

АЛГОРИТМЫ ПОСТРОЕНИЯ СИГНАЛОВ С ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКОЙ РАБОЧЕЙ ЧАСТОТЫ ДЛЯ ПОМЕХОЗАЩИЩЕННЫХ РАДИОСИСТЕМ

д.т.н., проф. Ю.В. Стасев, А.С. Коломиец, Я.Н. Кожушко

Рассматриваются алгоритмы построения сигналов с псевдослучайной перестройкой рабочей частоты. Анализируются достоинства и недостатки применения существующих методов формирования ППРЧ сигналов в дециметровых радиосетях управления.

При создании и оптимизации помехозащищенной дециметровой радиосети управления возникает ряд задач, связанных с особенностью их построения, в частности:

- учет характера распространения радиоволн дециметрового диапазона;
- синтез формы сложных сигналов, выбор параметров их модуляции и кодирования, адекватных уровню решаемых задач;
- многокритериальная оптимизация систем обработки и извлечения передаваемой информации;
- обеспечение заданной помехозащищенности, имитостойкости и скрытности радиолинии;
- реализация надежности управления.

Анализ результатов оценки помехозащищенности, имитостойкости и скрытности радиосети управления, приведенных в [1], показывает, что в условиях воздействия помех более высокие показатели достигаются при совместном использовании в радиосети сигналов с псевдослучайной перестройкой рабочей частоты (ППРЧ) и сигналов с псевдослучайной перестройкой рабочей частоты с дополнительной фазовой манипуляцией (ППРЧ-ФМ), как эффективного метода противодействия разведке и подавлению системы связи.

Псевдослучайная перестройка рабочей частоты представляет собой способ расширения спектра сигнала в пределах полосы частот системы, путем скачкообразного изменения частоты сигнала по псевдослучайному закону. К настоящему времени известен ряд методов формирования ППРЧ сигналов [2, 3, 4]. В настоящей статье проанализируем возможности применения данных методов формирования ППРЧ сигналов в дециметровых радиосетях управления.

Пусть число разрешенных частотных интервалов в помехозащищенной радиосети управления равно M . Тогда элементы ППРЧ сигнала мо-

гут быть построены на основе следующих правил [2 – 4].

Правило 1 [2]. Элементы ППРЧ сигнала строятся на основе метода перемешивания:

$$\begin{aligned} Z_i &= (Z_{i-1})^2 - 2 \quad \text{для} \quad Z_n \in [-2; 2]; \\ x_i &= \frac{4}{\pi} \arccos \frac{Z_i}{2} - 2 \quad \text{или} \\ x_i &= Z_i \quad \text{без } n \text{ старших бит.} \end{aligned} \quad (1)$$

Формируемые на основе этого метода сигналы имеют большой период, обладают хорошими статистическими свойствами, но имеют низкую структурную скрытность.

Правило 2 [4]. Формирование элементов ППРЧ сигнала проводится согласно теории клеточных автоматов

$$A_i^{k+1} = a_{i-1} A_{i-1}^k + a_i A_i^k + a_{i+1} A_{i+1}^k, \quad (2)$$

где i – номер разряда автомата; k – номер такта функционирования автомата; A_i^k – состояние i -го разряда автомата в k -й момент времени; a_j – коэффициент влияния j -го разряда автомата на последующее состояние i -го разряда автомата ($a_j \in \{0, 1\}$, $j \in \{i-1, i, i+1\}$); «+» – булева операция.

Состояние любого разряда устройства, в последующий момент времени зависит только от предыдущих состояний его самого и его ближайших соседей.

Сформированные по этому правилу сигналы имеют достаточно высокую структурную скрытность, но при увеличении конструктивных параметров аппарата усложняется его реализация.

