БИБЛИОТЕКА ТЕХНИЧЕСКОГО СПЕЦИАЛИСТА ОХРАНЫ

Министерство внутренних дел Российской Федерации
Главное управление вневедомственной охраны

РЕКОМЕНДАЦИИ
по организации централизованной охраны при проведении операторами связи модернизации сетей передачи данных, в том числе с применением PON-технологий

Р 78.36.019-2012

Москва 2012

gost.e-ecolog.ru

Министерство внутренних дел Российской Федерации
Главное управление вневедомственной охраны

УТВЕРЖДЕНО
Заместителем начальника
ГУВО МВД России
полковником полиции
А.В. Грищенко
06 апреля 2012 года

РЕКОМЕНДАЦИИ
по организации централизованной охраны при проведении операторами связи модернизации сетей передачи данных, в том числе с применением PON-технологий

Р 78.36.019-2012

Москва 2012

Рекомендации разработаны сотрудниками Федерального казенного учреждения «Научно-исследовательский центр «Охрана» Министерства внутренних дел Российской Федерации и утверждены Главным управлением вневедомственной охраны Министерства внутренних дел Российской Федерации 06 апреля 2012 года.

Рекомендации по организации централизованной охраны при проведении операторами связи модернизации сетей передачи данных, в том числе с применением PON-технологий: Типовые варианты. - М.: ФКУ НИЦ «Охрана» МВД России, 2012, 105 л.

Рассмотрены вопросы организации централизованной охраны и применения технических средств охранной сигнализации, представлены типовые варианты охраны объектов, квартир и мест хранения имущества граждан при внедрении операторами связи оптических технологий.

Предназначены для инженерно-технических работников вневедомственной охраны, занимающихся вопросами организации централизованной охраны объектов, квартир и мест хранения имущества граждан.

ФКУ НИЦ «Охрана» МВД России выражает признательность специалистам заводов-производителей систем централизованного наблюдения за предоставленный материал, участие в обсуждении документа, а также за высказанные ценные замечания и предложения.

@ ФКУ НИЦ «Охрана» МВД России, 2012.

1. ОПРЕДЕЛЕНИЯ И УСЛОВНЫЕ СОКРАЩЕНИЯ

1.1 В настоящих рекомендациях приняты следующие понятия и определения:

ADSL (Asymmetric Digital Subscriber Line — асимметричная цифровая абонентская линия) – технология высокоскоростной (несколько Мбит/сек) передачи данных по существующей абонентской телефонной линии с одновременным использованием этой линии как обычной телефонной.

BGP (Border Gateway Protocol) – протокол маршрутизации в среде Internet между автономными системами (AS). BGP обеспечивает обмен маршрутными данными, содержащими полные пути AS и обеспечивающими реализацию политики маршрутизации на основе конфигурационных параметров.

DHCP (*Dynamic Host Configuration Protocol* — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

GPRS (*General Packet Radio Service* — пакетная радиосвязь общего пользования) — надстройка над технологией мобильной связи GSM, осуществляющая пакетную передачу данных. GPRS позволяет пользователю сети сотовой связи производить обмен данными с другими устройствами в сети GSM и с внешними сетями, в том числе Интернет. При использовании GPRS информация собирается в пакеты и передаётся через неиспользуемые в данный момент голосовые каналы. При этом, что является приоритетом передачи — голосовой трафик или передача данных — выбирается оператором связи.

GSM – международный стандарт цифровой сотовой связи, глобальная система мобильной связи. GSM обеспечивает поддержку следующих услуг:

-услуги передачи данных (синхронный и асинхронный обмен данными, в том числе пакетная передача данных — GPRS);

-передача речевой информации;

-передача коротких сообщений (SMS);

-передача факсимильных сообщений.

Ethernet – пакетная технология передачи данных преимущественно локальных компьютерных сетей (стандарт IEEE 802.3).

IP (Internet Protocol) — межсетевой протокол, относящийся к маршрутизируемым протоколам семейства TCP/IP и неотъемлемой частью которого является адресация сети по средствам IP-адресов.

IP-адрес – уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP.

PON (*Passive optical network*) – пассивная оптическая распределительная сеть древовидной архитектуры с технологией широкополосного мультисервисного доступа по оптическому волокну и разветвлением оптического сигнала в одноволоконной оптической линии связи с помощью пассивных разветвителей оптической мощности – сплиттеров.

SIM-карта (*Subscriber Identification Module* — модуль идентификации абонента) — идентификационный модуль абонента, применяемый в мобильной связи стандарта GSM. При выпуске SIM-карты ей присваивается четырёхзначный цифровой PIN-код, который записывается на карту, а также передается абоненту вместе с картой.

SMS (*Short Message Service* — служба коротких сообщений) — технология, входящая в стандарты сотовой связи и позволяющая осуществлять приём и передачу коротких текстовых сообщений.

TCP (*Transmission Control Protocol* — протокол управления передачей) — сетевой протокол Интернета, предназначенный для управления передачей данных в сетях и подсетях TCP/IP.

VLAN (виртуальная локальная сеть) – группа персональных компьютеров, серверов и других сетевых ресурсов, которые физически находятся в различных сегментах, но логически связаны друг с другом.

VPN – (*Virtual Private Network* — виртуальная частная сеть) – это объединение локальных сетей или отдельных машин, подключенных к сети общего пользования, в единую сеть, обеспечивающую секретность и целостность передаваемой по ней информации. Условно сети VPN разделяются на три основные группы по способу реализации:

- традиционные сети VPN на основе криптографических сервисов шифрования и аутентификации данных, реализованных в таких протоколах, как IPSec;
- традиционные сети VPN на основе разделения каналов второго уровня (Frame Relay, ATM, Ethernet VLAN);
- сети VPN на основе разделения таблиц коммутации и маршрутизации (MPLS VPN). Сети MPLS L3 VPN строятся на основе разделения таблиц маршрутизации. Сетевые префиксы, принадлежащие определенной сети VPN, выносятся в отдельную таблицу маршрутизации, и продвижение трафика в рамках данной VPN происходит по маркированному пути LSP (Label Switched Path), построенному специально для префиксов в этой таблице.

WAN – глобальная компьютерная сеть, объединяющая территориально рассредоточенные компьютеры, находящиеся на больших расстояниях друг от друга;

Динамический IP-адрес – IP-адрес называют динамическим (непостоянным, изменяемым), если он назначается автоматически при подключении устройства к сети и используется в течение ограниченного промежутка времени, как правило, до завершения сеанса подключения.

Интегратор – компания-подрядчик, осуществляющая оказание консультационных услуг, настройку программного обеспечения и оборудования в области информационных технологий.

Маршрутизатор (роутер) – совокупность аппаратных и программных средств для управления потоком данных в сети.

Медиаконвертер (преобразователь среды) – устройство, преобразующее среду распространения сигнала из одного типа в другой. В современной терминологии медиаконвертер работает как связующее звено между двумя средами – оптическим и медным кабелями.

Мультиплексор – устройство, предназначенное для коммутации входящих информационных потоков на один выходной поток.

Сетевой шлюз - устройство, конвертирующее сигналы/данные в форму, пригодную для транспортировки по сети Интернет. Сетевой шлюз может быть специальным аппаратным маршрутизатором (роутером) или программным обеспечением, установленным на обычный сервер или персональный компьютер.

Статический IP-адрес – IP-адрес называют статическим (постоянным, неизменяемым), если он прописывается в настройках устройства пользователем, либо если назначается автоматически при подключении устройства к сети, но используется в течение неограниченного промежутка времени и не может быть присвоен другому устройству.

1.2 В настоящих рекомендациях приняты следующие сокращения:

АРМ ДПУ – автоматизированное рабочее место дежурного пульта управления;

АСПИ – автоматизированная система передачи извещений;

АТС – автоматическая телефонная станция;

ВОЛС – волоконно-оптическая линия связи;

МХИГ – место хранения имущества граждан;

ПЦО – пункт централизованной охраны;
ПЦН – пульт централизованного наблюдения;
СПИ – система передачи извещений;
УОО – устройство оконечное объектовое;
ШТК – шкаф телекоммуникационный;
ШС – шлейф сигнализации.

2. ОБЩИЕ ПРИНЦИПЫ ОРГАНИЗАЦИИ СЕТИ ЦЕНТРАЛИЗОВАННОЙ ОХРАНЫ С ИСПОЛЬЗОВАНИЕМ НОВЕЙШИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Бурное развитие информационных технологий в области коммуникаций предполагает дальнейшее использование различных каналов связи для целей охраны.

Внедрение оптических технологий требует внесения изменений в организацию централизованной охраны объектов. Основное направление изменений заключается в переводе информационных потоков, поступающих от объектов, в цифровую форму для их дальнейшей передачи на ПЦН с использованием универсальной среды.

В качестве универсальной среды передачи данных рассматривается сеть, использующая для передачи данных IP-протоколы.

Организация централизованной охраны объектов с использованием IP-сетей подразумевает:

- наличие опорной IP-сети, имеющей достаточную зону покрытия;
- наличие подключения оборудования пульта к опорной IP-сети;
- наличие подключения оборудования приемного комплекта к опорной IP-сети;

- наличие подключения объектового оборудования к IP-сети;

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

- Ethernet;
- ADSL;
- FTTC, FTTB, FTTH, xPON;
- GPRS и т.д.

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

В качестве опорной сети в подразделениях вневедомственной охраны создаётся IP/VPN-сеть, что позволяет повысить надежность передачи информации за счет контроля над каналами связи и структурой сети в целом, а также за счет закрытости сети от стороннего проникновения. На ПЦО, как правило, используется единственное подключение к опорной сети. Для подключения к IP/VPN-сети целесообразно использовать собственный маршрутизатор, который не только обеспечит защиту внутренней сети пульта (за счет использования встроенного FireWall), но и позволит получить доступ к сети другим компьютерам пульта, если в этом возникнет необходимость (технический/инженерный компьютер, стенд и т.п.).

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).

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). При использовании IP/VPN-сети элементы приемного комплекта и объектовое оборудование также может иметь статические IP-адреса, видимые со стороны пульта.

Порядок выделения IP-адресов определяется оператором связи (провайдером), который занимается поддержкой VPN-сети, для случая FTTH/xPON возможно (и наиболее оправдано) использование DHCP, администрирование которого также находится в ведении оператора связи.

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

3. ВЫБОР СПИ И ВСПОМОГАТЕЛЬНОГО ОБОРУДОВАНИЯ ДЛЯ ОРГАНИЗАЦИИ ЦЕНТРАЛИЗОВАННОЙ ОХРАНЫ НА МОДЕРНИЗИРОВАННЫХ АТС

При строительстве новых зданий связисты зачастую прокладывают к ним не медные кабели, а оптоволоконные. Это дает возможность операторам фиксированной связи предоставлять более конкурентно способные услуги по высокоскоростному доступу в Интернет и многопотоковому цифровому телевидению высокой четкости. При этом используются две технологии:

- оптический кабель прокладывается от головной АТС до так называемых выносов, которые могут располагаться как прямо на улице в железных контейнерах, так и в крупных многоквартирных зданиях. Вынос соединяется с абонентским оборудованием (телефоны, ADSL- модемы) обычными медными кабелями (технологии FTTC, FTTB).

- оптический кабель прокладывается до квартиры (офиса) абонента (технология FTTH).

Оптические технологии (FTTC, FTTB, FTTH, xPON) рассматриваются как один из способов организации передачи данных в рамках IP-сети, связывающей охраняемые объекты и ПЦО.

3.1 Организация оптических сетей доступа

Способы применения оптических технологий классифицируют по названию точки сопряжения с потребителем и объединяются названием FTTx – оптоволокно до точки «x»: FTTB (Fiber To The Building) - оптика до административного здания, FTTC (Fiber To The Curb) - до распределительного шкафа, FTTH (Fiber To The Home) - до жилого дома.

Технология «волокно в монтажный шкаф» FTTC обеспечивает один из простейших и наименее дорогих способов наращивания сети. В FTTC волоконно-оптический кабель из центрального узла (районной АТС или узла оператора услуг связи) приходит в монтажный шкаф (curb). Монтажный шкаф, который оснащается электронным распределительным оборудованием, может быть как уличного исполнения, так и исполнения для установки внутри помещений. От шкафа к абонентам идут медные витые пары. В отличие от телефонных пар, эти витые пары имеют лучшие технические характеристики и значительно меньшую длину до 500 м.

Технология FTTB (Fiber-To-The-Building) – оптика доведена до здания (строения).

В доме устанавливается коммутатор, который имеет число выходных портов, соответствующее количеству абонентов для их индивидуального подключения, и оптический входной порт для подключения к магистральному коммутатору или мультиплексору цифрового транспортного кольца. Коммутатор, устанавливаемый в доме, должен обеспечивать гарантированное предоставление требуемого качества для всех видов услуг, контролировать и управлять сервисными потоками по всем портам для каждого абонента в отдельности. Абоненты, как правило, подключаются с помощью стандартного витого парного кабеля.

Современные коммутаторы имеют модульную архитектуру и поддерживают широкий спектр интерфейсов

и протоколов, в том числе xDSL, HomePNA, 10/100 Base-TX/FX и т.д., и обеспечивают высокую гибкость при построении домовой распределительной сети. В квартире абонента устанавливается абонентский терминал (мультимедиа-адаптер), который обеспечивает преобразование цифровых потоков в аналоговые сигналы традиционных видов сервиса - видео и телефонии.

Технология FTTH (Fiber to the Home) - оптическое волокно до квартиры.

На сегодняшний день выделенная оптоволоконная линия является самой защищенной средой (на физическом уровне), особенно в сравнении с общими передающими средами. Кроме того, коммутаторы Ethernet, использующиеся в средах сервис-провайдеров, призваны обеспечить разделение физического уровня портов и логического уровня абонентов и имеют множество надежных функций защиты, которые в состоянии предотвратить практически все попытки вторжений.

В типовых конфигурациях сетей доступа Ethernet FTTH применяются недорогие одноволоконные линии, использующие технологию 100BX или 1000BX, с заданным максимальным радиусом действия 10 км. Для работы на больших расстояниях имеются оптические модули, позволяющие увеличить мощность оптического сигнала, а также оптоволоконные пары с оптическими модулями, которые можно подключить к порту любого Ethernet- оборудования.

Оптимальным решением для FTTH является технология пассивных оптических сетей Gigabit PON (GPON), характеризующаяся масштабируемостью и сверхбольшой пропускной способностью.

Суть технологии PON заключается в том, что между центральным узлом, расположенным на АТС и обеспечивающим подключение к магистрали, и абонентскими узлами создается полностью пассивная оптическая сеть древовидной

топологии. В промежуточных узлах дерева размещаются компактные пассивные оптические разветвители (сплиттеры), не требующие питания и обслуживания.

Так, компания ОАО «Ростелеком» применяет GPON для предоставления услуги доступа в Интернет в массовом порядке. В качестве абонентского терминала для доступа в Интернет в квартирах граждан применяется ONT (Optic Network Terminal) (абонентский узел), как правило, имеющий четыре Ethernet разъема FE (Fast Ethernet), один из которых можно использовать для организации централизованной охраны.

3.2 Технические критерии выбора СПИ

При организации централизованной охраны объектов, квартир и МХИГ по абонентским линиям городских телефонных сетей используются автоматизированные системы передачи извещений следующих типов: «Альтаир», «Атлас-20», «Атлас-20К», «Ахтуба», «Заря», «Приток-А», «Юпитер».

Для централизованной охраны при использовании оптических технологий СПИ должны удовлетворять следующим требованиям:

- наличие в составе системы ретрансляторов, устанавливаемых в выносы АТС;
- наличие свободного места в телекоммуникационном шкафе (выносе);
- наличие медной пары от выноса до абонента, где установлено объектовое оборудование;
- возможность установки ретранслятора в стойку внутри выноса;
- наличие связи от ретранслятора до ПЦО по оптическим каналам с использованием виртуальной локальной сети АТС по протоколу TCP/IP;
- наличие телефонной линии от ретранслятора до абонента;

- полная аппаратная и программная поддержка ретранслятором всего ранее установленного и имеющегося на объекте охраны объектового оборудования, не выработавшего установленные сроки службы;

- наличие между ретранслятором и ПЦН связи по каналам цифровой сети стандарта Ethernet, поддерживающим протокол TCP/IP;

- физическое подключение к сети Ethernet должно производиться через стандартный интерфейс, например 10/100 BaseT с соблюдением всех требований стандарта (тип разъема, разводка контактов, уровни сигналов и проч.).

В таблице 1 приведены типы СПИ, обеспечивающие организацию централизованной охраны при внедрении оптических сетей доступа с технологией FTTx.

Таблица 1 *– Типы СПИ для применения при внедрении оптических технологий*

Наименование СПИ	Наименование технологии			Приложение
	FTTC	FTTB	FTTH (GPON)	
Комплекс централизованного наблюдения «Альтаир»	*	*	*	А
Автоматизированная система передачи извещений «Приток-А»	+	+	+	Б
Автоматизированная система передачи извещений «Атлас-20»	+	+	+	В
Автоматизированная система передачи извещений «Юпитер»	+	+	+	Г
Автоматизированная система передачи извещений «Заря»	-	+	+	Д
Автоматизированная система передачи извещений «Ахтуба»	+	+	+	Е

Условные обозначения:
«+» - СПИ обеспечивает работу по технологии FTTx.
«-» - СПИ не обеспечивает работу по технологии FTTx.
«*» - оборудование находится в стадии разработки.

4. ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ОРГАНИЗАЦИИ ЦЕНТРАЛИЗОВАННОЙ ОХРАНЫ НА МОДЕРНИЗИРУЕМЫХ АТС

4.1 Прохождение и преобразование сигналов (извещений) от устройства оконечного до ПЦН

В основе архитектуры сети по технологии PON лежат построение и увязка трех основных участков.

Станционный участок - это активное оборудование OLT, WDM-мультиплексор и оптический кросс высокой плотности, смонтированные на узле электросвязи в помещении АТС.

Линейный участок, включающий в себя пассивные оптические разветвители и кабели, располагающиеся между станционным и абонентским оборудованием.

Абонентский участок представляет собой персональную абонентскую разводку одноволоконных линий от общих распределительных устройств до оптической розетки и активного оборудования ONT в квартире абонента или до группового сетевого узла ONU, смонтированного в офисе корпоративного клиента.

Оптимальным вариантом прохождения и преобразования сигнала является последовательность, в которой сигнал поступает с ONT на маршрутизатор оператора/интегратора, далее по протоколу TCP/IP попадает в сеть подразделения вневедомственной охраны и в зависимости от адреса назначения (IP-адреса), который прописывается в объектовом приборе, попадает на соответствующий АРМ ПЦО. При прохождении сигнала, с целью сохранить надежность охраны, обязательно требуется предусмотреть наличие резервного узла маршрутизации на основе BGP. Создание такого узла обеспечит резервирование основных путей преобразования сигнала и позволит гарантированно доставить сигнал от УО до ПЦО.

Также ядро сети, преобразовывающей сигналы передачи извещений, должно быть выполнено на технологии L3 VPN, что позволит подразделениям вневедомственной охраны сохранить постоянный контроль над сетью, даже в случае обслуживания такой сети сторонними организациями. Таким образом, все региональные подразделения вневедомственной охраны, имеющие сети связи должны привести их в соответствие со стандартом L3 VPN.

При использовании услуг интегратора для целей поддержки сети, необходимо включить в договор с интегратором условие еженедельного документирования состояния сети. В таком случае подразделение вневедомственной охраны будет полностью независимо от любого оператора связи или интегратора и сможет перейти к самостоятельному обслуживанию сети передачи извещений при наличии в штате достаточного количества специалистов нужной квалификации.

Рекомендуется при выборе способа прохождения сигналов не создавать единого цифрового ПЦО, так как это приведет к низкой отказоустойчивости и может обрушить всю сеть централизованной охраны.

4.2 Алгоритмы действий инженерно-технических работников вневедомственной охраны по организации централизованной охраны с использованием современных средств связи и технологий

При организации централизованной охраны по цифровым технологиям, в случае наличия в регионе более одного оператора связи, нужно провести квалификационный отбор интегратора для подключения максимального количества объектов в зоне действия ПЦО и определить соответствующее количество и квалификацию инженерно-технических работников подразделений вневедомственной охраны для выполнения следующих действий:

- создать отдельные рабочие места (АРМ) для работы с цифровыми технологиями или модернизировать существующие, установив программное обеспечение, реализующее возможность приема сигналов по протоколу TCP/IP, учитывая особенности такого прохождения (задержку, контроль наличия питания и т.п.);

- создать и принять в эксплуатацию IP/VPN-сеть подразделения, объединяющую АРМы, работающие по цифровым технологиям;

- провести испытания прохождения сигнала от УОО на АРМ ПЦО по участкам IP/VPN-сети каждого оператора связи, подключенного к корпоративной сети подразделения;

- разграничить зоны ответственности интегратора, подразделения вневедомственной охраны и персонала ПЦО;

- ввести в опытную эксплуатацию IP/VPN-сеть, предназначенную для подключения УОО;

- обеспечить каналообразующее оборудование гарантированным питанием и кондиционированием;

- разработать инструкции по действиям персонала ПЦО в нештатных ситуациях;

- обеспечить резервирование каналов подключения операторов связи к IP/VPN-сети подразделения и сигналов УОО с объектов подгрупп А1, А2 (по РД 78.36.003-2002 и РД 78.36.005-2005);

- обеспечить техническую поддержку (при возможности – и Интегратором) пользователей АРМ.

4.3 Порядок выделения IP-адресов для технических средств охраны, расположенных на ПЦО и квартирах

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).

Учитывая необходимость придерживаться единых стандартов маршрутизации, рекомендуется требовать от операторов выделения IP VPN сети третьего уровня, класса А (пример: 10.0.0.0 с маской 255.0.0). Далее сеть необходимо поделить на столько частей, сколько маршрутизаторов имеет оператор связи в регионе.

Следующим шагом ответственным в районах выдается пул (фиксированное количество) IP-адресов, соответствующий зоне обслуживания оператора (для решений с использованием статических IP-адресов), который используется при программировании УО.

При схеме с динамическим распределением IP-адресов, такие адреса выдаются сервером.

Учитывая, что при организации централизованной охраны по цифровым технологиям, подразделение вневедомственной охраны получает возможность использовать каналы разных операторов, количество подсетей растет пропорционально количеству операторов, подключенных к стыку.

Крайне важным моментом является наличие в подразделении вневедомственной охраны персонала, который способен:

обеспечивать интеграцию разных операторов связи, путем создания отдельных подсетей и VLANов, исключающих пересечение IP-адресов;

взаимодействовать с операторами связи в случае изменения конфигурации оборудования на территории оператора связи.

