УДК 621.396

# АНАЛИЗ ПОМЕХОУСТОЙЧИВОСТИ РАДИОСТАНЦИИ ПРИ ВОЗДЕЙСТВИИ ОРГАНИЗОВАННЫХ ПОМЕХ

**А. Х. Абед, В. М.Жуков**

*Кафедра «Конструирование радиоэлектронных и микропроцессорных систем»*
*ФГБУ ВПО «ТГТУ»; crems@crems.jesby.tstu.ru*

**Ключевые слова и фразы:** методы; помехозащищенность; помехоустойчивость, радиопомехи; радиоразведка, радиосвязь; радиостанция; радиоэлектронное противодействие.

**Аннотация:** Рассматриваются технические методы повышения эффективности радиосвязи, связанные с помехозащищенностью. Указываются и разбираются методы повышения помехозащищенности и помехоустойчивости, приведены факторы, их формирующие. В качестве наиболее опасных помех, воздействующих на работу радиостанции, выделены ретранслирующие.

Постоянное совершенствование средств радиоразведки (РР) и радиопомех (РП), внедрение автоматизированных комплексов радиоэлектронного противодействия (РЭП) привело за последние годы к существенному повышению возможностей вероятного противника по радио-подавлению КВ-УКВ радиостанций (РС) средней мощности. С учетом этого становится весьма сложной задача обеспечения устойчивой радиосвязи в условиях РЭП. Успешное ее решение невозможно без принятия специальных технических и организационных мер защиты от радиоразведки и радиопомех.

Технические методы повышения эффективности радиосвязи в условиях РЭП направлены на повышение их разведо-и помехозащищенности.

Для повышения помехозащищенности в существующих РС используются те же методы, что и для борьбы со случайными станционными помехами. Основными из них, являются:

- частотно-разнесенная передача и прием;
- связь через удаленный ретранслятор;
- применение компенсаторов помех и высокоскоростных модемов;
- метод группового использования частот;
- применение широкополосных сигналов.

В общем случае электронное подавление включает два последовательных этапа – техническую разведку и противодействие. Применительно к радиостанциям целью технической разведки является установление факта передачи информации между объектами и определение параметров сигналов. Целью противодействия является создание таких условий, которые затруднили бы работу РС или привели к срыву выполнения задачи. Критерий помехозащищенности РС может быть представлен в следующей форме:

$$p_{ПМЗ} = 1 - p_P p_H \ , \qquad (1)$$

где $P_P$ – вероятность разведки параметров сигналов; $P_H$ – вероятность нарушения работы РС.

По результатам анализа возможностей современных средств технической разведки можно утверждать, что $P_P$ в (1) практически всегда будет равна 1. Тогда (1) можно представить в виде:

$$p_{ПМЗ} = 1 - p_H = p_{ПМУ} \ , \qquad (2)$$

где $P_{ПМУ}$ – вероятность выполнения РС задачи в условиях подавления (критерий помехоустойчивости).

Формула (2) верна для случая, когда перед технической разведкой не ставится задача раскрытия смысла передаваемой информации, а только обнаруживается сигнал – носитель информации. Величина $PH$ является количественной мерой помехоустойчивости РС при действии на нее помех.

Помехоустойчивость зависит от сочетания большого количества факторов: формы полезного сигнала, вида (формы) помехи, ее интенсивности, структуры приемника, применяемых способов борьбы с помехами и т.д.

Помехоустойчивость РС по отношению к имитирующим помехам разного вида с различной степенью близости к полезному сигналу во многом определяется взаимно и автокорреляционными характеристиками рассматриваемых сигналов и их функцией неопределенности. Практика электронного подавления показывает, что эффективность имитирующих помех зависит от тактики их применения и степени раскрытия структуры полезного сигнала средствами технической разведки. Важным фактором структуры скрытности являются разнообразие и особенности ансамбля полезного сигнала.

Информационная скрытность РС определяется способностью противостоять мерам, направленным на раскрытие смысла передаваемой с помощью сигналов информации. Раскрытие смысла передаваемой информации означает отожествление каждого принятого сигнала с той командой, которая передается. Наличие априорной и

апостериорной информации делает эту задачу вероятностной, а в качестве меры информационной скрытности выступает вероятность раскрытия смысла передаваемой информации $p_{инф}$ при условии, что сигнал обнаружен и выделен [1].

