МИНИСТЕРСТВО ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ МОСКОВСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

03.12.2015 № 16-55/РВ

г. Красногорск

Об утверждении регламента подключения к защищенной виртуальной сети Правительства Московской области (Сеть ViPNet 2131)

В целях выполнения требований нормативных правовых актов и методических документов по технической защите информации на основании Положения о Министерстве государственного управления, информационных технологий и связи Московской области, утвержденного постановлением Правительства Московской области от 13 июня 2012 г. № 820/19,

1. Утвердить прилагаемый регламент подключения к защищенной виртуальной сети Правительства Московской области (Сеть ViPNet 2131) (далее – Регламент).

2. Руководителям центральных исполнительных органов государственной власти Московской области, государственных органов Московской области, органов местного самоуправления муниципальных образований Московской области и государственных учреждений Московской области, не входящих в систему исполнительных органов государственной власти Московской области, при организации работ по подключению к защищенной виртуальной сети Правительства Московской области (Сеть ViPNet 2131) руководствоваться Регламентом.

3. Директору Государственного казенного учреждения Московской области «Московский областной центр информационно-телекоммуникационных технологий» осуществлять подключение телекоммуникационных сетей

000485 *

центральных исполнительных органов государственной власти Московской области, государственных органов Московской области, органов местного самоуправления муниципальных образований Московской области и государственных учреждений Московской области, не входящих в систему исполнительных органов государственной власти Московской области, в соответствии с Регламентом.

4. Контроль за исполнением настоящего распоряжения возложить на заместителя министра государственного управления, информационных технологий и связи А.А. Герасимова.

Министр
государственного управления,
информационных технологий
и связи Московской области М.И. Шадаев

Согласовано:

Первый заместитель министра	А.А. Бородин
Заместитель министра	А.А. Герасимов
Заместитель министра	А.В. Лапунов
Заместитель министра	Ф.Ф. Хуснояров
Заместитель министра	В.Г. Метелев
Заместитель начальника управления специальных систем и информационной безопасности	Д.В. Березин

Исполнитель:

Заведующий отделом информационной безопасности управления специальных систем и информационной безопасности	С.А. Науменко

УТВЕРЖДЕН
распоряжением Министерства
государственного управления,
информационных технологий и связи
Московской области
от №

Регламент подключения к защищенной виртуальной сети Правительства Московской области (Сеть ViPNet 2131)

г. Красногорск, 2015 год

ОГЛАВЛЕНИЕ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

АРМ	-	автоматизированное рабочее место;
ВИС	-	ведомственная ИС;
ЗВС	-	защищенная виртуальная сеть;
ИС	-	информационная система;
ПАК	-	программно-аппаратный комплекс;
ПМО	-	правительство Московской области;
ПО	-	программное обеспечение;
РИС	-	региональная ИС;
РЦОД	-	резервный центр обработки данных;
СКЗИ	-	средство криптографической защиты информации;
ТТ	-	технические требования;
ЦОД	-	центр обработки данных;
ЦОД ДПМО-1	-	основной центр обработки данных;
ЦОД ПМО	-	центры обработки данных Правительства Московской области (в настоящее время - две территориально разнесенные площадки - ЦОД ДПМО-1 и РЦОД);
ЦУС	-	центр управления сетью;
ViPNet Administrator	-	программное обеспечение для администрирования и управления сетью ViPNet;
ViPNet Client	-	программный комплекс, выполняющий на рабочем месте пользователя функции VPN-клиента, персонального экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования;
ViPNet Coordinator	-	сетевой узел сети с установленным программным обеспечением ViPNet Coordinator, размещаемый на границах сетей или сегментов сети и выполняющий в рамках сети ViPNet серверные функции, маршрутизацию трафика и служебной информации;
ViPNet Сеть	-	сеть, организованная с помощью ПО ViPNet и представляющая собой совокупность защищенных сетевых узлов сети ViPNet. Сеть ViPNet имеет свою адресацию, позволяющую организовать обмен

		информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор);
Внешняя сеть	-	сеть, имеющая другое адресное пространство по отношению к внутренней сети. Как правило, этот термин используется для обозначения глобальной сети Интернет. *Внешняя сеть по отношению к рассматриваемой внутренней сети является физически и(или) логически самостоятельной и имеет свое адресное пространство, которое не должно пересекаться с адресным пространством рассматриваемой внутренней сети;*
Внутренняя сеть	-	локальная сеть, подлежащая защите. *Для организации внутренней сети используются IP-адреса из пространства адресов, не применяемых в Интернете (10.0.0.0-10.255.255.255; 172.16.0.0-172.31.255.255; 192.168.0.0-192.168.255.255);*
Дистрибутив ключей	-	файл с расширением .dst, создаваемый для каждого сетевого узла ViPNet и устанавливаемый на узел. В файл помещены адресные справочники, ключевая информация и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы сетевого узла;
Защищенный узел сети	-	оборудование сети с установленным ПО ViPNet с функцией шифрования трафика на сетевом уровне;
Коммуникационное ядро	-	комплекс сетевых устройств, обеспечивающих резервирование каналов и высокоскоростную передачу данных;
Открытый узел сети	-	оборудование сети, с которым обмен информацией происходит в незашифрованном виде;
Туннелирование	-	шифрование трафика открытых узлов сети при передаче через сеть общего пользования;
Туннелируемый узел	-	открытый узел сети, для которого трафик зашифровывается и расшифровывается ViPNet Coordinator для ее передачи другим узлам внутренней сети или во внешнюю сеть;
Файл экспорта	-	файл, содержащий данные об экспортированных сетевых узлах, коллективах и пользователях, данные об сервере-маршрутизаторе, через который будет осуществляться взаимодействие с другой сетью;

Частный адрес	-	IP-адрес из диапазона адресов, которые не применяются в Интернете (10.0.0.0-10.255.255.255; 172.16.0.0-172.31.255.255; 192.168.0.0-192.168.255.255).

2. НАЗНАЧЕНИЕ ДОКУМЕНТА

Настоящий документ разработан с целью определения порядка подключения центральных исполнительных органов государственной власти Московской области, государственных органов Московской области, органов местного самоуправления муниципальных образований Московской области и государственных учреждений Московской области, не входящих в систему исполнительных органов государственной власти Московской области (далее - заявители) к ЗВС Правительства Московской области для организации защищенного взаимодействия с размещаемыми в ЦОД Московской области информационными системами.

В документе приведены сведения для подключения к ЗВС и представлены варианты подключения в зависимости от состава программных или программно-технических средств.

3. ОБЩИЕ СВЕДЕНИЯ О ЗАЩИЩЕННОЙ ВИРТУАЛЬНОЙ СЕТИ

ЗВС организована на базе сертифицированных по требованиям безопасности информации СКЗИ[1], обеспечивающих создание защищенной доверенной среды передачи данных, транспортной средой для которой может являться как сеть Интернет, так и любой коммутируемый канал на базе протокола IP.

ЗВС обеспечивает выполнение требований безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

ЦУС ЗВС и его коммуникационное ядро размещены в ЦОД Правительства Московской области и реализованы с использованием соответственно программного комплекса ViPNet Administrator и программно-аппаратных комплексов ViPNet Coordinator HW. Структура ЗВС и необходимые пояснения представлены на рисунке 1.

Одной из функций ЦУС ЗВС является выдача дистрибутивов ключей, изготовленных организацией, лицензиатом ФСБ России на основании государственного контракта.

Дистрибутивы ключей используются для средств ViPNet, которые включаются в логическую структуру ЗВС, то есть могут рассматриваться как узлы ЗВС, но при этом в состав ЗВС не входят (например, по признаку собственника средства ViPNet).

---

[1] см. сведения о сертификатах ФСБ России, ФСТЭК России на сайте производителя ОАО «ИнфоТекс» http://infotecs.ru/products/cert/

В случае наличия у заявителя собственной защищенной сети ViPNet и обязательного в этом случае установленного в сети средства управления сетью[2] (программного комплекса ViPNet Administrator), средствами ЦУС изготавливается файл экспорта сети ЗВС и сети ViPNet заявителя.

