УДК 621.391

А.И. Кушнир[1], К.С. Васюта[2], О.И. Сухаревский[2], С.В. Озеров[2], А.Н. Королюк[2]

[1]*Командование Воздушных Сил Вооруженных Сил Украины*
[2]*Харьковский университет Воздушных Сил имени Ивана Кожедуба, Харьков*

АНАЛИЗ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ МУЛЬТИПЛИКАТИВНОГО КОНГРУЭНТНОГО МЕТОДА ЛЕМЕРА ДЛЯ СТЕГАНОГРАФИЧЕСКОЙ ПЕРЕДАЧИ ДАННЫХ В СИСТЕМЕ ВОЕННОЙ РАДИОСВЯЗИ

В работе проведен анализ статистических и динамических свойств базовой псевдослучайной последовательности чисел сформированной с помощью мультипликативного конгруэнтного метода Лемера. Показано, что применение данной последовательности в качестве модулирующей функции гармонической несущей позволяет получить информационный гармонический сигнал, обладающий повышенной скрытностью за счет схожести статистических и динамических характеристик информационного сигнала с аналогичными характеристиками шума наблюдения. Такой подход формирования скрытного сигнала развивает возможности стеганографических систем передачи данных.

Ключевые слова: *мультипликативный конгруэнтный метод Лемера, гармоническое колебание, шум наблюдения, стеганографическая передача данных.*

Введение

В современной теории военного противоборства все большее значение придается внедрению новых систем управления, основанных на сетецентрических принципах, при этом основой такой системы управления является система связи.

Основным требованием, предъявляемым к современным системам связи, является их повышенная помехозащищенность, которая характеризуется успешным противодействием системы деструктивному воздействию со стороны противника. Под основой современного деструктивного воздействия на системы радиосвязи (СРС) [1] следует понимать применение средств радиоэлектронной борьбы (РЭБ) и радиоэлектронного подавления (РЭП).

Одним из подходов повышения помехозащищенности СРС является применение стеганографических методов передачи информации [2], которые используются с целью формирования скрытого (незаметного) канала передачи информации. Его целью является не ограничивать или регламентировать доступ к сигналу (файлу-контейнеру), а в значительной степени гарантировать то, что встроенные данные останутся не обнаруженными и не подлежащими восстановлению [3].

Исходя из **анализа литературы** [4, 5] при построении радиотехнической стеганосистемы должны учитываться следующие требования:

– скрытие факта передачи информации для стороннего наблюдателя;

– обеспечение необходимой пропускной способности (что особенно актуально для скрытой передачи данных);

– обеспечение аутентичности и целостности конфиденциальной информации для авторизированного пользователя;

– обнаружение скрытого сообщения сторонним наблюдателем, не должно позволить последнему извлечь его до тех пор, пока принцип формирования сигнала («ключа») сохраняется в тайне.

К стеганографическим методам скрытия информации в радиосвязи можно отнести использование широкополосных (с применением псевдослучайных последовательностей) сигналов, т.е. работа под “шум”, когда разведывательный приемник не может обнаружить (накопить) передаваемый сигнал, за счет схожести сигнала со случайным процессом при визуальном, корреляционном и спектральном анализе. Однако псевдослучайные последовательности, (М-последовательности, линейные рекуррентные последовательности и т.д.) применяемые для расширения спектра гармонического сигнала не отвечают требованиям скрытности в полной мере, так как имеют сравнительно короткий период генерируемой последовательности, обладают ярко выраженной зависимостью между последовательными соседними значениями и неравномерностью распределения значений (амплитуд).

Целью работы является анализ возможности применения базовой псевдослучайной последовательности чисел сформированной с помощью мультипликативного конгруэнтного метода Лемера для обеспечения стеганографической передачи данных.

Изложение основного материала

Ниже в работе предполагается, что цифровая информация представляется в виде «кодов Лемера» [6] и далее этой информационной последовательностью модулируется гармоническая несущая по частоте.

Основная формула мультипликативного конгруэнтного метода Лемера имеет вид [6]:

$$R_{n+1} = aR_n (\mathrm{mod}\, m), \qquad (1)$$

где a и m – неотрицательные целые числа.