Данный порядок должен закрепляться приказом по подразделению, с назначением лиц ответственных за взаимодействие с оператором или интегратором, в случае, если последний берет на себя ответственность за обеспечение маршрутизации.

4.4 Порядок и нормативная база взаимодействия с операторами связи.

Любое взаимодействие с операторами связи должно происходить в рамках Федерального закона от 21.07.2005 г.

№ 94-ФЗ «О размещении заказов на поставку товаров, выполнение работ, оказание услуг».

Подразделение вневедомственной охраны готовит конкурсную документацию на создание и эксплуатацию телекоммуникационной инфраструктуры для организации централизованной охраны по цифровым технологиям, проводит анализ имеющейся материально-технической базы ПЦО и определяет конкретные параметры модернизации инфраструктуры, проводит выбор оператора или интегратора.

При выборе интегратора (оператора) необходимо убедиться в наличии у него материально-технической базы для выполнения практических мероприятий, а также установленного законодательством разрешения на предоставление услуг по передаче данных и телематических услуг.

После создания условий, позволяющих организовывать централизованную охрану по цифровым технологиям, подразделение вневедомственной охраны самостоятельно или совместно с интегратором определяет порядок дальнейших действий, включая:

1) проверку работы охранного оборудования в цифровой сети, в том числе PON с использованием абонентского устройства ONT;

2) согласование схемы включения основного и резервного узлов маршрутизации цифровой сети для передачи информации на ПЦО;

3) подготовку методики тестирования охранного оборудования на сети PON;

4) подготовку сервисной модели предоставления услуги «Охранная Сигнализация подразделения вневедомственной охраны через PON»;

5) проведение обучения сотрудников подразделения вневедомственной охраны новой услуге и работе с новыми АРМ;

6) проведение проектно-исследовательских и строительно-монтажных работ по подключению сетей связи

подразделений вневедомственной охраны к операторам цифровой связи;

7) проведение опытной эксплуатации услуги «Охранная Сигнализация подразделений вневедомственной охраны через PON»;

8) подготовка приказа о запуске услуги «Охранная Сигнализация подразделения вневедомственной охраны через PON» в эксплуатацию.

4.5 Основные монтажные и эксплуатационные затраты на оборудование для организации канала связи на ПЦО и на квартирах

При внедрении цифровых технологий основные затраты можно разделить на три категории.

Первая категория - единовременные затраты на создание современной сети связи, для обеспечения возможности приема охранных извещений с МХИГ и объектов.

Вторая категория - ежемесячные затраты на эксплуатацию сети (аренда волокон и каналов связи, обслуживание маршрутизаторов и т.п., устранение аварий).

Третья категория - ежемесячные затраты на аренду каналов связи от квартиры или объекта до ближайшей точки сети ПЦО.

При этом затраты по первой категории составляют фиксированную сумму и должны быть исключены в последующий год обслуживания (обычно составляют 10-15% от первоначальных затрат). Сумма таких затрат зависит от состояния телефонной канализации, удаленности объектов и рассчитывается исходя из технических условий компании, занимающейся проектированием.

Затраты по второй категории рассчитываются исходя из топологии построения сети, наличия резервирования на случай аварии, времени реагирования на неисправность и количества ПЦО.

Затраты по третьей категории обычно включаются в тариф за охрану или обеспечиваются собственником охраняемого помещения по прямому договору с оператором.

Типовые примеры организации централизованной охраны с помощью оборудования КЦН «Альтаир» по сетям Ethernet

Для организации централизованной охраны с помощью оборудования КЦН «Альтаир» в условиях развитии связи и услуг широкополосного доступа с использованием технологий построения сети FTTC – «оптика» до группы зданий и «медь» в квартиру разрабатываются два исполнения конструкции ретранслятора (01 и 02).

Конструктивно новые ретрансляторы встраиваются в девятнадцати дюймовые ШТК, которые изготавливаются предприятиями ООО «Компания АЛС и ТЕК», ООО «Телекор» и компанией «ISKRATEL» по заказу ОАО «Ростелеком».

Ретрансляторы КЦН «Альтаир» исполнение 01 и 02, устанавливаются внутрь ШТК, расположенного у группы зданий или внутри здания, и через VPN сеть, организованную оператором связи по протоколу TCP, подключаются к ПЦН. От ШТК до квартиры идет стандартная телефонная витая пара, которая используется для охраны как по переключаемым, так и по занятым телефонным линиям.

Ретранслятор исполнения 01 - выполнен в стандартном корпусе высотой 1U и имеет одно место для диспетчера и 3 места для линейных плат – рисунок А.1.

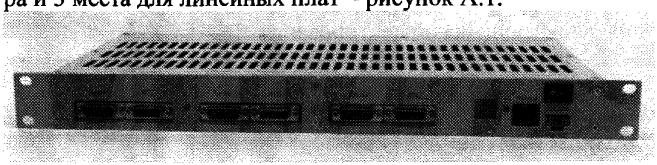


***Рисунок А.1**-Ретранслятор КЦН «Альтаир» – исполнение 01*

Ретранслятор исполнения 02 - выполнен в стандартном корпусе высотой 3U и имеет одно место для диспетчера и 12 мест для линейных плат – рисунок А.2.

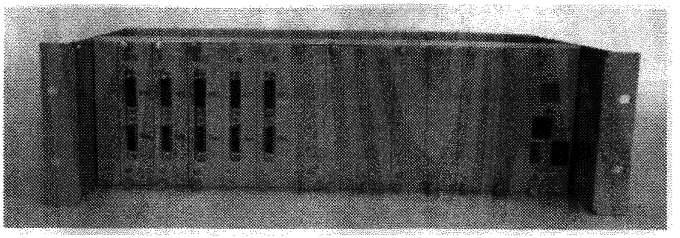


***Рисунок А.2** - Ретранслятор КЦН «Альтаир» – исполнение 02*

Передача команд и извещений производится по протоколу TCP/IP. Для обеспечения физической связи между АРМ ПЦН и ретрансляторами может использоваться любое оборудование, поддерживающее протокол TCP/IP в том числе и оптоволоконное. Ретранслятор обеспечивает работу как в локальных, так и в сетях общего пользования, и имеет ряд особенностей:

1. Сетевые настройки могут осуществляться дистанционно по сети с использованием любого WEB-браузера (например - Internet Explorer).

2. Ввод настроек защищен с помощью одноразовых паролей.

3. Обновление программного обеспечения может осуществляться дистанционно по сети с использованием специальных мер защиты.

4. Обеспечивается высокий уровень безопасности с помощью шифрования всех пакетов обмена данными между АРМом и ретрансляторами для чего применен профессиональный метод шифрования. Используется криптозащищенный протокол обмена с 80-битным ключом и 32-битным уникальным номером прибора.

5. Программное обеспечение модуля обеспечивает работу ретранслятора под управлением АРМ «Антей», «Радиосеть».

В состав ретранслятора входят:

- линейная плата переключаемых линий на 8 каналов (ЛПП-8К) для работы с объектовыми устройствами, использующими переключаемые на период охраны линии городской телефонной сети;

- линейная плата занятых линий на 8 каналов (ЛПЗ-8К) для работы с объектовыми устройствами, использующими занятые на период охраны линии городской телефонной сети и работающими на частоте 18 кГц.

Минимальные размеры линейных плат ЛПП-8К, ЛПЗ-8К и платы диспетчера - 176×100×25 мм, обеспечены за счет многослойности печатных плат, что позволило разработать ретранслятор в габаритах, обеспечивающих его размещение в любых конструкциях выносных телекоммуникационных шкафов.

Информационная емкость ретранслятора:

- исполнение 01 – 24;

- исполнение 02 – 96.

Информативность ретранслятора до 33 в зависимости от типа подключенных линейных плат и устройств оконечных.

Питание ретранслятора осуществляется от источника постоянного тока номинальным напряжением 48 или 60 В.

Организация централизованной охраны с использованием технологии FTTC приведена на рисунке А.3.

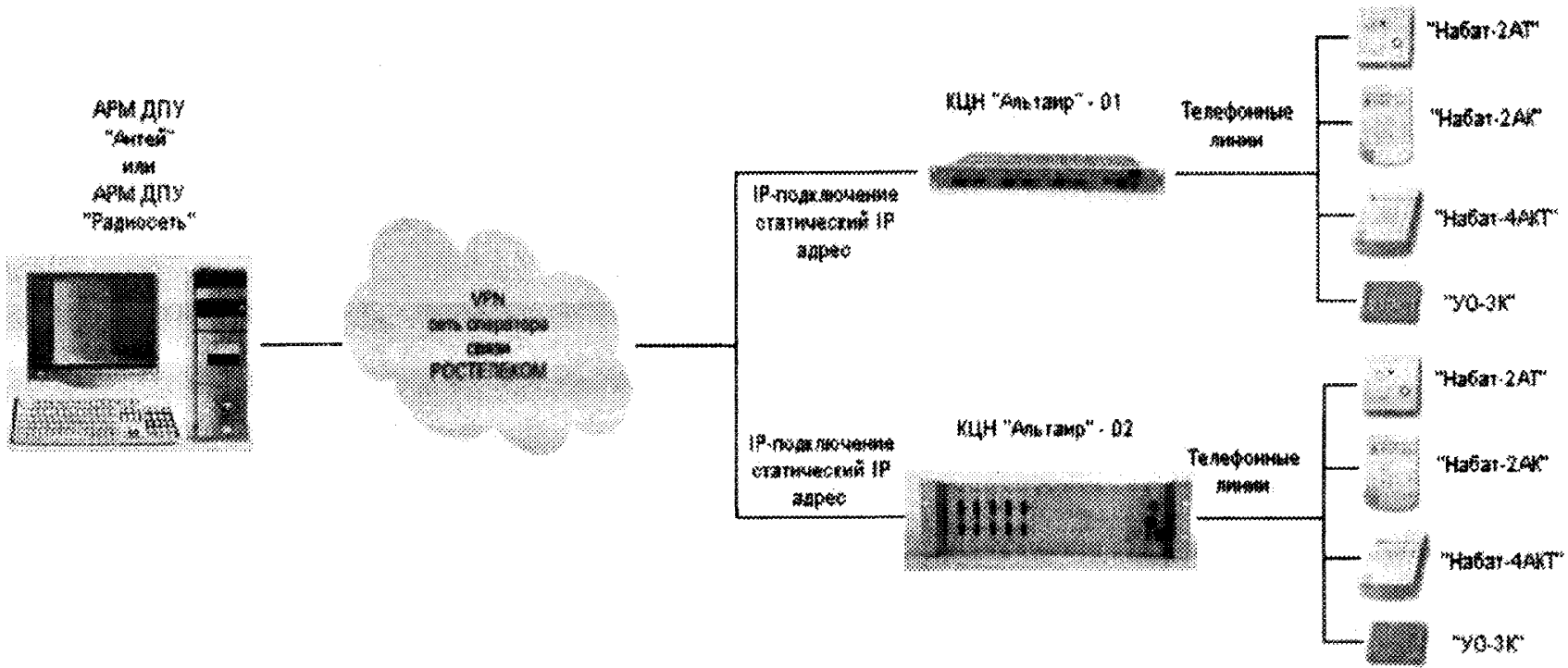


***Рисунок А.3** - Организация охраны с использованием КЦН «Альтаир»*

Организация централизованной охраны при использовании волоконно-оптической линии связи

Для организации централизованной охраны объектов с организацией связи по волоконно-оптическим линиям разрабатывается серия приборов:

1) прибор приемный контрольный охранно-пожарный «Редут-Net». Каналом передачи данных служит сеть Ethernet (окончание RG45). Питание осуществляется от внешнего резервированного источника питания 12В;

2) прибор приемный контрольный охранно-пожарный «Редут-Net-GSM». Основным каналом передачи данных служит сеть Ethernet (окончание RG45). Резервный канал реализован через сотового оператора (Beeline, МТС, MegaFon) с применением технологии GSM/GPRS, но допускается работа и только через GSM/GPRS (без подключения по Ethernet). Питание осуществляется от внешнего резервированного источника питания 12 В;

3) прибор приемный контрольный охранно-пожарный «Редут-Net-GSM-UPS». Основным каналом передачи данных служит сеть Ethernet (окончание RG45). Резервный канал реализован через сотового оператора (Beeline, МТС, MegaFon) с применением технологии GSM/GPRS, но допускается работа и только через GSM/GPRS (без подключения по Ethernet). Питание 12 В поступает от сетевого адаптера переменного тока напряжением 220В или встроенного резервированного источника питания. Емкость аккумуляторной батареи 2,2 А/ч;

4) прибор приемный контрольный охранно-пожарный «Редут-Net-Lcd». Каналом передачи данных служит сеть Ethernet (окончание RG45). Питание осуществляется от внешнего резервированного источника питания 12В. Наличие встроенного знакосинтезирующего дисплея;

5) прибор приемный контрольный охранно-пожарный «Редут-Net-GSM-Lcd». Основным каналом передачи данных служит сеть Ethernet (окончание RG45). Резервный канал реализован через сотового оператора (Beeline, МТС, MegaFon) с применением технологии GSM/GPRS, но допускается работа и только через GSM/GPRS (без подключения по Ethernet). Питание осуществляется от внешнего резервированного источника питания 12В. Наличие встроенного знакосинтезирующего дисплея;

6) прибор приемный контрольный охранно-пожарный «Редут-Net-GSM-UPS-Lcd». Основным каналом передачи данных служит сеть Ethernet (окончание RG45). Резервный канал реализован через сотового оператора (Beeline, МТС, MegaFon) с применением технологии GSM/GPRS, но допускается работа и только через GSM/GPRS (без подключения по Ethernet). Питание 12В поступает от сетевого адаптера переменного тока напряжением 220В или встроенного резервированного источника питания. Емкость аккумуляторной батареи 2,2 А/ч. Наличие встроенного знакосинтезирующего дисплея.

Приборы серии «Редут-Net» прошли тестовые испытания на сетях передачи данных ОАО «МГТС» (г. Москва), организованных по технологии PON.

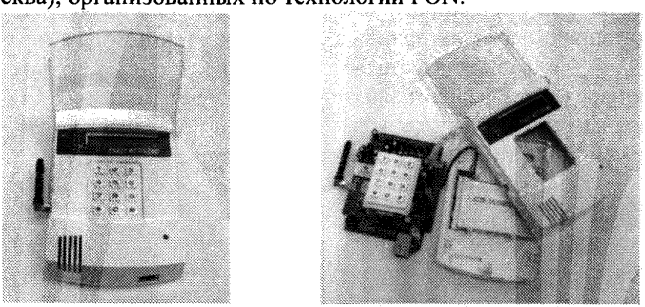


***Рисунок А.4** - Прибор приемно-контрольный охранный серии «Редут-Net»*

Назначение

Прибор предназначен для контроля состояния четырех ШС и передачи извещений о нарушении ШС по сети Internet, локальной вычислительной сети (ЛВС) или GSM/GPRS на ПЦН, оборудованный АРМ ДПУ. Область применения - охрана офисов, производственных и торговых помещений, квартир, дач и др. от несанкционированного проникновения и пожара – рисунок А.4 .

Особенности

- ППКО рассчитан на работу с АРМ «Антей» и «Радиосеть»;

- подключается к АРМ ПЦН по каналам Ethernet и GSM/GPRS. Основным каналом передачи данных является сеть Ethernet. Резервным каналом передачи информации является канал GSM. Допускается работа только через GSM/GPRS (без подключения по Ethernet);

- поддерживает совместную работу с Ethernet-оборудованием, поддерживающим скорость 10mbs/100mbs, работает как на статических, так и на динамических IP-адресах;

- разработан для работы через сеть Интернет или VPN, например, через технологию GPON;

- в зависимости от типа прибора питание осуществляется либо от внешнего резервированного источника питания 12В или встроенного резервированного источника питания с аккумуляторной батареей емкостью 1,8-2,2 А/ч;

- охрана осуществляется путем контроля состояния четырех шлейфов сигнализации с включенными в них охранными и пожарными извещателями и передачи тревожных и пожарных извещений на компьютеры АРМ ПЦН;

- имеет вход для подключения датчика отметки прибытия наряда;

- два программируемых выхода типа «открытый коллектор», предназначенных для подключения световых, звуковых оповещателей;

- взятие под охрану и снятие с охраны осуществляется с помощью встроенной клавиатуры или посредством применения персональных электронных идентификационных ключей Touch Memory;

- сетевые настройки прибора осуществляются дистанционно через WEB-интерфейс или с помощью специальной утилиты удаленно. Для работы с Web-интерфейсом может быть использован любой распространенный браузер (Internet Explorer, Opera, Firefox и др.);

- настройки прибора, такие как программирование типа шлейфов, задержки на вход и на выход, пошлейфное взятие (снятие), программирование кодов и паролей осуществляются удаленно с помощью специальной утилиты;

- предусмотрено удаленное обновление программного обеспечения прибора;

- обмен данными защищен шифрацией с псевдослучайными ключами;

- в зависимости от типа прибора вывод текущего состояния прибора, а также режимы работы выводятся на светодиодные индикаторы или дополнительно на встроенный знакосинтезирующий дисплей.

Технические характеристики

- 4 шлейфа сигнализации;

- в качестве канала связи используется сеть Ethernet или GSM/GPRS;

- поддержка протоколов ARP, ICMP, DHCP, UDP, HTTP, TFTP;

- обмен данными между ПЦН и УОО шифруется уникальным для каждого экземпляра УОО ключом шифрования, длина ключа шифрования 80 бит;

- 2 выхода типа «открытый коллектор» для подключения световых и звуковых оповещателей с защитой от перегрузки;

- возможность постановки и снятия с охраны как одиночных ШС, так и групп ШС;

- информативность – 22.

Для сопряжения, находящегося в эксплуатации ранее выпускавшегося объектового оборудования, и адаптации его к цифровым сетям новых оптических технологий разрабатываются устройства сопряжения:

1) устройство сопряжения для приборов, работающих по занятым телефонным линиям – «Редут-УС18»;

2) устройство сопряжения для приборов, работающих по переключаемым телефонным линиям – «Редут-УСПЛ».

Устройства однотипные и отличаются только интерфейсом сопряжения с разными типами приборов, поэтому приведено общее краткое описание.

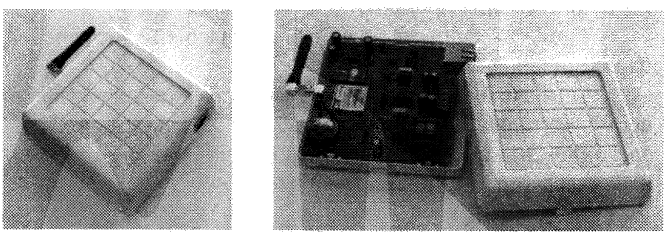


Рисунок А.5 - Устройство сопряжения

Назначение

Устройство предназначено для сопряжения старого парка приборов с каналами передачи данных, построенных по технологии FTTH и GPON. Осуществляет доставку извещений от приборов данного типа по сети Internet, ЛВС или GSM/GPRS на ПЦН, оборудованный АРМ ДПУ – рисунок А.5.

Особенности

- устройство рассчитано на работу с АРМ «Антей» и «Радиосеть»;

- подключается к АРМ ПЦН по каналам Ethernet и GSM/GPRS. Основным каналом передачи данных является сеть Ethernet. Резервным каналом передачи информации является канал GSM. Допускается работа только через GSM/GPRS (без подключения по Ethernet);

- поддерживает совместную работу с Ethernet-оборудованием, поддерживающим скорость 10mbs/100mbs, работает как на статических, так и на динамических IP-адресах;

- разработано для работы через сеть Интернет или VPN, например, через технологию GPON;

- питание осуществляется от внешнего резервированного источника питания 12В;

- сетевые настройки прибора осуществляются дистанционно через WEB-интерфейс или с помощью специальной утилиты удаленно. Для работы с Web-интерфейсом может быть использован любой распространенный браузер (Internet Explorer, Opera, Firefox и др.);

- предусмотрено удаленное обновление программного обеспечения устройства;

- обмен данными защищен шифрацией с псевдослучайными ключами.

Технические характеристики

- в качестве канала связи используется сеть Ethernet или GSM/GPRS;

- поддержка протоколов ARP, ICMP, DHCP, UDP, HTTP, TFTP;

- обмен данными между ПЦН и УОО шифруется уникальным для каждого экземпляра УОО ключом. Метод шифрования RC6, метод сцепления блоков CBC, длина ключа шифрования 80 бит.

Типовые примеры организации централизованной охраны с помощью оборудования КЦН «Альтаир».

На рисунке А.6 приведена возможная схема организации подключения приборов «Редут-Net» и устройств сопряжения с применением технологии GPON. Все охранные приборы могут иметь как статические, так и динамические IP-адреса. На ПЦН требуется публичный статический IP-адрес. Резервный канал обеспечивается с помощью операторов сотовой связи, находящихся в зоне развертывания охранного комплекса.

На рисунке А.7 приведена возможная схема организации подключения приборов «Редут-Net» по выделенной линии через ADSL-модем. Применение такой схемы возможно при построении сети по технологиям FTTB, FTTH, а также в сетях общего пользования. Количество охранных приборов, подключаемых по этой схеме, ограничивается только шириной канала ADSL-модема.

На рисунке А.8 приведена одна из возможных схем организации дополнительного резервного канала при построении сети с применением технологий FTTB, FTTH, а также GPON. В данной схеме применяется 3G-роутер TP LINK «TL-MR320» (или ему подобный) и подключенный к нему 3G-модем. Программное обеспечение роутера построено таким образом, что при отказе сети WAN он переходит на работу через подключенный к нему 3G- модем. При восстановлении сети автоматически завершается работа через 3G-модем. Роутер необходимо подключить к резервированному источнику питания.

На рисунке А.9 приведена схема построения сети, где все узлы работают на динамических IP-адресах, выделяемых провайдером. Связь всех узлов происходит через так называемый «Облачный сервер» с публичным IP-адресом. Специальное программное обеспечение, установленное на сервере, осуществляет маршрутизацию всех точек сети, зарегистрированных на этом сервере. В случае построения такой схемы возможно выделение только одного публичного IP-адреса для всех АРМ-ов и охранных приборов.

