ТЕКОН-АВТОМАТИКА
системы управления, диспетчеризации и учёта

ООО НПО "Текон-Автоматика"
Тел.: (495) 642-71-90, 971-41-21
Тел.: (499) 720-82-27 Факс: (499) 720-83-98
E-mail: tekon@tekon.ru Web: www.tekon.ru

РАСПРЕДЕЛЕННАЯ ДИСПЕТЧЕРИЗАЦИЯ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ (СОТОВЫХ) СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Значительное развитие и распространение компьютерных сетей в последние годы делает их весьма привлекательными для использования в сфере решения задач диспетчеризации.

Для возможности использования сетевой инфраструктуры в качестве среды передачи диспетчерской информации в системе АСУД-248, были разработаны контроллеры инженерного оборудования (КИО), IP-концентраторы, модернизировано программное обеспечение.

Наиболее простой случай развертывания АСУД-248 с использованием компьютерных сетей – это, когда все компоненты системы подключаются к сети одного Интернет-провайдера. Т.е. другими словами в районе существует одна компания (провайдер), предоставляющая услуги доступа к сети Интернет, и оборудования АСУД-248 использует для передачи данных выделенные провайдером ресурсы сети. Данный вариант можно условно назвать «локальной диспетчеризацией». При этом провайдер выделяет необходимый набор IP-адресов, которые следует настроить на ПК-диспетчера, КИО и IP-концентраторах. Трудностей, как правило, в данном случае не возникает.

Однако на практике, особенно при решении задач диспетчеризации разрозненных удаленных объектов, компоненты системы обычно подключаются к сетям разных Интернет-провайдеров. Кроме того на некоторых объектах может оказаться, что единственный вариант подключения - это использование мобильного интернета (сотовых сетей передачи данных). Данный вариант можно условно назвать «распределенной диспетчеризацией». Настройка несколько сложнее, имеет свои тонкости, которые, по возможности максимально подробно будут рассмотрены ниже.

На рисунке 1, представлен вариант, распределенной диспетчерской системы, в которой оборудование установлено в сетях 3-х разных Интернет-провайдеров.

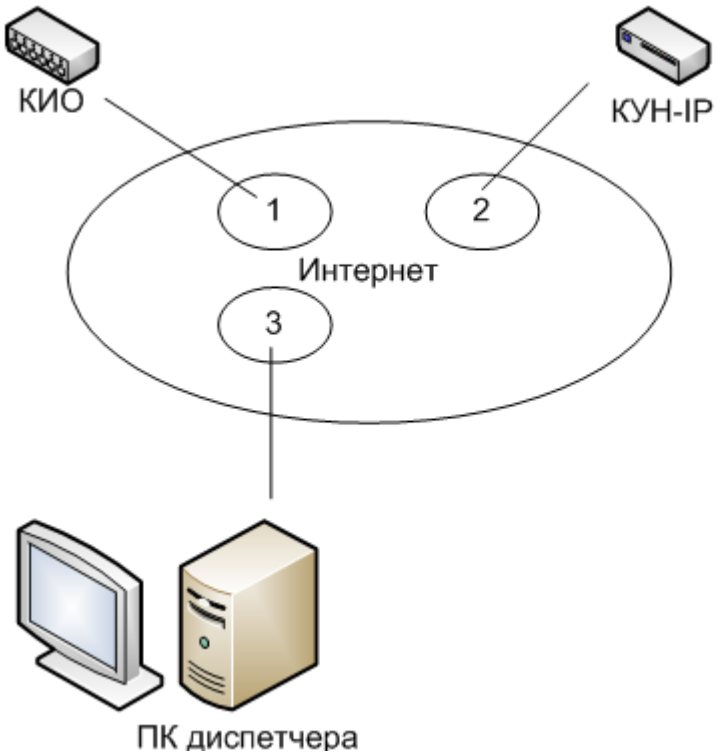

Рисунок 1 – Пример распределенной диспетчерской системы.

