Методические рекомендации медицинским организациям по обеспечению 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 обеспечения защищенного информационного обмена медицинских организаций (МО) 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 защиты каналов связи при информационном обмене в составе МИС на федеральном уровне используется средства криптографической защиты информации на базе технологии ViPNet и дальнейшие варианты по организации типовых подключений основываются на использовании данного типа средств защиты информации.

Используемые в настоящем документе сокращения приведены в Таблице 1.

Таблица 1.

Обозначение	Описание
АТК	Аппаратный тонкий клиент
АРМ	Автоматизированное рабочее место
ЕГИСЗ	Единая государственная информационная система в сфере здравоохранения
ЗСПД	Защищенная среда передачи данных
ЛВС	Локально-вычислительная сеть
ЛПУ	Лечебно-профилактическое учреждение
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
МО С	Медицинские организации субъектов Российской Федерации
МО ФП	Медицинские организации Федерального подчинения
МИАЦ	Медицинский информационной аналитический центр
МЭ	Межсетевой экран
Оператор	Телекоммуникационная компания, предоставляющая услуги защищенной среды передачи данных (ЗСПД)
ПАК	Программно аппаратный комплекс
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты данных
УД	Узел доступа
УЗ	Учреждение здравоохранения
ФО	Федеральный округ
ФЦОД	Федеральный центр обработки данных
ЦОД	Центр обработки данных
VPN	Virtual Private Network (виртуальная частная сеть)

2. Архитектура системы криптографической защиты ЗСПД ЕГИСЗ

Архитектура системы криптографической защиты должна учитывать объекты взаимодействия ЕГИСЗ:

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

Кроме того, при подключении медицинской организации к ФЦОД 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 к ФЦОД ЕГИСЗ, должны быть совестимы с 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 обеспечения защищенного взаимодействия с медицинскими организациями федерального подчинения в ФЦОД ЕГИСЗ организовывается VPN-сегмент на базе технологии ViPNet. Данный VPN-сегмент будет обслуживать подключение МО федерального подчинения.

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

Для организации подключения к ФЦОД ЕГИСЗ в МО ФП в точке подключения к среде передачи данных должен быть установлен шлюз безопасности на базе программно-аппаратного комплекса (ПАК) 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.

На этапе ввода в эксплуатацию шлюза безопасности МО ФП и его дальнейшего обслуживания потребуется привлечение администраторов безопасности VPN-сети ФЦОД ЕГИСЗ, либо организации обслуживающей данную VPN-сеть.

