Технологическая радиосеть обмена данными УКВ-диапазона

как базовый элемент интеллектуальной электроэнергетической сети

В настоящей статье рассматриваются вопросы организации современных технологических радиосетей[1] сбора данных и управления УКВ-диапазона в энергетике, позволяющих создать единое информационное пространство для функционирования интеллектуальной электроэнергетической сети и обеспечить управляемость сетью на уровнях доставки и распределения электроэнергии. Технологическая радиосеть рассматривается как элемент обеспечения функционирования автоматизированных систем диспетчерского управления объектами электроэнергетики (АСДУЭ), коммерческого учета электроэнергии (АИИС КУЭ, АСКУЭ), технического учета электроэнергии (АСТУЭ), сбора аварийной информации (АССАИ) и аварийной защиты (АСАЗ), которые являются составными частями перспективной интеллектуальной электроэнергетической сети. Представленные в статье данные также актуальны для построения технологических радиосетей сбора данных и управления на объектах топливной и теплоэнергетики.

Сергей Маргарян
sm@rodnik.ru

Обмен данными в УКВ-диапазоне применяется для сбора данных и управления уже более 30 лет и на сегодня представляет собой наиболее зрелую и проверенную технологию, обеспечивающую надежное функционирование обслуживаемых объектов. На территории Российской Федерации для строительства узкополосных технологических радиосетей обмена данными выделены полосы радиочастот в диапазонах ОВЧ 146–148 МГц, 149,9–162,7625 МГц и 163,2–168,5 МГц[2] и УВЧ 403–410 МГц, 417–422 МГц и 433–447 МГц[3]. В настоящее время в указанных диапазонах построены и функционируют несколько тысяч технологических радиосетей, обеспечивающих работу объектов топливной, электро- и теплоэнергетики. Выбор аппаратных средств для данных сетей обусловлен особенностями обслуживаемых объектов, в первую очередь их территориальной распределенностью и необходимостью функционирования в реальном масштабе времени при невысоких требованиях к скорости обмена данными. Работающие в УКВ-диапазоне технические средства являются лучшим решением для организации обмена данными на малых и средних скоростях (300–64000 бит/с) на дальность до 100 км, а гибкость и простота их комплексирования и сопряжения с аппаратурой магистральной связи позволяет строить радиосети для объектов, имеющих протяженность в тысячи километров (электрические сети, трубопроводы, железные дороги).

Актуальность применения узкополосных радиосетей обмена данными серьезно возросла с принятием решения о создании интеллектуальной электроэнергетической сети в ОАО «Федеральная сетевая компания Единой энергетической системы» («ФСК ЕЭС»).

Средства обмена данными в интеллектуальной электроэнергетической сети

Интеллектуальная электроэнергетическая сеть (Smart Grid, «умная» или активно-адаптивная сеть) представляет собой распределительную сеть, которая сочетает в себе комплексные инструменты контроля и мониторинга, информационные технологии и средства коммуникации, обеспечивающие значительно более высокую ее производительность и позволяющие генерирующим, сбытовым

[1] Технологическая сеть связи (англ. private network) — предназначена для обеспечения производственной деятельности организаций, управления технологическими процессами в производстве. Технологии и средства связи, применяемые для создания технологических сетей связи, а также принципы их построения устанавливаются собственниками или иными владельцами этих сетей. [Федеральный закон «О связи» от 07.07.2003 N 126-ФЗ.]
[2] Решение Государственной комиссии по радиочастотам от 28 апреля 2009 г. № 09-03-01-1.
[3] Решение Государственной комиссии по радиочастотам от 11 декабря 2006 г. № 06-18-04-001.

и коммунальным компаниям предоставлять населению энергию более высокого качества. Элементы такой сети всегда существовали в электроэнергетической системе России, которая является одной из крупнейших в мире и реально может функционировать только при наличии надежной и разветвленной системы управления, контроля и мониторинга.

