ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ В БЕСПРОВОДНЫХ СИСТЕМАХ БЕЗОПАСНОСТИ

Я. Мироненко
ООО «Аудит Сервис Оптимум»,
Владимирский Государственный Университет имени А.Г. и Н.Г. Столетовых

Беспроводные технологии прочно вошли в жизнь обывателя. Новые стандарты сотовой связи, беспроводная зарядка телефонов, Wi-Fi в каждом доме, корпоративные беспроводные сети… Вся эта масса навалилась на привыкшего к проводам российского человека и настойчиво требует своего места под солнцем.

Она (эта самая масса) его (это место) находит. Просто в некоторых отраслях, все еще сильно завязанных на отечественную промышленность, законы и стандарты, процесс внедрения беспроводных технологий затягивается. Например, в системах безопасности. Специфика отрасли не позволяет быстрое внедрение новшеств (вернее нормативные документы не позволяют), но один стандарт беспроводных систем все-таки развивается в этой области. Речь, разумеется, о радиоканале. По сути, развитие радиоканальных систем – это штандарт развития систем безопасности в целом в России. Эта сфера радует большим числом новинок, здесь проводятся интересные проектные решения, здесь осваиваются большие деньги, проводятся практические эксперименты.

Достоинств по сравнению с кабельными у беспроводных сетей масса:

- стоимость установки датчиков и извещателей снижается в разы;
- исключается необходимость профилактического обслуживания кабелей;
- уменьшается собственно количество кабелей;
- уменьшаются трудозатраты и время на монтаж и обслуживание системы;
- снижается стоимость системы за счет исключения кабелей;
- обеспечивается удобная модернизация системы при необходимости.

Получается, и денег сэкономили и трудозатраты уменьшили… Красота! Но наряду с этой лавиной положительных эмоций есть и неприятный осадок:

- помехозащищенность: беспроводные сети подвержены влиянию электромагнитных помех значительно сильнее, чем проводные;
- надежность связи: связь может исчезнуть при несвоевременной смене батарей питания, изменении расположения узлов сети или появлении объектов, которые вызывают затухание, отражение, преломление или рассеяние радиоволн;
- резкое падение пропускной способности сети при увеличении количества одновременно работающих станций и коэффициент использования канала;
- безопасность: возможность утечки информации, незащищенность от искусственно созданных помех, возможность незаметного управления технологическим процессом враждебными лицами;
- сложность внедрения: шеф-монтаж и наладка беспроводных сетей часто становится мукой даже для профессионалов.

Стоит отметить, что последний пункт стремительно уходит в прошлое. Крупные производители действительно пытаются упростить системы, сделать их более «дружелюбными». Не всегда опять же получается, но для начала (а я все-таки считаю ситуацию на сегодняшний день именно началом внедрения беспроводных сетей в системы безопасности) сойдет. Так что эта проблема исключительно на совести производителей. Она (совесть) выдержит.

Мы же обратимся к объявленной те-

ме – проблеме электромагнитной совместимости (ЭМС) в беспроводных системах. Изначально понятие электромагнитной совместимости относилось к радиотехнике и имело узкое смысловое значение – выбор частотного диапазона. А уже сейчас МЭК определяет ЭМС, как способность оборудования или системы удовлетворительно работать в данной электромагнитной обстановке без внесения в нее какого-либо недопустимого электромагнитного возмущения.

Все основные определения из ГОСТ 30372-95/ГОСТ Р 50397-92 уже были предложены читателям в статье «Вопросы электромагнитной совместимости в системах безопасности» (Алгоритм Безопасности. 2013. № 1). Но необходимо уделить внимание еще нескольким терминам, при этом опять постараемся максимально исключить из статьи сложные определения.

Термин помехи никуда не исчез и приобретает еще большее значение. Теперь основная цель – это обеспечение помехоустойчивости. Помехоустойчивость технического устройства (системы) – это его способность выполнять свои функции при наличии помех. Помехи есть, и от этого никуда не денешься. И все действия по обеспечению ЭМС – это необходимость работы с любой радиосистемой.