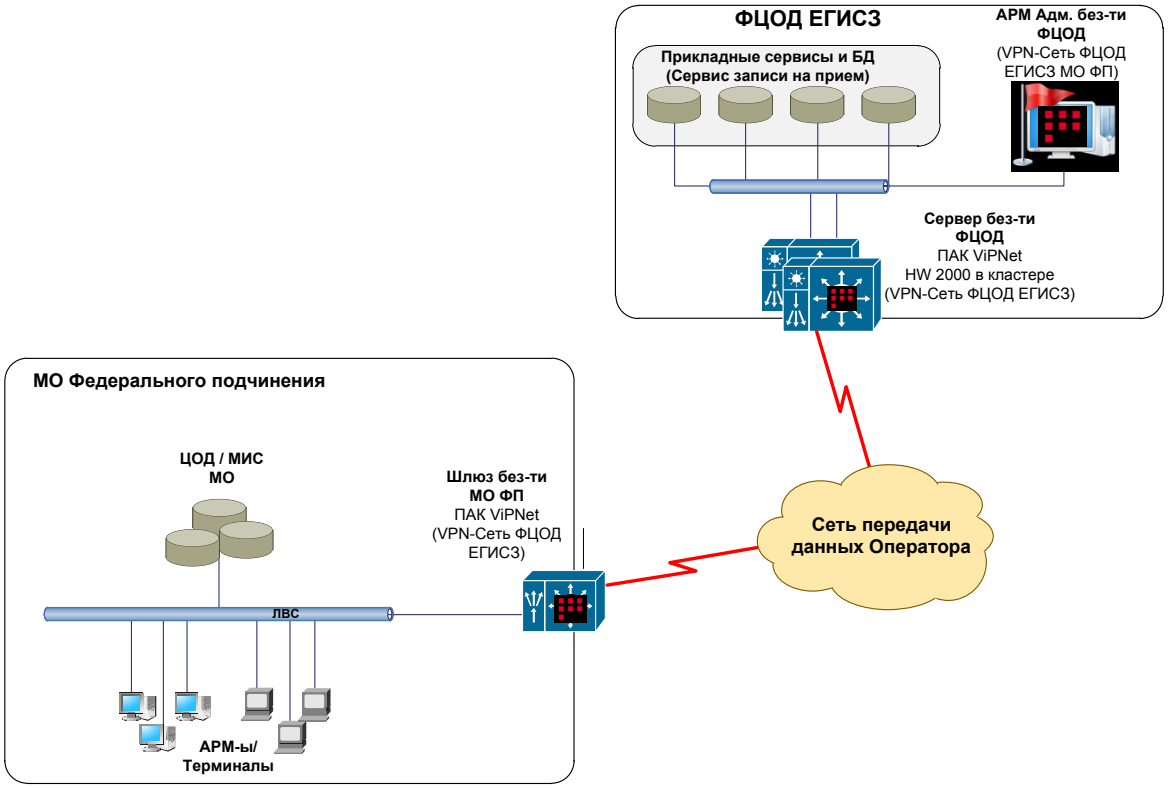

Рис.1. Типовая схема защищенного подключения МО ФП к ФЦОД ЕГИСЗ

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 ФЦОД 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, которые проходят 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 схема подключения представленная на рисунке 2.

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.