Согласно этому выражению, необходимо взять случайное число R_n, умножить его на постоянный коэффициент a и взять модуль полученного числа по m (т.е. разделить на aR_n и остаток считать как R_{n+1}). Поэтому для генерирования последовательности R_n необходимы начальные значения R_0, множитель a и модуль m. Выбор значений a, R_0 и m производится так, чтобы обеспечить максимальный период неповторяющейся последовательности R_n и минимальную корреляцию между генерируемыми числами.

На рис. 1 проиллюстрирована временная реализация псевдослучайной последовательности (ПСП) R_n.

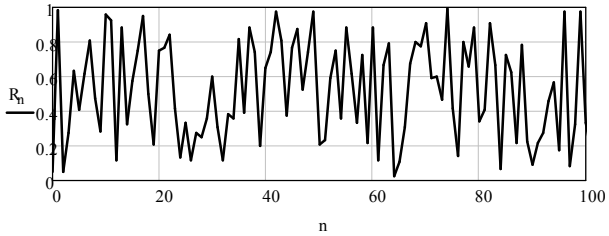


Рис. 1. Временная реализация псевдослучайной последовательности R_n

Для моделирования последовательности были использованы следующие значения: $a=5^{13}$, $m=2^{31}+1$, $R_0=0{,}052$, n=1000. Анализ рисунка показывает, что временная реализация имеет ярко выраженный шумоподобный характер.

Далее рассмотрим статистические и динамические характеристики ПСП: закон распределения амплитуд, автокорреляционная функция, амплитудно-частотный спектр, фазовый портрет (рис. 2). Из анализа рисунка следует, что закон распределения амплитуд, амплитудно-частотный спектр и фазовый портрет ПСП сходны с аналогичными характеристиками шума наблюдения; автокорреляционная функция последовательности подобна автокорреляционной характеристике простого гармонического радиоимпульса, что не удовлетворяет требованиям скрытности в полной мере, так как применение несанкционированным наблюдателем корреляционного анализа позволяет отличать ПСП от шума наблюдения. Также следует отметить, что ПСП полученная с помощью метода Лемера не обладает достаточной криптоустойчивостью (структурной скрытностью).

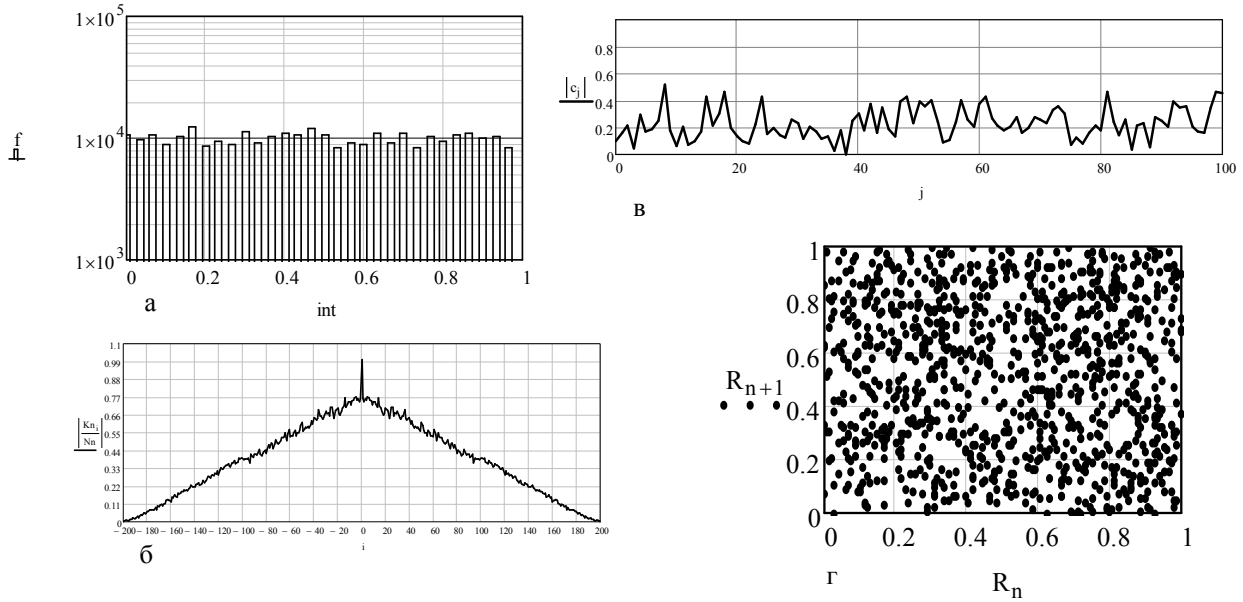


Рис. 2. Статистические и динамические характеристики ПСП сформированной методом Лемера:
а – закон распределения амплитуд; б – автокорреляционная функция;
в – амплитудно-частотный спектр; г – фазовый портрет