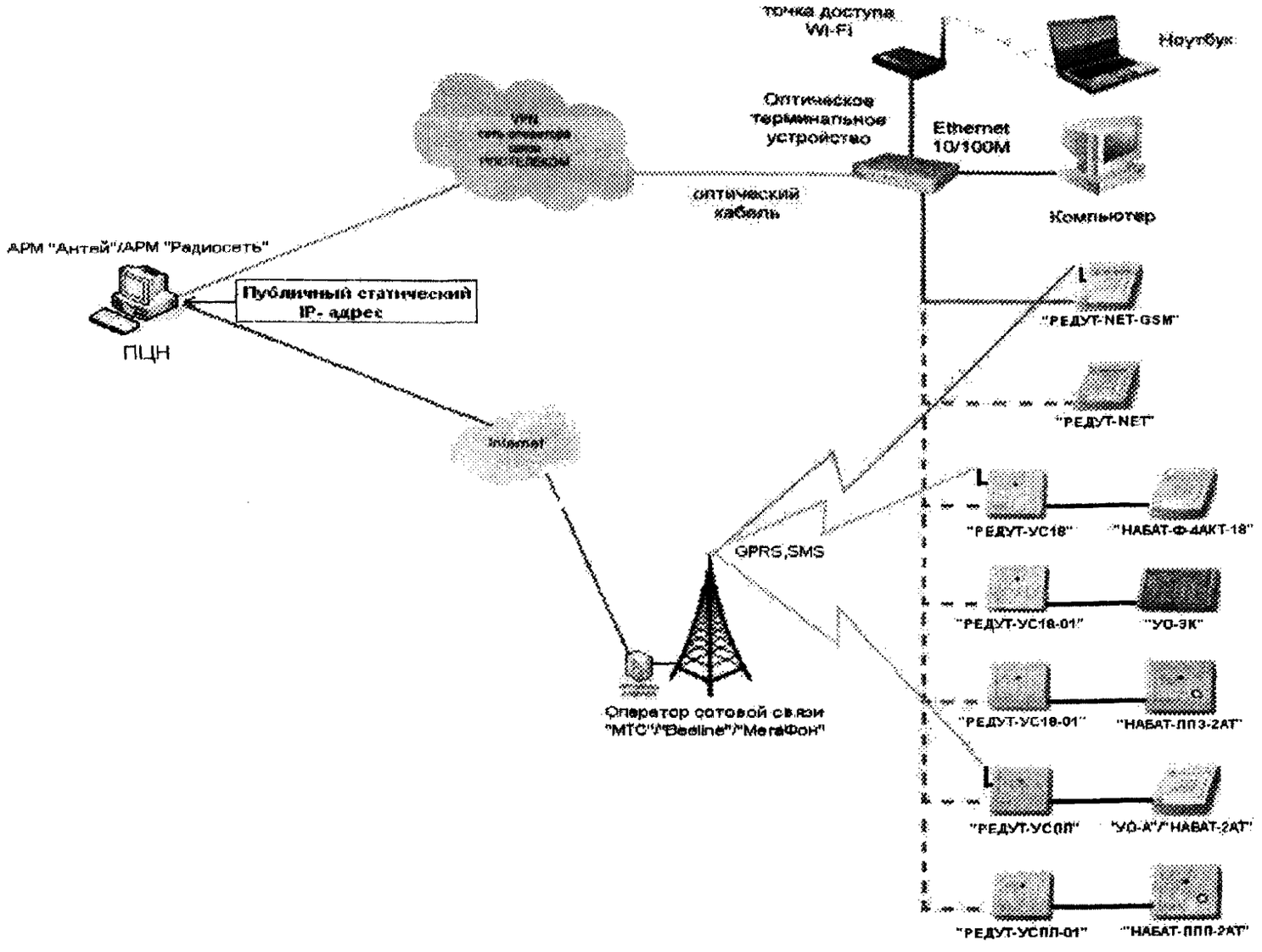


Рисунок А.6 *- Организация подключения приборов «Редут-Net» и устройств сопряжения с применением технологии GPON*

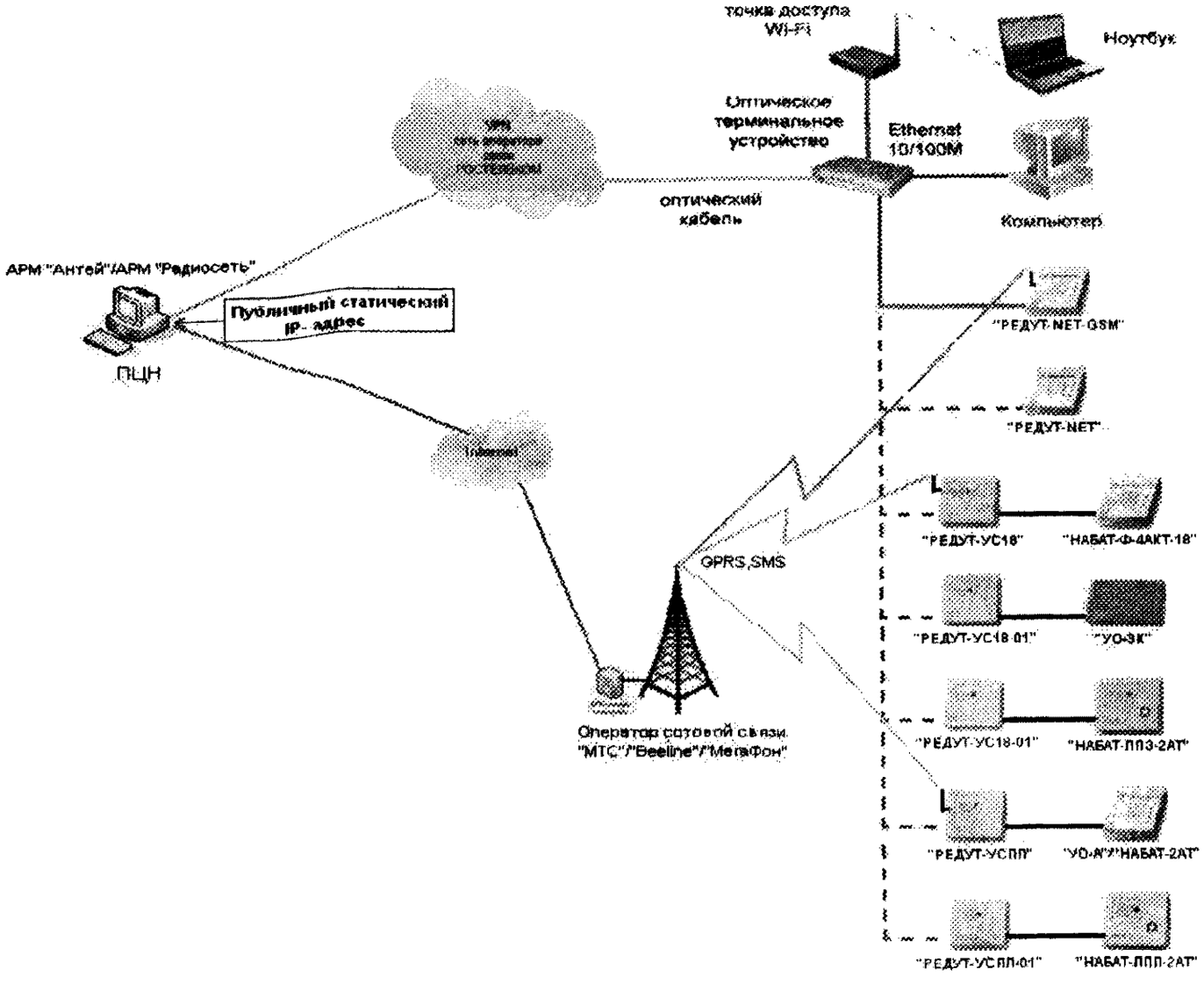


Рисунок А.7 *– Организация подключения приборов «Редут-Net» по выделенной линии через ADSL-модем*

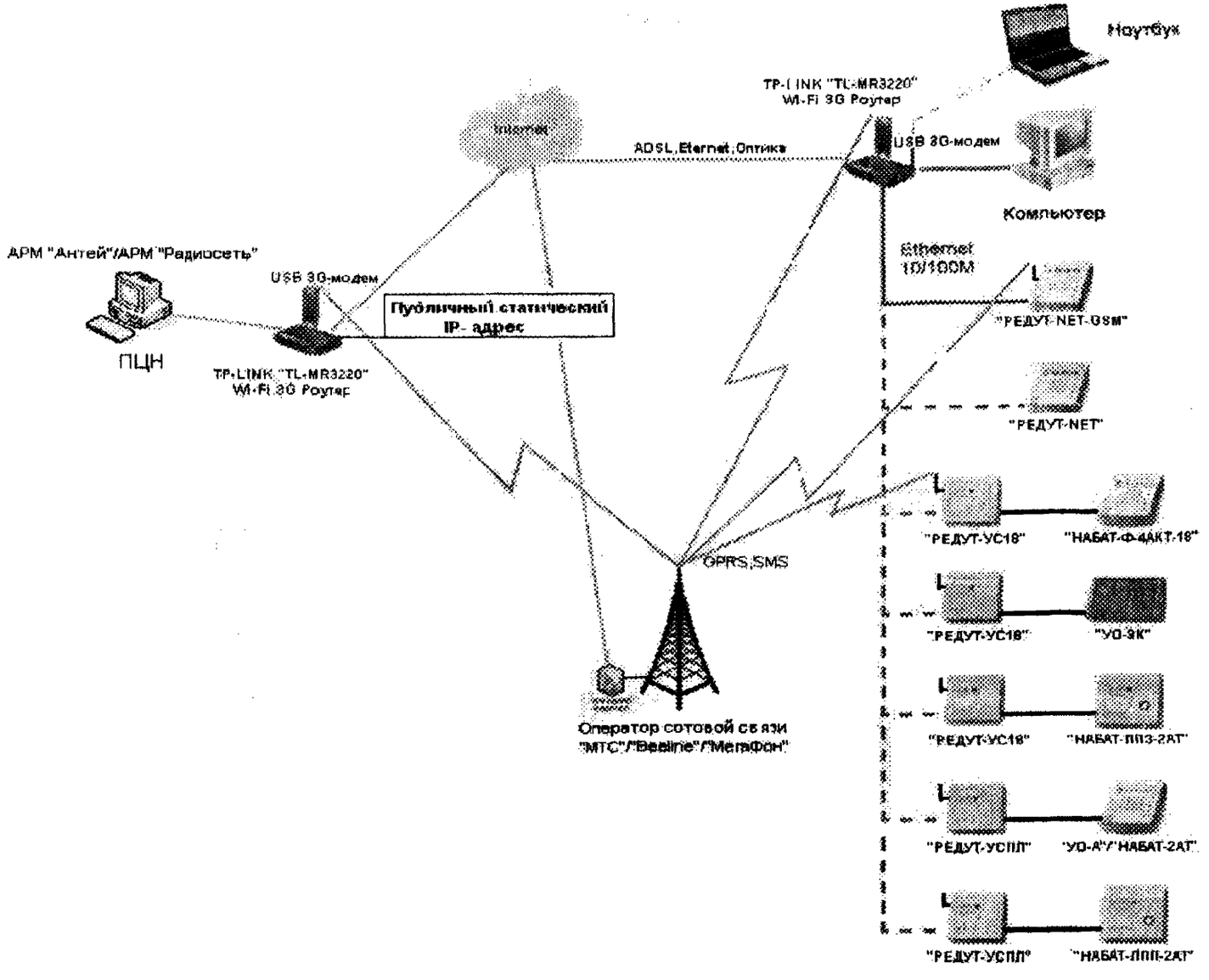


Рисунок А.8 *- Организация дополнительного резервного канала с применением USB-3G-модемов.*

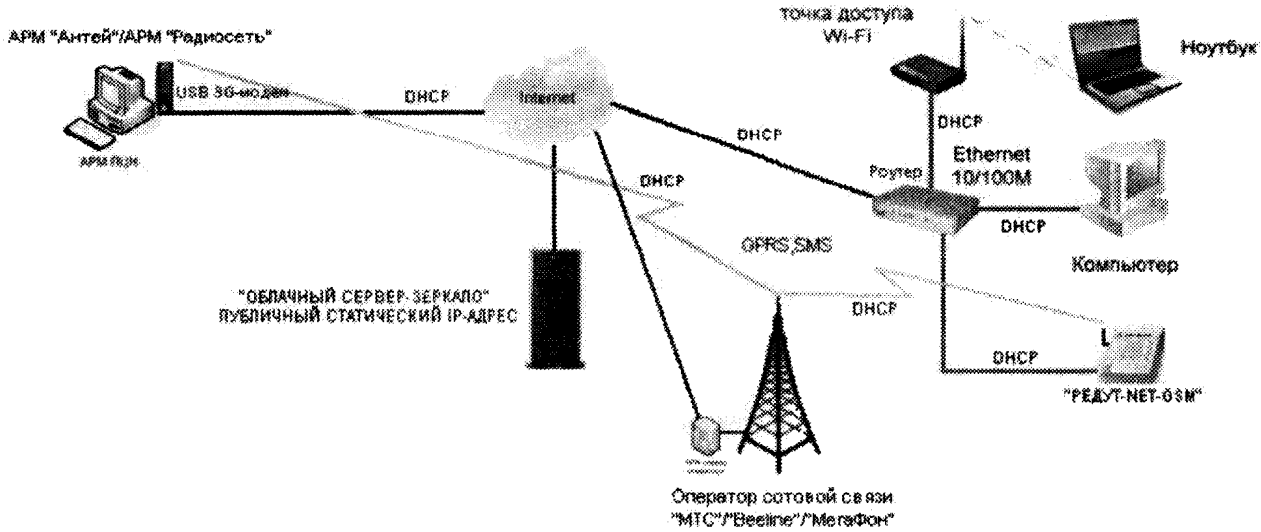


Рисунок А.9 *- Схема работы через дополнительный удаленный сервер.*

ПРИЛОЖЕНИЕ Б

Типовые примеры организации централизованной охраны с помощью оборудования СПИ «Приток-А» по сетям Ethernet

При организации телефонной связи города с помощью выносов и, возможно, без использования зданий АТС, для организации централизованной охраны возможно применение ретранслятора Приток-А, устанавливаемого в девятнадцатидюймовую стойку внутри выноса. Схема охраны представлена на рисунке Б.1.

Ретранслятор Приток-А, установленный внутрь выноса через VPN сеть, организованный оператором связи по протоколу TCP, подключен к ПЦН. От выноса до квартиры идет стандартная телефонная витая пара, которая используется для охраны как занятая телефонная линия. Ретрансляторы Приток-А выпускаются в трех вариантах исполнения по высоте и емкости:

Приток-А-01 - высота 6U – емкость 240 направлений;

Приток-А-02 - высота 3U – емкость 80 направлений;

Приток-А-03 - высота 1U – емкость 20 направлений.

К каждому из направлений ретранслятора подключается один из приборов серии Приток. Кроме этого, предусмотрен вариант ретранслятора, содержащий внутри aDSL модем, для возможного доступа к VPN сети оператора связи через aDSL подключение.

При организации связи по технологии GPON с применением ONT (абонентского узла), имеющего, как правило, четыре Ethernet разъема, один из разъёмов предлагается использовать для организации централизованной охраны.

Организация централизованной охраны с использованием технологии GPON изображена на рисунке Б.2.

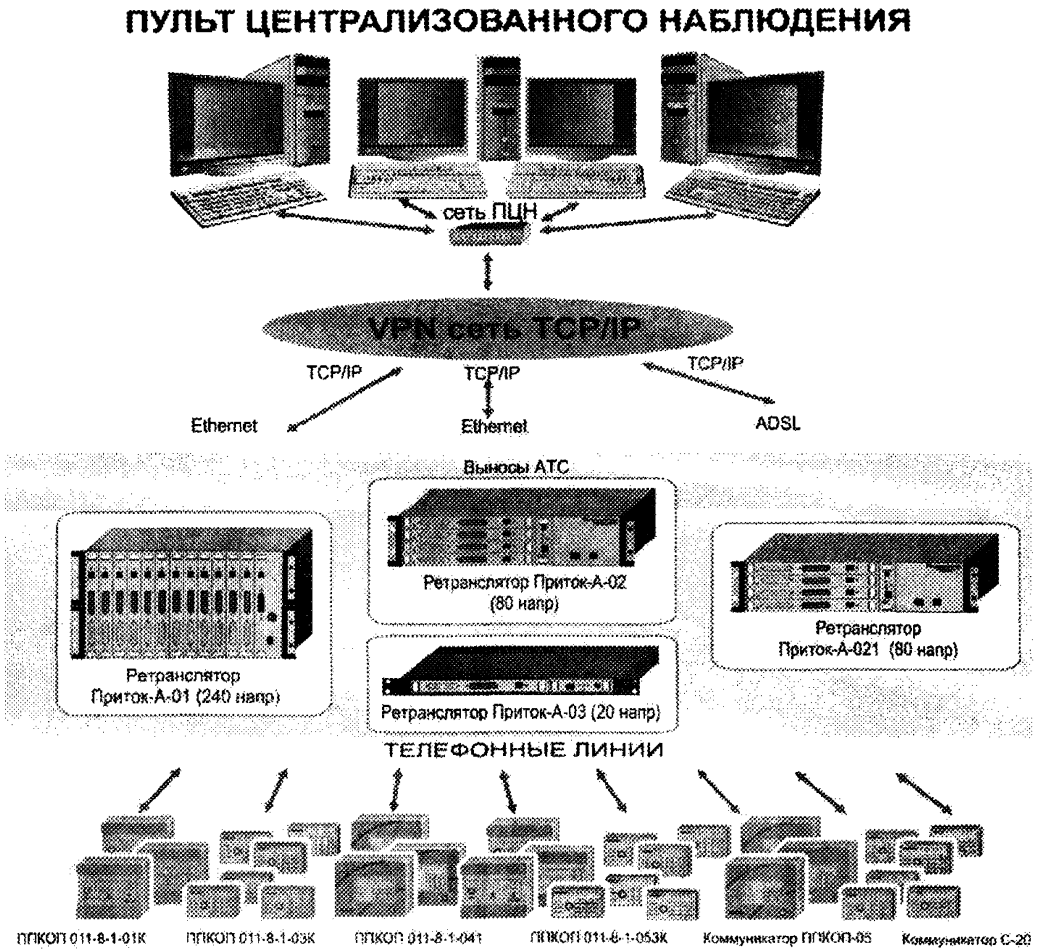


Рисунок Б.1 *- Организация охраны с применением ретранслятора Приток-А*

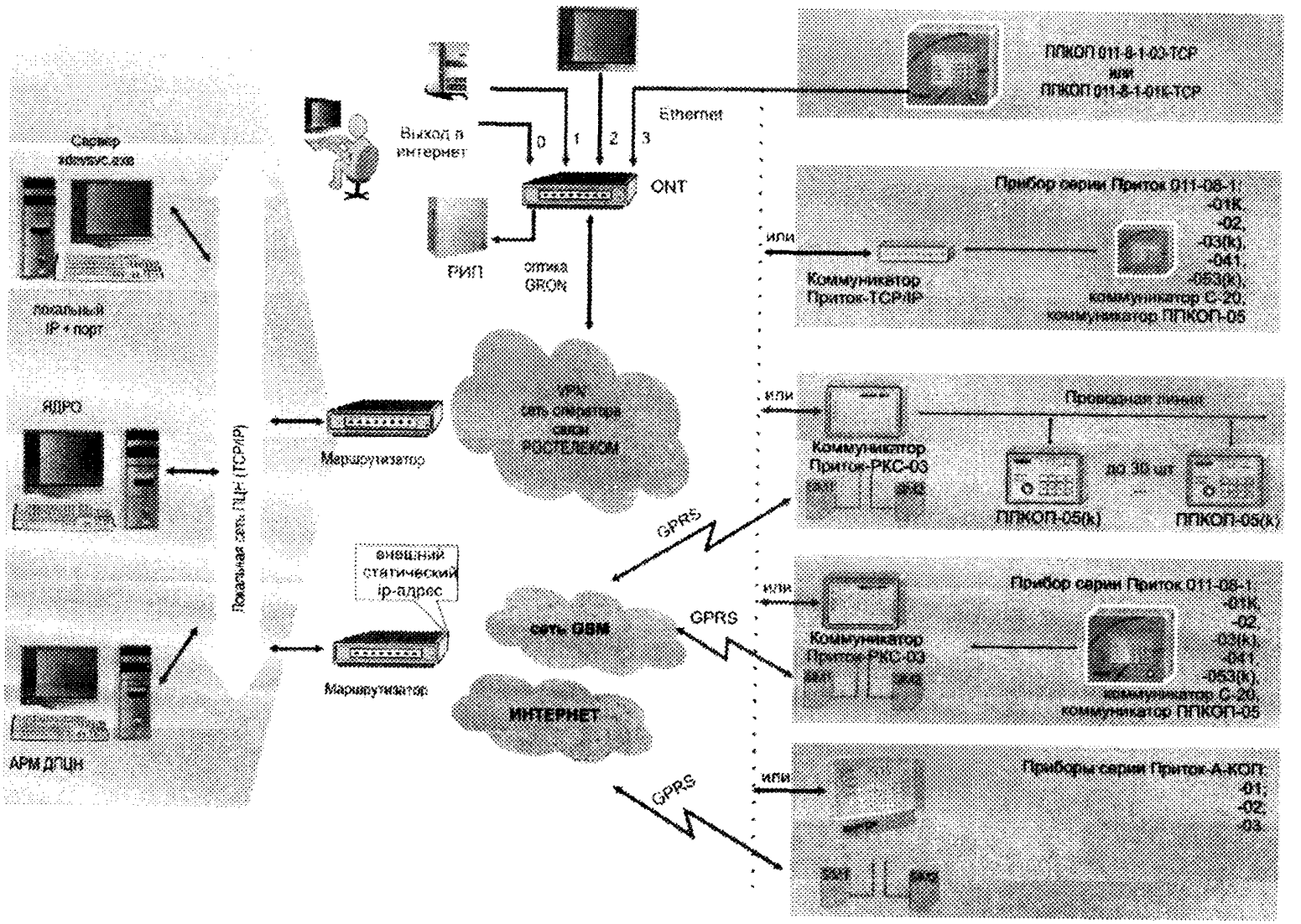


Рисунок Б.2 *- Организация централизованной охраны с использованием технологии GPON*

При организации централизованной охраны с использованием технологии GPON необходимо:

- оператору связи (провайдеру) организовать доступ с четвертого разъема ONT к сети ПЦН и предоставить клиенту услугу по передаче данных для целей охраны (стоимость услуги обычно не превышает стоимость по передаче данных для целей охраны по занятым телефонным линиям)
- VPN сеть на четвертом разъеме ONT;
- в сети ПЦН, в месте подключения сети оператора связи, установить маршрутизатор, обеспечивающий защиту и разделение сетей;
- ONT, установленный в квартире абонента, запитать от резервного источника питания;
- на ПЦН установить программное обеспечение АРМ Приток;
- к четвертому разъему ONT подключить один из вариантов:

▪ прибор приёмно-контрольный охранно-пожарный ППКОП 011-8-1-03-TCP Приток-А-4(8) или ППКОП-011-8-1-01К-TCP(8,16) Приток-А-4(8);

▪ Коммуникатор Приток-TCP/IP, а нему один из вариантов приборов:

1. ППКОП-011-8-1-01К;
2. ППКОП-011-8-1-02;
3. ППКОП-011-8-1-41;
4. ППКОП-011-8-1-03К;
5. ППКОП-011-8-1-053(к);
6. ППКОП-011-8-1-05(к) до 30 шт. или РПДУ-03;
7. Коммуникатор С-20;
8. Коммуникатор ППКОП-05, а к нему до 30 шт. ППКОП-011-8-1-05(к) или РПДУ-03;

▪ Коммуникатор Приток-РКС-03, а нему один из вариантов приборов:

1. ППКОП-011-8-1-01К;

2. ППКОП-011-8-1-02;
3. ППКОП-011-8-1-41;
4. ППКОП-011-8-1-03К;
5. ППКОП-011-8-1-053(к);
6. ППКОП-011-8-1-05(к) до 30 шт или РПДУ-03;
7. Коммуникатор С-20;
8. Коммуникатор ППКОП-05, а к нему до 30 шт. ППКОП-011-8-1-05(к) или РПДУ-03;

- Приборы серии Приток-А-КОП.

