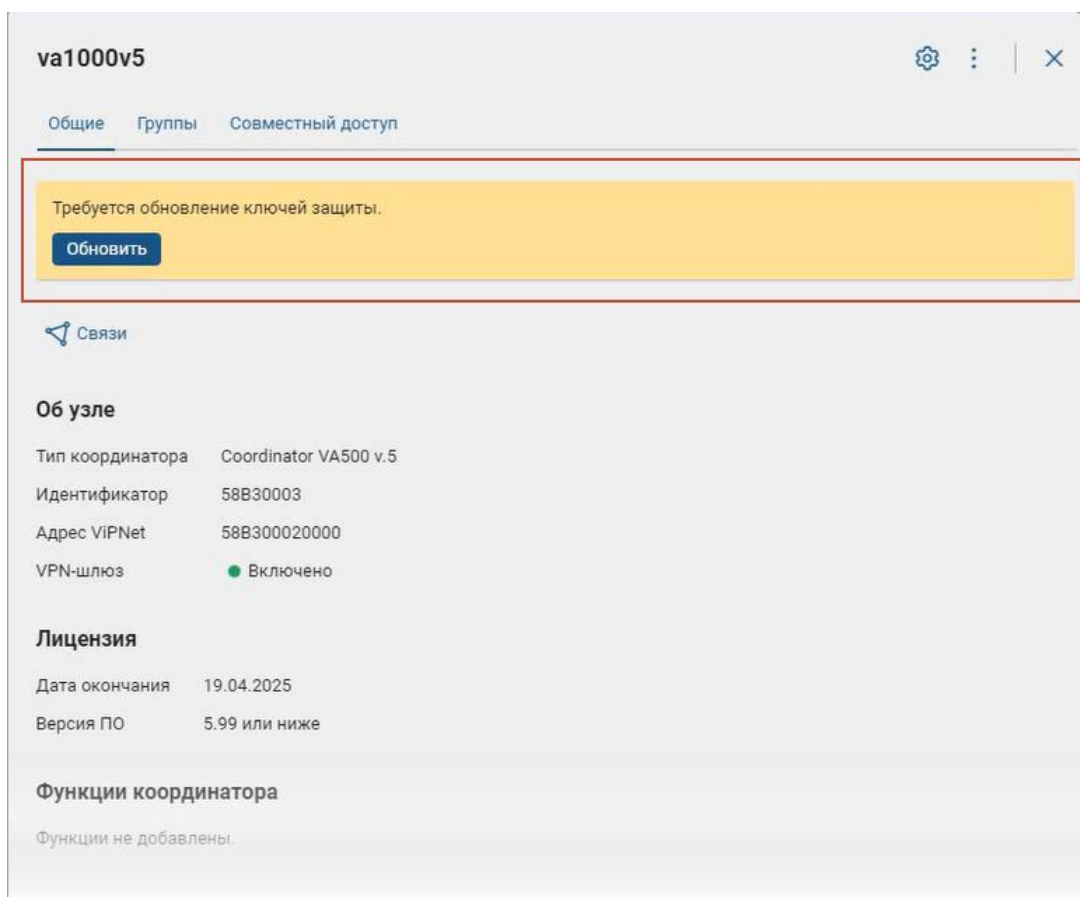


Рисунок 56. Обновление ключей узлов поколения ViPNet 5 (выборочно)

- локально, если по каким-то причинам отправить обновление нельзя. Для этого создайте и установите новые дистрибутивы ключей. Если вы создадите дистрибутив ключей для локального обновления, то обновить удаленно ключи защиты будет уже нельзя.

- 7 После смены мастер-ключей защиты обновлений суперадминистратор **включает автоматическую отправку обновлений ключей**.

Смена мастер-ключа ключей обмена и мастер-ключа ключей обмена для технической связи

Вручную вы можете сменить мастер-ключи только на алгоритмах ГОСТ 34.12-2018 «Магма» и «Кузнечик». Если мастер-ключи на алгоритме ГОСТ 28147–89, создать новые мастер-ключи таким образом нельзя. Мастер-ключ ключей обмена на алгоритме ГОСТ 28147–89 меняется автоматически при смене мастер-ключа сети.

- 1 Нажмите  **Создать новый мастер-ключ**.

- 2 Установите срок действия мастер-ключа.

По умолчанию — 1 год и 3 месяца. Датой начала действия мастер-ключа устанавливается текущая дата и ее нельзя изменить.

- 3 Нажмите **Сохранить**. Новый мастер-ключ примет статус **Не используется**.

- 4 Назначьте новый мастер-ключ текущим:

- 4.1 Выберите мастер-ключ.

- 4.2 Нажмите  и выберите **Сделать текущим**.

- 4.3 Установите дату ввода в эксплуатацию.

Задавайте дату с учетом времени на доставку обновлений на удаленно расположенные сетевые узлы. Минимум — через два дня, по умолчанию — через 15 дней от текущей даты. В этот период на сетевых узлах обновляется информация о новых мастер-ключах. Считается, что за это время все сетевые узлы организации успеют принять обновления ключей.

- 4.4 Нажмите **Сохранить**.

Новый мастер-ключ примет статус **Будет текущим** с и будет указана выбранная дата ввода в эксплуатацию. У старого мастер-ключа будет статус **Используется до** и будет указана дата на 1 день позже даты ввода в эксплуатацию нового ключа.

Если требуется отменить смену мастер-ключа, вы можете сделать это не позднее, чем за 24 часа до ввода их в эксплуатацию. Для этого на панели справа нажмите **Отменить смену мастер-ключа**. После этого у мастер-ключа появится статус **Не используется**.

Смена мастер-ключей сети

Мастер-ключи сети — ключи, которые администратор ViPNet Prime использует для формирования симметричных ключей пользователей и узлов поколения **ViPNet 4**. Набор мастер-ключей сети содержит:

- мастер-ключ персональных ключей;

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

Мастер-ключи сети создаются автоматически при инициализации ViPNet Prime. На их основе создаются персональные ключи, ключи защиты и ключи обмена для узлов поколения ViPNet 4. По умолчанию срок действия мастер-ключей сети — 365 дней. За 14 дней до окончания срока действия мастер-ключей начнет отображаться уведомление о необходимости их смены.

В результате смены мастер-ключей сети также изменяются мастер-ключи обмена организаций на алгоритме ГОСТ 28147-89.

После смены мастер-ключей сети сменятся ключи для работы узлов по алгоритму ГОСТ 28147-89 во всех организациях сети.



Внимание! Полностью ознакомьтесь с инструкцией перед тем, как начинать смену мастер-ключей сети.

Порядок смены мастер-ключей



Внимание! При смене мастер-ключей сети становятся недоступны узлы поколения ViPNet 5 (с * .ds5) с ViPNet Client 5 for Linux 5.0.2 и ниже, ViPNet Client 5 for Windows 5.1 и ниже, ViPNet Client 5 for Android 5.2.1, ViPNet Client 5 for iOS 5.1.0 и ниже и ViPNet Client 5 for macOS 5.1.0 и ниже.

Для восстановления связи с узлом создайте и установите дистрибутив ключей на узле вручную.

Порядок действий при смене мастер-ключей сети

- 1 Подготовьте сеть к смене мастер-ключей сети.
- 2 Убедитесь в наличии резервного набора персональных ключей на важных и труднодоступных узлах.
- 3 Смените мастер-ключи персональных ключей.
- 4 Убедитесь, что персональные ключи доставлены и приняты на узлах. Это может занять от 3 часов до нескольких дней в случае возникновения трудностей с доставкой ключей на узел.
- 5 Отключите автоматическую отправку справочников и ключей.
- 6 Смените мастер-ключи ключей обмена и защиты.
- 7 Убедитесь, что ключи обмена и защиты доставлены и приняты на узлах. Ключи будут приняты на узлах не ранее, чем через 48 часов.

До установки на узел новых ключей защиты и ключей обмена вы можете:

- изменять конфигурацию сети;

- расшифровать письма в ViPNet Деловая почта на узле пользователя, зашифрованные на старых ключах обмена.



Внимание! В процессе смены ключей на узлах не отправляйте обновление ПО на узлы, не изменяйте топологию сети, не настраивайте сеть, чтобы избежать ошибок.

Подготовка к смене мастер-ключей

После начала смены мастер-ключей сети, ее нельзя прервать или отменить, поэтому соблюдайте рекомендации:

- Проверьте сетевую связность узлов. Для этого вы можете отправить на узлы обновления справочников и ключей и убедиться, что они приняты.
- Обновите ПО на узлах до указанных в разделе [Совместимые продукты ViPNet](#) для поколения ViPNet 4.
- Выберите промежуток времени, в течение которого будете проводить смену мастер-ключей. Сообщите всем пользователям и администраторам сети ViPNet о планируемом обновлении ключей и сроках его проведения.
- Сообщите пользователям ViPNet Client for Windows версии 4.5.3, что после смены мастер-ключей им потребуется задать новый пароль для входа в ViPNet Client.
- Если вы используете ViPNet Coordinator IG в режиме **Межсетевой экран уровня промышленной сети (тип «Д»)**, смените режим на **Межсетевой экран сети (тип «А», тип «Б»)**.
- Не вносите изменения в структуру сети и не отправляйте вручную обновления справочников и ключей до окончания смены мастер-ключей.
- При смене мастер-ключей убедитесь, что сначала дошли все ключи до клиентских узлов, а потом до координаторов, иначе после смены ключей на координаторе, на клиентском узле конверт с новыми ключами не расшифруется.
- Ознакомьтесь с рекомендациями по смене мастер-ключей в документации на используемые продукты ViPNet.
- Совместно с администраторами сетевых узлов [убедитесь, что у каждого пользователя на узле есть резервный набор персональных ключей](#) (далее — РНПК).

На узле устанавливаются полученные ключи и расшифровывается новый персональный ключ при помощи ключа из РНПК, сгенерированного из старого мастер-ключа персональных ключей. Без РНПК новые ключи на узлах не вступят в действие.

Если у пользователя нет резервного набора персональных ключей, обновления справочников и ключей не будут применены на узле, так как не будут расшифрованы. На узле придется вручную установить дистрибутив ключей. Проверить наличие РНПК на узле можно только вручную, подробнее см. в документации на ПО ViPNet, установленное на узлах.

- Пользователям необходимо расшифровать все сообщения программы ViPNet Деловая почта, включая архивные. После того как на узлах будут установлены ключи, созданные на основе

новых мастер-ключей, сообщения, зашифрованные на старых ключах, будет невозможно прочитать. Подробнее см. в документации ViPNet Деловая почта.

- Сохраните дистрибутивы ключей для узлов с ролью «Деловая Почта», чтобы избежать потери зашифрованных писем, если пользователи не расшифровали их.
- Дистрибутив ключей придется развернуть вручную:
 - если для аутентификации пользователя на сетевом узле используется внешнее устройство;
 - если для пользователей ViPNet Client когда-либо были заданы минимальные полномочия, из-за чего на узле отсутствует РНПК.

Проверка наличия РНПК на сетевых узлах

При создании дистрибутива ключей в него помещается резервный набор персональных ключей (далее — РНПК) — набор из нескольких персональных ключей, который создает ViPNet Prime для каждого пользователя сети ViPNet на основе одного и того же мастер-ключа. В составе дистрибутива ключей РНПК попадает на каждый узел и хранится там. При смене мастер-ключей сети РНПК позволяет расшифровать полученный мастер-ключ персональных ключей.

На узле устанавливаются полученные ключи и новый персональный ключ расшифровывается при помощи ключа из РНПК, сгенерированного из старого мастер-ключа персональных ключей. Без РНПК новые ключи на узлах не вступят в действие.

Если у пользователя нет резервного набора персональных ключей, обновления справочников и ключей не будут применены на узле, так как не будут расшифрованы. На узле придется вручную установить дистрибутив ключей. Проверить наличие РНПК на узле можно только вручную.

Клиенты

На узлах с ViPNet Client РНПК хранится на узле, если:

- дистрибутив ключей был создан в ViPNet Prime или в ViPNet Administrator 4.6.1 и выше,
- после последней установки дистрибутива ключей на узле нет и не было установлено минимальных полномочий.

Если одно из этих требований не выполняется, установите дистрибутив ключей на узле вручную до или после смены мастер-ключей сети.

Координаторы и Другие узлы

Вы можете проверить наличие РНПК на шлюзах безопасности и узлах квантовой сети с помощью команды `iplir show key-info`: если в выводе команды в секции `Spare personals keys set info` есть информация о ключах, значит на узле есть РНПК. Если информации нет, после смены мастер-ключей сети вам потребуется вручную установить дистрибутив ключей на узле.

Смена мастер-ключей персональных ключей

- 1 Подготовьте сеть к смене мастер-ключей сети.
- 2 Войдите в ViPNet Prime как суперадминистратор.
- 3 Убедитесь, что на устройствах установлено верное и одинаковое время с учетом часовых поясов.
- 4 Выберите ViPNet VPN  > Мастер-ключи.
- 5 Выберите Мастер-ключи сети.
- 6 Нажмите  Сменить мастер-ключи.
- 7 Ознакомьтесь с уведомлением и нажмите **Сменить**. На узлы поколения ViPNet 4 отправятся новые персональные ключи.
- 8 Проверьте в журнале транспортных конвертов, что конверты с персональными ключами отправлены.
- 9 Проверьте статус отправленных на узлы персональных ключей, убедитесь, что у них статус **Приняты**. Для этого на панели сверху нажмите **Проверить статус ключей**, нажмите **Скачать**.

Скачается файл в формате CSV с таблицей, в которой вы можете просмотреть, какой статус у персональных ключей на каждом узле. Для удобства работы с информацией в файле открывайте файл в табличном представлении.

VNP ID	Имя узла	Статус персональных ключей	Статус ключей обмена и защиты
40CE0003	HW4	Приняты	Приняты
40CE0002	Control Center	Приняты	Приняты

Рисунок 57. Пример отчета о смене ключей на узлах

Проверяйте статус ключей не раньше, чем через 3 часа после начала смены мастер-ключей и назначения даты и времени применения ключей, так как ключи отправляются на все узлы постепенно.

Статусы персональных ключей:

- **Не отправлены** — значение по умолчанию. Найдите причину и повторно отправьте ключи и справочники вручную, если статус ключа не менялся в течение суток после смены персональных ключей.
- **Отправлены** — ключи отправлены на узлы. Если статус ключа не менялся в течение суток после отправки персональных ключей — конверт не был доставлен на узел. Повторно отправить персональные ключи на узел нельзя, поэтому повторно разверните дистрибутив ключей на узле.
- **Доставлены** — получена ответная квитанция от узла о доставке конверта с ключами.
- **Приняты** — получена ответная квитанция от узла об обработке конверта с ключами. Статус может быть установлен не раньше даты ввода в действие.
- **Не приняты** — получена ответная квитанция от узла об ошибке при обработке конверта с ключами.

Если персональный ключ не применился на узле, установите дистрибутив ключей на узле вручную.

- 10 Убедитесь, что у всех персональных ключей статус **Принято**. На вкладке **Мастер-ключи сети** у мастер-ключа персональных ключей должен быть статус **Текущий**.

Смена мастер-ключей ключей обмена и защиты



Внимание! Не планируйте время смены ключей обновлений и защиты, если какие-то устройства не приняли персональные ключи. Убедитесь, что устройства, у которых статус персональных ключей отличается от **Приняты**, включены и работоспособны. Если ключи не приняты, обратитесь к документации на управляемые продукты, изучите возможные неполадки и способы их решения.

Если какие-то узлы не получили персональные ключи, но получают ключи обмена и защиты, они не смогут их расшифровать, потребуется устанавливать дистрибутив ключей вручную.

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 Отключите автоматическую отправку справочников и ключей.
- 3 Выберите **ViPNet VPN**  > **Мастер-ключи**.
- 4 Выберите **Мастер-ключи сети**.
- 5 Выберите мастер-ключ со статусом **Ввод в действие** и на панели справа нажмите **Запланировать**.
- 6 Запланируйте отложенное обновление справочников и ключей, содержащее новые ключи обмена и защиты: выберите дату и время отложенной установки мастер-ключей, нажмите **Сохранить** и подтвердите дату отложенной установки. До даты и времени отложенной установки должно быть не меньше 48 часов и не больше срока действия мастер-ключей. По умолчанию устанавливается 48 часов до отложенной установки.



Внимание! Для одновременного перехода всех узлов сети на новые мастер-ключи рекомендуется указывать время перехода 00:00 UTC (+0). Не рекомендуется изменять это время. При выборе другого времени может нарушиться связность сети между узлами до вступления в действие мастер-ключа сети.

Не откладывайте установку новых ключей надолго, так как в это время будет отключена автоматическая отправка справочников и ключей.

После выбора даты и времени смены ключей узлы будут недоступны для управления из ViPNet Prime.

Узлы поколения ViPNet 5, использующие шифрование по ГОСТ 28147-89, тоже получают ключи обмена и установят их в выбранное время.

Статус новых мастер-ключей изменится на **Текущий**, старых — на **Не используется**.

- 7 Проверьте в журнале транспортных конвертов, что конверты с ключами защиты и обновлений отправлены.
- 8 В день, который вы указали как дату отложенной установки, после наступления времени установки мастер-ключей проверьте статус отправленных на узлы ключей защиты и обмена, убедитесь, что у них статус **Приняты**. Для этого на панели сверху нажмите **Проверить статус ключей**, нажмите **Скачать**.

Скачается файл в формате CSV с таблицей, в которой вы можете просмотреть, какой статус у ключей защиты и ключей обмена на каждом узле.



Внимание! Убедитесь, что устройства, у которых статус ключей обмена и защиты отличается от **Приняты**, включены и работоспособны. Если ключи не приняты, обратитесь к документации на управляемые продукты, изучите возможные неполадки и способы их решения.

Статусы ключей обмена и защиты:

- **Не отправлены** — значение по умолчанию. Найдите причину и повторно отправьте ключи и справочники вручную, если статус ключа не менялся в течение суток после задания даты установки ключей обмена и защиты.
- **Отправлены** — ключи отправлены на узлы. Если статус ключа не менялся в течение суток после задания даты установки ключей обмена и защиты — проверьте работоспособность узла и тракта передачи до узла, повторно отправьте справочники и ключи вручную.
- **Доставлены** — получена ответная квитанция от узла о доставке конверта с ключами.
- **Приняты** — получена ответная квитанция от узла об обработке конверта с ключами.
- **Не приняты** — получена ответная квитанция от узла об ошибке при обработке конверта с ключами.

Если персональный ключ не применился на узле, независимо от статуса ключей обмена и защиты, установите дистрибутив ключей на узле вручную.

9 Включите автоматическую отправку справочников и ключей.

Чтобы ускорить отправку новых справочников и ключей, отправьте их вручную на узлы поколения ViPNet 5 (см. [Обновление справочников и ключей](#)). Автоматически и гарантированно обновления отправятся в течение 60 минут.



Внимание! Не удаляйте неиспользуемые мастер-ключи сети минимум в течение суток после смены, так как в организациях с узлами поколения ViPNet 5 могут использоваться мастер-ключи ключей обмена на алгоритме ГОСТ 28147-89, производные от мастер-ключа сети. Мастер-ключи ключей обмена действуют еще сутки после смены мастер-ключей сети. Если вы удалите неиспользуемый мастер-ключ сети, может пропасть связь между узлами.

Чтобы удалить неиспользуемые мастер-ключи, убедитесь, что прошли сутки после смены мастер-ключей сети, выберите неиспользуемый мастер-ключ и на панели справа нажмите , подтвердите удаление.

Если на одном узле статус ключей **Приняты**, а на другом — любой другой статус, узлы не смогут взаимодействовать.

Если у вас создана цепочка серверов соединений и узел, который доступен напрямую, принял ключи раньше, чем узлы, использующие его в качестве сервера соединений, ViPNet Prime не будет получать конверты от узлов, которые находятся за сервером соединений, до смены ключей на них.

Если на узле возникли проблемы с обновлением ключей, создайте заново дистрибутив ключей и передайте его пользователям и администраторам узлов для установки вручную.

Если перед сменой мастер-ключей вы меняли режим работы ViPNet Coordinator IG, смените режим работы координатора обратно на **Межсетевой экран уровня промышленной сети (тип «Д»)**.

Если мастер-ключи сменились, но узел не получает справочники и ключи

- 1 В журнале событий найдите событие отправки ключей защиты и обмена на узел, посмотрите дату и время события.
- 2 В журнале транспортных конвертов по дате и времени найдите конверты с ключами, посмотрите статус конвертов.
- 3 Если персональные ключи **Приняты**, дата и время установки мастер-ключей уже наступила, а статусы конвертов с ключами защиты и обмена любые другие, кроме **Приняты**, проблема на узле.

Смена мастер-ключа доверенных организаций

Вы можете сменить мастер-ключ обмена с доверенной организацией, только если он на алгоритме ГОСТ 34.12-2018. Если мастер-ключ на алгоритме ГОСТ 28147-89, он сменится при смене мастер-ключей сети.

- 1 Войдите в ViPNet Prime как владелец организации.
- 2 Выберите **ViPNet VPN**  > **Доверенное взаимодействие** > **Организации**.
- 3 Выберите доверенную организацию.
- 4 Справа в разделе **Мастер-ключ** нажмите .
- 5 Установите дату окончания действия мастер-ключа.
- 6 Нажмите **Сохранить**. Мастер-ключ примет статус **Не используется**.
- 7 Нажмите  > **Сделать текущим**.
- 8 Установите дату ввода в эксплуатацию нового мастер-ключа.
- 9 Нажмите **Сохранить**. Будет отправлен запрос в доверенную организацию на смену мастер-ключа. Мастер-ключ примет статус **Ожидает подтверждения**.
- 10 В доверенной организации подтвердите смену мастер-ключа:
 - 10.1 Справа в уведомлении о запросе смены мастер-ключа нажмите **Подробнее**.

10.2 В окне **Запрос смены мастер-ключа** просмотрите информацию о мастер-ключе и нажмите **Подтвердить**.

Мастер-ключ примет статус **Будет текущим**.

11 Вы можете отменить смену мастер-ключа, для этого в доверенной организации подтвердите отмену смены мастер-ключа.

