Подвижные и стационарные технологические сети обмена данными.

Часть 1. Стационарные радиосети

В соответствии с новой редакцией Федерального закона «О связи» (№ 126-ФЗ), технологические сети связи предназначены для обеспечения производственной деятельности организаций и управления технологическими процессами в производстве. Новое определение практически объединило две ранее существовавшие категории: «ведомственные сети связи» и «внутрипроизводственные и технологические сети связи».
Данный материал открывает серию статей о технических средствах, используемых для создания узкополосных технологических радиосетей обмена данными в диапазоне ультракоротких волн (УКВ), принципах их построения, возможностях, преимуществах и недостатках. Основное внимание уделено описанию «конвенциональной» аппаратуры передачи данных и сравнению ее возможностей с оборудованием для транковых радиосетей.
В первой части речь пойдет о стационарных средствах обмена данными, вторая посвящена подвижным радиосетям, а в третьей будет рассказано об использовании транковых систем. Обращаем внимание, что по всей статье сохраняется сквозная нумерация рисунков и таблиц, а общий список литературы будет приведен в последней части материала.

Сергей Маргарян
serge@rodnik.ru

Несмотря на бурное развитие в последнее десятилетие широкополосных технологий высокоскоростного обмена данными в диапазоне сверхвысоких частот (СВЧ), традиционные узкополосные (шаг сетки радиочастот 25 кГц и менее) средства передачи данных диапазона УКВ продолжают играть важную роль в инфраструктуре связи различных ведомств и организаций. Это обусловлено уникальными возможностями средств связи данного типа, позволяющими строить стационарные и подвижные радиосети обмена данными с полностью детерминированными параметрами работы на обширных территориях, а также наличием значительного числа приложений, не требующих передачи больших объемов данных, но предъявляющих повышенные требования к оперативности их доставки потребителям.

Оборудование для стационарных радиосетей обмена данными

Наиболее широкое распространение узкополосные стационарные средства обмена данными получили на предприятиях топливно-энергетического комплекса, в горнодобывающей промышленности, лесном и водном хозяйстве, дорожных службах, на стационарных объектах авиационного, железнодорожного, автомобильного и электротранспорта.

Основными пользователями таких сетей являются:

- промышленность и транспорт — для управления телемеханическими устройствами и аппаратурой сбора телеметрической информации;
- банки и офисы — для подключения автономно функционирующих технических средств, например банкоматов;
- вооруженные силы и службы общественной безопасности — для дистанционного управления специальной техникой и оповещения.

Применение рассматриваемых радиосредств не только повышает надежность создаваемых автоматизированных систем управления технологическими процессами (АСУ ТП), но и снижает материальные и финансовые затраты на их эксплуатацию. Во многих случаях применение радиосредств обмена данными оказывается экономически более выгодным по сравнению с проводными, поэтому наряду с развертыванием новых систем управления телемеханическими устройствами по радиоканалу многие предприятия заменяют существующие проводные каналы на беспроводные.

Радиосети сбора телеметрической информации и управления телемеханическими устройства-

ми существуют уже более ста лет. Пионером в создании технических средств для них была компания Johnson Data Telemetry (США). Узкополосные радиосети для стационарных приложений характеризуются следующими основными данными:

- надежность среды передачи (линия передачи не подвергается механическим повреждениям и разрушающему влиянию окружающей среды);
- внешние детерминированные протоколы обмена данными, поддерживающие работу в режиме времени, близком к реальному;
- малое время доступа к каналу передачи данных;
- обширная оперативная зона;
- низкая стоимость эксплуатации;
- независимость от существующей инфраструктуры связи;
- совместимость с оборудованием сбора и обработки данных;
- простота перемещения и развертывания в новом районе;
- возможность эксплуатации в жестких условиях.

Правильно спроектированные и настроенные радиосети обмена данными позволяют создавать относительно недорогие, эффективные и гибкие телеметрические системы, способные функционировать на протяжении многих лет с минимальным техническим обслуживанием. Типовая схема коммутации стационарной радиосети обмена данными представлена на рис. 1.