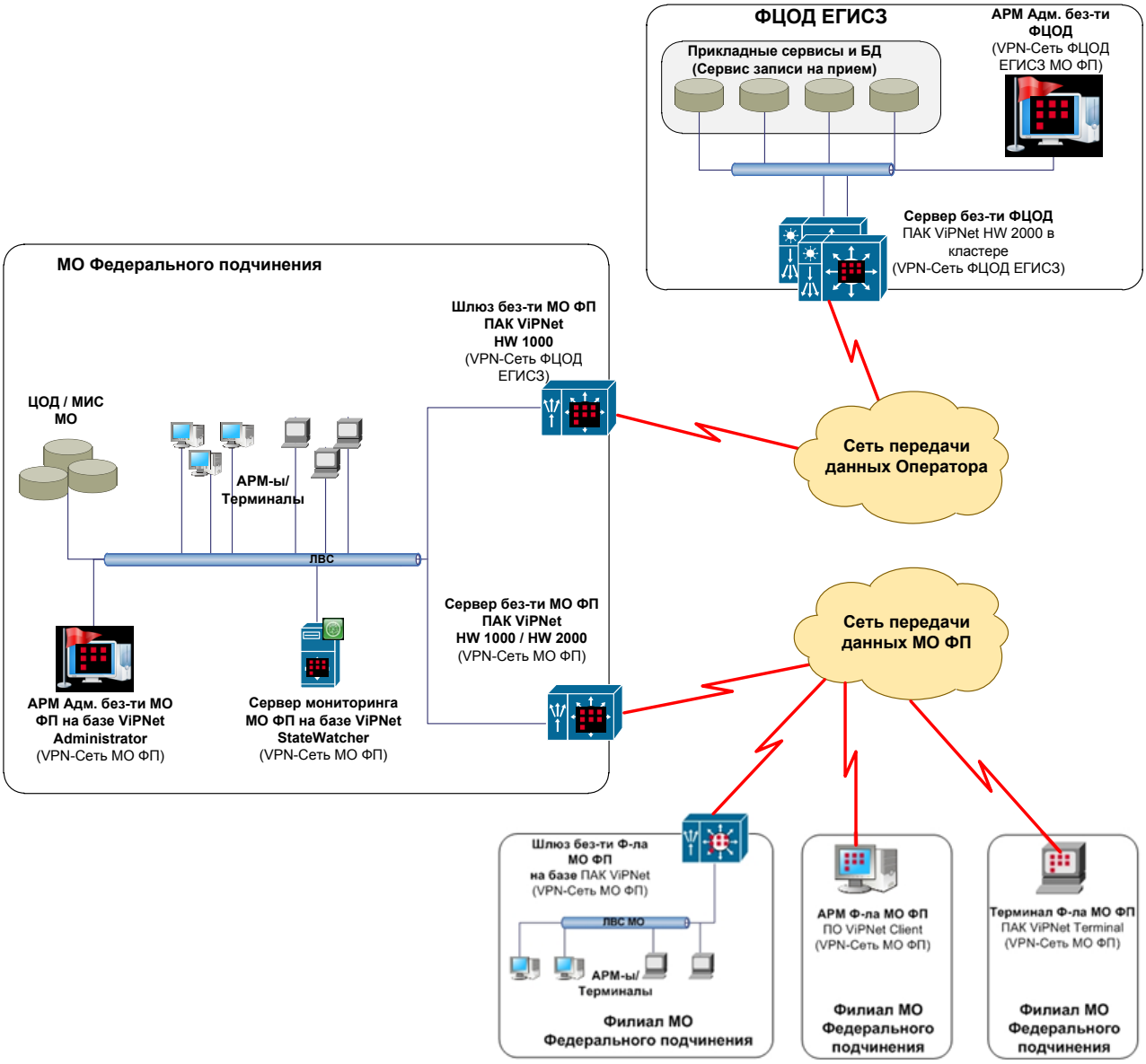

Рис.2. Типовая схема защищенного подключения к ФЦОД ЕГИСЗ медицинских организаций Федерального подчинения имеющих территориально распределенную филиальную структуру

4. Рекомендации по защите каналов медицинским организациям субъекта РФ

4.1 Рекомендации по архитектуре регионального сегмента системы криптографической защиты ЕГИСЗ

Для организации взаимодействия медицинских организаций субъекта РФ с ФЦОД 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 структура VPN-сети МО Субъекта РФ, которая представлена на рисунке 3.

