УДК 681.3

КОРРЕЛЯЦИОННЫЕ СВОЙСТВА ПСЕВДОСЛУЧАЙНОЙ БИНАРНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ НА ОСНОВЕ СИСТЕМЫ КЛАССОВ ВЫЧЕТОВ

В.С. ЛИТВИНОВ, Д.М. БИЛЬДЮК

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 4 июня 2018

Аннотация. Предложен алгоритм синтезирования стохастических кодовых структур на основе классов вычетов, позволяющих формировать ансамбли с приемлемыми корреляционными свойствами, криптографическим уровнем сложности формируемых ансамблей, зависимых от ключа, и произвольной длиной последовательностей, не влияющей на мощность кодовой структуры, а лишь определяющей ее верхнюю границу.

Ключевые слова: радиотехника, цифровой канал, криптографическое кодирование, псевдослучайные последовательности, система классов вычетов.

Abstract. It proposed to synthesize the stochastic code structures based on residue number system, which allows to form ensembles with acceptable correlation properties, cryptographic difficulty level of formed ensembles, depending on key, and with any length of sequence, which doesn't affect on the power of code structure, but defines its upper limit.

Keywords: radioengineering, digital channel, cryptographic coding, pseudorandom sequences, residue number system.

Doklady BGUIR. 2019, Vol. 123, No. 5, pp. 38-44
Correlation properties of binary pseudorandom sequence
based on residue number system
V.S. Litvinov, D.M. Bildziuk

DOI: http://dx.doi.org/10.35596/1729-7648-2019-123-5-38-44

Введение

При передаче информации по цифровым каналам в мобильных системах радиосвязи и радиоопределения стоит задача повышения устойчивости систем к случайным и преднамеренным помехам, обеспечивая при этом одновременную работу систем в общей полосе частот. Эта задача решается путем использования широкополосных сигналов в виде псевдослучайных последовательностей. Поскольку для систем цифровой связи актуальна защита не только от помех, но и от несанкционированного доступа к информации, передаваемые данные подвергают также и криптографическому кодированию.

В связи с этим существует необходимость формирования такой кодовой системы, которая позволит противостоять случайным и преднамеренным помехам, возникающим в канале связи, и в то же время обеспечивать высокую структурную скрытность передаваемой информации.

Свойства псевдослучайных последовательностей

В цифровых системах с множественным доступом с кодовым разделением (CDMA) каждому пользователю выделяется уникальная ключевая последовательность, которая

позволяет пользователю выделить предназначенный ему сигнал в выделенной полосе частот. Множественные сигналы в приемнике разделяются посредством корреляции принимаемого сигнала с персональной ключевой последовательностью пользователя. Для минимизации помех, возникающих при демодуляции сигналов, поступающих от многих передатчиков, формируют кодовые последовательности с относительно малыми значениями взаимной корреляции. Демодуляция и разделение этих сигналов в приемнике не вызывают затруднений ввиду того, что каждый сигнал посредством введения псевдослучайной последовательности расширяется по спектру.

Высокое значение избыточности широкополосных сигналов позволяет снижать уровни интерференции, возникающей в радио- и спутниковых каналах цифровой связи. Не менее важным свойством широкополосных сигналов является их псевдослучайность, благодаря которой передаваемые сигналы становятся похожи на случайный шум, и таким образом затрудняется его детектирование сторонними пользователями [1].

Поскольку в системах с *CDMA* псевдослучайные последовательности выполняют функцию «ключа», важной задачей, решаемой с их помощью, является разделение и выделение сигналов различных пользователей. Характеристика псевдослучайной последовательности, на основе которой принимается решение о выделении полезного сигнала, называется автокорреляционной функцией. Автокорреляционная функция $R_a(\tau)$ в общем виде определяется интегралом

$$R_a(\tau) = \int_{-\infty}^{\infty} f(t) f(t-\tau) d\tau. \qquad (1)$$

Она является мерой соответствия между сигналом $f(t)$ и его копией, сдвинутой во времени на τ.

В идеале псевдослучайная последовательность длины L должна иметь автокорреляционную функцию со свойством $\phi(0) = L$ и $\phi(j) = 0$ для $1 \le j \le L-1$, что необходимо для обеспечения точного времени начала синхронизации принятого сигнала и его гарантированного выделения.