Условно все помехи можно разделить на два класса: естественного и искусственного происхождения. Помехи искусственного происхождения возникают в процессе человеческой деятельности. Помехи естественного происхождения не связаны с процессами жизнедеятельности человека и существуют независимо от них. Помехи искусственного происхождения, в свою очередь, делятся на непреднамеренные и организованные. Непреднамеренные помехи возникают в процессе использования человеком различного рода устройств, генерация помех которыми является естественным следствием их функционирования. Организованные помехи создаются искусственно с целью ухудшения функционирования или вывода из строя радиоэлектронных средств (РЭС). Мы не будем останавливаться на организованных помехах. Тема информационной безопасности, безусловно, интересна, но требует отдельного обстоятельного разговора.

С практической точки зрения у помехи должен быть источник (источник искусственного или естественного происхождения, который создает или может создать электромагнитную помеху) и рецептор (техническое средство, реагирующее на электромагнитный сигнал и (или) электромагнитную помеху). Часто все так переплетено, что не знаешь где рецептор, а где источник. Нормальная работа в таких условиях – это и есть основная задача обеспечения ЭМС.

Тема электромагнитной совместимости в беспроводных сетях требует глубокого знания вопроса и физики распространения радиоволн. Конечно, можно не задумываться над этими вопросами и целиком положиться на производителей. Варианты готовых решений регулярно появляются на рынке, выбор есть. Но если мы говорим о радиоканале, то надо понимать, что электромагнитная обстановка на каждом объекте уникальна. И все готовые решения, предлагаемые производителями, в лучшем случае подходят для очень и очень небольших пространств. Любой же серьезный объект требует проекта и оценки электромагнитной обстановки (ЭМО). Часть необходимых знаний, надеемся, можно почерпнуть и в этой статье.

Физика процесса распространения радиоволн подробна была описана в статье «Радиоканал системы передачи извещений» (Алгоритм Безопасности. 2004. № 2). Изложенного в ней вполне достаточно для понимания принципа действия всех существующих систем и подхода к обеспечению помехоустойчивости. В беспроводных системах производители никак не могут закрыть глаза на ЭМС, поэтому все схемотехнические мероприятия уже включены в стоимость оборудования. Покупая радиопередающее (или приемное) устройство, вы уже оплачиваете специальные схемы умножителей с подавлением кратных частот, каскады фильтров, устройства для экранирования и компенсации помех, шумоподавители. Однако всего этого часто недостаточно. И уж тем более этого недостаточно для создания больших радиосетей. Здесь необходимо специальное оборудование, требующее больших капиталовложений. И не стоит думать, что достаточно будет одиночных инвестиций. Электромагнитная обстановка постоянно изменяется, и система должна модернизироваться вслед за ней.

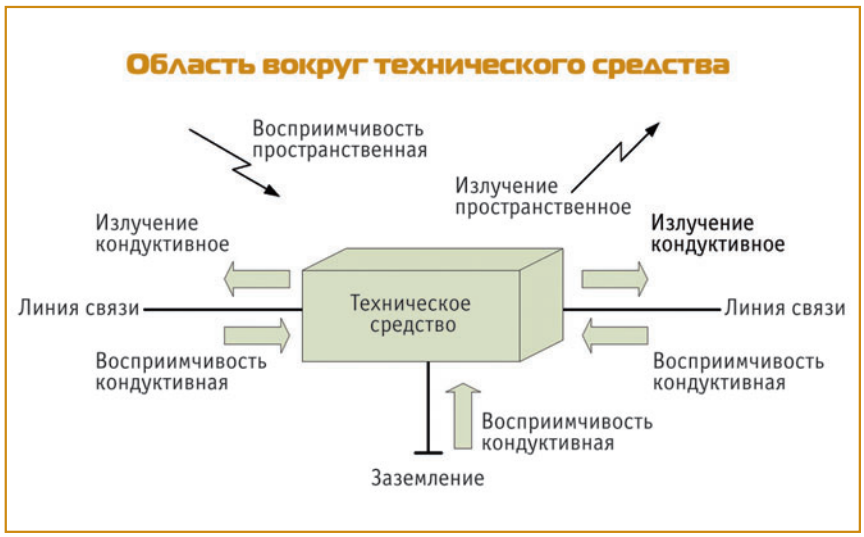
Условно разделим системы безопасности, использующие радиоканал, на собственно беспроводные и использующие беспроводную связь только для консолидации разбросанных по объекту (городу, области) небольших составляющих систем. И тот и другой случай достаточно распространен на практике. Обеспечение ЭМС внутри объекта и в условиях открытой местности (или городской застройки) – несколько разные задачи.