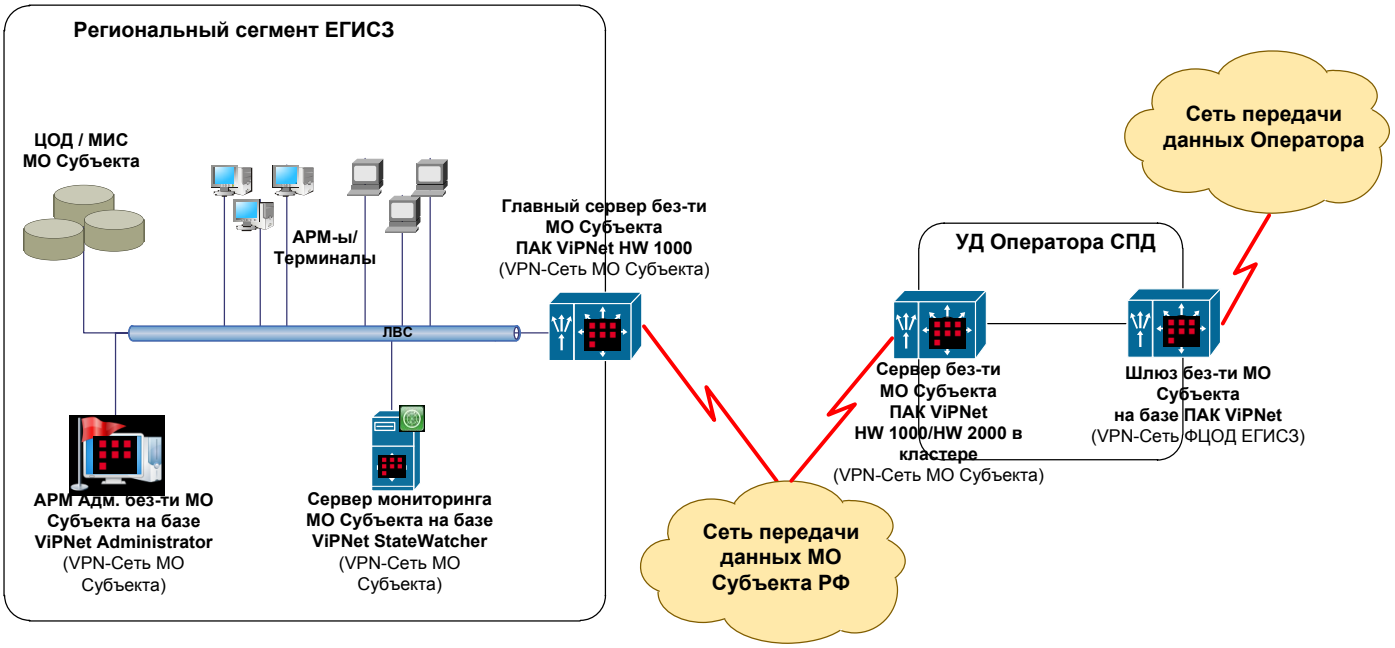

Рис.3. Структура регионального сегмента VPN-сети МО Субъекта РФ

Рекомендуется включение в состав VPN-сети МО Субъекта РФ двух серверов безопасности приведенных в таблице 3.

Таблица 3

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, для взаимодействия с другими VPN-сетями регионального уровня (собственные сети ЛПУ, ТФОМС).	ПАК Coordinator HW1000
Сервер безопасности МО Субъекта (VPN-Сеть МО Субъекта)	Криптографическая обработка информационных потоков от МО Субъекта РФ адресованного в ФЦОД ЕГИСЗ.	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 VPN-сети МО Субъекта РФ к ФЦОД ЕГИСЗ

Для организации подключения VPN-сети МО Субъекта РФ к ФЦОД ЕГИСЗ в УД оператора ЗСПД должен быть установлен Сервер безопасности из состава VPN-сети МО Субъекта РФ.

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

На этапе подключения регионального сегмента VPN-сети МО Субъекта РФ к ЗСПД федерального сегмента и его дальнейшего обслуживания потребуется привлечение администраторов безопасности организации обслуживающей данную VPN-сеть.

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

Межсетевое взаимодействие между VPN-сетями ФЦОД ЕГИСЗ и МО Субъекта РФ организуется в пределах контролируемой зоны УД Оператора. В пределах контролируемой зоны УД между VPN-сетями осуществляется обмен данными без шифрования.