При этом изготовление дистрибутива ключей для узлов сети ViPNet заявителя осуществляется самим заявителем без обращения к услугам ЦУС ЗВС.

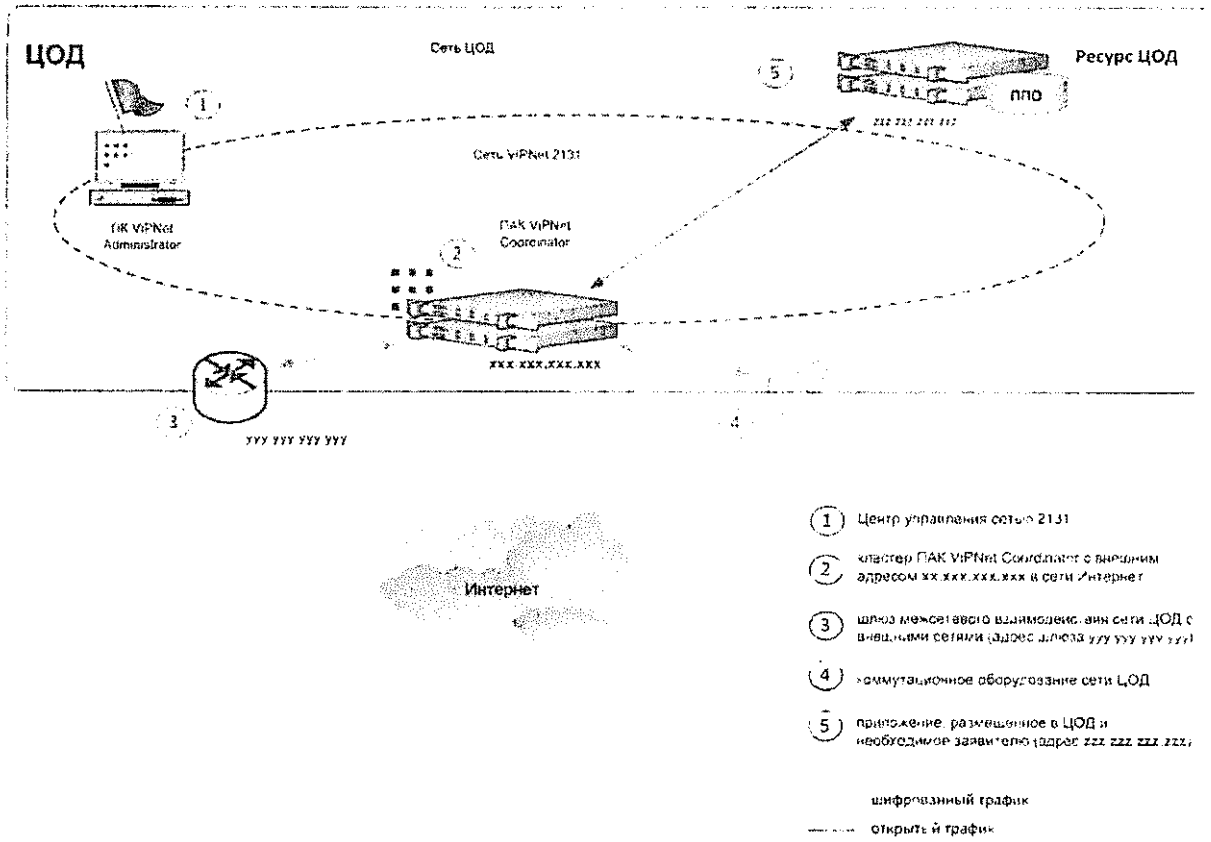

Рисунок 1 – Общая структура сети ViPNet 2131.

4. ОБЪЕКТЫ ПОДКЛЮЧЕНИЯ К ЗАЩИЩЕННОЙ ВИРТУАЛЬНОЙ СЕТИ И ВОЗМОЖНЫЕ СХЕМЫ ПОДКЛЮЧЕНИЯ

В качестве объектов сети заявителя, подключаемых к ЗВС, рассматриваются:

ПАК ViPNet Coordinator HW (100 A,B,C)/1000/2000);

АРМ с установленным ПО ViPNet Client.

