А.Н. Членов
(Академия ГПС МЧС России; e-mail: chlenov@mail.ru)

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ОПТОВОЛОКОННЫХ КАНАЛОВ СВЯЗИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ

Проведён анализ практических особенностей формирования централизованных систем охранно-пожарной сигнализации с использованием оптоковолоконных каналов связи.
Ключевые слова: система охранно-пожарной сигнализации, оптоволоконный канал связи.

A.N. Chlenov

FEATURES OF APPLICATION OF FIBER OPTIC COMMUNICATION CHANNELS IN THE AUTOMATED SECURITY-FIRE ALARM SYSTEMS

Analysis of the practical features of the formation of the centralized security-fire alarm systems with using fiber optic communication channels
Key words: security-fire alarm systems, fiber optic communication channel.

Статья поступила в редакцию Интернет-журнала 20 января 2014 г.

Особенностью развития информационных технологий в сфере коммуникаций является широкое использование различных каналов связи [1].

В настоящее время уже при строительстве новых зданий зачастую к ним прокладываются не медные, а оптоволоконные кабели. Это дает возможность операторам фиксированной связи повысить конкурентоспособность предоставляемых ими услуг по высокоскоростному доступу в Интернет и организации многопотоковой информации, используемой для различных целей.

Оптоволоконные технологии используются для организации передачи данных в рамках IP-сети, связывающей объекты защиты и ***пункт централизованной охраны (ПЦО)*** [2].

Способы применения оптоволоконых технологий классифицируют по названию точки сопряжения с потребителем и объединяются названием FTTx – оптоволокно до точки "x":

- FTTB (Fiber To The Building) – оптоволокно доведено до административного здания (предприятия);
- FTTC (Fiber To The Curb) – оптоволокно доведено до распределительного шкафа;
- FTTH (Fiber To The Home) – оптоволокно доведено до абонента (объекта защиты).

Технология FTTC обеспечивает один из простейших и наиболее дешевых способов наращивания сети. В FTTC волоконно-оптический кабель из центрального узла (районной АТС или узла оператора услуг связи) проложен к монтажному шкафу, оснащенному электронным распределительным обору-

дованием. Шкаф по конструктивному исполнению может быть предназначен как для наружного размещения, так для установки внутри отапливаемых или неотапливаемых помещений. От шкафа к абонентам идут медные витые пары. В отличие от телефонных пар, эти витые парные кабели имеют относительно небольшую длину (до 500 *м*) и более хорошие электротехнические характеристики.

На объекте охраны 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 здании, должен обеспечивать контроль и управление сервисными потоками по всем портам для каждого абонента в отдельности с гарантируемым высоким качеством. Абоненты, как правило, подключаются с использованием 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 объектовой распределительной сети. Непосредственно на объекте защиты устанавливается абонентский терминал (мультимедиа-адаптер), который обеспечивает преобразование цифровых потоков в аналоговые сигналы традиционных видов сервиса – видео и телефонии.

В настоящее время выделенная оптоволоконная линия на физическом уровне, по сравнению с обычными средами (электропроводной и радиоканальной), является самой защищённой для передачи данных. Кроме этого, коммутаторы Ethernet, использующиеся в средах сервис-провайдеров, обеспечивают разделение физического уровня портов и логического уровня абонентов, а также надёжную защиту, которая в состоянии предотвратить практически любые попытки вторжений.

В типовых конфигурациях сетей доступа Ethernet FTTH применяются относительно недорогие одноволоконные линии, использующие технологию 100BX или 1000BX, с максимальным радиусом действия 10 *км*. Для передачи информации на гораздо бо/льшие расстояния выпускаются модули, позволяющие увеличить мощность оптического сигнала, а также оптоволоконные пары с оптическими модулями, которые можно подключить к порту любого Ethernet-оборудования.

