Инструкция по подключению к закрытой части АСУ ИОГВ через защищенный канал ЕСПД.

В соответствии с приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» доступ к закрытой части АСУ ИОГВ должен осуществляться с рабочей станций, для которой выполнены мероприятий по технической защите информации и проведена ее аттестация.

1. На рабочем месте необходимо запустить программу работы с командной строкой **cmd** (Пуск-Все программы-Стандартные -Командная строка).
2. Прописать маршрут:
   route add –p 10.0.11.165 mask 255.255.255.255 XX.XX.XX.XX
   , где XX.XX.XX.XX - адрес вашего криптошлюза VipNet.
3. Для рабочей станции, на которой установлен VipNet-клиент, прописывать маршрут не требуется.
4. После добавления маршрута запустить команду **ping 10.0.11.165**
5. Если **ping** успешен, то вход а АСУ ИОГВ (закрытая часть) возможен по адресу https://asuiogv2.egov66.ru
   Так же необходимо добавить данный адрес в исключения браузера - не использовать прокси для локальных адресов (адрес должен считаться локальным).
6. Если **ping** не проходит (превышен интервал запроса), либо страница входа в систему АСУ ИОГВ не отображается, необходимо в консоли командной строки выполнить команду **tracert 10.0.11.165**
   и проверить, присутствует ли в выводе результатов адрес Вашего криптошлюза.
7. Если трассировка не доходит на ваш криптошлюз, то Вам необходимо обеспечить соответствующее подключение в Вашей ЛВС.
8. Если же трассировка проходит криптошлюз а дальше не идет, то необходимо направить Заявку в техподдержку ГБУ «Оператор электронного правительства» на адрес электронной почты **sd@egov66.ru** . К заявке приложить скриншот команды **tracert 10.0.11.165 ,** указать **ID узла** VipNet-клиента.