

КОЛОНКА РЕДАКТОРА

MythBusters,
или Хочу все знать!

Уверен, что те из вас, кто зачитывался журналом "Техника молодежи", кто радовался киножурналу "Хочу все знать!" вместо скучного "Фитиля", хотя бы раз в жизни с интересом наблюдали за хлестким

разрушением городских легенд, которые учиняют на экране специалисты по спецэффектам программы MythBusters Хайнеман и Севидж.

Вот и данный выпуск рубрики во многом построен по принципу любимой мной передачи: знания и опыт против различных баек, слухов, городских легенд и других порождений поп-культуры.

Речь о трех распространенных заблуждениях:

1. Беспроводную систему легко "заглушить".
2. С помощью беспроводной системы можно "прослушать" объект.

3. Проводные системы более устойчивы к электромагнитному мусору, чем беспроводные.

Основной миф – первый по счету: "Поднеси магическую коробочку к объекту, и она выведет из строя любую беспроводную систему". В теории все гладко, но как только принимаются во внимание следующие обстоятельства:

● в современных системах есть возможность автосмены частотных каналов;

● передача тестовых сигналов происходит каждые 10 секунд;

● злоумышленник находится вне здания, становится очевидным, что либо помеху нейтрализуют простым переходом на резервный канал или диапазон, либо действовать помеха будет только за первой стеной, а в глубине объекта ее уже никто и не заметит.

А представить себе преднамеренное "глушение" пожарной беспроводной системы крайне трудно! Вторая городская байка – радиоканал нельзя применять на режимных объектах, так как беспроводные системы можно использовать при прослушке. Сил для разрушения данной легенды потребуется гораздо меньше – достаточно вспомнить теорему Котельникова, а если проще, то учесть, что радиодатчики выходят на связь не чаще, чем раз в 10 секунд. Слишком редко!

И наконец – вопрос об устойчивости радиоканала к электромагнитному мусору. Много было сломано копий при обсуждении данного вопроса. Я бы привел следующий пример в качестве иллюстрации: за что проще зацепиться – за развесистый куст шиповника или за одинокий прутик $\lambda/4$?

Таким образом, все три мифа РАЗРУШЕНЫ!

М.С. Левчук

Редактор рубрики
"Беспроводные технологии"

Устойчивость радиосистем к помехам

Задачей любой системы безопасности является защита объекта. От скорости и корректности реагирования системы на возникшую угрозу зависит сохранение жизни людей и имущества.

Сегодня количество электронных устройств, создающих помехи, исчисляется миллионами, поэтому возникает вопрос: "Насколько надежной будет работа радиоканальной системы безопасности в таких условиях?". Чтобы ответить на него, проанализируем возможные типы электромагнитного воздействия и способы борьбы с ними



В.И. Зыков

Начальник кафедры связи Академии ГПС
МЧС России, д.т.н., профессор

Существует несколько видов воздействий, которые могут повлиять на работу радиоканальной системы безопасности. Для удобства изложения разобьем материал статьи на три составные части:

1. Преднамеренные радиопомехи ("саботаж").
2. Съем информации из охраняемых помещений ("прослушка").
3. Непреднамеренные помехи. Вероятность ложной тревоги.

Преднамеренная радиопомеха ("саботаж")

Защита от преднамеренных помех актуальна прежде всего на частных объектах, оборудованных охранной сигнализацией. Несмотря на то что изготовление и применение радиотехнических средств с недопустимо большой мощностью преследуется по закону, риск применения злоумышленниками "глушилок" на объекте остается.

Помехи можно классифицировать по соотношению спектра помех и полезных сигналов:

- Прицельные – излучаются на рабочей частоте технического средства.
- Заградительные – имеют ширину спектра, превышающую полосу частот сигнала.

Рассмотрим более подробно каждый из этих видов помех и способы противодействия им.

Прицельная помеха

Продолжим анализ, опираясь на предыдущий пример.

Обратимся к примеру воздействия прицельной помехи, когда помеха излучается на рабочей частоте технического средства. На рис. 1 представлены:

- приемно-контрольный прибор;
- извещатель, работающий на одном из частотных каналов;
- мощная радиостанция (источник помехи), работающая на том же частотном канале.

Если между источником помехи и приемно-контрольным прибором нет экранирующих препятствий, то на входе приемного тракта приемно-контрольного прибора получим сигнал, который будет полностью подавлять полезный сигнал.

При возникновении описанной выше ситуации проявляется одно из принципиальных преимуществ радиоканальных систем с двухсторонним протоколом обмена: обязательное подтверждение получения сообщения (квитирование).