В данном случае необходимо у каждого провайдера получить необходимый набор статических публичных (реальных) IP-адресов. Публичный IP-адрес – это IP-адрес, который позволяет получить доступ к устройству с любого другого, подключенного к сети Интернет. Термин «статический» указывает на то, что IP-адрес закреплен за устройством и не меняется при переподключении устройства к сети.

В отличии от публичного IP-адреса, частный IP-адрес позволяет обмениваться данными устройствам только в пределах локальной сети, где они установлены. Обычно провайдер выделяет устройствам при подключении к своей сети именно частные IP-адреса – этого вполне достаточно для обычных задач (например, доступа персонального компьютера) к сети Интернет. Однако для решения задач диспетчеризации выдвигается ряд дополнительных требований, которые требует наличия у устройства именно публичного IP-адреса.

Подытожив вышесказанное, еще раз отметим, что в примере, представленном на рисунке 1, необходимо получить по одному публичному IP-адресу у каждого из провайдеров.

На рисунке 2, представлен вариант, распределенной диспетчерской системы, в которой отдельное оборудование подключается с помощью сетей сотовой связи.

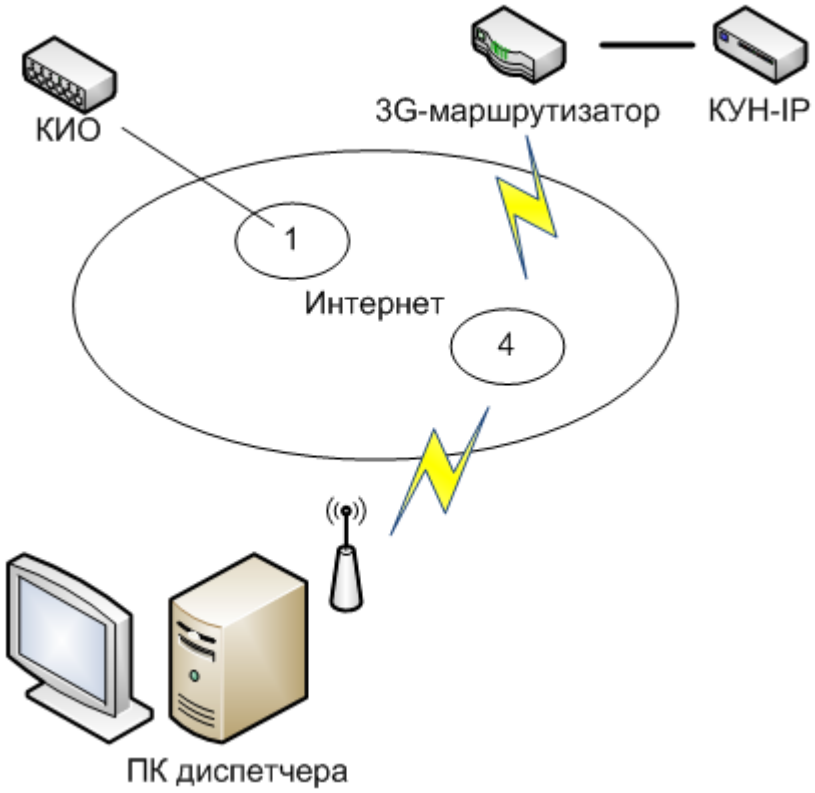

Рисунок 2 –Распределенной диспетчерской системы с использованием сотовых сетей.

КИО подключен к провайдеру 1, который предоставляет стандартное проводное подключение. А в месте установки КУН-IP, ПК-диспетчера выполнить подключение к какому-либо провайдеру невозможно (например, провайдеры отсутствуют).

Встает вопрос: возможно ли применить подключение по сотовой сети (провайдер 4)?

Для ответа на него следует учитывать, что канал передачи данных должен обеспечивать полосу порядка 130 кБит/с, поэтому следует ориентироваться на сотовые сети стандарта 3G или 4G. Если уровень сигнала сети в месте установки оборудования приемлим (исходя из проведенных тестов проверки связи с помощью, например, коммуникаторов),то ответить на вопрос можно положительно.