Для минимизации помехи по соседним каналам и определения порога принятия решения используют характеристику, называемую взаимокорреляционной функцией. Взаимокорреляционная функция $R_c(\tau)$ является мерой соответствия двух различных сигналов $f(t)$ и $g(t)$ при их сдвиге во времени на τ и определяется интегралом

$$R_c(\tau) = \int_{-\infty}^{\infty} f(t) g(t-\tau) d\tau. \qquad (2)$$

Полный ансамбль псевдослучайных последовательностей должен быть выбран таким, чтобы взаимная корреляция между любой парой последовательностей была достаточно мала. Согласно теории, нулевое значение взаимокорреляционной функции имеют ортогональные друг относительно друга сигналы. Но на практике требуется, чтобы в системах радиосвязи формирование ансамблей псевдослучайных последовательностей было как можно более простым.

Одними из наиболее известных и хорошо изученных псевдослучайных последовательностей являются *M*-последовательности, или последовательности максимальной длины. Если речь идет о системах связи, ориентированных на одного пользователя, *M*-последовательности выглядят весьма привлекательно. Однако в связи с требованиями к взаимокорреляционным свойствам ключевых псевдослучайных последовательностей в системах с *CDMA* Голд и Касами предложили последовательности с лучшими свойствами периодической функции взаимной корреляции.

Если сравнивать последовательности Голда с обычными *M*-последовательностями, первые являются более подходящими для систем спутниковой и сотовой связи с CDMA ввиду того, что для таких систем необходимо значительно большее число последовательностей с хорошими значениями взаимной корреляции между ними. Метод построения таких последовательностей состоит в сложении двух различных *M*-последовательностей по модулю 2.

В результате такого синтеза для длины псевдослучайной последовательности, равной N, можно получить ансамбль объемом $M = N + 2$ [2].

Последовательности Голда позволяют обеспечить минимизацию интерференционных помех в цифровом канале связи за счет большой мощности ансамбля псевдослучайных последовательностей. В то же время существуют две проблемы, которые данные последовательности не могут решить. Первый из них заключается в необходимости последующего криптографического кодирования с целью защиты передаваемой информации от несанкционированного доступа. Несмотря на свою шумоподобность, такие сигналы могут быть обнаружены и декодированы при помощи профессиональных систем, имеющих в своем составе наборы корреляторов. Второй проблемой является тот факт, что объем ансамбля последовательностей Голда строго фиксирован, что влечет за собой повышение требований к вычислительным мощностям приемопередающей аппаратуры систем цифровой связи.

Алгоритм формирования СКВ-кодов

Таким образом, приобретает актуальность задача формирования такой псевдослучайной последовательности, которая обладала бы криптографическими свойствами и давала возможность изменения объема ансамбля. В качестве возможного решения этой задачи был предложен метод синтеза псевдослучайной последовательности на основе системы классов вычетов (далее – СКВ-коды). Этот метод описывается ниже.

Формирование СКВ-кодов основано на представлении ортогональных базисов системы классов вычетов (СКВ) в обобщенной позиционной системе счисления (ОПСС) [3]. На рис. 1 представлена блок-схема алгоритма формирования псевдослучайных последовательностей.

Изначально задаются требуемый объем ансамбля псевдослучайных последовательностей C, длина последовательности N и разрядность чисел b, составляющих базис системы счисления. Затем генерируется система оснований (базис) $p_1, p_2, ..., p_n$, состоящая из попарно взаимно простых чисел, размером $n \geq \log_2 C$. Имея в распоряжении систему оснований, необходимо вычислить матрицу преобразования чисел из СКВ в обобщенную позиционную систему счисления.

Вместе с этим также необходимо сгенерировать расширение системы оснований $p_{n+1}, p_{n+2}, ..., p_{n+k}$ размером таким, чтобы выполнялось следующее условие:

$$N = k \cdot b - 1. \quad (3)$$

С использованием вычисленной матрицы преобразования из СКВ в ОПСС и расширения системы оснований выполняют расширение матрицы преобразования [4].

На основании базиса СКВ $p_1, p_2, ..., p_n$ определяется диапазон возможных входных значений a по формуле

$$P = \prod_{i=1}^{n} p_i. \quad (4)$$

При этом вводимое целочисленное значение a, находящееся на интервале $[0, P)$, в представлении системы классов вычетов соответствует $a \to (a_1, a_2, ..., a_n)$, где $a_i \equiv a \bmod p_i$. Мощность выходного ансамбля определяется количеством изменяемых старших бит в числах $a_1, a_2, ..., a_n$.