Поэтому с целью формирования шумоподобного информационного сигнала обладающего повышенной скрытностью факта передачи информации рассмотрим возможность расширения спектра гармонического колебания при помощи базовой ПСП полученной с помощью метода Лемера. Способ передачи информации с расширением спектра сигналов заключается: на передающей стороне – в одновременной и независимой модуляции параметров сигнала специальным кодом (расширяющей спектр функцией) и передаваемым сообщением. На приемной стороне – в синхронной демодуляции сигнала в соответствии с расширяющей спектр функцией и восстановлении переданного сообщения [7].

Методы расширения спектра могут базироваться на модуляции любого из параметров сигнала: амплитуды, фазы, частоты, временного положения (задержки) сигнала в соответствии со специальным кодом, формируемым на основе псевдослучайной последовательности. Основными, базовыми методами расширения спектра сигналов, широко применяемыми в современных СРС являются [7]:

– метод непосредственной модуляции несущей ПСП;

– метод псевдослучайной перестройки рабочей частоты (ППРЧ);

– метод псевдо-временной импульсной модуляции (ПВИМ);

– метод совместного (комбинированного) использования различных методов расширения спектра (например, метода непосредственной модуляции несущей ПСП и метода ППРЧ; метода ППРЧ и метода ПВИМ).

Рассмотрим метод непосредственной модуляции несущей ПСП. Данный метод модуляции несущей называется ″прямое расширение спектра сигналов с помощью ПСП″. При данном методе расширение спектра достигается непосредственной модуляцией несущей частоты, или за счет последовательной перестройки рабочей фазы передаваемого сигнала [7, 8]. Остановим свой выбор на методе непосредственной модуляции несущей частоты. Гармоническое колебание U_n описывается аналитическим выражением:

$$U_n = A\cos(\pi f_0 n), \qquad (2)$$

где A – амплитуда сигнала;

f_0 – частота колебания.

Путем частотной модуляции гармонического колебания ПСП (1) выражение (2) примет вид:

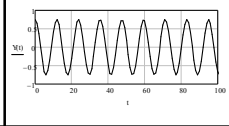
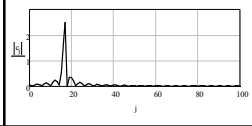
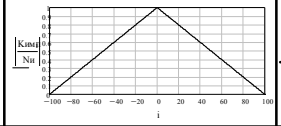
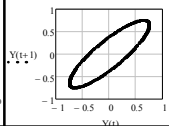
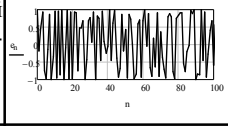
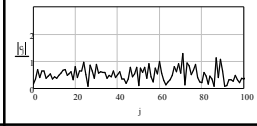
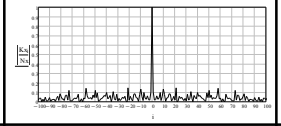
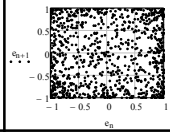
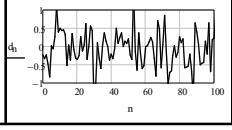
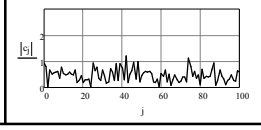
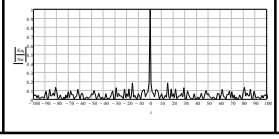
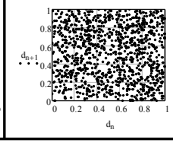
$$E_n = A\cos(\pi f_0 a R_n (\mathrm{mod}\, m) n). \qquad (3)$$

В табл. 1 приведены результаты математического моделирования информационного сигнала с расширением спектра.

Также для сравнения приведены статистические и динамические характеристики гармонического колебания и шума наблюдения.