Электромагнитная обстановка на конкретном объекте хороша тем, что она практически не меняется. Да, возможна масштабная реконструкция зданий, введение новых беспроводных систем внутри предприятия, появление наводок от вновь устанавливаемого силового оборудования. Как правило, все это прогнозируемо, и система строится с учетом всех этих возможных изменений.

Ситуация, правда, осложняется тем, что в большинстве случаев в реальных условиях при проектировании специалисты располагают неполной информацией о проектируемых, вводимых в эксплуатацию или уже функционирующих на предприятии радиосистемах. Спектральные характеристики радиосигналов в значительной степени зависят от таких параметров, как частота дискретизации, скорость передачи данных, тип используемой модуляции. Если неизвестен хотя бы один из вышеперечисленных параметров, то мощность мешающего сигнала будет носить характер априорной неопределенности. Что в свою очередь может привести к печальным результатам при запуске системы.

Немного остановимся на внутриобъектовой ЭМС. Для ее обеспечения используют следующие принципы разделения сигналов (излучений) радиоэлектронных средств: частотное, временное и простран-

Рис. 1. Электромагнитная обстановка (ЭМО) вокруг технического средства (ТС) (http://bre.ru/security/21099.html)



ственное. Первый из названных методов состоит в банальном выборе различных частот для различных радиосистем предприятия. Просто и эффективно. Система пожарной безопасности использует один спектр, а система телемеханики другой. И все было бы хорошо, если бы системы безопасности использовали собственный, выделенный исключительно для них диапазон. Но все системы, так или иначе, используют частоты общего пользования. Мы остановимся на этом подробней чуть позже. Пока примем как факт, что подбор разнесенных частот не всегда возможен. В этом случае используется временное разнесение излучения РЭС, при которых работа некоторых РЭС осуществляется в различные не перекрывающиеся интервалы времени. Отличная альтернатива, но системы безопасности и построены для того, чтобы срабатывать в любое время. Теперь посмотрим, что предлагает нам пространственное разнесение.

Пространственные параметры электромагнитной помехи характеризуются образованием «зоны мешания». Под «зоной мешания» понимают область пространства, в пределах которой уровень энергии и частотный спектр излучаемого техническим средством (ТС) электромагнитного поля не позволяет одновременно использовать другие ТС без снижения качества их функционирования. Размеры «зоны мешания» зависят от полосы частот, в которой генерируется поле, его энергетического уровня, а также способа его излучения и окружающих условий распространения. Соответственно, объекты надо разместить в пространстве таким образом, чтобы их «зоны мешания» не пересекались. Часто весь объект – это одна большая «зона мешания», что делает практику пространственного разнесения не всегда возможной.

Перечисленные решения проблемы ЭМС принято определять как организационные мероприятия по обеспечению электромагнитной совместимости.

Рассмотрим меры другого плана. Можно уменьшить помехи, применяя на выходе приемника дополнительные специальные фильтры, уменьшающие уровень излучения за пределами основной полосы частот, которую занимает передаваемый сигнал. Другой метод состоит в повышении развязки между антеннами и фидерами РЭС, расположенными на одном объекте. Ну и еще один интересный момент – это применение электромагнитных экранов.

На практике для увеличения электромагнитной развязки между антенно-фидерными устройствами РЭС опять-таки применяется метод пространственного разнесения. Данное решение не всегда является возможным, как уже отмечалось. Это обуславливается дополнительным рядом причин: трудностями, связанными с установкой связных мачт в условиях сложного территориального рельефа, ограничениями, связанными с инженерно-геологическими условиями местности, с классификацией по ветровому району и т.д.

Проблема размещения антенн различных диапазонов на ограниченной территории является сложной задачей и решается в настоящее время недостаточно эффективно даже для GSM диапазона. Достаточно сложно провести физическое моделирование для каждого отдельного случая ввиду большого количества источников как первичных, так и вторичных излучателей при их различном режиме включений и выключений.

Повышение развязки между антеннами может обеспечиваться применением металлоконструкций опор с четко заданными параметрами, что очень сложно реализуется в реальных условиях при развертывании сетей с достаточно большим количеством узлов.

