УДК 004.3

РАЗРАБОТКА МОДЕЛЕЙ ПРЯМОГО ПРЕОБРАЗОВАТЕЛЯ ИЗ ПОЗИЦИОННОГО КОДА В МОДУЛЯРНЫЙ КОД ДЛЯ ОТКАЗОУСТОЙЧИВОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ СПУТНИКА

Калмыков М.И., Кочеров Ю.Н., Малышев Б.Ю., Кухтин О.К., Алиев Г.С., Калмыков И.А., Ефимович А.В.

ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

Для обеспечения эффективной работы низкоорбитальной системы спутниковой связи, которая применяется в комплексе мониторинга, контроля и управления удаленными экологически опасными объектами, предлагается использовать систему опознавания «свой-чужой». Данная система позволяет аутентифицировать космический аппарат, который попадает в зону видимости станции спутниковой связи, расположенной на необслуживаемом объекте. Если космический аппарат не относится к своей группировке, то ему отказывают в сеансе связи, и он не сможет перехватить и задержать команду управления. Чтобы повысить отказоустойчивость системы опознавания «свой-чужой», предлагается использовать корректирующие модулярные коды. Так как данные коды работают с остатками, то разработка прямого преобразователя, осуществляющего преобразование позиционного кода в модулярный код, является актуальной задачей. В статье представлены разработанные модели преобразователей «позиционный код – модулярный код».

Ключевые слова: система опознавания «свой-чужой», отказоустойчивость, модулярные коды, преобразователь «позиционный код – модулярный код»

THE MODELLING OF THE DIRECT CONVERTER OF THE POSITIONAL CODE INTO MODULAR CODE FOR A FAILOVER AUTHENTICATION SYSTEM OF THE SATELLITE

Kalmykov M.I., Kocherov Yu.N., Malyshev B.Yu., Kukhtin O.K., Aliev G.S., Kalmykov I.A., Efimovich A.V.

Federal state Autonomous educational institution of higher professional education «North-Caucasus Federal University», Stavropol, e-mail: kia762@yandex.ru

To ensure the efficient operation of low-orbit satellite communication system, which is used in complex monitoring, control and management of remote and ecologically dangerous objects is proposed to use a system of identification «friend or foe». This system allows to authenticate a spacecraft that falls into the zone of visibility of the satellite communications station located on the unattended object. If the spacecraft does not belong to his group, he denied the communication session, and he will not be able intercepted and detained by the management team. To increase the fault tolerance of the system identification «friend or foe» is proposed to use corrective modular codes. As these codes are working with the remnants, the development of the direct Converter for converting a positional code into modular code that is an urgent task. The article presents the developed model of the converters positional code – modular code.

Keywords: system identification «friend or foe», fault tolerance, modular codes, converter «positional code – modular code»

Для обеспечения эффективной работы объектов добычи и транспортировки углеводородов, расположенных за Полярным Кругом, используются комплексы мониторинга, контроля и управления удаленными экологически опасными объектами. При этом для обеспечения связи с такими объектами используют низкоорбитальные системы спутниковой связи (ССС). Чтобы предотвратить возможность перехвата, задержки и навязывания управляющих команд спутником-нарушителем, в работах [1, 2] предлагается использовать систему опознавания «свой-чужой».

Чтобы повысить отказоустойчивость системы опознавания «свой-чужой» предлагается использовать модулярные корректирующие коды. Так как модулярные коды при выполнении вычислений в качестве операндов используют остатки, то разрабатываемая программно-аппаратная система определения статуса космического аппарата (КА) должна обеспечивать преобразование из позиционного кода в модулярный код. Поэтому разработка моделей прямого преобразователя из позиционного кода в модулярный код для отказоустойчивой системы аутентификации спутника является актуальной задачей.

Цель исследования

Очевидно, что использование системы опознавания «свой-чужой» на платформе КА приводит к увеличению схемных затрат. Чтобы обеспечить устойчивость к отказам, в условиях жестких масса-габаритных показателей, предлагается использовать избыточные модулярные коды. Такие коды, на

основе параллельной и независимой обработки остатков в вычислительных каналах, способны обнаруживать и корректировать ошибки, которые возникают в процессе вычислений.

Чтобы повысить эффективность работы системы опознавания «свой-чужой», необходимо провести изучение основных методы и алгоритмов, предназначенных для преобразования позиционного кода в модулярный код.

Поэтому целью данной работы является разработка моделей прямого преобразователя из позиционного кода в модулярный код для отказоустойчивой системы аутентификации спутника, применение которых позволит обосновать выбор алгоритма, обладающего минимальными схемными временными затратами.

Материалы и методы исследования

Для предотвращения последствий сбоев и отказов, которые могут возникнуть в процессе работы системы опознавания «свой-чужой», в работах [1, 2] предлагается использовать коды классов вычетов. Характерной чертой таких кодов является то, что вычисления производятся параллельно и по независимым вычислительным каналам. Таким образом, модулярные коды осуществляют параллельную обработку остатков. Значит, выбор эффективного алгоритма выполнения процедуры получения остатков из позиционного кода позволит повысить эффективность всей запросно-ответной системы.

Модулярные коды системы остаточных классов (СОК) представляют собой совокупность останков, которые были получены при делении операнда А на основания системы p_1, p_2, ..., p_k [3, 5]. Тогда справедливо равенство

$$A = (\alpha_1, \alpha_2, ..., \alpha_k), \quad (1)$$

где $\alpha_i \equiv A \bmod p_i$; $i = 1, ..., k$; НОД(p_i, p_j) = 1, $i \neq j$.

