Организация охраны с использованием IP-сетей.

1.Общая структура организации охраны

Организация охраны объектов с использованием IP-сетей подразумевает:

- Наличие опорной IP-сети, имеющей достаточную зону покрытия
- Наличие надежного подключения оборудования пульта к опорной IP-сети
- Наличие возможности подключения объектового оборудования к IP-сети

Подключение к опорной IP-сети может осуществляться с использованием разных сред передачи:

- Ethernet
- ADSL
- PON
- GPRS

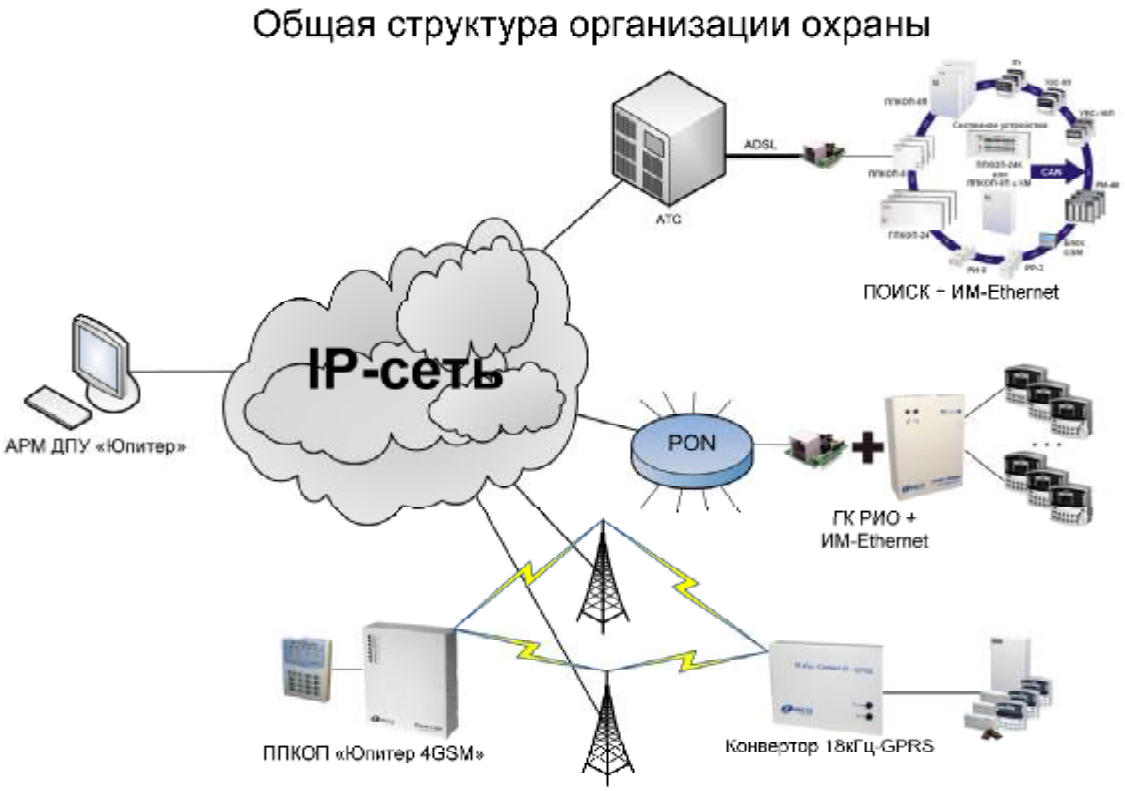
и т.д.

Указанные варианты подключения могут использоваться как на охраняемых объектах так и на пульте.

С целью обеспечения надежности рекомендуется, по возможности, использовать несколько вариантов подключения к опорной сети, как на пульте, так и на охраняемых объектах

Для функционирования системы необходимо, чтобы все каналы пультового подключения имели статические IP-адреса, видимые со стороны охраняемых объектов (объекты должны иметь возможность отправки пакетов на пульт).

Объектовое оборудование может использовать как статические, так и динамические IP-адреса. При этом сами объектовые приборы могут не иметь возможность прямой адресации с пульт (могут быть закрытыми от опорной сети маршрутизаторами и шлюзами).



2.Особенности IP-сетей

При рассмотрении различных схем организации подключения объектового оборудования на пульт с использованием IP-сетей следует осветить некоторые особенности построения охраны.