Выделенное подключение к Интернет.

Схема работы по «открытым» каналам Интернет может отличаться от схемы по технологии GPON. Основная причина - возможное нарушение связи при аварийных отключениях питающей городской сети 220 В. Провайдеры Интернет не устанавливают резервное питание на все узлы, участвующие в передаче данных. Поэтому, на период отключения Ethernet сети рекомендуется использовать приборы с встроенным сотовым терминалом в режиме GPRS. Выделенное подключение к Интернет на ПЦН также должно быть осуществлено через маршрутизатор, защищающий сеть ПЦН от нежелательного Интернет трафика. Более того, системой «Приток-А» предусмотрено возможность использования двух различных подключений ПЦН к Интернет через разных провайдеров. У абонента в этом случае может быть установлен:

1. Коммуникатор Приток-РКС-03, а нему один из вариантов приборов:
   - ППКОП-011-8-1-01К;
   - ППКОП-011-8-1-02;
   - ППКОП-011-8-1-41;
   - ППКОП-011-8-1-03К;
   - ППКОП-011-8-1-053(к);
   - ППКОП-011-8-1-05(к) до 30 шт или РПДУ-03;

– Коммуникатор С-20;

– Коммуникатор ППКОП-05, а к нему до 30 шт ППКОП-011-8-1-05(к) или РПДУ-03;

2. Приборы серии Приток-А-КОП

Эти устройства имеют в качестве основного канала связи сеть Ethernet и в качестве резервного два канала разных операторов GSM в режиме GPRS.

На рисунке Б.3 изображена локальная сеть ПЦН, подключенная через два маршрутизатора со статическими IP адресом к сети Интернет, используя два провайдера. На объекте или квартире установлен маршрутизатор, подключенный кабелем Ethernet через провайдера к сети Интернет. Провайдер для идентификации пользователя, как правило, использует протокол PPPoE, который может быть настроен и включен в маршрутизаторе. За маршрутизатором организована локальная сеть, в которой этот маршрутизатор является шлюзом для выхода в Интернет как домашнего компьютера, так и одного или нескольких приборов серии Приток.

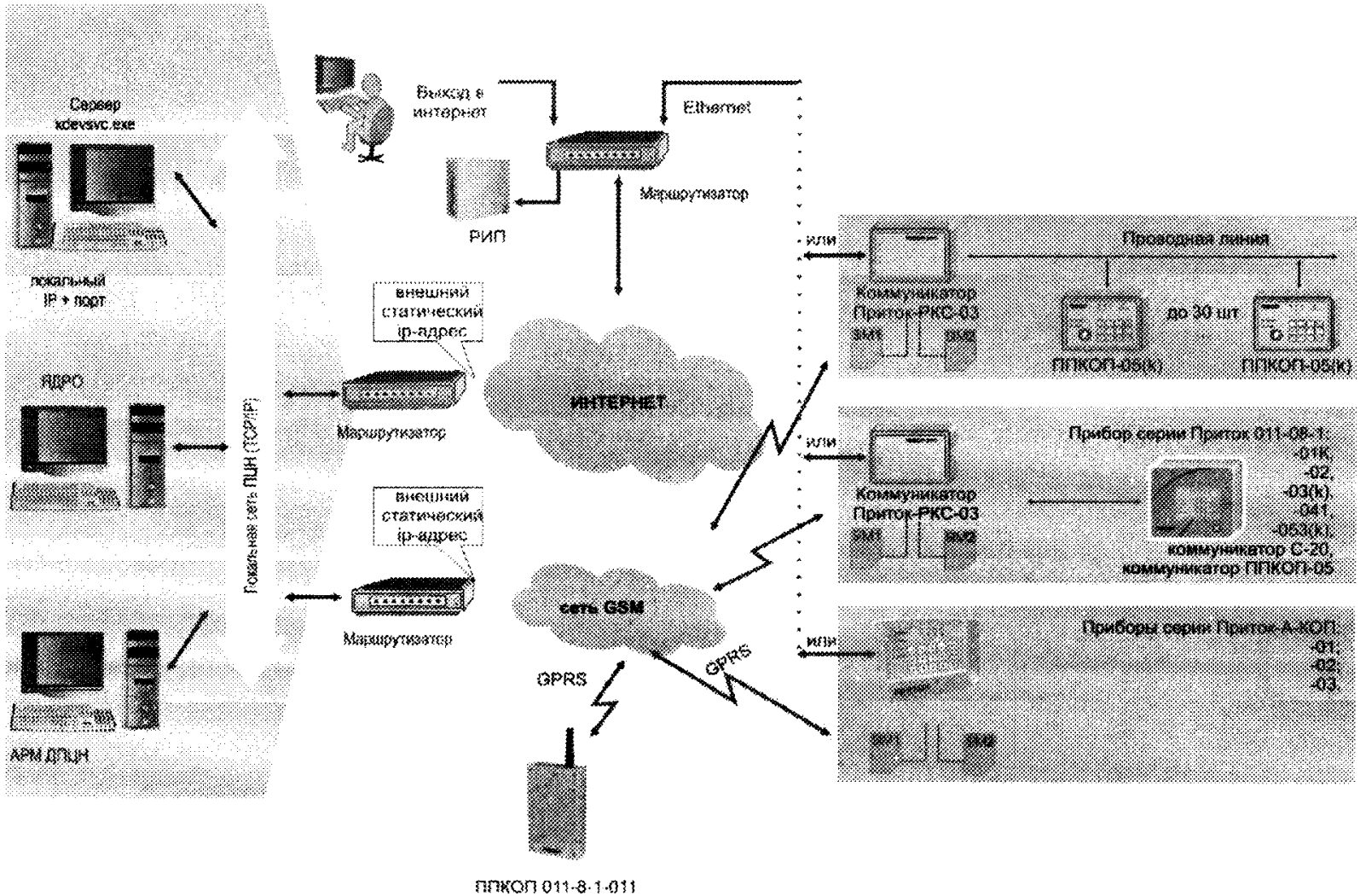


Рисунок Б.3 *- Работа системы «Прибор-А» по каналам Интернет и GSM*

Оборудование для организации централизованной охраны с использованием технологии GPON

Прибор приемно-контрольный охранно-пожарный ППКОП 011-8-1-03 ТСР

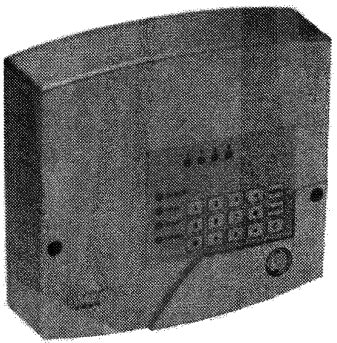


Рисунок Б.4 – Внешний вид прибора

Назначение

Прибор предназначен для организации охраны в составе «Автоматизированной системы охранно-пожарной сигнализации Приток-А» путем контроля состояния 4 шлейфов сигнализации через выделенное (постоянное) подключение к локальной сети или сети Интернет по протоколу UDP.

Особенности

- имеет 4 выхода типа «открытый коллектор» для подключения световых и звуковых оповещателей, два из которых могут контролировать исправность нагрузки (согласно требованиям НПБ для пожарных ШС);
- возможность постановки и снятия с охраны как одиночных ШС, так и групп ШС;
- возможность автономного взятия/снятия;

- для работы в автономном режиме включена возможность редактирования списка рабочих ключей для идентификации при помощи мастер-ключа.

Технические характеристики

- взятие под охрану и снятие с охраны осуществляется посредством ввода ИК доступа – при помощи ключей ТМ (Touch Memory), встроенной клавиатуры или внешней клавиатуры ППКОП.

Прибор имеет Ethernet-розетку для подключения к провайдеру сети Интернет.

- вход для подключения датчика отметки прибытия патруля.

- три выхода типа «открытый коллектор», предназначенных для подключения световых и звуковых оповещателей.

В корпусе прибора установлены:

основная плата прибора;

модуль связи МС-03, включающий в себя модуль TCP/IP-01 для работы по Ethernet;

плата индикации;

аккумулятор.

- программирование параметров типа ШС (охранный, охранный с возможностью пропуска, пожарный, тревожный), режимов работы внешних оповещателей .

- каждый прибор в локальной сети Ethernet должен иметь уникальный ip-адрес. Для установки ip-параметров используется программа wizArmConfig.exe .

- режим внутреннего тестирования и проверки работоспособности.

- электропитание прибора производится от сети переменного тока напряжением 220 (+10 -15%) или от встроенной аккумуляторной батареи.

Прибор приемно-контрольный охранно-пожарный ППКОП 011-8-1-01(к)-ТСР

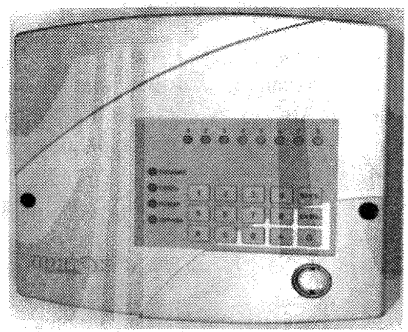


***Рисунок Б.5** – Внешний вид прибора*

Назначение

Прибор предназначен для организации охраны объектов (закрытых помещений) в системе «Приток-А» путем контроля состояния 8 ШС через выделенное (постоянное) подключение к локальной сети или сети Интернет по протоколу UDP.

Особенности:

имеет 4 выхода типа «открытый коллектор» для подключения световых и звуковых оповещателей, два из которых могут контролировать исправность нагрузки (согласно требованиям НПБ для пожарных ШС);

возможность постановки и снятия с охраны как одиночных ШС, так и групп ШС;

возможность автономного взятия/снятия;

для работы в автономном режиме включена возможность редактирования списка рабочих ключей для идентификации при помощи мастер-ключа.

Технические характеристики:

имеет 8 ШС;

в качестве канала связи используется сеть Интернет;

поддержка DHCP;

имеет 4 выхода типа «открытый коллектор» для подключения световых и звуковых оповещателей, два из которых могут контролировать исправность нагрузки;

возможность постановки и снятия с охраны как одиночных ШС, так и групп ШС;

возможность автономного взятия/снятия;

для работы в автономном режиме включена возможность редактирования списка рабочих ключей для идентификации при помощи мастер-ключа;

- электропитание прибора производится от сети переменного тока напряжением 220В или от встроенной аккумуляторной батареи емкостью 2,2 А*ч.

Прибор приемно-контрольный охранно-пожарный ППКОП 011-16-1-01(к)-ТСР

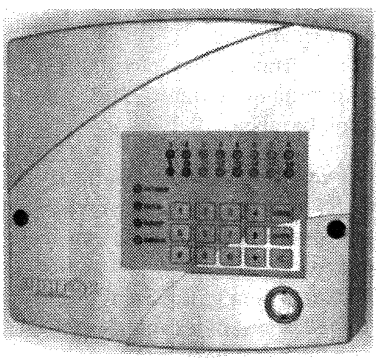


***Рисунок Б.6** – Внешний вид прибора*

Назначение

Прибор предназначен для организации охраны объектов (закрытых помещений) в системе «Приток-А» путем контроля состояния 16 ШС через выделенное (постоянное) подключение к локальной сети или сети Интернет по протоколу UDP.

Особенности:

- ПЦН и объект, на котором установлен прибор, должны иметь постоянное (выделенное) подключение к сети Интернет. Каждый прибор в локальной сети Ethernet должен иметь уникальный ip-адрес;
- программирование параметров типа ШС (охранный, охранный с возможностью пропуска, пожарный, тревожный), режимов работы внешних оповещателей;
- режим внутреннего тестирования и проверки работоспособности.
- взятие под охрану и снятие с охраны посредством персональных электронных идентификаторов – ключей ТМ, встроенной клавиатуры или внешней клавиатуры ППКОП. Прибор имеет Ethernet разъем для подключения к провайдеру сети Интернет.

Электропитание прибора производится от сети переменного тока напряжением 220В. или от встроенной аккумуляторной батареи.

Технические характеристики:

- 16 шлейфов сигнализации;
- в качестве канала связи используется сеть Интернет;
- поддержка DHCP;
- 4 выхода типа «открытый коллектор» для подключения световых и звуковых оповещателей, два из которых могут контролировать исправность нагрузки;
- возможность постановки и снятия с охраны как одиночных ШС, так и групп ШС;

- возможность автономного взятия/снятия;
- для работы в автономном режиме включена возможность редактирования списка рабочих ключей для идентификации при помощи мастер-ключа;
- наличие встроенного резервного источника питания.

Контроллер охранно-пожарный Приток-А-КОП-02

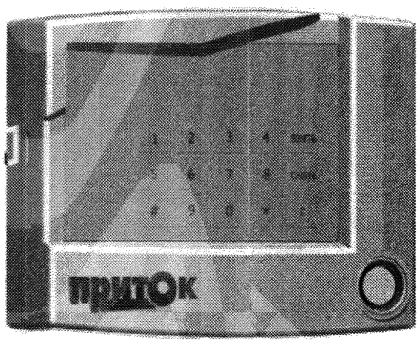


Рисунок Б.7 – Внешний вид прибора

Назначение

Контроллер охранно-пожарный Приток-А-КОП-02 предназначен для организации централизованной охраны объектов и квартир по современным каналам связи при работе в составе "Автоматизированной системы охранно-пожарной сигнализации Приток-А".

Особенности

- подключается к АРМ ПЦН по каналам Ethernet и GSM/GPRS . Каналы связи с сервером подключений – двунаправленные, с защитой от подмены контроллера и шифрованием;

- поддерживает совместную работу с Ethernet оборудованием, поддерживающим скорость 10mbs/half duplex;

- разработан для работы через сеть Интернет или VPN, например, через технологию GPON как основной канал связи, и сотового оператора как резервный, но допускается работа и только через GSM/GPRS (без подключения по Ethernet);

- питание осуществляется от внешнего резервированного источника питания 12В;

- охрана осуществляется путем контроля состояния четырех (или более, в случае использования расширителей) шлейфов сигнализации с включенными в них охранными и пожарными извещателями и передачи тревожных и пожарных извещений на АРМ ПЦН;

- имеет вход для подключения датчика отметки прибытия патруля;

- четыре программируемых выхода типа «открытый коллектор», предназначенных для подключения световых, звуковых оповещателей и любого пользовательского оборудования;

-взятие под охрану и снятие с охраны осуществляется посредством применения персональных электронных идентификаторов – ключей Touch Memory (в дальнейшем по тексту – ключ ТМ), встроенной клавиатуры (и)или внешней клавиатуры КОП.

Технические характеристики:

- информационная ёмкость (количество шлейфов сигнализации)
- время доставки тревожных извещений, с, не более
- скорость обмена по сети Ethernet, mbs
- типы шлейфов сигнализации
- количество внешних силовых ключей
- время технической готовности, с, не более

Коммуникатор резервного канала связи Приток-РКС-03 (GSM+TCP/IP)

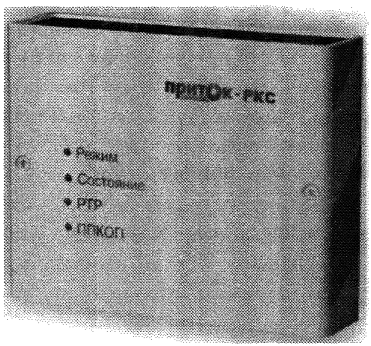


***Рисунок Б.8** – Внешний коммуникатора Приток-РКС-03*

Назначение

Коммуникатор резервного канала связи Приток-РКС-03 (GSM+TCP/IP) предназначен для организации двух резервных каналов связи по сети Ethernet и GSM для ППКОП при централизованной охране объектов и квартир в составе «Автоматизированной системы охранно-пожарной сигнализации Приток-А».

Особенности:

- канал связи между прибором и ретранслятором или коммуникатором TCP/IP

называется основным;

- два канала связи между АРМ ПЦН и коммуникатором РКС-03 называются резервными;

- из двух резервных каналов (Ethernet и GSM) приоритетным считается канал Ethernet;

- коммуникатор РКС-03 автоматически отслеживает работоспособность основного и приоритетного канала связи;

- коммуникатор РКС-03 подключается в разрыв линии связи между ППКОП и

ретранслятором или коммуникатором TCP/IP;

- в случае потери связи по основному каналу (обрыв, короткое замыкание, неисправность) коммуникатор РКС-03 автоматически переключается на приоритетный канал Ethernet, и только в случае ошибки переключается на GSM канал. Если во время работы по GSM каналу происходит восстановление приоритетного канала Ethernet, то коммуникатор РКС-03 переключается с GSM на Ethernet. При восстановлении линии связи коммуникатор РКС-03 возвращает управление РТР и переключается в режим слежения за работоспособностью основного канала.

Технические характеристики:

- количество sim-карт 2
- время доставки тревожных сообщений, с ..... 2 - 5
- тип встроенного модема GSM MC52i
- тип антенны GSM ..... Внутренняя
- шифрование данных AES128
- масса, не более, кг 0,3
- габаритные размеры, мм 150x100x40
- напряжение питания постоянного тока, В ..... 10,6 до 15
- ток потребления в дежурном режиме
  от источника постоянного тока, не более, мА 120
- режимы работы ..... GPRS/Ethernet

Типовые примеры организации централизованной охраны с помощью оборудования СПИ «Атлас-20» по сетям Ethernet

Организация работы оборудования СПИ «Атлас-20» по сетям Интернет.

На рисунке В.1 представлена типовая схема организации охраны – объектовое оборудование передает извещения по существующим «медным» телефонным линиям методом ВЧ-уплотнения (18 кГц). Связь станционного оборудования (ретрансляторов Р-112, Р-224, Р-448, Р-672 или блоков ретрансляторов) и ПЦО осуществляется посредством сети Интернет с резервированием по GSM каналу (data CSD).

В данной схеме задействованы помещения АТС, на которых устанавливаются ретрансляторы или блоки ретрансляторов. Емкость устанавливаемых ретрансляторов зависит от количества абонентских линий. Так, емкость блока ретранслятора составляет 20 линий (есть исполнение на 8 линий), емкость ретранслятора Р-112 – 112 линий и т.д.

Объектовое оборудование работает по телефонной линии методом ВЧ - уплотнения (18кГц). При этом имеется возможность подключения сторонних услуг, например Internet – через внешние DSL модемы (обязательным является работа в протоколе Annex B).

В этом случае, в качестве объектового оборудования могут быть использованы:

- УОО «Прима-3А»;
- ППКОП «Прима-4А»;
- ВОРС (внутриобъектовая радиосистема) Стрелец совместно с блоком высокочастотного уплотнения БВУ-02;
- ППКОП «Аккорд-3.00»;

- Концентратор объектовый (КО) с блоками объектовыми (БО).

Телефонные линии, идущие от объектов, могут либо непосредственно заходить на АТС, либо проходить через промежуточные кроссы в распределительных шкафах (РШ).

Для организации передачи извещений на ПЦО применяются устройства сопряжения:

- МУ-3 – модуль управления, встраиваемый в секции ретранслятора и позволяющий осуществлять подключение непосредственно к сети Интернет через стандартные сетевые коммутаторы (коммутаторы не входят в комплект поставки Атлас-20);

- дополнительное устройство сопряжения УС-10, необходимое для организации канала передачи данных по сети Интернет для блока ретранслятора.

Подключение устройства сопряжения УС-10 к блоку ретранслятора осуществляется посредством COM порта.

В обоих случаях, имеется возможность организации резервного канала передачи данных на ПЦО – по GSM каналу в режиме data CSD. Для этого используются внешние GSM терминалы.

Территориально аппаратура, находящаяся на АТС, может располагаться в любом сухом, отапливаемом и обслуживаемом помещении с наличием кросса. Основные требования к этому помещению:

- температура от +1°С до +55°С;

- наличие резервированных напряжений питания: 60 В (питание АТС), 220 В;

- наличие преобразующей аппаратуры Ethernet-ВОЛС;

- наличие физического места для размещения аппаратуры;

- должна быть предусмотрена возможность выноса в неэкранируемую часть помещения GSM-антенн от GSM-терминалов.

