ПСЕВДОСЛУЧАЙНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ НА ОСНОВЕ СИСТЕМЫ КЛАССОВ ВЫЧЕТОВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Литвинов В.С.

Карпушкин Э.М. – к.т.н.,доцент

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 её верхнюю границу.

Широко используемые псевдослучайные последовательности, например, последовательности Голда, позволяют минимизировать интерференционные помехи в цифровом канале за счёт большой мощности ансамбля псевдослучайных последовательностей. Несмотря на свою шумоподобность, такие сигналы могут быть обнаружены и декодированы при помощи профессиональных систем, имеющих в своём составе наборы корреляторов. Кроме того, объём ансамбля стандартных последовательностей строго фиксирован, что влечёт за собой повышение требований к вычислительным мощностям приёмопередающей аппаратуры систем цифровой связи [1].

Таким образом, приобретает актуальность задача формирования такой псевдослучайной последовательности, которая обладала бы криптографическими свойствами и давала возможность изменения объёма ансамбля. В качестве возможного решения этой задачи предлагается метод синтеза псевдослучайной последовательности на основе системы классов вычетов (далее – СКВ-коды) [2]. Блок-схема алгоритма формирования таких последовательностей представлена на рисунке 1.

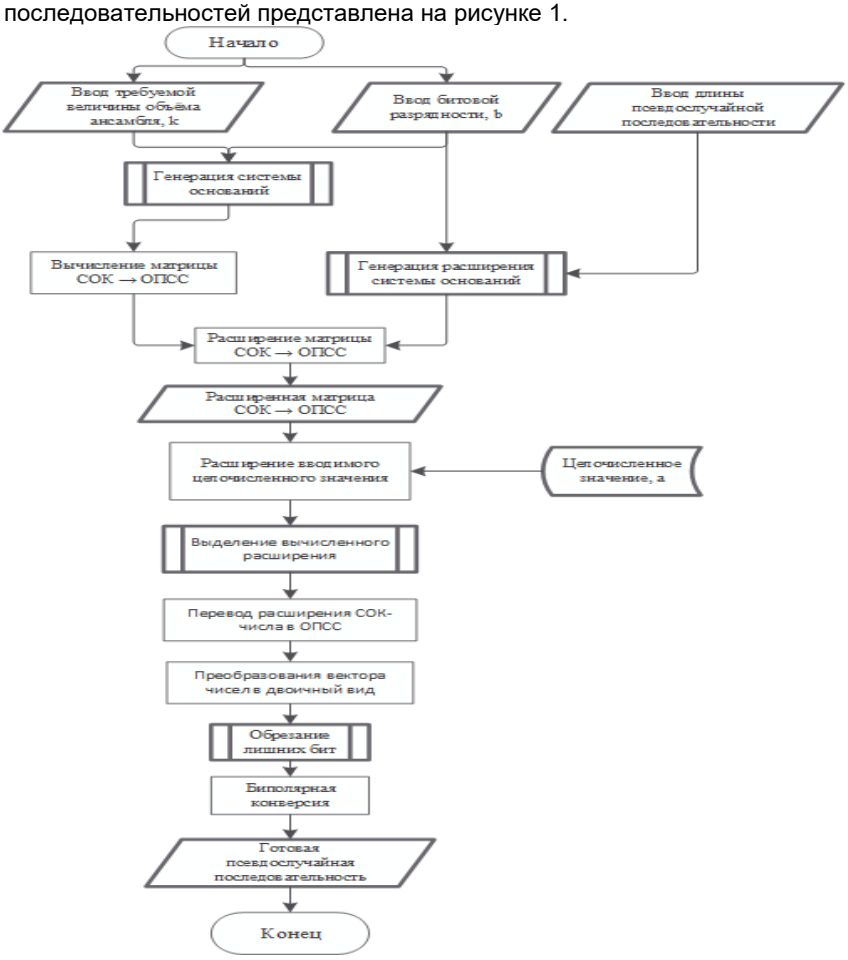

Рисунок 1 – Алгоритм формирования СКВ-кодов

Для оценки целесообразности применения СКВ-кодов необходимо было сравнить величины боковых выбросов автокорреляционной характеристики и характеристики взаимной корреляции СКВ-кодов и кодов Голда. Результаты исследований приведены на рисунках 2 и 3.