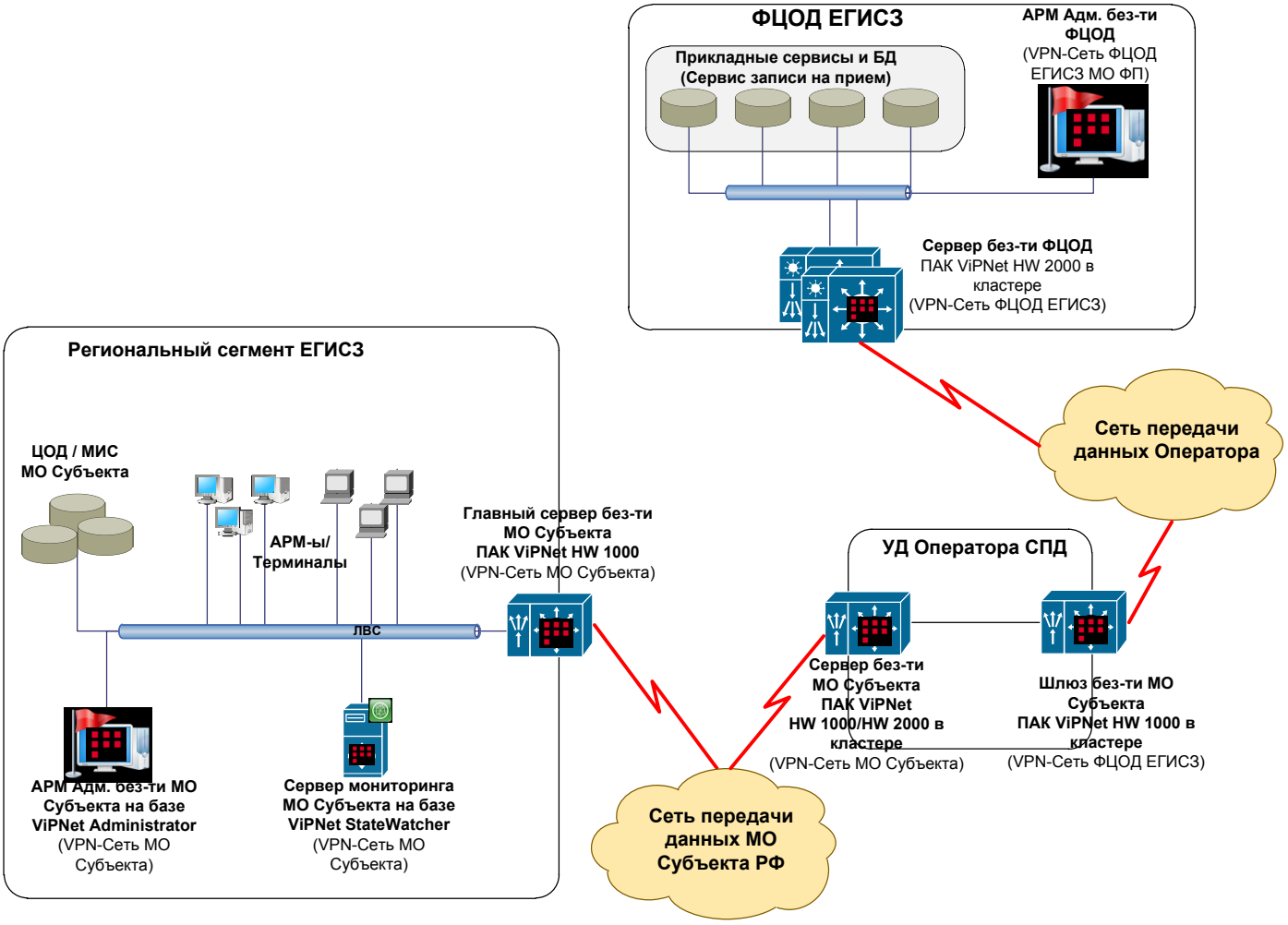

Рис.4. Типовая схема защищенного подключения Центрального Регионального сегмента VPN-сети МО Субъекта РФ к ФЦОД ЕГИСЗ

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

Для организации подключения МО Субъекта РФ к ФЦОД 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.