Смена межсетевого мастер-ключа

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 Для уменьшения нагрузки на сеть при смене нескольких межсетевых мастер-ключей [отключите автоматическую отправку ключей](#).
- 3 Выберите **ViPNet VPN**  > **Доверенное взаимодействие** > **Сети**.
- 4 Выберите межсетевое взаимодействие.
- 5 Если вы создаете новый межсетевой мастер-ключ:
 - 5.1 Справа в группе **Межсетевой мастер-ключ** нажмите  **Новый мастер-ключ**.
 - 5.2 Задайте дату окончания действия межсетевого мастер-ключа. По умолчанию 1 год и 3 месяца.
 - 5.3 Для межсетевого взаимодействия на алгоритмах ГОСТ 34.12-2018 «Магма» и «Кузнечик» выберите алгоритм шифрования **Магма** или **Кузнечик**.
 - 5.4 Нажмите **Скачать**.
 - 5.5 Передайте новый межсетевой мастер-ключ и пароль от него администратору доверенной сети для импорта и ввода в действие.
- 6 Если вы импортируете новый межсетевой мастер-ключ из доверенной сети:
 - 6.1 Справа в группе **Межсетевой мастер-ключ** нажмите **Загрузить**.
 - 6.2 Выберите полученный межсетевой мастер-ключ из доверенной сети и введите от него пароль.
 - 6.3 Нажмите **Сохранить**.
- 7 Одновременно с администратором доверенной сети введите в действие новый межсетевой мастер-ключ:
 - 7.1 Выберите новый межсетевой мастер-ключ. Он имеет статус **Не используется**.
 - 7.2 Нажмите  и выберите **Сделать текущим**:
 - Для межсетевого взаимодействия с шифрованием ГОСТ 34.12-2018 «Магма» и «Кузнечик» укажите дату ввода в эксплуатацию не раньше чем через двое суток.Вы сможете отменить смену мастер-ключа, если до ввода его в эксплуатацию осталось не менее 24 часов.

- Для межсетевого взаимодействия с шифрованием ГОСТ 28147-89 межсетевой мастер-ключ будет назначен текущим мгновенно.

Смена межсетевого мастер-ключа не изменяет межсетевую информацию — ее не требуется отправлять в доверенную сеть. Новые ключи будут отправлены автоматически.

Взаимодействие между организациями и защищенными сетями

В ViPNet Prime вы можете создавать взаимодействие:

- [с доверенными сетями](#) — межсетевое взаимодействие;
- [с организациями вашей сети](#) — межорганизационное взаимодействие.

Доверенные защищенные сети могут находиться под управлением ViPNet Administrator или ViPNet Prime.

Вы можете создать взаимодействие с доверенной сетью из любой организации вашей сети. Межсетевое взаимодействие создается для всех организаций сети сразу. Но для предоставления доступа к устройствам вашей организации необходимо создать еще и межорганизационное взаимодействие с организацией доверенной сети.

Если в вашей сети уже создано межсетевое взаимодействие с доверенной сетью для одной из организаций, для других вы можете так же создать запрос на взаимодействие с этой сетью, взаимодействие установится автоматически. Вам потребуется только отправить новую межсетевую информацию. Доверенная сеть будет отображаться в списке доверенных организаций в разделе

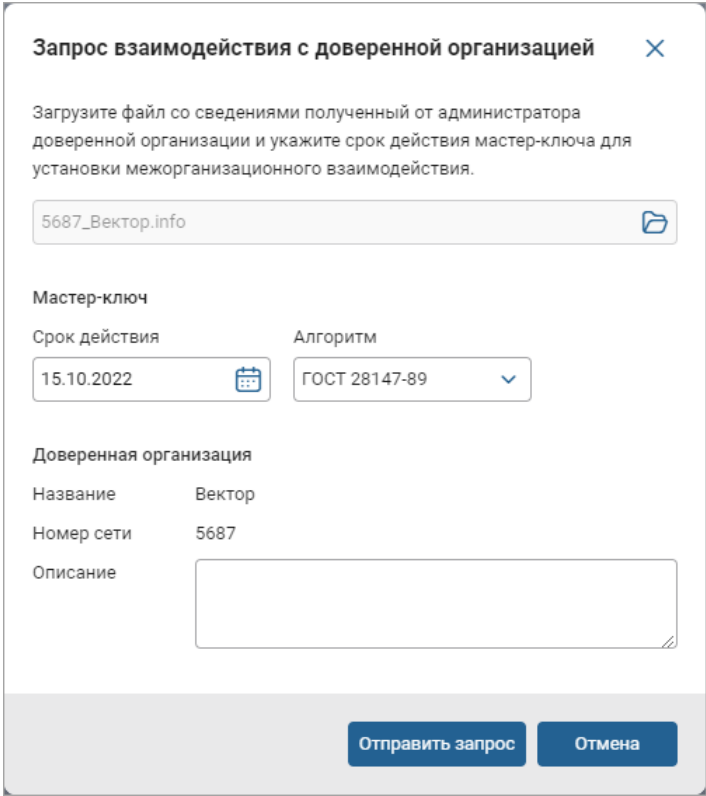
ViPNet VPN  > **Доверенное взаимодействие** > **Организации**, но как одна организация, независимо от количества организаций в доверенной сети, которые установили взаимодействие с вашей сетью.

Вы не можете выбирать организации доверенной сети, которым предоставляете доступ к вашим узлам или ресурсам: узлы доверенной сети, которые могут взаимодействовать с узлами вашей сети, предоставленными для совместного использования, выбирает администратор доверенной организации.

Создание взаимодействия между организациями одной сети

- 1 Войдите в ViPNet Prime как владелец организации.
- 2 Сохраните файл инициализации *.info с информацией о вашей организации:
 - 2.1 Выберите **ViPNet VPN**  > **Доверенное взаимодействие** > **Организации**.
 - 2.2 Нажмите **Скачать сведения для установки взаимодействия**.

- 2.3 Нажмите **Скачать файл сведений**. Файл инициализации *.info появится в загрузках браузера.
- 3 Передайте файл инициализации *.info администратору организации, с которой требуется установить взаимодействие.
- 4 Администратору другой организации необходимо загрузить файл инициализации *.info:
- 4.1 Выбрать организацию.
- 4.2 Выбрать **ViPNet VPN**  > **Доверенное взаимодействие** > **Организации**.
- 4.3 Нажать **Установить взаимодействие** и в списке выбрать **Из файла**.
- 4.4 В окне **Запрос взаимодействия с доверенной организацией**:
- 4.4.1 Загрузить файл инициализации *.info.
- 4.4.2 Задать алгоритм шифрования и срок действия мастер-ключа. По умолчанию 15 месяцев.
- 4.4.3 Нажать **Отправить запрос**. Статус взаимодействия изменится на **Запрошено**.



Запрос взаимодействия с доверенной организацией ✕

Загрузите файл со сведениями полученный от администратора доверенной организации и укажите срок действия мастер-ключа для установки межорганизационного взаимодействия.

5687_Вектор.info 

Мастер-ключ

Срок действия: 15.10.2022  Алгоритм: ГОСТ 28147-89 

Доверенная организация

Название: Вектор

Номер сети: 5687

Описание:

Отправить запрос **Отмена**

Рисунок 58. Запрос взаимодействия с доверенной организацией

- 5 Вы получите запрос на подтверждение установки взаимодействия со статусом **Требуется подтверждения**. Подтвердите взаимодействие с организацией:
- 5.1 Выберите **ViPNet VPN**  > **Доверенное взаимодействие** > **Организации**.
- 5.2 Выберите организацию и справа нажмите **Установить взаимодействие**. Взаимодействие примет статус **Установлено**.

После создания взаимодействия с организацией вы можете изменить название взаимодействия с организацией, отображаемое в вашем списке доверенных организаций. При этом, если у организации изменится название в ViPNet Prime, в вашем списке доверенных организаций останется прежнее название этой организации.

Порядок создания взаимодействия между сетями

- 1 [Создайте запрос на взаимодействие с доверенной сетью.](#)
 - 2 Как суперадминистратор ViPNet Prime [создайте межсетевое взаимодействие на выбранных мастер-ключах](#):
 - 2.1 Подтвердите запрос на межсетевое взаимодействие.
 - 2.2 Выберите межсетевой шлюз:
 - [поколения ViPNet 4](#) (при создании взаимодействия на мастер-ключах ГОСТ 28147-89) или [поколения ViPNet 5](#) (при создании взаимодействия на мастер-ключах ГОСТ 28147-89 или ГОСТ 34.12-2018);
 - из списка координаторов организации Core Network;
 - с подключением напрямую к внешней сети.
 - 2.3 Выберите алгоритм шифрования трафика.
-
- 

Внимание! При выборе алгоритма по ГОСТ 34.12-2018 вы сможете передавать межсетевую информацию только вручную.
-
- 2.4 Создайте два файла и передайте их администратору доверенной сети:
 - файл с межсетевым мастер-ключом *.key или *.bin;
 - файл с межсетевой информацией *.lzh.
 - 3 Администратор доверенной сети загружает переданные ему файлы и формирует файл с ответной межсетевой информацией. Подробнее см. [Завершение установки взаимодействия с сетью](#) или в документации ViPNet Administrator.
 - 4 В ViPNet Prime загрузите файлы с межсетевой информацией и межсетевой мастер-ключ, полученные от администратора доверенной сети. Если вы создали мастер-ключ и его установил администратор доверенной сети, вам не нужно загружать новый мастер-ключ.
 - 5 Если необходимо, [инициируйте взаимодействие с этой же сетью для других организаций вашей сети.](#)
 - 6 [Обработайте межсетевую информацию и отправьте ее в доверенную сеть.](#)
 - 7 [Предоставьте объекты для совместного использования с доверенной сетью и создайте связи с объектами, которые вам предоставил администратор доверенной сети.](#)

Особенности взаимодействия с сетью под управлением ViPNet Administrator

- Иницилируйте межсетевое взаимодействие с сетью под управлением ViPNet Administrator 4.6.11.
- В качестве шлюзового координатора используйте координатор из организации Core Network.
Если сеть под управлением ViPNet Prime создана с узлом центра управления поколения ViPNet 5 (с лицензией Client for Linux v.5), чтобы автоматически обмениваться межсетевой информацией, на узле центра управления используйте ViPNet Client 5 for Linux версии 5.1.3 и выше. Шлюзового координатора выберите [поколения ViPNet 4](#) или [поколения ViPNet 5](#).
- Для создания межсетевого взаимодействия на компьютере с ViPNet Administrator должен быть установлен один из клиентов:
 - ViPNet Client 5 for Windows версии 5.1,
 - ViPNet Client for Windows версии 4.5.3 hotfix 7,
 - ViPNet Client for Windows версии 4.5.5 hotfix 9.
- В качестве шлюзового координатора не выбирайте координатор центра управления (Core Coordinator). Это может привести к превышению допустимой нагрузки на координатора.
- В сети под управлением ViPNet Prime в качестве DNS-сервера вы можете использовать DNS-сервер из доверенной сети под управлением ViPNet Administrator, даже если этот узел не поддерживает функции DNS-сервера в ViPNet Prime.
- В ViPNet Prime межсетевая информация должна быть [обработана вручную](#).

В ViPNet Administrator администратор должен учитывать:

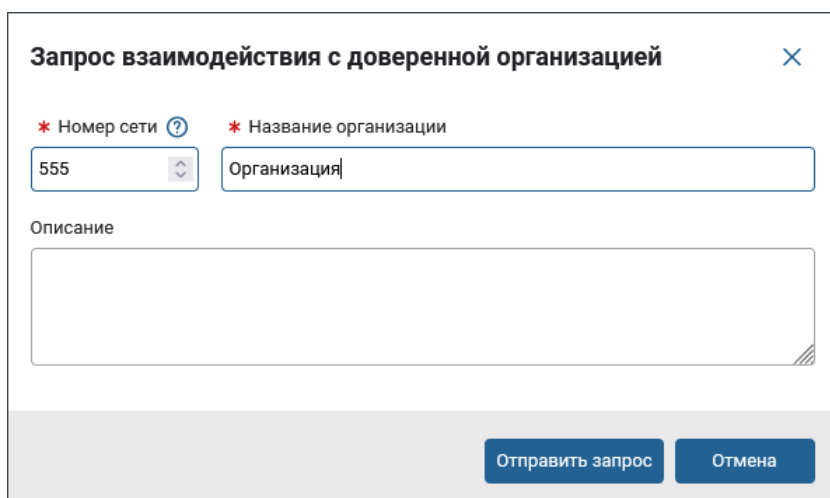
- ViPNet Prime не сможет загрузить или обновить межсетевую информацию, если в межсетевом взаимодействии участвуют:
 - узлы, у которых несколько пользователей;
 - пользователи с несколькими узлами, один из которых координатор или координатор без функции VPN-сервера;
 - узлы без пользователей;
 - IP-адреса, туннелируемые узлами, которые не поддерживают функцию туннелирования в ViPNet Prime.
- В ViPNet Administrator отсутствует разделение сети на организации. Объекты из нескольких доверенных организаций из сети под управлением ViPNet Prime отображаются в общем списке объектов доверенной сети с одинаковым номером сети.

Создание запроса на взаимодействие с сетью

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите ViPNet VPN  > Доверенное взаимодействие > Организации.
- 3 Нажмите **Установить взаимодействие** и в списке выберите **По номеру сети**.
- 4 В окне **Запрос взаимодействия с доверенной организацией** введите:
 - номер защищенной сети, с которой хотите установить взаимодействие;
 - название организации, которое будет отображаться в списке доверенных организаций;
 - краткое описание запроса.



Внимание! После установки межсетевого взаимодействия изменить название доверенной организации, которое отображается в списке **Организации**, невозможно.



Запрос взаимодействия с доверенной организацией X

* Номер сети ? * Название организации

555 Организация

Описание

Отправить запрос Отмена

Рисунок 59. Отправка запроса на установку межсетевого взаимодействия

- 5 Нажмите **Отправить запрос**. Статус взаимодействия изменится на **Запрошено**.

Создание взаимодействия между сетями

Вы можете создать взаимодействие:

- С защищенными сетями под управлением ViPNet Administrator.

С такими сетями необходимо создавать взаимодействие на мастер-ключах [поколения ViPNet 4](#) (алгоритм шифрования [ГОСТ 28147–89](#)). Для этого:

- в качестве узла центра управления требуется клиент [поколения ViPNet 4](#) или ViPNet 5 (с [ViPNet Client 5 for Linux версии 5.1.3 и выше](#)),
- в качестве шлюзового координатора — координатор поколения ViPNet 4 или [ViPNet 5](#).

- С защищенными сетями под управлением ViPNet Prime.

С такими сетями вы можете создать взаимодействие на мастер-ключах поколения [ViPNet 4](#) или [ViPNet 5](#) (алгоритмы шифрования ГОСТ 28147-89 и ГОСТ 34.12-2018):

- Для [межсетевого взаимодействия с шифрованием по алгоритмам ГОСТ 28147-89](#) в качестве узла центра управления требуется клиент поколения ViPNet 4 или ViPNet 5 (ViPNet Client 5 for Linux версии 5.1.3 и выше), в качестве шлюзового координатора — координатор поколения ViPNet 4 или ViPNet 5.
- Для [межсетевого взаимодействия с шифрованием по алгоритмам ГОСТ 34.12-2018](#) «Магма» и «Кузнечик» (режим шифрования «Не задан» в параметрах доверенной сети) в качестве узла центра управления требуется клиент поколения ViPNet 5, в качестве шлюзового координатора — координатор поколения ViPNet 5.

Шифрование трафика по алгоритмам ГОСТ 34.12-2018 «Магма» и «Кузнечик» при взаимодействии защищенных сетей под управлением ViPNet Prime возможно только в версии 1.9.5 и выше.

Если хотя бы с одной стороны межсетевого взаимодействия используется клиент поколения ViPNet 4 в качестве узла центра управления, создавайте межсетевое взаимодействие с шифрованием по алгоритмам ГОСТ 28147-89.

Если в качестве узла центра управления вы используете ViPNet Client 5 for Linux версии 5.1.3 и выше, обновите шлюзовой координатор до версий: ViPNet Coordinator HW 4 версии 4.5.8 или ViPNet Coordinator HW 5 версии 5.3.3.

На мастер-ключах ГОСТ 28147-89

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 Создайте межсетевую информацию и межсетевой мастер-ключ для передачи администратору доверенной сети:
 - 2.1 Перейдите в раздел **ViPNet VPN**  > **Доверенное взаимодействие** > **Сети**.
 - 2.2 Подтвердите создание взаимодействия с доверенной сетью. Для этого в списке доверенных сетей выберите сеть и нажмите **Установить взаимодействие**.

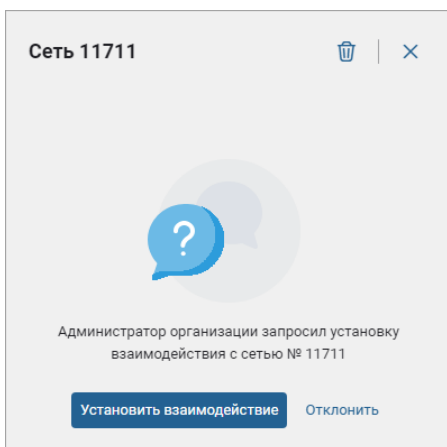


Рисунок 60. Подтверждение запроса на взаимодействие с сетью

2.3 Укажите координатор, который будет выполнять роль межсетевого шлюза:

2.3.1 Убедитесь, что для координатора создан и установлен дистрибутив ключей, и включены функции VPN-шлюза. В свойствах координатора на вкладке **Общие** в списке поддерживаемых функций присутствует функция межсетевого шлюза.

2.3.2 В окне **Параметры доверенной сети** в поле **Межсетевой шлюз** выберите координатор поколения **ViPNet 4** или **ViPNet 5**. Не рекомендуется выбирать Core Coordinator, это может привести к превышению допустимой нагрузки на координатор.



Внимание! Если в одной доверенной сети в качестве межсетевого шлюза выбран ViPNet Coordinator KB, то запрещается использовать ViPNet Coordinator KB в качестве межсетевого шлюза в другой доверенной сети.

2.3.3 В поле **Режим шифрования для взаимодействия с сетью** выберите алгоритм шифрования трафика другой сети **ГОСТ 28147-89**.

2.3.4 Нажмите **Сохранить**.

Параметры доверенной сети

Номер сети: 22

* Межсетевой шлюз: связь с 222

* Режим шифрования для взаимодействия с сетью: ГОСТ 28147-89

Описание: оп

Сохранить Отмена

Рисунок 61. Выбор шлюзового координатора

2.4 Сохраните межсетевой мастер-ключ и межсетевую информацию для доверенной сети:

2.4.1 В группе **Межсетевая информация** нажмите **Скачать**. Файл с межсетевой информацией (<номер своей сети>-<номер доверенной сети>.lzh) загрузится на компьютер.

2.4.2 В группе **Межсетевой мастер-ключ** нажмите **Скачать**.

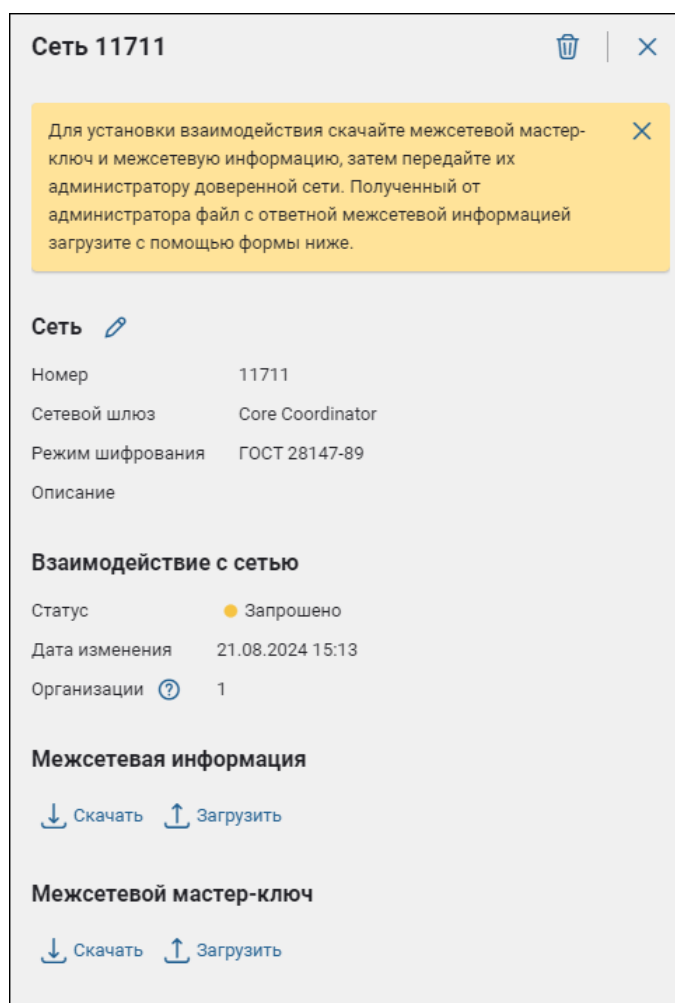


Рисунок 62. Создание межсетевой информации и межсетевого мастер-ключа

2.4.3 Скопируйте пароль от файла с межсетевым мастер-ключом. Для этого в окне **Скачивание межсетевого мастер-ключа** напротив поля **Пароль от файла межсетевого мастер-ключа** нажмите **Копировать**.

2.4.4 Нажмите **Скачать**. Файл с межсетевым мастер-ключом (`net_<номер сети>.key`) загрузится на компьютер.

Рисунок 63. Экспорт межсетевого мастер-ключа

- 3 Передайте межсетевой мастер-ключ и межсетевую информацию администратору доверенной сети доверенным способом.

На мастер-ключах ГОСТ 34.12-2018

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 Выберите ViPNet VPN  > Доверенное взаимодействие > Организации.
- 3 Выберите номер сети и нажмите **Установить взаимодействие**.
- 4 В запросе на межсетевое взаимодействие укажите параметры доверенной сети:
 - 4.1 В качестве межсетевого шлюза выберите координатор, который подключен напрямую к внешней сети. В списке доступны только координаторы из организации Core Network. Не рекомендуется выбирать Core Coordinator, это может привести к превышению допустимой нагрузки на координатор.



Внимание! Если в одной доверенной сети в качестве межсетевого шлюза выбран ViPNet Coordinator KB 5, запрещается использовать ViPNet Coordinator KB 4 или KB 5 в качестве межсетевого шлюза в другой доверенной сети.

- 4.2 Выберите режим шифрования **Не задан** — для шифрования по алгоритмам ГОСТ 34.12-2018 «Магма» и «Кузнечик».
- 4.3 Нажмите **Сохранить**.
- 5 Скачайте файл с межсетевым мастер-ключом:
 - укажите дату окончания действия межсетевого мастер-ключа и алгоритм шифрования **Магма** или **Кузнечик**.
 - скопируйте пароль от межсетевого мастер-ключа.
 - нажмите **Скачать ключ**, скачается файл *.bin.