Традиционные системы охраны сроятся на основе постоянного контроля канала передачи данных. Это может происходить как при использовании прямого контроля объекта (радиоканал), так и при передаче информации по цепочке ретранслирующих устройств (проводные системы охраны по занятым линиям).

В первом случае канал состоит из одного участка передачи информации и пульт непосредственно контролирует наличие постоянного потока информации с охраняемых устройств (происшествия, сигналы контроля линии и т.п.)

Во втором случае контроль линий связи осуществляют устройства, непосредственно отвечающие за примыкающий к ним участок канала передачи. Сигнал о неисправности участка передается вверх по цепочке ретрансляторов и достигает пульт в ряду обычных сообщений о происшествиях на объектах. Данный вариант позволяет децентрализовать процесс контроля.

В обоих случаях контроль канала осуществляется специализированным **охранным** оборудованием, и неисправности могут быть выявлены и исправлены в рамках настройки и конфигурирования только **охранного** оборудования и силами сотрудников технической службы охранной структуры.

В случае использовании для передачи данных IP-каналов возникает видимость отсутствия промежуточных звеньев между объектовым оборудованием и пультом. Создается иллюзия того, что сигнал, переданный объектовым оборудованием, напрямую достигает пульта.

В реальности IP-пакет передается по длинной цепочке устройств, большинство которых являются активными элементами.

Диагностирование причин непрохождения пакетов от объекта на пульт (или обратно, с пульта на объект) зачастую затруднено как сложностью IP-сети, так и отсутствием непосредственного доступа к элементам её образующим (используется сеть Интернет или IP/VPN-сеть сроиться сторонними организациями)

Многие провайдеры, предоставляющие свои сети для передачи данных, не имеют возможности или желания организовывать систему автоматического изменения маршрутов передачи при возникновении аварий в отдельных участках сети.

Кроме того для передачи информации от охраняемых приборов используются сети изначально ориентированные на передачу трафика общего назначения, не предъявляющего требований ни к скорости, ни к надежности.

Именно сложностью построенной опорной сети и наличием в ней возможности задержки и пропадания сигналов при её работе в штатном режиме обусловлено достаточно большое время определения реальной неисправности приборов. В противном случае велик риск получения большого числа ложных неисправностей, либо объем трафика, формируемого каждым прибором, значительно возрастет.

3.Соединение с использованием Интернет

Использование в качестве опорной сети Интернет является удачным решением, как на этапе начального развертывания пульта, так и при эксплуатации пульта небольшого размера.

3.1 Подключение пульта

Основным условием развертывания пульта является получение одного (лучше 2-х) каналов для подключения к сети Интернет, с привязанными к ним **статическими** **публичными** IP-адресами (адреса «видимые» из любой точки глобальной сети).

В качестве канала подключения к сети может использоваться как фиксированный проводной канал (ADSL, Ethernet, оптика, выделенная линия), так и беспроводной вариант (GPRS, 3G, WiMax, CDMA).

Так как статические публичные IP-адреса являются ограниченным ресурсом, то услугу по их предоставлению предлагают не все операторы и она всегда платная (200-400 руб./месяц).

Если получение статического адреса у проводных операторов, как правило, не вызывает проблем, то операторы мобильной связи предоставляют эту услугу не во всех регионах (Мегафон, МТС, местные операторы). Официальная информация о предоставлении статических адресов на всей территории покрытия имеется только по трем операторам: Beeline (GSM), Yota (WiMax) и SkyLink (CDMA).

Подключение каждого оператора на пульт целесообразно выполнять с использованием собственного маршрутизатора, который не только обеспечит защиту внутренней сети пульта (за счет использования встроенного FireWall-а), но и позволит получить доступ к сети другим компьютерам пульта, если в этом возникнет необходимость (технический/инженерный компьютер, стенд и т.п.)

Для автоматического переключения на работающий канал в составе программного обеспечения АРМ ДПУ «Юпитер» имеется специализированная утилита, позволяющая следить за исправным функционированием текущего канала связи и, при обнаружении потери связи с эталонной точкой в глобальной сети, переключиться на использование запасного канала (с периодической автоматической проверкой восстановления основного).

3.2 Подключение объектов

Подключение объектовых приборов к сети может производиться либо с использованием GPRS, либо с использованием Ethernet.

При использовании GPRS имеется возможность задействовать в приборе SIM-карты двух операторов, что повышает надежность соединения. Прибор автоматически отслеживает наличие ответов пульта при использовании текущей SIM-карты и адреса пульта, и, при отсутствии ответов в течение заданного времени, пытается переключиться на другой адрес пульта и/или SIM-карту.