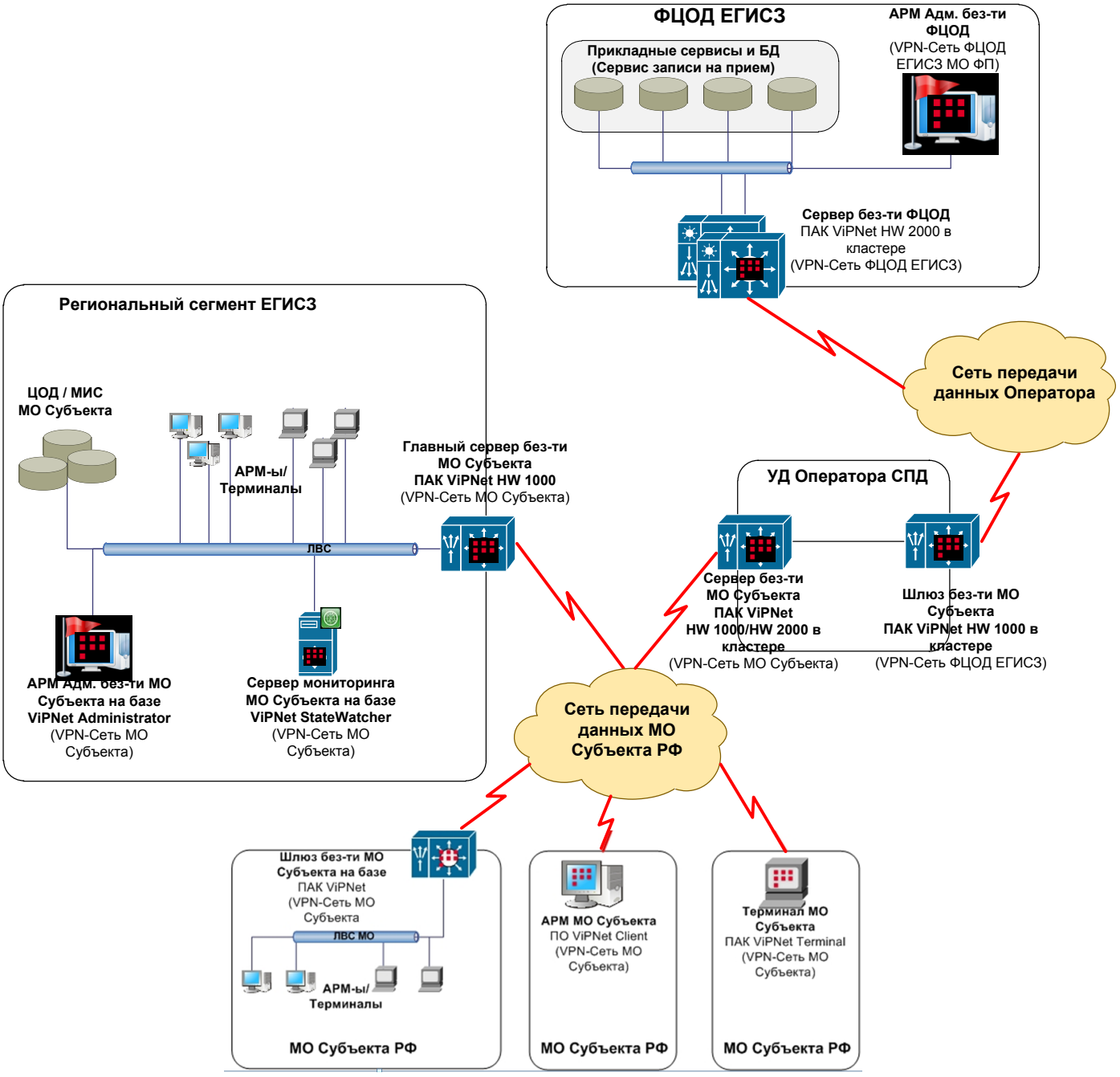

Рис.5. Типовая схема защищенного подключения МО Субъекта РФ к ФЦОД ЕГИСЗ

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 ФЦОД 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 ФЦОД 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.