Указанные средства создают шифрованный канал передачи данных и по терминологии сетей ViPNet называются защищенными узлами сети.

[2] см. документацию «ViPNet Administrator Центр управления сетью. Руководство администратора», ФРКЕ.00006-05 32 01»

При организации взаимодействия открытых узлов сети заявителя и РИС и ВИС, размещенных в ЦОД, применяется механизм туннелирования трафика.

В режиме туннелирования передаваемые данные остаются незащищенными только на участке от АРМ заявителя до его ViPNet Coordinator HW, в дальнейшем все данные подвергаются шифрованию (рисунки 2а, 2б).

Количество туннелируемых узлов определяется конфигурацией оборудования ViPNet Coordinator HW. В частности, координаторы ПАК ViPNet Coordinator HW100 A/B/C могут поддерживать соответственно 2/5/10 туннелей, координатор ПАК ViPNet Coordinator HW1000 может поддерживать неограниченное количество туннелей[3].

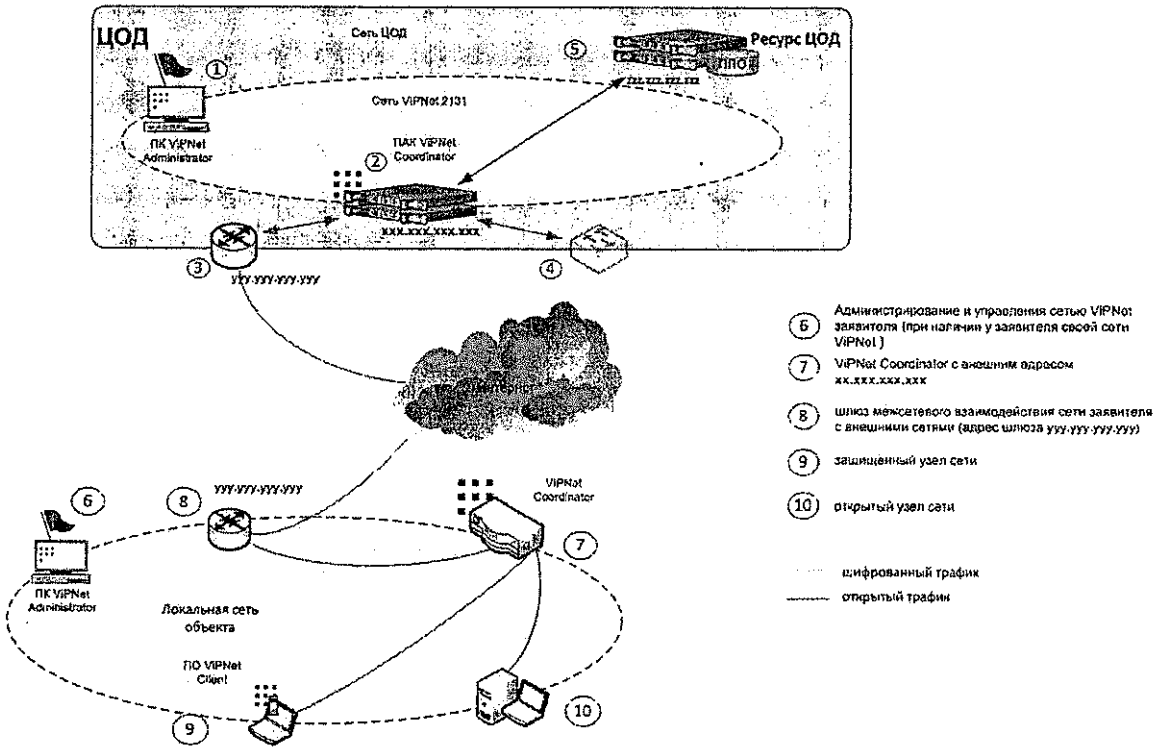

Рисунок 2а – Подключение к сети ViPNet 2131 с использованием арендуемых каналов связи