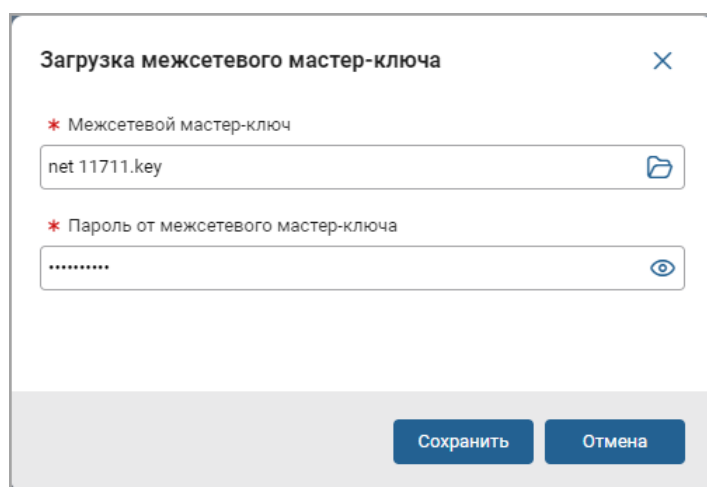
- 6 Скачайте файл с межсетевой информацией (*.lzh).
- 7 Передайте скачанные файлы администратору доверенной сети вместе с паролем от межсетевого мастер-ключа доверенным способом.

Завершение установки взаимодействия с сетью

Администратор другой сети принял и обработал полученную от вас межсетевую информацию, а затем передал вам файл с ответной межсетевой информацией. [Примите ответную информацию и обработайте ее.](#)

Чтобы завершить установку взаимодействия с доверенной сетью:

- 1 Получите у администратора доверенной сети файл, который содержит ответную межсетевую информацию (*.lzh).
- 2 Войдите в ViPNet Prime как суперадминистратор.
- 3 В ViPNet VPN  > **Доверенное взаимодействие** > **Сети** выберите сеть.
- 4 На панели сверху нажмите **Загрузить файл межсетевой информации**.
- 5 Выберите файл с межсетевой информацией, полученный от администратора доверенной сети.
- 6 Проверьте на актуальность дату формирования межсетевой информации и номер доверенной сети и нажмите **Загрузить**.
- 7 [Обработайте межсетевую информацию](#).
- 8 Если межсетевой мастер-ключ был создан в доверенной сети, загрузите его:
 - 8.1 В группе **Межсетевой мастер-ключ** нажмите **Загрузить**.
 - 8.2 Выберите файл с межсетевым мастер-ключом и введите от него пароль.



Загрузка межсетевого мастер-ключа

* Межсетевой мастер-ключ

net 11711.key

* Пароль от межсетевого мастер-ключа

.....

Сохранить Отмена

Рисунок 64. Загрузка межсетевого мастер-ключа

Если при установке межсетевого взаимодействия с доверенной сетью статус длительное время имеет значение **В обработке**, убедитесь, что справочники и ключи дошли до узлов управления

и шлюзового координатора. Для этого выберите **ViPNet VPN**  > **Журнал транспортных конвертов** (для ключей поколения ViPNet 4) или **Управление организацией**  > **Журнал транспортных конвертов** (для ключей поколения ViPNet 5). Если ключи и справочники не дошли до узлов, попробуйте отправить их снова.

Когда в своей сети будут приняты обновления справочников, взаимодействие с доверенной сетью примет статус **Установлено**. При этом автоматически установится связь между межсетевыми шлюзами.

После установки межсетевого взаимодействия вы сможете [установить связи с клиентами, пользователями и координаторами доверенной сети](#).

Обработка межсетевой информации

Для защиты сети под управлением ViPNet Prime при получении межсетевой информации из доверенной сети как суперадминистратор вручную обработайте межсетевую информацию. Автоматическая обработка межсетевой информации недоступна.

При загрузке файла с межсетевой информацией окно для ее обработки открывается автоматически, но вы можете закрыть его и вернуться позже к обработке межсетевой информации.

Чтобы обработать полученную межсетевую информацию:

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 В **ViPNet VPN**  > **Доверенное взаимодействие** > **Сети** выберите сеть, в которой требуется принять межсетевую информацию.
- 3 На уведомлении о получении межсетевой информации нажмите **Обработать**.

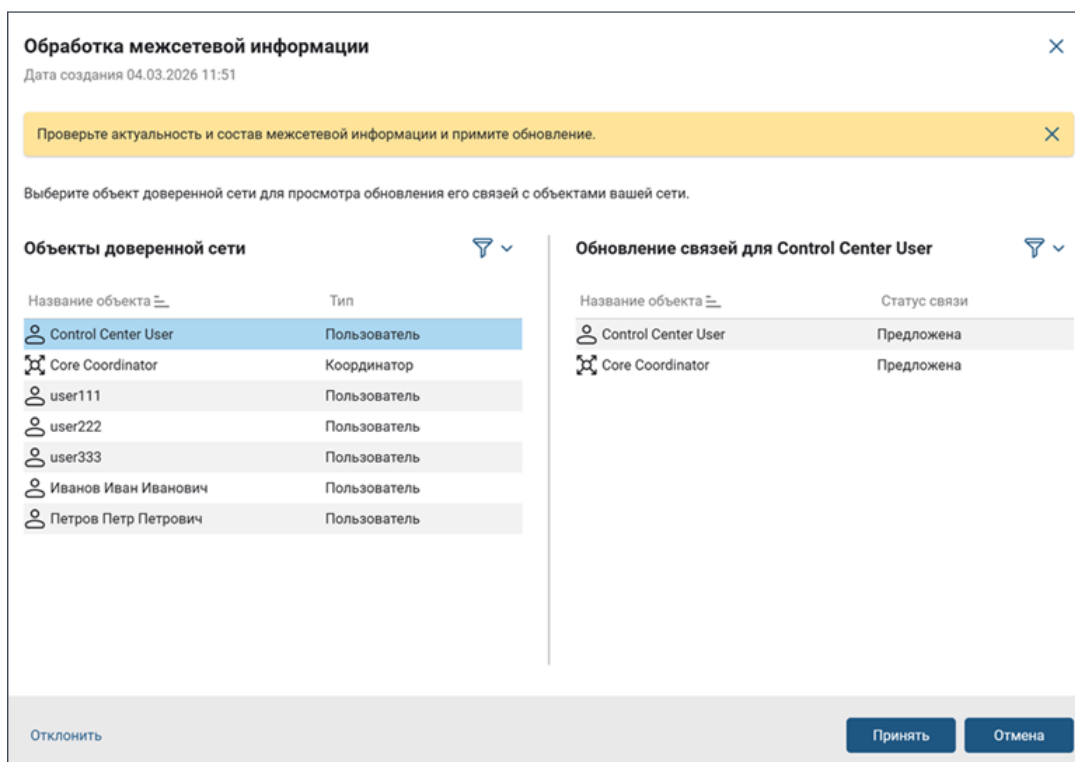


Рисунок 65. Обработка межсетевой информации

- 4 Выбирайте объекты доверенной сети в списке слева, чтобы просмотреть, какие связи изменены. Проверьте, что список связей справа актуальный. Если полученная межсетевая информация не последней версии, появится уведомление.

В списке отображаются измененные связи и их статусы. Если измененных связей нет, но межсетевая информация изменилась, например изменился шлюзовой координатор, список будет пустым.

При подтверждении межсетевой информации, которая была создана раньше, чем последняя принятая, будут потеряны все связи, которые изменились после создания этой межсетевой информации.

- 5 При просмотре связей вы можете воспользоваться фильтром по объектам доверенной сети или по статусам связей.

У связей могут быть статусы:

- **Запрещена** — запрещено создавать связь с узлом. Этот статус актуален только для взаимодействия с сетью под управлением ViPNet Administrator. Появляется, если администратор сети под управлением ViPNet Administrator запретил устанавливать связь с пользователем или узлом.
- **Подтверждена** — предложенную связь приняли в доверенной сети.
- **Предложена** — администратор доверенной сети создал новую связь.
- **Удалена** — администратор доверенной сети удалил связь с узлом или удалил узел из списка предоставленных для совместного доступа. Появляется, если ранее связь с узлом была установлена или запрошена. Связь удалится в обеих сетях.

- 6 Чтобы принять межсетевую информацию, нажмите **Принять**. Если вы не согласны с предлагаемыми изменениями, слева нажмите **Отклонить**. Изменить принятое решение будет невозможно, но вы можете попросить администратора доверенной сети отправить межсетевую информацию повторно. Управлять связями по-отдельности вы не можете.

Чтобы принять решение позже, нажмите **Отмена** или закройте окно.

Если взаимодействие еще не установлено, межсетевая информация может быть пустой, но ее необходимо принять, чтобы взаимодействие установилось.

После принятия межсетевой информации в ViPNet Prime обновятся связи с объектами доверенной сети.

- 7 После принятия межсетевой информации, [отправьте ответную межсетевую информацию](#).

Отправка межсетевой информации

При изменении параметров межсетевого взаимодействия с доверенной организацией или сетью (например, если вы изменили связи между объектами вашей сети и объектами доверенной сети) передайте новую межсетевую информацию для этой доверенной организации или сети.

Если для доверенной сети требуется создать или отправить межсетевую информацию, в модуле VPN на панели слева напротив раздела **Доверенное взаимодействие > Организации** отобразится значок оповещения.

Таблица 5. Особенности обмена межсетевой информацией

	ViPNet Client 5 for Linux версии 5.1.3 и выше		ViPNet Client 5 for Linux версии ниже 5.1.3	
	*.dst	*.ds5	*.dst	*.ds5
ГОСТ 28147-89	Межсетевая информация отправляется по сети	Межсетевая информация отправляется по сети	Межсетевая информация отправляется по сети	Межсетевая информация передается только вручную
ГОСТ 34.12-2018	Межсетевое взаимодействие недоступно	Межсетевая информация передается только вручную	Межсетевое взаимодействие недоступно	Межсетевая информация передается только вручную

Если в качестве узла центра управления используется ViPNet Client 5 for Linux версии ниже 5.1.3 с дистрибутивом ключей *.ds5, или ViPNet Client 5 for Linux версии 5.1.3 и выше с дистрибутивом ключей *.ds5, но межсетевое соединение установлено по ГОСТ 34.12-2018, вы можете передать межсетевую информацию только вручную, для этого скачайте её и передайте доверенным способом администратору доверенной сети.

Если в качестве узла центра управления в обеих сетях используется клиент [поколения ViPNet 4](#), вы можете отправить межсетевую информацию по защищенному каналу, установленному между вашей и доверенной сетью.

Если:

- в качестве узла центра управления используется ViPNet Client 5 for Linux версии 5.1.3 и выше с дистрибутивом ключей *.ds5,
- и межсетевое взаимодействие установлено по ГОСТ 28147-89,

вы можете отправить межсетевую информацию по защищенному каналу, установленному между вашей и доверенной сетью. Как настроить обмен межсетевой информацией по защищенному каналу см. в документах «ViPNet Client 5. Руководство администратора», раздел «Обмен межсетевой информацией с доверенными сетями».

Для автоматической отправки межсетевой информации необходимо, чтобы в качестве центра управления в обеих сетях были установлены клиенты одной версии. Особенности межсетевого взаимодействия с ViPNet Administrator см. в разделе [Особенности взаимодействия с сетью под управлением ViPNet Administrator](#).

Для отправки межсетевой информации по защищенному каналу, межсетевое взаимодействие с доверенной сетью должно быть в статусе **Установлено**.

Для отправки межсетевой информации:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 В ViPNet VPN  > **Доверенное взаимодействие** > **Организации** выберите организацию.
- 3 На панели справа в разделе **Межсетевая информация** нажмите  **Отправить**.

Чтобы отправить межсетевую информацию сразу в несколько организаций или сетей:

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 Выберите ViPNet VPN  > **Доверенное взаимодействие** > **Организации** или ViPNet VPN  > **Доверенное взаимодействие** > **Сети**.
- 3 Выберите организации или сети.
- 4 Нажмите **Отправить актуальную межсетевую информацию**.

Изменение шлюзового координатора

В качестве шлюзового координатора вы можете выбрать координаторы из организации Core Network с функциями VPN-шлюза, которые подключены к внешней сети напрямую:

- при взаимодействии сетей на алгоритмах ГОСТ 34.12-2018 «Магма» и «Кузнечик» — координаторы поколения [ViPNet 5](#).

- при взаимодействии сетей на алгоритмах ГОСТ 28147-89 — координаторы поколения ViPNet 4 и ViPNet 5.



Внимание! Не выбирайте координатор, который подключен через сервер соединений, в качестве шлюзового координатора. Иначе межсетевое взаимодействие не будет работать.

Для нового шлюзового координатора создайте и установите дистрибутив ключей. После развертывания координатора отправьте на него справочники и ключи вручную.

Чтобы изменить координатор своей сети, который используется в качестве шлюзового для связи с доверенной сетью:

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 Убедитесь, что для нового шлюзового координатора установлен или создан дистрибутив ключей.
- 3 На новом шлюзовом координаторе [включите функции VPN-шлюза](#).
- 4 [Отключите автоматическую отправку справочников и ключей](#).
- 5 Выберите **ViPNet VPN**  > **Доверенное взаимодействие** > **Сети**.
- 6 Выберите сеть.
- 7 На панели справа в группе **Сеть** нажмите .
- 8 В списке **Межсетевой шлюз** выберите координатор.



Внимание! Смена алгоритма шифрования с **Не задан** на **ГОСТ 28147-89** и наоборот для межсетевого мастер-ключа недопустима. Чтобы изменить алгоритм шифрования межсетевого взаимодействия, создайте новое межсетевое взаимодействие.

- 9 Нажмите **Сохранить**.
- 10 [Включите автоматическую отправку справочников и ключей](#).
- 11 Для доверенной сети [отправьте новую межсетевую информацию](#).
- 12 Если при установке межсетевого взаимодействия с доверенной сетью статус длительное время имеет значение **В обработке**, убедитесь, что справочники и ключи дошли до узлов вашей сети под управлением ViPNet Prime, для этого выберите **Управление организацией**  > **Журнал транспортных конвертов**. Если ключи и справочники не дошли до узлов, попробуйте отправить их снова.
- 13 После того, как межсетевая информация будет доставлена в доверенную сеть, для старого шлюзового координатора и нового шлюзового координатора создайте и отправьте новые справочники и ключи.

Связи с доверенными объектами

Администратор доверенной организации определяет объекты, которые могут взаимодействовать с вашей организацией. Управление связями между объектами доверенных организаций осуществляется с помощью разрешения доверенной организации устанавливать связи с объектом вашей организации.

Порядок действий

- 1 Администратор доверенной организации разрешает создавать связи с объектом.
- 2 При межсетевом взаимодействии Администратор доверенной организации передает файл с межсетевой информацией администратору организации. Администратор организации принимает ее и передает файл с ответной межсетевой информацией администратору доверенной организации.
- 3 Администратор организации создает связи с объектами доверенных организаций.

Чтобы создать связь с ресурсом в доверенной организации при межсетевом взаимодействии, администратор организации создает связь пользователей с координатором доверенной организации, туннелирующим ресурс.



Внимание! Нельзя добавить связь пользователя из доверенной сети с туннелируемым ресурсом. При попытке добавить связь туннелируемого ресурса с пользователем из доверенной сети связь не добавится.

- 4 Администратор доверенной организации [разрешает использовать ресурс в доверенных сетях](#).

Особенности связей с объектами доверенной организации

- Связь с пользователем доверенной организации означает связь со всеми устройствами этого пользователя. Создание связей с отдельными узлами одного пользователя невозможно.
- Связь с координатором доверенной организации, сеть которой управляется с помощью ViPNet Administrator, также автоматически создает связи со всеми IP-адресами, которые туннелирует координатор. То есть связь объекта доверенной сети с координатором предоставляет доступ ко всем его туннелируемым IP-адресам.

При создании связей между объектами доверенных организаций, управляемых с помощью Prime и имеющих одинаковый номер защищенной сети, вы можете создать связи с отдельными ресурсами доверенных организаций.

Если администратор одной из доверенных организаций изменит параметры взаимодействия с вашей организацией, ему потребуется отправить в вашу сеть новую межсетевую информацию. Межсетевая информация может быть отправлена в вашу сеть по защищенному каналу VPN.

Ограничения создания связей между ViPNet Coordinator KB

Запрещается создавать связи между ViPNet Coordinator KB из разных защищенных сетей, так как связь между такими координаторами создается не на ключах обмена, а на единой серии ДСДР.

Предоставление объектов организации для совместного доступа

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 В ViPNet VPN  > **Управление защищенной сетью** выберите раздел с объектами.
- 3 Выберите объект.
- 4 На панели справа выберите **Совместный доступ**.
- 5 Нажмите **Разрешить использование для связей**.
- 6 Выберите доверенные организации.
- 7 Нажмите **Сохранить**.

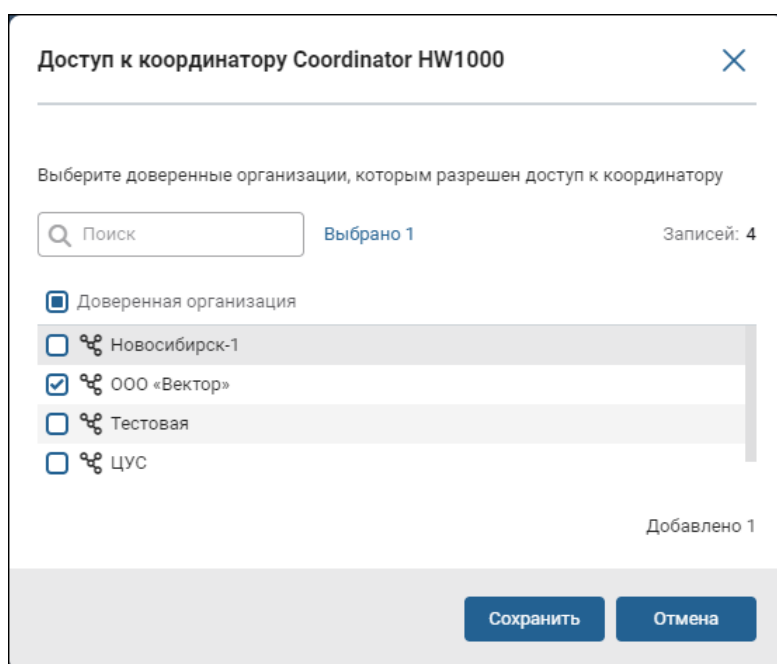


Рисунок 66. Предоставление прав доверенной организации на создание связей с координатором

Создание связей между объектами доверенных организаций

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 В ViPNet VPN  выберите раздел с объектами.
- 3 Выберите объект.
- 4 На панели справа нажмите  **Связи**.
- 5 Нажмите **Добавить связь**.

6 Выберите вкладку **Доверенные организации**.

7 Выберите доверенные организации.

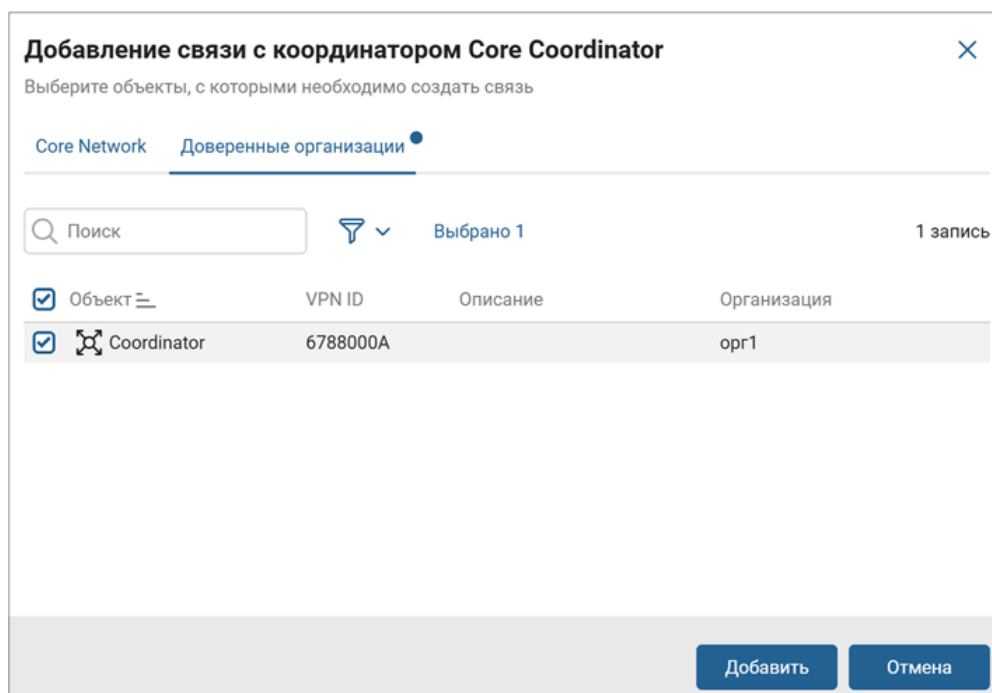


Рисунок 67. Добавление связи с объектом доверенной организации

Чтобы отобразить объекты нужных доверенных организаций, нажмите  и в списке **Доверенная организация** выберите организации.

- 8 Выберите объекты, с которыми нужно создать связь. Нажмите **Добавить**. Выбранные объекты будут добавлены в список связей, добавленных вручную администратором.
- 9 Нажмите **Сохранить**. Новая связь примет статус **Запрошена**.
- 10 Отправьте актуальную межсетевую информацию в доверенную организацию (см. [Отправка межсетевой информации](#)). Если доверенные организации имеют одинаковые номера защищенной сети, то актуальная информация об изменении связей отправится автоматически.
- 11 [Обработайте ответную межсетевую информацию](#).
- 12 Дождитесь, пока связь примет статус **Установлена**.

Управление доступом к ресурсам при межсетевом взаимодействии

После установления межсетевого взаимодействия и предоставления совместного доступа доверенным организациям к координатору вы можете предоставить доступ к его ресурсам.

После предоставления доступа к координатору ресурсы остаются недоступными доверенным организациям доверенных сетей. Чтобы разрешить использование ресурса в организациях доверенных сетей:

- 1 Войдите в ViPNet Prime как суперадминистратор, владелец организации или администратор организации.
- 2 Выберите организацию.
- 3 Выберите ViPNet VPN  > Ресурсы.
- 4 Выберите объект.
- 5 Справа выберите **Совместный доступ**.
- 6 В разделе **Использование ресурса в организациях доверенных сетей** нажмите **Разрешить доступ**.
- 7 Выберите доверенные организации и нажмите **Сохранить**.
- 8 Отправьте межсетевую информацию в доверенную организацию (см. [Отправка межсетевой информации](#)).
- 9 [Обработайте ответную межсетевую информацию](#).