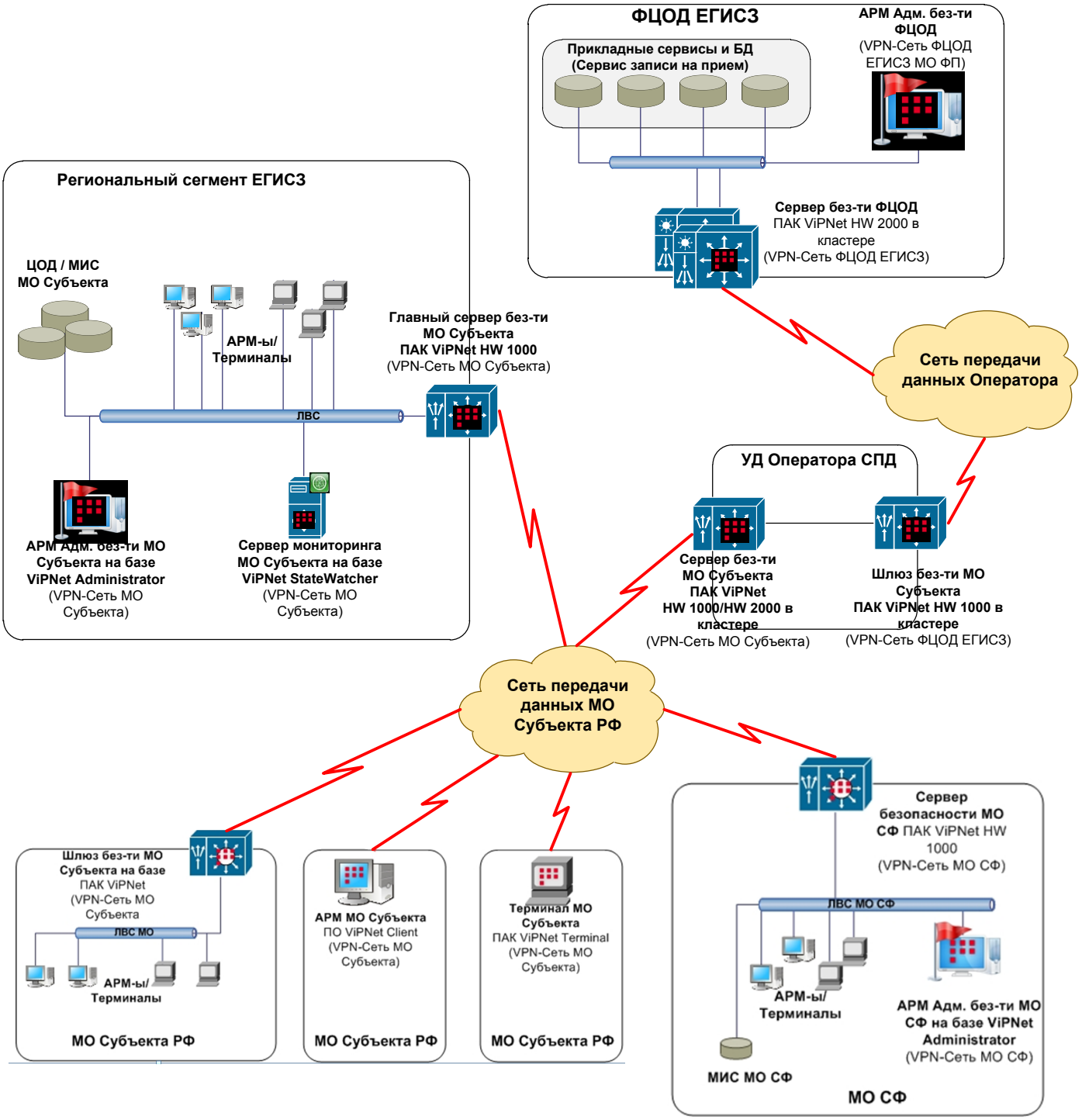

Рис.6. Типовая схема подключения МО Субъекта РФ имеющего филиальную структуру к ФЦОД ЕГИСЗ