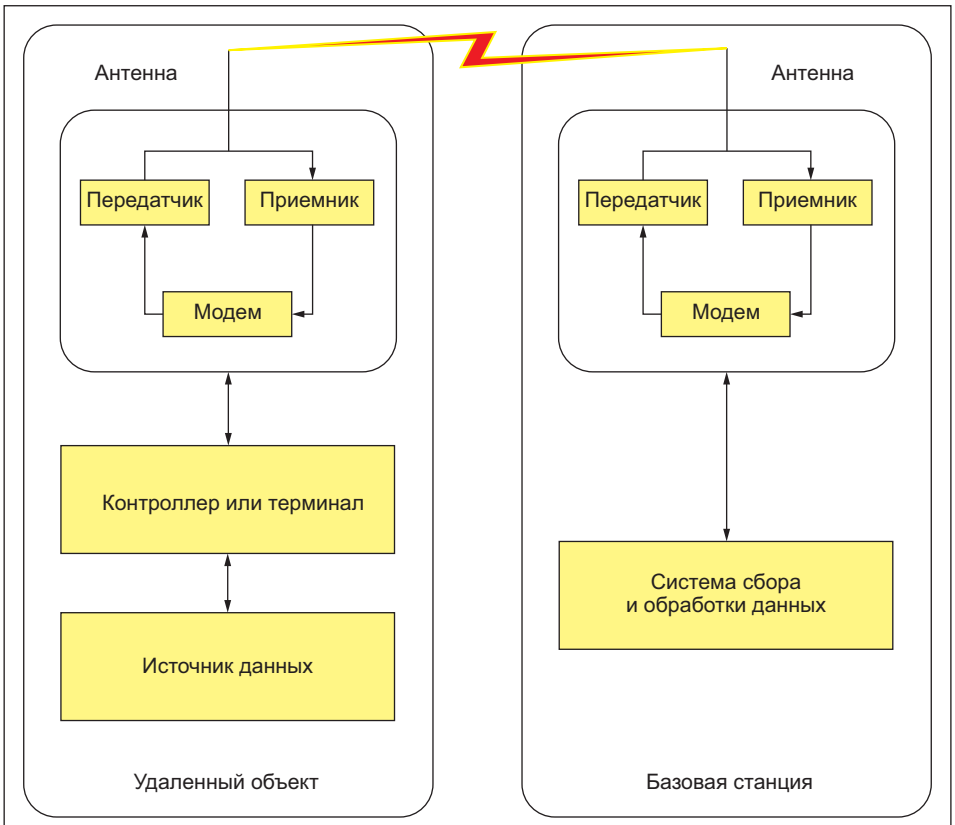

Рис. 1. Типовая схема коммутации стационарной радиосети обмена данными

Источником данных на удаленном объекте является датчик или группа датчиков. Получаемая от датчиков информация принимается и обрабатывается программируемым контроллером (Programmable Logic Controller, PLC) или удаленным терминалом (Remote Terminal Unit, RTU), который подключается к радиомодему по последовательному интерфейсу (как правило, RS-232). Радиомодем служит для преобразования поступающих цифровых данных в аналоговый сигнал, который посредством радиопередатчика передается в пункт управления (например, диспетчерскую). Здесь процесс обработки происходит в обратном порядке: модем преобразует поступивший от радиоприемника аналоговый сигнал в цифровую форму, пригодную для его дальнейшей обработки центральным компьютером.

В типовых приложениях обмен данными в составе системы производится под управлением центрального объекта или базовой станции (БС) методом опроса (как правило, применяются хорошо освоенные промышленностью протоколы, например ModBus). Аппаратура связи удаленного объекта постоянно находится в режиме приема. БС направляет в адрес удаленного объекта запрос на передачу имеющейся информации, после чего переходит в режим приема и ожидает получения запрошенной информации. Получив запрос, аппаратура связи удаленного объекта переходит в режим передачи и транслирует имеющиеся данные в адрес БС (при отсутствии информации передается соответствующее сообщение). После завершения передачи аппаратура связи удаленного объекта переходит в режим приема. С получением сообщения от удаленного объекта БС передает очередной запрос в адрес того же или другого удаленного объекта. Этот процесс продолжается до тех пор, пока не будет собрана информация от всех удаленных объектов.

Возможные варианты построения стационарных радиосетей обмена данными представлены на рис. 2.

