МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ МЕДИЦИНСКИМ ОРГАНИЗАЦИЯМ ПО ОРГАЗАЦИИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ КАНАЛОВ ПРИ ВЗАИМОДЕЙСТВИИ В РАМКАХ ЕДИНОЙ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ В СФЕРЕ ЗДРАВООХРАНЕНИЯ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящим документом определен состав средств защиты информации и архитектура построения защищенной информационно-телекоммуникационной сети для организации защищѐнного информационного обмена медицинских организаций в рамках функционирования единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ).

Документ подготовлен в соответствии с «Концепцией создания единой государственной информационной системы в сфере здравоохранения», утвержденной Приказом Минздравсоцразвития России от 28 апреля 2011г. № 364, «Методическими рекомендациями для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости» Минздравсоцразвития России от 24.12.2009г. и письмом Минздравсоцразвития России от 21 февраля 2011г., регламентирующим порядок организации и функционирования защищенного межведомственного взаимодействия по телекоммуникационным каналам передачи данных общего пользования при обмене электронными документами между участниками корпоративной информационной системы на основе технологии ViPNet.

Для организации криптографической защиты каналов связи при информационном обмене в составе МИС на федеральном уровне используется средства защиты информации комплекса VIPNet и дальнейшие варианты по организации типовых подключений основываются на использовании данного типа средств защиты информации.

Обозначение	Описание
ПО	Программное обеспечение
АТК	Аппаратный тонкий клиент
АРМ	Автоматизированное рабочее место
ЕГИСЗ	Единая государственная информационная система в сфере здравоохранения
МО	Медицинские организации - учреждение здравоохранения, медицинская организация, орган исполнительной власти и органы местного самоуправления, осуществляющие деятельность по оказанию государственных и муниципальных услуг в сфере здравоохранения, аптечная и фармацевтическая организации
ЛПУ	Лечебно-профилактическое учреждение
ПАК	Программно аппаратный комплекс

СКЗИ	Средство криптографической защиты данных
VPN	Virtual Private Network (виртуальная частная сеть)
ФО	Федеральный округ
МИАЦ	Медицинский информационной аналитический центр
УЗ	Учреждение здравоохранения
ФЦОД	Федеральный центр обработки данных
МЭ	Межсетевой экран

2. АРХИТЕКТУРА СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ЕГИСЗ

Архитектура системы криптографической защиты должна учитывать объекты взаимодействия ЕГИСЗ:

- Федеральный ЦОД ЕГИСЗ;
- Медицинские организации субъектов Российской Федерации (МО С);
- Медицинские организации Федерального подчинения (МО ФП).

Структура VPN-сети ФЦОД ЕГИСЗ приведена в Приложении 1.

Кроме того при подключении медицинской организации к ЕГИСЗ необходимо различать и отдельно рассматривать:

- МО, имеющие собственную систему защиты каналов;
- МО, имеющие территориально распределенную филиальную структуру с собственными ЛВС;

Технические средства, используемые для подключения должны быть совестимы с используемой в Федеральном ЦОД ЕГИСЗ технологией виртуальных частных сетей – VPN, реализованной на базе продуктов семейства ViPNet, сертифицированных на соответствие требованиям ФСБ России к СКЗИ по классу КС3 и требованиям ФСТЭК России по 3-му классу к МЭ.

3. РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ КАНАЛОВ МЕДИЦИНСКИМ ОРГАНИЗАЦИЯМ ФЕДЕРАЛЬНОГО ПОДЧИНЕНИЯ

В рамках организации защищенных соединений с медицинскими организациями федерального подчинения в ФЦОД ЕГИСЗ организовывается специальный VPN-сегмент на базе технологии ViPNet. Данный VPN-сегмент будет обслуживать подключение МО федерального подчинения.

3.1. Рекомендации по защите каналов при подключении к ЕГИСЗ МО ФП

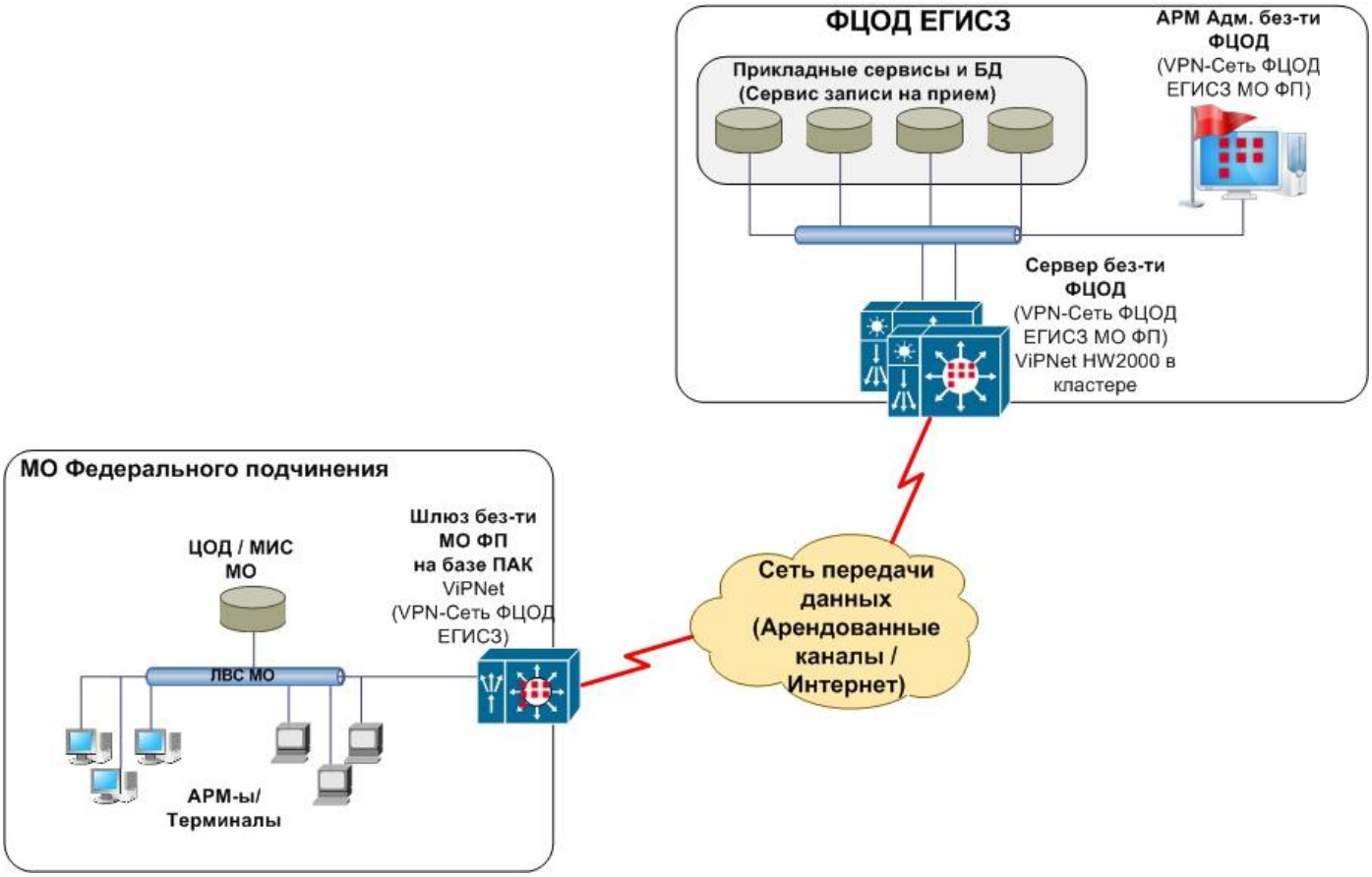
Для организации подключения к ЕГИСЗ в МО федерального подчинения в точке подключения к среде передачи данных должен быть установлен шлюз безопасности на базе программно-аппаратного комплекса ViPNet.