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

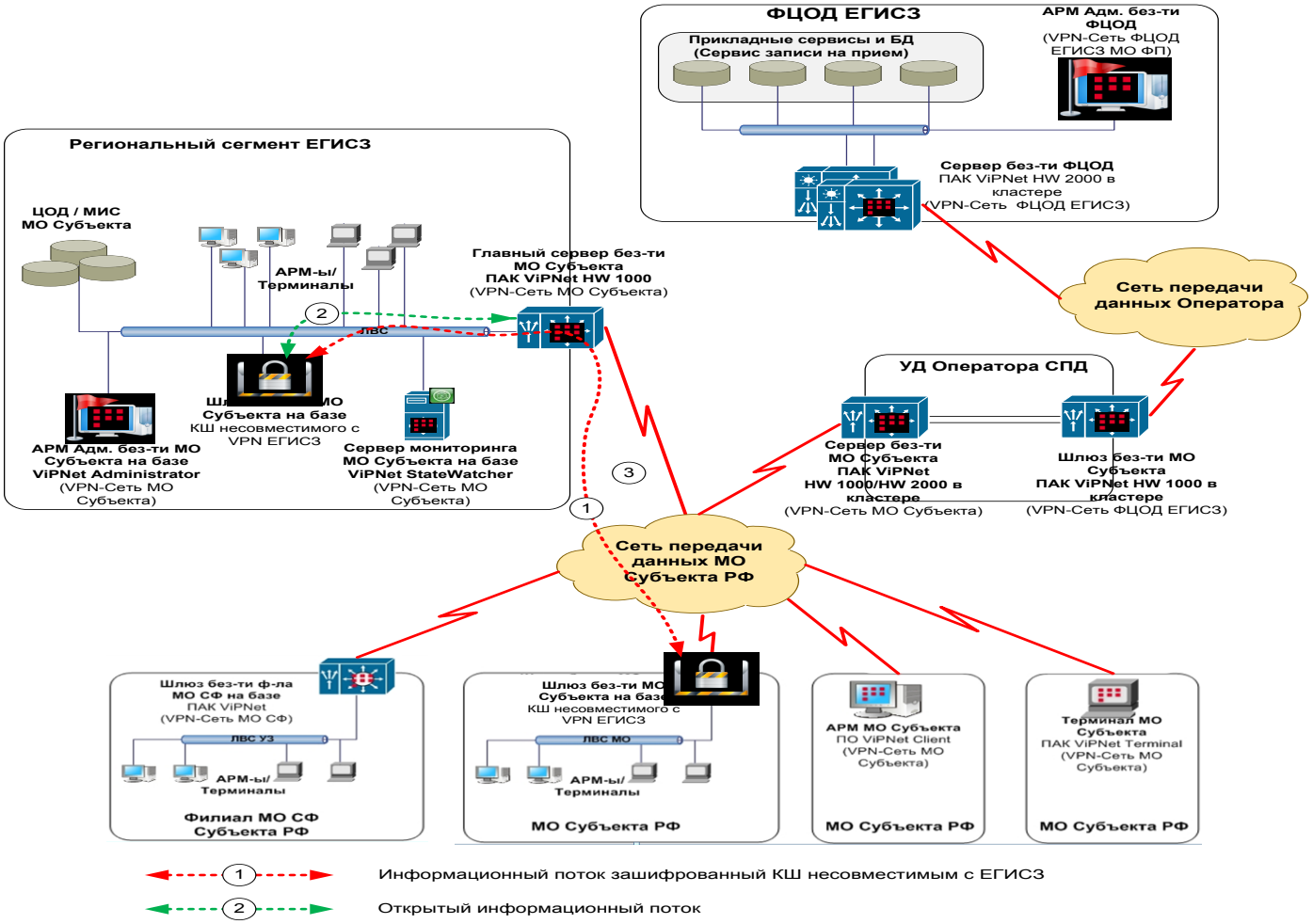

Рис.7. Типовая схема защищенного подключения МО Субъекта РФ к ФЦОД ЕГИСЗ

Если в VPN-сети МО Субъекта используются иные устройства СКЗИ (отличные и несовместимые с технологией VipNet), допускается установка на УД Оператора устройства СКЗИ, совместимого с технологиями, используемыми в региональной ЗСПД МО Субъекта.

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.

Таблица 4.

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 необходимой пропускной способности при подключении Медицинской организации к каналу передачи данных:

Таблица 5.

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:

Таблица 6.

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 оборудования	ViPNet Client

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 Оператора (любой региональной СПД);
  - 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 УД одним из следующих способов:
  - обеспечить NAT-трансляцию приватного IP-адреса (приватной диапазона IP адресов) в IP-адрес (трафик по протоколу UDP, порт 55777), предоставляемый Оператором;
  - маршрутизация в VPN-сети МО Субъекта должна осуществляться таким образом, чтобы трафик с адресов хостов в VPN-сети МО Субъекта, отправляемый в ФЦОД ЕГИСЗ, направлялся на внутренний интерфейс СКЗИ VPN-сети ФЦОД ЕГИСЗ.

Для организации настройки и подключения ПАК ViPNet МО может потребоваться выделение IP-адресов приведенных в таблице 7.

Таблица 7.

№	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. 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.