Критерии надежности беспроводных охранно-пожарных систем

М.С. Левчук,
руководитель департамента маркетинга и продаж ЗАО "Аргус-Спектр"

Бурное развитие беспроводных технологий в конце XX века привело к созданию целого ряда радиосистем охранно-пожарной сигнализации. Однако первоначальные разговоры о том, что радиосистемы полностью заменят традиционные проводные системы, позднее сменилась более трезвыми оценками. Получив к концу 80-х годов широкое распространение в Европе и Америке, радиосистемы, однако, снискали себе дурную славу среди профессионалов: прежде всего, по причине низкого качества компонентов, входивших в состав радиосистем того времени, а, следовательно, высокого уровня ложных тревог. Неудивительно, что многие годы охранно-пожарные радиосистемы рассматривались как "любительские", пригодные только для использования на объектах с низкой степенью риска технически подготовленного взлома (загородные дома, квартиры и т.д.). Применение же радиосистем для охраны действительно важных объектов носило эпизодический характер.

В начале XXI века ситуация начала меняться к лучшему. Появление новой элементной базы и современных протоколов доступа к среде качественно изменили характеристики радиосистем. И сегодня производители и инсталляторы охранно-пожарной техники приходят к общему мнению, что перед радиосистемами последнего поколения открываются области применения, которые ранее считались "вотчиной" проводных охранно-пожарных систем.

В настоящий момент на рынке представлено множество радиоканальных внутриобъектовых систем как российского, так и зарубежного производства. Ответить на вопрос о том, какой же должна быть по-настоящему надежная радиосистема непросто. И все же, существует ряд принципиальных технических характеристик, анализ которых может помочь специалистам в области охранно-пожарной техники в выборе той или иной радиосистемы.

Помехоустойчивость

В число параметров, определяющих помехоустойчивость радиосистемы, входят такие параметры, как:

- количество частотных диапазонов;
- количество частотных каналов;
- автовыбор резервных каналов;
- автоматическая регулировка мощности излучения.

Рассматривая данный пункт, на наш взгляд, будет интересно обратиться к опыту европейских центров сертификации. Впервые нормативные документы, регламентирующие функционирование охранно-пожарных радиоканальных систем, появились в Германии уже в 1994 году. И с тех пор работа не прекращалась ни на один год. Достаточно заметить, что вначале следующего года ожидается появление новой части известного стандарта EN-54, который будет посвящен радиоканальным системам.

В соответствии с европейской классификацией, существует три класса охранных проводных и радиоканальных систем, отличающиеся между собой, прежде всего, по степени риска технически подготовленного взлома:

- класс А: низкая степень риска; объекты частного пользования (загородные дома, квартиры);
- класс В: средняя степень риска; объекты общественного пользования (магазины, учебные заведения);
- класс С: высокая степень риска; объекты государственной важности (музеи, исторические памятники).

Представим себе типичную ситуацию на объекте, находящемся под охраной охранно-пожарной радиосистемы. Время от времени пропадает связь с тем или иным радиоустройством. Скорее всего, причиной является не преднамеренное саботирование работы системы, а работа других приборов и систем на выбранном при установке системы канале связи (литере). Напомним, что диапазон частот 433 и 868 МГц является нелицензируемым, и его используют не только охранно-пожарные радиосистемы, но и бытовые устройства: переносные радиостанции, игрушки, шлагбаумы и т.д. В зависимости от класса, радиосистемы должны реагировать по-разному:

- класс А: индикация о временной потери связи с радиоустройством системы отсутствует;
- класс В и С: радиосистема обязана максимально использовать все возможные способы доставки сигнала и только после этого передать сигнал "Тревога".

Например, извещатель, не получив квитанцию от приемно-контрольного прибора после передачи тестового сигнала (квитирование возможно только в системе с двухсторонним протоколом), немедленно меняет частотный канал, мощность излучения, периодичность выхода в эфир и т.д. Если связь не может быть восстановлена даже после всех упомянутых действий, то в данном случае имеет место преднамеренное саботирование работы системы.

Криптозащита

В последнее время автомобильные кражи все чаще совершаются с применением, так называемых, "грабберов", которые записывают, а в дальнейшем воспроизводят радиосигналы "Снятие". Для большинства автомобильных сигнализаций использование односторонней радиоканальной связи (передатчик находится в носимом хозяином автомобиля брелоке, а приемная часть - в охраняемом автомобиле) оправдано, так как время работы в эфире ограничено одной - двумя посылками, а охраняемый объект (автомобиль) постоянно перемещается.

Рассматривая вопросы применения охранно-пожарных радиосистем в данной статье, мы, прежде всего, говорим об охране стационарных объектов. Следовательно, необходимо принимать во внимание тот факт, что злоумышленник может скрытно на протяжении длительного времени проводить сканирование, запись и анализ всех сигналов радиосистемы. Поэтому необходимо обеспечить криптографическую защиту сигналов, т.е. при каждой передаче контрольных сигналов и сигналов управления участники обмена должны, помимо использования динамически изменяемые ключей, обеспечить невозможность саботирования системы с использованием предварительно записанных сигналов системы.

Число адресуемых устройств

Емкость радиосистемы (число адресуемых устройств) во многом определяется способностью системы регулировать объем передаваемой информации, а также мощностью излучения всех радиоустройств. Чем больше информации необходимо передать и чем сильнее устройства "экранируют" друг друга, тем меньшее число устройств могут работать на одном частотном канале связи. Например, использование механизмов, исключающих передачу одного и того же сигнала "Тревога" несколько раз, существенно снижает объем передаваемой информации, а, следовательно, увеличивает максимальное число совместно работающих устройств.

Время работы радиоизвещателей от источника питания

Бурное развитие беспроводных технологий за последние годы подтолкнуло производителей радиоэлектроники на создание компонентов, существенно снизивших энергопотребление радиоустройств, таких как микропроцессоры, приемо-передатчики и т.д. Это, несомненно, помогло разработчикам охранно-пожарных

радиосистем значительно увеличить продолжительность работы извещателей от батарей. Кроме того, специалист заметит, что существует ряд алгоритмов, которые могут существенно увеличить время работы периферийных устройств от источников питания. А именно:

- алгоритм регулирования мощности излучения;
- передача сообщений с квитированием;
- режим работы "День"/"Ночь".

Температурный диапазон

Для того чтобы радиоканальные охранно-пожарные системы действительно стали надежной альтернативой традиционным проводным системам, необходимо обеспечить их работоспособность в диапазоне температур от -30 до +55 °С (стандартном для проводных систем). Причем сложнее обеспечить стабильную работу радиосистемы в области отрицательных температур. Однако суть проблемы заключается не столько в характеристиках используемых источников питания (которые стабильно работают и при более низких температурах), сколько в обеспечении автоматической подстройки частоты радиоустройств, находящихся в различных температурных условиях.

Выводы

На наш взгляд, выбирать среди множества предложений по-настоящему надежную радиосистему необходимо на основании следующих критериев:

- помехоустойчивость,

- криптозащищенность,

- температурный диапазон работы.

Надежной альтернативой проводным системам являются лишь радиосистемы, соответствующие указанным требованиям.