Итак, сформулируем основные методы повышения развязки, зная основные механизмы возникновения помех в антенно-фидерных трактах различных радиотехнических систем:

- оптимальное взаимное расположение антенн на приемно-передающих радиотехнических обьектах;
- применение поляризационного разнесения (использование близкорасположенных излучателей с различным типом поляризации);
- учет при размещении на объекте направленных свойств антенн, а также влияния металлоконструкций опор;
- использование экранирующих свойств элементов металлоконструкций опоры, а также дополнительных экранирующих структур.

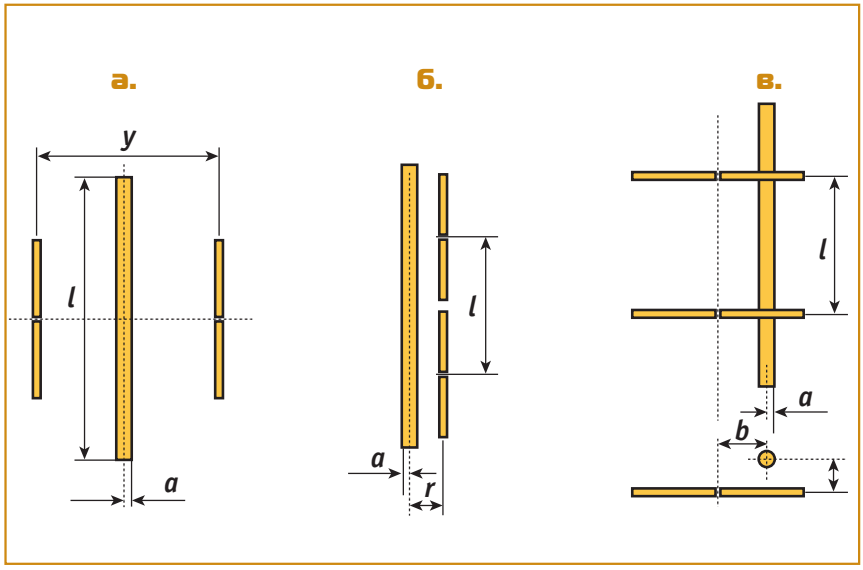
Остановимся подробнее на последнем методе. Металлическая антенная опора оказывает влияние, как на характеристики отдельной антенны, так и на характеристики развязки между антеннами при их размещении на общей опоре или при близкорасположенных опорах различных антенн. Причем влияние металлоконструкций может как увеличивать, так и уменьшать уровень развязки.

Как правило, выбор происходит между следующими основными вариантами взаимного расположения антенн и металлоконструкций:

1) два вертикальных симметричных антенных вибратора, разнесенных по горизонтали и расположенных на одной высоте по обе стороны от металлоконструкции, которая представляет собой вертикально ориентированный цилиндрический проводник *(рис. 2а)*;
2) два вертикальных симметричных вибратора, разнесенных по вертикали и расположенных вблизи вертикально ориентированного цилиндрического проводника *(рис. 2б)*;
3) два горизонтальных симметричных вибратора, разнесенных по вертикали и расположенных вблизи вертикально ориентированного цилиндрического проводника *(рис. 2в)*.

Применение помехоподавляющих фильтров – основной способ ослабления кондуктивных помех в цепях управления и электропитания РЭС. Для подавления таких помех в основном используют различные виды LC-фильтров, состоящие из Г-, Т- и П-образных звеньев, продольные ветви которых содержат индуктивности, а поперечные – емкости. Помехоподавляющие фильтры включают как можно ближе к источнику помехи на пути ее распространения к рецептору помехи. Эффективность фильтра характеризуется параметром ослабления помехи в месте ее влияния на рецептор. Некоторый эффект

Рис. 2. Примеры взаимного расположения металлоконструкций и антенн
(Управление радиочастотным спектром и электромагнитная совместимость радиосистем / Под редакцией д.т.н., проф. М.А. Быховского. Москва, 2006. С. 317)



может также дать включение дополнительного фильтра на входе РПМ.