В системе управления, контроля и мониторинга применяются средства связи и обмена данными различных типов, которые включают в себя аппаратуру передачи данных по слаботочным медным и оптическим кабелям, проводам высоковольтных линий электропередачи, беспроводным каналам технологической связи и связи общего пользования, включая спутниковые. Выбор средства связи определяется функциональными требованиями подключаемого к сети объекта. Для связи с объектами «нижнего уровня» (счетчиками и устройствами телемеханики), не требующими передачи больших объемов информации, в настоящее время используются сети сотовой связи общего пользования GSM/GPRS/EDGE и узкополосые технологические радиосети обмена данными.

Сети сотовой связи GSM/GPRS/EDGE

Использование сетей сотовой связи общего пользования GSM/GPRS/EDGE для обеспечения функционирования автоматизированных систем в энергетике представляется весьма привлекательным, поскольку не требует серьезных начальных финансовых и временных затрат на развертывание инфраструктуры связи. Применяемые в таких сетях модемы имеют относительно низкую стоимость и достаточно надежны в эксплуатации. Разработчикам данной аппаратуры удалось решить практически весь комплекс проблем, связанных с подключением электросчетчиков и контроллеров к сети сотовой связи, основными из которых были следующие:

- Обеспечение постоянного доступа к приборам учета с применением пакетной передачи данных. Наилучшие результаты достигаются при использовании соединения по каналу EDGE («улучшенный» GPRS), обеспечивающего обмен данными со средней скоростью 30 кбит/с.
- Использование встроенной многоуровневой системы безопасности, включающей в себя:
  - защиту SIM-карты от ее использования не по назначению за счет применения автоматического ввода PIN-кода доступа или специальных SIM-карт с блокировкой по IMEI первого устройства;
  - применение имени точки доступа, выделенного GSM-оператором под конкретный проект с аутентификацией доступа;
  - использование специальных алгоритмов шифрования;
  - формирование VPN-туннеля между GSM-оператором и центром обработки данных;
  - применение дополнительного контроля идентификаторов при установлении TCP/IP-соединения и контроль используемых телефонных номеров при CSD-соединении.
- Повышение надежности канала передачи данных, включая:
  - подключение к сетям различных операторов сотовой связи и обеспечение автоматического перехода на SIM-карту резервного оператора с автоматическим возвратом на SIM-карту основного оператора в случае сбоев в работе сети сотовой связи;
  - переход на CSD-канал при неисправности GPRS/EDGE в рамках одного GSM-оператора;
  - передача SMS-сообщения при потере связи по каналам GPRS/EDGE;
  - обеспечение гарантированной и подтвержденной доставки информации;
  - контроль наличия питания и возобновление работы после его восстановления (модем должен автоматически устанавливать соединение при подаче питания);
  - выполнение автоматической перезагрузки в случае возникновения сбоев в работе как при установлении соединения, так и в процессе эксплуатации.

Однако широкие функциональные возможности применяемой аппаратуры не позволяют избавиться от ограничений, связанных с техническими возможностями собственно сотовых сетей связи общего назначения, и обеспечить функционирование ответственных автоматизированных систем, требующих работы в реальном масштабе времени.

Основными такими ограничениями являются:

- Отсутствие гарантии непрерывности связи. Основной причиной, по которой радиосети общего пользования не рекомендуется использовать для обеспечения работы ответственных систем, является непредсказуемость их функционирования. Работа радиосети сотовой связи в значительной степени зависит от текущей нагрузки (количества одновременно работающих абонентов). Изменения этой нагрузки предсказать очень сложно, поэтому даже в самых современных сетях сотовых операторов возможны отказы от обслуживания и задержки в предоставлении доступа к сети. Передача данных в режимах GPRS/EDGE для операторов сотовой связи является второстепенной, поэтому даже при незначительном возрастании голосового трафика выделяемые для обслуживания обмена данными ресурсы сотовой сети могут сокращаться.
- Относительно низкая надежность соединения. В связи с технологическими особенностями радиосетей сотовой связи второго поколения (2G, к этому поколению относятся все основные существующие сети операторов сотовой связи) невозможна гарантированная доставка отправленных сообщений. Доступ к радиосети в режимах GPRS/EDGE в процессе работы может периодически пропадать. Эта ситуация не изменится и после появления сетей связи третьего поколения, поскольку наряду с возрастанием скорости обмена и общей пропускной способности этих радиосетей пропорционально возрастет и нагрузка на них за счет обмена мультимедийной информацией (MMS, интерактивное телевидение, скоростной доступ в Интернет и т. п.).
- Отсутствие оперативности связи. Использование коротких сообщений SMS не гарантирует своевременную доставку информации для ее дальнейшей обработки. В этом случае автоматизация функций, связанных, например, с оценкой текущего состояния, выполняемой в интеллектуальной электроэнергетической сети в реальном масштабе времени, оказывается принципиально невозможной.
- Относительно короткий срок эксплуатации. Технологии сотовой связи бурно развиваются. В настоящее время практически все операторы сотовой связи в Российской Федерации ведут активные работы по развертыванию радиосетей третьего поколения (3G), а за рубежом уже созданы экспериментальные сети четвертого поколения (4G). С внедрением новых технологий потребуется модернизация средств сопряжения интеллектуальной электроэнергетической сети с сетью сотовой связи.
- Определенные трудности при использовании сотовых сетей общего пользования для обеспечения функционирования ответственных приложений интеллектуальной электроэнергетической сети связаны с созданием системы единого времени, которая должна быть общей для всех программно-технических средств, включая средства связи и передачи данных.

Поскольку развертывание перспективных сотовых сетей сопряжено с крупными финансовыми затратами, а их технические возможности существенно шире, операторы сотовой связи имеют все объективные основания для изменения тарифов в сторону их увеличения, что негативно скажется на эксплуатации созданной интеллектуальной электроэнергетической сети.

Узкополосные технологические радиосети обмена данными

Узкополосные технологические радиосети обмена данными свободны от ограничений, присущих сетям связи общего пользования. Современные технические средства позволяют создавать относительно недорогие, эффективные и гибкие технологические радиосети обмена данными, способные функционировать на протяжении многих лет с минимальным техническим обслуживанием, обеспечивая обмен данными в реальном масштабе времени. Типовая упрощенная схема коммутации технологической радиосети обмена данными представлена на рис. 1.

Источником данных на удаленном объекте является счетчик (группа счетчиков) или контроллер. Информация от источника принимается радиомодемом по стандартному интерфейсу (как правило, RS-232 или Ethernet). Радиомодем служит для преобразования поступающих цифровых данных в радиочастотный сигнал, который посредством радиопередатчика передается в пункт управления (например, диспетчерскую или полевой пункт). Здесь процесс

Рис. 1. Типовая упрощенная схема коммутации технологической радиосети обмена данными

обработки происходит в обратном порядке. Модем преобразует поступивший радиосигнал в цифровую форму, пригодную для его дальнейшей автоматизированной обработки.

В типовых приложениях обмен данными производится под управлением центрального объекта (топология «звезда»), работающего через базовую станцию по принятым для конкретной радиосети протоколам обмена данными.

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

Таким образом, создается радиосеть обмена данными с полностью детерминированными параметрами, исключающая флуктуации информационного потока, способные привести к сбоям в ее работе, и поддерживающая работу удаленных устройств в реальном режиме времени.