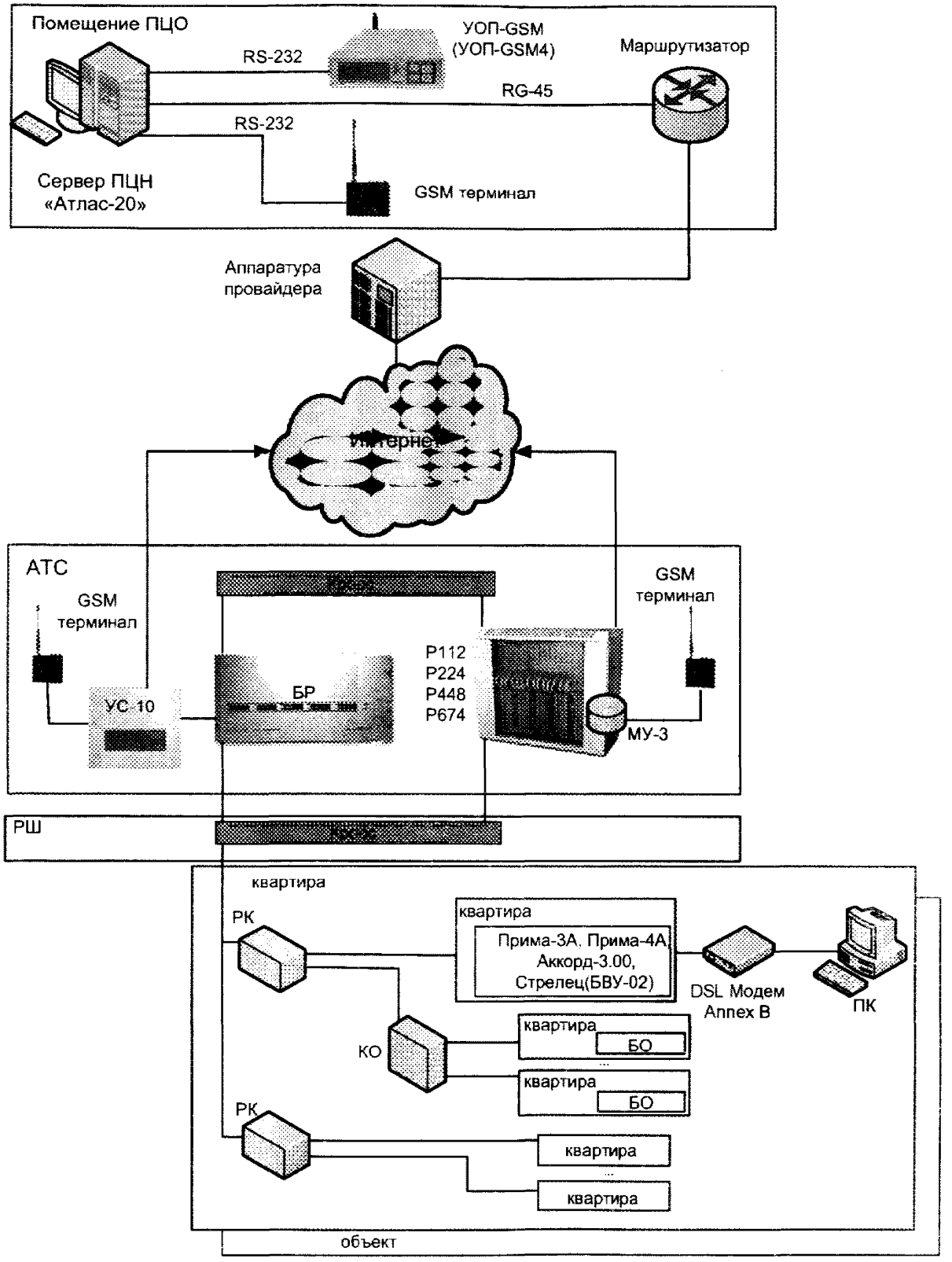


Рисунок В.1 *- Типовая схема организации охраны при использовании технологии FTTC*

Для устройства сопряжения УС-10 и модуля управления МУ-3, используемых для работы по сети Ethernet, обязательным условием является наличие публичного статического IP-адреса. Сеть, которую образуют между собой устройство сопряжения УС-10 (модуль управления МУ-3) и ПЦН может быть локальной или с выходом в Интернет. Вариант локальной сети (например, при использовании пары DSL модемов) является предпочтительным, поскольку лучше защищен от внешнего вмешательства. SIM – карты, устанавливаемые в GSM-терминалы, должны быть с подключенным сервисом DATA CSD.

На ПЦО в этом случае необходимо установить следующее оборудование.

Персональный компьютер, который будет являться сервером аппаратуры, подключенный к сети Интернет. Обязательным условием должен быть фиксированный IP адрес. На этом компьютере запускается сервер Аппаратуры «Сетевой». Подключение компьютера в сеть Интернет осуществляется посредством сетевого маршрутизатора, который не является элементом «Атлас-20» и не входит в комплект поставки.

Для приема извещений по GSM каналу необходимо подключить к компьютеру внешний GSM терминал (подключение осуществляется через COM-порт).

В случае необходимости организации сетевой структуры программного обеспечения все остальные компьютеры должны подключаться к серверному компьютеру, на котором запущен сервер «Сетевой».

На рисунке В.2 показана схема, которая применяется в случае невозможности установки аппаратуры на АТС. Ввиду ограниченного свободного места, установка ретрансляторов (Р-112-674) в РШ невозможна. Единственным решением является размещение блоков ретранслятора малой емкости.

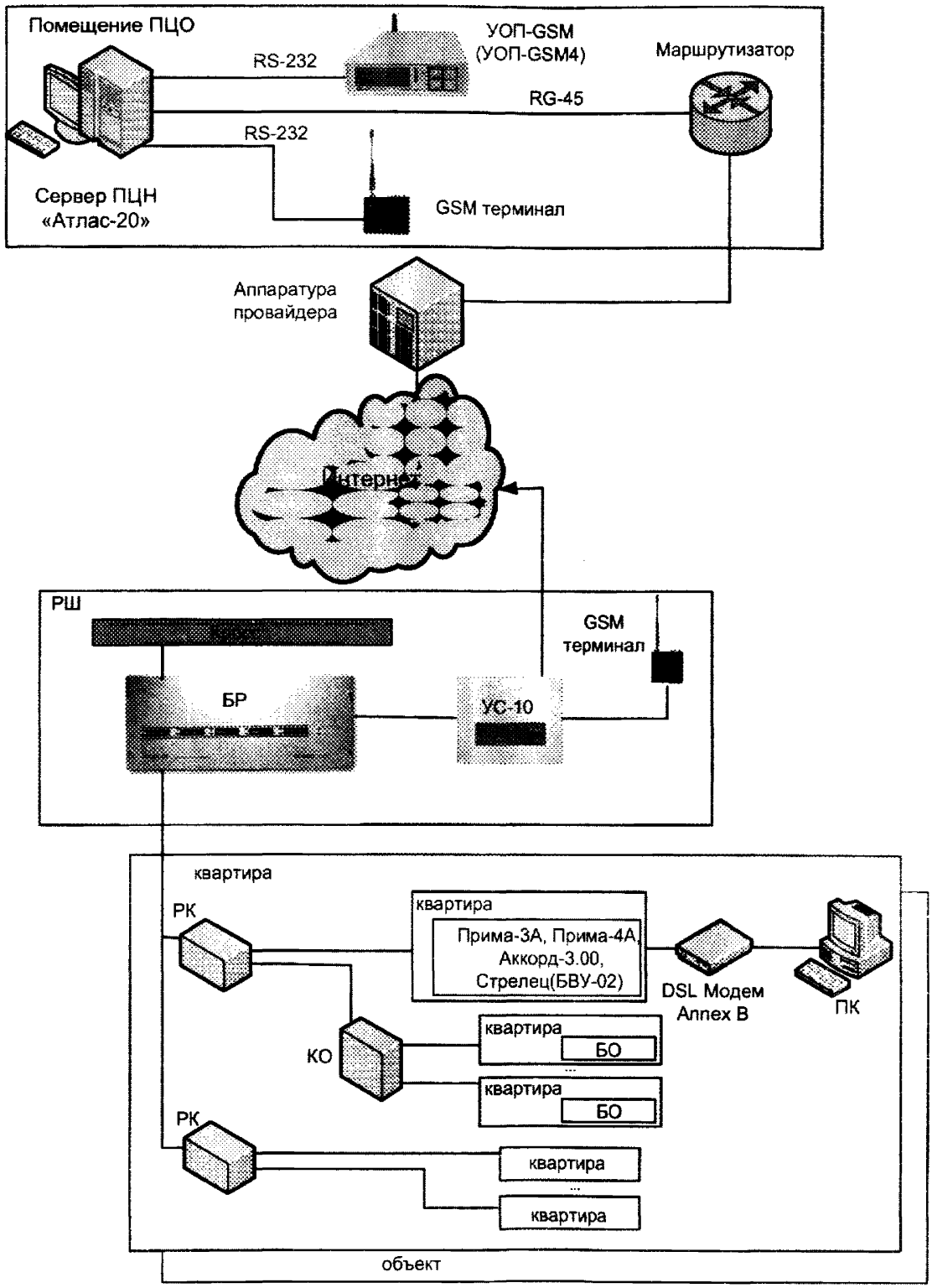


***Рисунок В.2** - Установка ретрансляторов «малой» емкости при использовании технологии FTTB*

При такой схеме необходимо обеспечить свободное место в РШ, и обеспечить устройства (устройство сопряжения УС-10, внешний GSM терминал и блок ретранслятора) гарантированным питанием от внешних источников.

Вывод извещений на ПЦО в этом случае также осуществляется посредством устройства сопряжения УС-10 и внешнего GSM терминала.

На рисунке В.3 приведена схема, при которой полностью исключен промежуточный вариант установки ретрансляторов в помещениях АТС или РШ.

Передача извещений осуществляется по следующим каналам:

1) **Ethernet / Internet.** В качестве объектовых устройств применяют:

- ИСБ Стрелец-Интеграл и УОО «Тандем IP-И»;
- ППКОП «Тандем-1».

2) **GSM.** В качестве объектовых устройств применяют:

- ИСБ Стрелец-Интеграл и УОО «Тандем IP-И»;
- ППКОП «Тандем-1»;
- ППКОП «Тандем-2М».

3) **GPRS.** В качестве объектовых устройств применяют:

- ИСБ Стрелец-Интеграл и УОО «Тандем IP-И»;
- ППКОП «Тандем-1».

Объектовое оборудование, работающее по сетям Интернет должно подключаться посредством промежуточного маршрутизатора (DSL модема), так как сами приборы не имеют возможности автоматической авторизации в сети. Данные модемы не являются элементами «Атлас-20» и не входят в комплект поставки.

Аппаратура, устанавливаемая между квартирным (объектовым) маршрутизатором и провайдером не подлежит точному описанию, поскольку принадлежит интернет-провайдеру и может отличаться как по техническим характеристикам, так и по цене. Обычно, это несколько многопортовых Switch-ей, выходящих на еще один маршрутизатор.

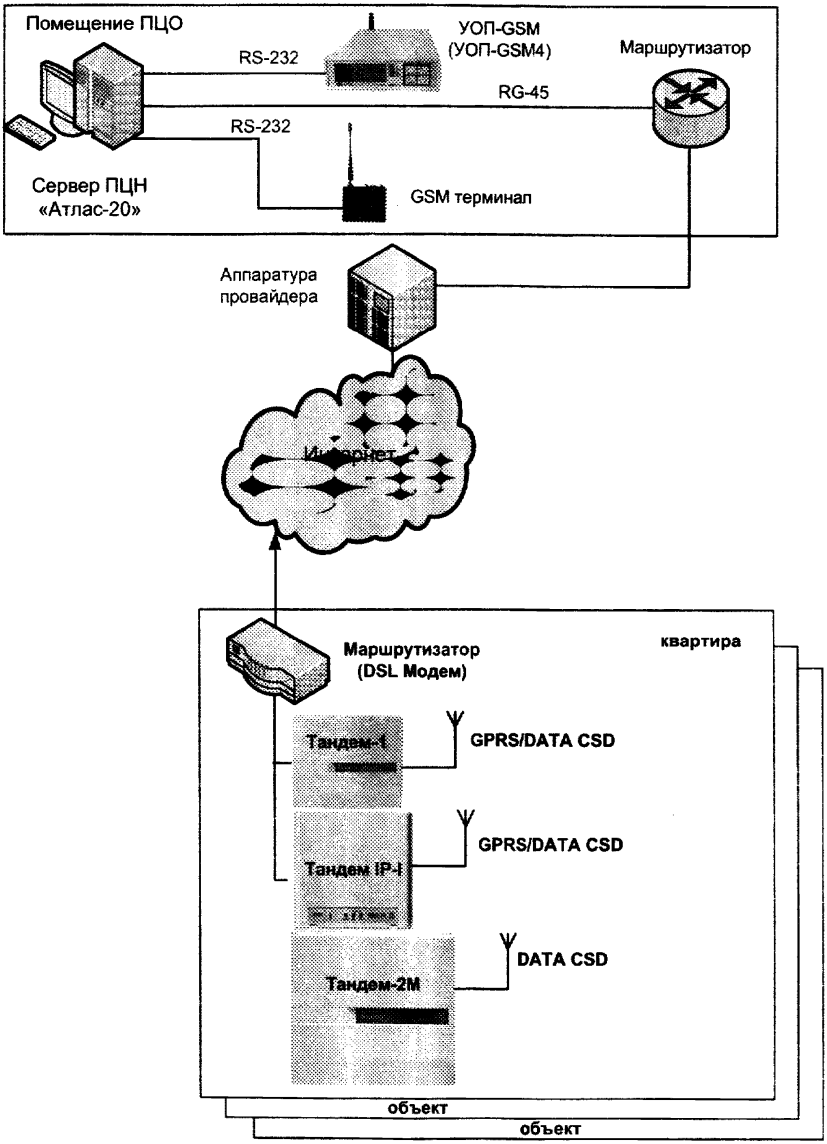


Рисунок В.3 *- Работа объектовых устройств по сетям Интернет и GSM при использовании технологии FTTH*

А данный маршрутизатор, через преобразователь «Ethernet-ВОЛС» выходит наружу здания, и ВОЛС идет к провайдеру (через промежуточные «собирательные» узлы).

Кроме того, необходим прямой доступ этих устройств в сеть без использования Proxy-серверов.

Следует помнить, что при использовании доступа в Интернет по технологии ADSL многие провайдеры закрывают доступ ко всем портам, оставляя открытыми на PROXY-сервере только общеизвестные порты - 80, 8080, 21, 25. Выход прибором в Интернет по данным портам может быть проблематичным. Для решения данной проблемы необходимо приобретение у провайдера статического IP- адреса со всеми открытыми портами.

Для приема извещений на ПЦО необходимо установить следующее оборудование.

Персональный компьютер, который будет являться сервером аппаратуры, подключенный к сети Интернет. Обязательным условием является наличие публичного статического IP адреса на ПК ПЦО. На этом компьютере запускается сервер Аппаратуры «Стрелец-Универсальный». Подключение компьютера в сеть Интернет осуществляется посредством сетевого маршрутизатора, который не является элементом «Атлас-20» и не входит в комплект поставки.

Пультовое оборудование УОП-GSM4, подключаемое к ПК посредством COM порта требует резервированного источника питания ~220 В.

В случае необходимости организации сетевой структуры программного обеспечения, все остальные компьютеры должны подключаться к серверному компьютеру, на котором запущен сервер «Стрелец-Универсальный».

Для объектового оборудования достаточно иметь динамический IP-адрес.

Оборудование для организации централизованной охраны с использованием технологии GPON

Варианты построения систем с использованием прибора Тандем IP-И при использовании технологии FTTH иллюстрируется на рисунках В.4 – В.7.

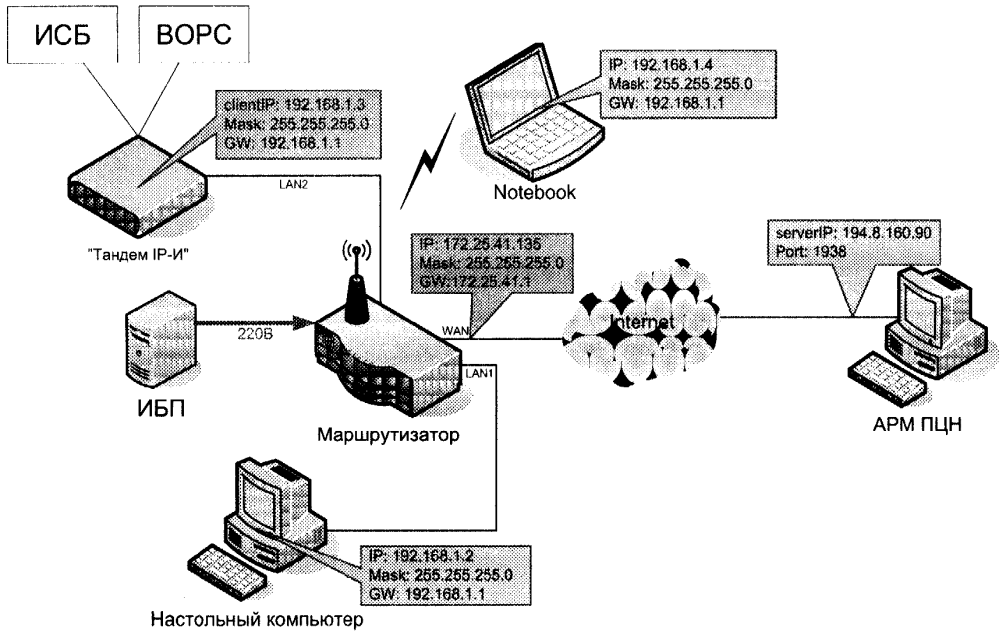


Рисунок В.4 *- Выход в Интернет по выделенной линии через маршрутизатор*

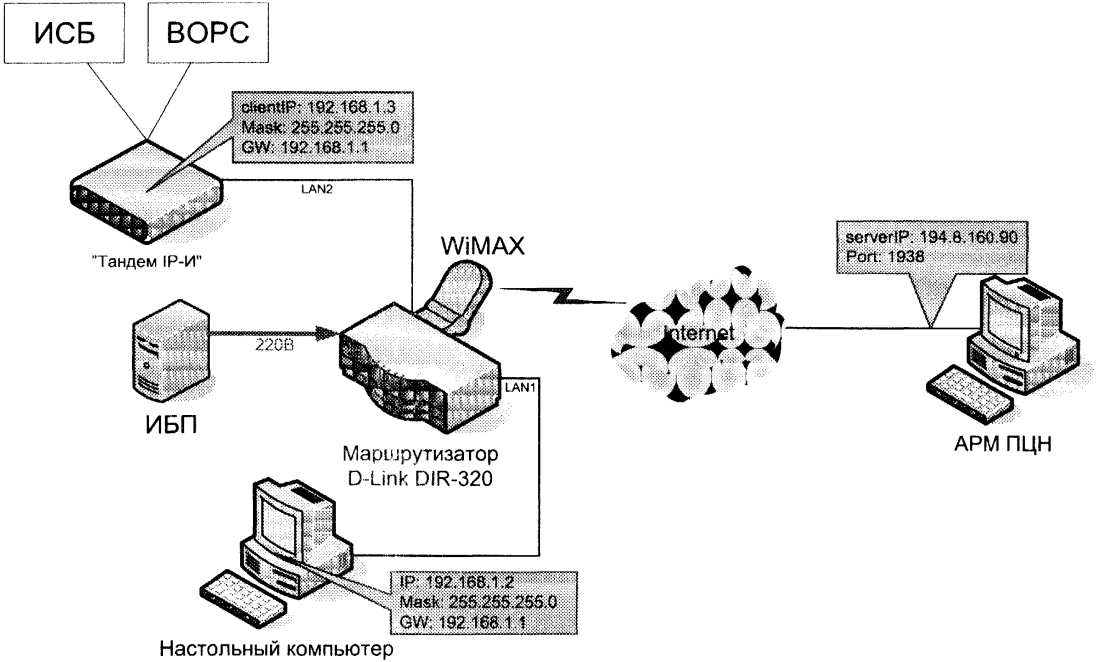


Рисунок В.5 *- Выход в Интернет по технологии WiMAX через маршрутизатор*

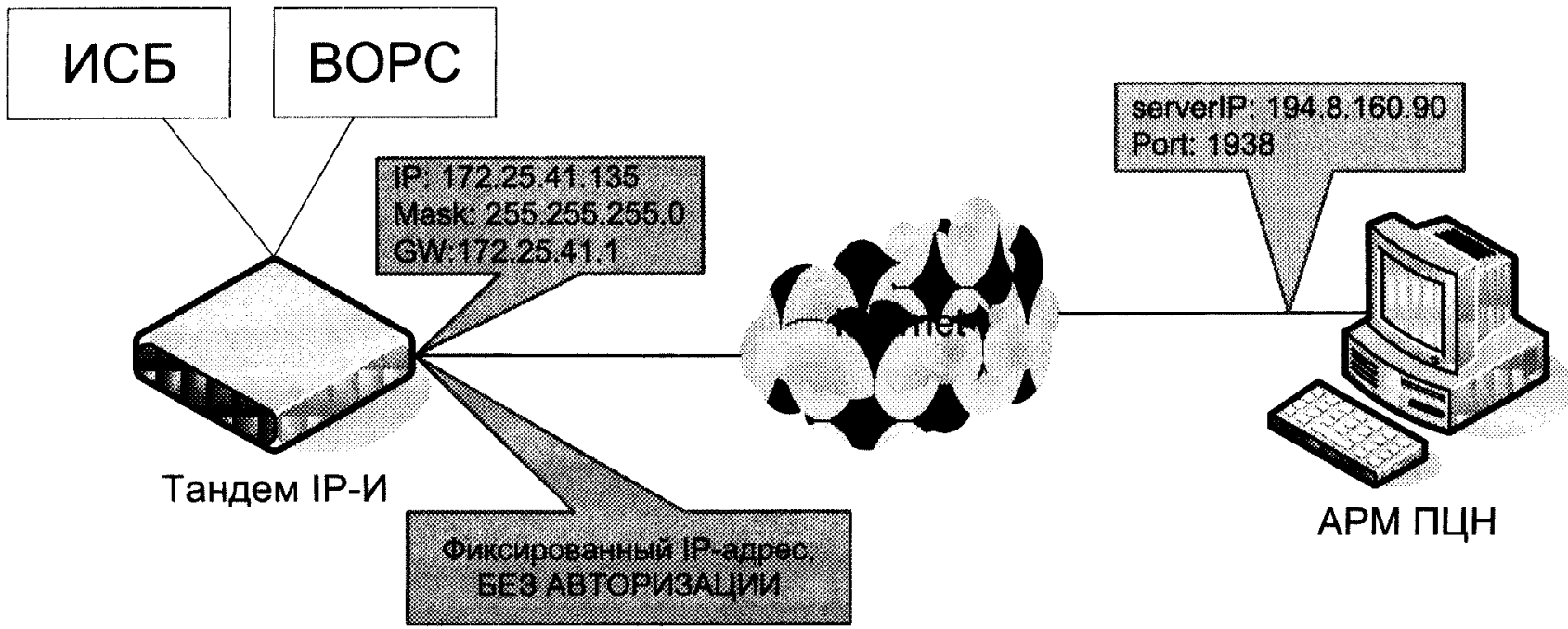


Рисунок В.6 *- Прямое подключение прибора к Интернету с использованием фиксированного IP-адреса и без авторизации*

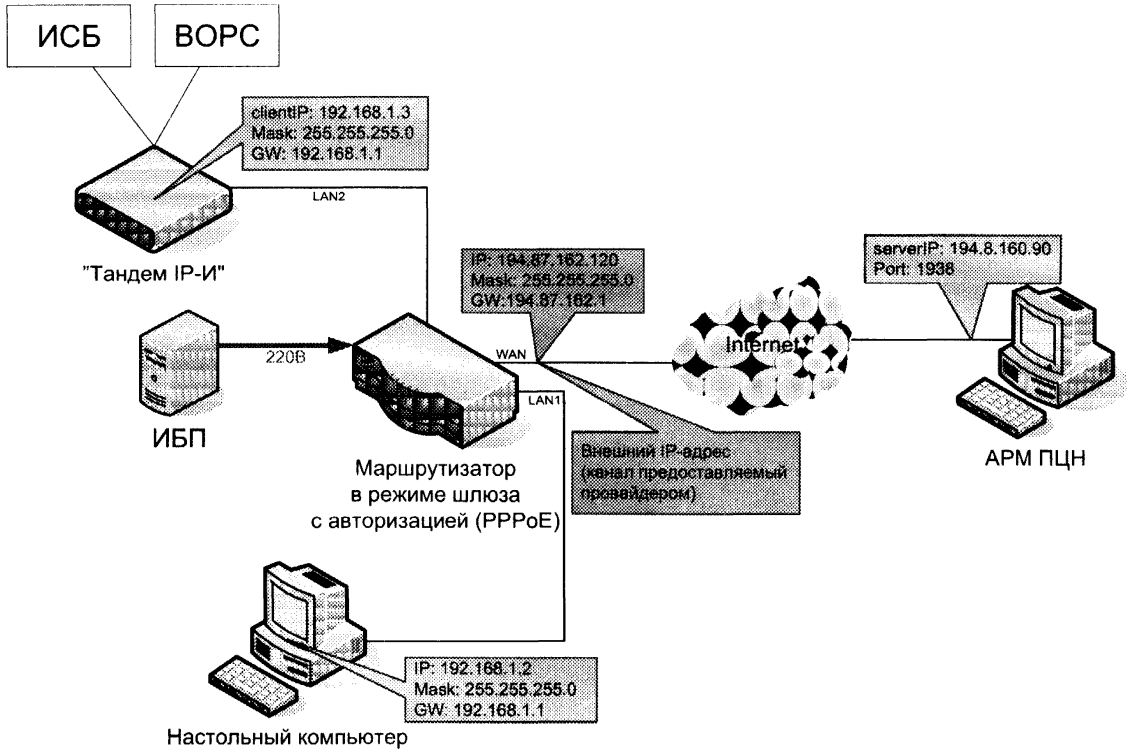


Рисунок В.7 *- Выход в Интернет через маршрутизатор с настроенной авторизацией (PPPoE)*

Отличие технологии xPON от технологии FFTH не значительно. Технология xPON – это непосредственное подведение ВОЛС к квартире (объекту), где за счет интернет-провайдера ставится (на правах аренды) преобразователь ONT (Optical Network Terminal) «ВОЛС-Ethernet» (например, Huawei HG850). Охранные приборы (Тандем-1, Тандем IP-И) подключаются к свободным портам RJ-45 данного преобразователя при помощи UTP-кабеля категории 5.