Часто возникает ситуация (особенно на действующих объектах), когда на одну антенну объединены сразу несколько приемных устройств. Тогда для уменьшения помех, наряду с фильтрами, используют ферритовые циркуляторы, пропускающие с минимальными потерями сигнал радиопередатчика (РПД) в антенну и препятствующие прохождению его на выходы других РПД многоканальной системы. Кроме этого положительного эффекта, использование циркуляторов повышает надежность работы РПД, так как циркуляторы поглощают также собственный сигнал, отраженный от антенны в случае ее рассогласования или поломки.

Снижение чувствительности радиоприемника (РПМ), как уже отмечалось, в основном решается при разработке аппаратуры на схемотехническом уровне. Конструктивно различные РЭС выполняются с достаточно высокой эффективностью экранирования корпусов и других конструктивных узлов и элементов, что обеспечивает выполнение требований к электромагнитной восприимчивости. Однако в условиях неординарной электромагнитной обстановки при недостаточной эффективности других мер для обеспечения требований по ЭМС могут использоваться дополнительные электромагнитные экраны. При этом целью экранирования является либо зашита оборудования от воздействия внешних полей, либо, напротив, локализация излучения каких-либо средств, препятствующая проявлению этих излучений в окружающей среде.

Установка дополнительных экранов в случае необходимости применяется в местах размещения передающего и приемного оборудования, в трассах (канатах) прокладки высокочастотных фидеров и т.д. Наряду с обеспечением ЭМС РЭС применение электромагнитных экранов позволяет решать и ряд других задач, среди которых защита информации в помещениях и технических каналах, защита персонала от повышенного уровня электромагнитных полей и т.д.

Совсем другое дело – это обеспечение ЭМС в условиях прохождения радиоволной городской среды. Строительство новых зданий и предприятий, работа в одних частотах с другими системами, появление регулярных искусственных помех – здесь уже не обойтись организационными мероприятиями, нужно искать другие пути. В таких условиях создание и содержание надежной сети связи требует постоянных усилий на весь период ее эксплуатации.

Первая проблема, с которой сталкиваются при создании широкой сети – это выбор частотного диапазона. Выбор частот для системы – сложная и нетривиальная задача. Самый главный выбор – какой частотный диапазон взять за основу. Назначение радиочастот для вводимых в эксплуатацию РЭС осуществляет Государственная комиссия по радиочастотам (ГКРЧ). Возможны следующие варианты: CB (частоты 26945 кГц и 26960 кГц), LB (33-48 МГц), VHF (146-173 МГц) или UHF (433-470 МГц). Проблема этой альтернативы не раз описывалась и на страницах нашего журнала. Поэтому кратко изложим основные преимущества, чтобы освежить их в памяти. Наибольшее распространение для систем безопасности получили два диапазона частот – CB-канал и UHF-канал.

CB диапазон начал применяться гораздо раньше. Решением комиссии ГКРЧ (протокол № 170 от 30.12.88) частоты 26945 кГц и 26960 кГц общего пользования были выделены для охранных систем. Регистрировать оборудование для работы в этих частотах не требуется. Антенны для этого диапазона достаточно громоздки, и тут уже ничего не поделаешь – чем габаритней антенна, тем она эффективней. Зато оборудование остаточно надежно и относительно недорого стоит. Дифракция волн этого диапазона на различных строениях достаточно велика, поэтому обеспечена хорошая проникающая способность через строительные конструкции. Из недостатков можно отметить высокий уровень индустриальных помех и зависимость от активности Солнца.