Если вы предоставили доступ ко всем ресурсам координатора, при появлении новых ресурсов предоставляйте доступ к ним.

Вы можете изменить решение о предоставлении доступа к ресурсу:

- 1 Войдите в ViPNet Prime как суперадминистратор, владелец организации или администратор организации.
- 2 Выберите организацию.
- 3 Выберите ViPNet VPN  > Ресурсы.
- 4 Выберите объект.
- 5 Справа выберите **Совместный доступ**.
- 6 В разделе **Использование ресурса в организациях доверенных сетей** нажмите .
- 7 Снимите флажок напротив организации, которой больше не нужен доступ к ресурсу.
- 8 Нажмите **Сохранить**.
- 9 [Отправьте межсетевую информацию](#).
- 10 [Обработайте ответную межсетевую информацию](#).

Если в ViPNet Prime вы предоставляете для доверенного взаимодействия ресурсы, туннелируемые координатором, который выполняет функции DNS-сервера, при загрузке межсетевой информации в ViPNet Administrator вы можете любой из туннелируемых адресов указать в качестве DNS-сервера. Если вы предоставляете доступ к большому диапазону ресурсов, в ViPNet Administrator вы получите большой список DNS-серверов.

Управление совместным доступом к сервисным функциям

В доверенных организациях вашей сети вы можете не развертывать свой координатор или сервер с прикладным ПО ViPNet Connect и можете разрешить использовать функции узлов из доверенной организации:

- чтобы выбрать координатор доверенной организации в качестве серверов соединений или для регистрации на нем клиентов;
- чтобы выбрать узел в качестве DNS-серверов в [профилях DNS](#);
- чтобы использовать сервисные функции сервера групповых чатов ViPNet ConServer, сервера push-уведомлений ViPNet CPNS и других из доверенной организации.

Рекомендации:

- Если функции DNS-сервера используются несколькими организациями, клиенты этих организаций разрешают имена доменов всех организаций, которым передан в совместный доступ DNS-сервер. Если это недопустимо в вашей сети, для каждой организации создайте свои DNS-серверы для профилей DNS.
- Сервисные функции транспортного сервера Connect Hub, сервера хранения файлов Connect File Exchange, сервера групповых чатов ConServer и сервера пуш-уведомлений CPNS разрешайте использовать в доверенной организации во время одной настройки.

Чтобы разрешить использовать функции объекта сети в доверенной организации:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 В **ViPNet VPN**  выберите раздел с объектами.
- 3 Выберите объект.
- 4 Справа выберите **Совместный доступ**.
- 5 Нажмите **Разрешить использование функций**.
- 6 Выберите функции для доверенных организаций.
- 7 Нажмите **Сохранить**.

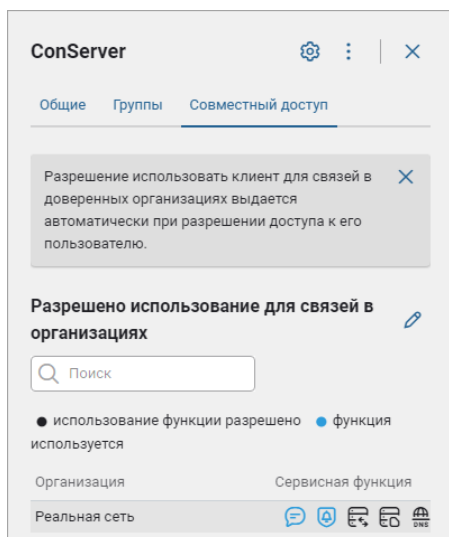


Рисунок 68. Просмотр используемых сервисных функций узла

Прекращение совместного доступа к сервисным функциям

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию, из которой хотите прекратить предоставлять сервисные функции в совместный доступ.
- 3 В ViPNet VPN  выберите раздел с объектами.
- 4 Выберите объект.
- 5 Справа выберите **Совместный доступ**.
- 6 Нажмите .
- 7 Выберите доверенную организацию и отключите сервисную функцию.
- 8 Нажмите **Сохранить**.

Прекращение взаимодействия

С доверенной организацией

- 1 Войдите в ViPNet Prime как владелец организации или организации.
- 2 Выберите организацию, для которой требуется прекратить взаимодействие.
- 3 В ViPNet VPN  > **Доверенное взаимодействие** > **Организации** выберите доверенную организацию.

- 4 Нажмите .
- 5 Ознакомьтесь со списком функций объектов доверенной организации, которые будут отменены, и нажмите **Да**.
- 6 Нажмите **Заккрыть**.

С доверенной сетью

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 В ViPNet VPN  > **Доверенное взаимодействие** > **Сети** выберите сеть.
- 3 Нажмите .
- 4 Ознакомьтесь со списком организаций, для которых будет прекращено взаимодействие с доверенной сетью, и нажмите **Да**.
- 5 Нажмите **Заккрыть**.

Отправка обновлений на узлы

Обновить программное обеспечение ViPNet на узлах вы можете:

- локально;
- удаленно из ViPNet Prime.

Для ViPNet xFirewall вы можете обновить отдельно файл с набором приложений и протоколов для правил DPI без обновления ПО ViPNet xFirewall. В свойствах файла обновления правил DPI будет отображаться дополнительная информация о версии файла. В этом случае на выбранные узлы будет отправлен файл обновления DPI-классификатора.

Перед отправкой обновления ПО ViPNet как суперадминистратор загрузите файл обновления ПО ViPNet в модуль VPN. Файлы обновлений хранятся на сервисе обновлений и могут отправляться на узлы несколько раз. Если такое же обновление уже загружено в ViPNet Prime, повторно его загружать не нужно — появится предупреждение об обнаружении дубликата.

При обновлении ViPNet Prime на версию 1.9.14 удаляются все файлы обновления, загруженные администратором. После обновления ViPNet Prime снова загрузите эти файлы.

Начиная с версии 1.9.14 ViPNet Prime поддерживает обновление ПО поколения ViPNet 5 с помощью сервиса обновлений. Это позволяет снизить нагрузку на ViPNet Prime и избежать отправки неверного ПО на устройства. Если управляемое ПО не поддерживает скачивание файлов с сервиса обновлений, файлы обновления автоматически будут отправляться на устройство по поддерживаемому им протоколу.

Управление файлами обновления ПО ViPNet

Загрузка файл обновления

- 1 Проверьте целостность и достоверность файла обновления с помощью ViPNet PKI Client. Подробнее см. в документации ViPNet PKI Client.
- 2 Войдите в ViPNet Prime как суперадминистратор.
- 3 Выберите **ViPNet VPN**  > **Обновление ПО**.
- 4 Нажмите  **Загрузить обновление**.
- 5 Для координаторов поколения ViPNet 5 создайте архив *.zip с произвольным именем файла. Рекомендуется в имени файла указать платформу, для которой предназначено обновление.

Название файла может содержать:

- буквы латинского алфавита от A до Z;
- буквы латинского алфавита от a до z;
- цифры от 0 до 9;

- символы `_ . - ~`

6 Добавьте в архив:

- архив с обновлением ПО `driv.zip`;
- открепленную электронную подпись `driv.zip.sig`.

7 Укажите путь к файлу обновления:

- для поколения ViPNet 4 — `*.lzh`;
- для поколения ViPNet 5 — архиву `*.zip`, в котором содержатся два файла: обновление `*.zip` и его электронная подпись `SIG`.

Если при загрузке обновления появилось сообщение о нехватке свободного места на диске, убедитесь, что свободное место больше чем в шесть раз превышает размер файла с обновлением.

Удаление файла обновления

Если обновление ПО устарело:

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 Выберите **ViPNet VPN**  > **Обновление ПО**.
- 3 Выберите обновление.
- 4 На панели справа нажмите .
- 5 Подтвердите удаление.

Скачивание файл обновления

Вы можете скачать файл обновления, например, если у вас распределенная сеть и нужно обновить узел локально:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet VPN**  > **Обновление ПО**.
- 3 Выберите обновление.
- 4 На панели справа нажмите **Скачать**.

Обновление ПО ViPNet на узлах

- Не поддерживается отправка обновлений DPI на узлы поколения ViPNet 5, такие как ViPNet Coordinator HW 5 и другие.
- Перед отправкой обновлений на шлюзы безопасности Coordinator HW версии 5.2.1 и ниже, убедитесь, что название архива с обновлением ПО и его подпись имеют названия `driv.zip` и

driv.zip.sig соответственно. Иначе на шлюзе не будет распаковано и установлено обновление ПО.

- Если в защищенной сети установлен ViPNet Coordinator HW версии 5.2.1, то включите для него функцию VPN-шлюз, либо обновите ПО до версии 5.3.1. Иначе могут не применяться справочники и ключи на координаторе.
- Чтобы перейти с ПО координатора поколения ViPNet 4 до поколения ViPNet 5:
 - [смените поколение координатора](#),
 - вручную обновите ПО ViPNet локально на координаторе,
 - установите новый дистрибутив ключей.

См. в документации на координатор, например, «ViPNet Coordinator HW 5. Настройка с помощью командного интерпретатора», раздел «Обновление ПО с версий 4.5.x до версии 5.3.x».

- Нельзя удалённо обновить ViPNet Coordinator KB 4 из ViPNet Prime.
- Если в вашей сети много устройств, которые не поддерживают работу с сервисом обновлений, убедитесь, что на компьютере ViPNet Prime достаточно свободного места. Например, для 100 одинаковых координаторов с размером файла обновления 500 Мбайт потребуется 50 Гбайт свободного места.

При обновлении нескольких однотипных устройств с помощью сервиса обновлений на сервере хранится общий файл обновлений для этих устройств. Если же устройства не поддерживают работу с сервисом обновлений, для каждого однотипного устройства на транспортный сервер отправляется собственная копия файла обновлений, что приводит к дополнительному расходу места на сервере. Поэтому рекомендуется устройства, не поддерживающие работу с сервисом обновлений, обновлять по очереди или небольшими партиями.

- При обновлении ViPNet РУКС Лайт, ViPNet КУКС Лайт, ViPNet РУКС обновление ПО применяется на узлах, но в ViPNet Prime отправляется статус с ошибкой обновления (статус конверта **Не принято**).

Чтобы отправить обновление ПО:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию или подразделение.
- 3 Выберите **ViPNet VPN**  > **Обновление ПО**.
- 4 Выберите обновление ПО ViPNet.
- 5 На панели справа нажмите  **Отправить обновление**.
- 6 На шаге 1 выберите узлы:

6.1 Нажмите  **Добавить** и в списке выберите:

- **Выборочно из списка всех узлов.** Вы можете найти узлы по идентификатору узла VPN ID.

Выберите узлы и нажмите **Добавить**.

- **Все узлы из конкретной группы.** Выберите группы узлов и нажмите **Добавить**.

При отправке обновления на клиенты в списке будут отображаться только те узлы, которые поддерживают работу с сервисом обновлений. Если клиент не поддерживает сервис обновлений, отправьте обновления с помощью расширенных настроек.

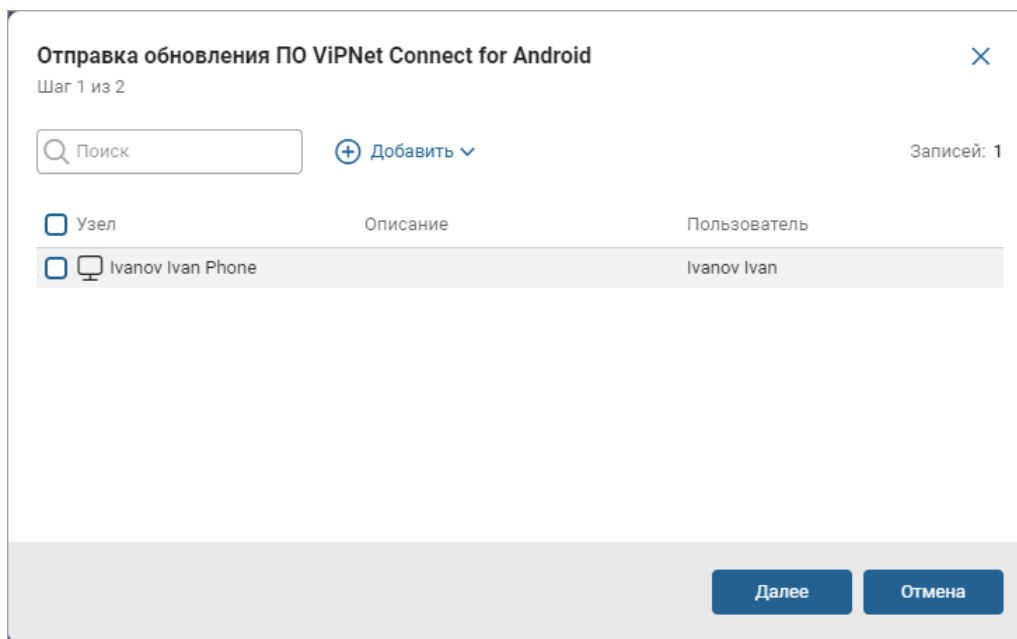


Рисунок 69. Отправка обновления программного обеспечения

6.2 Чтобы удалить узлы из списка, выберите узлы и нажмите .

6.3 Нажмите **Далее**.

7 На шаге 2 выберите срок обновления ПО ViPNet на узлах.

- Чтобы обновление вступило в действие сразу после доставки на узлы, выберите **Установить сразу после доставки на узел**.
- Чтобы установить дату и время применения обновления на узлах, выберите **Установить в указанное время** и установите дату и время с помощью календаря , затем нажмите **Применить**. Время указывается локальное, но обновление отправляется по UTC+0.

8 Нажмите **Отправить**.

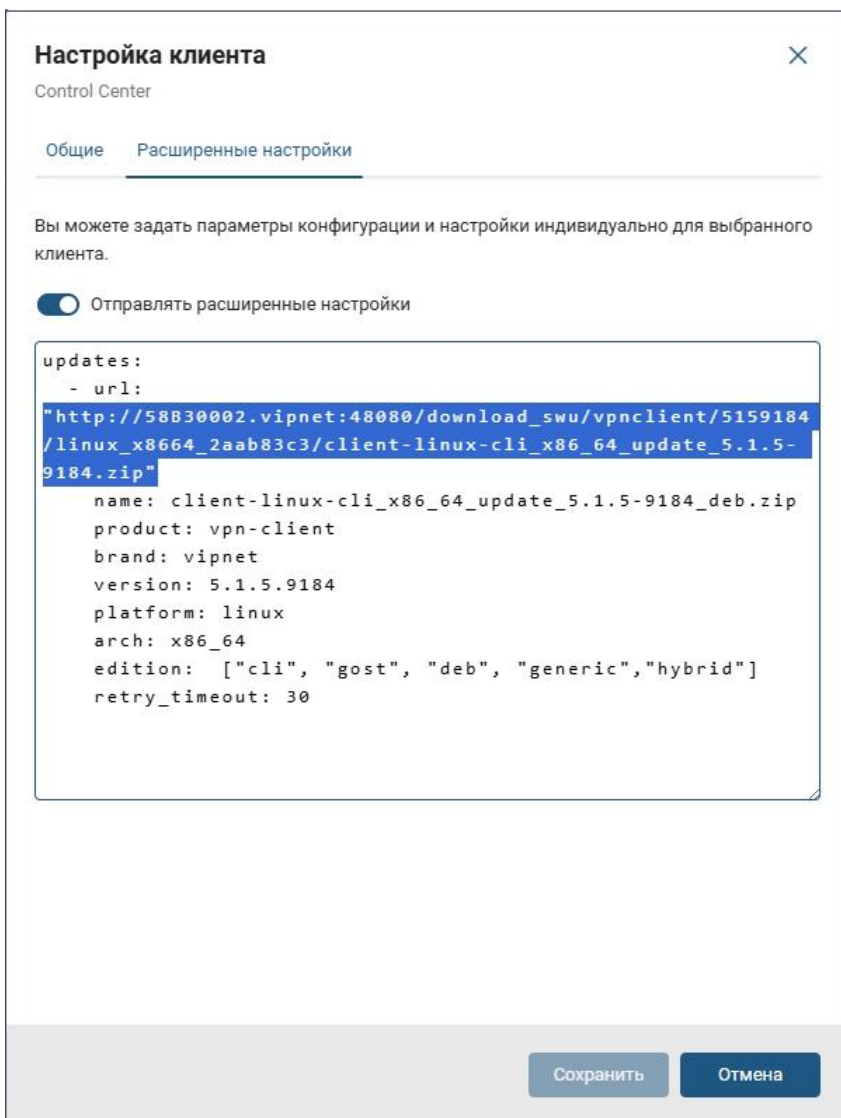
Отправка обновления с помощью расширенных настроек клиента

Если клиенты, на которые требуется отправить обновление, не поддерживают работу с сервисом обновлений, вы можете скопировать ссылку на обновление и добавить ее в файл с [расширенными настройками](#) `custom.yaml`. Ссылка не позволяет напрямую переходить на сервис раздачи обновлений.

1 Войдите в ViPNet Prime как владелец организации или администратор организации.

2 Выберите ViPNet VPN > Обновление ПО.

- 3 Выберите обновление.
- 4 На панели справа нажмите .
- 5 Вставьте ссылку в расширенные настройки.



Настройка клиента ✕

Control Center

Общие Расширенные настройки

Вы можете задать параметры конфигурации и настройки индивидуально для выбранного клиента.

☒ Отправлять расширенные настройки

```
updates:
- url:
"http://58830002.vipnet:48080/download_swu/vpnclient/5159184/
/linux_x8664_2aab83c3/client-linux-cli_x86_64_update_5.1.5-
9184.zip"
  name: client-linux-cli_x86_64_update_5.1.5-9184_deb.zip
  product: vpn-client
  brand: vipnet
  version: 5.1.5.9184
  platform: linux
  arch: x86_64
  edition: ["cli", "gost", "deb", "generic", "hybrid"]
  retry_timeout: 30
```

Сохранить Отмена

Рисунок 70. Пример добавления ссылки на обновление в файл *custom.yaml*

- 6 Нажмите **Сохранить**.
- 7 Отправьте обновление справочников и ключей на узел.

Просмотр журнала транспортных конвертов

Чтобы проверить получение узлами обновления или изменения настроек в организации, вы можете просмотреть историю отправленных центром управления обновлений (ПО, справочников и ключей) на устройства организации в журнале транспортных конвертов. В нем содержатся:

- имена устройств-получателей;

- статус отправленных конвертов;
- дата и время отправки конвертов;
- тип обновления (обновление лицензии, служебные настройки, программное обеспечение, справочники и ключи, конфигурация и другие);
- история статусов отправленных конвертов;
- номер ревизии настроек в конверте.

Ревизия конверта — счетчик, который используется системой управления для защиты от повторных передач конвертов на узлы. Если пришел новый конверт с большей ревизией, будут отброшены все последующие с меньшими номерами ревизии.

Индивидуальная конфигурация — список возможностей узла. Его отправляют координаторы поколения ViPNet 5 в ViPNet Prime после инициализации узла, обновления ПО.

Для каждого узла, на который отправлено обновление, в журнале отображается информация о последнем отправленном конверте и его статус, а также история статусов. Для узлов, которые получают конверты по UT:

- **В процессе** — транспортный клиент UT отправил конверт транспортному серверу UT.
- **Доставлено.**
- **Принято.**
- **Ошибка.**

Для узлов, которые получают конверты по MFTP:

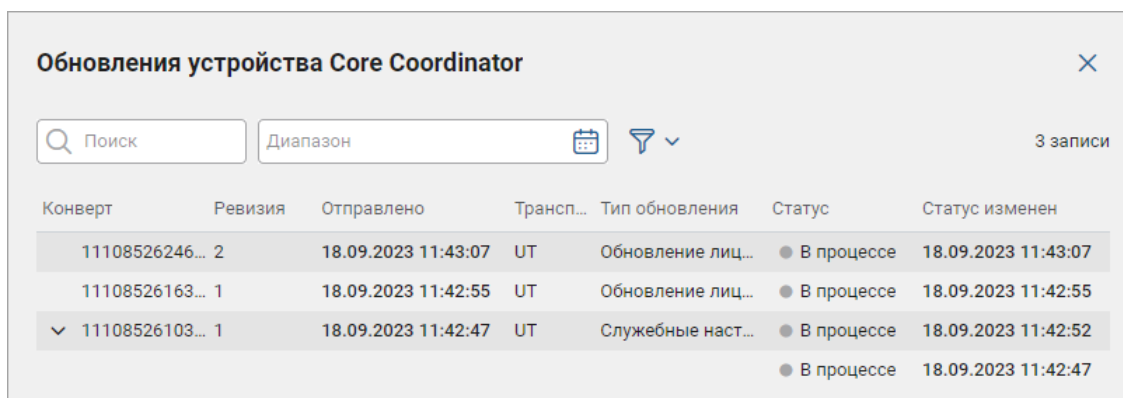
- **Создано.**
- **Отправлено.**
- **Доставлено.**
- **Принято.**
- **Не принято.**

В журнале отображаются клиенты, координаторы и межсетевые экраны на которые отправлены обновления настроек.

Просмотр журнала транспортных конвертов

- 1 Войдите в ViPNet Prime как владелец организации, администратор организации или аудитор устройств.
- 2 Выберите организацию.
- 3 Выберите **Управление организацией**  > **Журнал транспортных конвертов**.
- 4 Чтобы найти конверты с определенным статусом, нажмите  и выберите статус конверта.
- 5 Чтобы найти конверты, полученные в определенное время, нажмите  и выберите диапазон времени.

- 6 Чтобы просмотреть все конверты, отправленные на устройство, в журнале выберите устройство и просмотрите конверты и их статус.



Обновления устройства Core Coordinator

Поиск Диапазон 3 записи

Конверт	Ревизия	Отправлено	Трансп...	Тип обновления	Статус	Статус изменен
11108526246...	2	18.09.2023 11:43:07	UT	Обновление лиц...	● В процессе	18.09.2023 11:43:07
11108526163...	1	18.09.2023 11:42:55	UT	Обновление лиц...	● В процессе	18.09.2023 11:42:55
▼ 11108526103...	1	18.09.2023 11:42:47	UT	Служебные наст...	● В процессе	18.09.2023 11:42:52
					● В процессе	18.09.2023 11:42:47

Рисунок 71. Просмотр отправленных конвертов UT

- 7 Чтобы просмотреть историю статусов отправленного конверта, выберите конверт.
- 8 Чтобы найти конверты с определенным обновлением, нажмите  и в списке **Тип обновления** выберите: Программное обеспечение, Политики безопасности, Обновление лицензии, Справочники и ключи, Служебные настройки.



Внимание! Если конверт не принят на устройстве, [повторно отправьте обновление справочников и ключей вручную](#).

