К ВЫБОРУ СТРУКТУР АРИФМЕТИЧЕСКИХ БЛОКОВ ДЛЯ УСТРОЙСТВ ТЕОРЕТИКО-ЧИСЛОВОГО ПРЕОБРАЗОВАНИЯ.

Ивашко А.В., Лунин Д.А.

Національний технічний університет "Харківський політехнічний інститут", м. Харків

В последние годы получили широкое распространенение так называемые теоретико-числовые преобразования (ТЧП). При их вычислении все расчёты производятся над конечным полем $GF(p)$, то есть по модулю простого числа p. Эти преобразования обладают свойством свертки и могут найти применение для фильтрации и сжатия сингналов и изображений.

Применение на практике таких преобразований во многих случаях ограничено в связи с большим требуемым объемом вычислений. В то же время существует ряд так называемых быстрых алгоритмов, позволяющих вычислять коэффициенты преобразования существенно проще.

Структурная схема процессора вычисления ТЧП содержит устройство управления и арифметико-логическое устройство (АЛУ). Устройство управления генерирует адреса, подаваемые на ОЗУ и ПЗУ из которых считываются входные данные и элементы матрицы преобразования соответственно. Структурная схема АЛУ содержит два основных элемента: сумматор и умножитель по модулю p. Было выявлено, что представление чисел в коде «diminished-1» наиболее подходяще для представления элементов конечного поля $GF(p)$. Кодирование чисел в код «diminished-1» можно осуществлять перед началом вычисления ТЧП.

Рассмотрены алгоритмы для умножителей и сумматоров по модулю p работающие в коде «diminished-1». Это АЛУ, в которых используются параллельно-префиксные сумматоры Ладнер-Фишер и Когге-Стоуна со структурами переноса префикса. Архитектура умножителя по модулю p основана на массиве сумматоров дерева Уоллеса.

Рассмотренные сумматоры и умножители используют модуль p вида $2^n \pm 1$. Моделирование на ПЛИС показало, что структуры сумматоров и умножителей по модулю 2^n-1 работают быстрее и содержат меньше логических элементов, чем структуры по модулю 2^n+1. Также моделирование выявило различие между структурами переноса префикса Ладнер-Фишер и Когге-Стоуна. Структура Ладнер-Фишер работает медленнее, но содержит меньше логических элементов, чем структура Когге-Стоуна.