Тип ПАК ViPNet необходимо выбирать в соответствии с рекомендациями, приведенными в разделе 5.

Рекомендации по организации сетевого подключения ПАК ViPNet HW приведены в разделе 6.

Шлюз безопасности МО ФП должен быть подключен к VPN-Сети ФЦОД ЕГИСЗ, таким образом, на этапе ввода в эксплуатацию и дальнейшего обслуживание потребуется привлечение администраторов безопасности VPN-Сеть ФЦОД ЕГСЗ либо организации обслуживающей эту VPN-Сеть.

Схема подключения



3.2. Рекомендации по защите каналов при подключении МО ФП имеющих территориально распределенную филиальную структуру

В том случае если МО ФП имеет территориально распределенные филиалы, каждый из которых необходимо подключить к ЕГИСЗ, рекомендуется на базе МО ФП развернуть собственную VPN-Сеть на базе технологии ViPNet (далее VPN-сеть МО ФП) с последующей интеграцией с VPN-Сетью ЕГИСЗ.

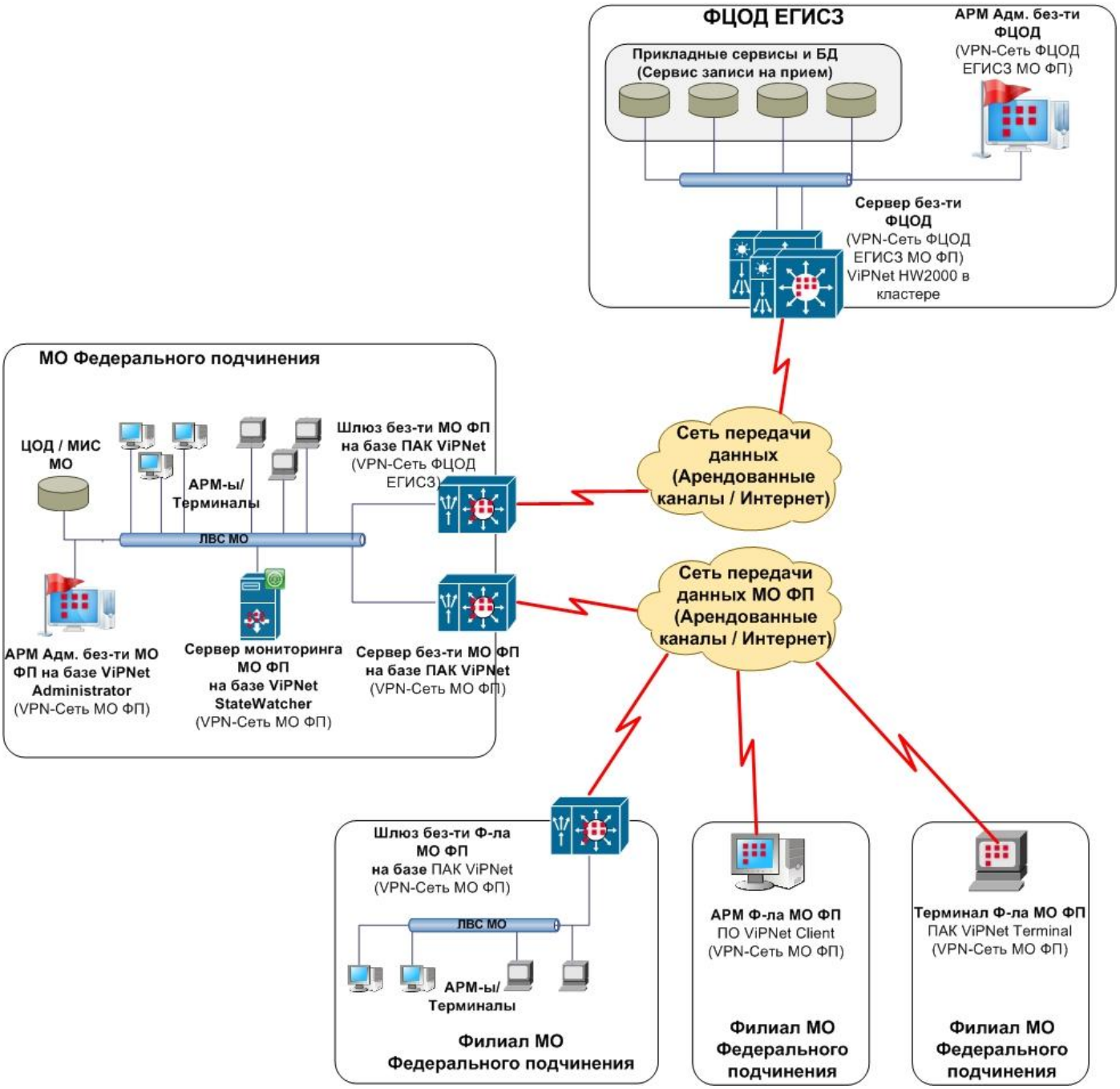
Также рекомендуется развертывание собственной VPN-Сети, если ЛВС МО ФП:

– представляет собой несколько сегментов, расположенных в разных зданиях и объединенных линиями связи, проходящими за пределами контролируемой зоны;

– не находится в пределах контролируемой зоны или контролируемую зону нельзя обеспечить, например в одном здании с МО ФП находятся сторонние

организации, не имеющие никакого отношения к ЕГИСЗ, и у МО ФП и сторонней организации общая ЛВС.

В том случае если в МО ФП развертывается собственная VPN-сеть рекомендуется следующая схема подключения.



С учётом использования в VPN-сети ФЦОД ЕГИСЗ средств СКЗИ сертифицированных по классу КС3 рекомендуется придерживаться этого класса при выборе средств для построения собственной VPN-сети МО ФП.

Тип ПАК ViPNet необходимо выбирать в соответствии с рекомендациями, приведенными в разделе 5.1.

Тип Клиентской компоненты ViPNet необходимо выбирать в соответствии с рекомендациями в разделе 5.2.

Рекомендации по организации сетевого подключения ПАК ViPNet HW приведены в разделе 6.

Для построения собственной VPN-сети должны привлекаться специализированные организации, обладающие лицензиями на следующие виды деятельности:

Лицензии ФСБ России на:

- техническое обслуживание шифровальных (криптографических) средств;
- распространение шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации.

Лицензия ФСТЭК России на:

- осуществление деятельности по технической защите конфиденциальной информации.

4. РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ КАНАЛОВ МЕДИЦИНСКИМ ОРГАНИЗАЦИЯ СУБЪЕКТА РФ

В рамках организации защищенных соединений в ФЦОД ЕГИСЗ организовываются восемь сегментов VPN-сети на базе технологии ViPNet. Один сегмент VPN-сети будет обеспечивает подключение к ЕГИСЗ медицинских организаций одного федерального округа РФ.

Структура VPN-сети ФЦОД ЕГИСЗ приведена в Приложении 1.

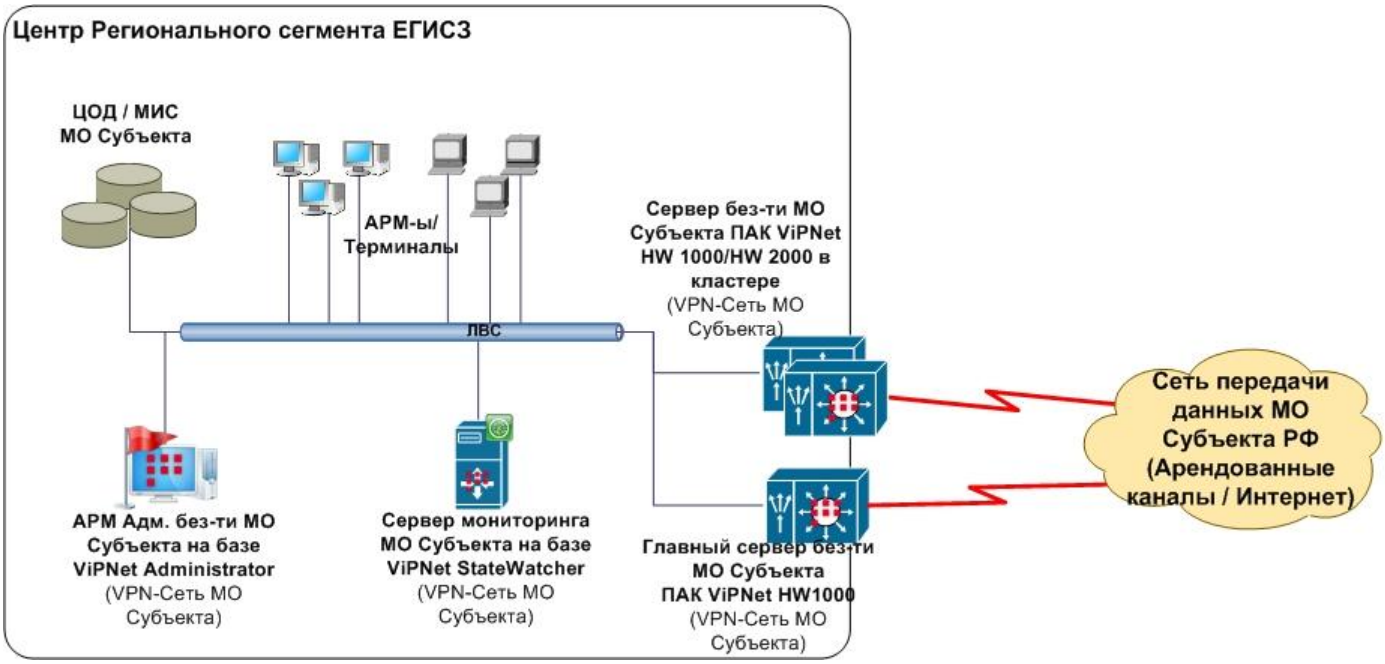
4.1. Рекомендации по архитектуре регионального сегмента системы криптографической защиты ЕГИСЗ

Для организации взаимодействия медицинских организаций субъекта РФ с ЕГИСЗ рекомендуется создание отдельной VPN-сети МО Субъекта РФ.

В качестве организации, на базе которой должен быть создан центр регионального сегмента ЕГИСЗ, рекомендуется выбирать организацию, уполномоченную на модернизацию здравоохранения в регионе или подведомственную ей организацию.