Правило 3 [4]. Элементы ППРЧ сигнала строятся по рекуррентному соотношению:

$$b_i = \begin{cases} a_i, & i = 0, 1, \dots, n-1; \\ \sum_{k=1}^n b_{i-k} h_{n-k} \pmod{M}, & i = n, n+1, \dots \end{cases} \quad (3)$$

Линейный рекуррентный регистр с обратной линейной связью, формирует выходной сигнал полностью определяемый начальным значением a_0, a_1, \dots, a_{n-1} и отводами обратных связей h_i ($i = 1, 2, \dots, n$), $h_i(0,1)$. Обратные связи регистра формируются по закону примитивного полинома

$$h(x) = h_n x^n + h_{n-1} x^{n-1} + \dots + h_1 x + h_0 = \sum_{i=1}^n h_i x^i + 1. \quad (4)$$

Правило 4 [4]. ППРЧ сигнал может быть сформирован по следующему правилу:

$$b(t) = \sum_{s=0}^{P_3-1} C_s(t) V_s(t), \quad t = 0, 1, 2, \dots, \quad (5)$$

где $V_s(t) = a(t - \Phi_s(x_t)), \quad t = 0, 1, 2, \dots, P_3 - 1;$

$$C_s(t) = \begin{cases} 1, & t - s = 0 \pmod{P_3}; \\ 0, & t - s \neq 0 \pmod{P_3}, \end{cases} \quad s = 0, 1, \dots, P_3 - 1;$$

x_t – последовательность адресов считывания элементов сигнала с периодом P_2 , принимающих значения из множества $K = \{0, 1\}^k$; $\Phi_s(j), j \in k$ есть инъективное отображение $K \rightarrow \{1, \dots, P_3\}$; P_1, P_2, P_3 – периоды последовательностей генерируемых 1-м, 2-м и 3-м линейным рекуррентным регистром соответственно.

Выражение (5) описывает работу управляемого регистра сдвига, который изменяет свое состояние по управляющим импульсам генератора сигналов или по закону управляющей последовательности, источником которой является другое устройство. Другим вариантом регистра является обобщенный регистр сдвига, работа которого описывается выражением:

$$a_i = h_1 a_{k-1} + h_2 a_{k-2} + \dots + h_n a_{k-n} \pmod{M}, \quad (6)$$

где a_k – последнее m -битное значение в последовательности; h – коэффициенты примитивного полинома; n – степень полинома, количество m -битных запоминающих элементов.

Выражение (6) описывает работу аддитивного генератора, который формирует последовательность с периодом $L = (2^n - 1)2^{r-1}$ для любого примитивного полинома степени n и r разрядных выходных значений.

Регистры, описанные (3), (5) и (6), обладают неудовлетворительной структурной скрытностью. Использование нелинейных обратных связей не позволяет теоретически обосновать длину периода и статистические свойства сигналов, с уменьшением управляемого регистра уменьшается сложность формируемых сигналов, в обобщенном регистре сдвига каждый линейный рекуррентный регистр является абсолютно коррелированным с другими, что существенно ухудшает структурные свойства формируемых сигналов.

Правило 5 [4]. ППРЧ сигнал может быть построен с использованием рекуррентной формулы вида

$$x_i = g(x_{i-1}) = (\beta + 1) \cdot \left(1 + \frac{1}{\beta}\right)^\beta x_{i-1} (1 - x_{i-1})^\beta, \quad 1 \leq \beta \leq 4. \quad (7)$$

ППРЧ сигналы, построенные по этому правилу, имеют тенденцию к вырождению при

$$x_{i-1} = 1 - \frac{\beta}{(1 + \beta)^{1 + \frac{1}{\beta}}}. \quad (8)$$

Анализ этого метода показал, что достаточно сложные системы сигналов определяются простыми уравнениями с довольно высокой сложностью генерируемых сигналов. Но при программной реализации метода

необходимы относительно большие вычислительные затраты.

