Условия подключения и дальнейшей работы участников защищенной сети в Единой защищенной сети передачи данных государственных органов Удмуртской Республики

1 Подключение участников защищенной сети (далее – участники) к Единой защищенной сети передачи данных государственных органов Удмуртской Республики (далее - защищенная сеть) осуществляется при помощи оборудования, соответствующего:

- требованиям ФСБ России к средствам криптографической защиты информации (СКЗИ) класса КС3 (на применяемое криптоядро и программно-аппаратный комплекс);
- требованиям ФСБ России к устройствам типа межсетевые экраны по 4 классу защищенности и иметь разрешение для использования для защиты информации от несанкционированного доступа в информационно-телекоммуникационных системах органов государственной власти Российской Федерации;
- требованиям ФСТЭК России к межсетевым экранам не ниже 3 класса, по контролю отсутствия недекларированных возможностей не ниже 4 уровня, иметь разрешение для использования в автоматизированных системах не ниже класса 1Г и при создании информационных систем персональных данных до 1 класса включительно.

2 Указанным требованиям удовлетворяют следующие программно-аппаратные комплексы (криптошлюзы):

Производитель	Артикул	Модель
ОАО «Инфотекс», г. Москва	SC-119/1	ViPNet Coordinator HW1000
ОАО «Инфотекс», г. Москва	SC-118/A	ViPNet Coordinator HW100A
ОАО «Инфотекс», г. Москва	SC-118/B	ViPNet Coordinator HW100B
ОАО «Инфотекс», г. Москва	SC-118/C	ViPNet Coordinator HW100C

3 Участник осуществляет выбор модели криптошлюза (при самостоятельном приобретении) исходя из требуемых характеристик по пропускной способности, количеству взаимодействующих ресурсов и возможности кластеризации (горячего резервирования):

Модель	Пропускная способность	Количество туннелируемых ресурсов	Возможность кластеризации
HW1000	250 Мбит/с	Не ограничено	Есть
HW100A	20 Мбит/с	2	Нет
HW100B	20 Мбит/с	5	Нет
HW100C	20 Мбит/с	10	Нет

4 Для обеспечения совместимости с существующими средствами криптозащиты передаваемой информации, установленными в региональных сегментах инфраструктуры электронного правительства применение эквивалентного оборудования не допускается.

5 Для подключения криптошлюза на территории участника должны быть обеспечены:

5.1 Подключение к одному из провайдеров сети «Интернет». Рекомендуется иметь резервный канал доступа в сеть общего пользования «Интернет».

5.2 Физическое размещение оборудования на площадке участника, находящейся в пределах контролируемых зон:

- Для каждого экземпляра ViPNet Coordinator HW1000 - 1 (одно) место размером 19 дюймов Rack 1U (для установки в стойку глубиной от 480 мм и более) 432x43x355 мм (ШхВхГ);
- Для каждого экземпляра ViPNet Coordinator HW100A/ HW100B/ HW100C - 1 (одно) место размером 187x130x52 мм (ШхВхГ) на горизонтальной поверхности.

5.3 Климатические условия:

- Температура окружающего воздуха от 0 до +40 °С;
- Относительная влажность от 5 до 95 %.

5.4 Подключение криптошлюзов максимальной потребляемой мощностью 200 Вт на устройство к сети гарантированного и бесперебойного электропитания напряжением 220 В с помощью кабеля типа С13 – CEE7/7 (евровилка).

5.5 Подключение к сетевому оборудованию участника интерфейсов криптошлюза с использованием интерфейсов Ethernet Base T 100/1000. Требуется 2 патч-корда, которые позволят обеспечить подключение сетевых интерфейсов криптошлюза в локальную сеть участника и к оборудованию, обеспечивающее доступ в сеть общего пользования «Интернет».

5.6 Доступность внешнего интерфейса криптошлюза из сети Интернет одним из следующих способов:

- Выделить для интерфейса публичный статический IP-адрес.
- Обеспечить NAT-трансляцию приватного IP-адреса в публичный IP-адрес (трафик по протоколу UDP, порт 55777) (по предварительному согласованию с Оператором).

5.7 Отсутствие логических препятствий для прохождения трафика по порту UDP 55777 между внешним интерфейсом криптошлюза и адресами криптошлюзов других участников.

5.8 Маршрутизация в локальной сети участника должна осуществляться таким образом, чтобы трафик с адресов серверов участников, отправляемый в защищенную сеть, направлялся на внутренний интерфейс криптошлюза.

5.9 Определены информационные ресурсы локальной сети участника, трафик которых в защищенную сеть должен туннелироваться через криптошлюзы. Последующая перенастройка криптографических туннелей через криптошлюзы осуществляется Администратором защищенной сети по заявкам участника по форме, установленной Администратором защищенной сети.

6 Назначается администратор безопасности, обеспечивающий работу установленного оборудования защищенной сети. Контактная информация администратора безопасности для экстренной связи представляется Администратору защищенной сети в течение 14 дней с момента подписания Соглашения о подключении к Единой защищенной сети передачи данных государственных органов Удмуртской Республики и своевременно актуализируется при ее изменении.

7 Участник обязан в соответствии с Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13 июня 2001 года № 152, организовать:

- размещение, специальное оборудование, охрану и режим в помещениях, в которых размещены СКЗИ и хранятся ключи;
- режим учета СКЗИ, дистрибутивов, эксплуатационно-технической документации, ключевых документов (журналы учета используемых СКЗИ и ключей).