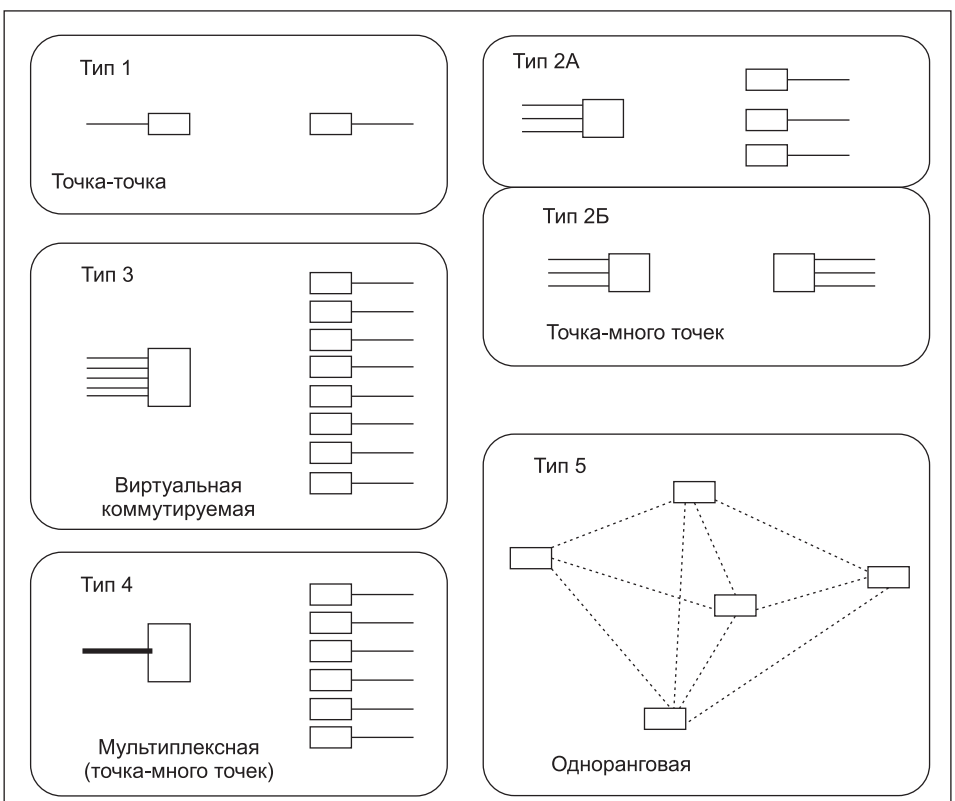

Рис. 2. Варианты топологии стационарных радиосетей обмена данными

Таким образом, создается сеть сбора телеметрической информации или управления телемеханическими устройствами с полностью детерминированными параметрами, исключающая флуктуации информационного потока, способные привести к сбоям в ее работе, и поддерживающая работу удаленных устройств в режиме времени, близком к реальному. При этом наиболее высокая надежность работы достигается в системах, в которых обеспечивается прямая радиовидимость между объектами, т. е. радиосигнал беспрепятственно распространяется от передающей до приемной антенны. Номинально в создаваемых радиосетях радиовидимость составляет 25–30 км на открытой местности и 8–12 км в условиях города со средней плотностью застройки.

Современные стационарные радиосети строятся на специализированных радиомодемах. Общими требованиями к этим устройствам считаются:

- «Прозрачный» режим работы. Используется протокол верхнего уровня, что упрощает интеграцию с АСУ ТП и различными типами оборудования.
- Высокая пропускная способность. Пакетная передача и дополнительные методы повышения надежности доведения информации, связанные с увеличением объема служебной информации, не применяются, что обусловлено относительно стабильными условиями канала радиосвязи между стационарными объектами. Пропускная способность радиоканала в таком режиме в несколько раз больше, чем в «пакетном» для подвижных приложений на аналогичной скорости.
- Малое время доступа к радиоканалу. Основное время при передаче затрачивается на выполнение процедур связи, поскольку объем данных, передаваемых от контролируемых объектов за один сеанс связи, относительно мал и обычно составляет десятки байт.
- Высокая скорость обмена данными. В составе системы может функционировать значительное количество объектов, последовательный опрос которых должен производиться за короткий промежуток времени, обычно от нескольких десятков секунд до нескольких минут.
- Работа оборудования базовой станции в дуплексном режиме, что позволяет сократить период опроса в системах с большим количеством удаленных контролируемых объектов. Контролируемые объекты в этом случае используют полудуплексное оборудование.
- Удаленная диагностика и настройка. Поскольку создаваемые системы размещаются, как правило, на обширной территории, только наличие данной функции позволяет обеспечить их надежное функционирование и снизить затраты на обслуживание в процессе эксплуатации.