Правило 6 [2]. Частотные составляющие ППРЧ сигнала строятся по правилу усечения

$$x_i = \underset{1}{\overset{k}{\parallel}} x_{i-1} x_{i-2} \underset{3k+1}{\overset{4k}{\parallel}}, \quad (9)$$

где x_{i-1} , x_{i-2} – числа разрядностью $2k$; $\underset{1}{\overset{k}{\parallel}} \underset{3k+1}{\overset{4k}{\parallel}}$ – операция выделения $2k$ элементов из числа разрядностью $4k$, причем разряды $1 \div k$ и $3k+1 \div 4k$ отбрасываются.

Этот метод отличается простотой реализации, но ППРЧ сигналы, построенные на основе этого утверждения, имеют тенденцию превращаться в короткие циклы повторяющихся элементов и вырождаться, а также не обеспечивается требуемая величина периода сигналов, и в сигналах наблюдается межэлементная зависимость, которая носит линейный характер.

Правило 7 [4]. Пусть число разрешенных частотных интервалов равно M . Тогда элементы ППРЧ сигнала могут быть построены на основе конгруэнтного датчика

$$x_i = (ax_{i-1} + c) \pmod{M}, \quad (10)$$

где x_{i-1} – начальное состояние датчика, причем $x_{i-1} \geq 0$; a_i – множитель, $a_i > 0$.

При этом приращение c определяется как

$$c = \left(\frac{1}{2} - \frac{1}{6} \sqrt{3} \right) M. \quad (11)$$

При $c = 0$ выражение (10) принимает вид

$$x_i = ax_{i-1} \pmod{M}. \quad (12)$$

Если $c \neq 0$ и не удовлетворяет (11), то выражение (10) принимает вид:

$$x_i = (x_{i-1} + x_{i+2}) \pmod{M}. \quad (13)$$

Формируемые по данному правилу сигналы имеют статистические свойства, удовлетворяющие большинству статистических критериев, обладают простым математическим аппаратом, но наряду с этим имеют низкую структурную скрытность, а также на параметры сигнала накладываются ограничения, которые приводят к ограничению периода ППРЧ сигнала.

Правило 8 [4]. Элементы ППРЧ сигнала могут быть построены так:

$$x_i = x_{i-1}^2 \pmod{N}, \quad (14)$$

где N – произведение двух больших чисел.

Конечное значение составляющей сигнала x'_i вычисляется как $x'_i = x_i \pmod{M}$.

Известно, что такие ППРЧ сигналы имеют стойкость, сравнимую со

сложностью задачи разложения числа N на сомножители. Для обеспечения большого периода и высокой стойкости формируемых сигналов должны выполняться требования:

- простые числа должны удовлетворять сравнениям вида:

$$P \equiv 3 \pmod{4}; Q \equiv 3 \pmod{4};$$

- простые числа должны быть специального вида:

$$P = 2P_1 + 1; Q = 2Q_1 + 1;$$

$$P_1 = 2P_2 + 1; Q_1 = 2Q_2 + 1,$$

где P_1, P_2, Q_1, Q_2 – простые числа.

Такие сигналы имеют большие вычислительные затраты на получение одного ППРЧ сигнала.

Правило 9 [3]. При формировании сигналов ППРЧ можно также использовать математический аппарат теории полей Галуа. Обосновывается это тем, что элементы поля Галуа $GF(p)$ принимают значения $a_i \in \{1, 2, 3, \dots, p - 1\}$ и они могут быть использованы как элементы ППРЧ сигнала. Элементы ППРЧ сигнала формируются таким образом:

$$a_i = a_{i-1}\theta \pmod{p}, \quad (15)$$

где θ – первообразный элемент; p – размерность поля $GF(p)$.

При этом соотношения, показывающие взаимосвязь a_i -го элемента с элементами мультипликативной группы, определяются так:

$$a_{i+\frac{p-1}{2}} = p - a_i;$$

$$a_i a_{p-i-1} = 1 \pmod{p};$$

$$a_{\frac{p-1}{2}-m} a_{\frac{p-1}{2}+m+1} = \theta \pmod{p}, \quad (16)$$

где $m = 1, 2, 3, \dots$; $a_{p-i+k-1} a_i = \theta^k \pmod{p}$, $k = 0, 1, 2, \dots$.