Устанавливать две SIM-карты одного оператора не имеет смысла, так как в случае аварии связи будет отсутствовать на всех картах.

Для улучшения качества приема могут использоваться антенны, отличные от поставляемых с прибором.

При использовании Ethernet-соединения, непосредственное подключение и тип канала зависит от оператора.

Это может быть:

- ADSL-модем со встроенным или установленным дополнительно маршрутизатором;
- PON-маршрутизатор, один из дополнительных портов которого активируется для подключения охранного оборудования (в этом случае можно оговорить с оператором возможность задания гарантированной фиксированной полосы для охранного трафика).
- установка маршрутизатора поверх любого существующего Ethernet-подключения.

Подробности организации объектового подключения к Ethernet сети рассматриваются в пятой части нашего семинара.

Некоторые устройства («ГК РИО» и «ППКОП 4/8/16 GPRS/IP») предполагают возможность задействовать для подключения каналы разного типа (Ethernet и GPRS) .

3.3 Достоинства и недостатки

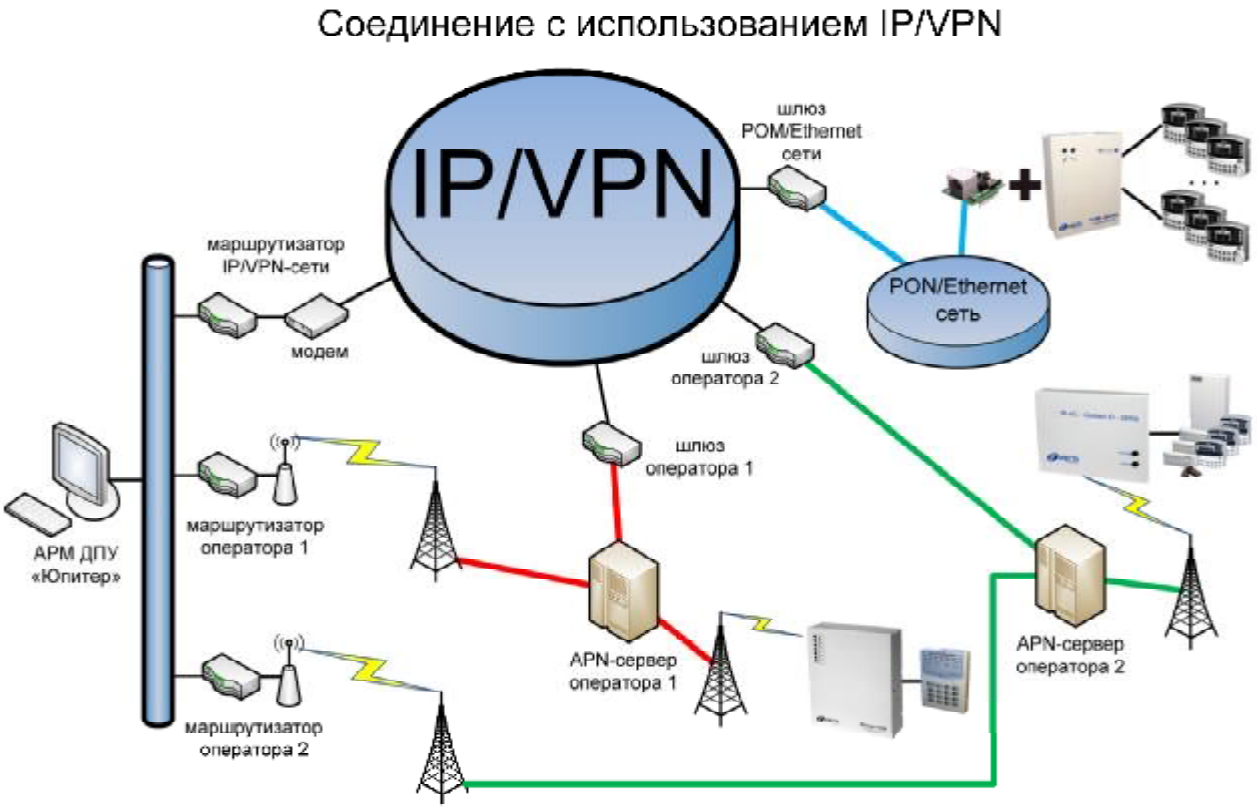
При любом способе подключения основным достоинством использования глобальной сети является широкая территория охвата и полностью симметричная структура полученной сети связи (вне зависимости от способа подключения прибор использует один и тот же набор IP-адресов пульта).

