

# ВЫБОР ТИПА КАНАЛА СВЯЗИ ДЛЯ ОРГАНИЗАЦИИ ПОЖАРНОГО МОНИТОРИНГА

А. Зайцев

научный редактор журнала «Алгоритм безопасности»

В конце 2013 года планируется принять новую редакцию свода правил СП 5. 13130 «Установки пожарной сигнализации и пожаротушения автоматические. Нормы и правила проектирования». В ней в обязательном порядке должны быть учтены все изменения как новой редакции «Технического регламента о требованиях пожарной безопасности», так и вступающей в силу с января 2014 года новой редакции ГОСТ Р 53325-2012 «Технические средства пожарной автоматики». В данной статье я решил поднять вопрос выбора типа канала связи для организации пожарного мониторинга.

## ПОЖАРНЫЙ МОНИТОРИНГ И СУЩЕСТВУЮЩИЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ

Вопросом организации пожарного мониторинга озадачивается все больше и больше специалистов, работающих в области пожарной безопасности.

Некоторые вопросы по организации пожарного мониторинга я уже попытался рассмотреть в более ранних публикациях [1,2]. Наиболее полно и подробно существующие проблемы я попытался описать в публикации на сайте [www.avtoritet.net](http://www.avtoritet.net) в разделе «Статьи» [3].

С одной стороны, вступление в силу новой редакции Федерального закона № 123-2008 года «Технический регламент о требованиях пожарной безопасности» с принципиально новой формулировкой п. 7 статьи 83 уже неотвратимо, июль 2014 года не за горами.

С другой стороны, уже третий год действует программа по оборудованию дежурно-диспетчерских служб центральным пультовым оборудованием для приема с объектов данных об их противопожарном состоянии. И наконец появляется возможность реализовать требования нормативных документов более раннего поколения – НПБ 110-03 «Перечень зданий, сооружений, помещений и оборудования, подлежащих защите автоматическими установками пожаротушения и автоматической пожарной сигнализацией» и НПБ 88-01 «Установки пожаротушения и сигнализации. Нормы и правила проектирования». В них уже был определен некий порядок по организации пожарного мониторинга, но при условии наличия технической возможности. Все предыдущие годы возможности не было и такой задачи перед проектно-монтажными организациями не стояло. Но сейчас, в рамках подготовки к реализации требований ФЗ № 123, решение этой задачи стало актуально. Параллельно стали появляться и требования от органов Госпожнадзора, что вполне естественно, и их приходится выполнять, независимо от наличия возможностей.

В новой редакции ГОСТ Р 53325-2012 «Технические средства пожарной автоматики», вступающей в силу с 01.01.2014 техни-

ческим средствам для организации пожарного мониторинга – объектовым и пультовым приборам систем передачи извещений о пожаре (СПИП) – отведен самостоятельный раздел. Но этим стандартом не рассматривается и не может рассматриваться вопрос выбора канала связи для взаимодействия между собой этих приборов. Это все-таки вопрос практического применения технических средств, и он должен найти свое отражение в своде правил СП 5. 13130 «Установки пожарной сигнализации и пожаротушения автоматические. Нормы и правила проектирования». И если для внутриобъектовых СПИП, при объединении на объекте нескольких установок пожарной сигнализации в одну систему, возможно и оправдано использование практически любых типов каналов связи, то для государственного пожарного мониторинга вопрос выбора канала связи стоит очень остро.

Но есть ли надежда, что в этом своде правил появятся действительно обоснованные решения по выбору канала связи для организации пожарного мониторинга с требуемыми характеристиками? А время уходит.

## КЛАССИФИКАЦИЯ КАНАЛОВ СВЯЗИ

В статье «Радиоканал в охранных и пожарных системах сигнализации» [4] я попытался обосновать свое видение классификации радиоканалов в системах охранно-пожарной сигнализации объектов. Сейчас допустимо использовать этот материал в какой-то степени, по крайней мере потом будет легче разбираться со всем остальным.

По физическому принципу каналы связи могут быть проводными, беспроводными (радиоканалы), оптоволоконными и комбинированными.

Каналы обмена данными для всех физических принципов организации в первую очередь подразделяются на дуплексные, с двухсторонним обменом данными, и симплексные, с односторонним обменом данными.