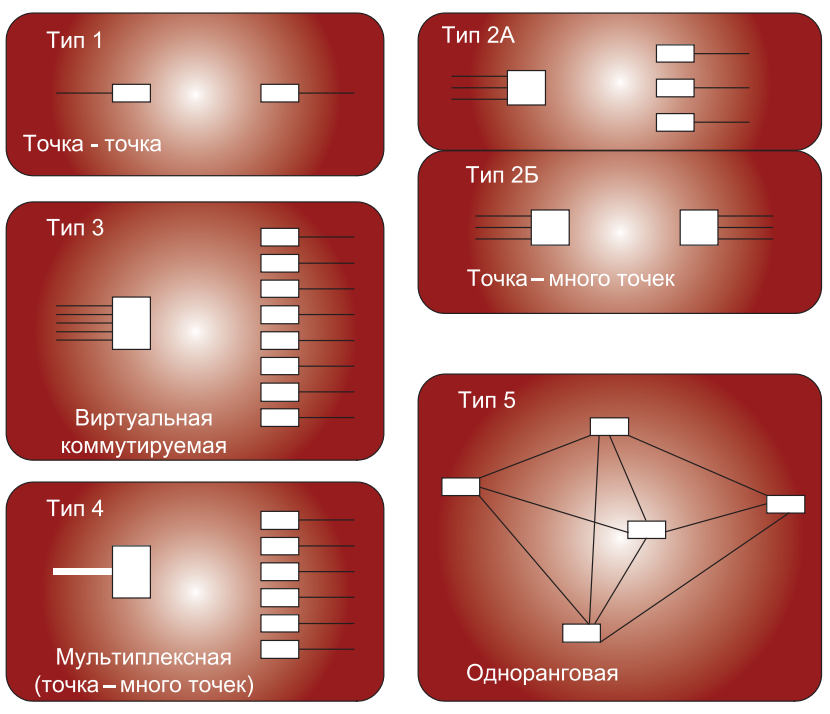

Рис. 2. Варианты построения технологических радиосетей обмена данными

Наиболее высокая надежность работы достигается в системах, в которых обеспечивается прямая радиовидимость между объектами, то есть радиосигнал беспрепятственно распространяется от передающей до приемной антенны. Номинально в создаваемых радиосетях зона радиовидимости с одной позиции имеет радиус 30 км на открытой местности и 10 км в условиях города со средней плотностью застройки. Минимальные и максимальные значения зависят от условий местности и могут отличаться на порядок. Обеспечение прямой радиовидимости относительно просто достигается в стационарных технологических радиосетях, но оказывается практически невыполнимым для подвижных радиосетей[4], в которых условия приема радиосигнала постоянно изменяются. В связи с этим при создании подвижных радиосетей применяется специальное радиотехническое оборудование, существенно отличающееся от используемого в стационарных радиосетях.

Обеспечение безопасности данных

Задача создания и эксплуатации интеллектуальной электроэнергетической сети напрямую связана с обеспечением безопасности циркулирующей в ней информации и исключением возможности несанкционированного внешнего воздействия на ее компоненты. Безопасность данных в радиосетях является одним из ключевых условий их использования, а строительство таких радиосетей осуществляется с учетом полного исключения или максимального затруднения компрометации передаваемой по ним информации. В радиосетях обмена данными широко применяются различные методы и способы защиты информации. Степень защиты данных оказывает непосредственное влияние на надежность радиосети и ее живучесть, поскольку постороннее вмешательство в работу может существенно снизить эти параметры. Ниже представлена информация о возможностях данных радиосетей противостоять основным угрозам: перехвату данных, несанкционированной работе в составе радиосети и радиоэлектронным помехам[5].

Вопросы обеспечения безопасности информации в сетях сотовой связи неоднократно рассматривались в специальной литературе и хорошо известны. Обеспечение безопасности является одной из основных задач оператора сотовой сети, который должен предпринимать все усилия для исключения компрометации циркулирующей в его сети информации. Однако следует отметить, что доступ к сотовой сети открыт для любого пользователя, поэтому сотовому оператору приходится сталкиваться и бороться с постоянно растущими угрозами и попытками несанкционированного использования ресурсов.

[4] Подвижные радиосети используются для управления, контроля и мониторинга параметров тока на промышленном горном и транспортном оборудовании (электровозы, экскаваторы, включая роторные, буровые станки).
[5] Вопросы противодействия профессиональным средствам радиоэлектронной борьбы и радиоэлектронного подавления в настоящей статье не рассматриваются.