[3] см. технические характеристики ПО ViPNet Coordinator, ПАК ViPNet Coordinator HW, ПО ViPNet Client на сайте производителя http://infotecs.ru/products/ispolnenie.php?SECTION_ID=&ELEMENT_ID=14322 , http://www.infotecs.ru/products/line/custom.php

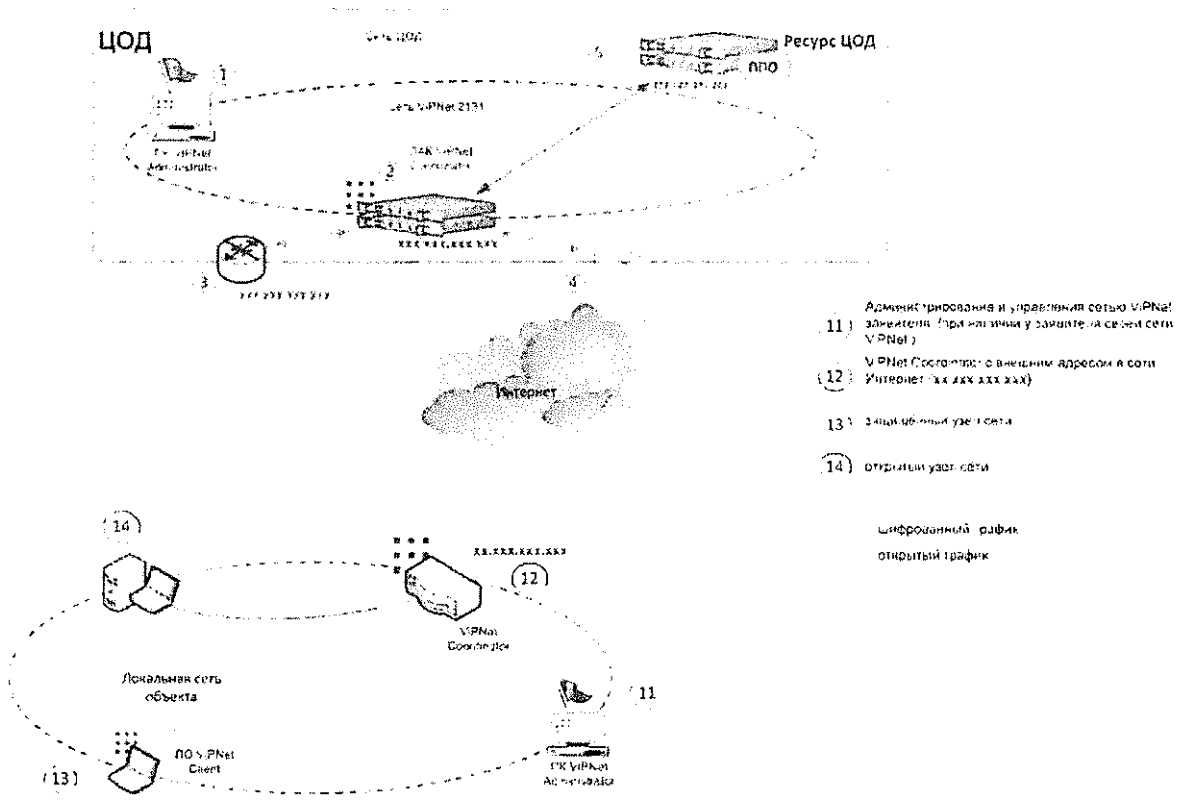

Рисунок 2б – Подключение к сети ViPNet 2131 с использованием сети Интернет

5. ПРОЦЕДУРА ПОДКЛЮЧЕНИЯ К ЗАЩИЩЕННОЙ ВИРТУАЛЬНОЙ СЕТИ И ПОРЯДОК ЕЕ ИСПОЛНЕНИЯ

Заявка на подключение к ЗВС, подписанная руководителем заявителя, направляется в адрес Министерства государственного управления, информационных технологий и связи Московской области (далее – Министерство) по Межведомственной сети электронного документооборота Московской области.