VPN-сеть МО Субъекта РФ рекомендуется строить на базе технологии ViPNet.

Рекомендуется следующая структура Центрального сегмента VPN-сети МО Субъекта РФ:



Рекомендуется включение в состав VPN-сети МО Субъекта РФ двух серверов безопасности:

Название на схеме	**Функция**	**Рекомендуемое оборудование**
Главный сервер безопасности МО Субъекта (VPN-Сеть МО Субъекта)	Выполнение служебных функций для эксплуатации VPN-сети Субъекта РФ: рассылка обновлений ключевой и справочной информации, рассылка обновлений ПО, сервер IP-адресов, сервер для взаимодействия с другими VPN-сетями (собственные сети ЛПУ, ТФОМС).	ПАК Coordinator HW1000
Сервер безопасности МО Субъекта (VPN-Сеть МО Субъекта)	Криптографическая обработка информационных потоков от МО Субъекта РФ адресованного как в ФЦОД ЕГИСЗ, так и в ЦОД Субъекта РФ.	2 ПАК Coordinator HW1000 (режим горячего резервирования) В случае если информационный поток взаимодействия с ЦОД Субъекта РФ значительно превосходит информационный поток взаимодействия с ФЦОД ЕГИСЗ рекомендуется установка 2 ПАК Coordinator HW2000 (режим горячего резервирования)

С учётом использования в VPN-сети ФЦОД ЕГИСЗ средств СКЗИ сертифицированных по классу КС3 рекомендуется придерживаться этого класса при выборе средств для построения VPN-сети МО Субъекта РФ.

Для построения VPN-сети МО Субъекта РФ должны привлекаться специализированные компании, обладающие лицензиями на следующие виды деятельности:

Лицензии ФСБ России на:

- техническое обслуживание шифровальных (криптографических) средств;
- распространение шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации.

Лицензия ФСТЭК России на:

- осуществление деятельности по технической защите конфиденциальной информации.

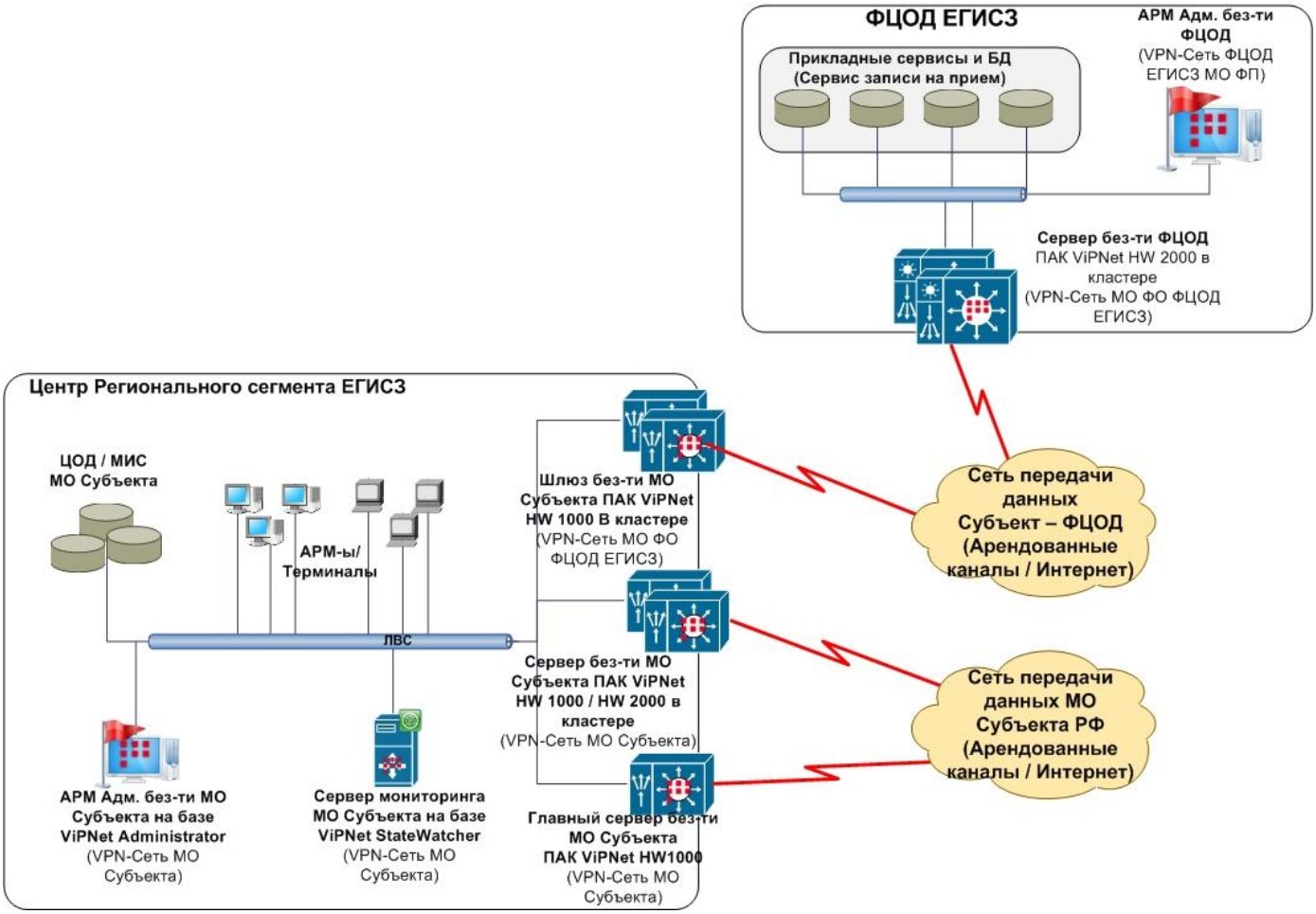
4.2. Рекомендации по подключению Центрального сегмента VPN-сети МО Субъекта РФ к ЕГИСЗ

Для организации подключения Центрального сегмента VPN-сети МО Субъекта РФ к ЕГИСЗ в состав сегмент должен быть установлен Шлюз безопасности из состава VPN-сети ФЦОД ЕГИСЗ, соответствующего федерального округа.