Таблица 1

Статистические и динамические свойства гармонических сигналов и случайных процессов

№	Вид сигнала (процесса)	Временная реализация	Частотный спектр	Автокорреляционная функция	Фазовый портрет
1	Гармоническое колебание				
2	Информационный сигнал с расширением спектра				
3	Шум с равномерным распределением				

Сравнительный анализ приведенных выше характеристик сигналов и шума наблюдения показывает, что в результате частотной модуляции гармонического колебания базовой ПСП сформированной при помощи метода Лемера синтезирован информационный сигнал, статистические и динамические характеристики которого подобны шуму наблюдения.

Следует отметить важное замечание. Визуальная оценка фазового портрета на предмет отсутствия его структурированности носит чисто субъективный характер, поэтому адекватно проанализирована быть не может. Для качественного анализа фазовых портретов необходимо применять более ″тонкие″ инструменты″, например BDS-статистику [9], которая учитывает дополнительные свойства сигнала в фазовом пространстве. Количественное вычисление BDS-теста (BDS≤1,96), по методике подробно изложенной в работе [9] показывает, что фазовый портрет синтезированного информационного сигнала с расширением спектра не обладает структурированностью в фазовом пространстве и соответственно обладает повышенной скрытностью. Для оценки качества выделения информационного сообщения была рассчитана вероятность (коэффициент) битовых ошибок (BER) [10], которая характеризует качество передачи информации. Этот коэффициент представляет собой количество ошибок, отнесенное к количеству переданных битов, при условии, что ошибки имеют характер стационарного случайного процесса.

Рассматривалось два случая – когерентная обработка информационного сигнала (4) и некогерентная обработка (5):

$$\mathrm{BER} = Q\sqrt{E_b/N_0}\,; \qquad (4)$$

$$\mathrm{BER} = \frac{1}{2}Q\left(-E_b/(2N_0)\right), \qquad (5)$$

где Q(x) – гауссов интеграл ошибок; E_b/N_0 – отношение мощности сигнала к спектральной плотности шума.

Зависимость вероятности битовых ошибок от спектральной плотности мощности шума на бит информации приведена на рис. 3.

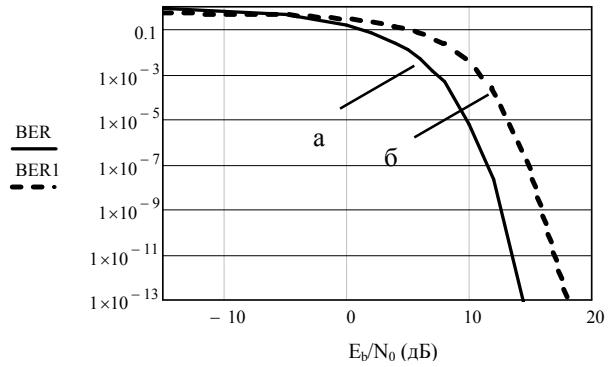


Рис. 3. Зависимость вероятности битовых ошибок от спектральной плотности мощности шума на бит информации: а – при когерентной обработке; б – при некогерентной обработке

Сравнивая BER при некогерентной и когерентной обработке, можно отметить, что при равных значениях сигнала и шума, некогерентная обработка требует приблизительно на 1 – 2 ДБ большего отношения мощности сигнала к спектральной плотности шума, чем когерентная. Однако некогерентная обработка легче реализуется, поскольку не требуется генерировать когерентные опорные сигналы [10].

Выводы

Проведенный в работе анализ статистических и динамических характеристик базовой псевдослучайной последовательности чисел сформированной с помощью мультипликативного конгруэнтного метода Лемера показывает, что характеристики ПСП подобны характеристикам шума наблюдения, за исключением автокорреляционной функции.

Модуляция по частоте гармонической несущей информационной последовательностью, полученной с помощью «кодов Лемера» позволяет получить информационный сигнал, который обладает повышенной скрытностью за счет схожести его фазового портрета с портретом шума наблюдения.

Таким образом, идея применения такого сигнала может быть реализована для развития стеганографических методов передачи цифровой информации в комплексах широкополосной радиосвязи военного назначения, что в свою очередь является актуальным при создании систем управления, основанных на сетецентрических принципах.