Просмотр транспортных конвертов, отправленных в доверенную сеть

- 1 Войдите в ViPNet Prime как владелец организации, администратор организации.
- 2 Выберите организацию.
- 3 Выберите ViPNet VPN  > Доверенное взаимодействие > Организации.
- 4 Выберите сеть, с которой у вашей организацией установлено взаимодействие.
- 5 На панели справа перейдите на вкладку **Журнал конвертов**.

Обновление справочников и ключей

По умолчанию обновления справочников и ключей на узлы организаций отправляются автоматически:

- Через 6 минут после последнего изменения.
- Если до отправки справочников будут внесены изменения, таймер отправки будет сброшен и задержка отправки будет постепенно увеличиваться.
- Если через 60 минут после первых изменений не выполнены условия отправки справочников и ключей, то в любом случае справочники и ключи отправятся на узлы.

В защищенной сети с 1000 и более узлов и при работе нескольких администраторов это помогает отправлять справочники и ключи реже и выполнять другие операции быстрее. Например, дистрибутивы ключей будут создаваться и скачиваться быстрее, так как будут создаваться до автоматического обновления справочников и ключей. Также менее частые обновления справочников и ключей помогают сохранить доступность координаторов.

В защищенной сети с количеством узлов менее 1000 вы можете изменить максимальный интервал обновления справочников и ключей, чтобы ускорить их отправку:

1 Остановите ViPNet Prime:

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

2 В файле `/usr/share/infotecs/prime/deployment/vpn-ms/vpn-ms.env` добавьте параметр `NSMS_AutoUpdateMaxIntervalInMinutes` и укажите значение в минутах от 0 до 1440 (24 часа). По умолчанию 60.

Например, если `NSMS_AutoUpdateMaxIntervalInMinutes=0`, то справочники и ключи будут отправляться на каждое изменение в защищенной сети, что приведет к повышенной нагрузке на сеть.

3 Запустите ViPNet Prime:

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

Если обновления нет на узлах (например, после непредвиденной перезагрузки ОС компьютера новый клиент не появился в защищенной сети), отправьте повторно обновление справочников и ключей вручную.

Если на узел пришло обновление, которое не прошло проверку целостности и подлинности, оно не применится на узле. Подозрительный конверт будет заблокирован и об этом отправится уведомление на узел центра управления ViPNet Prime, имя конверта-уведомления будет начинаться с символа **!**. В [журнале транспортных конвертов](#) системы ViPNet Prime статус конверта будет обозначен как **Не принято**. Этот статус будет отображаться, если обновление отправлено с узла ViPNet Prime. Подробнее о блокировке конвертов с подозрительными обновлениями см. в документе «ViPNet Client. Руководство пользователя» или «ViPNet Client. Руководство администратора», в разделе «Рекомендации по безопасности».

Время хранения обновлений справочников и ключей ограничено. Обновление удаляется с транспортного сервера после получения клиентом транспортного сервера или через 90 дней. Возможно, если узел был выключен, конверты не были доставлены до него и были удалены на транспортном сервере. Отправьте на узел актуальные справочники и ключи повторно.

Обновление справочников и ключей вручную на нескольких узлах



Примечание. Перед отправкой справочников и ключей на координатор поколения ViPNet 5 включите функцию **VPN-шлюз**, иначе обновление не отправится.

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите ViPNet VPN  > Клиенты (или Координаторы, или Другие узлы).

- 4 Выберите узлы.
- 5 Нажмите  > **Отправить справочники и ключи.**

Обновление справочников и ключей на узлах вручную на одном узле

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию и подразделение.
- 3 Выберите **ViPNet VPN**  > **Клиенты** (или **Координаторы**, или **Другие узлы**).
- 4 Выберите узел.
- 5 Нажмите .
- 6 Для координатора поколения ViPNet 5 убедитесь, что включена функция **VPN-шлюз**.
- 7 Закройте окно и справа нажмите  > **Отправить справочники и ключи.**
- 8 Чтобы локально обновить справочники и ключи, скачайте их в виде файла обновлений и установите на узле. Для этого выберите **Файл обновлений** > **Создать и скачать**. В загрузки браузера скачается файл `cms_<Номер сетевого узла ViPNet>_<порядковый номер ключа защиты обновлений>.bin`.

Просмотр статуса конвертов

Чтобы проверить получение обновления на узле:

- 1 Войдите в ViPNet Prime как владелец организации, администратор организации или аудитор устройств.
- 2 Выберите организацию и подразделение.
- 3 Выберите **ViPNet VPN**  > **Клиенты**.
- 4 Выберите клиент.
- 5 На панели справа нажмите **Перейти в журнал конвертов**.

Откроется журнал транспортных конвертов, отфильтрованный по выбранному узлу. Для узлов поколения ViPNet 4 вы можете увидеть в таблице статус последнего обновления.

Компрометация ключей

Компрометация узла

При компрометации узла считаются скомпрометированными ключи узла. При компрометации узла удалите скомпрометированный узел, создайте новый узел и выдайте дистрибутив ключей новому узлу:

- 1 В ViPNet Prime выберите узел, который был скомпрометирован.
- 2 Если узел выполняет **критически важные функции**, снимите с узла эти функции и назначьте их на другие узлы.
- 3 Удалите скомпрометированный узел из модуля VPN.
- 4 Создайте и настройте новый узел.
- 5 Создайте и скачайте дистрибутив ключей для нового узла и передайте администратору узла.

Компрометация узлов управления

При компрометации одного из узлов управления — центра управления или его координатора выполните смену мастер-ключей в зависимости от поколения узла. После смены мастер-ключей создайте новый дистрибутив ключей скомпрометированному узлу.

Узел поколения ViPNet 4

- 1 В ViPNet Prime выполните **смену мастер-ключей сети**.
- 2 Создайте дистрибутивы ключей для узлов поколения ViPNet 4.

Узел поколения ViPNet 5

- 1 В ViPNet Prime в организации Core Network выполните **смену мастер-ключей организации**.
- 2 Создайте дистрибутив ключей для скомпрометированного узла.

8

Управление адресной книгой ViPNet Connect Book

Интерфейс модуля ViPNet Connect Book	237
Настройка SIP-сервера	238
Добавление контакта	239
Создание и назначение полномочий	240
Импорт дополнительных данных о контакте из Active Directory	241

Интерфейс модуля ViPNet Connect Book

Раздел **ViPNet Connect Book**  предназначен для управления адресной книгой и полномочиями пользователей в приложении ViPNet Connect. Вход в модуль адресной книги и действия в нем доступны суперадминистратору, владельцу организации и администратору организации.

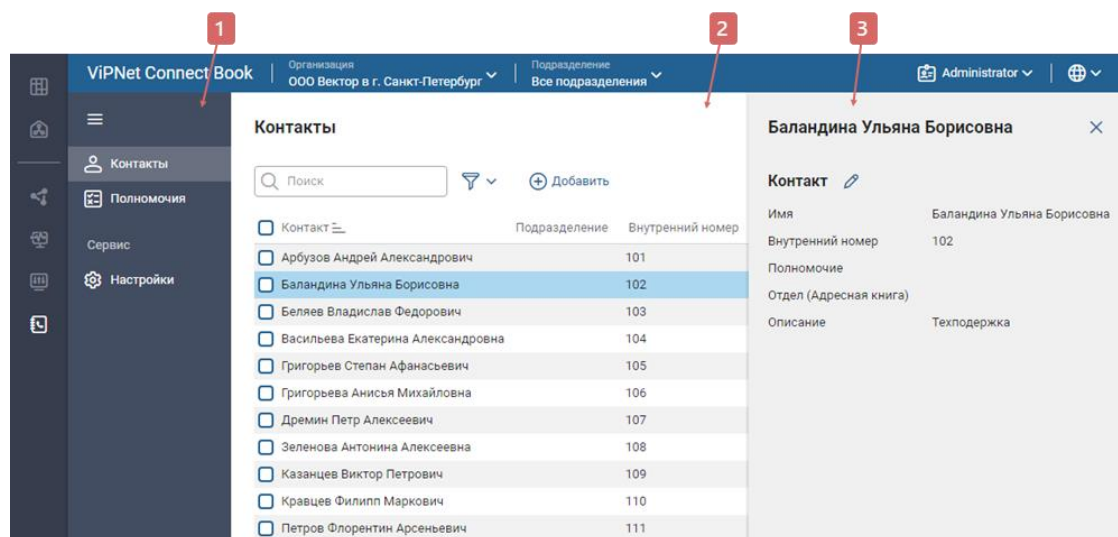


Рисунок 72. Внешний вид раздела ViPNet Connect Book

Цифрами на рисунке обозначены:

- 1 Панель навигации. Содержит подразделы:
 - **Контакты** — общий список пользователей, добавленных в разделах **Управление организацией** > **Пользователи** и адресной книги.
 - **Полномочия** — объединяют пользователей в группы по полномочиям. Пользователи с более низким полномочием не могут звонить или писать сообщения в приложении ViPNet Connect пользователям с более высоким полномочием.
 - **Настройки** — [настройки SIP-сервера стороннего производителя](#) и [сопоставление дополнительных полей Active Directory с контактами адресной книги \(внутренний номер, дополнительная информация\)](#).
- 2 Панель просмотра.
- 3 Панель свойств.

Настройка SIP-сервера

Вы можете централизованно задать настройки SIP-сервера для пользователей приложения ViPNet Connect. Пользователям не придется самостоятельно их задавать в приложении ViPNet Connect.

В организации может быть задан только один SIP-сервер. SIP-сервер должен быть указан в настройках приложения ViPNet Connect и его адрес должен туннелироваться координатором. Перечень поддерживаемых SIP-серверов см. в «ViPNet Connect. Руководство администратора».

Чтобы задать параметры SIP-сервера:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Если вы администрируете несколько организаций, [выберите организацию](#).
- 3 Выберите **ViPNet Connect Book**  > **Настройки**.
- 4 В разделе **SIP-сервер** нажмите .
- 5 Введите адрес SIP-сервера и укажите порт. По умолчанию 5060.
- 6 При использовании прокси-сервера введите его адрес и порт.
- 7 Нажмите **Сохранить**.

Добавление контакта

Адресная книга — это список контактов для пользователей в приложении ViPNet Connect.

Вы можете добавить контакты в адресную книгу несколькими способами:

- автоматически при добавлении пользователей ViPNet Prime в разделе **Управление организацией**  > **Пользователи**. При этом в модуле ViPNet Connect Book недоступно изменение информации об этих пользователях.
- вручную при создании контакта в модуле адресной книги.



Примечание. В адресной книге не отображаются контакты пользователей из доверенных организаций.

Чтобы вручную добавить SIP-контакт в адресную книгу:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Если вы администрируете несколько организаций, [выберите организацию и подразделение](#).
- 3 Выберите **ViPNet Connect Book**  > **Контакты**.
- 4 Нажмите  **Добавить**.
- 5 Введите имя контакта.
- 6 При необходимости [создайте и укажите полномочие](#).
- 7 Нажмите **Сохранить**.

Чтобы найти контакты, нажмите   и выберите:

- **Без полномочий.**
- **Создан в Prime.**
- **Создан в Connect Book.**

Создание и назначение полномочий

Уровни полномочий ограничивают контакты, которым пользователь звонит и пишет сообщения в ViPNet Connect. Функциональность поддерживается в ViPNet Connect версии 2.13.2 и выше.

Максимальный уровень полномочий — полномочие с приоритетом 1. При создании полномочия приоритет задается автоматически с номером по порядку. После создания полномочия вы можете изменить его приоритет. Пользователи с меньшим уровнем полномочий не могут звонить и отправлять сообщения в приложении ViPNet Connect контактам с большим уровнем полномочий.

Чтобы ограничить возможность пользователей с низким уровнем полномочий писать или звонить пользователям с более высоким уровнем полномочий, задайте им разный уровень полномочий. Пользователи без полномочий не могут звонить и отправлять сообщения другим контактам в приложении ViPNet Connect, но могут отвечать на звонки или сообщения.

Чтобы создать полномочие:

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите **ViPNet Connect Book**  > **Полномочия**.
- 3 Нажмите  **Добавить**.
- 4 Введите название полномочия и нажмите **Сохранить**.
- 5 Чтобы изменить приоритет полномочия:
 - 5.1 Выберите полномочие.
 - 5.2 Нажмите  или .

Чтобы создать полномочие с приоритетом выше или ниже другого полномочия:

- 1 Выберите полномочие.
- 2 Нажмите  или .
- 3 Введите название полномочия и нажмите **Сохранить**.

Чтобы назначить полномочие контакту:

- 1 Выберите **ViPNet Connect Book**  > **Контакты**.
- 2 Выберите контакты.
- 3 Нажмите **Назначить полномочия**.
- 4 Выберите полномочие и нажмите **Сохранить**.

Импорт дополнительных данных о контакте из Active Directory

- 1 Войдите в ViPNet Prime как владелец организации или администратор организации.
- 2 Выберите организацию.
- 3 Убедитесь, что заданы [настройки подключения к коннектору AD](#).
- 4 Введите названия дополнительных параметров импорта:
 - 4.1 Выберите **Управление организацией**  > **Импорт данных**.
 - 4.2 Нажмите **Настроить**.
 - 4.3 Нажмите **Далее**.
 - 4.4 В разделе **Дополнительное поле** введите параметры LDAP-запроса для внутреннего номера и дополнительной информации.
 - 4.5 Нажмите **Сохранить**.
- 5 Выберите **ViPNet Connect Book**  > **Настройки**.
- 6 В разделе **Дополнительные поля из Active Directory** нажмите .
- 7 Введите названия полей из AD для внутреннего номера и информации об отделе.
- 8 Нажмите **Сохранить**.

9

Администрирование

Просмотр версии	243
Просмотр журнала событий	244
Интеграция с сервисами отправки уведомлений по электронной почте и СМС	246
Контроль целостности и работы ПО ViPNet Prime	248
Срок хранения записей в журнале транспортных конвертов	249

Просмотр версии

Вы можете просмотреть версию ViPNet Prime и его модулей. Версия отображается для всех модулей, которые зарегистрированы в ViPNet Prime.

Чтобы просмотреть версию ViPNet Prime или его модулей:

- 1 [Войдите в ViPNet Prime](#).
- 2 На панели сверху нажмите .
- 3 На вкладке **Основное** вы можете просмотреть версию ViPNet Prime.
- 4 На вкладке **Модули** вы можете просмотреть версии зарегистрированных модулей.

При обращении в службу поддержки, чтобы скопировать версии модулей, нажмите **Скопировать номера версий**.

Просмотр журнала событий

В журнале событий вы можете просмотреть информацию о действиях администраторов в ViPNet Prime. По умолчанию записи о событиях хранятся в журнале 365 дней. Вы можете задать другой период. По истечении этого времени неактуальные записи о событиях удаляются из журнала. При удалении журнала событий удаляются все записи, кроме записей за последние три дня.

При изменении параметров администратором в журнал событий записывается информация о новом и предыдущих значениях.



Примечание. Если вы получили сообщение «В работе сервисов приложения были обнаружены ошибки» или «Ошибка обращения к функции КС», просмотрите события сервисов в системном журнале ViPNet Prime или обратитесь к [администратору безопасности](#). См. «ViPNet Prime. Руководство по установке», «Настройка журналов ViPNet Prime» и «Просмотр журналов ViPNet Prime».

Для просмотра журнала событий:

- 1 Войдите в ViPNet Prime как сервисный администратор, владелец организации или администратор организации.
- 2 Выберите **Главная консоль**  > **Журнал событий**.
- 3 Задайте параметры поиска записей в журнале:
 - 3.1 Чтобы найти записи о событиях, которые произошли в определенный период времени, нажмите  и в календаре укажите начало и конец периода.
 - 3.2 Чтобы найти записи о событиях, в которых был задействован некоторый основной объект, над которым выполнялось действие (например, организация, в которую распределена лицензия), выберите событие и на панели справа в группе **Объект события** > **Идентификатор** нажмите идентификатор объекта события.
 - 3.3 Чтобы найти записи о событиях, в которых был задействован некоторый второстепенный объект (например, тип лицензионного объекта, выбранный для устройства), выберите событие и в группе **Дополнительные данные** скопируйте идентификатор лицензионного объекта и вставьте значение в поле поиска.
 - 3.4 Чтобы найти записи о событиях, завершившихся успешно либо с ошибкой, нажмите   и выберите значение.
- 4 Чтобы изменить время хранения записей в журнале событий, нажмите  и введите значение в днях.



Примечание. Для события «Изменение периода хранения журнала событий» нельзя посмотреть новое и старое значения в интерфейсе ViPNet Prime. Вы можете посмотреть это событие на сервере ViPNet Prime до его перезагрузки. Для этого введите команду:

```
sudo docker logs smp_smp-service_1 | grep RetentionPeriodDays
```

Отобразится запись вида:

```
[INF] Activity log settings updated. Settings=LogSettings  
{RetentionPeriodDays=<период хранения в днях>}
```

- 5 Чтобы сохранить журнал событий в файл, нажмите **Экспортировать**. На ваш компьютер будет сохранен файл в формате JSON.
- 6 Чтобы удалить записи из журнала событий, нажмите . Будут удалены все записи, кроме записей за последние 72 часа.

Интеграция с сервисами отправки уведомлений по электронной почте и СМС

Чтобы отправлять уведомления пользователям о событиях в модулях, настройте интеграцию с почтовым сервисом (или корпоративным почтовым сервером) или СМС-провайдером. Например, чтобы отправлять уведомления на электронную почту при выявлении проблем в показателях здоровья системы модулем ViPNet NVS.

Настройка распространяется на все организации.

Чтобы обеспечить работу STARTTLS при интеграции с сервисами уведомлений:

- 1 Проверьте цепочку сертификатов для SMTP-сервера на Prime и добавьте корневой и промежуточный сертификаты в один файл.
- 2 Добавьте корневой сертификат SMTP-сервера в /usr/share/infotecs/shared_certs на машине с ViPNet Prime.

- 3 Перезапустите ViPNet Prime:

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

Для настройки интеграции с сервисами уведомлений:

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 Выберите **Главная консоль**  > **Настройки**.
- 3 Выберите группу **Email-уведомления** или **SMS-уведомления** и нажмите .
- 4 Для отправки уведомлений по электронной почте укажите:
 - **Адрес отправителя**.
 - Настройки почтового сервиса (адрес, порт).
 - **Имя пользователя и пароль** для соединения с почтовым сервером (если на сервере требуется аутентификация).
 - **Протокол шифрования** — STARTTLS или SSL/TLS. По умолчанию **Не используется**.

Чтобы проверить настройку уведомлений, нажмите **Отправить тестовое сообщение**.

- 5 Для отправки СМС-уведомлений укажите:
 - **SMS-сервис** > **СМС-центр**.

- Имя отправителя рассылки (SenderID), зарегистрированное в личном кабинете СМС-провайдера. Вы можете просмотреть ограничения на использование имени отправителя на сайте СМС-провайдера [СМС-центр](#).
- **API-ключ** и **Секрет**, предоставляемые СМС-провайдером.

Чтобы проверить настройку СМС-уведомлений, нажмите **Отправить тестовое сообщение**.

6 Нажмите **Сохранить**.

Контроль целостности и работы ПО ViPNet Prime

При запуске ПО ViPNet Prime автоматически проверяется его целостность. Если целостность ПО нарушена, то вход в ViPNet Prime блокируется. Если отсутствует свободное место на диске и сервис не может запуститься и пройти контроль целостности, вы увидите сообщение о том, что ViPNet Prime работает в режиме ограниченной функциональности.

При появлении сообщения, что целостность приложения нарушена, обратитесь к суперадминистратору.

Рекомендуемый срок регламентного контроля целостности ПО — один раз в месяц.

Если правилами организации предусмотрен регламентный контроль целостности ПО:

- 1 Войдите в ViPNet Prime как суперадминистратор.
- 2 Выберите Главная консоль  > Контроль приложения.
- 3 Нажмите Начать проверку.

Если целостность ПО нарушена и ViPNet Prime недоступен, см. «ViPNet Prime. Руководство по установке», «Нарушение целостности и работы ПО ViPNet Prime».

Срок хранения записей в журнале транспортных конвертов

- 1 Войдите в ViPNet Prime как сервисный администратор.
- 2 Выберите Главная консоль  > Настройки > Журнал транспортных конвертов.
- 3 Нажмите .
- 4 Введите срок хранения записей в журнале. Вы можете установить от 1 до 1100 дней. По умолчанию — 90 дней.



Ограничения в названиях объектов

В именах пользователей, устройств или названий организаций в системе управления ViPNet Prime запрещено использовать:

- специальные символы: \ / : * ? < > | &
- знаки абзаца и другие знаки форматирования, кроме пробелов.

Если использовать указанные символы или зарезервированные слова в качестве имени объекта, возникнет ошибка создания объекта.

Чтобы с помощью модуля Prime фильтровать трафик по пользователям, имена пользователей должны быть заданы латинскими буквами.



Поддерживаемые лицензии в ViPNet Prime

Ниже перечислены названия лицензий в интерфейсе ViPNet Prime.