Оптимальной для FTTH является технология пассивных оптических сетей Gigabit PON (GPON), которая отличается масштабируемостью и сверхбольшой пропускной способностью. Суть технологии 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, например, технологию GPON для предоставления услуги доступа в Интернет в массовом порядке применяет компания ОАО "Ростелеком". В качестве абонентского терминала для доступа в Интернет на объектах применяется ONT (Optic Network Terminal) – абонентский узел, как правило, имеющий четыре Ethernet разъема FE (Fast Ethernet), один из которых можно использовать для формирования централизованной охранно-пожарной сигнализации с использованием ***автоматизированных систем передачи извещений (АСПИ)*** и ***комплексов централизованного наблюдения (КЦН)***.

В настоящее время для этой цели во вневедомственной охране МВД России применяются АСПИ и КЦН следующих типов: "Альтаир", "Атлас-20", "Атлас-20К", "Ахтуба", "Заря", "Приток-А", "Юпитер" [3].

В табл. 1 представлены возможности этих систем по использованию оптических сетей с технологией FTTx.

Таблица 1

Наименование АСПИ и КЦН	**Наименование технологии**		
	FTTC	**FTTB**	**FTTH (GPON)**
"Приток-А"	+	+	+
"Ахтуба"	+	+	+
"Атлас-20"	+	+	+
"Юпитер"	+	+	+
"Заря"	-	+	+
"Альтаир"	$\pm$	$\pm$	$\pm$

Примечание: "+" – обеспечивается работа по технологии FTTx;
"-" – не обеспечивается работа по технологии FTTx;
"$\pm$" – оборудование находится в стадии разработки

Возможность применения технологии FTTx определяет наличие специального оборудования для сопряжения с ВОЛС, ретрансляторов, устанавливаемых в выносы АТС, обеспечивающих связь от ретранслятора до пульта централизованного наблюдения (ПЦН) по оптическим каналам с использованием виртуальной локальной сети АТС по протоколу TCP/IP. Общим требованием к АСПИ также является полная аппаратная и программная поддержка ретранслятором всего ранее установленного и имеющегося на объекте охраны объектового оборудования, невыработавшего установленные сроки службы.

Можно сформулировать следующие дополнительные технические условия, необходимые при использовании оптических технологий для формирования централизованной системы охранно-пожарной сигнализации [2]:

- наличие свободного места в телекоммуникационном шкафу (выносе);
- наличие медной пары от выноса до абонента, где установлено объектовое оборудование;
- возможность установки ретранслятора в стойку внутри выноса;
- наличие телефонной линии от ретранслятора до абонента;
- 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 качестве примера на рис. 1-4 представлены возможные схемы организации охранно-пожарной сигнализации с использованием современных АСПИ и КЦН [2, 4, 5].

На рис. 1 представлена схема подключения входящих в "Альтаир" приборов "Редут-Net" и устройств сопряжения с применением технологии GPON. Все приборы могут иметь как статические, так и динамические IP-адреса. На ПЦН формируется публичный статический IP-адрес.

