

**ДОСЛІДЖЕННЯ ТА РЕАЛІЗАЦІЯ АЛГОРИТМУ ОТРИМАННЯ
ПСЕВДОВИПАДКОВОЇ ПОСЛІДОВНОСТІ НА МІКРОКОНТРОЛЕРІ**

Створення, вдосконалення вже існуючих алгоритмів отримання псевдовипадкових послідовностей, їх реалізація в засобах технічного захисту інформації виконує величезну роль в цій сфері, зокрема в криптографії.

Даний алгоритм генерації випадкових чисел дещо схожий з алгоритмом виділення дробової частини многочлена першої степені, або синуса числа. Алгоритм описується таким аналітичним виразом:

$$a_{n+1} = \begin{cases} \left(\frac{a_n}{b_n}\right) \bmod(1), \left(\frac{a_n}{b_n}\right) \bmod(1) > 1; \\ \left(\frac{a_n}{b_n} \cdot 1000\right) \bmod(1), \left(\frac{a_n}{b_n}\right) \bmod(1) < 1; \end{cases} \quad (1)$$

$$a_{n+1,m+1} = (i(a_{n+1})) \bmod(255)$$

Тут операція $i(\cdot)$ означає виділення цілої частини числа. Кінцева послідовність чисел алгоритму формується членами $a_{n,m}$, які обчислюються з попередньо обчислених членів a_n . Обмеження чисел за модулем 255 – для запису в восьми розрядний регістр лічильника мікроконтролера. Записуючи в регістр лічильника числа, що генеруються за алгоритмом (1), на вихідному виводі мікроконтролера формуються імпульси з тривалостями та «паузами», що пропорційні цим числам.

Щоб перевірити отриману послідовність чисел на псевдовипадковість – було проведено порівняння її характеристик з характеристиками стандартної функції `rand()` мови програмування СИ. Такі характеристики як автокореляційна функція, спектр потужності (розраховані та побудовані в програмному середовищі Wolfram Mathematica 8) та гістограма послідовності що перевірялась, підтвердили її псевдовипадковість. Часові та спектральні характеристики сигналу на виході схеми були зняті на реальному макеті за допомогою цифрового осцилографа TDS1012B, що підтвердило моделювання в Proteus 6.0.

Отже, генератор псевдовипадкової послідовності може використовуватись в захищеній лінії зв'язку любительської категорії (оскільки послідовність не перевірялась на криптостійкість), а також має методичну цінність (може використовуватись як лабораторний макет).

Науковий керівник – к.в.н., доц., С.Я. Довбня