Анализ этих соотношений позволяет сделать вывод о том, что ППРЧ сигналы, элементы которых являются значениями полей Галуа, содержат частотные составляющие, равномерно распределенные во всем диапазоне, и появление элементов в сигналах происходит равновероятно.

Рассматриваемые сигналы имеют хорошие корреляционные и ансамблевые свойства, а также обладают удовлетворительными структурными характеристиками, что не позволяет в полной мере обеспечить требуемое качество передачи информации.

Таким образом, так как декаметровый диапазон является равнодоступным для всех пользователей, можно сделать вывод о том, что существующие методы построения ППРЧ сигналов на сегодняшний день не удовлетворяют требованиям по помехозащищенности, имитостойкости и

скрытности радиосети управления. Поэтому возникает необходимость формирования сигналов ППРЧ с требуемыми структурными свойствами, использование которых приведет к повышению показателей функционирования радиосети.

ЛИТЕРАТУРА

1. Стасев Ю.В., Горбенко И.Д., Макаренко Б.И. и др. Применение сложных сигналов в командно-телеметрических радиоприемниках // *Космическая наука и технология*. – 1997. – Т. 3, № 5 / 6. – С. 104 – 108.
2. Борисов В.И., Зинчук В.М., Лимарев А.Е. и др. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты. – М.: Радио и связь, 2000. – 384 с.
3. Свердлик М.Б. Оптимальные дискретные сигналы. – М.: Сов. радио, 1975. – 200 с.
4. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.

Поступила 26.07.2002

СТАСЕВ Юрий Владимирович, доктор техн. наук, профессор, начальник факультета ХВУ. Окончил ХВВКИУ в 1981 году. Область научных интересов – защита информации в автоматизированных системах управления и связи.

КОЛОМИЕЦ Андрей Станиславович, адъюнкт ПВИС. Окончил КВИУС в 1998 году. Область научных интересов – защита информации в автоматизированных системах управления и связи.

КОЖУШКО Ярослав Николаевич, курсант ХВУ.

УДК 681.518.3

ОБОСНОВАНИЕ ЗАДАЧИ ОПТИМАЛЬНОГО ПОСТРОЕНИЯ СИСТЕМЫ ОХРАНЫ

к.т.н. И.Я. Гайворонский
(представил д.т.н., проф. Е.А. Артеменко)

В статье рассматривается обоснование задачи синтеза системы охраны с учетом основных влияющих факторов.

Сокращение численности Вооруженных Сил, наличие большого числа важных (опасных) объектов вызывают повышенный интерес к системам охраны (СО). Поэтому создание систем охраны нового поколения становится актуальным, а для построения экономичных и эффективных систем охраны требуется в первую очередь обоснование задачи синтеза системы охраны и анализ ее показателей.

Рассмотрим показатели, описывающие основные характеристики системы охраны и оценивающие качество ее функционирования.

1. *Вероятность срабатывания системы охраны при проникновении нарушителя на охраняемый объект* $P_{фс}$, которая определяется как

$$P_{фс} = P_{обн} \times P_{лс} \times P_{нас},$$

где $P_{обн}$ – вероятность обнаружения нарушителя датчиками СО, которая определяется следующим образом [1]:

$$P_{обн} = \sum_{i=0}^b P_{ни} \times P_{oi},$$

где $P_{ни}$ – вероятность нахождения системы в состоянии, при котором отказали i датчиков; P_{oi} – вероятность обнаружения нарушителя системой в состоянии, при котором отказали i датчиков; b – максимально допустимое число датчиков, которые могут отказаться в системе при наиболее удачном их расположении, без потери ее работоспособности; $P_{лс}$ – вероятность достоверного функционирования линий связи; $P_{нас}$ – вероятность безотказной работы программно-аппаратных средств, которая оценивается следующим образом [2]:

$$P_{нас} = \left[\sum_{i=1}^K P_{\bar{0}}(S_i(P_{ас}, P_{ус}, P_{п})) \right] \times P_k,$$

где $P_{\bar{0}}(S_i(P_{ас}, P_{ус}, P_{п}))$ – вероятность безотказной работы структуры программно-аппаратных средств в состоянии S_i ; S_i – допустимое состояние системы, при котором на выходе будет получено достоверное решение; $P_{ас}$ – вероятность возникновения аппаратного сбоя; $P_{ус}$ – вероятность возникновения устойчивого отказа; $P_{п}$ – вероятность возникновения программного отказа; P_k – вероятность безотказной работы коммутаторов; K – число допустимых состояний системы.