Приложение, его модули и функции

- Prime
- VPN module
- Policy Management module
- Policies nodes
- Network Visibility System
- Monitoring nodes
- Multitenancy mode

Шлюзы безопасности

- Coordinator KB100
- Coordinator KB1000
- Coordinator KB2000
- Coordinator KB5000
- Coordinator KB100 v.5
- Coordinator KB1000 v.5
- Coordinator KB2000 v.5

- Coordinator KB5000 v.5
- Coordinator HW50
- Coordinator IG10
- Coordinator IG10 A0/B0
- Coordinator IG10 A1/B1
- Coordinator IG100 A0/B0
- Coordinator IG100 A1/B1
- Coordinator IG10-I2 A0/A1
- Coordinator IG10-I2 B0/B1
- Coordinator IG100-I4 A0/A1
- Coordinator IG100-I4 B0/B1
- Coordinator IG10 v.5
- Coordinator IG10-I2 v.5
- Coordinator IG100 v.5
- Coordinator IG100-A1 v.5
- Coordinator IG100-I4 v.5
- Coordinator IG1000 v.5
- Coordinator IG-VA1000 v.5
- Coordinator HW50 v.5
- Coordinator HW50 A/B
- Coordinator HW10
- Coordinator HW100 v.5
- Coordinator HW100 A/B/C
- Coordinator HW1000 v.5
- Coordinator HW1000 C/D v.5
- Coordinator HW1000 (Ru)
- Coordinator HW2000 (Ru)
- Coordinator HW2000 v.5
- Coordinator HW5000 v.5
- Coordinator HW100 CU
- Coordinator HW100
- Coordinator HW1000
- Coordinator HW1000 C

- Coordinator HW1000 D
- Coordinator HW2000
- Coordinator HW5000
- Coordinator HW-VA
- Coordinator VA10000 v.5
- Coordinator VA100/500/1000/2000/5000
- Coordinator VA100/500/1000/2000/5000 v.5
- Coordinator HW50 AU
- xFirewall xF100
- xFirewall xF1000 C
- xFirewall xF1000 D
- xFirewall xF5000
- xFirewall xF-VA
- xFirewall xF-VA100/500/1000/2000/5000
- xFirewall xF65000
- L2Q-10G
- L2-10G

Функции шлюзов безопасности

- Failover
- Failover KB100
- Failover KB100 v.5
- Failover KB1000 v.5
- Failover KB2000 v.5
- Failover KB5000 v.5
- Failover 50/100/1000/2000/5000
- Failover 10/50/100/1000/2000/5000/10000 v.5
- Failover xF-VA100/500/1000/2000/5000
- DPI 50/100/500/1000/2000/5000/10000
- DPI 50/100/500/1000/2000/5000/10000 update
- VPN 10/50/100/1000/2000/5000/10000
- IPS 50/100/1000/2000/5000/10000
- IPS 50/100/1000/2000/5000/10000 update

- IPS 100
- IPS IG 100/1000
- IPS 100/1000 update IG
- IPS 1000 C/D
- IPS 5000
- IPS-VA
- IPS xF-VA100/500/1000/2000/5000
- IPS xF65000
- IEC101-IEC104 Converter
- Malware Detection update IG 100/1000
- Malware Detection update 50/100/500/1000/2000/5000/10000
- URL-categories update 50/100/500/1000/2000/5000/10000
- SSL-inspection 50/100/500/1000/2000/5000/10000
- IPF
- Modbus Gateway
- VPN IG 10/100/1000
- Failover IG 10/100/1000
- GeoIP update

Клиентское ПО ViPNet

- Client for Windows
- Client for Windows v.5
- Client for Android
- Client for Android v.5
- Client for iOS v.5
- Client for macOS, iOS
- Client for macOS v.5
- Client for Aurora v.5
- Client for KasperskyOS v.5
- Client for Android, Client for iOS, Client for macOS, Client for Aurora
- Client for Linux
- Client for Linux v.5
- Universal Client v.5 (лицензия для любой ОС узла)

- CSS Connect HW

Прикладное ПО ViPNet

- Connect
- ConServer
- CPNS
- Connect Hub
- Connect File Exchange
- StateWatcher
- HardPhone

Решения на базе ViPNet QTS и QTS Lite

- КУКС Лайт
- РУКС Лайт
- КУКС
- РУКС
- КУКС VA
- РУКС VA

Решения на базе ViPNet QCL

- Client Academic Edition (QCL)
- Server Academic Edition (QCL)

С

Поддерживаемые функции сетевых узлов

Тип узла	Функции
Coordinator HW10	• DNS-сервер • туннелирование • защищенный интернет-шлюз • сервер соединений
Coordinator HW50	• Failover 100
Coordinator HW50 A	• DNS-сервер
Coordinator HW50 B	• туннелирование • сервер соединений для координатора
Coordinator HW50 AU	• Failover 100 • DNS-сервер • туннелирование • защищенный интернет-шлюз
Coordinator HW100	• Failover 100 • DNS-сервер • туннелирование • сервер соединений для координатора • регистрация узлов (клиентов и МЭ) • защищенный интернет-шлюз • межсетевой шлюз
Coordinator HW100 A	• Failover 100

Тип узла	Функции
Coordinator HW100 B	• DNS-сервер • туннелирование • сервер соединений для координатора
Coordinator HW100 C	• Failover 100 • DNS-сервер • туннелирование • сервер соединений для координатора • регистрация узлов (клиентов и МЭ) • защищенный интернет-шлюз • межсетевой шлюз
Coordinator HW100 CU	• Failover 100 • DNS-сервер • туннелирование • межсетевой шлюз • регистрация узлов (клиентов и МЭ) • сервер соединений • защищенный интернет-шлюз
Coordinator HW1000	• Failover 1000 • DNS-сервер • туннелирование • сервер соединений для координатора • регистрация узлов (клиентов и МЭ) • защищенный интернет-шлюз • межсетевой шлюз
Coordinator HW1000 (Ru)	• DNS-сервер
Coordinator HW1000 C	• туннелирование
Coordinator HW1000 D	• сервер соединений для координатора • регистрация узлов (клиентов и МЭ) • защищенный интернет-шлюз • межсетевой шлюз
Coordinator HW2000	• Failover 2000 • DNS-сервер • туннелирование • сервер соединений для координатора • регистрация узлов (клиентов и МЭ) • защищенный интернет-шлюз • межсетевой шлюз
Coordinator HW2000 (Ru)	• DNS-сервер
Coordinator HW5000	• туннелирование

Тип узла	Функции
Coordinator HW10000	• сервер соединений для координатора • регистрация узлов (клиентов и МЭ) • защищенный интернет-шлюз • межсетевой шлюз
Coordinator HW50 v.5	• Failover • DPI • IPS • обновление DPI • обновление IPS • обновление базы вредоносного ПО • обновление базы URL-категорий При включении функции VPN доступны функции: • DNS-сервер, • туннелирование (65535 туннелей), • сервер соединений для координатора
Coordinator HW100 v.5	• Failover
Coordinator HW1000 v.5	• DPI
Coordinator HW1000 C v.5	• IPS
Coordinator HW1000 D v.5	• обновление DPI
Coordinator HW1000 v.5	• обновление IPS
Coordinator HW2000 v.5	• обновление базы вредоносного ПО • обновление базы URL-категорий
Coordinator HW5000 v.5	При включении функции VPN доступны функции:
Coordinator HW10000 v.5	• DNS-сервер • туннелирование (65535 туннелей) • сервер соединений для координатора • регистрация узлов (клиентов и МЭ) • защищенный интернет-шлюз • межсетевой шлюз
Coordinator VA100	• Failover 100 • DNS-сервер • туннелирование • сервер соединений для координатора • регистрация узлов (клиентов и МЭ) • защищенный интернет-шлюз • межсетевой шлюз

Тип узла	Функции
Coordinator VA500	• Failover 500 • DNS-сервер • туннелирование • сервер соединений для координатора • регистрация узлов (клиентов и МЭ) • защищенный интернет-шлюз • межсетевой шлюз
Coordinator HW-VA	• DNS-сервер • туннелирование • сервер соединений для координатора • регистрация узлов (клиентов и МЭ) • защищенный интернет-шлюз • межсетевой шлюз
Coordinator VA1000	• Failover 1000 • DNS-сервер • туннелирование • сервер соединений для координатора • регистрация узлов (клиентов и МЭ) • защищенный интернет-шлюз • межсетевой шлюз
Coordinator VA2000	• Failover 2000 • DNS-сервер • туннелирование • сервер соединений для координатора • регистрация узлов (клиентов и МЭ) • защищенный интернет-шлюз • межсетевой шлюз
Coordinator VA5000	• Failover 5000 • DNS-сервер • туннелирование • сервер соединений для координатора • регистрация узлов (клиентов и МЭ) • защищенный интернет-шлюз • межсетевой шлюз
Coordinator VA100 v.5	• Failover
Coordinator VA500 v.5	• DPI
Coordinator VA1000 v.5	• IPS
Coordinator VA1000 v.5	• обновление DPI
Coordinator VA2000 v.5	• обновление IPS

Тип узла	Функции
Coordinator IG10-I2 v.5	• IPF • Modbus Gateway • IEC101-IEC104 Converter • При включении функции VPN доступны функции: • DNS-сервер • туннелирование • сервер соединений для координатора • режимы работы МЭ (А и Д)
Coordinator IG100 v.5	• Failover • IPF • Modbus Gateway • IEC101-IEC104 Converter При включении функции VPN доступны функции: • DNS-сервер • туннелирование • регистрация узлов (клиентов и МЭ) • сервер соединений для координатора • режимы работы МЭ (А и Д) • межсетевой шлюз
Coordinator IG100-A1 v.5. Coordinator IG100-I4 v.5	• Failover • IPF • Modbus Gateway • IEC101-IEC104 Converter • IPS IG • обновление IPS • обновлнение базы вредоносного ПО При включении функции VPN доступны функции: • DNS-сервер • туннелирование • регистрация узлов (клиентов и МЭ) • сервер соединений для координатора • режимы работы МЭ (А и Д) • межсетевой шлюз
Coordinator IG1000 v.5	• Failover

Тип узла	Функции
Coordinator IG-VA1000 v.5	• IPF • Modbus Gateway • IEC101-IEC104 Converter • IPS IG • обновление IPS • обновление базы вредоносного ПО При включении функции VPN доступны функции: • DNS-сервер • туннелирование • регистрация узлов (клиентов и МЭ) • сервер соединений для координатора • режимы работы МЭ (А и Д) • защищенный интернет-шлюз • межсетевой шлюз
xFirewall xF100	• Failover • IPS • SSL
xFirewall xF1000 C	• IPS
xFirewall xF1000 D	• SSL
xFirewall xF5000	
xFirewall xF-VA	
xFirewall xF65000	
xFirewall xF-VA100	• Failover
xFirewall xF-VA500	• IPS
xFirewall xF-VA1000	• SSL
xFirewall xF-VA2000	
xFirewall xF-VA5000	
Coordinator KB100	• Failover • DNS-сервер • туннелирование • регистрация узлов (клиентов и МЭ) • сервер соединений для узлов • межсетевой шлюз
Coordinator KB1000	• DNS-сервер
Coordinator KB2000	• сервер соединений для узлов

Тип узла	Функции
Coordinator KB5000	• туннелирование • регистрация узлов (клиентов и МЭ) • межсетевой шлюз
Coordinator KB100 v.5	• Failover
Coordinator KB1000 v.5	• DNS-сервер
Coordinator KB2000 v.5	• туннелирование
Coordinator KB5000 v.5	• регистрация узлов (клиентов и МЭ) • сервер соединений для координатора • межсетевой шлюз
КУКС Лайт	подключение СКЗИ-потребителей
Client for Windows	• Connect (через пользователя) • StateWatcher • Policy Manager • Business Mail • DNS-сервер
Client for Android	• Connect (через пользователя) • DNS-сервер
Client for iOS	• Connect (через пользователя) • DNS-сервер
Client for MacOS	Connect (через пользователя) • DNS-сервер
Client for Linux	• Connect (через пользователя) • CPNS • ConServer • DNS-сервер • Connect Hub • Connect File Exchange • Policy Module
Client for Aurora	Connect (через пользователя)
Client for Windows v.5	• Connect (через пользователя) • StateWatcher • Policy Manager • Business Mail • DNS-сервер

Тип узла	Функции
Client for Linux v.5	• Connect (через пользователя) • CPNS • ConServer • DNS-сервер • Connect Hub • Connect File Exchange • Policy Module
Client for macOS v.5	• Connect (через пользователя) • DNS-сервер
Client for Android v.5	• Connect (через пользователя) • DNS-сервер
Client for iOS v.5	• Connect (через пользователя) • DNS-сервер
Client for Aurora v.5	• Connect (через пользователя) • DNS-сервер
Client for KasperskyOS v.5	• Connect (через пользователя) • DNS-сервер



Возможные неполадки

Не создаются дистрибутивы ключей для узлов поколения ViPNet 5

Если на узле центра управления Control Center по каким-либо причинам удалена программа ViPNet Client, то не создаются обновления справочников и ключей, а также дистрибутивы ключей для узлов поколения ViPNet 5.

Чтобы устранить проблему:

- 1 Перезапустите ViPNet Prime:

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

Введите мастер-ПИН.

- 2 Установите ViPNet Client на узел Control Center. См. документацию на клиент.

Сессия истекает слишком быстро

Если по каким-то причинам вы не можете получить результат операции (например, скачать дистрибутив ключей) и сессия истекла, измените максимальную длительность сессии без активности пользователя:

- 1 На сервере ViPNet Prime откройте файл `/usr/share/infotecs/smp-kc/config.env`.

- 2 Для параметра `SILSO_CookieAuthenticationOptions__ExpireTimeSpan` измените значение в формате ЧЧ:ММ:СС от 15 минут (по умолчанию) до 8 часов. Если параметр отсутствует, добавьте его.



Внимание! В синтаксисе параметра

`SILSO_CookieAuthenticationOptions__ExpireTimeSpan` используются одинарный (`'`) и двойной (`"`) символы нижнего подчеркивания.

Пример: `SILSO_CookieAuthenticationOptions__ExpireTimeSpan=00:15:00`

- 3 Перезапустите ViPNet Prime:

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

Не приходит подтверждение связей при межсетевом взаимодействии

- 1 Настроено межсетевое взаимодействие между ViPNet Administrator и ViPNet Prime.
- 2 Добавлена связь между пользователем ViPNet Administrator и ViPNet Prime.
- 3 Присутствует связь в свойствах узла на стороне ViPNet Administrator. После отправки ответной информации в ViPNet Prime статус связей между пользователями находится в состоянии **Запрошено**.

Возможные причины

ViPNet Prime не принимает межсетевую информацию, где есть пользователи координаторов или координаторов без функций VPN-сервера, зарегистрированные на нескольких узлах

Устранение проблемы

- 1 В ЦУСе на одном из узлов удалите этого пользователя.
- 2 Создайте нового пользователя для другого узла.
- 3 Обменяйтесь новой межсетевой информацией.

Не удастся создать мастер-ключи

После установки базовых компонентов и регистрации модуля VPN не получается создать мастер-ключи, отображается ошибка «Алгоритм не найден».

Возможные причины

Нарушена цепочка доверия сертификатов.

Устранение проблемы

- 1 Перевыпустите все сертификаты.
- 2 Запустите установку ViPNet Prime. При установке укажите путь к новому сертификату.

Устройство устанавливает удаленное в ViPNet Prime обновление

Устройство скачивает с ViPNet Prime и устанавливает устаревшее обновление, которое было удалено в веб-интерфейсе ViPNet Prime.

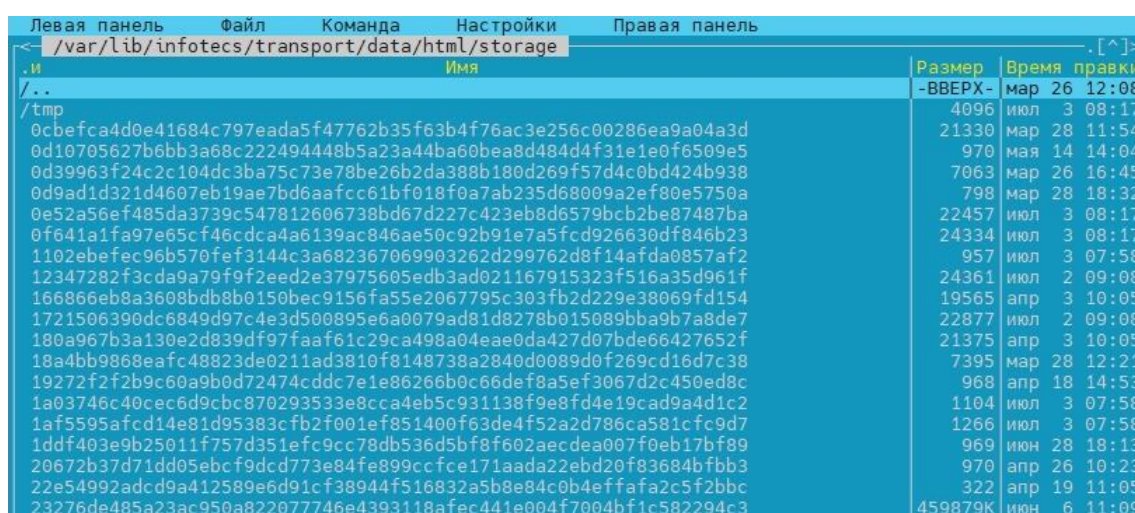
Возможная причина

При удалении обновления в ViPNet Prime оно не удаляется с транспортного сервера UT и устройство может его скачать.

Устранение проблемы

Удалите неактуальные обновления на сервере:

- 1 На компьютере с ViPNet Prime перейдите в папку
`/var/lib/infotecs/transport/data/html/storage/`



Имя	Размер	Время правки
0cbe4d0e41684c797eada5f47762b35f63b4f76ac3e256c00286ea9a04a3d	4096	июл 3 08:17
0d10705627b6bb3a68c222494448b5a23a44ba60bea8d484d4f31e1a0f6509e5	21330	мар 28 11:54
0d39963f24c2c104dc3ba75c73e78be26b2da388b180d269f57d4c0bd424b938	970	мая 14 14:04
0d9ad1d321d4607eb19ae7bd6aaacc61bf018f0a7ab235d68009a2ef80e5750a	7063	мар 26 16:45
0e52a56ef485da3739c547812606738bd67d227c423eb8d6579bcb2be87487ba	798	мар 28 18:32
0f641a1fa97e65cf46cdca4a6139ac846ae50c92b91e7a5fcd926630df846b23	22457	июл 3 08:17
1102ebefec96b570fef3144c3a682367069903262d299762d8f14afda0857af2	24334	июл 3 08:17
12347282f3cda9a79f9f2eed2e37975605edb3ad021167915323f516a35d961f	957	июл 3 07:58
16686eb8a3608bdb8b0150bec9156fa55e2067795c303fb2d229e38069fd154	24361	июл 2 09:08
1721506390dc6849d97c4e3d500895e6a0079ad81d8278b015089bba9b7a8de7	19565	апр 3 10:05
180a967b3a130e2d839df97faaf61c29ca498a04eae0da427d07bde66427652f	22877	июл 2 09:08
18a4bb9868eafc48823de0211ad3810f8148738a2840d0089d0f269cd16d7c38	21375	апр 3 10:05
19272f2f2b9c60a9b0d72474cddc7e1e86266b0c66def8a5ef3067d2c450ed8c	7395	мар 28 12:21
1a03746c40cec6d9c8c870293533e8cca4eb5c931138f9e8fd4e19cad9a4d1c2	968	апр 18 14:53
1af5595afc1d4e81d95383cfb2f001ef851400f63de4f52a2d786ca581cfc9d7	1104	июл 3 07:58
1ddf403e9b25011f757d351efc9cc78db536d5bf8f602aecdea007f0eb17bf89	1266	июл 3 07:58
20672b37d71dd05ebcf9dcd773e84fe899ccf171aada22ebd20f83684bfb3	969	июн 28 18:13
22e54992adc9a412589e6d91cf38944f516832a5b8e84c0b4effafa2c5f2bbc	970	апр 26 10:23
23276de485a23ac950a82207746e4393118afec441e004f7004bf1c582294c3	322	апр 19 11:05
	459879K	июн 6 11:09

Рисунок 73. Поиск файла обновления

- 2 Найдите файл обновления: откройте поочередно все файлы обновлений и внутри каждого перейдите в `body` — ZIP-архив, который формируется при загрузке обновления в ViPNet Prime. По названию вложенных файлов убедитесь, что нашли верный файл.

body/uz ip: //			Имя		Размер	Время правки
va_vipnet_base_x86_64_driv_5.3.1-8730.zip					-ВВЕРХ-	июн 6 11:09
va_vipnet_base_x86_64_driv_5.3.1-8730.zip.sig					459876K	мая 28 12:28
					2529	мая 28 12:31

Рисунок 74. Архив с обновлением на транспортном сервере



Примечание. Объем обновления для координатора около 300 Мбайт.

3 Удалите файл обновления в папке `/var/lib/infotecs/transport/data/html/storage/:`

```
sudo rm <название_файла_обновления>
```

Например:

```
sudo rm fdd5724fd40813a6a583ccc95b83e99ccc4a808c976841328a63bef782e54248
```

Не сопоставились лицензии при загрузке файла

Если при обновлении лицензии на функцию ViPNet Prime не сопоставил новые лицензии старым автоматически и не предложил сделать это вручную, чтобы назначить новую лицензию на функцию или устройство, выполните:

- 1 [Распределите лицензии в организацию](#).
- 2 Если при смене лицензий требуется контролировать отправку обновлений справочников и ключей, [отключите автоматическую отправку](#).
- 3 Перейдите к управлению функцией на узле, нажмите , выберите нужную лицензию и сохраните изменения.
- 4 [Включите автоматическую отправку обновлений справочников и ключей](#), если отключали, или отправьте справочники и ключи вручную.

Не принимается межсетевая информация из доверенной сети

Возможная причина

На узле центра управления ViPNet Prime и в доверенной сети установлены разные версии ViPNet Client.

Устранение проблемы

Чтобы межсетевая информация принималась, администратору доверенной сети необходимо установить на узле с ViPNet Administrator или с центром управления ViPNet Prime актуальную версию ViPNet Client:

- ViPNet Client for Windows 4.5.3 hotfix 7 и выше,
- ViPNet Client for Windows 4.5.5 hotfix 9 и выше,
- ViPNet Client 5 for Windows 5.1 и выше,
- ViPNet Client 5 for Linux 5.0.0 или 5.1.3 и выше.

До установки актуальной версии ViPNet Client в доверенной сети вы можете загрузить межсетевую информацию вручную. Для этого получите от администратора доверенной сети файл с межсетевой информацией доверенным способом.

Отображаются неверные дата и время mftp-конвертов

После обновления ViPNet Prime до версии 1.9.14 в журнале транспортных конвертов неверно отображаются дата и время статусов mftp-конвертов.

Устранение проблемы

Не включайте автоматическую отправку справочников и ключей и дождитесь, пока дата и время статусов mftp-конвертов синхронизируется с информацией из модуля VPN.



История версий

Что нового в версии 1.9.12

- **Смена типа, поколения или лицензии для узла ViPNet Client**

Ранее, чтобы сменить лицензию на узле вручную, нужно было создать новый узел в ViPNet Prime и заново настраивать его. Теперь вы можете вручную сменить тип, поколение или только лицензию узла. Подробнее см. в разделе [Смена типа узла и лицензии клиента](#).

- **Смена типа узла координатора поколения ViPNet 5**

Ранее вы могли сменить тип только для координаторов поколения ViPNet 4. Для координаторов поколения ViPNet 5 требовалось создавать новый узел. Теперь вы можете в ViPNet Prime сменить тип или лицензию координатора поколения ViPNet 5 без создания нового узла. Подробнее см. в разделе [Смена типа и лицензии координатора](#).

- **При создании узла для ViPNet HardPhone необходимо включать функцию Защищенный смартфон HardPhone**

Начиная с ViPNet Prime версии 1.9.12 меняется порядок лицензирования ViPNet HardPhone. Подробнее см. в разделе [Создание узла ViPNet HardPhone](#).