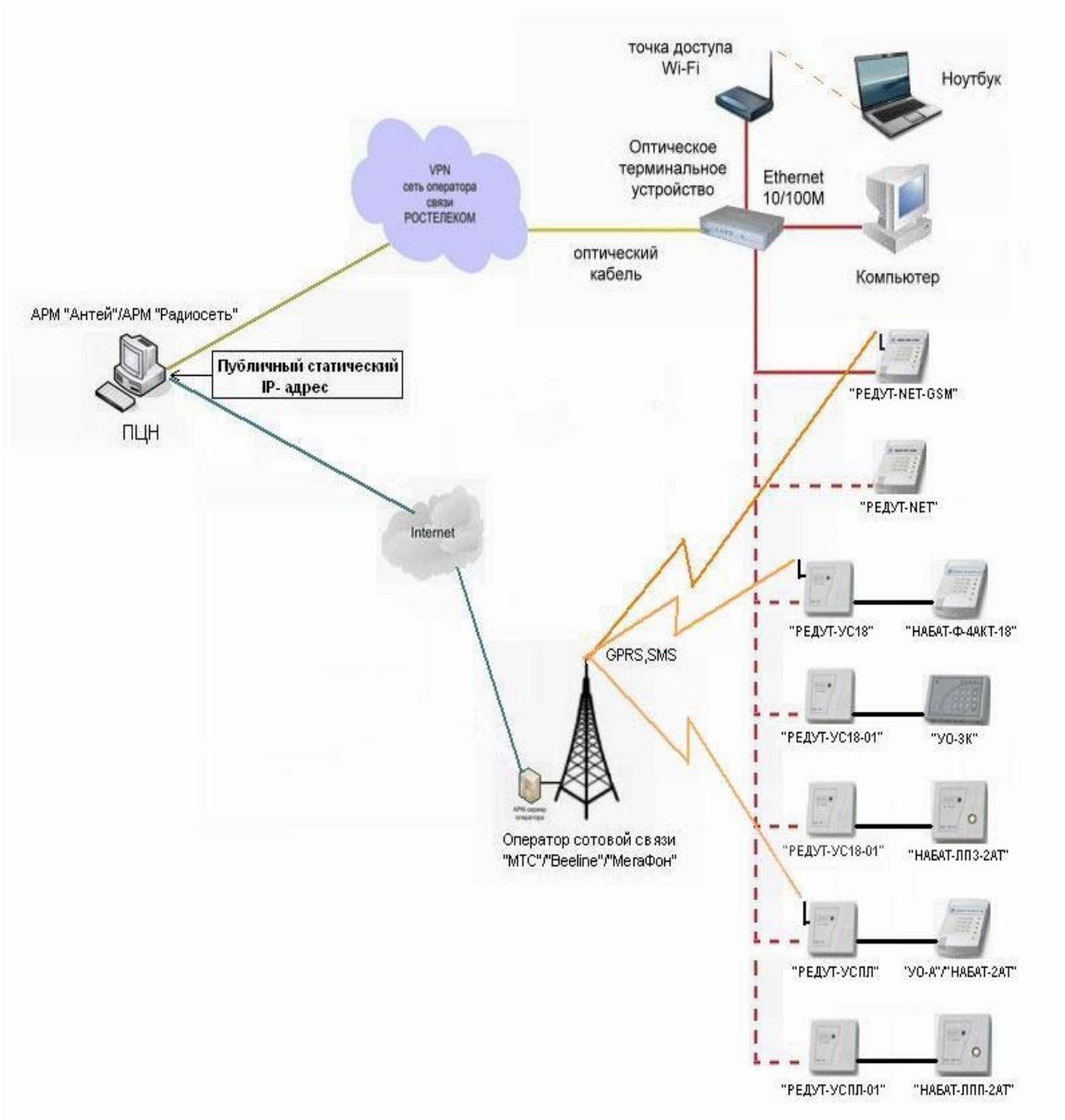

Рис. 1. Организация подключения приборов "Редут-Net" и устройств сопряжения с применением технологии GPON

Резервный канал формируется с использованием операторов сотовой связи, находящихся в зоне развертывания комплекса. Организация резервного канала, имеющего отличный от основного способ прохождения сигналов, обусловлена необходимостью повышения отказоустойчивости системы охранно-пожарной сигнализации в целом.

Кроме этого, с целью обеспечения надежности охраны объекта, обязательно наличие резервного узла маршрутизации на основе BGP (Border Gateway Protocol – протокол маршрутизации в среде Internet между автономными системами). Создание такого узла обеспечит резервирование основных путей преобразования сигнала и позволит гарантированно передать сигнал от устройства оконечного (УО), расположенного на объекте защиты, до ПЦН.

Ядро сети, сформированное для преобразования и передачи извещений, должно использовать технологию ***VPN (виртуальную частную сеть)*** что позволит сохранить постоянный контроль над сетью, даже в случае обслуживания такой сети сторонними организациями [6].

На рис. 2 представлена возможная схема организации подключения приборов "Редут-Net" по выделенной линии через ADSL-модем (Asymmetric Digital Subscriber Line – технология высокоскоростной передачи данных по существующей абонентской телефонной линии с одновременным использованием этой линии как обычной телефонной). Применение такой схемы возможно при построении сети по технологиям FTTB, FTTH, а также в сетях общего пользования. Количество охранно-пожарных приборов, подключаемых по этой схеме, ограничивается только шириной канала ADSL-модема.

