АНАЛИЗ НАИБОЛЕЕ ОПАСНЫХ ПОМЕХ, ВЛИЯЮЩИХ НА РАБОТУ РЕТРАНСЛЯЦИОННОЙ РАДИОСТАНЦИИ

Аттокуров Урмат Тологонович
Директор Института прикладных наук, канд. техн. наук, проф. ОшТУ
Оморова СалтанатТоронбековна
Магистр Кафедра «Информатика, программирование и связи», Ошский технологический университет
Эшмурадов Дилшод Элмурадович
Доцент Ташкентского государственного технического университета

https://doi.org/10.5281/zenodo.7185811

Аннотация. *В статье рассматриваются технические методы повышения эффективности радиосвязи при воздействии помех. Авторы исследуют методы повышения помехозащищенности и помехоустойчивости радиостанций, а также анализируют факторы, влияющие на них. Шум при повторной передаче оказывает наиболее вредное влияние на работу радиостанции. Анализ показал, что шум при повторной передаче опасен для радиостанции. Корреляционная функция желаемого сигнала и шума повторной передачи имеет большие значения по сравнению со значениями псевдослучайного шума и гармонического шума. Варианты кодирования источника информации не влияют на помехоустойчивость радиостанций при воздействии данного вида помех.*

Ключевые слова: *радиоэлектроника, автоматизация, передачи информации, мощность, радиосвязь, радиостанция, радиоэлектронное противодействие.*

ANALYSIS OF THE MOST DANGEROUS INTERFERENCE AFFECTING THE OPERATION OF A RELAY RADIO STATION

Abstract. *The paper considers technical methods to improve the efficiency of radio communication under the influence of noise. The authors explore the methods to improve noise immunity and noise resistance of radio stations, and analyze the factors influencing them. Retransmission noise produces the most harmful influence on the work of a radio station. The analysis showed that retransmission noise is dangerous for a radio station. The correlation function of the desired signal and retransmission noise has bigger values compared to the values of pseudo-random noise and harmonic noise. Coding options for information source do not affect the noise immunity of radio stations under the action of the given kind of noise.*

Keywords: *radio electronics, automation, information transmission, power, radio communication, radio station, electronic countermeasures.*

ВВЕДЕНИЕ

Устойчивое улучшение средств радиоразведки (РР) и радиопомех (РП), внедрение автоматизированных комплексов радиоэлектронного противодействия (РЭП) привело за последние годы к существенному повышению возможностей вероятного противника по радиоподавлению коротковолновых и ультракоротковолновых (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

радиоэлектронного противодействия направлены на увеличение 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 р транслятор;

– применение компенсаторов помех и высокоскоростных модемов;

– метод группового использования частот;

– применение широкополосных сигналов.

МАТЕРИАЛЫ И МЕТОДЫ

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. Противодействие – создание таких условий, которые затруднили бы работу РС или привели к срыву выполнения задачи. Критерий помехозащищенности РС может быть представлен в следующей форме

$$P_{ПМЗ} = 1 - P_р P_н \qquad (1)$$

где $P_р$ – вероятность разведки параметров сигналов;

$P_н$ – вероятность нарушения работы РС.

По результатам анализа возможностей современных средств технической разведки можно утверждать, что в формуле (1) практически всегда $P_р = 1$. Тогда (1) можно представить в виде

$$P_{ПМЗ} = 1 - P_н = P_{ПМУ}, \qquad (2)$$

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 $P_н$ является количественной мерой помехоустойчивости РС при действии на нее помех.

РЕЗУЛЬТАТЫ

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

Для создания помехоустойчивой передачи и приема сигналов используются специальные способы кодирования, которые позволяют существенно повысить качество приема [3].

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 отождествление 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 $P_{ПМЗ}$ РС влияют следующие существенные факторы: вид сигнала, являющегося физическим носителем информации и обеспечивающим спектральную и энергетическую эффективность; структура сигнала, обеспечивающего 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

$$P_{ПМЗ} = 1 - P_н - P_{стр}\, P_{инф}\, P_н \quad (3)$$

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; частотный диапазон работы радиоканала РС; 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, так как местонахождение объектов известно. Наилучшими характеристиками в этом смысле обладают модулированные сигналы с непрерывной фазой.

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

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

где A_0 – амплитуда сигнала;

h_i – индекс модуляции на *i*-м тактовом интервале;

ω_0 – несущая частота разного вида;

ϕ_0 – начальная фаза;

$C_k = [C_1, C_2\ \ldots\ldots C_k]$ - вектор *m*-х информационных символов, принимающих одно значение из ряда $C_i = \pm1; \pm3; \ldots; \pm(m-1)$; *q(t)* – фазовый импульс (ФИ) длиной *L* тактовых интервалов.