Обеспечение безопасности данных в технологических радиосетях

Обеспечение безопасности является одним из наиболее важных требований к технологическим радиосетям обмена данными. Следует отметить, что защита данных в любой системе представляет собой непрерывный комплекс организационно-технических и специальных мероприятий, ни одно из которых в отдельности 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.

Уровень безопасности данных в технологической радиосети может быть сопоставим и даже выше уровня безопасности данных в проводных сетях связи.

Устойчивость к перехвату данных

На первый взгляд, перехват данных в проводных технологических сетях связи сопряжен с серьезными трудностями. Однако эта задача не так сложна для специалиста, имеющего соответствующую подготовку (подтверждением этому являются многочисленные успешные атаки хакеров[6] на информационные системы). Кабельная сеть прокладывается внутри здания или комплекса зданий. При этом отдельные сегменты могут укладываться в подвалах зданий, коллекторах и потернах, не контролируемых службами безопасности, и представлять собой потенциальные точки для несанкционированного подключения. Теоретически любой человек, знающий структуру кабельной сети, может получить доступ к ней в этих точках. После подключения к проводной сети 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.

Средой передачи данных в технологических 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.

Для организации перехвата необходимо точно знать номинал рабочей частоты, используемой для обмена данными. При соблюдении пользователями минимальных правил безопасности получение этой информации затруднено. Поскольку передаваемые данные не могут восприниматься на слух, то при использовании для определения номинала рабочей частоты доступных средств перехвата, например частотных сканеров, фиксируется только факт передачи сигнала на определенной частоте, который представляется как набор шумов. Определение принадлежности этого сигнала тому объекту, поиск которого ведется, без доступа к передаваемой информации оказывается практически невозможным.

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 соответствующего радиомодема или специального оборудования для анализа сигналов. В отличие от проводных модемов, распространение радиотехнического оборудования для технологических радиосетей имеет известные ограничения, а все его пользователи регистрируются. В связи с этим вероятность легального приобретения оборудования, которое может использоваться для обеспечения доступа к передаваемой в технологической радиосети обмена данными информации, практически равна нулю.

Большинство радиосетей, особенно имеющих топологию типа «звезда», в которых обмен данными производится через базовую станцию, в отдельно взятой точке могут принимать только данные, передаваемые в одном направлении (от базовой станции к удаленному объекту). Это связано с принципами построения сети, в которой базовая станция разворачивается на возвышенности и имеет высоко подвешенную приемо-передающую антенну, что обеспечивает возможность организации связи со всеми удаленными станциями сети. Для организации перехвата используемое для него оборудование необходимо разместить на такой же выгодной позиции, что в большинстве случаев оказывается невозможным. В противном случае обеспечивается перехват только данных от базовой станции, которые, в большинстве стационарных технологических радиосетей, представляют наименьший с точки зрения перехвата интерес (например, запросы, которые дают минимальное представление о работе сети и циркулирующих в ней данных).

В отличие от проводных сетей обмена данными, где кабельная инфраструктура и аппаратура для ретрансляции сигналов распределены на больших территориях, 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 и обмена данными в части перехвата информации.

Устойчивость к несанкционированному подключению

Основной целью несанкционированного подключения к сети обмена данными является получение доступа к работе в составе информационной системы или «просмотру» передаваемых данных. Для решения этой задачи требуется соответствующий терминал, поддерживающий используемые в сети обмена данными протоколы. Такой терминал может быть легко реализован на базе современного компьютера, но решение второй части задачи представляется не таким простым.

Перечисленные выше трудности с организацией перехвата возникают и при попытке получить доступ к работе в составе сети обмена данными. Кратко описанные ниже свойства применяемых протоколов связи и обмена данными в равной степени относятся к радио- и проводным сетям и характеризуют их способности по обеспечению безопасности информации.