Прибор приемно-контрольный охранно-пожарный «Тандем-1»

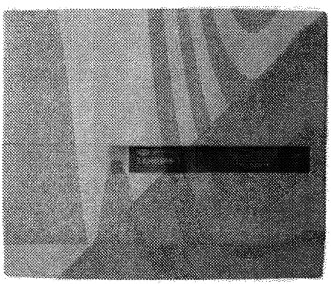


***Рисунок В.8** – Внешний вид прибора*

Назначение

Прибор предназначен для контроля состояния шлейфов сигнализации, передачи извещений о состоянии охранно-пожарной сигнализации на пульты централизованного наблюдения или сотовые телефоны пользователей. Передача извещений осуществляется по сети Ethernet и по GSM-каналу.

Особенности

- режим внутреннего тестирования и проверки работоспособности.

- электропитание прибора производится от сети переменного тока напряжением 220 (+10 -15%) или от встроенной аккумуляторной батареи.

Технические характеристики

- 4 шлейфа сигнализации (охранный, пожарный или тревожный);
- управление с помощью пульта (ПУ-ТМ) или ключей Touch Memory (16 пользователей, поддержка ключей DS1990A и с защитой от копирования DS1971);
- 2 реле и 1 выход «Открытый коллектор» с программируемой логикой работы;
- память на 8 телефонных номеров для SMS-сообщений.

Прибор передает извещения в протоколах:

- по GSM каналу: Data-CSD; GPRS; SMS сообщения (в том числе управление); звонок с тональными сигналами.
- по сети Ethernet: IP ver.4; DHCP.
- напряжение питания -220 В.
- встроенный аккумулятор - 2,2 Ач.

Устройство оконечное объектовое «Тандем IP-И»

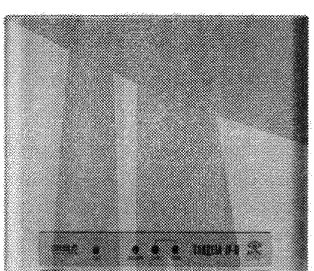


***Рисунок В.9** – Внешний вид прибора*

Назначение

Устройство оконечное объектовое "Тандем IP-И" предназначено для контроля состояния четырех входов подключения объектового оборудования посредством релейных входов, для передачи извещений от внутриобъектовой

охранной радиоканальной системы ВОРС «Стрелец», для передачи извещений от оборудования интегрированной системы безопасности «Стрелец-Интеграл"» (далее - ИСБ) на пульт централизованного наблюдения.

Особенности

- сменный модуль сетевого интерфейса S2 (стандарт ANSI/EIA/CEA –709.1 EN14908, ISO/IEC 14908, скорость – 78 кбит/с, длина линии – до 2,7 км);
- съемный модуль сетевого интерфейса Ethernet 10BaseT/100BaseTx (W5100);
- встроенный GSM-модем с поддержкой протоколов передачи данных GPRS, DATA CSD и SMS-сервиса;
- работа GSM-модема с двумя SIM-картами с тактикой резервирования сотовых операторов;
- порт RS-232 для подключения оборудования ВОРС «Стрелец»;
- входы контроля основного и резервного питания.

Технические характеристики

- интерфейс S2 (LON) для подключения к ИСБ «Стрелец-Интеграл»;
- интерфейс RS-232 для подключения к ВОРС «Стрелец»;
- 4 входа для подключения других устройств/приборов с релейными выходами.
- память на 8 телефонных номеров для SMS-сообщений;
- режим эмуляции УОО-GSM-С1.

Прибор передает извещения в протоколах:

- по GSM каналу: Data-CSD; GPRS; SMS сообщения (с ВОРС «Стрелец»); - звонок с тональными сигналами.
- по сети Ethernet: IP ver.4; DHCP.
- напряжение питания -12 В.

ПРИЛОЖЕНИЕ Г

Организация централизованной охраны с помощью оборудования СПИ «Юпитер» по сетям Ethernet

По назначению оборудование СПИ «Юпитер», допускающее работу с использованием цифровых сетей, подразделяется на две группы:

- устройства, используемые для адаптации к цифровым сетям ранее выпускавшегося оборудования, не имеющего в своем составе интерфейсов подключения к IP-сети;
- устройства изначально ориентированные на работу с цифровыми IP-сетями.

Первая группа представлена линейкой конверторов, позволяющих подключить к IP-сети как оборудование приемного комплекта (конверторы TCP/IP-RS232, TCP/IP-RS485), так и объектовое оборудование, использующее телефонные линии (конверторы «18 кГц-Ethernet», «18 кГц-GPRS»).

Вторая группа представлена, для приемного комплекта, модификацией КПЦО (коммутатора пульта централизованной охраны) для установки в шкаф 19" (конвертор включен в состав блока).

Объектовые приборы второй группы:

ППКОП «Юпитер» 4GSM ..... - подключение с использованием GPRS

ГК РИО с ИМ-Ethernet..... - подключение с использованием Ethernet

ГК РИО с ИМ-GSM ..... - подключение с использованием GPRS

ГК РИО с ИМ-Ethernet и ИМ-GSM..... - подключение с использованием Ethernet и GPRS

ГК РИО с ИМ-GSM ..... - подключение с использованием GPRS

ПОИСК с ИМ-Ethernet..... - подключение с использованием Ethernet
ПОИСК с ИМ-GSM ..... - подключение с использованием GPRS
ППКОП «Юпитер» 24К с ИМ-Ethernet..... - подключение с использованием Ethernet
ППКОП «Юпитер» 24К с ИМ-GSM ..... - подключение с использованием GPRS
РИО-Т/РИО-5Т..... - подключение с использованием Ethernet
ППКОП «Юпитер» 4/8/16 IP/GPRS..... - подключение с использованием Ethernet и GPRS

1. Подключение оборудования приемного комплекта.

Оборудование приемного комплекта размещается в телефонных узлах (квартальных или домовых выносах), куда сводятся традиционные телефонные линии, поступающие от охраняемых объектов.

Вне зависимости от типа предполагаемого подключения к опорной сети (ADSL, FTTC, FTTB), оборудование приемного комплекта имеет дело с Ethernet-подключением.

Тип оборудования, используемого для формирования Ethernet-интерфейса, зависит от телефонного оператора (тип используемого оптического волокна, задействованные протоколы, применяемая линейка оборудования и т.д.)

При использовании ADSL для организации Ethernet-подключения задействуются ресурсы оборудования выноса (платы DSLAM) ориентированного на обслуживание абонентов. Отдельная ячейка DSLAM программируется для подключения к IP/VPN-сети. Для формирования Ethernet-интерфейса используется ADSL-модем, предоставляемый, как правило, телефонным оператором.

Варианты подключения приемного комплекта разнятся только объемом телефонных линий требующих контроля, что определяет состав используемого оборудования.

1.2 Подключение приемного комплекта на АТС

При размещении на районных АТС задействуется следующее оборудование, представленное в таблице Г.1.

***Таблица Г.1** – Количество и перечень оборудования устанавливаемого на АТС*

Оборудование	Назначение	Кол-во
КПЦО 19" (1)	Объединение информационных потоков от более чем 16-и УТ	1
УТ 19"	Контроль объектового оборудования, подключаемого по телефонным линиям	1 на 20 линий
Шкаф 19"	Монтажный конструктив для установки оборудования приемного комплекта, в зависимости от ситуации может использоваться шкаф на 7/12 или 16 УТ	По числу УТ
Кросс-рамки (2)	Используются для подключения абонентских и станционных линий внутри шкафа.	1 на 2 УТ

Примечания:

1) Если число УТ (устройств трансляции) на АТС не превышает шестнадцати, то АТС может рассматриваться как квартальный вынос, и использовать КПЦО не требуется;

2) При необходимости шкафы на 12/16 УТ могут быть использованы для размещения 24/32-х УТ, при условии установки дополнительных кросс рамок и наличия доступа к задней двери шкафа.

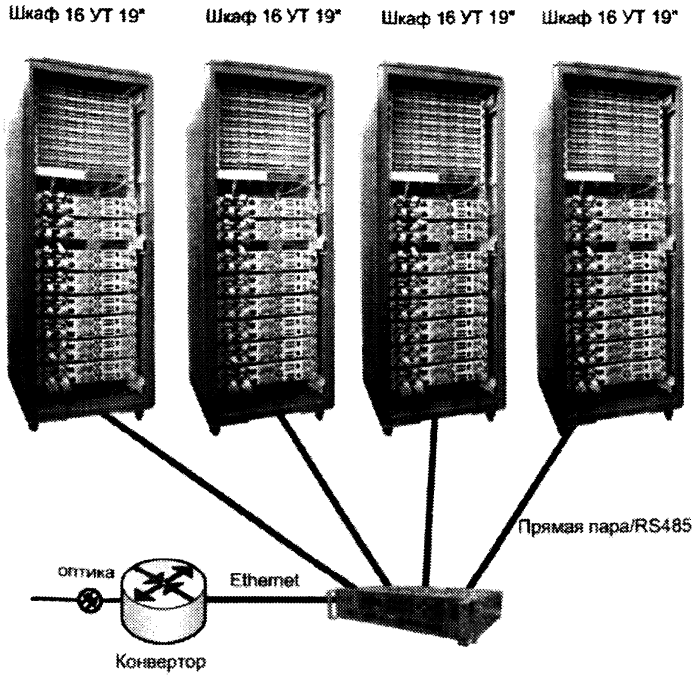


***Рисунок Г.4** - Подключение оборудования приемного комплекта на АТС*

1.2 Подключение приемного комплекта на квартальных выносах

При формировании приемных комплектов квартальных и домовых вносов приходится, дополнительно к традиционным, решать задачу обеспечения оборудования приемного комплекта гарантированным питанием. Это связано с тем, что на выносах, как правило, предоставляется

только возможность подключения к сети 220 В, при этом данное подключение не защищено от кратковременных отключений. При размещении на районных АТС данная проблема, как правило, не стоит, так как имеется возможность получения гарантированного питания станционного типа.

Для решения данной задачи комплект оборудования приемного комплекта может быть доукомплектован источниками бесперебойного питания РБП-54/2.5. Использование данного блока позволяет решить проблему резервированного питания оптических преобразователей и модемов, так как источник также предоставляет резервированное питания 12 В (см. рисунки Г.5, Г.6).

При размещении на квартальных выносах задействуется следующее оборудование, представленное в таблице Г.2.

***Таблица Г.2** – Количество и перечень оборудования устанавливаемого на выносах*

Оборудование	Назначение	Кол-во
УТ 19"	Контроль объектового оборудования, подключаемого по телефонным линиям	1 на 20 линий
TCP/IP-RS232	Преобразование сигналов из Ethernet в RS-232	1
Шкаф 19"	Монтажный конструктив для установки оборудования приемного комплекта, в зависимости от ситуации может использоваться шкаф на 7/12 или 16 УТ	По числу УТ
РБП-54/2.5	Обеспечение бесперебойного питания оборудования приемного комплекта	1

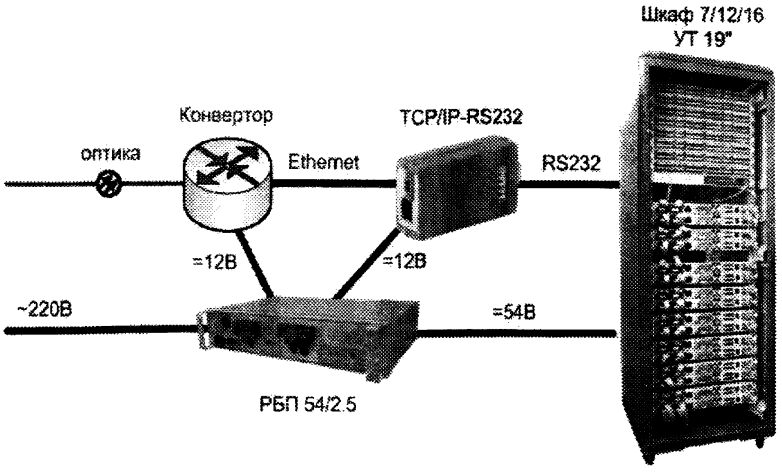


***Рисунок Г.5** - Подключение оборудования приемного комплекта на квартальном выносе.*

1.3 Подключение приемного комплекта на квартальных выносах

Размещение оборудования приемного комплекта в домовых выносах характеризуется, как правило, отсутствием возможности установки отдельного шкафа для монтажа охранного оборудования (при наличии возможности установки шкафа подключение аналогично случаю использования квартального выноса, см. выше п. 2.2).

Число абонентских линий, требующих контроля, на домовом выносе относительно невелико, что позволяет арендовать место для установки охранного оборудования в шкафу оператора связи.

При заказе места в телекоммуникационном шкафу следует использовать информацию из таблицы Г.3.

Таблица Г.3 *– Размеры оборудования устанавливаемого на выносах*

№	Прибор	Размер по высоте
1	УТ 19"	1U
2	Кросс рамки (одна на 2 УТ)	1U
3	РБП 54/2.5	2U
4	Соединительные кабели (на каждые 2 УТ)	1/3 U

При размещении на квартальных выносах задействуется оборудование, представленное в таблице Г.4.

Таблица Г.4 *– Перечень оборудования устанавливаемого на выносах*

Оборудование	Назначение	Кол-во
УТ 19"	Контроль объектового оборудования, подключаемого по телефонным линиям	1 на 20 линий
TCP/IP-RS232	Преобразование сигналов из Ethernet в RS-232	1
Кросс-рамки	Используются для подключения абонентских и станционных линий внутри шкафа.	1 на 2 УТ
РБП-54/2.5	Обеспечение бесперебойного питания оборудования приемного комплекта	1

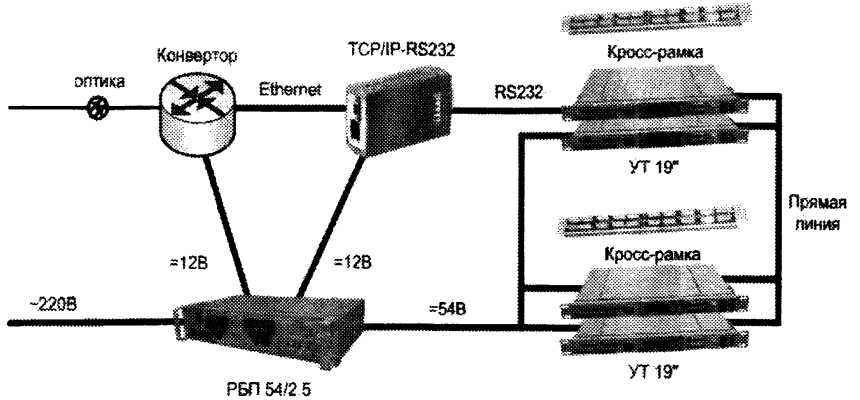


***Рисунок Г.6** - Подключение оборудования приемного комплекта на домовом выносе*

2. Подключение объектового оборудования

При подключении объектового оборудования для подключения опорной сети используется интерфейс Ethernet. Способ организации Ethernet-подключения на объекте не имеет значения, основным критерием является постоянство подключения и доступность пульта при посылке IP-пакетов.

Особенности функционирования оборудования на охраняемом объекте требуют выполнения следующих дополнительных требований, предъявляемых к телекоммуникационному оборудованию:

• Так как для организации подключения используется активное оборудование, то для него следует обеспечить наличие бесперебойного питание. Это становится особенно актуально при использовании xPON -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 12 В, что позволит использовать источник питания охранного прибора.

• Необходимо ограничить доступ к активному оборудованию, размещая его в защищенных от проникновения шкафах, оборудованных датчиками вскрытия.

• Необходимо ограничить доступ пользователей к настройкам активного оборудования.

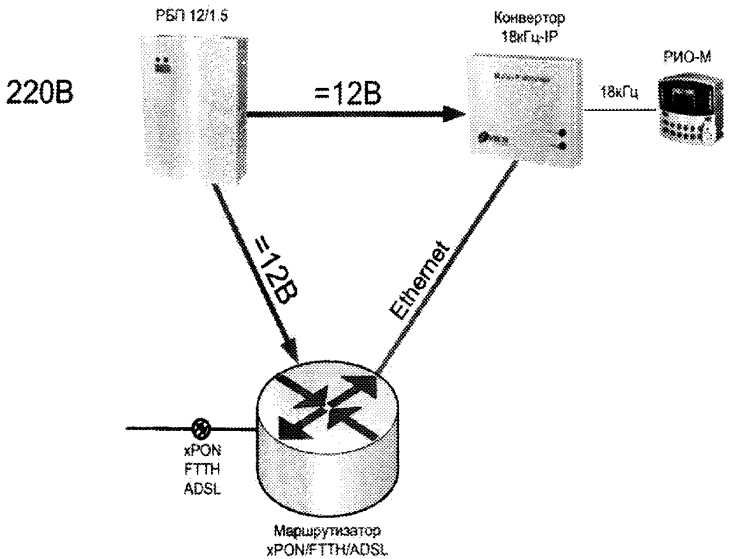


***Рисунок Г.7** - Подключение оборудования (с использованием внешнего источника питания).*

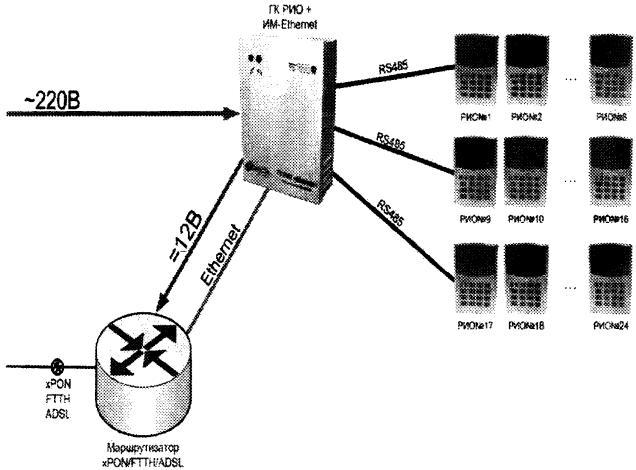


***Рисунок Г.8** - Подключение оборудования (с использованием встроенного источника питания).*

3. Экономические затраты на одно абонентское подключение

Расчет экономических затрат строится на основе данных из таблицы Г.5, приведенной ниже (розничные цены оборудования по состоянию на 01.11.2011 года). В таблице представлено оборудование СПИ «Юпитер», используемое для подключения охраняемых объектов по IP-сетям. Выбор объектового оборудования зависит от специфики объекта и не относится к выбранному каналу подключения.

В таблице Г.6 представлены затраты на охранное оборудование в пересчете на один охраняемый объект содержит расчет пяти вариантов организации охраны. Цены указаны розничные, могу быть использованы как ориентир при сравнении схем подключения, при закупке по госзаказу действуют специальные цены.

Таблица Г.5.

№	Наименование	Цена (руб.)
1	КПЦО «Юпитер» 19"	22163
2	УТ «Юпитер» 19"	52492
3	Монтажный шкаф 16 УТ	98670
4	Монтажный шкаф 12 УТ	72864
5	Монтажный шкаф 7 УТ	30360
6	Конвертор TCP/IP-RS232	11901
7	Кросс-рамка	6300
8	РБП 54/2.5	27096
8	РБП 12/1.5	1640
9	Конвертор 18кГц-IP	6831
10	ИМ-Ethernet	5313

***Таблица Г.6** – Стоимость оборудования на один охраняемый объект.*

№	Вариант	Стоимость на одно направление
1	Подключение приемного комплекта на АТС (1280 абонентских линий): - 2 шкафа на 16 УТ - 64 УТ 19" с установкой в каждый шкаф по 32 УТ - 16 дополнительных кросс-рамок - КПЦО 19"	2875 руб.
2	Подключение приемного комплекта на квартальном выносе (320 абонентских линий): - 1 шкаф на 16 УТ - 16 УТ 19" - конвертор TCP/IP-RS232 - блок питания РБП 54/2.5	3055 руб

Продолжение таблицы Г.6

3	Подключение приемного комплекта на домовом выносе (80 абонентских линий): - 4 УТ 19" - 2 кросс-рамки - конвертор TCP/IP-RS232 - блок питания РБП 54/2.5	3270 руб
4	Подключение объектового комплекта к опорной сети с использованием конвертора 18 кГц-IP: - конвертор 18 кГц-IP - блок питания РБП 12/1.5	8471 руб
5	Подключение объектового комплекта к опорной сети с использованием ИМ-Ethernet - ИМ-Ethernet	5313 руб

4. Приборы СПИ «Юпитер», использующие оптические линии связи

Для использования с оптическими линиями связи (в том числе GPON) предназначена линейка оборудования, использующего для связи с пультом Ethernet-канал.