- **Ранее при использовании в сети ViPNet Coordinator KB требовалось не менее двух координаторов KB, чтобы они получили информацию о ДСДР. Теперь достаточно одного такого координатора**
- **Поддержка ViPNet Coordinator IG100-A1 версии 5**

Что нового в версии 1.9.11.1

- **Увеличено допустимое количество ресурсов в одной организации**

Теперь в одну организацию вы можете добавить до 65535 ресурсов. При этом общее количество туннелируемых IP-адресов в связях клиента не должно превышать 3000, иначе вы не сможете установить дистрибутив ключей на узле ViPNet Client 4U или ViPNet Client 5.

- **Поддержка Astra Linux Special Edition 1.8.3.8**
- **Улучшение интерфейса:**
 - Рекомендации по выбору времени применения ключей на узлах при смене мастер-ключей сети

Что нового в версии 1.9.11

- **Смена поколения для узлов координаторов**

Раньше вы могли в ViPNet Prime поменять тип или лицензию координатора только в рамках поколения ViPNet 4. Теперь вы можете сменить поколение в рамках одного семейства. Подробнее см. [Смена поколения координатора](#).
- **Поддержка узлов виртуальной сети квантового распределения ключей:**
 - ViPNet КУКС VA
 - ViPNet РУКС VA

Подробнее см. [Создание узлов сети квантового распределения ключей](#).
- **Поддержка функции «межсетевой шлюз» для ViPNet Coordinator IG 4 и IG 5**

Теперь вы можете использовать координаторы ViPNet Coordinator IG 100 в качестве межсетевого шлюза при создании межсетевого взаимодействия.
- **Поддержка централизованного обновления ViPNet L2Q-10G**
- **Рекомендуемое свободное место на диске:**
 - 1 Тбайт, если установлены только Ядро и модуль VPN,
 - 2 Тбайт, если установлены все модули.

Что нового в версии 1.9.10

- **Возможность сменить мастер-ключи сети без переразворачивания узлов сети**

Теперь после смены мастер-ключей сети поколения ViPNet 4 вам не потребуется заново разворачивать узлы защищённой сети. Чтобы ключи были приняты на узлах и работа сети не нарушилась, выполните обязательные подготовительные действия. Подробнее см. [Смена мастер-ключей сети](#).
- **Поддержка клиентского узла сети квантового распределения ключей ViPNet QTS — ViPNet КУКС**

Подробнее см. [Создание узлов сети квантового распределения ключей](#).

- **Возможность вручную обрабатывать полученную межсетевую информацию**

Теперь при получении межсетевой информации вы можете просмотреть изменившиеся связи и принять или отклонить всю межсетевую информацию. Автоматическая обработка межсетевой информации больше недоступна. Межсетевая информация обрабатывается только вручную администратором. Подробнее см. [Обработка межсетевой информации](#).

- **Одностороннее удаление связей при взаимодействии с доверенной сетью**

Раньше при удалении связи одной из сторон межсетевого взаимодействия она передавалась в межсетевой информации в статусе Запрошена. Чтобы связь удалась, требовалось удалить её в обеих сетях. Теперь при удалении связи в одной из сетей в межсетевой информации связь передается в статусе Удалена и удаляется в обеих сетях. Подробнее см. [Обработка межсетевой информации](#).

- **Возможность установить ViPNet Prime на компьютер с Astra Linux Special Edition («Смоленск») 1.8 или Astra Linux Special Edition («Воронеж») 1.8**
- **Прекращена поддержка ViPNet Terminal**

Что нового в версии 1.9.9

- **Обновление истёкших сертификатов и CRL в командной строке**

Теперь суперадминистратор может обновлять свои истёкшие сертификаты и CRL в командной строке. Подробнее см. [Обновление сертификата администратора](#).

- **Возможность задания минимальной длины и максимального срока действия пароля**

Подробнее см. [Настройка длины и срока действия пароля](#).

- **Индикаторы истечения срока действия сертификатов и CRL**

В веб-интерфейсе появились индикаторы, которые помогают отслеживать истечение срока действия сертификатов и CRL. Подробнее см. [Отслеживание срока действия сертификатов и Общая информация](#).

- **Запрет использования символа / в имени учётной записи ViPNet Prime**

Что нового в версии 1.9.8

- **Управление функциями для ViPNet Coordinator HW 5**

- Обновление базы вредоносного ПО.
- Обновление базы URL-категорий.
- SSL-инспекции.

- **Поддержка устройств поколения ViPNet 4:**

- ViPNet L2Q-10G.
- ViPNet Client для ОС Аврора.
- **Совместный доступ к ресурсам координатора**
Теперь вы можете выбирать, к каким туннелируемым ресурсам координатора предоставлять совместный доступ доверенным организациям при межсетевом взаимодействии. Подробнее см. [Управление доступом к ресурсам при межсетевом взаимодействии](#).
- **Роль Сетевой администратор шлюза безопасности**
Сетевой администратор шлюза безопасности может удаленно подключаться к ViPNet Coordinator HW версии 5.4.1 и выше через веб-интерфейс и управлять его настройками, не связанными с фильтрацией трафика. Подробнее см. [Сетевой администратор шлюза безопасности](#).
- **Настройка интервала блокировки входа в учетную запись**
Теперь вы можете [настроить время блокировки входа в учетную запись](#) после четырех неуспешных попыток ввода пароля.

Что нового в версии 1.9.6

- **Поддержка узлов сети квантового распределения ключей ViPNet QTS и QTS Lite**
 - «КУКС Лайт» — клиентский узел ViPNet КУКС Лайт.
 - «РУКС Лайт» — распределительный узел ViPNet РУКС Лайт.
 - «РУКС» — распределительный узел ViPNet РУКС.
- **Копирование связей шлюза безопасности**
Вы можете скопировать связи для координатора, узла ViPNet xFirewall или узлов квантовой сети с другого шлюза, [чтобы упростить замену или развертывание шлюзов со схожими связями](#).
- **Передача VPN-трафика от клиентов через сервер соединений**
По умолчанию VPN-трафик от клиентов направляется до других узлов оптимальным маршрутом. Если некоторый координатор недоступен, трафик перенаправляется через другой координатор. В этом случае нагрузка на другой координатор увеличивается. Чтобы контролировать нагрузку на координаторы, вы можете [направлять VPN-трафик от клиентов к другим узлам строго через их сервер соединений \(координатор\)](#).
- **Лицензирование продукта и его модулей**
Теперь продукт ViPNet Prime и его модули лицензируются. Поддержаны лицензии:
 - «Prime» (обязательная);
 - «VPN module» (обязательная);
 - «Policy Management module»;

- «Network Visibility System».

Эти лицензии не учитываются в биллинге. В свойствах лицензии «VPN module» можно посмотреть номер сети ViPNet, идентификатор, срок окончания действия, максимальную версию ПО в сети ViPNet, имя владельца сети ViPNet, номер головной сети ViPNet.

В ViPNet Prime версии 1.9.6 и выше больше нельзя использовать лицензию *.itcslic, которая не содержит обязательные лицензии «Prime» и «VPN module». Если лицензия на продукт или модуль отсутствует, функциональность будет ограничена. При обновлении ViPNet Prime с версии 1.9.5.3 на 1.9.6 для сохранения функциональности обновите лицензию.

Раньше уведомление об истечении срока действия лицензии отображалось за 7 дней, теперь для удобства — за 30 дней.

- **Лицензирование управления устройствами в модулях**

Лицензируется количество устройств, которыми вы можете управлять в модулях ViPNet Prime Policy Management и ViPNet NVS соответственно:

- «Policies nodes» — определяет количество устройств в организации, политиками безопасности которых можно управлять в ViPNet Prime Policy Management.
- «Monitoring nodes» — определяет количество устройств в организации, которые можно установить на мониторинг в ViPNet NVS.

Эти лицензии учитываются в биллинге.

- **Лицензирование создания новых организаций**

Поддержана лицензия «Multitenancy mode». Она позволяет создавать новые организации в ViPNet Prime. По умолчанию доступна только одна организация. Если у вас уже существует несколько организаций, то ограничивается только создание новых организаций. Создание подразделений не ограничивается лицензией.

- **Поддержка ViPNet Coordinator KB 4**

Поддержано централизованное управление шлюзами ViPNet Coordinator KB 4. В ViPNet Prime поддерживаются лицензии «Coordinator KB100», «Coordinator KB1000», «Coordinator KB2000», «Coordinator KB5000», функция кластера «Failover KB100». На координаторах KB1000, KB2000 и KB5000 функциональность кластера входит в лицензию на координатор и не лицензируется отдельно.

- **Смена алгоритма шифрования для следующей серии ключей ДСДР**

Чтобы перейти на алгоритмы ГОСТ 34.12-2018 «Магма» и «Кузнечик» на ViPNet Coordinator KB 5, вы можете сменить алгоритм шифрования следующей серии ключей ДСДР. Алгоритм сменится на всех координаторах KB 5 в защищенной сети.

- **Лицензирование дополнительной функции ViPNet Coordinator IG 5**

Поддержана лицензия «IEC101-IEC104 Converter» — включает возможность использования преобразователя протоколов IEC 60870-5-101 и IEC 60870-5-104 на ViPNet Coordinator IG версии 5.

- **Выбор источника случайных чисел при установке ViPNet Prime**

Для выполнения требований безопасности теперь при установке продукта требуется выбрать источник случайной последовательности для криптографических операций:

- `hardware` — физический датчик случайных чисел (ФДСЧ). Требуется предварительной настройки ФДСЧ.
- `biological` — биологический датчик случайных чисел (электронная рулетка). Требуется обслуживания один раз в месяц.
- `native` — нативный источник энтропии или программный датчик, который для случайной последовательности использует встроенный генератор случайных чисел UNIX-системы.