На рис. 3 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 и подключенный к нему 3G-модем. Программное обеспечение роутера построено таким образом, что при отказе глобальной сети (WAN) он переходит на работу через подключенный к нему 3G- модем. При восстановлении сети автоматически завершается работа через 3G-модем. Роутер необходимо подключать к резервированному источнику питания.

На рис. 4 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 приборов охранно-пожарной сигнализации.

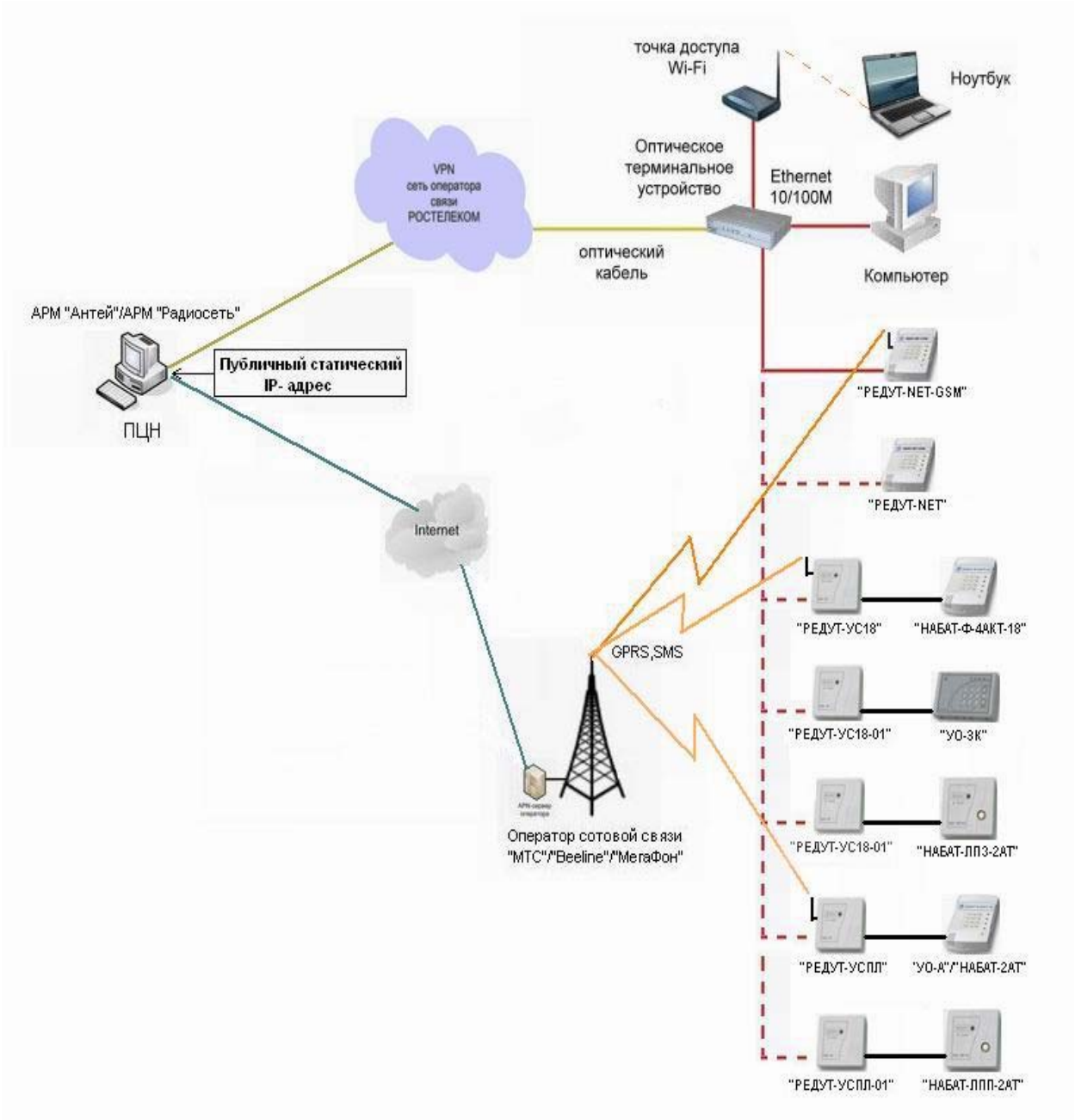

Рис. 2. Организация подключения приборов "Редут-Net"
по выделенной линии через ADSL-модем