Недостатком использования глобальной сети является возможная нестабильность работы канала, включая и пультовой. При этом бывает трудно добиться от операторов быстрого локализации причины и исправления ситуации.

4.Соединение с использованием IP/VPN

Построение собственной IP/VPN-сети позволяет повысить надежность передачи информации за счет более полного контроля над каналами связи и структурой сети в целом, а также за счет закрытости сети от стороннего проникновения.

Построение IP/VPN-сети является достаточно затратной задачей и оправдано при использовании её в больших масштабах, а также для решения не только охранных, но и дополнительных задач (ведомственная телефония, видеонаблюдение, пересылка документов и т.п.)



4.1 Подключение операторов

Для передачи информации по IP/VPN-сети следует обеспечить специальные точки подключения объектовых операторов (как мобильных, так и стационарных) с использованием выделенных шлюзов.

На данный момент мобильные операторы начали активно предлагать услугу предоставления выделенного сервера (APN-сервера). В случае использовании данной услуги данные, пересылаемые с устройства, не попадают в глобальную сеть, а передаются на специальный сервер клиента, связанный с узлом передачи данных оператора выделенным каналом связи.

Указанный сервер, в свою очередь, подключается к корпоративной сети с использованием отдельного шлюза, в задачу которого входит пропуск в сеть только тех данных, которые необходимы для организации процесса охраны. Тем самым достигается защита корпоративной сети от возможных атак с использованием корпоративных SIM-карт.

Подключение операторов стационарной связи производится полностью аналогично, только в этом случае настройка передачи данных от объекта до выделенного сервера входит в круг обязанностей оператора. Процедура настройки аналогична выполнению кроссировки при использовании проводных систем охраны по занятой линии.

4.2 Подключение пульта

Для организации охраны с использованием IP/VPN-сети необходимо обеспечить надежное подключение к ней пульта.

Каналы, используемые для подключения к сети в этом случае, как правило, значительно более надежны, чем при использовании сети Интернет. Это связано с тем, что структура сети и используемые технические решения находятся под большим контролем, что позволяет выбирать наиболее надежные варианты.

Практически все устройства, используемые для организации канала, находятся в собственности организации и обслуживаются «своими» специалистами, благодаря этому они могут быть зарезервированы и оперативно заменены в случае аварии.

В тоже время цена поддержка запасного канала в данном случае является неоправданно высокой. Это вызвано тем, что если быстро исправить ситуацию заменой устройств в рамках канала подключения не удается, то, как правило, это говорит о наличии серьезных проблем в самой сети, и, в этом случае, резервный канал также будет находиться в неисправном состоянии и его наличие не сможет исправить ситуацию.

Решением, позволяющим частично смягчить проблемы при аварии опорной сети, является наличие на пульте альтернативных каналов подключения непосредственно к серверам операторов мобильной связи. Такое подключение может быть достигнуто путем установки пультовых маршрутизаторов с модемами, в которых будут задействованы SIM-карты, аналогичные картам, используемым в объектовых приборах. Данные каналы задействуются в том случае, когда штатный канал недоступен, а в остальное время находятся в режиме ожидания, так как постоянный пропуск пультового трафика по мобильным каналам гораздо более дорог, чем по стационарным.

Разумеется, данный вариант не позволит обеспечить резервирование связи пульта с приборами, работающими по Ethernet.

5.Объектовое подключение с использованием PON/Ethernet/ADSL

Наличие на объекте стационарного канала связи (ADSL/PON/КТВ/Ethernet) можно, во всех случаях, рассматривать как наличие на объекте **Ethernet**-канала. Способ его получения не имеет никакого значения, так как результат во всех случаях одинаков.

Во всех случай для организации подключения используется некое активное оборудование, бесперебойное питание которого следует обеспечить. Это становится особенно актуально при использовании PON-технологий, так как весь остальной канал связи до АТС функционирует без дополнительного питания.

Выполнение данного требования накладывает ограничение на список используемого оборудования, так как желательно, чтобы оно питалось от источников питания напряжением 12В, что позволит использовать источник питания охранного прибора.

Также желательно предусмотреть возможность ограничения доступа к активному оборудованию, размещая его в защищенных от проникновения шкафах, оборудованных датчиками вскрытия.

Также желательно ограничить доступ пользователей к настройкам активного оборудования.

Объектовое подключение к PON/Ethernet/ADSL-сети
(на примере РИО-М)