В частности, оба типа каналов при работе по радиоканалу задействуют выделенный или закрепленный за ними частотный диапазон (ресурс). Для разделения по направлению обмена дуплексные радиоканалы имеют

временное (TDD), частотное (FDD), кодовое (CDD), пространственное (SDD) и поляризаационное (PDD) разделение. Выделенный частотный ресурс при работе по радиоканалу ограничен и он в большинстве случаев платный, и чаще используется метод TDD. В проводных каналах связи таких проблем нет, так как для этого используются раздельные физические линии.

Системы, использующие двухсторонний обмен данными, в свою очередь, между собой разделяются на системы с фиксированным закреплением каналов (FAMA), т.е. вот тебе навсегда кусочек связи, или системы с предоставлением каналов по требованию (DAMA).

Протокол DAMA предполагает распределение ресурса центральным устройством системы с жесткой синхронизацией из центра. Тут широко используется опросный метод в любых его вариантах, типа:

- Сидоров?
- Я!
- Петров?
- Я!
- Иванов?
- Где Иванов?

Это очень характерно для проводных систем и почти не используется в радиоканальных.

Если же распределение ресурса, используемого системой, происходит по каким-то алгоритмам работы самих оконечных устройств, то это уже относится к протоколам множественного доступа (ПМД). То есть инициатором сеанса связи является не центральное устройство, а любое оконечное – по его требованию. Среди этих протоколов наиболее известен множественный доступ с контролем несущей (МДКН), когда оконечное устройство, прежде чем включить свой передающий тракт, контролирует наличие свободного для обмена ресурса и только при его наличии передает запрос на организацию сеанса связи с центральной станцией.

Следующий уровень классификации относится не к собственно каналу, а к сети, в рамках которой он существует.

В специализированной радиосети могут быть как прямые каналы (объект-пульс) с радиальной топологией, так и каналы с использованием ретрансляторов (радиально-узловая топология). Причем в качестве ретрансляторов могут использоваться как самостоятельные устройства, так и все объектовые станции данной сети.

Телефонные сети подразделяются на сети, предоставляемые операторами фиксированной и мобильной (подвижной) связи, и сети общего доступа типа Internet, включая в свою очередь и сети по каналу GSM.

## **ПРОВОДНЫЕ И ОПТОВОЛОКОННЫЕ КАНАЛЫ СВЯЗИ ДЛЯ ОРГАНИЗАЦИИ ПОЖАРНОГО МОНИТОРИНГА**

Исторически сложилось, что первым и основным каналом связи для охраны объектов силами вневедомственной охраны бы-

ли проводные телефонные линии связи. Надежность их работы позволяла гарантировать максимальную достоверность получаемых извещений с объектов.

Но в конце девяностых годов появилась проблема совместной работы охранной техники с использованием высокочастотного уплотнения телефонной линии и каналов Internet по технологии ADSL. Это было началом вытеснения вневедомственной охраны с проводных телефонных линий.

Дальше ситуация еще больше усложнилась. Первой ласточкой стало появление цифровых телефонных выносов (подстанций) прямо в подъездах жилых домов и в производственных зданиях. От них до здания автоматической телефонной станции (АТС) сигнал передавался в цифровом виде, но места для передачи извещений от технических средств охранной сигнализации в них не нашлось. Оборудование было, в основном, импортное, и проблемы вневедомственной охраны России никак не учитывались. Более того, при отключении электропитания в самом жилом доме или на предприятии телефонная связь, организованная на этом оборудовании, обрывается полностью, что для охранного, а тем более для пожарного мониторинга в принципе недопустимо.

А дальше мы все быстрее и быстрее уходим в технологию PON, и в частности GPON, когда оптоволоконная линия с предельной скоростью обмена в несколько Гбит/с заканчивается от коммуникационного центра прямо в квартире абонента. От коммуникационного центра абонент по этой технологии может получать доступ в различные сети: и Internet, и кабельного, в том числе интерактивного, телевидения. Конечно, и в таком канале связи можно было бы найти место для передачи извещений от охранных и пожарных систем, но это будет очень накладно и малоэффективно, и опять-таки без каких-либо гарантий работы в условиях чрезвычайных ситуаций. А то, что эти абонентские оптоволоконные преобразователи не имеют резервных источников питания лучше не напоминать – у них совсем другие задачи.