Таким образом, на помехозащищенность РС влияют следующие существенные факторы: вид сигнала, являющегося физическим носителем информации и обеспечивающим спектральную и энергетическую эффективность; структура сигнала, обеспечивающая структурную и информационную скрытность; методы и алгоритмы преобразования сигнала в передатчике и приемнике, обеспечивающие устойчивость к воздействию организованных помех.

Критерий помехозащищенности РС, учитывающий основные факторы влияния, имеет вид

$$p_{пмз} = 1 - p_н - p_{стр} \cdot p_{инф} \cdot p_н , \qquad (3)$$

где $p_{стр}$, $p_{инф}$ - вероятности раскрытия структуры и смысла передаваемой информации соответственно.

Исходные условия, при которых необходимо обеспечить требуемый уровень помехозащищенности РС, следующие: противоборствующей стороне-организатору радиоэлектронного подавления (криптоаналитику) известны пространственные координаты передатчиков и приемников сигналов; известен частотный диапазон работы радиоканала РС; известна структура передаваемой информации; обмен информацией между объектами осуществляется непрерывно; вероятность организованного противодействия практически равна единице. В этих условиях выбор сигнала для радиоканала РС определяется, исходя из спектральной и энергетической эффективности, а не из маскирующих свойств, т.к. местонахождение объектов известно. Наилучшими характеристиками в этом смысле обладают модулированные сигналы с непрерывной фазой (МНФ).

В общем виде сигнал, манипулированный фазой, (МНФ) на $k$-ом тактовом интервале можно записать следующим образом:

$$S(t, C_k) = A_0 \cos\left\{\omega_0 t + 2\pi \sum_{i=1}^{k} C_i h_i q[t - (i-1)T] + \varphi_0\right\} , t \in [(k-1)T, kT], \qquad (4)$$

где $A_0$ – амплитуда сигнала; $h_i$ – индекс модуляции на $i$-ом тактовом интервале; $\omega_0$ – разного вида несущая частота; $\varphi_0$ – начальная фаза; $C_k = [C_1, C_2, \ldots C_k]$ – вектор $m$-ичных информационных символов, принимающих одно значение из ряда $C_i = \pm 1; \pm 3; \ldots \pm (m-1)$; $q(t)$ – фазовый импульс (ФИ) длиной $L$ тактовых интервалов.

Длина $L$ фазового импульса является одной из наиболее важных характеристик, определяющих свойства сигнала; при $L=1$ сигнал МНФ принято называть сигналом с полным откликом, а при $L \geq 2$ – сигналом с частичным откликом.

Среди большого разнообразия сигналов МНФ наибольшую известность приобрели сигналы (для $t \in [0, LT]$), которые могут быть использованы в РС:

$q(t) = t/2LT$ – прямоугольный;

$q(t) = [1-\cos(\pi t/LT)]/4$ – полупериод синусоиды;

$q(t) = t/2LT - [\sin(2\pi t/LT)]/4\pi$ – приподнятый косинус.

Вид ФИ напрямую определяет спектральные характеристики сигнала МНФ, в частности, скорость $B_S$ спада внеполосного изучения.

Наряду с белым шумом в радиоканале РС могут присутствовать организованные помехи. Наиболее вероятными помехами, учитывая условия функционирования РС, следует считать:

$S_{Пг}(t) = A_П \cos(\omega_0 t + \varphi)$ – гармоническую помеху;

$S_{П\,\text{ПСП-ФМ}}(t) = A_П a_k^m \cos(\omega_0 t + \varphi)$ – сигнал с бинарной фазовой манипуляцией псевдослучайной последовательностью (ПСП-ФМ) помеху;

$$S_{Пр}(t) = A_П \cos\left\{\omega_0(t-\tau) + 2\pi \sum_{i=1}^{k} C_i h_i q[(t-\tau)-(i-1)T] + \varphi\right\} -$$

ретранслированную помеху,

где $A_П = \mu A_0$ - амплитуда помехи; $\mu$ –относительная интенсивность помехи; $a_k^m$ – случайный бинарный символ помехи ПСП-ФМ длительностью $T_П = T/M$; $M$ – относительная скорость манипуляции помехи; $\tau$ – задержка ретранслированной помехи.