Для реализации такого подключения рекомендуется использовать ПАК ViPNet Coordinator HW1000, установленный в режиме горячего резервирования.

На этапе ввода в эксплуатацию Шлюза безопасности и дальнейшего обслуживание потребуется привлечение администраторов безопасности VPN-Сети ФЦОД ЕГСЗ, либо организации обслуживающей эту VPN-Сеть.

Рекомендации по организации сетевого подключения ПАК ViPNet HW приведены в разделе 6.



4.3. Рекомендации по защите каналов при подключении к ЕГИСЗ медицинских организаций Субъекта РФ

Для организации подключения МО Субъекта РФ к ЕГИСЗ:

– в медицинских учреждениях Субъекта РФ, подключающих сегмент ЛВС в точке подключения к среде передачи данных, должен быть установлен шлюз безопасности на базе программно-аппаратного комплекса ViPNet HW из состава VPN-сети МО Субъекта РФ;

– в МО Субъекта РФ, подключающих один или два рабочих места, должны быть установлены клиентские компоненты ViPNet из состава VPN-сети субъекта РФ.

Тип ПАК ViPNet необходимо выбирать в соответствии с рекомендациями, приведенными в разделе 5.1.

Тип Клиентской компоненты ViPNet необходимо выбирать в соответствии с рекомендациями в разделе 5.2.

Рекомендации по организации сетевого подключения ПАК ViPNet HW приведены в разделе 6.

Для проведения работ должны привлекаться специализированные компании, обладающие лицензиями на следующие виды деятельности:

Лицензии ФСБ России на:

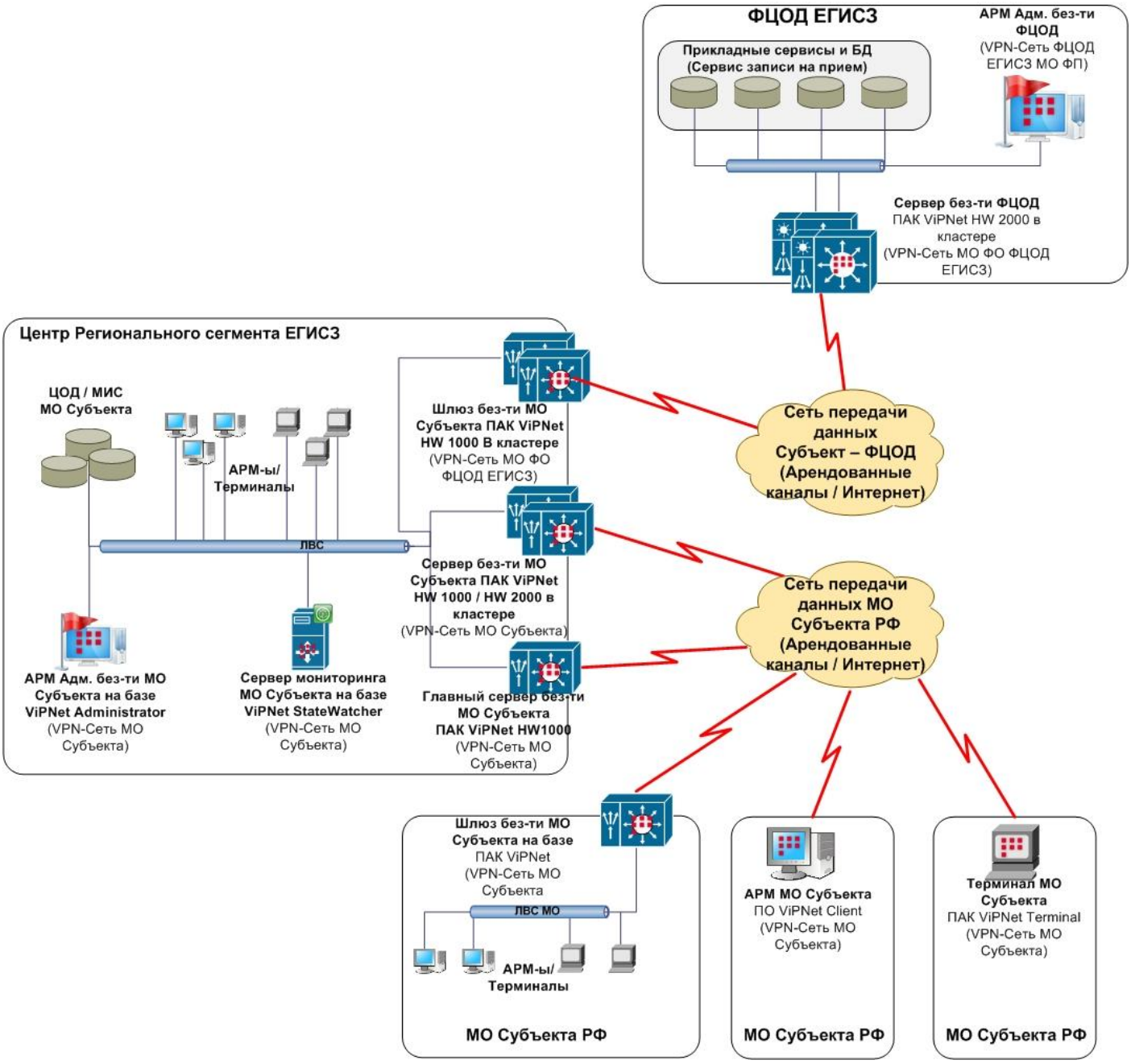
– техническое обслуживание шифровальных (криптографических) средств;

– распространение шифровальных (криптографических) средств;

– предоставление услуг в области шифрования информации.

Лицензия ФСТЭК России на:

– осуществление деятельности по технической защите конфиденциальной информации.



4.4. Рекомендации по защите каналов при подключении МО, имеющего филиальную структуру

Подключение МО Субъекта РФ имеющего филиальную структуру (далее МО СФ) можно осуществить двумя способами:

– подключить главную организацию и каждый филиал МО СФ к VPN-сети МО Субъекта РФ и к ЕГИСЗ как отдельные организации (подробное описание дано в п.4.3.);

– развернуть собственную VPN-сеть на базе технологии ViPNet (далее сеть VPN-сеть МО СФ) с последующей интеграцией этой сети с VPN-сетью МО Субъекта РФ и VPN-сетью ЕГИСЗ.