Конечно, есть еще системы информаторного типа, работающие по так называемому методу автодозвона с использованием стандартных протоколов обмена типа Ademko Contact ID. Произошло событие – автоматически набрался нужный телефонный номер и модулированный по частоте сигнал передал всю необходимую с объекта информацию. Но такой канал не может иметь контроля исправности, его наличие и исправность зависит от состояния оборудования операторов связи. Впрочем и проблема с электропитанием у него такая же, как и у предыдущих.

Кстати, совсем недавно на правительственном уровне рассматривался вопрос о резервировании электропитания базовых станций сотовой связи. Не вдаваясь в по-

дробности, заявляю: ничего общего у них со временем работы систем противопожарной защиты от резервных источников питания как не было, так и не будет.

В итоге все попытки по старинке использовать проводные и оптоволоконные каналы для организации пожарного мониторинга уже не имеют перспективы и их, скорее всего, не следует рассматривать при разработке требований в новой редакции СП 5.13130.

## **БЕСПРОВОДНЫЕ (РАДИОКАНАЛЬНЫЕ) ТЕХНИЧЕСКИЕ СРЕДСТВА ДЛЯ ОРГАНИЗАЦИИ ПОЖАРНОГО МОНИТОРИНГА**

Практически все типы радиоканалов можно разделить на три основные группы:

- радиоканалы на выделенных частотах;
- радиоканалы на нелицензируемых частотах;
- радиоканалы операторов мобильной связи.

Каждая такая группа типов радиоканалов имеет свои, только им присущие особенности.

Начну с последней – GSM.

Ни для кого не секрет, что пропускная способность сетей мобильной связи для каналов по передаче данных в формате SMS и GPRS не является фиксированной, а определяется трафиком речевых (голосовых) каналов. С работоспособностью систем передачи извещений от охранной сигнализации это связано мало, т.к. если на каком-либо объекте попытаются утащить телевизор или кофеварку, то общественность, находящаяся в зоне действия этой базовой станции, вряд ли кто будет ставить в известность. Совершенно противоположная ситуация наблюдается в чрезвычайных ситуациях, к которым можно отнести возникновение пожара, когда все одновременно хватаются за мобильные телефоны. Возникает перегруз трафика ближайших базовых станций, и тут уже не до передачи данных.

Необходимо еще добавить кое-что из Приказа Министерства РФ по связи и информатизации № 113 от 27 сентября 2007 «Об утверждении требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования». В соответствии с этим приказом доля несостоявшихся вызовов из-за технических неисправностей или перегрузки сети связи в общем количестве попыток вызовов (потери вызовов) при установлении соединений в сети подвижной связи не должна превышать 5 %, а это даже без учета чрезвычайных ситуаций достаточно большая цифра. В чрезвычайных ситуациях этот показатель многократно увеличивается и нормированию указанным приказом уже не подлежит, а значит, и виноватых в несвоевременном получении извещений о пожаре с объекта или вообще полном отсутствии таковых можно будет и не искать. Я еще



как-то допускаю, что базовые станции соевой связи, расположенные в малонаселенной местности вряд ли будут перегружены незначительным количеством пользователей, находящихся в зоне их действия, даже в чрезвычайных ситуациях. В этом случае с учетом большой протяженности каналов связи других типов, а, следовательно, их низкой надежности, скорее всего этим каналам мобильной связи в рамках пожарного мониторинга не будет другой альтернативы, за исключением мест массового пребывания или проживания людей. Но в оборудовании, работающем по этим каналам, должен быть организован контроль целостности и работоспособности канала как со стороны объектового оборудования, так и со стороны центральной станции. А вот как определить критерий малонаселенной местности, я пока и сам не знаю.

Если говорить об организации контроля целостности и работоспособности каналов передачи данных по сетям GSM, то на рынке уже представлены системы с технологией Ping. Вообще-то Ping – это утилита для проверки соединений в сетях на основе TCP/IP, а также обиходное наименование самого запроса. Эта утилита является неотъемлемой частью любых сетевых операционных систем. Но при определенных условиях можно это как-то позиционировать и применить на каналах сетей GSM.

Время между отправкой запроса и получением ответа позволяет определять двухсторонние задержки по маршруту и частоту потери пакетов, т.е. косвенно определять загруженность на каналах передачи данных и промежуточных устройствах, а также и наличие работоспособных маршрутов. К сожалению, даже наличие такой информации что-либо изменить в организации и поддер-

жании работоспособности самого канала не способно, поэтому многие производители используют эту информацию для перехода на резервный проводной канал, который, как я тут уже показал, в чрезвычайных ситуациях не работоспособен.