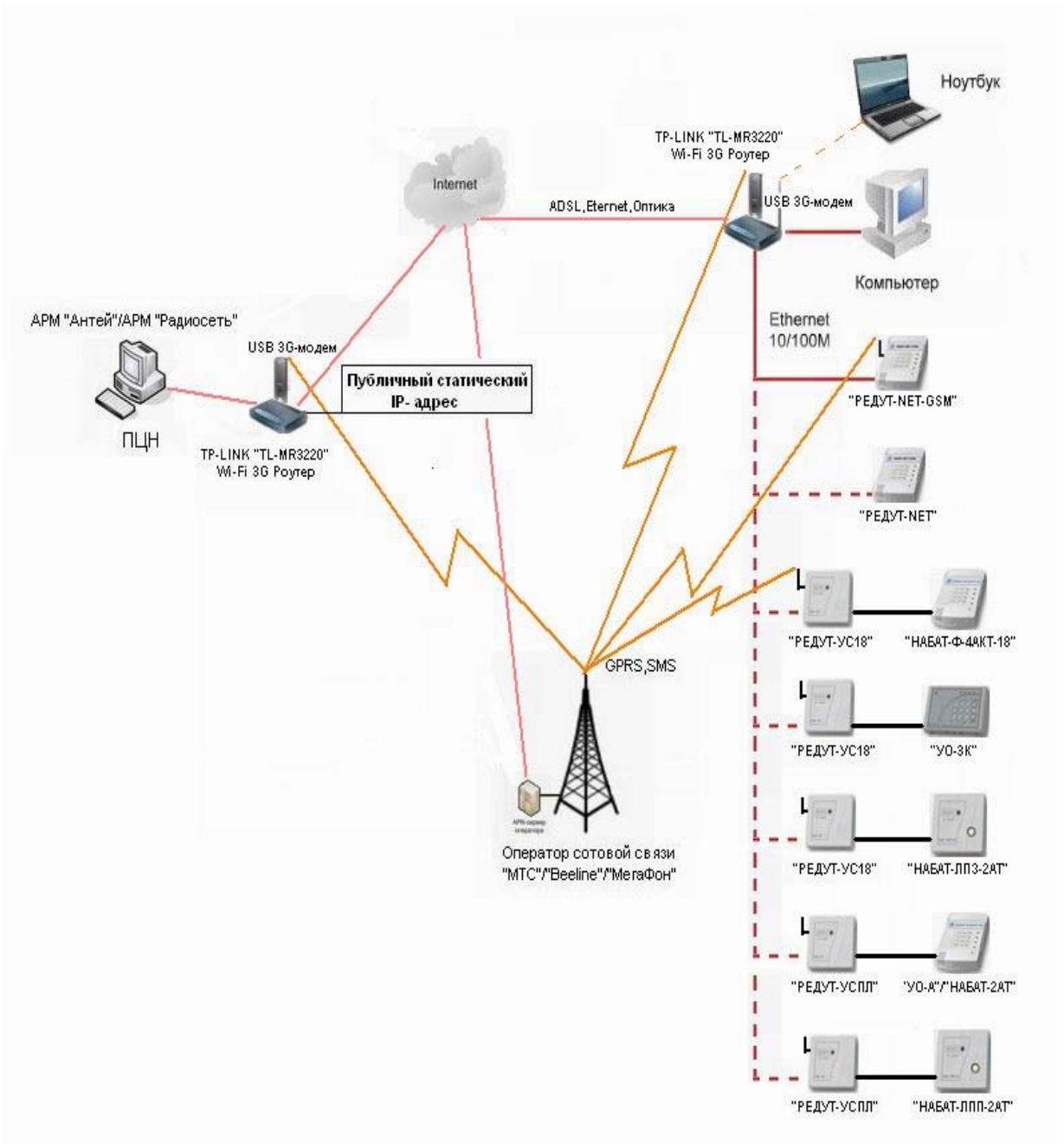

Рис. 3. Организация дополнительного резервного канала с применением USB-3G-модемов