Особенностью показателя является учет надежностных характеристик элементов СО.

2. *Среднее время между ложными срабатываниями системы* $T_{лс}$.

Среднее время ложных срабатываний не имеет точного аналитического выражения ввиду своей сложности и может быть рассчитано либо приближенными формулами, либо с использованием имитационного моделирования [1]. Среднее время ложных срабатываний является важной эргономической характеристикой СО ввиду того, что частые ложные срабатывания приводят к тому, что личный состав перестает адекватно реагировать на каждое срабатывание СО, что значительно снижает эффективность функционирования СО.

3. *Стоимость системы* C_c , рассчитываемая как

$$C_c = \sum_{i=1}^N (C_{дi} + C_{лci}) \times K_i + C_{вя} ,$$

где $C_{дi}$ – стоимость датчика i -го типа; $C_{лci}$ – стоимость линии связи до i -го датчика; K_i – количество датчиков в i -м рубеже; N – число рубежей; $C_{вя}$ – стоимость вычислительного ядра, которая находится по формуле:

$$C_{вя} = \sum_{j=1}^{K_{пр}} C_{прj} + \sum_{z=1}^{K_{ап}} C_{апz} + C_{ком} ,$$

где $C_{прj}$ – стоимость j -й версии программного средства; $C_{апz}$ – стоимость z -го аппаратного канала; $C_{ком}$ – стоимость аппаратных средств для различных вариантов подключения каналов и определяется индивидуально для каждой конкретной программно-аппаратной структуры. По своему виду стоимость СО представляет собой линейную функцию.

Основным показателем эффективности системы охраны является вероятность срабатывания системы охраны при проникновении нарушителя на охраняемый объект, что и отражает задание этого показателя в техническом задании на создаваемую СО. Повышение вероятности срабатывания системы охраны при проникновении нарушителя на охраняемый объект приводит к возрастанию стоимости системы. С учетом этого противоречия задача выбора оптимальных параметров системы охраны, формулируется следующим образом:

$$P_{фс} \rightarrow \max \quad \text{при} \quad C_c \leq C_{сзад} \quad \text{и} \quad T_{лс} \geq T_{лсзад} .$$

Количество датчиков является целым числом, поэтому для решения задач данного типа необходимо применение методов нелинейного целочисленного программирования.

Таким образом, в статье рассмотрены основные показатели систем охраны и их вид. Особенностью рассмотренных показателей является учет надежностных характеристик систем охраны, что позволяет более точно оценить реальные характеристики систем охраны, а также сформулирована задача синтеза оптимальной системы охраны.

ЛИТЕРАТУРА

1. Гайворонский И.Я., Белащков А.В. Разработка моделей системы охраны, обнаружения и мониторинга / Открытые информационные и компьютерные интегрированные технологии. – X.: ХАИ. – 1998. – Вып. 1. – С. 153 – 160.
2. Харченко В.С., Гайворонский И.Я. Задача оптимального резервирования вычислительных машин локальной сети // Надежность, живучесть и безопасность систем летательных комплексов. – X.: ХВУ. – 1996. – Вып.1. – С. 112 – 118.

Поступила 26.07.2002

ГАЙВОРОНСКИЙ Игорь Ярославович, канд. техн. наук, доцент кафедры Харьковского военного университета. В 1992 году окончил Харьковское ВВКУРВ. Область научных интересов – задачи оптимизации, эффективность систем охраны.