Теперь о системах передачи извещений на нелицензируемых частотах.

Наиболее часто для этого используется диапазон 433 МГц. Однако использовать допустимую в данном частотном диапазоне мощность передающего устройства 10 МВт для внутриобъектовых систем охранно-пожарной сигнализации возможно, другое дело – для построения систем передачи извещений о пожаре в городах и поселках городского типа. И хотя есть положительный опыт построения таких систем, и даже попытки подвести под это какую-то научную базу [5], их использование еще как-то возможно в системах передачи извещений по охране объектов, но не в пожарном мониторинге. Надеяться на необходимый стопроцентный результат не приходится, чем-то это напоминает игру в «орел-решка». Кстати, автор упомянутого здесь материала занимался и занимается именно охранной тематикой, так что совесть у него по отношению к пожарному мониторингу чиста.

Радиоканал на выделенных частотах.

Очень часто можно услышать вопрос: а что это такое – «выделенные частоты». Весь радиочастотный спектр является национальным достоянием. Имеется порядок получения для использования того или иного частотного ресурса на той или иной территории с последующей регистрацией всех используемых получателем этого ресурса средств излучения. Выделение частотного ресурса производится на возмездной основе. Это гарантирует, что никто, кроме зарегистри-

рованного пользователя, не сможет использовать выделенный ему частотный ресурс. Заплатил и пользуйся единолично.

С самого начала работ по организации систем передачи извещений в частных охранных организациях (ЧОО) в подавляющем большинстве использовался и используется по настоящее время односторонний (симплексный) радиоканал. Он даже во вневедомственной охране использовался до недавнего времени. Да, все специалисты прекрасно понимали, что конфликтные ситуации между несинхронизированными между собой по времени излучения передающими устройствами неизбежны. Одно излучающее средство будет глушить другое, и не от одного, и не от другого в итоге сигнал получен не будет. Но в этой игре между производителями, охранными предприятиями и потребителями их услуг у каждого своя роль, и никто не хочет менять правила игры.

После обобщения большого количества данных о достоверности получаемой по таким каналам информации с объектов, в МВД не так давно принято решение полностью отказаться от симплексных объектовых устройств и использовать только дуплексные каналы радиосвязи. А вроде ничего не предвещало беды, но разум наконец-то восторжествовал. И этим опытом необходимо воспользоваться при построении систем новой структуры в пожарной безопасности, и не повторять чужих ошибок, тем более нас к этому призывают еще и европейские нормы.

В пожарном мониторинге двухсторонний обмен еще со временем понадобится для дистанционного пуска приборов управления систем противопожарной защиты, когда этого, по понятным причинам, не может сделать дежурный персонал при заблокированном автоматическом пуске (подобное можно наблюдать сплошь и рядом). Плюс появляется дополнительная возможность оповещения людей в рамках гражданской обороны и чрезвычайных ситуаций. Так что, если выбирать между односторонним и двухсторонним обменом, здесь вопросов не должно возникнуть.

## ПРОГРАММНАЯ И ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Наличие только дуплексных радиоканалов в системах передачи извещений не является всеобъемлющим и законченным решением, т.е. панацеей от всех проблем. В радиальных структурах построения в условиях городской застройки антенные устройства приходится размещать на крышах зданий. Хорошо бы, только на своих, а то подчас приходится это делать на соседних, более высоких. Потери сигнала в фидерных устройствах, их неустойчивая работа в различных погодных условиях делает подчас невозможным организовать устойчивую радиосвязь.

Для решения этой проблемы потребуется уже использовать радиально-узловую

**ДЛЯ СПРАВКИ.** В европейских нормах, в частности EN 54 часть 21 в разделе 5.1 предусматривается, что системы передачи тревожных сигналов должны быть способны обрабатывать следующие сигналы:

- б) передачи сигналов предупреждения о неисправности (имеется ввиду своей) на ППКП,
- в) приема сигналов предупреждения о неисправности сети (канала) связи,
- д) сигнал подтверждения приема переданных сигналов от центра получения сигналов тревоги,
- е) передачи подтверждения приема переданных сигналов от центра получения сигналов тревоги, на ППКП.