Получив число a и расширенную матрицу преобразования, производят расширение числа a, выделяя при этом добавленную в процессе расширения часть. Выделенное расширение числа a переводится из СКВ в ОПСС (рис. 2), после чего производится битовая конкатенация и преобразование вектора чисел в двоичный код. Затем обрезаются лишние биты, и бинарная последовательность приводится к биполярному виду (–1; 1).

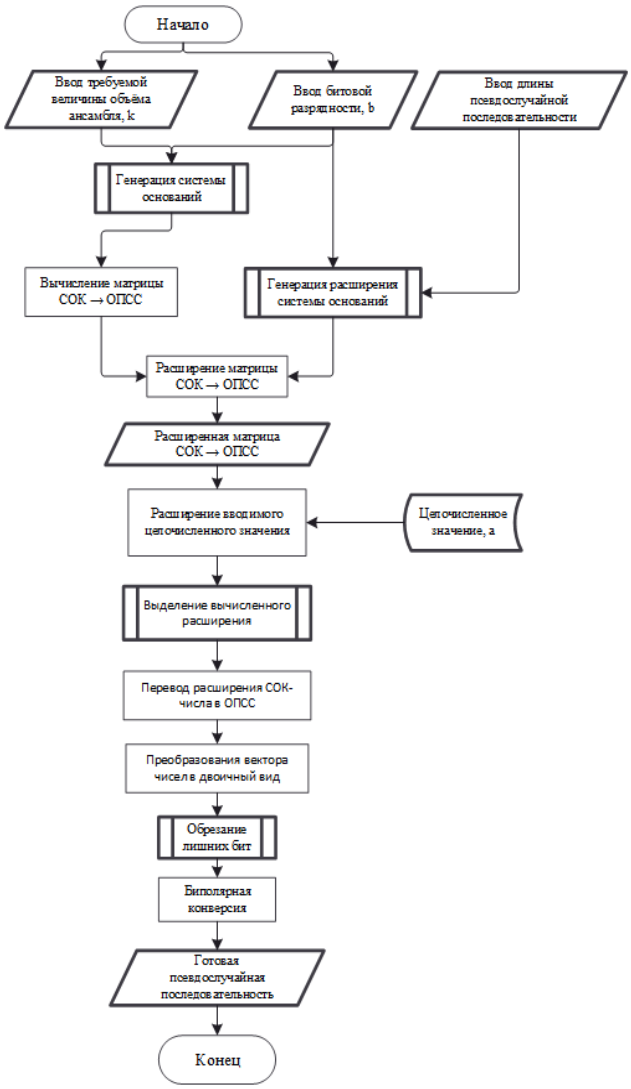

Рис. 1. Алгоритм формирования СКВ-кодов

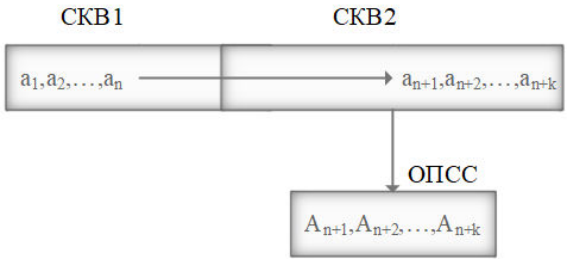

Рис. 2. Краткая схема преобразования СКВ-числа в расширение ОПСС

Полученная последовательность и есть генерируемая псевдослучайная последовательность, называемая псевдослучайной последовательностью на основе системы классов вычетов, или СКВ-кодом.

Для оценки целесообразности применения СКВ-кодов необходимо было сравнить величины боковых выбросов автокорреляционной характеристики и характеристики взаимной корреляции СКВ-кодов и кодов Голда. Исследование проводилось для последовательностей, имеющих длины 15, 31, 63, 127, 511 и 1023, с приблизительно равными мощностями ансамблей псевдослучайных последовательностей.

Исследование корреляционных свойств СКВ-кодов

В процессе построения корреляционных характеристик для СКВ-кодов согласно вышеприведенному алгоритму генерировались ансамбли определенного объема и заданной длины последовательностей. После этого внутри ансамбля проводились вычисления автокорреляционной и взаимокорреляционной функций. Таким образом, вычислялись $K_{ac} = M$ автокорреляционных характеристик и $K_{cc} = \frac{M^2 - M}{2}$ характеристик взаимной корреляции, где M – мощность ансамбля псевдослучайных последовательностей. В каждой вычисленной автокорреляционной функции выделялся максимальный боковой выброс, а затем среди этих максимумов находилось и сохранялось наибольшее значение. Аналогичная операция производилась для максимальных выбросов взаимокорреляционной функции. Для кодов Голда также генерировались ансамбли фиксированного объема и находились максимумы выбросов корреляционных характеристик. Зависимости выделенных максимумов корреляционных функций от длины псевдослучайной последовательности показаны на рис. 3–6.