В [2] приведены результаты анализа помехоустойчивости оптимального демодулятора сигнала МНФ с глубиной решения $N$ тактовых интервалов при воздействии 3-х указанных организованных помех. Считалось, что несущие частоты полезных сигналов и организованных помех совпадают. Анализ проводился с использованием евклидова расстояния между точками концов векторов, соответствующих информативных сигналов.

Евклидово расстояние между сигнальными точками $D_{ab}$ рассчитывалось по формуле

$$D_{ab} = \int_0^{NT} S_a(t) S_b(t) dt = (A_0^2/2) \int_0^{NT} \left\{1 - \cos\left[2\pi \sum_{i=1}^{N} (\mathbf{C_a} - \mathbf{C_b}) h_i q\right][t-(i-1)T]\right\} dt,$$

(5)

где векторы информационных символов $\mathbf{C_a}$ и $\mathbf{C_a}$ обязательно отличаются первыми позициями.

Анализ проводился при отношении сигнал/шум $2E/N_0 = 20$ и относительной интенсивности той или иной помехи $\mu = 0{,}2$, количество тактовых интервалов принималось оптимальным $N = 3$.

На рис.1 показана вероятность ошибочного распознавания сигнала в виде приподнятого косинуса при действии организованных помех.

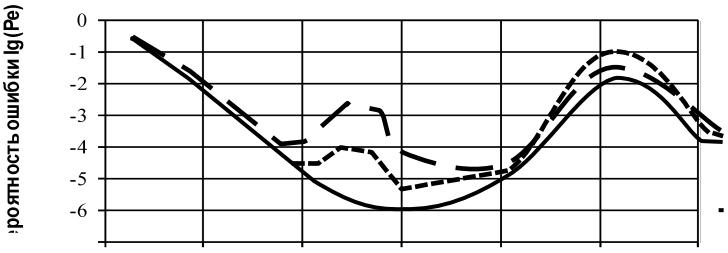


**Рис 1. Вероятность ошибочного распознавания сигнала при действии организованных помех: -в беспомеховой ситуации; …… - при действии ПСП-ФМ помехи; - при действии ретранслированной помехи.**

Проведенный анализ показывает, что наиболее опасной для РС является ретранслированная помеха. Это обусловлено тем, что корреляционная функция полезного сигнала и ретранслированной помехи принимает большие значения по сравнению со значениями для ПСП-ФМ и гармонической помех. Необходимо заметить, что различные варианты кодирования источника информации принципиально не влияют на помехоустойчивость РС при действии указанных помех.

*Список литературы*

1. Жуков, В.М. Оперативное определение воздействия помех в каналах связи / В.М. Жуков // Радиотехника. –2006. – №5. – С.92-94.

2. Жуков, В.М. Особенности приема ортогональных многопозиционных сигналов в многолучевых каналах связи / В.М. Жуков, И.Г. Карпов, Г.Н. Нурутдинов// Радиотехника. – 2006. – № 5. – С.86-88.

# An analysis of Radio Interference Immunity Under the Influence of Organized Interference

**A.H. Abed, V.M. Zhukov**

*Department "Design of Radio and Microprocessor System",TSTU;*
*crems@crems.jesby.tstu.ru*

**Key words and phrases**: methods; immunity; interference; radio reconnaissance; radio; radio station; electronic countermeasures.

**Abstract:** The technical methods to improve the efficiency of radio-related interference protection. Include and understand methods to improve noise immunity and immunity, given the factors forming them. The most harmful interference affecting the work of the station, allocated rebroadcast.

*References*

1. Zhukov, V.M. The operational definition of interference in the communication channels / V.M. Zhukov // Radio engineering. –2006. – №5. – S.92-94.

2. Zhukov, VM Features multi-position reception orthogonal signals in multipath channels of communication / V.M. Zhukov, I.G. Karpov G.N. Nurutdinov // Radio engineering. – 2006. – № 5. – S.86-88.