Операторы сотовой связи широко предлагают доступ к сети Интернет на основе USB-модемов. Однако USB-модем может быть подключен только к ПК диспетчера, Пульту-ПК или КИО-8(4). В случае необходимости подключения КУН-IP или КИО-2М (у которых отсутствует USB-порт) необходимо промежуточное оборудование: 3G(4G) маршрутизатор (или роутер, например, Zyxel Keenetic или DLink), к которому по интерфейсу RJ-45 кроссоверным кабель подключается КУН-IP (КИО-2М).

В данном случае необходимо также (как и в варианте 1) у каждого провайдера получить необходимый набор статических публичных IP-адресов.

У операторов сотовой связи выделение публичного IP-адреса – это дополнительно оплачиваемая услуга. При этом обязательно следует уточнить, что IP-адрес статический (не изменяется при переподключении к сотовой сети). Если получить статический адрес не возможно, см. далее организация VPN-сети.

Особым образом должны быть настроены 3G-роутеры. Публичный IP-адрес будет присвоен роутеру при его регистрации в сотовой сети.

На КУН-IP (КИО-2М), подключаемых к 3G-роутеру, в настройках сети указывается:

IP	192.168.1.100
Маска	255.255.255.0
Шлюз	192.168.1.1 (это IP-адрес LAN интерфейса 3G-роутера)

IP адрес ПК-диспетчера – публичный IP-адрес ПК-диспетчера (настройка только для КИО-2М).

Далее на 3G-роутере в разделе «Домашняя сеть / Серверы / Открыть домашний сервер» (на других роутерах данная настройка может называться «Сервер DMZ», «DMZ») указать IP-адрес КУН-IP(КИО-2М), т.е. 192.168.1.100.

После этого все запросы, которые идут на публичный IP-адрес 3G-роутера, будут ретранслироваться на подключенный к нему КУН-IP (КИО-2М).

Крайне рекомендуется на 3G-роутере настроить в разделе Фильтры фильтрацию входящих WAN-соединений, указав, что разрешены подключения только с IP-адреса ПК диспетчера.

На ПК диспетчера в программном обеспечении регистрируется КУН-IP (КИО-2М), указывая реальный IP-адреса 3G-роутера.

Существенное ограничение в данном случае – это возможность подключение только одного КУН-IP (КИО-2М) к 3G-роутеру. Если необходимо подключить несколько устройств, см. далее организация VPN-сети.

Поскольку оборудование диспетчеризации и в 1 и во 2 случаях работает по открытым каналам передачи данных следует уделить особое внимание обеспечению информационной безопасности: ограничению доступа к компонентом системы (установка и настройка файрвола, изменение паролей по умолчанию), защиты от компьютерных вирусов (установка антивирусного программного обеспечения).

В некоторых случаях невозможно организовать подключения по указанным схемам 1 или 2, ввиду отсутствия возможности получить необходимый набор статических публичных IP-адресов или другим причинам. Тогда следует рассмотреть возможность настройки VPN-сети (виртуальной частной сети). Для ее работы потребуется только один статический публичный IP-адрес на стороне ПК-диспетчера. Кроме того развертывание данной сети обеспечит хороший уровень информационной безопасность системы в целом. Поскольку, несмотря на физическую распределенность отдельных устройств, после настройки VPN, все компоненты оказываются логически в рамках одной локальной изолированной VPN-сети.

Для настройки VPN-сети потребуется дополнительное устройство: аппаратный VPN-шлюз (например, DLink) установленный со стороны ПК-диспетчера, как показано на рисунке 3.

Обязательное требование к шлюзу – поддержка входящих PPTP.