Список литературы

1. Макаренко С.И. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты / С.И. Макаренко, М.С. Иванов, С.А. Попов. – СПб.: Свое издательство, 2013. – 166 с

2. Васюта К.С. Особенности построения стеганографических систем радиосвязи / К.С. Васюта, С.В. Озеров, А.Н. Королюк // Проблемы телекоммуникаций. – Х.: ХНУРЭ, 2012. – Вип. 3(8). – С. 94-104.

3. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К: "МК-Пресс", 2006. – 288 с.

4. Основи комп'ютерної стеганографії / В.О. Хорошко, О.Д. Азаров и др. – Вінниця: ВДТУ, 2003 – 143 с.

5. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, В.Н. Оков, И.В. Туринцев. – М: Солон-пресс, 2002 – 272 с.

6. Денисова Э.В. Основы вычислительной математики: учебно-метод. пос. / Э.В. Денисова, А.В. Кучер. – СПб.: СПбГУ ИТМО, 2010 – 164 с.

7. Борисов В.И. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / В.И. Борисов, В.М. Зинчук, А.Е. Лимарев. – М.: РадиоСофт, 2008. – 512 с.

8. Иванов М.С. К вопросу помехоустойчивости систем воздушной радиосвязи при действии сосредоточенных и импульсных помех / М.С. Иванов, В.Е. Федосеев // Актуальные проблемы вузов ВВС: межвузовский сборник. Вып. 28. – М.: МО РФ, 2009. – С. 150-153.

9. Использование BDS-статистики для оценки скрытности сигнала, полученного перемешиванием хаотической несущей / П.Ю. Костенко, К.С. Васюта, А.Н. Барсуков [и др.] // Известия вузов. Радиоэлектроника. – 2010. – № 5 (53). – С. 41-45.

10. Скляр Б. Цифровая связь. Теоретические основы и практическое применение: пер. с англ. / Б. Скляр. – М: Издательский дом Вильямс, 2003 – 1104 с.

Поступила в редколлегию 9.10.2013

Рецензент: д-р техн. наук, проф. П.Ю. Костенко, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

АНАЛІЗ МОЖЛИВОСТІ ЗАСТОСУВАННЯ МУЛЬТИПЛІКАТИВНОГО КОНГРУЕНТНІСТЮ МЕТОДУ ЛЕМЕРА ДЛЯ СТЕГАНОГРАФІЧНОЇ ПЕРЕДАЧІ ДАНИХ У СИСТЕМІ ВІЙСЬКОВОГО РАДІОЗВ'ЯЗКУ

О.І. Кушнір, К.С. Васюта, О.І. Сухаревський, С.В. Озеров, О.М. Королюк

У роботі проведено аналіз статистичних і динамічних властивостей базової псевдовипадкової послідовності чисел сформованої за допомогою мультиплікативного конгруентного методу Лемера. Показано, що застосування даної послідовності в якості модулюючої функції гармонійної несучої дозволяє отримати інформаційний гармонійний сигнал, що має підвищену скритність за рахунок схожості статистичних та динамічних характеристик інформаційного сигналу з аналогічними характеристиками шуму спостереження. Такий підхід формування скритного сигналу розвиває можливості стеганографічних систем передачі даних.

Ключові слова: *мультиплікативний конгруентний метод Лемера, гармонійне коливання , шум спостереження , стеганографічна передача даних.*

ANALYSIS OF POSSIBILITY OF APPLICATION THE MULTIPLICATIVE CONGRUENT METHOD OF LEMER FOR STEGANOGRAPHIC TRANSMITTING DATA IN THE MILITARY RADIOSYSTEM

A.I. Kyshnir, K.S. Vasyta, O.I Syharevsky, S.V. Ozerov, A.N. Korolyk

The paper analyzes the statistical and dynamical properties of the base sequence of pseudo-random numbers generated by multiplicative congruent method of Lemer. It is shown that the use of this sequence as the modulation function provides a harmonic carrier wave signal information that has greater secrecy due to the similarity of statistical and dynamic characteristics of an information signal with similar observation noise. This approach is the formation of covert signal builds the capacity of steganographic data transmission systems.

Keywords: *multiplicative congruent method of Lemer, harmonic motion, observation noise, steganographic data transfer.*