Развертывание собственной VPN-сети МО СФ снизит нагрузку на эксплуатационный персонал VPN-сети МО Субъекта РФ.

Также рекомендуется развертывание собственной VPN-Сети, если ЛВС МО СФ:

– представляет собой несколько сегментов, расположенных в разных зданиях и объединенных линиями связи, проходящими за пределами контролируемой зоны;

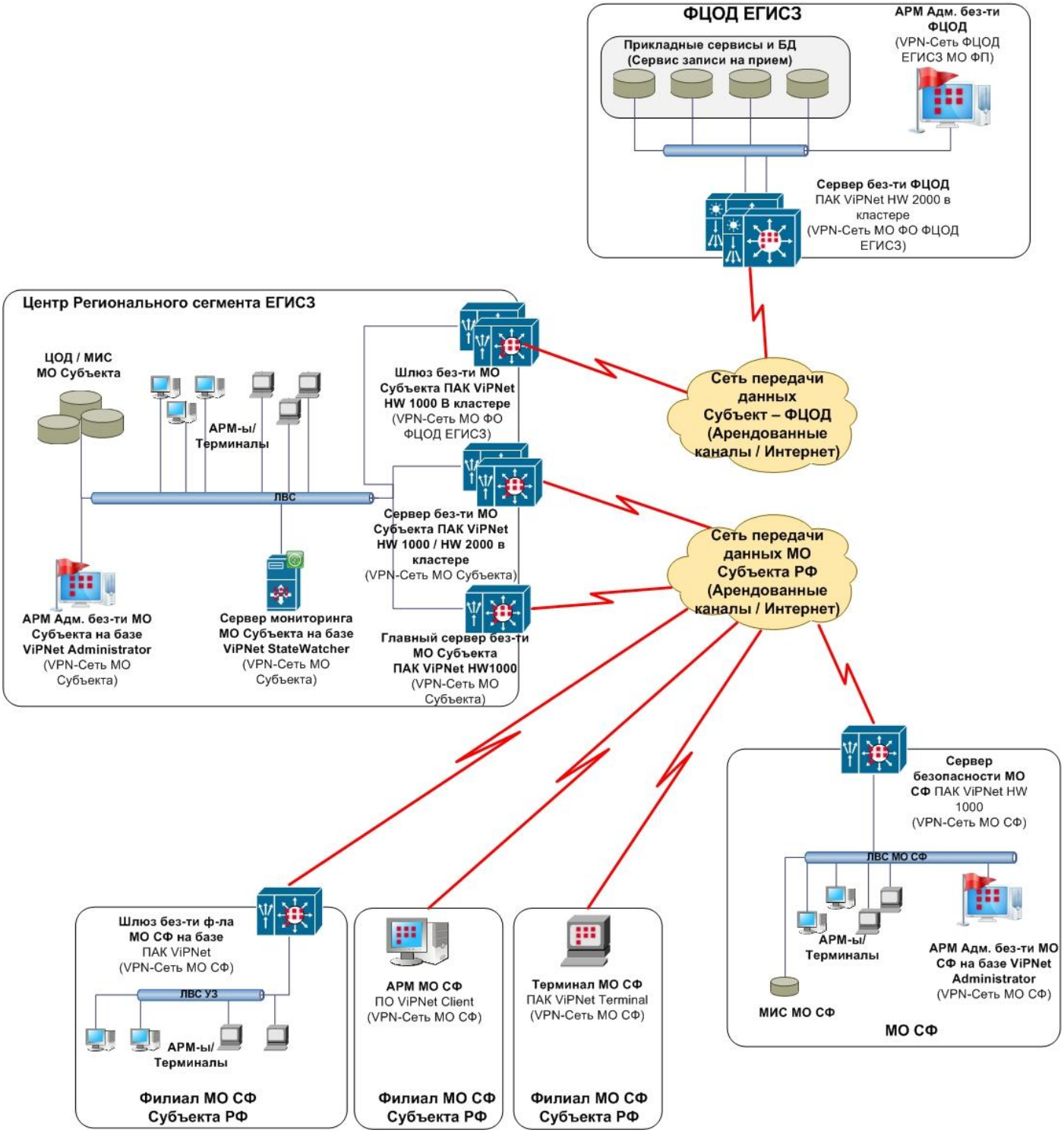
– не находится в пределах контролируемой зоны или контролируемую зону нельзя обеспечить, например в одном здании с МО СФ находятся сторонние организации, не имеющие никакого отношения к ЕГИСЗ, и у МО СФ и сторонней организации общая ЛВС.

В том случае если в МО СФ Субъекта РФ развертывается собственная VPN-сеть рекомендуется следующая схема подключения.