В большинстве технологических радиосетей обмена данными используются протоколы «опроса», в которых заложены определенные возможности по обеспечению безопасности. 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 терминалы и автоматически вносить их в таблицу, содержание таблицы постоянно контролируется администратором сети и специальными программами, которые могут локализовать нового пользователя, получившего доступ к сети, и предпринять соответствующие меры по исключению возможности его дальнейшей работы. Если терминал не будет внесен в таблицу, он не сможет работать в составе сети.

Значительная часть стационарных технологических радиосетей используется для обслуживания строго определенного количества терминалов, поэтому появление в их составе новых вообще не предусматривается.

Профессиональный крэкер[7] или хакер может 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 несанкционированного подключения).

Попытки работы через технологическую радиосеть обмена данными под «прикрытием» другого терминала за счет дублирования его идентификационного номера приводят к генерации некорректных данных и подтверждений, получаемых центральным компьютером. Этот факт незамедлительно привлечет внимание администратора сети. На данном этапе достаточно просто выявить попытку получения несанкционированного доступа к работе в сети и предпринять соответствующие меры для предоставления контролируемой работы или предотвращения доступа к сети. Поскольку основным условием успешного проникновения в сеть является скрытность, уже сам факт выявления попытки несанкционированного доступа делает его дальнейшие действия бессмысленными.

На практике выявить и локализовать несанкционированную работу в технологической радиосети обмена данными намного проще, чем в проводной системе связи. В случае предоставления крэкеру или хакеру возмож-

[6] Хакер (от англ. hack — разрубать) — особый тип компьютерных специалистов. Компьютерные взломщики, т. е. люди, осуществляющие неправомерный доступ к компьютерам и информации.
[7] Крэкер (англ. cracker) — тип компьютерного взломщика: человек, взламывающий системы защиты информационных систем или создающий программные средства для взлома систем защиты. Вне профессиональной среды применяется общий термин «компьютерный взломщик» или чаще «хакер», что также часто не является правильным. В абсолютном большинстве случаев крэкер не располагает исходным кодом программы, поэтому программа изучается связкой дизассемблера и отладчика с применением специальных утилит.

ности продолжения контролируемой работы в сети излучаемые его приемопередатчиком сигналы при посылке запросов и подтверждении приема сообщений могут быть легко запеленгованы (а поскольку работа в сети управляется с базовой станции администратором, последний может инициировать работу передатчика злоумышленника с необходимой периодичностью), что существенно проще, чем определить точку подключения к проводной сети обмена данными.

Устойчивость к подавлению и воздействию помех

Подавление или намеренная постановка помех работе технологической радиосети обмена данными является существенно более сложной задачей, чем физическое нарушение соединения в проводной системе, и для большинства таких сетей маловероятно.

Подверженность радиосигналов воздействию помех и возможность их подавления являются непреложным фактом. Однако для выполнения этой задачи необходимо знать номинал рабочей частоты системы обмена данными, установить который не так просто, поскольку передача ведется короткими сеансами. Факт появления помех немедленно выявляется администратором радиосети, а источник излучения становится объектом пеленгования и локализации, в том числе при поддержке соответствующих организаций, контролирующих использование радиочастотного спектра.

Поэтому 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 не более 30 секунд, а установка и использование специального оборудования радиопротиводействия требует времени и крупных финансовых затрат, но при этом его воздействие не может быть продолжительным.

Таким образом, оперативно-технические возможности современных узкополосных технологических радиосетей обмена данными позволяют рассматривать последние как важный базовый элемент для построения интеллектуальных электроэнергетических сетей и обеспечения функционирования в их составе ответственных автоматизированных систем реального времени.

Литература

1. Гуревич В. И. Интеллектуальные сети: новые перспективы или новые проблемы? Ч. 1 // Электротехнический рынок. 2010. № 6 (36).
2. Дианов И. В. Типовые решения для каналов GPRS-связи в системах АИИС КУЭ розничного рынка электроэнергии // Информатизация и системы управления в промышленности. 2010. № 3 (27).