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

$S_{пг}(t) = A_п \cos(\omega_0 t + \phi)$ – гармоническую;

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

$S_{пр}(t) = A_п \cos\{\omega_0 (t - r) + 2\pi \sum_{i=1}^{k} C_i\ h_i q[(t - r) - (i - 1)T] + \varphi\}$,– ретранслированную, где $A_п = \mu A_0$ – амплитуда помехи;

μ – относительная интенсивность помехи;

a_k^m – случайный бинарный символ помехи ПСП-ФМ длительностью $T_n=T/M$;

M – относительная скорость манипуляции помехи;

τ – задержка ретранслированной помехи.

ОБСУЖДЕНИЕ

В источнике [2] приведены результаты анализа помехоустойчивости самолучшего демодулятора сигнала МНФ с глубиной решения N тактовых интервалов при воздействии трех указанных организованных помех. Сообразовалось, 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 Dab рассчитывалось по формуле

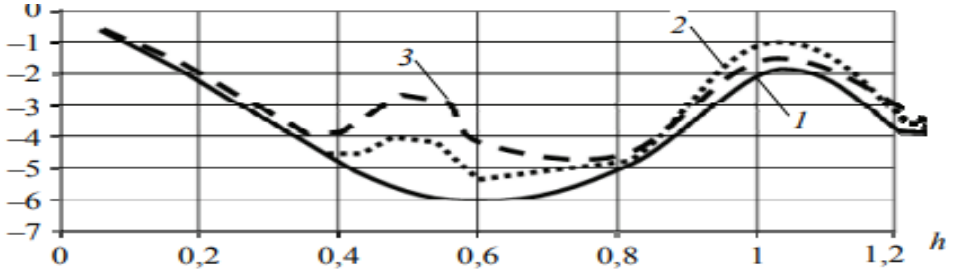
Рис. 1.

Вероятность ошибочного распознавания сигнала при действии организованных помех:

1 – в без помеховой ситуации;

2 – при действии (ПСП-ФМ) - помехи;

3 – при действии ретранслированной помехи



$$D_{ab} = \int_o^{NT} S_a(t) S_b(t) dt = \left(\frac{A_0^2}{2}\right) \int_0^{NT} \{1 - \cos[2\pi \sum_{i=1}^{N} (C_a - C_b) h_i q]\ [t - (i - 1)T]\} dt, \quad (5)$$

где векторы информационных символов C_a и C_b обязательно отличаются первыми позициями. Исследование проводилось при отношении сигнал/шум $2E/N_0 = 20$ и

относительной интенсивности той или иной помехи μ = 0,2, число тактовых интервалов принималось оптимальным N = 3. На рисунке 1 показана вероятность ошибочного распознавания сигнала в виде приподнятого косинуса при действии организованных помех.

ВЫВОДЫ

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.

REFERENCES

1. Денисов, Б.Б. Проблемы наращивания телекоммуникационного ресурса в интересах функционирования информационно-управляющих систем специального назначения / Б.Б. Денисов // Доклад на научной конференции «Современные тенденции развития теории и практики управления в системах специального назначения-2012». – М.: ОАО «Концерн «Системпром», 2012.
2. Макаренко, С.И. Анализ воздействия преднамеренных помех на функционирование расширенного протокола маршрутизации внутреннего шлюза (EIGRP) / С.И. Макаренко // Информационные технологии моделирования и управления. – 2010. – № 2 (61). – С. 223–229.
3. Эшмурадов Д.Э., Рахманова Ф.К. Анализ помехоустойчивости бортовых радиоприемных устройств // Материалы конференции «Проблемы формирования и внедрения инновационных технологий в условиях глобализации». Сборник научных трудов. ч. 2. (Ташкент, 22-24 сентября 2010 года), стр. 122-123.
4. Жуков, В. М. Оперативное определение воздействия помех в каналах связи / В. М. Жуков // Радиотехника. – 2006. – № 5. – С. 92 – 94.
5. 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
6. Борисов, В.И. Пространственные и вероятностно-временные характеристики эффективности станций ответных помех при подавлении систем радиосвязи / В.И. Борисов, В.М. Зинчук, А.Е. Лимарев, А.В. Немчилов, А.А. Чаплыгин. – Воронеж: ОАО «Концерн «Созвездие»», 2007. – 354 с.
7. Сикорский, А.Б. Методы повышения помехоустойчивости систем подвижной сотовой связи в условиях преднамеренных помех / А.Б. Сикорский // Проблемы информационной безопасности. Компьютерные системы. – 2001. – № 3. – С. 54–67.
8. Иванов, М.С. Помехозащищенность широкополосных систем радиосвязи с расширением спектра методом псевдослучайной перестройки рабочей частоты / М.С. Иванов, С.А. Попов // Сборник докладов XI Всероссийской научно-практической конференции «Актуальные вопросы разработки и внедрения информационных технологий двойного применения». – Ярославль: ЯВВЗРУ, 2011. – С. 322–329.