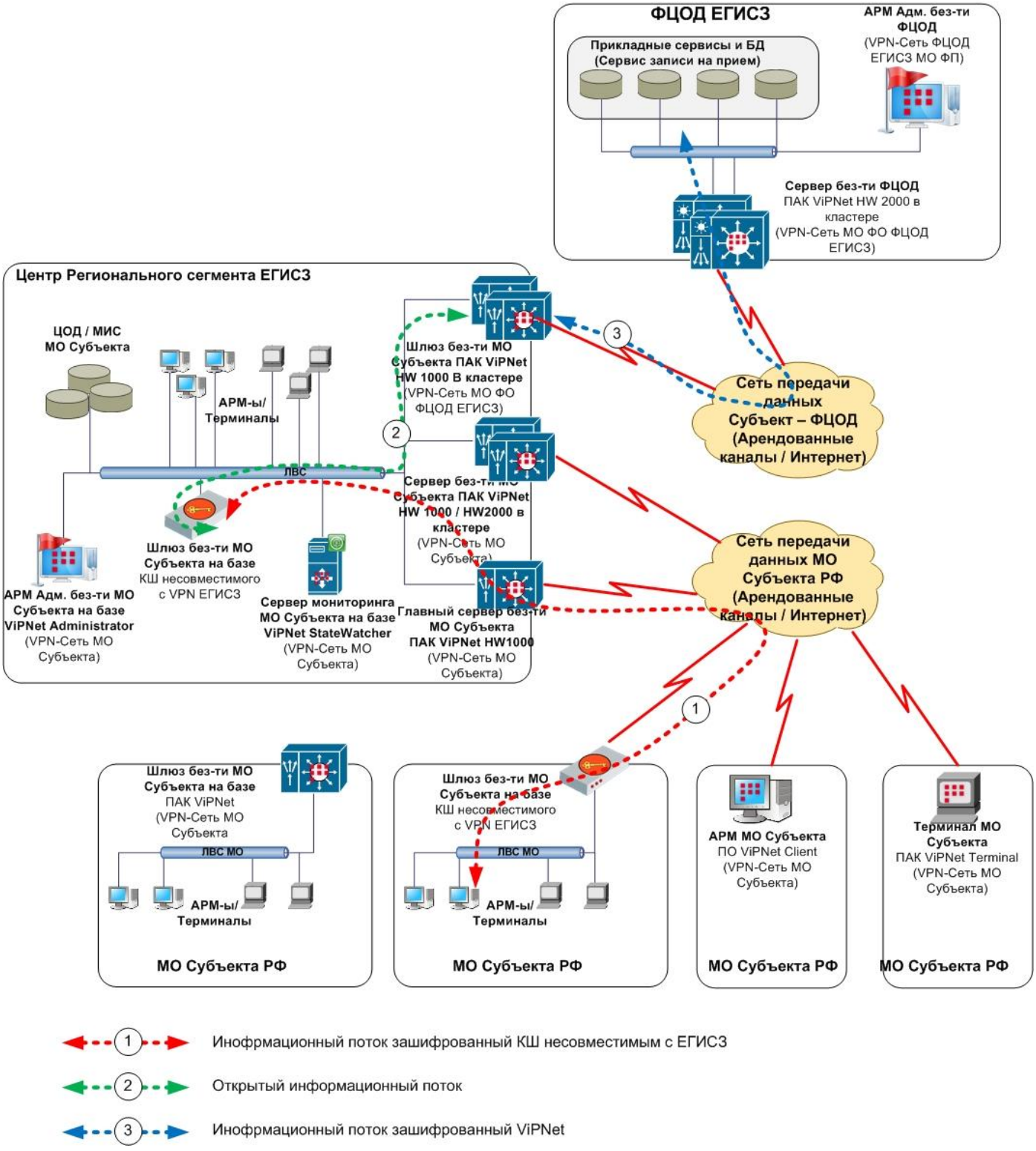
Тип ПАК ViPNet необходимо выбирать в соответствии с рекомендациями, приведенными в разделе 5.1.

Тип Клиентской компоненты ViPNet необходимо выбирать в соответствии с рекомендациями в разделе 5.2.

Рекомендации по организации сетевого подключения ПАК ViPNet HW приведены в разделе 6.


ФЦОД ЕГИСЗ
Прикладные сервисы и БД (Сервис записи на прием)
АРМ Адм. без-ти ФЦОД (VPN-Сеть ФЦОД ЕГИСЗ МО ФП)
Сервер без-ти ФЦОД ПАК ViPNet HW 2000 в кластере (VPN-Сеть МО ФО ФЦОД ЕГИСЗ)
Центр Регионального сегмента ЕГИСЗ
ЦОД / МИС МО Субъекта
АРМ-ы/ Терминалы
ЛВС
Шлюз без-ти МО Субъекта ПАК ViPNet HW 1000 В кластере (VPN-Сеть МО ФО ФЦОД ЕГИСЗ)
Сервер без-ти МО Субъекта ПАК ViPNet HW 1000 / HW 2000 в кластере (VPN-Сеть МО Субъекта)
Главный сервер без-ти МО Субъекта ПАК ViPNet HW1000 (VPN-Сеть МО Субъекта)
АРМ Адм. без-ти МО Субъекта на базе ViPNet Administrator (VPN-Сеть МО Субъекта)
Сервер мониторинга МО Субъекта на базе ViPNet StateWatcher (VPN-Сеть МО Субъекта)
Сеть передачи данных Субъект – ФЦОД (Арендованные каналы / Интернет)
Сеть передачи данных МО Субъекта РФ (Арендованные каналы / Интернет)
Сервер безопасности МО СФ ПАК ViPNet HW 1000 (VPN-Сеть МО СФ)
ЛВС МО СФ
АРМ-ы/ Терминалы
АРМ Адм. без-ти МО СФ на базе ViPNet Administrator (VPN-Сеть МО СФ)
МИС МО СФ
МО СФ
Шлюз без-ти ф-ла МО СФ на базе ПАК ViPNet (VPN-Сеть МО СФ)
ЛВС УЗ
АРМ-ы/ Терминалы
Филиал МО СФ Субъекта РФ
АРМ МО СФ ПО ViPNet Client (VPN-Сеть МО СФ)
Филиал МО СФ Субъекта РФ
Терминал МО СФ ПАК ViPNet Terminal (VPN-Сеть МО СФ)
Филиал МО СФ Субъекта РФ

4.5. Рекомендации по защите каналов при подключении медицинских учреждений, имеющих VPN-сеть построенной на технологии отличной от технологии ViPNet



5. РЕКОМЕНДАЦИИ ПО ВЫБОРУ ТИПА ОБОРУДОВАНИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ КАНАЛА ПЕРЕДАЧИ ДАННЫХ

5.1. Рекомендации по выбору ПАК ViPNet HW

В следующей таблице представлены рекомендации по выбору типа ПАК ViPNet в зависимости от количества используемых в подключаемом Медицинской организацией сетевых узлов (АРМ, серверов, терминалов) обрабатывающих подлежащую защите информацию.