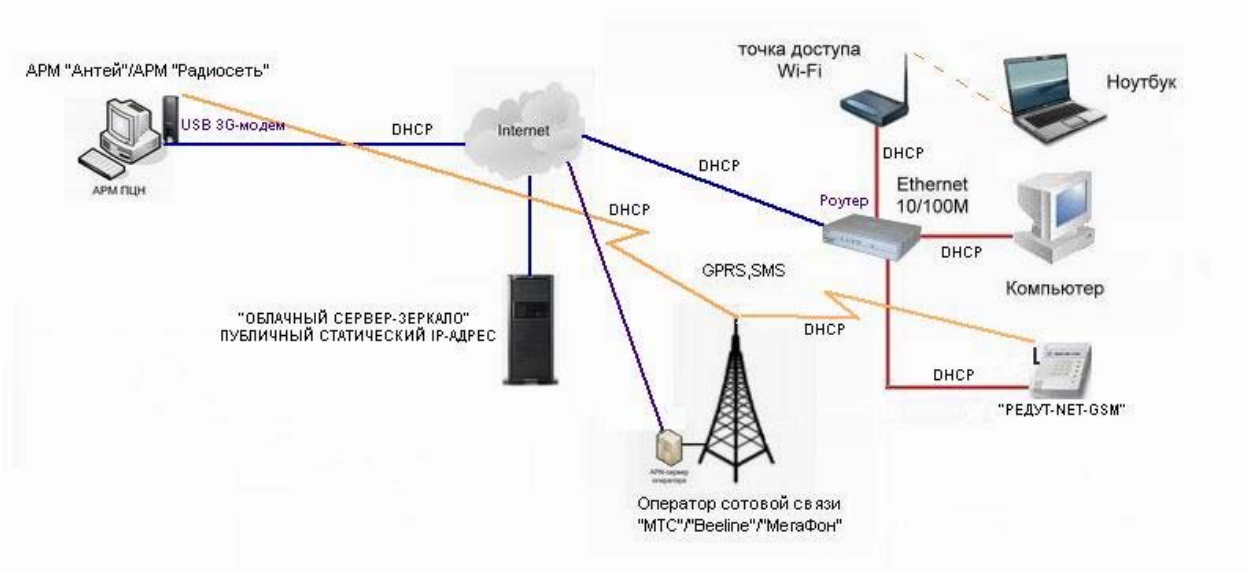

Рис. 4. Схема работы АСПИ через дополнительный удаленный сервер

Выводы

1. Оптоволоконные технологии являются одной из составных частей организации передачи данных в рамках IP-сети. Высокий технологический уровень разработки и производства обеспечивает их широкое внедрение в централизованные системы охранно-пожарной сигнализации различных объектов.

2. Имеющийся опыт применения цифровых каналов связи с использованием PON-технологий в подразделениях вневедомственной охраны МВД России может быть успешно использован для формирования систем противопожарной защиты на промышленных предприятиях.

Литература

1. ***Членов А.Н., Буцынская Т.А., Дровникова И.Г.*** Особенности управления в системе охраны и безопасности объекта // Проблемы безопасности и чрезвычайных ситуаций. 2009. № 1. С. 85-94.

2. ***Рекомендации*** по организации централизованной охраны на модернизированных АТС, использующих цифровые каналы связи, в том числе с применением PON-технологий, с помощью современных СПИ, используемых в подразделениях вневедомственной охраны: Типовые варианты. М.: НИЦ "Охрана" МВД России, 2012. 73 с.

3. ***Список*** технических средств безопасности, удовлетворяющих "Единым техническим требованиям к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны" и "Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны". М.: ГУВО МВД России, 2012.

4. http://www/nicohrana.ru/altair.

5. http://ahtuba-plus.ru.

6. ***Членов А.Н.*** Применение современных информационных технологий в автоматизированных системах противопожарной защиты // Технологии техносферной безопасности: интернет-журнал. 2014. Вып. № 1 (53). http://ipb.mos.ru/ttb.