Также, для обеспечения возможности перевода на Ethernet оборудования, работающего с телефонными линиями на частоте 18кГц («Юпитер», «Фобос-3») выпускается конвертор 18кГц-IP, позволяющий модернизировать имеющиеся объекты без выполнения монтажных работ.

В таблице Г.7 приведены характеристики оборудования, использующего для связи с пультом Ethernet-канал.

Все приборы используют для связи с пультом единый протокол. Выпускаемые приборы имеют сертификаты соответствия.

***Таблица Г.7** – Оборудование, использующее для связи с пультом Ethernet-канал*

№	Наименование	Описание
1	ГК РИО с ИМ-Ethernet	Групповой концентратор 24-х РИО (3 шлейфа каждый), встроенный РИП
2	Конвертор 18кГц-IP	Преобразователь интерфейса 18кГц для передачи на пульт по IP-каналам. Позволяет переключать на Ethernet проводные устройства «Юпитер», использующие 18кГц (АК «Юпитер», УОО «Юпитер», РИО-М, ППКОП «Юпитер 5П»)
3	Конвертор 18кГц-IP v.2	Преобразователь интерфейса 18кГц для передачи на пульт по IP-каналам. Позволяет переключать на Ethernet как проводные устройства Юпитер»,так и проводные устройства «Фобос-3» (УО-3К, Сигнал ВК4, УО-1А, УО-1Р, УО-2Р, УО-2А)
4	РИО-Т	Объектовый прибор на 3 шлейфа, связывающийсяс пультом по Ethernet. Допускает расширение при помощи 7-и РИО
5	УОО-5 IP	Объектовый прибор на 5 шлейфов, связывающийся с пультом по Ethernet. Допускает расширение при помощи 7-и РИО, встроенный РИП
6	ППКОП «Юпитер» 4 IP/GPRS	Объектовый охранно-пожарный прибор на 4 шлейфа, связывающийся с пультом по Ethernet. Имеет возможность резервирования по GPRS, встроенный РИП
7	ППКОП «Юпитер» 8 IP/GPRS	Объектовый охранно-пожарный прибор на 8 шлейфов, связывающийся с пультом по Ethernet, встроенный РИП. Имеет возможность резервирования по GPRS

Групповой концентратор РИО «Юпитер»

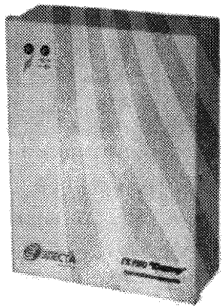


Рисунок Г.9 – Внешний вид прибора

Назначение

Групповой концентратор РИО «Юпитер» (в дальнейшем - ГК РИО) предназначен для связи группы индивидуальных ответчиков с расширенными функциональными возможностями (в дальнейшем - РИО) с ПЦН системы передачи извещений «Юпитер» по существующим каналам связи, включающим в себя телефонные сети, сети Ethernet и сети GSM (CSD и GPRS).

Особенности

- для обеспечения интерфейсов связи используются интерфейсные модули ИМ-ПП18, ИМ-Ethernet или ИМ-GSM, устанавливаемые в штатные места на плате ГК РИО. Интерфейсы можно использовать парами 18 кГц /GSM, Ethernet /GSM.

- для передачи извещений по телефонным линиям и с помощью CSD используется протокол «Юпитер», для остальных интерфейсов - ПК4;

- для конфигурирования ГК РИО используется интерфейс USB;

- для подключения ответчиков используется интерфейс RS485. Имеется 3 линии для подключения ответчиков. Общее количество подключённых к ГК РИО ответчиков не более 24-х;

- имеются встроенные часы реального времени с календарём. Предусмотрена синхронизация времени с компьютером посредством USB.

Технические характеристики

- информационная ёмкость (максимальное количество подключаемых РИО) – 24;

- нформативность (количество видов извещений) -26. Виды извещений: «Тревога», «Взлом», «Невзятие», «Тихая» тревога», «Подбор кода», «Неисправность», «Подмена», «Запуск», «Восстановление», «Закрытие корпуса», «Начало обучения», «Конец обучения», «Сброс памяти тревог», «Вход», «Взятие», «Снятие», «Патруль», «Резервное питание», «Восстановление питания», «Ответ на опрос», «Ответ на перевзятие», «Номер версии устройства», «Имитостойкость», «Невзятие шлейфа», «Восстановление аккумулятора», «Потеря аккумулятора».

- при использовании интерфейсного модуля ИМ-ПП18 ГК РИО передаёт информацию в телефонную линию в виде кодированного сигнала частотой (18±0,18) кГц;

- при использовании интерфейсного модуля ИМ-Ethernet ГК РИО передаёт информацию для ПЦН в сеть Ethernet. Для обмена используется протокол ПК4 с поддержкой шифрования данных. Для передачи через сети Ethernet данные ПК4 инкапсулируются протоколом UDP стека TCP/IP. Поддерживается DHCP (автоматическое получение настроек TCP/IP у шлюза);

- при использовании интерфейсного модуля ИМ-GSM данные на пульт могут передаваться через сети GSM с помощью CSD соединения или с помощью GPRS;

- питание от сети переменного тока 220 В. Так же предусмотрено использование свинцово-кислотного аккумулятора 12В в целях резервирования питания.

- потребляемая ГК РИО мощность - не более 10 ВА;

- максимальное количество РИО, питающихся от внутреннего источника ГК РИО – 3;

- габаритные размеры 180 х 235 х 80 мм.

Конвертор 18 кГц – IP «Юпитер»

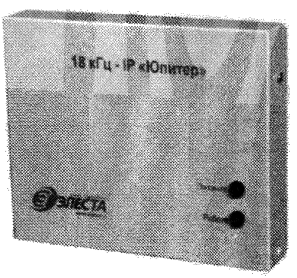


***Рисунок Г.9** – Внешний вид прибора*

Назначение

Конвертор 18 кГц-IP «Юпитер» предназначен для передачи информации от объектовых устройств СПИ «Юпитер», использующих занятые или выделенные телефонные линии, непосредственно на ПЦН, применяя канал IP.

Особенности

- прибор преобразует интерфейс 18 кГц «Юпитер» в интерфейс IP;

- прибор поддерживается программным обеспечением АРМ ДПУ «Юпитер», начиная с версии 7.3.107;

- конфигурирование прибора осуществляется с помощью «Программы конфигурирования «Конвертор 18 кГц-

Ethernet». Программу конфигурирования необходимо скачать с сайта производителя: gost.e-ecolog.ru

- предусмотрены передача сообщений на ПЦН при переходе источника питания (РБП) на резервное питание, а также при не санкционированном вскрытии корпуса.

Технические характеристики

- напряжение передатчика на частоте (18±0.18) кГц) на сопротивлении нагрузки (180±4,0) Ом ..... (0.45±0.05)В
- чувствительность приёмника на частоте (18±0.18) кГц ..... от 20 до 30 мВ
-ток потребления, не более ..... 300 мА
- напряжение питания ..... 9…15 В
- габаритные размеры, не более ..... 175х140х40 мм

Типовые примеры организации централизованной охраны с помощью оборудования СПИ «Заря» по сетям Ethernet

В случае обслуживания выносом АТС одного здания можно использовать аппаратуру «Заря-ГК-IP-М1», соединенную цифровым каналом с ПЦН и четырех проводным кабелем с абонентской аппаратурой «Заря-ИО», «Заря-УСИ2», размещаемой непосредственно в квартирах. На практике такое решение используется очень редко, так как сложно согласовать установку, питание и кроссировку охранной аппаратуры в помещении или шкафе микро-выноса, а высокая стоимость цифрового канала делает нерентабельной охрану 1-10 квартир. Оптимальным решением в этом случае обычно является использование аппаратуры «Заря-УО-IP-GPRS» или «Заря-ГК-IP-М2», взаимодействующих с ПЦН через сеть операторов GSM в режиме пакетной передачи. В упрощенном виде схема подключения приведена на рисунке Д.1.

В случае реализации на объекте PON-технологии к специально выделенному для охраны порту ONT стандартным кабелем (как патч-корд для локальной сети) подключается либо ПКП «Заря-УО-IP», обеспечивающий охрану одной квартиры, либо «Заря-ГК-IP-М1» с цепочкой «Заря-ИО», «Заря-УСИ2», обеспечивающих охрану до 50 квартир. На рисунке Д.1 приведена упрощенная структурная схема подключения охранной аппаратуры и АРМ ДПУ с использованием PON и сети сотовой связи GSM. Существенной особенностью предлагаемого технического решения является межсетевой экран – маршрутизатор (Firewall-Router) на основе операционной системы Linux. Он обеспечивает одновременно объединение подсистем на основе PON-VPN и GPRS на одном ПЦН, в том числе и на одном АРМ ДПУ, защиту от несанкционированных воздействий из чужих сетей, управление переключением между основным и резервными каналами, отслеживание состояние и, при необходимости, инициализацию GSM(GPRS/EDGE/3G) модемов.

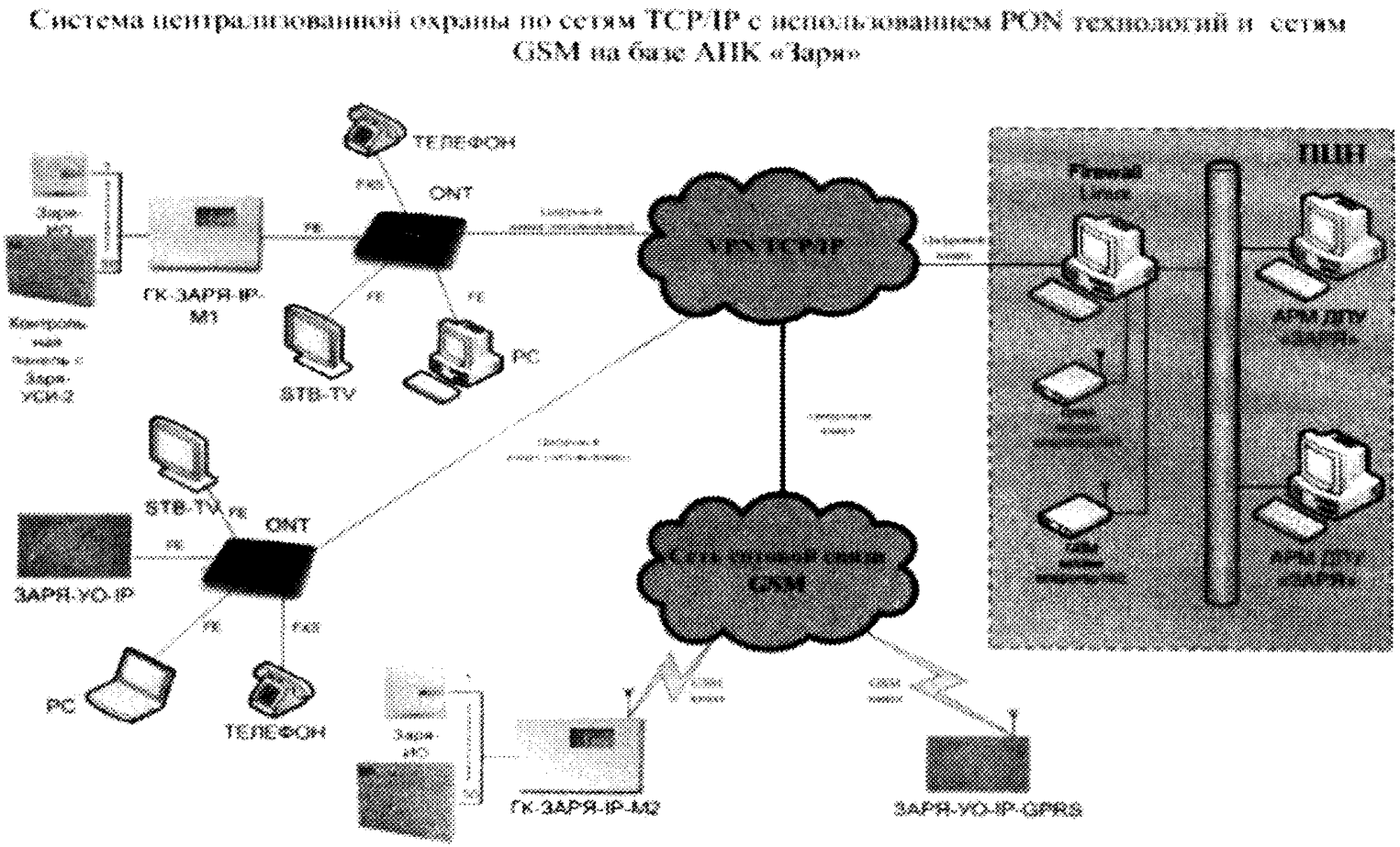


***Рисунок Д.1** - Структурная схема подключения с использованием PON*

Оборудование для организации централизованной охраны с использованием технологии GPON

Прибор приемно-контрольный охранно-пожарный Заря–УО-IP

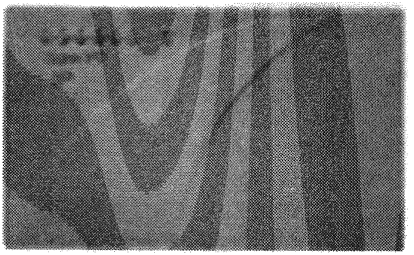


Рисунок Д.2 – Внешний вид прибора

Назначение

Прибор приемно-контрольный охранно-пожарный «Заря-УО-IP» (далее – ППКОП) предназначен для передачи сообщений на ПЦН об изменении состояния охранных и пожарных шлейфов сигнализации.

***Таблица Д.1** – Состав ППКОП «Заря-УО-IP»*

Обозначение	Наименование	Кол-во (шт.)	Примечание
ТАВР.425513.006	Блок приемно-контрольный охранно-пожарный «Заря -УО-IP»	1	-
ГЛТЦ.437241.307- 01	Устройство ВУПС		1 Общее количество устройств (в любой их комбинации) не более двух.
ГЛТЦ.437241.307- 03	Устройство ВУПС-К		

	Электронный кодовый ключ типа «Touch Memory»		2 Вариант комплектации по согласованию с заказчиком. Только для ВУПС. Количество в соответствии с договором с заказчиком.
	Резистор С2-23-0,25-12 кОм±10%	6	

Обозначения:

ВУПС - выносное устройство постановки/снятия с электронными ключами типа

ВУПС-К - выносное устройство постановки/снятия клавиатурного типа.

Особенности

- программное обеспечение и протокол обмена сообщениями ППКОП с пультовой ПЭВМ совместимы с программным обеспечением и протоколом обмена, применяемыми в системах передачи извещений «Заря» и «Заря-К» для связи с ПЦН, что позволяет осуществлять совместную работу ППКОП с СПИ;
- управление работой ППКОП производится централизованно от ПЦН, размещённого в ПЦО;
- связь между ПЦН и ППКОП двухсторонняя. ПЦН каждые несколько секунд опрашивает все ППКОП, что гарантирует обнаружение нарушения связи;
- обмен данными защищен шифрацией с псевдослучайными ключами;
- подключение к сети Интернет через постоянный канал. При этом внешний IP-адрес для ППКОП не нужен.

Возможно использование Интернет-канала любого вида, например:

- оптоволокно;
- DSL;
- радио Ethernet;
- телевизионный кабель.

Технические характеристики

- время готовности к работе – не более 2 с;
- информативность – 20;
- количество контролируемых ШС – шесть, каждый из которых может быть охранным или пожарным;
- количество одновременно подключаемых к Блоку приемно-контрольному охранно-пожарному «Заря–УО-IP» устройств ВУПС и ВУПС-К, в любом их сочетании, не более двух;
- количество электронных ключей или секретных кодов пользователей, программируемых в один ППКОП – от 1 до 70;
- питание от внешнего бесперебойного источника питания постоянного тока с номинальным напряжением 12 В.

Прибор приемно-контрольный охранно-пожарный «Заря-УО-IP-GPRS»



***Рисунок Д.4** – Внешний вид прибора*

Назначение

Прибор приемно-контрольный охранно-пожарный «Заря-УО-IP-GPRS» (далее – ППКОП) предназначен для передачи сообщений на ПЦН об изменении состояния охранных и пожарных шлейфов сигнализации охраняемого объекта через корпоративную сеть TCP/IP, Интернет или GPRS модем на ПЦН и обратно.

Таблица Г.2 - Состав ППКОП «Заря-УО-IP-GPRS»

Обозначение	Наименование	Кол-во (шт.)	Примечание
ТАВР.425513.008	Блок приемно-контрольный охранно-пожарный «Заря - УО-IP-GPRS»	1	С антенной «ANTENNA 915±12 MHz», подключенной к модулю Q2686H
ГЛТЦ.437241.307-01	Устройство ВУПС		1 Общее количество устройств (в любой их комбинации) не более двух. 2 Вариант комплектации по согласованию с заказчиком.
ГЛТЦ.437241.307-03	Устройство ВУПС-К		
	Электронный кодовый ключ типа «Touch Memory»		Только для ВУПС. Количество в соответствии с договором с заказчиком.
	Резистор С2-23-0,25-12 кОм±10%	6	

Особенности

- программное обеспечение и протокол обмена сообщениями ППКОП с ПЦН совместимы с программным обеспечением и протоколом обмена, применяемыми в системах передачи извещений «Заря» и «Заря-К» для связи с ПЦН, что позволяет осуществлять совместную работу ППКОП с СПИ;
- управление работой ППКОП производится централизованно от ПЦН, размещаемой в ПЦО;
- обмен сообщениями между ППКОП и ПЦН ведется с использованием сети сотовой связи в формате протокола TCP/IP;
- связь между ПЦН и ППКОП двухсторонняя. ПЦН каждые несколько секунд опрашивает все ППКОП, что гарантирует обнаружение нарушения связи;
- обмен данными защищен шифрацией с псевдослучайными ключами;

- программно задаваемая с ПЦН, разнообразная тактика взятия под охрану и снятия с охраны объектов;

- операционная система, установленная на ПЦН, должна быть не ниже Windows-2000;

- SIM карта, устанавливаемая в ППКОП «Заря-УО-IP-GPRS», должна быть открытой для оказания услуг сотового оператора на весь отрезок времени, планируемый для охраны объекта, обеспечивать выход в Сеть в режиме GPRS и содержать в себе данные о фиксированном IP адресе ПЦН в Сети.

Технические характеристики

- время готовности к работе – не более 2 с;

- информативность – двадцать;

- количество контролируемых ШС – шесть, каждый из которых может быть охранным или пожарным;

- количество одновременно подключаемых к Блоку приемно-контрольному охранно-пожарному «Заря–УО-IP» устройств ВУПС и ВУПС-К, в любом их сочетании, не более двух;

- количество электронных ключей или секретных кодов пользователей, программируемых в один ППКОП – от 1 до 70;

- питание от внешнего бесперебойного источника питания постоянного тока с номинальным напряжением 12 В.

Устройство оконечное объектовое «Заря-ГК-IP-М1»

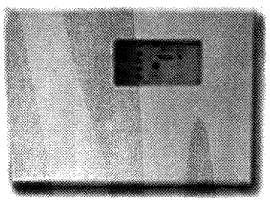


***Рисунок Д.5** – Внешний вид прибора*

Назначение

Устройство оконечное объектовое «Заря-ГК-IP-М1» предназначено для приема и передачи сообщений об изменении состояния охраняемых шлейфов от приборов "Заря-ИО" и "Заря УСИ-2" через корпоративную сеть TCP/IP, Интернет.

Особенности

Обеспечивает подключение до 50 устройств "Заря-ИО" или "Заря УСИ-2" по 4-проводной магистрали, обмен информацией осуществляется по интерфейсу RS-485.

Технические характеристики

- обмен информацией между УОО и ПЦН осуществляется по сети передачи данных в формате протокола TCP/IP;
- обмен данными защищен шифрацией с псевдослучайными ключами. Это обеспечивает защиту от сканирования и от несанкционированной подмены УОО;
- программное обеспечение УОО и протокол TCP/IP обмена УОО с ПЦН совместимы с программным обеспечением и протоколом обмена, применяемым в СПИ «Заря» для связи с ПЦН;
- электропитание осуществляется от сети переменного тока напряжением от 150 до 242 В или резервного источника питания от 10,5 до 14,5 В.
- имеется возможность установки АКБ емкостью до 7А/ч;
- обеспечивает питание до 50 ППКО «Заря- ИО»;
- габариты размеры - 320х270х90 мм.

Типовые примеры организации централизованной охраны с помощью оборудования СПИ «Ахтуба» по сетям Ethernet

При использовании оператором связи технологии FTTC следует размещать концентраторы КЦ-400, КЦ-50М и резервное питание для них в уличных шкафах, где будет находиться телекоммуникационное оборудование операторов связи. При отсутствии места в шкафах операторов связи размещать оборудование в собственных шкафах уличного размещения рядом со шкафами операторов связи.

При использовании оператором связи технологии FTTB концентраторы КЦ-400, КЦ-50М и резервное питание для них следует размещать в подсобных помещениях, где будет находиться оборудование операторов связи.

Мультиплексоры при этом должны размещаться на ПЦО. Связь с ближайшим узлом оператора связи должна обеспечиваться либо через HSDSL модемы (в перспективе VDSL2-модемы) согласно рис. Е.1, либо через ВОЛС (при их наличии на ПЦО) согласно рис. Е.2. В мультиплексорах должна быть установлена программа версии АМ4.1009 и выше, в концентраторы – управляющая программа АМ4.1005 и выше.

Оператор связи организует виртуальную частную сеть для связи между мультиплексорами и концентраторами АСПИ «Ахтуба».

Кроме использования охраны по телефонным линиям с помощью концентраторов КЦ-400, КЦ-50М возможно использование маршрутизатора МС-800 GSM/GPRS/Ethernet и устройств оконечных объектовых УОО 4Е с использованием ADSL-модемов (в перспективе VDSL2-модемов) при технологии FTTC и FTTB и без дополнительного оборудования при технологии FTTH (оптика в квартиру) согласно рисунка Е.2.