См. «ViPNet Prime. Руководство по установке», «Выбор источника энтропии случайных чисел».

```
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 75. Выбор источника случайных чисел при установке

Чтобы изменить источник энтропии, требуется заново запустить установщик ViPNet Prime. Если выбран ФДСЧ и он не настроен, то установка прервется и отобразится ошибка с просьбой настроить датчик. См. документацию производителей АПМДЗ «Соболь» и «Аккорд-АМДЗ».

Если в ViPNet Prime версии 1.9.5.x вы использовали скрипт настройки нативной энтропии `enable-native-entropy.sh` из комплекта поставки, то в версии 1.9.6 этот скрипт больше не используется.

- **Обновление TLS-сертификатов сервера ViPNet Prime с помощью специального скрипта**

Теперь вы можете обновить TLS-сертификаты с помощью скрипта `install-certificates.sh`. См. «ViPNet Prime. Руководство по установке».

- **Изменения в работе контроля целостности**

Раньше если сервис из состава ViPNet Prime Management Services не проходил контроль целостности, то блокировался только сам сервис. Теперь это также приводит к блокировке сервисов, отвечающих за создание ключей, из состава ViPNet Prime Key Center. В результате блокируется работа в модуле VPN.

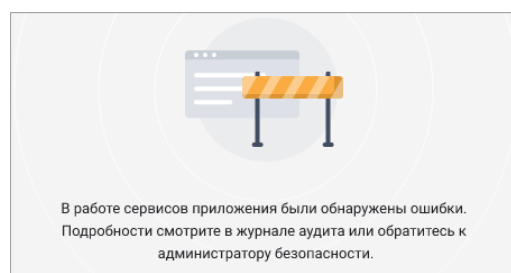


Рисунок 76. Ошибка при проверке целостности и работоспособности ПО

- **Изменения интерфейса**

Удалена возможность назначить функцию «Защищенный интернет-шлюз» на ViPNet Coordinator KB, так как она не поддерживается координатором.

Что нового в версии 1.9.5.3

- **Оптимизация производительности**

Увеличили скорость работы модуля VPN. Теперь быстрее на 30% выдаются дистрибутивы ключей, обрабатываются справочники и ключи, межсетевая информация.

Раньше минимальные системные требования к базовой установке ViPNet Prime Core и VPN — 8 CPU и 16 Гбайт RAM подходили для сети ViPNet размером до 2000 узлов, теперь — до 6000 узлов.

- **Поддержка сред виртуализации**

- VMware Workstation Pro 15.x, 16.x
- zVirt 4.1

Что нового в версии 1.9.5.2

- **Исправление ошибок**

- **Стабильное обновление ViPNet Prime с версий 1.7.2 и 1.7.2 fix4**

Что нового в версии 1.9.5.1

- **Смена мастер-ПИНа**

Исправлена ошибка при смене мастер-ПИНа, которая приводила к потере сетевой связности узлов поколения ViPNet 5.

- **Исправление ошибок**

Ограничение обновления ПО ViPNet Prime на версию 1.9.5.1

При обновлении на версию 1.9.5.1 не изменяйте порты модулей, иначе модули станут недоступны. Для устранения этого придется переустановить ПО и указать предыдущие значения портов, затем подключить модули заново.

Что нового в версии 1.9.5

- **Лицензии**

- **ViPNet CSS Connect HW** — аппаратный телефон ViPNet CSS Connect HW поколения ПО ViPNet 4 с дистрибутивом ключей *.dst.
- **ViPNet Coordinator HW10 F1**
 - «Coordinator HW10» — для ViPNet Coordinator HW10 F1 версии 4.
 - «VPN 10» — функции VPN-шлюза.

На ViPNet Coordinator HW10 F1 не поддерживается функция кластера и не регистрируются клиенты.

- **ViPNet Coordinator IG1000**
 - «Coordinator IG1000 v.5».
 - «Coordinator IG-VA1000 v.5».
 - «VPN IG1000» — функции VPN-шлюза.
 - «Failover IG1000» — функции кластера.

Регистрируйте не более 100 клиентов на этом типе координатора.

- **Расширенные настройки ViPNet Client 4U**

Теперь вы можете [задать дополнительные настройки на клиенте в формате YAML](#).

- **Блокировка VPN без EPP**

Если на клиенте не установлено приложение ViPNet EPP Агент, то вы можете [настроить блокировку пользовательского защищенного трафика на узле](#). DNS-трафик и служебный трафик не блокируются при этом. Блокировка VPN-трафика защитит сеть от подключений с узлов, которые не соответствуют требованиям безопасности.

- **Использование клиентов и ресурсов из доверенных организаций в политиках безопасности**

Клиенты и ресурсы, предоставленные в совместный доступ доверенным организациям, теперь доступны для выбора в ViPNet Prime Policy Management в доверенных организациях.

- **Новые возможности журнала транспортных конвертов**

- **Статусы результирующих политик**

Теперь вы можете просмотреть статусы при отправке, получении и применении на устройствах с ПО ViPNet 5 результирующих политик безопасности из ViPNet Prime Policy Management.

- **Статусы обновлений VPN**

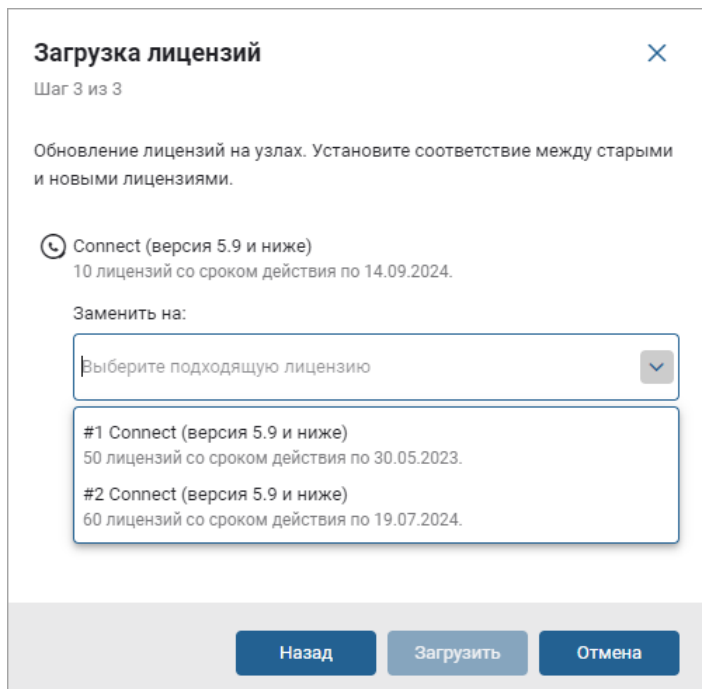
Теперь вы можете просмотреть статусы при отправке, получении и применении на устройствах с ПО ViPNet 5 справочников и ключей, обновлений ПО ViPNet из ViPNet Prime VPN.

- **Загрузка лицензий с истекшим сроком действия**

Теперь, если в общем файле лицензии на сеть есть просроченные лицензии на продукты и их функции, загрузка файла не блокируется, и вы можете загрузить его в ViPNet Prime.

- **Нумерация новых лицензий при обновлении лицензии**

Для удобства сопоставления старых и новых лицензий на продукты и их функции при обновлении общего файла лицензии нумеруются новые лицензии в выпадающем списке.



Загрузка лицензий ✕

Шаг 3 из 3

Обновление лицензий на узлах. Установите соответствие между старыми и новыми лицензиями.

 Connect (версия 5.9 и ниже)
10 лицензий со сроком действия по 14.09.2024.

Заменить на:

Выберите подходящую лицензию ▼

- #1 Connect (версия 5.9 и ниже)
50 лицензий со сроком действия по 30.05.2023.
- #2 Connect (версия 5.9 и ниже)
60 лицензий со сроком действия по 19.07.2024.

Назад Загрузить Отмена

Рисунок 77. Установка соответствия между старыми и новыми лицензиями при обновлении лицензии

- **Изменения интерфейса в отчетах для биллинга**

График использования лицензий **Отчет для биллинга** больше не отображается. В **Статистика использования** столбец **Расход лицензий за период** переименован в **На конец периода**.

- **Поддержка Astra Linux Special Edition 1.7**

Поддерживаются варианты лицензирования (уровни защищенности) «Смоленск» и «Воронеж». См. «ViPNet Prime. Руководство по установке».

Что нового в версии 1.9.0

- **Взаимодействие между сетями под управлением ViPNet Prime**

Теперь вы можете создать взаимодействие между сетями под управлением ViPNet Prime с использованием алгоритмов шифрования ГОСТ 34.12-2018 «Магма» и «Кузнечик».

- **Лицензирование и биллинг по пользователям**

Теперь приложения ViPNet Client и ViPNet Connect могут лицензироваться по пользователям. Лицензии пользователя содержатся в одном пакете лицензий. Пакет лицензий назначается пользователю, и лицензии для ПО расходуются из этого пакета лицензий. Это позволит приобретать и учитывать лицензии по количеству пользователей, а не используемых устройств.

- **Фиксированное распределение лицензий**

Теперь вы можете ограничивать количество лицензий, распределяемых в организацию, для контроля их перерасхода.

Распределение лицензий для организации

Организация 1

Поиск

Лицензия	Дос...	Распределено	В дочерних	Использ...
Coordinator HW1000 C v.5 (версия 5.9 и ниже) Неограниченное количество со сроком действия по 30.12....		0	0	0
Coordinator HW1000 D v.5 (версия 5.9 и ниже) Неограниченное количество со сроком действия по 30.12....		0	0	0
Coordinator HW2000 v.5 (версия 5.9 и ниже) Неограниченное количество со сроком действия по 30.12....		5	0	0
Coordinator HW5000 v.5 (версия 5.9 и ниже) Неограниченное количество со сроком действия по 30.12....		0	0	0
Coordinator HW10000 v.5 (версия 5.9 и ниже) Неограниченное количество со сроком действия по 30.12....		0	0	0
Coordinator VA100 v.5 (версия 5.9 и ниже) Неограниченное количество со сроком действия по 30.12....		0	0	0
Coordinator VA500 v.5 (версия 5.9 и ниже) Неограниченное количество со сроком действия по 30.12....		0	0	0
Coordinator VA1000 v.5 (версия 5.9 и ниже) Неограниченное количество со сроком действия по 30.12....		0	0	0

Сохранить Отмена

Рисунок 78. Фиксированное распределение лицензий

- **Изменения в отчетах для биллинга**

- **В отчете для биллинга организации**

Изменено отображение количества используемых лицензий. Раньше лицензии отображались за весь выбранный период, теперь — на начало периода. В XML- и XLSX-отчетах теперь отображается номер сети ViPNet, имя организации, ИНН, идентификатор лицензионного объекта.

- **В отчете для биллинга перед ИнфоТеКС**

Раньше лицензии отображались за весь и неполный отчетный период, теперь — на начало и конец отчетного периода. Это позволяет оценить динамику и количество использованных лицензий. В XML- и XLSX-отчетах теперь отображается номер сети ViPNet,

имя организации, ИНН, идентификатор лицензионного объекта, количество используемых лицензий на начало и конец отчетного периода, количество списанных и освобожденных лицензий, количество распределенных лицензий на дату выдачи отчета.

- **Идентификатор лицензионного объекта в отчетах биллинга**

Теперь в отчетах биллинга вы можете различать одноименные лицензии по идентификатору лицензионного объекта (в XML-отчетах по параметру `license_object_id`).

- **Тип организации**

Теперь вы можете фильтровать организации по типу в отчетах биллинга. Для этого при создании организации укажите произвольное название типа организации, например партнер, дистрибьютер, реселлер и тому подобное.

- **Поддержка ViPNet Деловая почта для Linux**

Раньше вы могли назначить приложение ViPNet Деловая почта только клиентам на платформе Windows. Теперь вы можете [назначить приложение клиентам на Linux](#). Настройка действует для всех клиентов сети ViPNet.

- **Новые возможности управления ViPNet Coordinator HW 5**

- **Смена способа аутентификации на координаторе**

Когда вы изменяете способ аутентификации администратора с аутентификации по сертификату на аутентификацию по паролю и обратно, теперь информация об этом отправляется на узел.

- **Использование координатора в качестве шлюза между доверенными сетями**

- **Удаленное обновление ПО ViPNet 5.x из ViPNet Prime**

Теперь вы можете удаленно обновить ПО ViPNet версии 5.x на:

- ViPNet Coordinator HW 5;
- ViPNet Coordinator IG 5;
- ViPNet Coordinator KB 5.

Администратор загружает в ViPNet Prime архив ZIP, затем отправляет на узлы. Архив содержит два файла: обновление в формате ZIP и его электронную подпись в формате SIG.

- **Поддержка лицензий устройств и их функций**

- **ViPNet Coordinator KB 5**

Поддержаны лицензии Coordinator KB100 v.5/KB1000 v.5/KB2000 v.5/KB5000 v.5.

- **Кластер на базе ViPNet Coordinator KB 5**

Поддержаны лицензии Failover KB100 v.5/KB1000 v.5/KB2000 v.5/KB5000 v.5.

- **ViPNet Client 5**

Поддержаны лицензии «Client for Linux v.5», «Universal Client v.5».

- **ViPNet Coordinator IG 5**

- Поддержаны лицензии ViPNet Coordinator IG 5 для исполнений IG10 I1, IG10-I2, IG100, IG100-I4 соответственно «Coordinator IG10 v.5», «Coordinator IG10-I2 v.5», «Coordinator IG100 v.5», «Coordinator IG100-I4 v.5». И теперь вы можете использовать исполнения ViPNet Coordinator IG100 в качестве шлюзового координатора при взаимодействии с другой защищенной сетью.
- **ViPNet xFirewall VA**
Поддержаны лицензии виртуальных исполнений xFirewall VA100/VA500/VA1000/VA2000/VA5000.
- **Инспекция SSL/TLS-трафика для ViPNet xFirewall**
Поддержаны лицензии для инспекции SSL/TLS трафика на шлюзах ViPNet xFirewall для исполнений VA100/VA500/VA1000/VA2000/VA5000/VA/100/1000C/1000D/5000/65000. По умолчанию функция отключена.
- **Кластер и функции IPS для ViPNet xFirewall VA**
Поддержаны лицензии для работы ViPNet xFirewall VA в кластере и лицензии на функции IPS соответственно:
 - Failover xF-VA100/500/1000/2000/5000.
 - IPS xF-VA100/500/1000/2000/5000.
- **ViPNet xFirewall xF65000**
Поддержаны лицензии xFirewall xF65000 для новой аппаратной платформы и соответствующие лицензии для инспекции SSL/TLS-трафика и функций IPS.
- **Регистрация клиентов за ViPNet Coordinator IG100 версии 4**
Теперь вы можете регистрировать клиенты за ViPNet Coordinator IG100 I1 и ViPNet Coordinator IG100 I4 с лицензиями «Coordinator IG100 A0», «Coordinator IG100 B0», «Coordinator IG100 A1», «Coordinator IG100 B1», «Coordinator IG100», «Coordinator IG100-I4».
- **Журнал транспортных конвертов UT**
Раньше для устройств с ПО ViPNet версии 5 (кроме ViPNet xFirewall) вы могли косвенно отследить статус транспортного конверта UT в журналах транспортного сервера. Теперь вы можете просмотреть журнал транспортных конвертов UT в веб-интерфейсе ViPNet Prime.

Если не передан конверт от транспортного сервера к транспортному клиенту, то теперь при разборе неполадок вы можете просмотреть, на каком этапе произошел сбой отправки конверта. По умолчанию журнал хранится 90 дней. Журнал транспортных конвертов доступен в разделе **Управление организацией** в отличие от журнала транспортных конвертов MFTP в модуле VPN.
- **Контроль срока действия мастер-ключей**
Теперь в журнал аудита записываются события, если срок действия мастер-ключа истек.
- **Улучшение внутренней функциональности**
 - **Взаимодействие узлов с использованием алгоритмов шифрования ГОСТ 34.12-2018 «Магма» и «Кузнечик»**

Поддержана маршрутизация трафика между узлами поколения 5 по новым алгоритмам ГОСТ. Теперь в сети ViPNet под управлением ViPNet Prime версии 1.9 стал возможен переход на алгоритмы ГОСТ 34.12-2018 «Мagma» и «Кузнечик» для узлов, которые их поддерживают. Это доступно в сети из узлов ViPNet Coordinator KB 5, ViPNet Coordinator HW 5.3 и выше и ViPNet Client 5.

В частности, теперь координаторы поколения 5 определяют для своего узла и связанных координаторов возможность автоматического перехода на новые протоколы IPLir6.

- **Хранение только актуальных обновлений справочников и ключей на транспортном сервере UT**

Раньше на транспортном сервере UT хранились все обновления и занимали свободное место на сервере ViPNet Prime. Теперь хранятся только последние отправленные справочники и ключи.

- **Новые автоматические связи**

- Если координаторы поколения ViPNet 5 связаны между собой и подключены к внешней сети через сервер соединений, то между их серверами соединений создается связь автоматически. При этом если координатор подключен к внешней сети через цепочку серверов соединений, то связь создается между серверами соединений, которые подключены к внешней сети напрямую и являются последними в цепочке серверов соединений.
- Если связаны координатор, подключенный к внешней сети через сервер соединений, и координатор, который подключен напрямую к внешней сети, автоматически создается связь между сервером соединений узла и координатором, который подключен напрямую к внешней сети.

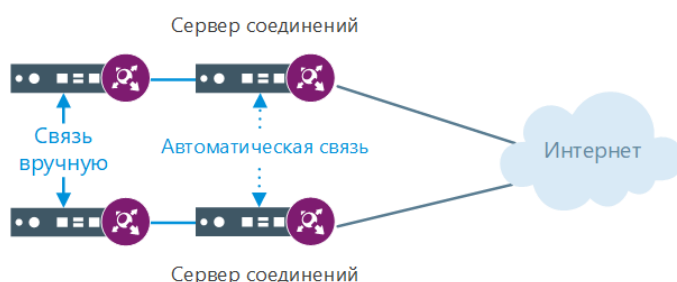


Рисунок 79. Автоматическая связь связанных узлов. Часть 1

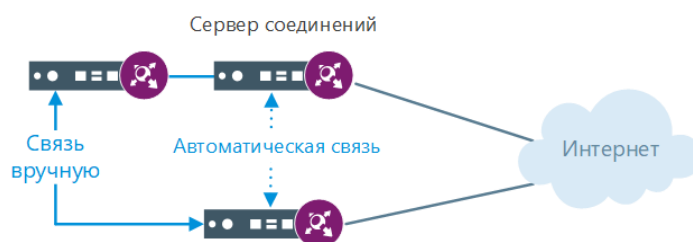


Рисунок 80. Автоматическая связь связанных узлов. Часть 2

- Если создана связь между координатором с ПО ViPNet версии 5, подключенным к внешней сети через сервер соединений, и узлом из доверенной сети, автоматически

создается связь между сервером соединений координатора (последним в цепочке серверов соединений) и шлюзовым координатором в доверенную сеть.

Такие связи отображаются в списке связей узла с причиной **Технологическая связь для поддержания работоспособности сети**.

- **Оптимизация и резервирование маршрутов для узлов поколения ViPNet 5**

Раньше трафик следовал от координатора к координатору согласно топологии сети ViPNet. Теперь часть промежуточных координаторов исключается на пути следования трафика от точки А к точке Б, и трафик передается оптимальным образом.

- **Улучшение поиска и выбора серверов соединений для узлов**

Теперь узлы, которые подключены к внешней сети через сервер соединений, получают информацию от всех серверов соединений об адресах их доступа. Когда для узла не задан адрес доступа, то узел использует адрес последнего сервера соединений в цепочке серверов соединений, который подключен напрямую к внешней сети. Если сервер соединений недоступен для узла, то в качестве сервера соединений автоматически выбирается альтернативный маршрут через доступные координаторы с учетом балансировки нагрузки.

- **Оптимизация контроля целостности приложения**

Приложение блокируется реже в результате проверки контроля целостности, так как проверяется целостность только наиболее важных и выполняющих криптографические функции сервисов приложения и удалены избыточные проверки. См. «ViPNet Prime. Руководство по установке», «Проверка целостности и работы ПО ViPNet Prime».

- **Поддержка домена .vipnet для транспортного сервера**

Теперь транспортному серверу UT назначается ViPNet-идентификатор узла Control Center, который передается на другие узлы. Это позволяет развернуть центр управления Control Center [в туннеле за координатором](#), перенести центр управления на другой компьютер и не зависеть от смены IP-адреса транспортного сервера UT.

- **Возобновление передачи конвертов с прерванного места**

В случае потери связи между транспортными клиентами UT и транспортным сервером UT конверты передаются с прерванного места для экономии трафика.

- **Защита от повторной передачи конвертов на узлы**

При поступлении конверта UT с большим номером ревизии, все последующие конверты UT с меньшей ревизией отбрасываются.

- **Полномочия в ViPNet Client для узлов без пользователей**

Раньше вы создавали узлы ViPNet ConServer и ViPNet CPNS без пользователей и [информация о полномочиях](#) не применялась на узлах. Поэтому вы не могли управлять на узлах без пользователей такими настройками как ввод пароля при запуске приложения ViPNet Client и другими. Теперь информация об уровне полномочий всегда применяется к [клиентам](#) независимо от наличия пользователя на узле.

- **Передача конфигурации и лицензии на узлы с ПО ViPNet 5.x в зашифрованном виде**

- **Оптимизация регистрации событий аудита**

Раньше события аудита могли иметь разные названия при успешном и не успешном событиях. Теперь все события имеют одинаковое название и маркируются [INF] или [ERR] соответственно, что упрощает поиск событий. Также журнал аудита стал подробнее, так как расширен связанными промежуточными событиями для основных действий. Например, событие «Создание базовой сети» теперь сопровождается событиями «Создание клиента» и «Создание координатора».

- **Улучшение взаимодействия с веб-интерфейсом**

- **Удаление нерабочих сценариев из веб-интерфейса**

Теперь вы не можете выбрать ViPNet xFirewall в качестве сервера соединений для координаторов и защищенного DNS-сервера в профилях DNS.

- **Упрощение работы при выборе организаций с вложенной структурой**

Теперь при создании отчетов для биллинга вы можете выбрать все дочерние организации или снять выбор с них, или выбрать все дочерние организации без вложенных.

Если выбраны не все дочерние организации, то вложенный список теперь нельзя свернуть. Это позволяет видеть выбранные организации, не разворачивая структуру.

- **Выбор импортируемых пользователей AD вручную по умолчанию**

Раньше флажок **Выбор импортируемых записей вручную** был отключен по умолчанию, и если вы не замечали его, то импортировались все пользователи из AD в ViPNet Prime. Теперь этот флажок включен по умолчанию, чтобы вы могли просмотреть и отобрать пользователей для импорта сразу, без дополнительных действий.

- **Изменение комплекта документации**

Раньше в поставку входили документы:

- «ViPNet Prime. Руководство главного администратора» для сценариев [поставщика услуг](#) в модели SaaS (Software as a service) или при развертывании ViPNet Prime на собственных серверах.
 - «ViPNet Prime. Руководство администратора организации» для администраторов организаций-потребителей поставщика услуг в модели SaaS.

Теперь эти документы объединены в одном документе «ViPNet Prime. Руководство администратора». Для каждого сценария указаны доступные роли администраторов, за исключением суперадминистратора, так как для него доступны все сценарии.

Что нового в версии 1.7.2 fix4

- Поддержка модуля ViPNet Prime Policy Management версии 1.4
- Поддержка модуля Network Visibility System версии 1.6
- Установка ViPNet Prime без подключения к интернету
- Поддержка Astra Linux Special Edition 1.7.5 («Смоленск»)

- Прекращена поддержка Astra Linux Common Edition Opел 2.12 для новых установок

Что нового в версии 1.7.2 fix3

- Поддержка модуля ViPNet Prime Policy Management версии 1.3.1
- Обновлен транспортный сервер ViPNet Universal Transport

В новой версии транспортного сервера 1.0 hotfix (1.0.0.1655) поддержано переключение кластера ViPNet Coordinator HW 5. Также теперь транспортный сервер автоматически перезапускается после перезагрузки компьютера и его не требуется запускать вручную.

Что нового в версии 1.7.2 fix2

- Поддержка лицензии xFirewall 65000
- Поддержка модуля Network Visibility System версии 1.5.1

Что нового в версии 1.7.2 fix

- Продление срока действия мастер-ключей
- Поддержка модуля ViPNet Prime Policy Management версии 1.3
- Поддержка модуля Network Visibility System версии 1.5

Что нового в версии 1.7.2

Обзор изменений в версии 1.7.2 по сравнению с 1.7.1.

- Поддержка модуля ViPNet Prime Policy Management версии 1.2
- Поддержка модуля Network Visibility System версии 1.4

Что нового в версии 1.8

- Поддержка TLS ГОСТ

Теперь вы можете защитить подключение к веб-интерфейсу ViPNet Prime с помощью российских криптографических алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012. Подробнее о наборе поддерживаемых криптографических алгоритмов см. «ViPNet OSSSL. Руководство разработчика», раздел «Работа с TLS».

Для подключения к веб-интерфейсу по TLS ГОСТ на рабочем месте администратора установите программу ViPNet PKI Client.

- **Поддержка Astra Linux Special Edition «Смоленск» 1.6**

- **Общая установка серверных компонентов ViPNet Prime**

Раньше вы устанавливали серверные компоненты по отдельности. В новой версии эти компоненты устанавливаются вместе.

- **Аутентификация администраторов по сертификатам**

Раньше вы входили в веб-интерфейс ViPNet Prime по имени учетной записи и паролю. Теперь вы можете входить в ViPNet Prime [по личному сертификату](#).

- **Смена мастер-ключей**

Для повышения безопасности реализована смена мастер-ключей по окончании срока действия.

- **Выдача паролей пользователей ViPNet в ПИН-конверте**

Теперь пароль от дистрибутива ключей выдается в распечатанном виде и не сохраняется в ViPNet Prime.

- **Исключена роль офицера безопасности**

Роль офицера безопасности больше не используется. Полномочия роли включены в состав полномочий владельца организации. При обновлении ViPNet Prime с предыдущих версий роль офицера безопасности будет отсутствовать у администраторов.

- **Проверка целостности ПО**

Теперь при запуске ПО ViPNet Prime автоматически проверяется его целостность. Если целостность нарушена, то вход в веб-интерфейс блокируется. Также если правилами организации предусмотрен регламентный контроль целостности используемого ПО, то вы можете [выполнить проверку вручную](#).

- **Поддержка лицензий Connect Hub и Connect File Exchange**

Для уменьшения сетевой нагрузки на узел [с серверным ПО ViPNet Connect](#) теперь вы можете использовать лицензии:

- «Connect Hub» — транспортный сервер на дополнительном узле;
- «Connect File Exchange» — сервер хранения файлов групповых чатов на дополнительном узле.

Серверы предназначены для работы ViPNet Connect версии 3.x. Они выполняют сервисные функции и могут быть предоставлены в совместный доступ доверенным организациям.

Что нового в версии 1.7.1

- **Улучшена работа транспортного сервера Universal Transport (UT)**

Обновлен транспортный сервер UT до версии 1.0. Устранены критичные недостатки, улучшена внутренняя функциональность компонента.

- **Исправление ошибок**

Исправлены ошибки, обнаруженные при эксплуатации предыдущей версии программы.

Что нового в версии 1.7

- **Поддержка ViPNet Coordinator HW версии 5 и выше**

Для нового поколения координаторов формируются дистрибутивы ключей в новом формате (*.ds5).

- **Поддержка нового модуля ViPNet Prime Policy Management**

С помощью нового модуля вы можете:

- централизованно управлять правилами фильтрации трафика на ViPNet Coordinator HW и ViPNet xFirewall;
- импортировать правила фильтрации трафика из оборудования Check Point.

Подробнее см. в документации этого модуля. Установка модуля описана в документе «ViPNet Prime. Руководство по установке».

- **Поддержка нового модуля ViPNet Connect Book**

С помощью нового модуля вы можете создать общий список контактов сотрудников организации для пользователей, которые используют приложение ViPNet Connect. В адресную книгу автоматически добавляются все пользователи из ViPNet Prime. Также вы можете [добавить контакты вручную](#). ПО модуля предоставляется по запросу.

Что нового в версии 1.6

- **Поддержка межсетевых экранов ViPNet xFirewall версии 5.4.1 и выше**

- Централизованное управление функциями кластера горячего резервирования и подсистемой IPS.
- Удаленное обновление ПО и подсистемы DPI.

- **Поддержка ViPNet Coordinator VA5000**

Теперь вы можете управлять с помощью ViPNet Prime координатором ViPNet Coordinator VA5000, который может быть объединен в кластер горячего резервирования.

- **Поддержка новых исполнений ViPNet Coordinator HW версии 4.5.1**

Теперь вы можете управлять с помощью ViPNet Prime исполнениями Coordinator HW100 CU и Coordinator HW50 AU, которые могут быть объединены в [кластер горячего резервирования](#).

Подробнее см. «ViPNet Coordinator HW 4. Подготовка к работе».

- **Поддержка HTTPS при подключении к веб-интерфейсу шлюзов безопасности**

Вы можете выбрать протокол HTTPS и задать порт для перехода к веб-интерфейсу координатора из интерфейса ViPNet Prime. При этом повторно вводить пароль не нужно, так как используется централизованная аутентификация ViPNet Prime. По умолчанию используется протокол HTTP. Настройка поддерживается ViPNet Coordinator HW версии 5.

- **Улучшение структуры отчетов для биллинга**

В выгружаемых XLSX-файлах отчета для биллинга улучшено отображение информации.

- **Загрузка SIP-контактов для пользователей ViPNet Connect**

Импортируйте SIP-контакты из файла CSV. Данные о SIP-контактах будут автоматически и централизованно отправлены для всех пользователей организации. Пользователи смогут найти по имени нужный SIP-контакт в адресной книге приложения ViPNet Connect.



Термины и сокращения

DPI (Deep Packet Inspection)

Технология расширенной инспекции содержимого сетевого трафика на уровнях 2 — 7 модели OSI и накопления статистики. На основании анализа полученных данных идентифицируются приложения и прикладные протоколы.

Администратор безопасности

Администратор, в обязанности которого входит установка, конфигурация и поддержка средств криптографической защиты информации и средств защиты информации.

Базовая сеть

Организация, созданная по умолчанию с названием Core Network. Содержит [центр управления](#) и [центральный координатор](#).

Группа

Клиенты, координаторы или пользователи ViPNet, объединенные под общим именем для удобства администрирования. Задаёт общие свойства (например, создать связь с общим ресурсом) для сетевых объектов ViPNet, входящих в данную группу. Группы можно связывать с другими объектами сети ViPNet.

Дистрибутив ключей

Файл с расширением *.dst или *.ds5 для каждого пользователя узла ViPNet. Создаётся в управляющем ПО ViPNet. Содержит справочники, ключи и файл лицензии для первичного запуска и последующей работы программы ViPNet на сетевом узле. Для работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Доверенная организация

Организация, с которой установлено взаимодействие для обмена информацией по защищенным каналам VPN.

Доверенная сеть

Защищенная сеть, с которой установлено взаимодействие для обмена информацией по защищенным каналам VPN.

Защищённое устройство

Узел **защищённой сети**, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика.

Защищенный интернет-шлюз (открытый интернет)

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

Кластер горячего резервирования

Два взаимосвязанных сервера, один из которых (активный) выполняет функции шлюза безопасности, а другой сервер (пассивный) находится в режиме ожидания. В случае сбоев на активном сервере, пассивный сервер переключается в активный режим для выполнения функций сбойного сервера. При этом сбойный сервер перезагружается и становится пассивным.

С точки зрения сети ViPNet, кластер представлен одним устройством ViPNet.

Клиент (ViPNet-клиент)

Защищённое устройство ViPNet, которое является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Компрометация ключей

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

Координатор (ViPNet-координатор)

Защищённое устройство ViPNet, которое в сети ViPNet VPN выполняет серверные функции, маршрутизацию трафика и служебной информации.

Мастер-ключ

Ключ, который администратор использует для создания симметричных ключей узлов организации.

Мастер-ключ формируется с помощью генератора случайных чисел. Компрометация мастер-ключа приводит к компрометации всех ключей, сформированных на его основе.

Межсетевая информация

Информация о доверенной сети или своей сети, предназначенная для инициации или изменения межсетевого взаимодействия. В состав межсетевой информации входят связи между сетевыми объектами и параметры сетевых узлов ViPNet.

Межсетевое взаимодействие

Передача информации между сетями ViPNet. Позволяет узлам различных сетей ViPNet обмениваться информацией по защищенным каналам VPN.

Межсетевой мастер-ключ

Ключ, служащий для формирования ключей обмена между сетевыми узлами разных сетей ViPNet.

Модуль ViPNet Connect Book

Модуль системы ViPNet Prime для управления адресной книгой пользователей приложения ViPNet CSS Connect.

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](#).

Объект ViPNet

Координатор, клиент, ресурс, пользователь, группа устройств или пользователей, межсетевой экран ViPNet xFirewall, между которыми можно установить связь ViPNet.

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.

Пароль пользователя

Индивидуальный пароль пользователя для работы в приложениях ViPNet на устройстве сети ViPNet. Первоначально создается администратором при создании дистрибутива ключей в управляющем ПО ViPNet. Этот пароль может быть изменен пользователем на устройстве.

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.

Политика безопасности

Набор правил фильтрации трафика и правил трансляции IP-адресов, настроек устройств, которые регулируют безопасность устройств [защищенной сети](#).

Пользователь ViPNet

Лицо, которое использует программное обеспечение ViPNet и имеет ключи для работы с ним.

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.

Профиль DNS

Список доменных зон и закрепленных за ними DNS-серверов.

Ресурс

Отдельное сетевое устройство или целая подсеть, трафик с которыми шифруется не самими устройствами, а координатором, установленным в той же маршрутизируемой сети, с помощью [туннелирования](#) трафика при передаче данных через интернет или другие открытые сети.

Связь ViPNet

Возможность соединения по VPN-каналу устройств защищённой сети.

Сервер IP-адресов

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

Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую.

Сервисные функции

Функции, предоставляемые узлами с установленным управляющим и серверным ПО ViPNet.

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.

Справочники

Набор файлов с информацией об объектах защищенной сети: их именах, идентификаторах (ID), адресах, связях. Эти файлы создаются в ViPNet Prime при создании структуры и конфигурировании сети ViPNet VPN.

Тип межсетевого экрана (ФСТЭК)

Совокупность особенностей межсетевых экранов в зависимости от их применения в информационных системах и технического исполнения (программное или программно-аппаратное), выделяемые классификацией ФСТЭК России. Выделены несколько типов межсетевых экранов: тип «А», тип «Б», тип «В», тип «Г», тип «Д». Подробнее см. [на сайте ФСТЭК России](#).

Туннелирование

Технология для защиты соединений между устройствами локальных сетей, которые связаны через интернет или другие публичные сети. Шифрование трафика устройств выполняется координаторами, установленными на границах локальных сетей. Устройства могут не быть узлами сети ViPNet. Такие устройства называются [ресурсами](#).

Уровень полномочий пользователя ViPNet

Разрешения на определенные действия пользователей на [клиенте](#) по изменению настроек приложений ViPNet.

Устройство

Сетевой объект, который зарегистрирован в ViPNet Prime, но пока еще не задействован в модулях ViPNet Prime.

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.

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.

Центральный координатор

Обязательное устройство сети ViPNet и сервер IP-адресов для [центра управления](#). Маршрутизирует информацию служб и приложений и доставляет на защищённые устройства ViPNet.

Шлюзы безопасности

Координаторы и устройства ViPNet xFirewall.