АЛГОРИТМ УДОСКОНАЛЕННЯ БЛОКА МНОЖЕННЯ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ЧИСЕЛ В СКІНЦЕННОМУ ПОЛІ GF(3)

канд. техн. наук, проф. О.М. Рисований, Національний технічний університет "Харківський політехнічний інститут", м. Харків

Необхідність використовування випадкових чисел у науковій роботі виникла давно. З появою комп'ютера та зі збільшенням щільності запису на магнітних та оптичних носіях стало можливим використання великих таблиць випадково згенерованих байтів. Однак ні табличний метод, ні апаратна генерація випадкових чисел не могли задовольнити потребу в надійних, швидких та ефективних генераторах випадкових чисел через властиві цим методам відомі недоліки.

Найчастіше застосовують такі генератори псевдовипадкових чисел у полі GF(2). Один із недоліків таких генераторів – короткий період генерації таких двійкових послідовностей.

Найбільш цікавими властивостями та можливостями володіють генератори в скінченному полі GF(3), які побудовані з використанням блоку множення коефіцієнтів поля.

У роботі розглянуто математичну модель нелінійного генератора, показано зв'язки одноканальної та багатоканальної нелінійних структур, наведено схему такого генератора і, як приклад, повну матрицю вихідних станів нелінійного генератора, який має максимальний період. Крім того, показаний приклад запису початкового стану загального випадку нелінійності.

Запропоновано метод синтезу генераторів нелінійної псевдовипадкової послідовності у скінченному полі GF(3) зі спрощенням блоку множення [1, 2]. Таке спрощення можливе при певному кодуванні сигналів [3], що дозволяє як операцію множення застосовувати перехресні лінії виходів тригерів відповідного каналу регістра.

Список літератури: 1. *Рысованый А.Н.* Метод синтеза нелинейных генераторов в конечном поле GF(3) на основе использования матриц связей и состояний / *А.Н. Рысованый* // Системи управління, навігації та зв'язку. – Полтава –2018. – №5 (51).– С. 111-114. **2.** *Иванов М.А.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей / *М.А. Иванов, И.В. Чугунков.* – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с. **3.** *Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов. – М.: Мир. – 1989 . – 448 с.