Необходимо в графе «Краткое содержание» указать «Заявка на подключение к ЗВС», к заявке приложить данные согласно п. 5.1. по форме, указанной в Приложении 1.

После рассмотрения заявка направляется в подведомственное Министерству Государственное казенное учреждение Московской области «Московский областной центр информационно-коммуникационных технологий» (далее - ГКУ МО «МОЦ ИКТ»), которое организует выдачу заявителю дистрибутива ключей, файлов экспорта, а также их хранение.

В заявке на получение файлов в зависимости от требуемой схемы подключения к сети ЗВС указываются следующие сведения:

5.1. При отсутствии у заявителя собственной защищенной сети ViPNet:

полное наименование заявителя (органа/ организации/ учреждения);

подключаемые к сети защищенные узлы;

тип ПАК ViPNet Coordinator HW 100 (A/B/C)/ 1000, тип ПО ViPNet Client, с указанием серийного номера оборудования ViPNet Coordinator (s/n);

фамилия, имя, отчество сотрудников (пользователей) заявителя, подключаемых к сети ЗВС;

фамилия, имя, отчество лица, назначенного для решения организационно-технических вопросов в случае их возникновения, (далее - ответственное лицо), его контактный телефон и/или адрес электронной почты;

фамилия, имя, отчество лица, наделенного правом получить дистрибутив ключей (далее – уполномоченное лицо), его контактный телефон и/или адрес электронной почты.

Данные о наличии у заявителя архива регистрационных файлов подключаемых защищенных узлов (предоставляется заявителю поставщиком ViPNet) могут запрашиваться у заявителя сотрудниками ГКУ МО «МОЦ ИКТ» в рабочем порядке.

5.2. При наличии у заявителя собственной сети ViPNet:

полное наименование заявителя (органа/ организации/ учреждения);

номер собственной сети ViPNet;

подключаемые к сети защищенные узлы:

тип ПАК ViPNet Coordinator HW 100 (A/B/C)/ 1000, тип ПО ViPNet Client, с указанием серийного номера оборудования ViPNet Coordinator (s/n);

фамилия, имя, отчество сотрудников (пользователей) заявителя, подключаемых к сети ЗВС;

фамилия, имя, отчество ответственного лица, его контактный телефон и(или) адрес электронной почты;

фамилия, имя, отчество уполномоченного лица, его контактный телефон и(или) адрес электронной почты.

Данные о наличии у заявителя файла импорта сети ViPNet для первоначального обеспечения межсетевого взаимодействия с сетью ЗВС могут запрашиваться у заявителя сотрудниками ГКУ МО «МОЦ ИКТ» в рабочем порядке.

ГКУ МО «МОЦ ИКТ» организует изготовление дистрибутива ключей, файла экспорта в течение 5 рабочих дней с момента регистрации заявки.

Подключение к ЗВС проводится после получения заявителем файлов дистрибутива ключей для настраиваемых защищенных узлов сети или файла экспорта межсетевого взаимодействия сети ЗВС с сетью ViPNet заявителя (файл экспорта), необходимых для настроек ПО ViPNet сети заявителя.

Дистрибутив ключей создается для каждого защищенного узла сети (ViPNet Coordinator, ViPNet Client) и содержит справочники, ключи, данные о лицензиях и другие сведения, необходимые для настройки, первичного запуска и последующей работы ПО ViPNet.

В случае, если для одного АРМ с установленным ПО ViPNet Client требуется организовать доступ к сети ЗВС нескольким пользователям, для каждого пользователя создается отдельный файл *.dst.

Файл экспорта изготавливается при наличии у заявителя собственной сети ViPNet.

По факту изготовления файла уполномоченное лицо оповещается по телефону и(или) электронной почте о возможности получения файла (день, время, кабинет, контактное лицо).

Получение уполномоченным лицом файлов *.dst (файла экспорта) осуществляется под роспись в журнале установленной формы (дата, подпись, расшифровка подписи).