Следует отметить, что важным параметром, влияющим на работу любой системы обмена данными, является мощность радиосигнала. Известно, что в общем случае мощность сигнала при увеличении расстояния снижается в геометрической прогрессии. Например, при удвоении расстояния от точки передачи до точки приема мощность радиосигнала падает в четыре раза. Однако на практике мощность снижается значительно сильнее в связи с затуханием, вызванным влиянием местных предметов, зеленых насаждений и других препятствий. В результате при удвоении расстояния мощность сигнала снижается более чем в четыре раза. Однако значение параметра выходной мощности аппаратуры для построения рассматриваемых стационарных радиосетей может быть относительно низким, поскольку условия распространения и, соответственно, мощность принимаемого радиосигнала в процессе работы остаются стабильными и могут быть достаточно точно определены на этапе проектирования системы.

Возможности современного оборудования для стационарных приложений позволяют использовать их и для работы с подвижными объектами или в «смешанных» радиосетях, в состав которых входят стационарные и подвижные объекты. Как правило, такие системы предназначены для широковещательной (циркулярной) передачи информации и не рассчитаны на прием «ответных» данных от подвижных объектов. Примером таких приложений является трансляция сигналов дифференциальной поправки для объектов, использующих данные от спутниковой радионавигационной системы «Навстар»/GPS или нуждающихся в получении метеорологических данных (системы оповещения). В отдельных случаях «стационарное» оборудование может применяться и на подвижных объектах (например, в России прошла успешные государственные испытания система контроля тормозной системы железнодорожного состава, реализованная на радиомодемах для стационарных приложений), однако в этом случае на разработчика такой системы ложится решение дополнительных технических задач, связанных с обеспечением ее надежной работы.

Таблица 1. Перечень государств с работающими стационарными узкополосными радиосетями

АВСТРАЛИЯ	Австралия, Новая Зеландия
АЗИЯ	Азербайджан, Бахрейн, Бруней, Иордания, Израиль, Индия, Казахстан, Кувейт, Малайзия, Оман, Сингапур, Тайвань, Таиланд, Турция, Узбекистан, Филиппины, Шри-Ланка, Южная Корея
АМЕРИКА	Аргентина, Боливия, Бразилия, Венесуэла, Гаити, Гондурас, Канада, Колумбия, Коста-Рика, Мексика, Панама, Парагвай, Перу, Суринам, США, Уругвай, Чили, Эквадор
АФРИКА	Египет, Заир, Мавритания, Марокко, Нигерия, Чад, ЮАР
ЕВРОПА	Белоруссия, Бельгия, Великобритания, Венгрия, Германия, Италия, Латвия, Литва, Норвегия, Польша, Португалия, Россия, Финляндия, Франция, Украина
АНТАРКТИДА	

Применяемое для создания современных стационарных радиосетей обмена данными оборудование является специализированным, и обобщенные данные об объемах его выпуска отсутствуют (значительная часть оборудования применяется в закрытых системах в интересах вооруженных сил и специальных служб). Более того, часть вновь выпускаемого оборудования используется для модернизации или поэтапного расширения уже существующих систем. В связи с этим наиболее правильная оценка масштабов применения рассматриваемого оборудования может быть получена при учете количества функционирующих радиосетей и регионов, в которых оно развернуто. По имеющимся данным, в настоящее время количество таких радиосетей (в составе каждой может работать от нескольких до нескольких сотен, а в отдельных случаях — нескольких тысяч объектов) составляет более пятидесяти тысяч, включая несколько сот систем на территории Российской Федерации. Перечень государств, на территории которых развернуты и функционируют стационарные узкополосные радиосети обмена данными, приведен в таблице 1.