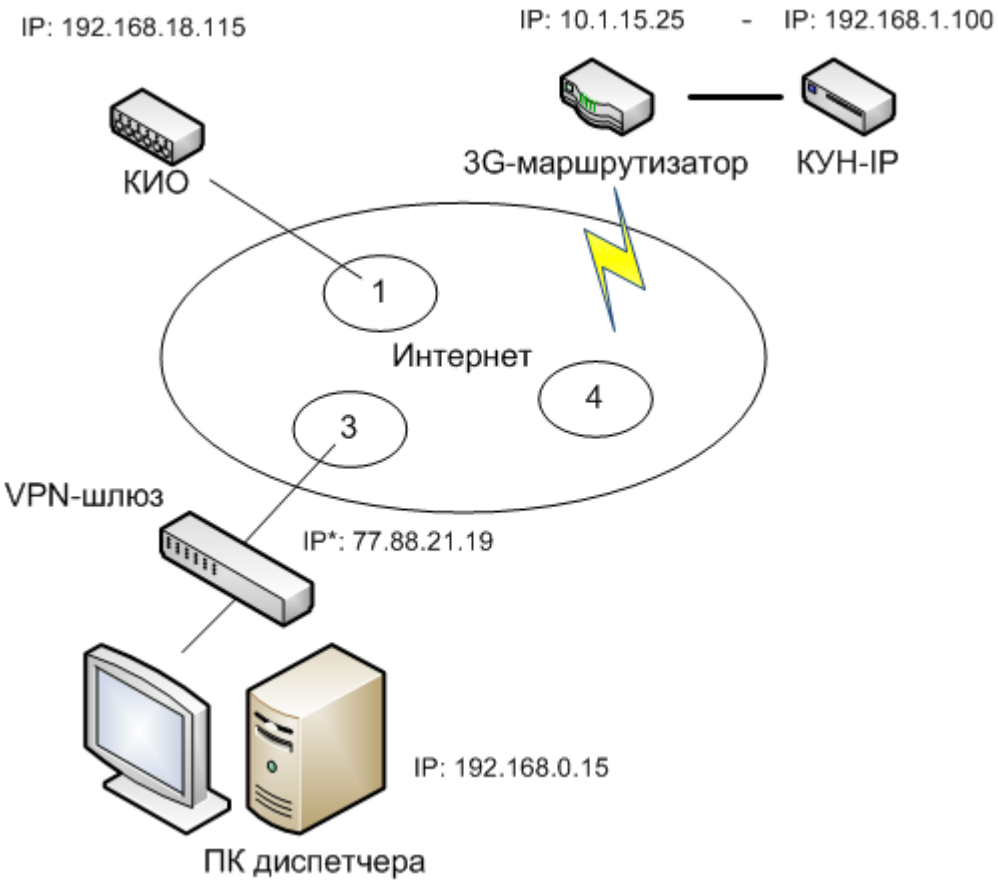

Рисунок 3 – Развертывание VPN-сети.

Рассмотрим приведенную типовую конфигурацию. На КИО настроен частный IP-адрес сети провайдера 1, на 3G-роутере частный IP-адрес сети провайдера 4, на КУН-IP частный IP-адрес, на ПК-диспетчера частный IP-адрес. Единственное устройство, которому необходим статический публичный IP – это VPN-шлюз. (все устройства могут получить доступ к шлюзу, но между собой никто не виден).

VPN-шлюз настраивается специальным образом для приема входящих PPTP подключений согласно руководству.

В настройках КУН-IP (КИО-2М) рисунок 4, устанавливается флажок «Включить VPN».