На рис. 3, 4 показаны зависимости максимальных нормированных величин боковых выбросов автокорреляционной функции от длины псевдослучайной последовательности для кодов Голда и СКВ-кодов. Как видно из рисунков, автокорреляционные свойства СКВ-кодов несколько хуже, чем у кодов Голда.

На рис. 5, 6 показаны зависимости максимальных нормированных величин выбросов взаимокорреляционной функции от длины псевдослучайной последовательности для кодов Голда и СКВ-кодов. Здесь также можно видеть, что по свойствам взаимной корреляции СКВ-коды уступают кодам Голда.

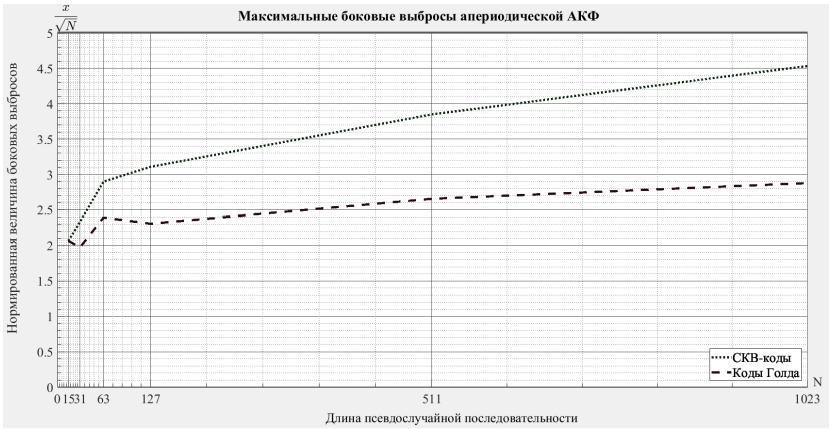

Рис. 3. Зависимость величины боковых выбросов апериодической АКФ от длины последовательности

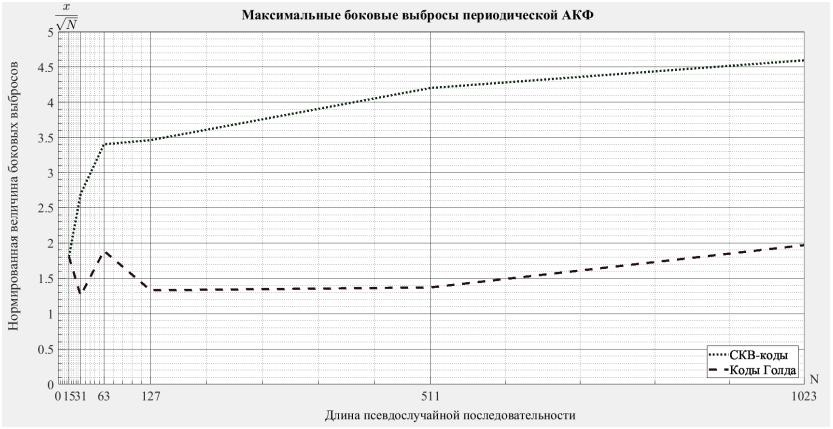

Рис. 4. Зависимость величины боковых выбросов периодической АКФ от длины последовательности

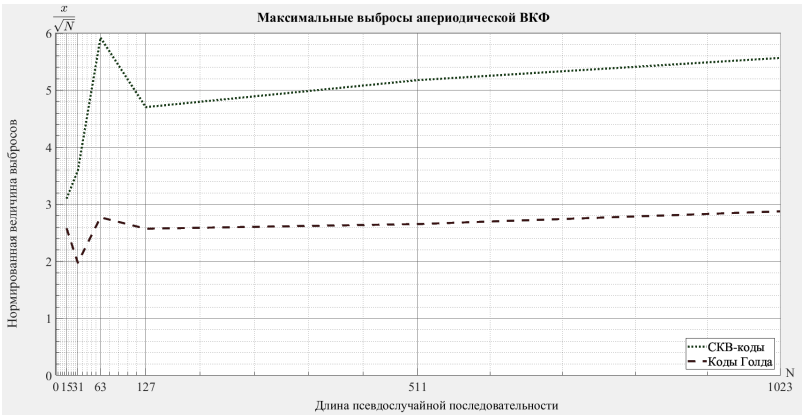

Рис. 5. Зависимость величины выбросов апериодической ВКФ от длины последовательности