Это сделано для того, чтобы на объекте при нарушении связи с центральным пультом не рассчитывали на автоматическую доставку извещений о пожаре, с одной стороны, и принимали меры по восстановлению канала связи, с другой стороны.

Вопрос в этом случае рассматривается следующим образом. Если есть ППКП, то на нем должна выводиться вся необходимая информация о выполнении им своих функций. Объектовый сегмент системы передачи сигналов о пожаре в данном случае рассматривается как составная часть этого ППКП, и независимо от его места размещения, вся информация должна быть именно на нем. Тогда для выполнения этой функции в ППКП, работающем в системе пожарного мониторинга, должны быть дополнительные средства индикации, чего в наших отечественных ППКП не предусматривается.

А это как раз и есть то, что предусмотрено в п.14.4. СП5.13130 «...В помещении с круглосуточным пребыванием дежурного персонала должны быть выведены извещения о неисправности приборов контроля и управления, установленных вне этого помещения, а также линий связи, контроля и управления техническими средствами оповещения людей при пожаре и управления эвакуацией, противоподымной защиты, автоматического пожаротушения и других установок и устройств противопожарной защиты». Только в европейских нормах это намного более конкретизировано и имеет законченный и логический вид.

Более того в этих европейских нормах четко указано, что ни о каких системах передачи извещений с односторонним каналом связи речи вестись не может.

топологию построения сети, в которой роль узлов будут выполнять ретрансляторы. Но как показывает опыт построения таких сетей, и это не панацея, или придется размещать ретранслятор на крыше чуть ли не каждого дома. Можно представить, как это скажется стоимости.

Поэтому еще лет двадцать назад достаточно известная в области связи и коммуникаций корпорация AES разработала систему охранного мониторинга «AES IntelliNet». По тем временам это был очень серьезный проект, почему многим специалистам запомнилось это оборудование. Я к нему тоже лет пятнадцать назад имел непосредственное отношение. Проблемы с ним, конечно, некоторые были, но в целом это был очень положительный опыт.

Система «AES IntelliNet» представляла собой сеть из объектовых приемо-передатчиков, в которой каждое объективное устройство являлось ретранслятором для других. Объективное устройство состоит из связанного контроллера серии 7000, включающего микропроцессор и радиомодем, и приемопередатчика мощностью 5 или 2 Вт. В каждом объективном устройстве хранятся и постоянно перепроверяются 8 наиболее удачных по условиям прохождения маршрутов. При первичной установке устройства эти маршруты выбираются специалистом на основе полу-

ченных измерений. В последующем они могут корректироваться. Такая особенность системы позволила значительно повысить надежность как канала связи объект – пульт, так и всей системы в целом по сравнению со всеми другими стандартными решениями. В нашей стране есть немало частных охраняемых организаций, до сих пор эксплуатирующих эту систему.

Но время не стоит на месте. Уже почти столько же лет в компьютерных сетях существует термин «динамическая маршрутизация». И если первоначально эту функцию могли выполнять только серверы, используя упомянутую мною ранее утилиту Ping, то со временем эта функция появилась и у коммутаторов низшего уровня, рассчитанных даже для использования в промышленной автоматике.

Но именно радиосети, как ничто другое, более приспособлены по своей структуре к реализации механизма динамической маршрутизации, т.к. у них нет ограничений, как у проводных систем, по количеству радиальных ответвлений.

При динамической маршрутизации между объектовыми устройствами в системе появляется возможность организовать многосвязную сетевую топологию с прокладкой маршрутов «по требованию». Под многосвязностью здесь понимается возможность

передачи данных каждым источником через все множество узлов сети, функции которых выполняют объектовые устройства. Маршрутом в данном случае является последовательность участков ретрансляции пакета данных между объектовыми устройствами, при передаче его от удаленного объекта к центральному пульту, либо в обратном направлении. В итоге многосвязность радиоканальных систем может быть значительно больше по сравнению с любыми проводными.

