

УДК 004.421

UDC 004.421

**ГЕНЕРАЦИЯ ЦЕЛОЧИСЛЕННЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ЗАДАНЫМ ВЕСОМ И ОГРАНИЧЕНИЕМ ПО ЗНАЧЕНИЮ РАЗРЯДА****INTEGER SEQUENCE GENERATION WITH A GIVEN WEIGHT AND WITH LIMITATION BY POSITION VALUE***Е. А. Зайцева**E. A. Zaytseva*

Донской государственной технической университет, Ростов-на-Дону, Российская Федерация

Don State Technical University, Rostov-on-Don, Russian Federation

[ekstrasitro@gmail.com](mailto:ekstrasitro@gmail.com)[ekstrasitro@gmail.com](mailto:ekstrasitro@gmail.com)

Рассмотрена задача по искусственному созданию (генерации) целочисленных последовательностей с заданным весом и ограничением по значению разряда. На основе проведенного анализа алгоритма работы такого генератора были сформулированы основные задачи реализации данного метода на ЭВМ, а также решены некоторые дополнительные задачи.

The article considers the problem of artificial creation (generation) of integer sequences with a given weight and the limitation by position value. On the basis of the analysis of the algorithm of this generator the author has generated the main tasks to implement this method on a computer, and solved some of the additional tasks

**Ключевые слова:** генерация последовательности, шифрование, целочисленные последовательности.

**Keywords:** sequence generation, encryption, integer sequence.

**Введение.** Для шифрования зачастую используются искусственно созданные цифровые последовательности, которые смешиваются на передающей стороне с кодограммами, а на принимающей стороне отфильтровываются от пришедших кодовых посылок, с выделением исходных кодограмм [1].

**Основная часть.** Для вышеописанных способов шифрования как передающей, так и принимающей стороне необходимо знать алгоритмы получения искусственно созданных цифровых последовательностей. Одним из способов получения таких последовательностей может быть создание алгоритма формирования десятичных чисел заданной разрядности  $n$  и заданного веса  $S$  (вес — сумма значений числа в разрядах) с ограничениями по значениям каждого разряда, заданным в паспорте кода.

Продемонстрируем работу алгоритма на следующем примере: формируется четырехразрядный код с весовой суммой разрядов каждого числа, равной 15. Ограничения по значениям чисел в разрядах: 5 — для первого разряда, 5 — для второго, 6 — для третьего и 8 — для четвертого разряда.

Описательный алгоритм формирования последовательности может быть проиллюстрирован таблицей 1. Инвертируем в таблице последовательность разрядов таким образом, чтобы в первой колонке ограничение равнялось 8, в соответствии с первым разрядом.

Таблица 1

Последовательности, полученные в результате работы алгоритма

|     |   |   |   |   |
|-----|---|---|---|---|
| $S$ | 5 | 5 | 6 | 8 |
| 15  | 0 | 1 | 6 | 8 |
| 15  | 0 | 2 | 6 | 7 |
| 15  | 0 | 3 | 6 | 6 |
| 15  | 0 | 4 | 6 | 5 |
| 15  | 0 | 5 | 6 | 4 |
| 15  | 1 | 5 | 6 | 3 |
| 15  | 2 | 5 | 6 | 2 |

Основными задачами для формирования подобного кода являются составление алгоритма формирования и определение числа значений генерируемых последовательностей (числа строк в таблице). Последняя задача в настоящее время аналитически не решена. Для каждой конкретной задачи возможно вычислить количество строк в зависимости от веса, ограничений и количества разрядов, но в общем виде, к сожалению, это пока невозможно.

**Заключение.** Приведем пример, иллюстрирующий эту проблему. Если вес установить равным 1, то получаем четыре последовательности: 0001, 0010, 0100, 1000. При увеличении веса до 3 количество последовательностей резко возрастает. Генерация таких последовательностей в настоящее время не описана, хотя возможности их применения широки. Основным их достоинством является то, что при шифровании число степеней свободы равно  $N+1$ , где  $N$  — возможное число комбинаций с ограничением в разрядах ( $\sum b_i \geq S$ ), при условии  $\sum b_i \geq S, i = \overline{1, n}$ ,  $n$  — число разрядов.

#### Библиографический список.

1. Гмурман, В. Е. Теория вероятностей и математическая статистика / В. Е. Гмурман. — Москва : Высшая школа, 2003. — 479 с.