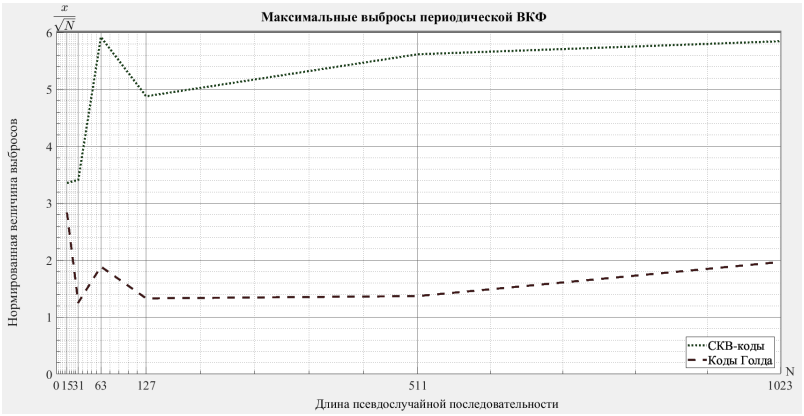

Рис. 6. Зависимость величины выбросов периодической ВКФ от длины последовательности

Заключение

На основании проведенных исследований можно рекомендовать использование СКВ-кодов в ряде ситуаций, когда приоритетной является задача создания защищенного канала связи без задействования больших вычислительных мощностей. СКВ-коды не требуют обязательного криптографического шифрования, поскольку количество комбинаций составления системы оснований и ее расширения достаточно большое, чтобы гарантировать высокий уровень защиты от подбора ключа и, как следствие, получения несанкционированного доступа к передаваемой информации. Также метод формирования этих кодов позволяет изменять объем их ансамбля, что дает возможность синтеза ограниченного количества ключевых псевдослучайных последовательностей большой длины, не прибегая к излишним вычислениям.

Список литературы

1. Прокис Дж. Цифровая связь. М.: Радио и связь. 2000. 800 с.
2. Феер К. Беспроводная цифровая связь. Методы модуляции и расширения спектра. М.: Радио и связь, 2000. 520 с.
3. Srubo N. Residue arithmetic and its applications to computer technology. New York, 1967. 238 p.
4. Червяков Н.И. Методы масштабирования модулярных чисел, используемые при цифровой обработке сигналов // Инфокоммуникационные технологии. 2006. № 4 (3). С. 15–24.

References

1. Prokis Dzh. Cifrovaja svjaz'. M.: Radio i svjaz'. 2000. 800 s. (in Russ.)
2. Feer K. Besprovodnaja cifrovaja svjaz'. Metody moduljacii i rasshirenija spektra. M.: Radio i svjaz', 2000. 520 s. (in Russ.)
3. Srubo N. Residue arithmetic and its applications to computer technology. New York, 1967. 238 p.
4. Chervjakov N.I. Metody masshtabirovanija moduljarnyh chisel, ispol'zuemye pri cifrovoj obrabotke signalov // Infokommunikacionnye tehnologii. 2006. № 4 (3). S. 15–24. (in Russ.)

Сведения об авторах

Бильдюк Д.М., старший преподаватель кафедры информационных радиотехнологий Белорусского государственного университета информатики и радиоэлектроники.

Литвинов В.С., магистрант кафедры информационных радиотехнологий Белорусского государственного университета информатики и радиоэлектроники.

Адрес для корреспонденции

220013, Республика Беларусь,
Минск, ул. П. Бровки, 6,
Белорусский государственный университет
информатики и радиоэлектроники
тел.: +375-29-198-33-20;
e-mail: anix.mig29@gmail.com
Литвинов Валентин Сергеевич

Information about the authors

Bildziuk D.M., senior lecturer of information radiotechnologies department of Belarusian state university of informatics and radioelectronics.

Litvinov V.S., master student of information radiotechnologies department of Belarusian state university of informatics and radioelectronics.

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovki, 6,
Belarusian state university
of informatics and radioelectronics
tel.: +375-29-198-33-20;
e-mail: anix.mig29@gmail.com
Litvinov Valentin Sergeevich