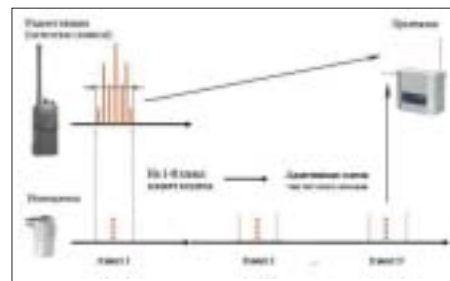


Рис. 1. Пример воздействия прицельной помехи

Предположим, что при установке системы на объекте был выбран частотный канал 1 (всего в системах может быть до 10 частотных каналов в диапазонах 433 и 868 МГц).

Один из извещателей, передающий контрольные сигналы с периодом T_0 , не получив квитанцию от приемно-контрольного прибора после передачи тестового сигнала, немедленно задействует все предусмотренные способы доставки сигнала, которые перечислены ниже.

1. Автоматическая регулировка периода выхода в эфир.

Специалистам известно, что емкость радиосистемы (число адресуемых устройств) во многом определяется способностью системы регулировать объем передаваемой информации (трафика). Чем больше объем информации, который необходимо передать, тем меньшее число устройств может работать на одном частотном канале связи. Поэтому в нормальных условиях периодичность выхода радиоустройств в эфир снижается до необходимого минимума. При

возникновении нештатной ситуации извещатель прежде всего пытается "достучаться" до контрольной панели, уменьшая период выхода в радиоэфир T_1 по сравнению с исходным периодом T_0 .

2. Автоматическая регулировка мощности излучения.

Для того чтобы извещатели, расположенные рядом с приемно-контрольным прибором, не мешали работе извещателей, находящихся на значительном удалении, применяется механизм автоматической регулировки мощности излучения радиоприемных устройств. Однако в особых случаях все радиоприемные устройства имеют право менять мощность своего излучения.

3. Автовыбор резервных каналов.

И наконец, наиболее действенный метод из всех упомянутых выше – автоматическая смена частотного канала на один из десяти в диапазонах 433 и 868 МГц.

Заградительная широкополосная помеха

Рассмотрим пример воздействия помехи на приемное устройство, когда имеется радиостанция, формирующая широкополосную помеху (см. рис. 2).

Спектр такой помехи получается путем перемножения несущей частоты и импульсного сигнала большой скважности. Ширина спектра и расстояние между спектральными составляющими помехи определяются периодом следования импульсов и их длительностью. Мощность излучения спектральных составляющих широкополосного спектра будет в десятки раз меньше исходного сигнала. Дальность влияния широкополосной помехи на приемно-контрольный прибор в разы меньше, чем для прицельной помехи. Переносная радиостанция может заглушить систему в радиусе 20–30 метров в прямой видимости. Если учесть, что радиостанцию и приемно-контрольный прибор разделяет 2–3 стены, блокирование системы практически невозможно. Пример: устройства подавления GSM-сигнала, радиус действия которых составляет от 5 до 20 метров. Пара стен плюс железная дверь сводит работу таких "глушилок" на "нет". Тем не менее вероятность заглушить приемно-контрольный прибор существует. Решающее преимущество систем с двухсторонней связью в данной ситуации заключается в том, что система уже через несколько секунд распознает помеху и начнет бороться с этой проблемой посредством изменения мощности излучения, периода выхода в эфир, смены частотных каналов.

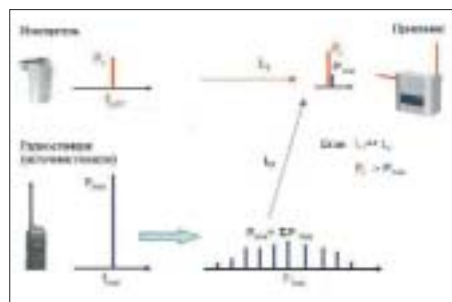


Рис. 2. Пример воздействия заградительной помехи

Если связь не может быть восстановлена даже после всех описанных выше действий, то имеет место преднамеренное технически подготов-

ленное саботирование работы системы, например постановка мощной широкополосной помехи во всем разрешенном диапазоне частот. В этом случае сигнал "Потеря связи" действительно должен передаваться на пульт охраны для дальнейшего анализа ситуации.

Съем информации из охраняемых помещений ("прослушка")

Обеспечение защиты от прослушивания помещений – одно из необходимых условий применения системы на режимных объектах. Если в помещении находятся радиоэлектронные устройства, то возникает риск прослушивания речи с помощью особо чувствительных приемников за счет акустического воздействия на элементы радиопередаточных устройств.

Рассмотрим, насколько опасна угроза съема информации из охраняемого помещения через устройства радиоканальной сигнализации.