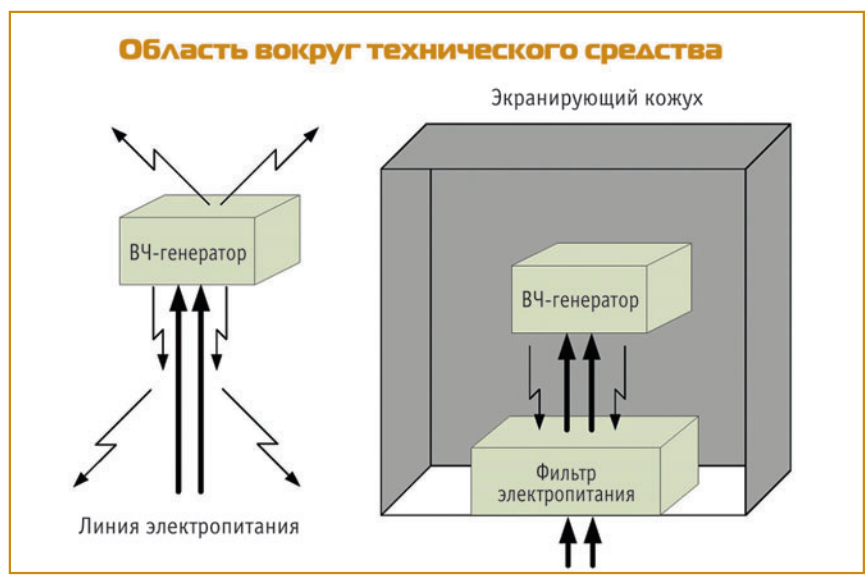
UHF диапазон широко развивается в последнее время. Его основной недостаток – это ограничение мощности передатчика до 10 мВт. Конечно, мощность передатчика не всегда является определяющим фактором, но дальность распространения волны сильно от нее зависит. Впрочем, практически все производители отдают предпочтение именно этому диапазону частот. Здесь и уровень индустриальных помех пониже, и антенны при тех же размерах более эффективны. Естественно, что ограничение мощности передатчика требует применения направленных антенн и создания более густой ретрансляционной сети. Но для них (производителей) это даже выгодно. Еще один серьезный недостаток этого диапазона – его популярность. Помехоустойчивость все-таки определяется именно избирательность частотного диапазона и зависит от соседей по нему.

Другая серьезная проблема при построении сети в городской среде – это дальность распространения сигнала. Часто заявленные 10-15 км оказываются не совсем достоверными. И реальная дальность сигнала хорошо если переваливает за 5 км. Поэтому и возникает необходимость в ретрансляции. Есть и другие способы увеличения дальности, никто не спорит. Можно увеличить радиус прямой видимости, можно получить выделенный частотный спектр, но не всегда это реально. А ретрансляция возможна практически всегда. Другое дело, что цепочки ретрансляторов желательно делать дублирующими – это увеличивает надежность системы и оптимизирует трафик в сети. И еще один интересный момент – многочастотная ретрансляция. Работа сразу с несколькими радиоканалами увеличивает помехоустойчивость в разы.

Ну и последние организационные моменты для разветвленной сети – протокол передачи данных должен иметь помехоустойчивое кодирование, а длительность сообщения не должна превышать десятой доли секунды. В этом случае мы надеемся получить на выходе почти не искаженный сигнал.

Помимо помех искусственного происхождения, существуют и более естественные «проблемы». В прошлой статье подробно расписывались источники помех

Рис. 3. Применение электромагнитного экрана (http://bre.ru/security/21099.html)



и методы защиты от импульсного перенапряжения. Потенциально каналы РЭС более уязвимы для молний и нуждаются в грамотно организованной грозозащите. Подверженные ударам молний антенны, помехи, создаваемые в эфире, непосредственная угроза для дорогой сети ретрансляторов и пунктов приема данных – даже небольшая гроза может наделать много бед. Поэтому для систем с высокими требованиями к надежности (а системы безопасности к таковым без сомнения относятся) необходимо не просто организовать грозозащиту. Нужно также организовать максимальное дублирование каналов передачи информации. Хорошо построенная сеть ретрансляторов и разнесенные пульты ПЦН – это залог успешной доставки тревожного сообщения.

Если мы немножко пофантазируем и представим будущее развитие беспроводных сетей в системах безопасности, то, так или иначе, придем к трем сетевым стандартам: Bluetooth [Specification] на основе стандарта IEEE 802.15.1, ZigBee [ZigBee] на основе IEEE 802.15.4 [IEEE] и Wi-Fi на основе IEEE 802.11 [Vieira, ANSI]. Основное внимание сейчас направлено на развитие именно стандарта IEEE 802.11. Разработкой и совершенствованием стандарта занимается рабочая группа по беспроводным локальным сетям (Working Group for Wireless Local Area Networks) комитета по стандартизации Института Инженеров Электротехники и Электроники (Institute of Electrical and Electronic Engineers, IEEE). Однако, для нас интересней другой промышленный стандарт – ZigBee, который изначально разрабатывался как низкоскоростной канал связи для объединения в сеть различных датчиков. Применительно к безопасности это могут быть датчики охранной и пожарной сигнализации. Этот стандарт определяет работу на частотах 2.4 ГГц (в мире, не лицензированная частота), 915 МГц (Американский континент) и 868 МГц (Европа) диапазон ISM. Применение сетей ZigBee в Российской Федерации в частотном диапазоне 2,405-2,485 ГГц не требует получения частотных разрешений и дополнительных согласований (Решение ГКРЧ при Мининформсвязи России от 07.05.2007 № 07-20-03-001).