Наиболее крупные из развернутых систем функционируют на площадях от ста до миллиона квадратных километров, что сравнимо по своим масштабам с европейской частью территории нашей страны.

Кроме того, узкополосные радиомодемы применяются в ходе космических экспедиций на Марс и при освоении околоземного космического пространства, а также для работы радиосетей обмена данными военного и специального назначения под землей, на земле, на воде и в воздухе.

Обеспечение безопасности данных в стационарных радиосетях

Одним из наиболее важных требований к технологическим радиосетям обмена данными является обеспечение их безопасности. Следует отметить, что защита данных в любой системе представляет собой непрерывный комплекс организационно-технических и специальных мероприятий, ни одно из которых самостоятельно не позволяет добиться поставленной задачи. Тем не менее рассматриваемые средства обмена данными обладают свойствами, позволяющими существенно снизить существующие угрозы, главными из которых являются перехват и несанкционированный доступ к работе в радиосети, что обусловлено уже самой средой передачи.

На первый взгляд, перехват данных в проводных технологических сетях связи сопряжен с серьезными трудностями. Однако эта задача не так сложна для злоумышленника, имеющего соответствующую подготовку. Кабельная сеть прокладывается внутри здания или комплекса зданий. При этом отдельные сегменты могут укладываться в подвалах, коллекторах, патернах и т. п., не контролируемых службами безопасности, и представлять собой потенциальные точки для несанкционированного подключения. Теоретически любой человек, знающий

структуру кабельной системы, может получить доступ к ней в этих точках. После подключения к проводной системе связи получение доступа к информации является делом техники, поскольку во всех открытых проводных сетях используются стандартные протоколы связи и обмена данными, а также серийно выпускаемые и общедоступные программно-технические средства.

В свою очередь, средой передачи данных в радиосетях являются радиоволны, которые могут приниматься любым приемником на относительно большом расстоянии от передатчика. Однако радиосигналы, передаваемые в системах обмена данными с использованием современных радиомодемов, не так доступны, как это может показаться на первый взгляд.

Во-первых, для организации перехвата злоумышленник должен точно знать номинал рабочей частоты, используемой для обмена данными. В случае соблюдения пользователями минимальных правил безопасности получение этой информации крайне затруднено. Передаваемые данные не могут восприниматься на слух, поэтому даже при использовании частотных сканеров для определения номинала рабочей частоты злоумышленник сможет только зафиксировать передачу сигналов, которые будут представляться как набор шумов, и не сможет произвести «привязку» (определить, что на данной частоте работает именно тот обьект, поиск которого ведется).

Во-вторых, оборудование использует специальные схемы модуляции сигнала и собственные преамбулы (структуру пакета данных). На практике это выливается в невозможность получения доступа собственно к передаваемой информации при отсутствии у злоумышленника соответствующего радиомодема или специального оборудования для анализа сигналов. В отличие от проводных модемов, распространение радиооборудования имеет известные ограничения, а все его пользователи регистрируются. В связи с этим вероятность легального приобретения оборудования злоумышленником практически равна нулю.

В-третьих, в большинстве радиосетей, особенно имеющих топологию типа «звезда», в которых обмен данными производится через БС, в отдельно взятой точке злоумышленник сможет принимать данные, передаваемые только в одном направлении. Это связано с принципами построения сети, в которой БС разворачивается на возвышенности, что обеспечивает возможность организации связи со всеми удаленными станциями сети. Злоумышленнику же вряд ли удастся разместить свое оборудование на такой выгодной позиции.

И наконец, в отличие от проводных средств связи, радиооборудование передачи данных может быть полностью развернуто в охраняемых помещениях, физический доступ в которые строго ограничен.

Совокупность всех перечисленных выше качеств делает радиосети обмена данными более безопасными по сравнению с технологическими проводными сетями связи.

Устойчивость к несанкционированному подключению к сети обмена данными

При подключении к сети обмена данными злоумышленник может ставить целью получение доступа к базам данных информационной системы или просто «просмотр» передаваемых данных. Это предполагает, что он должен располагать соответствующим терминалом, поддерживающим используемые в сети обмена данными протоколы. Такие терминалы вполне доступны, но решение второй части проблемы представляется не таким простым.