Тип	Количество серверов, АРМ и терминалов в защищаемом сегменте	Рекомендуемое оборудование ПАК ViPNet Coordinator HW
1	более 500	HW2000
2	от 10 до 500	HW1000
3	от 6 до 10	HW100C
4	от 3 до 5	HW100B
5	2	HW100A

В следующей таблице представлены рекомендации по выбору типа ПАК ViPNet в зависимости от необходимо пропускной способности при подключении Медицинской организации к каналу передачи данных:

Тип	Количество серверов, АРМ и терминалов в защищаемом сегменте	Рекомендуемое оборудование ПАК ViPNet Coordinator HW
1	до 2,7 Гбит/с	HW2000
2	до 250 Мбит/с	HW1000
3	До 20 Мбит/с	HW100A/B/C

5.2. Рекомендации по выбору типа клиентской компоненты ViPNet

В следующей таблице представлены рекомендации по выбору клиентской компоненты ViPNet в зависимости от режима работы с информацией:

Тип	Режима работы с МИС	Рекомендуемое оборудование ПАК ViPNet Coordinator HW
1	«Тонкий» клиент (WEB-Браузер)	ViPNet Terminal
2	«Толстый» клиент для работы с МИС Необходимость подключения различного специализированного медицинского	ViPNet Client

	оборудования	

6. РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ СЕТЕВОГО ПОДКЛЮЧЕНИЯ

С учётом объединения в рамках VPN-сети большого количества медицинских организаций имеющих свою собственную IP –адресацию, рекомендуется:

– использовать виртуальную IP-адресацию для идентификации подключаемых МО на серверах безопасности ФЦОД ЕГИСЗ

– использовать виртуальную IP-адресацию для идентификации подключаемых МО на серверах безопасности регионального сегмента ЕГИСЗ.

Для подключения ПАК ViPNet на территории МО должны быть обеспечены:

– подключение к одному из каналов передачи данных:

- IP/MPLS-сеть ОАО «Ростелеком»;
- Сеть Интернет (любые провайдеры, доступные в регионе).

– подключение к сетевому оборудованию МО интерфейсов криптошлюза с использованием интерфейсов Ethernet Base T 100/1000;

– доступность внешнего интерфейса криптошлюза (IP внеш./маска) из сети Интернет одним из следующих способов:

- обеспечить NAT-трансляцию приватного IP-адреса в публичный IP-адрес (трафик по протоколу UDP, порт 55777);
- выделить для интерфейса публичный IP-адрес;

– маршрутизация в локальной сети МО должна осуществляться таким образом, чтобы трафик с адресов серверов ОУЗ, отправляемый на серверы КЦОД, направлялся на внутренний интерфейс криптошлюза;

– отсутствие логических препятствий для прохождения трафика по порту UDP 55777 между внешним интерфейсом криптошлюза (1-«IP внеш.») и адресом криптошлюза КЦОД.

Для организации настройки и подключения ПАК ViPNet МО может потребоваться выделение следующих IP-адресов:

№	IP адрес/маска	Назначение
1	IP внеш./маска	IP-адрес и маска сети внешнего интерфейса криптошлюза. Может быть как из приватного, так и из публичного адресного пространства.
2	IP gw внеш.	Адрес шлюза по умолчанию в сети, в которую включается внешний интерфейс криптошлюза. В случае подключения кластера должны быть выделены 3 адреса в одной подсети.
3	IP fw (NAT)	В случае использования приватного адреса на внешнем интерфейсе криптошлюза - публичный адрес NAT-трансляции, через который осуществляется доступ к внешнему интерфейсу криптошлюза. При подключении криптошлюза без использования NAT, указывать 3-«IP fw» совпадающим с адресом 1-«IP внеш./маска».
4	IP внут./маска	Адрес и маска сети внутреннего интерфейса криптошлюза. В случае подключения кластера должны быть выделены 3 адреса в одной подсети. IP внеш. и IP внут.

№	IP адрес/маска	Назначение
		обязательно должны принадлежать разным подсетям.
5	IP gw внут.	Адрес шлюза для маршрутизации внутрь ведомства для сети, в которую включается внутренний интерфейс криптошлюза. Если адреса 6-«IP тун» и 4-« IP внут» принадлежат одной подсети, то адрес 5-«IP gw внут» указывать совпадающим с адресом 4-« IP внут».
6	IP тун.	Адрес (а) сервера (ов) МО, которые будут взаимодействовать с серверами ФЦОД ЕГИСЗ.
7	IP вирт.	В случае пересечения адресов туннелируемых ресурсов со стороны МО с адресами туннелируемых ресурсов в ФЦОД ЕГИСЗ, в рабочем порядке для таких ресурсов назначается необходимое количество дополнительных виртуальные адресов.

Приложение 1.
Структура VPN-сети ФЦОД ЕГИСЗ

№	Название VPN-сегмента	Краткое описание назначения VPN-сегмента	
1	VPN-МО ФП	VPN-сегмент ЕГИСЗ, в который подключаются медицинские организации федерального подчинения	
2	VPN-МО ЦФО	VPN-сегмент ЕГИСЗ, в который подключаются медицинские организации регионального подчинения в Центральном федеральном округе	
3	VPN-МО ЮФО	VPN-сегмент ЕГИСЗ, в который подключаются медицинские организации регионального подчинения в Южном федеральном округе	
4	VPN-МО СЗФО	VPN-сегмент ЕГИСЗ, в который подключаются медицинские организации регионального подчинения в Северо-Западном федеральном округе	
5	VPN-МО ДФО	VPN-сегмент ЕГИСЗ, в который подключаются медицинские организации регионального подчинения в Дальневосточном федеральном округе	
6	VPN-МО СФО	VPN-сегмент ЕГИСЗ, в который подключаются медицинские организации регионального подчинения в Сибирском федеральном округе	
7	VPN-МО УФО	VPN-сегмент ЕГИСЗ, в который подключаются медицинские организации регионального подчинения в Уральском федеральном округе	
8	VPN-МО ПФО	VPN-сегмент ЕГИСЗ, в который подключаются медицинские организации регионального подчинения в Приволжском федеральном округе	
9	VPN-МО СКФО	VPN-сегмент ЕГИСЗ, в который подключаются медицинские организации регионального подчинения в Северо-Кавказском федеральном округе	