У систем, работающих на частоте 2,4 Ггц наибольшая проблема – это дальность распространения. Проникающая способность волн этого диапазона через строительные конструкции достаточно низкая, энергия сравнительно небольшая. Получается, что сегодня этот формат возможен лишь для очень и очень небольших объектов (порядка 15 метров в округе от ПКП). Но в перспективе предлагается использовать другой подход. Изначально стандарт ZigBee разрабатывался именно как ретранслирующий сам себя. Основная особенность технологии ZigBee заключается в том, что она при малом энергопотреблении поддерживает не только простые топологии сети, но и самоорганизующуюся и самовосстанавливающуюся ячеистую (mesh) топологию с ретрансляцией и маршрутизацией сообщений. Каждый извещатель, датчик, прибор одновременно становится также ретранслятором и закладывает свой «кирпичик» в обеспечение надежной связи. При этом, даже в случае выхода из строя одного из устройств, цепочка, за счет большого количества перекрытий ретрансляционных зон, сохраняется. С точки зрения обеспечения ЭМС такой подход получается практически идеальным.

Другой разговор, что реализовать его непросто:

- возникают проблемы надежности работы совмещенного с извещателем ретранслятора;
- проблема надежности электроснабжения;
- вопрос стоимости данной системы;
- лучшая работа сетей на более низких частотах (815 Ггц и 916 Ггц);
- требования к «густой» топологии – сам принцип работы стандарта не позволяет с помощью него реализовывать радиоканал между объектами, расположенными на значительных расстояниях друг от друга.

При нынешнем развитии технологии такая система станет очень дорогой и очень громоздкой. Но промышленные стандарты постоянно развиваются. Уже сейчас ZigBee может активироваться (то есть переходить от спящего режима к активному) за 15 миллисекунд или меньше, задержка отклика устройства может быть очень низкой. При этом ZigBee большую часть времени находится в спящем режиме, уровень потребления энергии очень низок, благодаря чему достигается длительная работа от батарей. Возможно, этот стандарт потеснит многие из существующих сегодня радиоканальных ОПС. Ведь почти все они разработаны вне каких-либо стандартов. У каждого производителя – свои протоколы обмена, и заменить имеющиеся на объекте беспроводные датчики на оборудование другого производителя невозможно. Если стандарт ZigBee получит распространение и избавится от перечисленных выше проблем, что вполне вероятно, то заказчик получит возможность использовать в системах ОПС практически любые датчики на выбор.

Если рассматривать альтернативу применения радиоканала в целом, то на ум приходит только инфракрасные каналы. Инфракрасный канал также не требует соединительных проводов, так как использует для связи инфракрасное излучение. Главное его преимущество по сравнению с радиоканалом – нечувствительность к электромагнитным помехам, что позволяет применять его, например, в производственных условиях, где всегда много помех от силового оборудования. Правда, в данном случае требуется довольно высокая мощность передачи, чтобы не влияли никакие другие источники теплового (инфракрасного) излучения. Плохо работает инфракрасная связь и в условиях сильной запыленности воздуха.

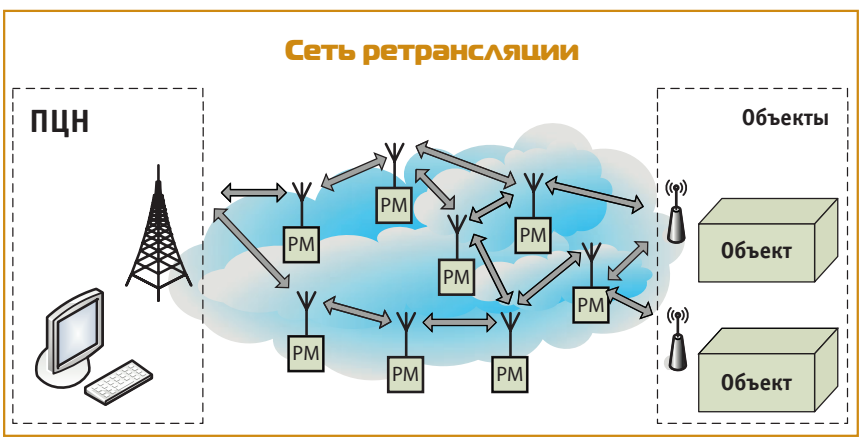
Инфракрасные каналы делятся на две группы:

- Каналы прямой видимости, в которых связь осуществляется на лучах, идущих непосредственно от передатчика к приемнику. При этом связь возможна только при отсутствии препятствий между компьютерами сети. Зато протяженность канала прямой видимости может достигать нескольких километров.
- Каналы на рассеянном излучении, которые работают на сигналах, отраженных от стен, потолка, пола и других препятствий. Препятствия в данном случае не помеха, но связь может осуществляться только в пределах одного помещения.

Едва ли можно говорить о широком применении инфракрасных каналов в системах безопасности. Проблемы их внедрения – это в первую очередь условия их применения, чаще всего неприемлемые.

На этом наш обзор заканчивается. Не думаю, что можно в одной статье осветить

Рис. 4. Организация ретрансляционной сети



все проблемы ЭМС в беспроводных сетях. Тут не справляются даже многотомные учебники высшей школы. Но задача этой статьи – обозначить суть проблемы и элементарные пути ее устранения. Данные в дополнение к непременной составляющей любой настройки радиоаппаратуры – немного покрутить и поперемещать антенну (хорошо обоснованный, кстати, физический эксперимент, основанный на явлении наложения волн).

Надежность и помехоустойчивость беспроводных систем все еще не позволяют им стать серьезной альтернативой для кабельных систем. Да и при передаче радиоканалом на дальние расстояния рекомендуется использовать дублирующий проводной канал. Оно так надежней получается. Можно, конечно, оставаясь в беспроводной сфере, использовать GSM-передачу данных. Но тут целая куча своих недостатков: продолжительное время установления соединения, низкая надежность коммутационного оборудования и необоснованные сбои при установлении этого самого соединения. Да и плата за пользование CSD немалая. Поэтому беспроводные системы безопасности не спеша развиваются в русле радиоканала. А вместе с ними развивается и электромагнитная совместимость, повышая надежность этих ответственных за жизнь и имущество людей систем.

ЛИТЕРАТУРА

1. *Управление радиочастотным спектром и электромагнитная совместимость радиосистем. Учебн. пособие // Под ред. д.т.н., проф. М.А. Быховского. – М.: Эко-Трендз, 2006. – 376 с.*
2. *Малков Н.А. Электромагнитная совместимость радиоэлектронных средств. Учеб. пособие // Н.А. Малков, А.П. Пудовкин. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2007. – 88 с.*
3. *Актуальные вопросы исследований распространения радиоволн, электромагнитной совместимости, антенно-фидерных устройств, средств радиосвязи и радиовещания. Учеб. пособие // Под ред. Г.И. Трошина. – М.: САЙНС-ПРЕСС, ИПРЖР, 2002. – 128 с.*
4. *Дробышев В. Радиоканальные системы ОПС дальнего радиуса действия. Проблемы внедрения и эксплуатации в условиях города // Алгоритм Безопасности. – 2006. № 6.*
5. *Белкин В. Радиоканал системы передачи извещений // Алгоритм Безопасности. – 2004. № 2.*
6. *Вахпаков В. Обеспечение защиты информации от непреднамеренного воздействия техническими средствами // Специальная техника. – 2007. № 2.*
7. *Мироненко Я. Вопросы электромагнитной совместимости в системах безопасности // Алгоритм Безопасности. – 2013. № 1.*
8. *Олимпиева И. Проблемы ЭМС цифровых радиосистем в корпоративных сетях технологического назначения // Технологии и средства связи. – 2008. № 2.*
9. *ГОСТ 30372-95 (ГОСТ Р 50397-92). Совместимость технических средств электромагнитная. Термины и определения. Принят Межгосударственным советом по стандартизации, метрологии и сертификации 12 октября 1995 г. Постановлением Госстандарта России от 15 мая 1996 г. № 308 ГОСТ 30372-95 введен в действие.*