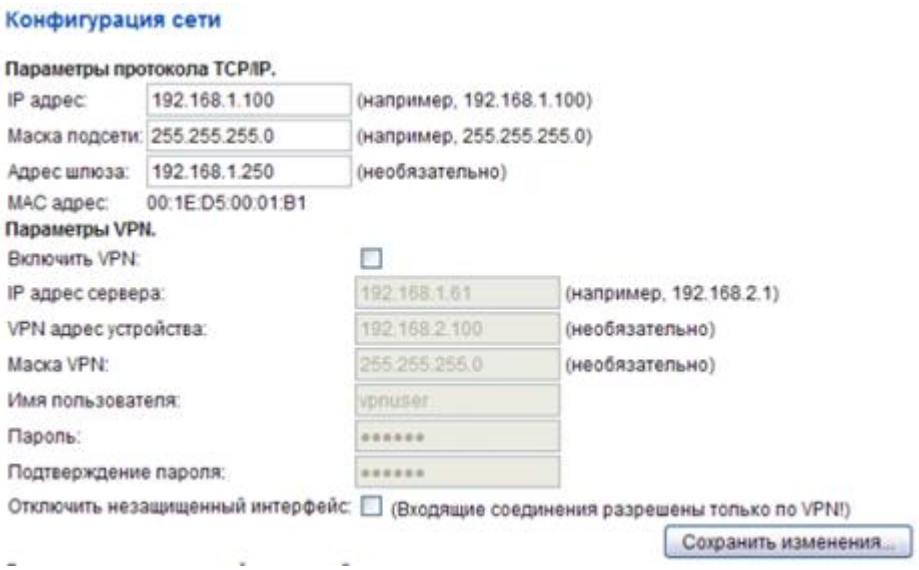

Рисунок 4 – Настройка концентратора КУН-IP.

Указываем:

- IP адрес сервера: 77.88.21.19
- VPN адрес устройства: 192.168.0.20 (уникальный для каждого устройства, подключаемого к создаваемой VPN-сети. Внутри сети устройство будет идентифицироваться по этому адресу).
- Маска VPN: 255.255.255.0
- Имя пользователь: (как прописано на VPN-шлюзе)
- Пароль: (как прописано на VPN-шлюзе)

На КИО-8(4) настраиваем исходящее VPN-подключение средствами Windows.

В итоге, после подключения устройств к VPN-шлюзу мы получим представленную на рисунке 5 VPN-сеть.

Образно говоря, VPN-шлюз «пробросил» все наши удаленные устройства во внутреннюю локальную сеть, в которой находится ПК-диспетчера.

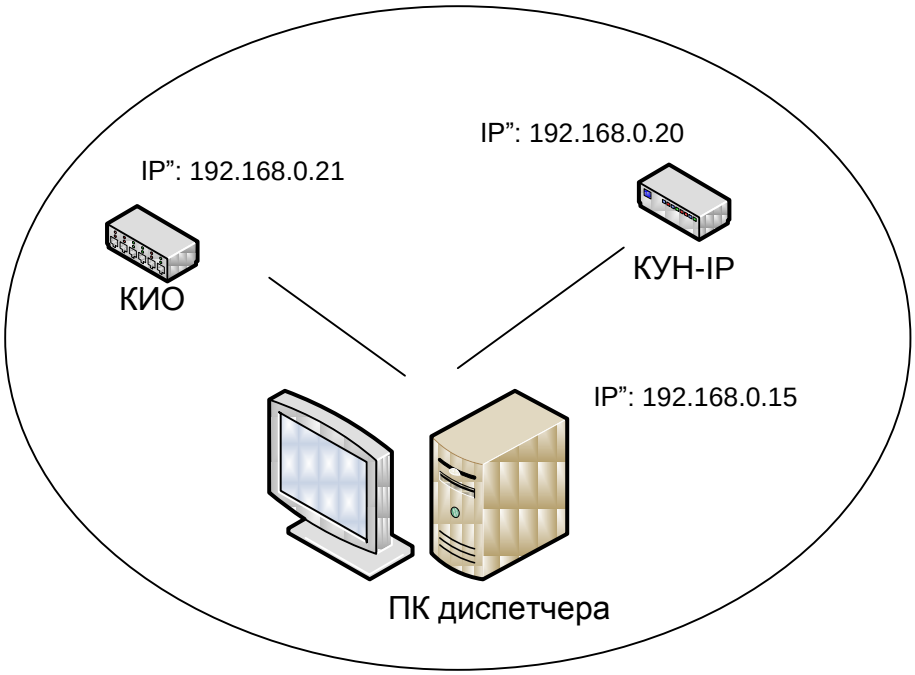

Рисунок 5 – Логическая структура VPN-сети

В программном обеспечении на ПК-диспетчера следует настраивать устройства, указывая их vpn IP"-адреса(т.е., например, для КУН-IP следует указывать IP"-адрес 192.168.0.20).