Если в симплексных радиоканальных системах рабочий трафик не может превышать 5-10 % от максимальной пропускной способности, из-за необходимости постоянного разрешения конфликтных ситуаций между источниками излучений, то в дуплексных системах этот вопрос не столь актуален. Как следствие, в дуплексных радиосистемах вся имеющаяся пропускная способность системы может быть задействована не только для передачи информационных сигналов, но и для постоянного тестирования и поиска маршрутов. А это очень важная особенность, т.к. в условиях городской застройки на тех или иных радиointервалах системы возможны глубокие и длительные медленные затухания сигнала, вызванные переотражением сигналов от тех или иных строительных конструкций, а также рефракцией

(отклонением направления радиоволны от прямой линии), сильно зависящей от погодных условий. И вот тут без динамической маршрутизации не обойтись. При наличии достаточно большой плотности размещения объектов устройств-ретрансляторов можно будет, в итоге, практически полностью отказаться от выносных антенно-фидерных устройств, что будет становиться все более очевидным по мере развития пожарного мониторинга. Причем порядок построения такой сети заключается в том, чтобы постепенно развивать сеть от центрального пульта в сторону максимально удаленных объектов устройств. Таким образом, изначально будет формироваться абсолютно достаточная плотность оконечных станций-ретрансляторов, с последующим ее продвижением к удаленным объектам.

Постоянное тестирование радиointервалов и поиск кратчайших маршрутов с максимальной достоверностью обмена данными позволяет создавать реально работающие в любых условиях среды радиосистемы. Будучи независимыми от желаний и возмож-

ностей операторов как фиксированной, так и мобильной связи, радиосети с динамической маршрутизацией могут обеспечить получение достоверной информации о противопожарном состоянии объектов в любых кризисных ситуациях. Очень важное их отличие – это организационно-техническая независимость от любых других соответствующих сетей связи общего применения.

Важно отметить принципиальную разницу в технических решениях, используемых в системе «AES IntelliNet» и в компьютерных сетях. В первом случае они были уникальны и использовались только в этом оборудовании, а во втором случае это стандартная функция, независящая от конкретного производителя периферийного оборудования.

Не буду лукавить, что я не знаком с имеющимся оборудованием, реализующим динамическую маршрутизацию в радиоканальных системах пожарного мониторинга. В какой-то степени я знаком с продукцией двух достаточно известных производителей, выпускающих совместимое между собой

оборудование. Где есть двое, рано или поздно появится и третий, и четвертый. Главное – не нарушать принцип совместимости этого оборудования между собой, иначе сможем получить лоскутное одеяло.

В заключение было бы необходимо напомнить, что если при разработке новой редакции свода правил СП 5. 13130 не будет учтен многолетний опыт построения систем охранного мониторинга, если этот опыт не будет спроецирован на особенности и отличия в передаче информации о противопожарном состоянии объектов и других чрезвычайных ситуациях, то, при внешней благополучности строящейся системы пожарного мониторинга, мы получим за очень большие деньги налогоплательщиков обычные, так нами любимые потемкинские деревни. Очень бы этого не хотелось.

А теперь, после написания данной статьи, мяч находится на стороне команды ФГБУ ВНИИПО МЧС РФ. Что они думают по этому поводу, и думают ли вообще, когда и куда дальше полетит этот мяч – в чьи ворота, мы узнаем в ближайшем обозримом будущем.

#### ЛИТЕРАТУРА:

1. Зайцев А. В. Пожарный мониторинг, как он будет работать / Системы безопасности. 2011. № 4.
2. Зайцев А. В. Системы передачи извещений в противопожарной защите объектов / Системы безопасности. 2011. № 6.
3. Зайцев А. В. Зачем, куда и как передаются сигналы / [http://avtoritet.net/press\\_articles/zachem-kuda-i-kak-peredayutsya-signalny](http://avtoritet.net/press_articles/zachem-kuda-i-kak-peredayutsya-signalny)
4. Зайцев А. В. Радиоканал в охранных и пожарных системах сигнализации / Алгоритм безопасности. 2012. № 6.
5. Брауде-Золотарев Ю. М. Алгоритмы безопасности радиоканалов / Алгоритм безопасности. 2013. № 1.

## Обнаружение вторжений в полной темноте

**FLIR**



Видимый спектр



ИК-изображение



### FLIR серии D

Мультисенсорные сетевые тепловизионные камеры для систем безопасности в купольных корпусах для наружного размещения

Тепловизионные камеры серии D для наружного размещения обеспечивают прецизионное управление углами поворота и наклона камеры, сканирование пространства по заданной программе, а также совместную работу с радаром.

- Работа в сетях TCP/IP
- Разрешение ИК-изображения 640 x 480 или 320 x 240 пикселей
- Видеокамера день/ночь с 36-кратным масштабированием.

ONVIF

[www.flir.com](http://www.flir.com)