При получении файлов уполномоченное лицо обязано иметь при себе доверенность от имени заявителя на получение файлов *.dst (файла экспорта) (форма приведена в Приложении 2), а также паспорт.

6. СВЕДЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ НАСТРОЙКИ ПОДКЛЮЧЕНИЯ К ЗАЩИЩЕННОЙ ВИРТУАЛЬНОЙ СЕТИ

Настройка и подключение средств ViPNet заявителя к ЗВС возможна при наличии файлов *.dst (файла экспорта) и сведений по IP-адресации взаимодействующих ресурсов сети ЦОД и сети заявителя, а именно:

ip-адреса (xxx.xxx.xxx.xxx) внешних интерфейсов ViPNet Coordinator HW в сети Интернет (рисунок 1, 2б – позиции 2, 12);

ip-адреса (yyy.yyy.yyy.yyy) внешних интерфейсов шлюза межсетевого взаимодействия (рисунок 1, 2а – позиции 3, 8);

ip-адрес (zzz.zzz.zzz.zzz) сервера ресурса в сети ЦОД, с которым организуется взаимодействие (рисунок 1 – позиция 5);

ip-адреса узлов локальной сети заявителя (например, АРМ), для которых должен быть организован шифрованный трафик путем установки ПО ViPNet Client на данные узлы (частные IP-адреса из адресного пространства сети), (рисунок 2а, 2б – позиции 9, 13);

ip-адреса АРМ в пространстве адресов локальной сети заявителя, для которых должен быть разрешен режим туннелирования в сеть ЗВС (частные ip-адреса из адресного пространства сети), (рисунок 2а, 2б – позиции 10, 14).

При модернизации сети ЗВС и ЦОД, настройки и порядок подключения к сети ЗВС уточняются ответственным лицом заявителя.

Приложение 1

Заявка
на изготовление файлов дистрибутива ключей для подключения средств ViPNet заявителя к сети ЗВС Московской области

№ п/п	Необходимые сведения	Представленные сведения
1.	полное наименование заявителя (органа/ организации/ учреждения)	Указать наименование
2.	подключаемые к сети средства ViPNet (серийные номера)	Указать тип средств и их серийные номера
3.	количество сотрудников заявителя, подключаемых к сети ЗВС с указанием Ф.И.О. и должности	Указывается количество сотрудников (Ф.И.О., должность), работающих на АРМ с установленными средствами ViPNet
4.	фамилия, имя, отчество лица, его контактный телефон и(или) эл. почта для уточнения организационно-технических вопросов в случае их возникновения (ответственное лицо)	Знатоков Иван Иванович, +7(498) 123-45-67, znatokov@mosreg.ru , znatokovII@e-mail.ru
5.	фамилия, имя, отчество лица. наделенного правом получить файлы *.dst, его контактный телефон и(или) эл. почта (уполномоченное лицо).	Получателева Мария Ивановна. +7(498) 234-56-78, polucateleva@mosreg.ru, poluchatelevaMI@e-mail.ru

Приложение 2

Адрес

телефон:
факс:
электронная почта:

Должность адресата

И.О. Фамилия адресата

ДОВЕРЕННОСТЬ
на выполнение действий от лица организации

Московская область
г. Красногорск «__» _____ _____ г.

Настоящей доверенностью ГО/ЦИОГВ/ОМСУ Московской области в лице _____ (должность) _____ (Ф.И.О.) уполномочивает _____ (должность) _____ (Ф.И.О.), паспорт: _____, совершать следующие действия:

1. Получать в Государственном казенном учреждении Московской области «Московский областной центр информационно-коммуникационных технологий» дистрибутив ключей/файл экспорта.

2. Расписываться в соответствующих учетных формах, предназначенных для исполнения поручения, определенного настоящей доверенностью.

Настоящая доверенность выдана по _____ (дд мм гггг) Без права передоверия.

Собственноручную
Подпись /_____/ _____(Ф.И.О.)
удостоверяю.

Должность руководителя
ГО/ЦИОГВ/ОМСУ Московской области /_____/ (Ф.И.О.

М.П. «__» _____ _____ г.