Перечисленные выше трудности, возникающие при организации перехвата, сопровождают и попытки получить доступ к работе в составе сети обмена данными. Кратко описанные ниже свойства применяемых протоколов связи и обмена данными в равной степени относятся к проводным и радиосетям и характеризуют их способности по обеспечению безопасности информации.

Большинство коммерческих пользователей синхронных систем (например, банков) используют протоколы «опроса» (например синхронный протокол SDLC), в которых заложены определенные возможности по обеспечению безопасности. Для того чтобы терминал распознавался системой, он должен быть внесен в «опросную таблицу», которая ведется и поддерживается на центральном компьютере. Несмотря на то, что система может самостоятельно распознавать новые термиалы и автоматически вносить их в таблицу, ее содержание постоянно контролируется администратором сети, который без труда может локализовать нового пользователя, получившего доступ к системе, и предпринять соответствующие меры. В случае если терминал не будет внесен в таблицу, он не сможет работать в составе сети.

Возможно, что профессиональный «крекер» или «хакер» сможет перепрограммировать компьютер таким образом, чтобы получать данные без внесения дополнительного адреса в «опросную таблицу», однако в этом случае он не сможет передавать свои данные в центральный компьютер (что в большинстве случаев является основной целью).

Попытки работы под «прикрытием» другого терминала за счет дублирования его идентификационого номера в любом случае приведут к генерации некорректных данных и подтверждений, получаемых центральным компьютером, что незамедлительно привлечет внимание администратора сети. На данном этапе достаточно просто выявить попытку получения несанкционированного доступа к работе в сети и предпринять соответсвующие меры для взятия работы под контроль или предотвращения доступа к сети. Поскольку основным условием успешного проникновения злоумышленника в сеть является скрытность, уже сам факт выявления попытки несанкционированного доступа делает его дальнейшие действия бессмысленными.

На практике выявить и локализовать злоумышленника в радиосети обмена данными намного проще, чем в проводной системе связи. В случае предоставления ему возможности продолжить работу в сети под контролем администратора, излучаемые его приемопередатчиком сигналы при посылке запросов и подтверждении приема сообщений могут быть легко запеленгованы (поскольку работа в сети управляется с БС администратором, последний может инициировать работу передатчика злоумышленника с необходимой периодичностью), а это существенно проще, чем определить точку подключения к проводной сети обмена данными.

Устойчивость к подавлению и воздействию помех

Подавление или постановка помех работе радиосистемы — задача существенно более сложная, чем физическое нарушение соединения в проводной системе, и для большинства коммерческих систем маловероятна.

Подверженность радиосигналов воздействию помех и возможность их подавления являются непреложным фактом. Однако, во-первых, злоумышленник должен точно знать номинал рабочей частоты системы обмена данными, установить который не так просто, поскольку передача ведется коротким сеансами. Во-вторых, факт появления помех немедленно выявляется администратором системы обмена данными, а источник излучения становится объектом пеленгования и локализации, в том числе при поддержке соответствующих организаций, контролирующих использование радиоспектра.

Физическая безопасность

Злоумышленнику гораздо проще незаметно перекусить кусачками пару проводов, чем поставить помеху радиосистеме, используя сложное и дорогостоящее специализированное оборудование, серьезно рискуя при этом быть пойманным. Работа кусачками займет несколько секунд, а установка и использование специального оборудования радиопротиводействия требует времени и крупных финансовых затрат. При этом такое воздействие не может быть продолжительным. Поэтому, как уже упоминалось выше, для обеспечения безопасности данных, передаваемых по кабельной линии связи, необходимо обеспечить контроль за линией на всей ее протяженности. В радиосистемах достаточно защитить небольшие помещения, в которых размещается приемопередающая аппаратура.

Таким образом, первое впечатление действительно обманчиво: присущая кабельным системам связи и обмена данными безопасность информации — такой же миф, как слабая защита данных в радиосистемах.

* * *

Мы рассмотрели особенности стационарных средств обмена данными. Вторая часть статьи будет посвящена подвижным радиосетям, а в третьей мы расскажем об использовании транковых систем. ■

Продолжение следует.