Все устройства радиоканальных систем ОПС работают в режиме дискретной передачи сигналов с частотой передачи $f_{\text{дискр}}$. В соответствии с теоремой Котельникова для восстановления исходного речевого сигнала с частотой $f_{\text{сигн}}$ должно выполняться условие: $f_{\text{дискр}} > f_{\text{сигн}}$, что проиллюстрировано на рис. 3.

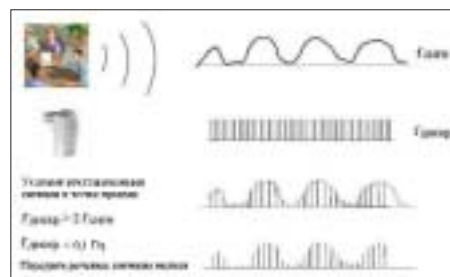


Рис. 3. Съем информации из охраняемых помещений

Спектр речевого сигнала $f_{\text{сигн}}$ находится в диапазоне частот 0,3–6 кГц. Для передачи и последующего восстановления этих сигналов требуется, чтобы частота следования дискретных отсчетов была не менее 12 кГц.

Частота дискретных импульсов $f_{\text{дискр}}$ устройств радиоканальных систем ОПС не больше 0,1 Гц (период передачи устройств от 10 с до нескольких минут). Таким образом, частота $f_{\text{сигн}}$ не должна превышать 0,05 Гц. Поэтому восстановление речевых акустических сигналов из помещений, оборудованных беспроводными средствами ОПС, невозможно.

Непреднамеренные помехи. Вероятность ложной тревоги

Вопрос о причинах ложных срабатываний систем безопасности (особенно систем пожарной сигнализации) уже неоднократно обсуждался. В рамках данной статьи остановимся на одной из возможных причин появления ложных срабатываний – из-за воздействия электромагнитных помех. Проведем аналогию с проводными пожарными извещателями.

Наведенная помеха по цепям питания может влиять как на входную, так и на выходную цепь проводного извещателя.

Извещатель должен обеспечить определенную чувствительность входного каскада, чтобы при

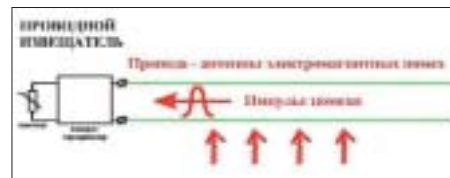


Рис. 4. Наведенная помеха

изменении оптической плотности среды принять однозначное решение о тревоге. Если в момент проведения измерений на шлейф сигнализации, который является и шиной питания, будет наведена помеха, то проводной извещатель сформирует ложное срабатывание. В пожарных извещателях редко ставят фильтры по питанию, откуда все они становятся чувствительны к индуктивным ЭМП. На рис. 4 представлен механизм воздействия наведенной помехи на проводной извещатель. По результатам испытаний большинство проводных средств не может иметь степень жесткости выше II. В то время как радиоканальные системы обеспечивают IV степень жесткости.

Чувствительность выходных каскадов к наведенным помехам по шлейфу значительно меньше, чем у входных каскадов. Вместе с тем выходные каскады всегда подвержены воздействию наведенных помех. В этом случае наведенная помеха может накапливаться за достаточно продолжительный период, что в итоге вызывает ложное срабатывание системы сигнализации.

Следует отметить, что для радиоканальных устройств внешняя помеха может воздействовать только на приемно-передающий тракт, что приводит к событию "Внешняя помеха устройству" и не приводит к ложному срабатыванию. Таким образом, чувствительность беспроводных систем сигнализации к наведенным электромагнитным помехам существенно ниже проводных систем сигнализации.

Выводы

1. В современных радиоканальных системах безопасности используются эффективные способы защиты и адаптации устройств к воздействию различных электромагнитных помех.
2. Прослушка помещений, оборудованных беспроводной сигнализацией, исключена в силу технической особенности построения радиоканальных систем безопасности (использование редких коротких импульсов передачи сигнала).
3. Вероятность ложного срабатывания радиоканальной системы сигнализации гораздо ниже, чем проводной.

Использование современных технологий и алгоритмов работы позволяет создать надежную беспроводную систему безопасности.

Надежность радиоканальных систем безопасности может быть обеспечена только при наличии следующих технических характеристик:

- двухсторонний протокол обмена данными между всеми устройствами радиосистемы;
- автоматический переход на резервные частотные каналы;
- разнесенный радиоприем;
- динамическая маршрутизация доставки сигналов.

Ваше мнение и вопросы по статье направляйте на

ss@groteck.ru