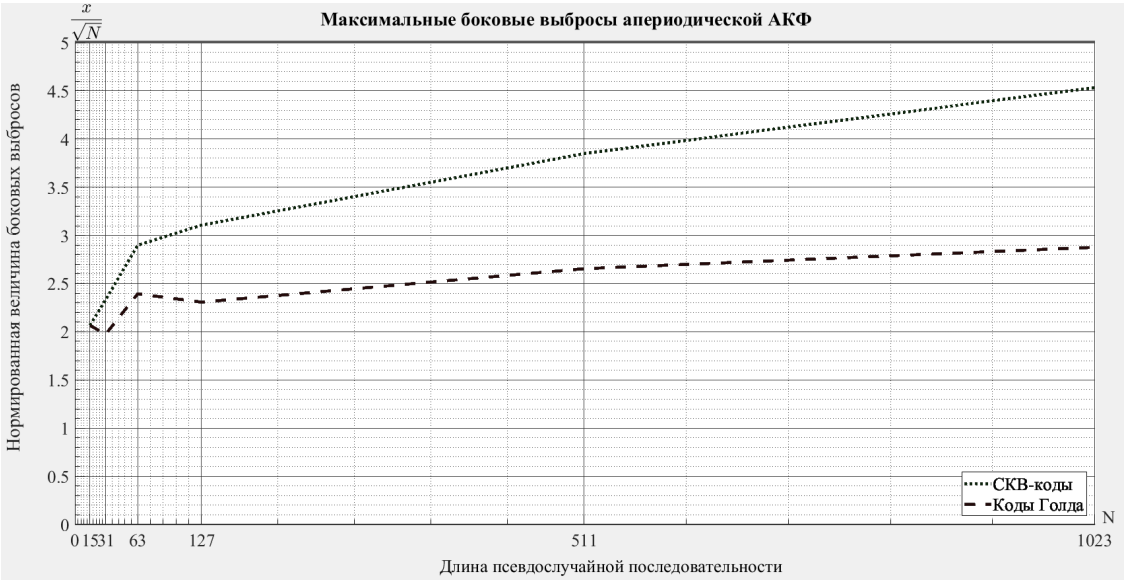

Рисунок 2 – Зависимость величины боковых выбросов АКФ от длины последовательности

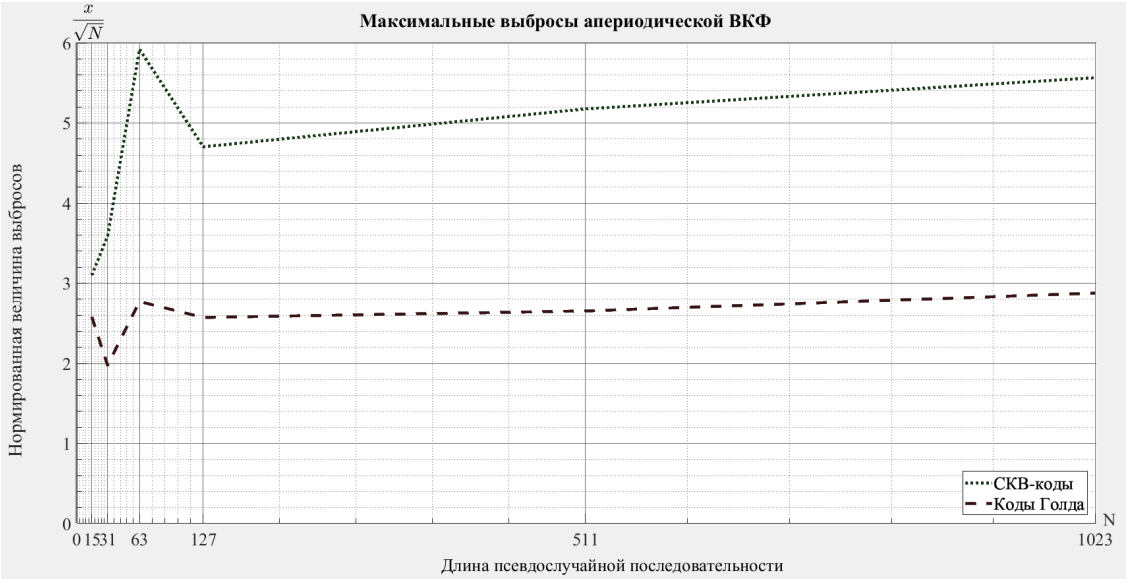

Рисунок 3 – Зависимость величины выбросов ВКФ от длины последовательности

На основании проведённых исследований можно рекомендовать использование СКВ-кодов в ряде ситуаций, когда приоритетной является задача создания защищённого канала связи без задействования больших вычислительных мощностей.

Список использованных источников:
1. Прокис Дж. Цифровая связь. Пер. С англ. / Под ред. Д.Д. Кловского. – М.: Радио и связь. 2000. – 800 с.: ил.
2. Srubo N., Tanako. Residue arithmetic and its applications to computer technology. – New York, 1967. – P.238.