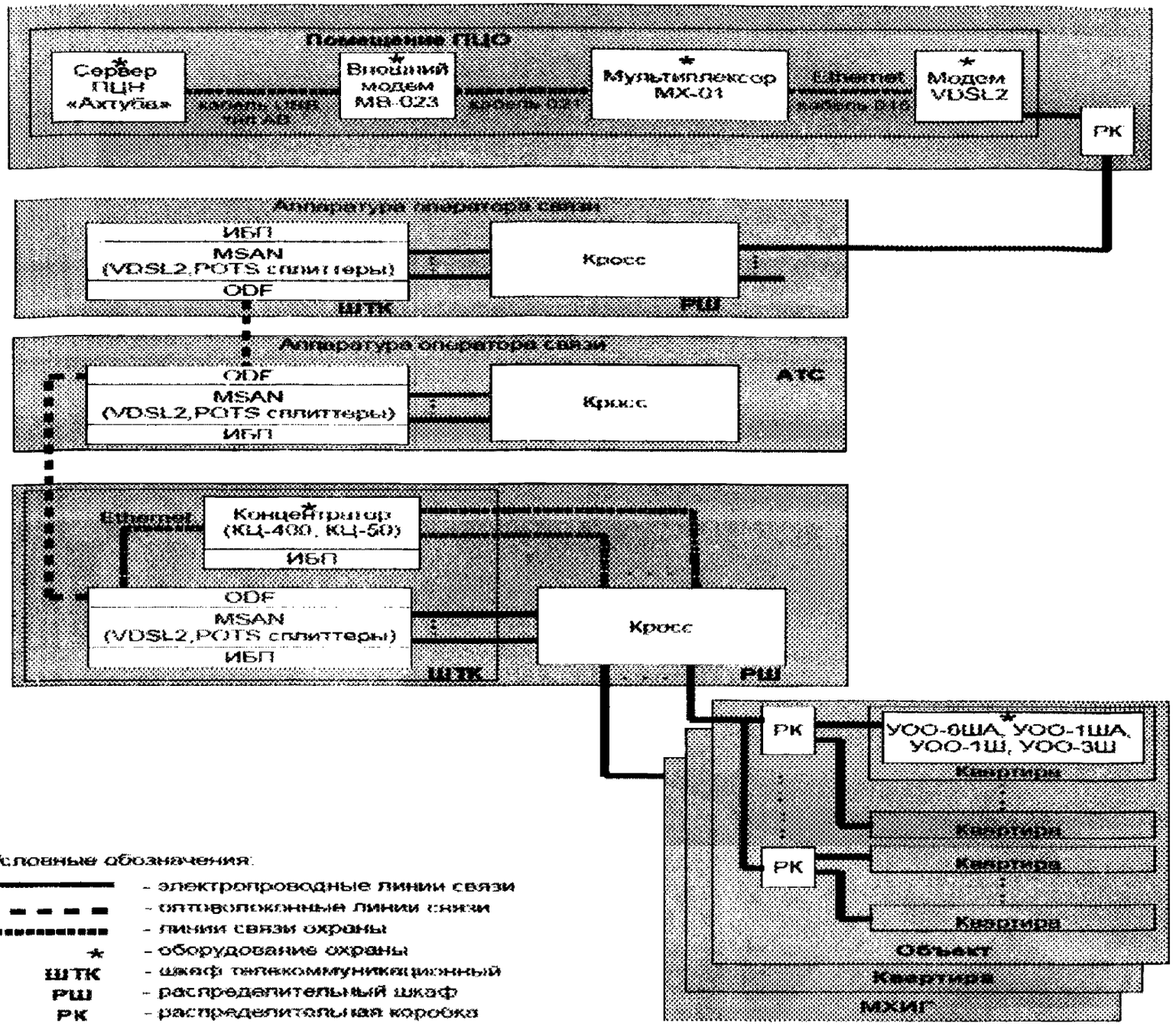
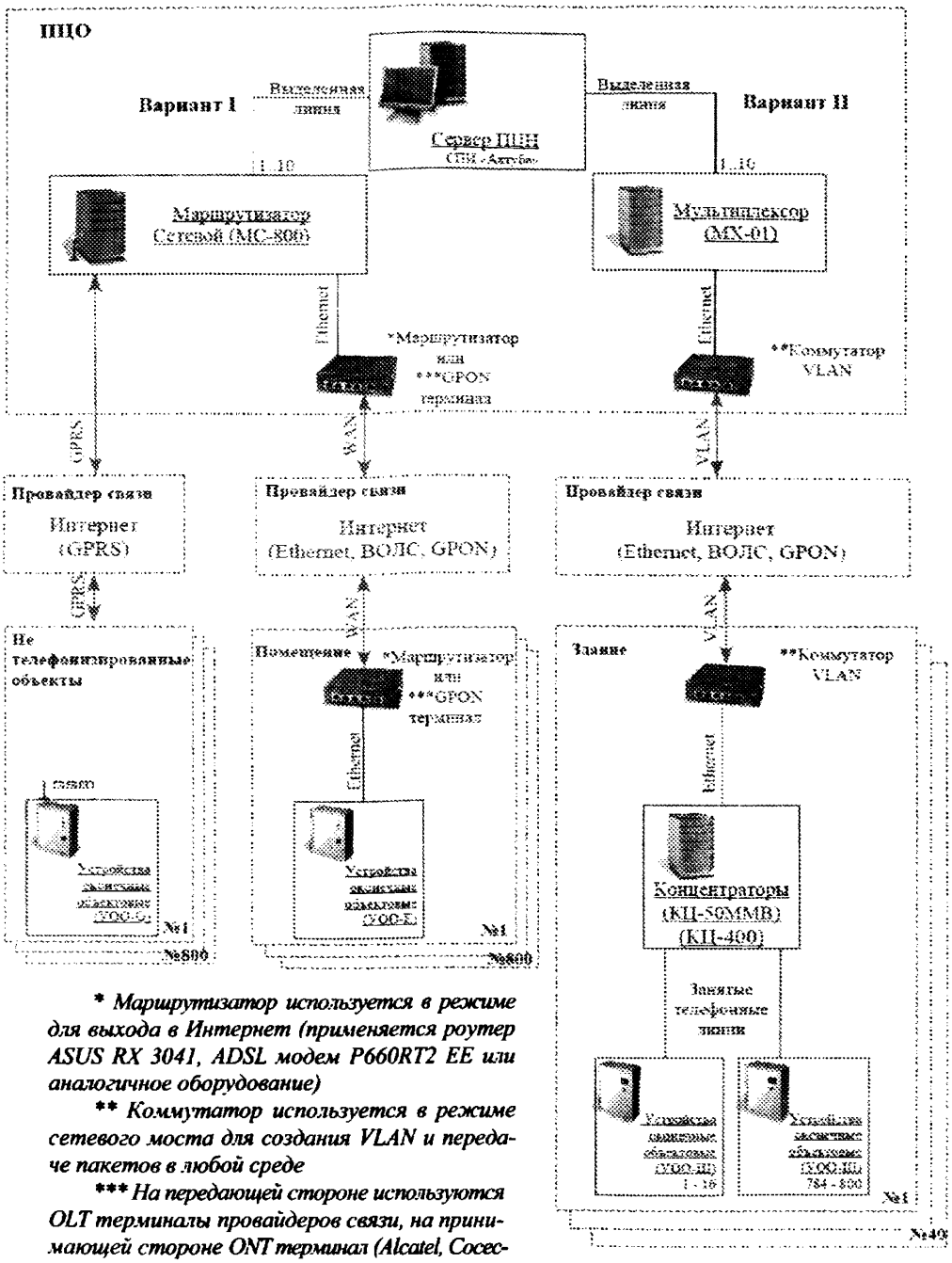


Рисунок Е.1 *- Вариант организации охраны с помощью АСПИ «Ахтуба» при использовании ВОЛС оператором связи*



** Маршрутизатор используется в режиме для выхода в Интернет (применяется роутер ASUS RX 3041, ADSL модем P660RT2 EE или аналогичное оборудование)*

*** Коммутатор используется в режиме сетевого моста для создания VLAN и передаче пакетов в любой среде*

**** На передающей стороне используются OLT терминалы провайдеров связи, на принимающей стороне ONT терминал (Alcatel, Cocecess, D-Link, Ericsson, NEC и др.)*

***Рисунок Е.2** - Вариант организации охраны с помощью АСПИ «Ахтуба» с использованием каналов GSM/GPRS/Ethernet/GPON*

Универсальным вариантом, вне зависимости от используемого оператором связи типа магистральных линий, является применение беспроводного канала АСПИ «Ахтуба» с использованием маршрутизатора МС-800 с установкой на охраняемых объектах устройств оконечных объектовых УОО 4G.

Представленные варианты успешно используются на практике. УВО г. Астрахани разместило свое оборудование в нескольких десятках уличных шкафов, связанных по ВОЛС (технология FTTC). Оборудование АСПИ «Ахтуба» работает по каналам связи операторов Евротелеком (г. Волжский) и Телеконнект (г. Новосибирск), использующих технологию FTTB. Оператор связи Сибирьтелеком, строящий сеть GPON (технология FTTH) в г. Новосибирске, с успехом использует устройства оконечные объектовые УОО 4E.

Оборудование для организации централизованной охраны с использованием технологии GPON

Устройство оконечное объектовое УОО 4E

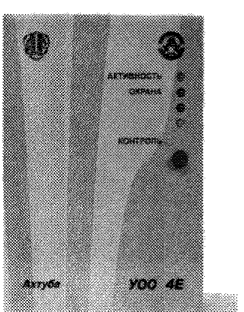


***Рисунок Е.3** – Внешний вид прибора*

Назначение

Устройство оконечное объектовое УОО 4Е (в дальнейшем – УОО 4Е) предназначено для контроля состояния четырех шлейфов сигнализации, передачи извещений на маршрутизатор сетевой (МС-800) и приема команд от МС-800 по интерфейсу Ethernet в составе системы передачи извещений «Ахтуба».

Состав УОО 4Е приведен в таблице Е.1

Таблица Е.1*- Состав УОО 4Е*

Обозначение	Наименование	Кол-во	Примечание
АИДВ.425533.026	Блок объектовый УОО 4Е (корпус, плата, аккумулятор)	1	
АИДВ.425721.006	Считыватель touch memory СТМ	1	По заказу
АИНП.425721.002	Считыватель touch memory накладной СТМН	1	По заказу
DS 1990 A	Электронный ключ	1	
DS 9093 N	Брелок	1	
ОЖ0.467.104 ТУ	Резистор С2-23-0,125-3,3 кОм-5%	4	

Особенности

- данные, передаваемые между УОО4Е и МС-800, зашифровываются в соответствии с требованиями ГОСТ 28147-89. Длина ключа 256 бит;

- электропитание УОО 4Е осуществляется от сети переменного тока напряжением 220 В +10%-15% и частотой (50±1) Гц через источник питания первичной сети (ИППС) с выходным стабилизированным напряжением 12В±10% и током нагрузки не менее 0,5 А;

- встроенный источник резервного питания (ИРП) на основе герметичной свинцово-кислотной аккумуляторной батареи 6 В - 1,2 А/ч;

- возможность работы через коммутаторы, шлюзы и роутеры;

- возможность работы с одним каналом МС-800 через канал одного провайдера на объекте: только через шлюз №1. УОО 4Е имеет возможность работы с двумя каналами МС-800 через каналы двух провайдеров на объекте: шлюз №1 и шлюз №2. Последний вариант позволяет резервировать канал связи с МС-800. Переключение обмена через шлюзы №1 и №2 происходит автоматически при потере связи между УОО 4Е и МС-800 по текущему каналу связи.

- для организации обмена между МС-800 и УОО 4Е в настройках МС-800 необходимо правильно указать все подсети IP адресов УОО с указанием маски. Для канала GPRS в настройках МС-800 рекомендуется указать маску 0.0.0.0 (шлюз по умолчанию). Для канала Ethernet в настройках МС рекомендуется указывать маску 255.0.0.0 или 255.255.0.0;

- провайдер Интернета для охраняемого объекта может предоставлять как статический, так и динамический IP адрес из своей подсети.

Технические характеристики

- обмен данными с маршрутизатором сетевым МС-800 по интерфейсу Ethernet стандарта 10/100BASE – T;

- на охраняемом объекте может работать через одного или двух объектовых провайдеров Интернета. Подключение к сети провайдера на объекте производится через роутеры, которые для УОО 4Е является шлюзами для выхода в Интернет. УОО 4Е и роутер образуют локальную сеть объекта (LAN объекта);

- если на объекте используется только один провайдер Интернета (только шлюз №1), то УОО 4Е программируется на обмен только с одним пультовым каналом МС-800 WAN1 или WAN2 (при программировании УОО 4Е все поля утилиты с пометкой «WAN2» должны совпадать с аналогичными полями «WAN1»);

- если на объекте используется два провайдера Интернета (шлюз №1 и шлюз №2), то УОО 4Е программируется на обмен с 2-мя пультовыми каналами МС-800 WAN1 и WAN2, что позволяет зарезервировать канал связи и не зависеть от технического состояния того или иного канала связи. При обрыве текущего канала связи УОО 4Е автоматически переключится на другой шлюз и переходит на 2-й канал связи;

- один и тот же провайдер Интернет предоставляющий подсеть IP адресов на охраняемых объектах, должен программироваться во всех УОО 4Е на один и тот же канал МС-800. В настройках МС необходимо указать все подсети, в которых работают УОО с указанием маски подсети;

- если в локальной сети объекта используется несколько УОО 4Е, то порт и локальный IP адрес каждого УОО 4Е должны быть уникальными;

- 4 ШС. Тип сигнализации для шлейфов (охранный/пожарный/тревожный) задается при программировании на ПЦН.

Концентратор КЦ-50М

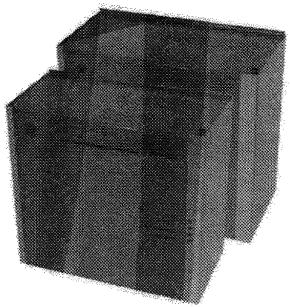


Рисунок Е.5 – Внешний вид приборов

Назначение

Концентратор КЦ-50М предназначен для получения по занятым телефонным линиям информации от УОО о текущем состоянии, предобработки и хранения полученной информации, передачи полученной информации на соответствующие ПЦН отделов вневедомственной охраны, пожарной охраны или милиции, передачи команд управления и контроля на УОО от ПЦН. На каждое направление может подключаться до 16 блоков объектовых. Общая информационная ёмкость - до 800 объектов. Для связи с концентратора с ПЦН используются мультиплексоры МХ- 01.

Особенности

- концентраторы соединяются в единую сеть с мультиплексорами МХ-01 через Ethernet с использованием VLAN каналов в любой среде передачи ВОЛС или GPON;

- концентратор КЦ-50М выпускается в пяти исполнениях – основном, в исполнениях 01, 02, 03,04;

- концентраторы основного исполнения и исполнения 01 передают сообщения через локальную сеть Ethernet на мультиплексор.

Технические характеристики

- обеспечивает прием и передачу цифровых сигналов методом амплитудной манипуляции с несущей частотой (18±0,045) кГц по коммутируемым и выделенным телефонным линиям;
- количество телефонных линий -50;
- скорость передачи информации по занятым телефонным линиям 600, 1200 или 2400 бит/с;
- скорость передачи информации по выделенным телефонным линиям 2400 бит/с;
- автоматическая подстройка чувствительности и устойчивый прием при изменении входного сигнала в выделенной линии в диапазоне от 25 мВ до 700 мВ.

Концентратор базовый на 400 направлений КЦ-400

Назначение

Предназначен для получения по занятым телефонным линиям информации от УОО о текущем состоянии, предобработки и хранения полученной информации, передачи полученной информации на соответствующие ПЦН отделов вневедомственной охраны, пожарной охраны или милиции, передачи команд управления и контроля на УОО от ПЦН. На каждое направление может подключаться до 2 блоков объектовых. Общая информационная ёмкость - до 800 объектов. Для связи с концентратора с ПЦН используются мультиплексоры МХ-01.

Особенности

- концентраторы соединяются в единую сеть с мультиплексорами МХ-01 через Ethernet с использованием VLAN каналов в любой среде передачи ВОЛС или GPON;
- выпускается в четырех исполнениях – основном, в исполнениях 01, 02, 03;

- концентраторы основного исполнения и исполнения 01 передают сообщения через локальную сеть Ethernet на мультиплексор;

- концентраторы исполнения 02 и 03 являются выделенными концентраторами и передают сообщения по выделенным телефонным линиям непосредственно на ПЦН;

- концентраторы основного исполнения и исполнения 02 комплектуются устройствами оконечными объектовыми;

- двухсторонняя связь с УОО с обязательным квитированием извещений;

- выносные концентраторы, установленные на разных АТС, могут соединяться в единую сеть с мультиплексором через ВОЛС, xDSL-модем или радио- Ethernet.

Технические характеристики

- обеспечивает прием и передачу цифровых сигналов методом амплитудной манипуляции с несущей частотой 18±0,045 кГц по коммутируемым и выделенным телефонным линиям;

- количество телефонных линий -50;

- количество контролируемых телефонных линий от 80 до 400;

- количество УОО, контролируемых по одной телефонной линии, до двух;

- скорость передачи информации по занятым телефонным линиям 600, 1200 или 2400 бит/с;

- скорость передачи информации по выделенным телефонным линиям 2400 бит/сек;

- автоматическая подстройка чувствительности и устойчивый прием при изменении входного сигнала в выделенной линии в диапазоне от 25 до 700 мВ.

Мультиплексор МХ-01

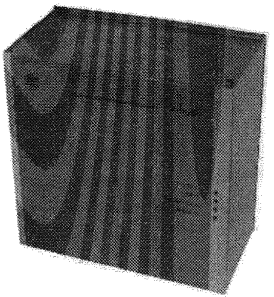


***Рисунок Е.6** – Внешний вид мультиплексора*

Назначение

Предназначен для объединения до 40 концентраторов и передачи изменения состояний УОО на соответствующие ПЦН, получения команд от ПЦН и передачи этих команд на соответствующий концентратор. При наличии в ретрансляторе двух мультиплексоров МХ-01, один из них используется в режиме горячего резервирования.

Мультиплексор объединяет концентраторы в единую сеть через Ethernet с использованием VLAN, ВОЛС или GPON.

Состав УОО 4Е приведен в таблице Е.2.

***Таблица Е.2** - Состав УОО 4Е*

Обозначение	Наименование	Кол-во	Примечание
АИДВ.425533.026	Блок объектовый УОО 4Е (корпус, плата, аккумулятор)	1	
АИДВ.425721.006	Считыватель touch memory СТМ	1	По заказу
АИНП.425721.002	Считыватель touch memory накладной СТМН	1	По заказу
DS 1990 A	Электронный ключ	1	
DS 9093 N	Брелок	1	
ОЖ0.467.104 ТУ	Резистор С2-23-0,125-3,3 кОм-5%	4	

Особенности

- мультиплексор МХ-01 предназначен для работы совместно с концентраторами КЦ-400, КЦ-50М и КЦ-50 с программным обеспечением версии V03;
- в состав ретранслятора с резервированием должны входить однотипные мультиплексоры МХ-01 либо МА.

Технические характеристики

- обеспечивает прием и передачу цифровых сигналов методом амплитудной манипуляции с несущей частотой 18±0,045 кГц по коммутируемым и выделенным телефонным линиям;
- количество каналов - 4;
- скорость передачи информации - 2400 бит/сек;
- количество контролируемых телефонных линий от 80 до 400;
- уровень передаваемого сигнала – (0,7±0,14) В;
- автоматическая подстройка чувствительности и устойчивый прием при изменении уровня входного сигнала от 25 до 700 мВ.

Маршрутизатор сетевой МС800

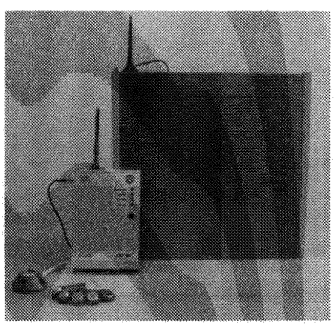


Рисунок Е.7 *– Внешний вид маршрутизатора МС800 с УОО-4G*

Назначение

Предназначен для получения информации от объектового оборудования по Ethernet каналу и передачи этих извещений на ПЦН.

Состав маршрутизатора МС800 приведен в таблице Е.3

Таблица Е.3 - *Состав маршрутизатора МС800*

Обозначение	Наименование	Кол-во
АИДВ.466514ю015-01	Маршрутизатор сетевой МС 800	1
Maestro 100 TCP/IP	Модем	1
ADA-0070-SMA	Антенна	1
ADA-2000-100	Кабель	1
ASUS RX 3041	Роутер	1
P660RT2 EE	Модем	1

Особенности

- маршрутизатор работает с устройствами оконечными объектовыми УОО-4Е и УОО-4G;
- подключение к сети оператора связи по интерфейсу Ethernet через коммутаторы, роутеры, xDSL –модемы;
- для связи с УОО-4G используется каналы GPRS операторов сотовой связи.

Технические характеристики

- обеспечивает прием и передачу цифровых сигналов методом амплитудной манипуляции с несущей частотой 18±0,045 кГц двухпроводным линиям;
- количество каналов связи с ПЦН - 2;
- скорость передачи информации по двухпроводным линиям - 2400 бит/сек;
- наличие в составе абонентской радиостанции стандарта GSM 900/1800 модели Maestro 100 TCP/IP;
- максимальная выходная мощность передатчика 2 Вт;

- интерфейс Ethernet стандарта IEEE 802.3 10 BASE;

- резервирование каналов связи с УОО-4Е и УОО-4G за счет подключения к интерфейсу Ethernet второго оператора мобильной или проводной связи с помощью стандартного внешнего оборудования: ADSL-модема или роутера, входящих в коплект поставки маршррутизатора;

- питание от сети переменного тока напряжением (220 +22/-44) В;

- габаритные размеры 320х300х170 мм.

СОДЕРЖАНИЕ

1. Определения и условные сокращения 3

2. Общие принципы организации сети централизованной охраны с использованием современных информационных технологий 7

3. Выбор СПИ и вспомогательного оборудования для органи-зации централизованной охраны на модернизируемых АТС 9

3.1 Организация оптических сетей доступа 10

3.2 Технические критерии выбора СПИ 12

4. Основные мероприятия по организации централизованной охраны на модернизируемых АТС 14

4.1 Прохождение и преобразование сигналов (извещений) от устройства оконечного до ПЦН 14

4.2 Алгоритмы действий инженерно-технических работников вневедомственной охраны по организации централизованной охраны с использованием современных средств связи и технологий 15

4.3 Порядок выделения IP-адресов для технических средств охраны, расположенных на ПЦО и квартирах .. 16

4.4 Порядок и нормативная база взаимодействия с операторами связи 17

4.5 Основные монтажные и эксплуатационные затраты на оборудование для организации канала связи на ПЦО и на квартирах 19

Приложение А Комплекс централизованного наблюдения «Альтаир» 20

Приложение Б Автоматизированная система передачи извещений «Приток-А» 35

Приложение В Автоматизированная система передачи извещений «Атлас-20» 51

Приложение Г Автоматизированная система передачи извещений «Юпитер» 66

Приложение Д Автоматизированная система передачи извещений «Заря» 83

Приложение Е Автоматизированная система передачи извещений «Ахтуба» 91

gost.e-ecolog.ru