Основным достоинством кодов СОК является ускоренное выполнение модульных операций. Пусть даны два числа $A = (\alpha_1, \alpha_2, ..., \alpha_k)$ и $B = (\beta_1, \beta_2, ..., \beta_k)$, представленные в коде СОК. Тогда справедливо

$$|A + B|_{p_i}^{+} = (|\alpha_1 + \beta_1|_{p_1}^{+}, |\alpha_2 + \beta_2|_{p_2}^{+}, ..., |\alpha_k + \beta_k|_{p_k}^{+}), \quad (2)$$

$$|A - B|_{p_i}^{+} = (|\alpha_1 - \beta_1|_{p_1}^{+}, |\alpha_2 - \beta_2|_{p_2}^{+}, ..., |\alpha_k - \beta_k|_{p_k}^{+}), \quad (3)$$

$$|A \cdot B|_{p_i}^{+} = (|\alpha_1 \cdot \beta_1|_{p_1}^{+}, |\alpha_2 \cdot \beta_2|_{p_2}^{+}, ..., |\alpha_k \cdot \beta_k|_{p_k}^{+}), \quad (4)$$

где $\alpha_i \equiv A \bmod p_i$; $\beta_i \equiv B \bmod p_i$.

Для реализации вычислительного процесса с использованием СОК необходимо осуществить преобразование из позиционной системы счисления (ПСС) в модулярный и обратно. Согласно [5, 8, 9] такие операции являются немодульными и относятся к классу позиционных операций, которые являются наиболее трудоемкими в непозиционной системе классов вычетов. Одним из самых простых методов получения остатка является метод последовательного деления. Образование остатка α_i осуществляется следующим образом:

$$\alpha_i = A - [A/p_i]\, p_i, \quad (5)$$

где $[A/p_i]$ – наименьшее целое от деления А на основание СОК p_i; $i = 1, 2, ..., k$.

Наряду с последовательным методом получения остатка можно выделить и параллельные методы. Все множество методов перевода из позиционной системы счисления в систему классов вычетов можно свести к нескольким основным группам. Как показано в работах [3, 8, 9], основу первой группы методов перевода составляет метод понижения разрядности операнда. теорема, согласно которой вычисление остатка осуществляется с помощью итерационного алгоритма. Для этого необходимо определить остатки от деления на p_j степеней основания, которые дадут набор чисел C_i, $i = 1, 2, ..., r$. Если остаток от деления степени основания C_i превосходит половину модуля p_j, то в качестве значения C_i необходимо взять число, дополняющее до значения p_j, со знаком минус. Значения C_i можно знать заранее, и они являются константами для выбранной системы счисления. Количество разрядов C_i определяется разрядностью исходного числа А. Затем цифры исходного числа умножаются на соответствующие числа C_i, полученная сумма определяется

$$A_1 = A_k C_k + ... + A_1 C_1 + \\ + A_0 C_0 < A_k \cdot S^k + ... + A_1 \cdot S^1 + A_0. \quad (6)$$

Таким образом, для получения $\alpha_i = |A|_{p_i}^{+}$ предлагается использовать модель

$$|A|_{p_i}^{+} = \sum_{i=0}^{k} |2^i|_{p_i}^{+} \{a(j)\}^{[i]}, \; j = 0, 1, 2, ... \quad (7)$$

Основу второй группы составляют методы, обеспечивающие пространственное распределение вычислительного процесса перевода из ПСС в модулярный код. Отказ от обратных связей позволяет повысить скорость выполнения операции перевода. В работе [7] предложена математическая модель вычислительного устройства, реализующего прямое преобразование позиционного двоичного кода в код СОК. Число слоев в такой сети определяется количеством итераций m, необходимых для преобразования входных данных. В этом случае итеративный алгоритм преобразования А по модулю р определяется выражением

$$A(m+1) = \sum_{i=0}^{L} |2^i|_{p}^{+} \left| \left[A(l)/2^i \right] \right|_2^{+}, \quad (8)$$

где $m = 0, 1, 2, ...$ – число итераций; $L = \log_2 A(m)$.

Однако, обеспечивая пространственное распределение вычислительного процесса перевода из ПСС в модулярный код, данные методы требуют значительных аппаратурных затрат, что может негативно сказаться на надежности работы непозиционного процессора в целом. Для оценки эффективности рассмотренных последовательного и параллельного методов получения остатка разработаем модели.

Результаты исследования и их обсуждение

Для создания и проектирования цифровых устройств широко применяются про-

граммируемые логические интегральные схемы (ПЛИС) [4]. Это связано с тем, что логика работы ПЛИС не определяется при ее изготовлении, а создается в процессе проектирования на языках описания аппаратуры (Verilog HDH, VHDL, AHDL и др.).

Для задачи выбора метода порогового разделения данных при проектировании цифровых схем выбраны следующие критерии оценки: время разделения данных при реализации на ПЛИС; количество затраченных логических элементов(LEs) ПЛИС; потребляемая мощность ПЛИС Вт. Данные критерии помогут оценить требуемые ресурсы ПЛИС. В ходе эксперимента описание аппаратуры проводилось на языке Verilog HDL. Для моделирования выбран процессор фирмы Altera из семейства Cyclone III модели EP3C80F484C6 [6]. Следующим шагом для моделирования является разработка программы для их реализации на языке описания аппаратуры Verilog HDL. Рассмотрим каждую модель прямого преобразователя из ПСС в модулярный код.

На рис. 1 представлена модель функционального устройства вычисления остатка от деления последовательным методом. Так как вычисление значения аккумулятора происходит с положительной обратной связью, то необходима синхронизация, поэтому расчет для каждого разряда входной шины данных происходит по положительному фронту внешнего генератора частоты тактового сигнала (рис. 2).

Из временной диаграммы видно, что для вычисления остатка от деления потребуется n тактов генератора, и вычисления в каждом из тактов происходят примерно за 8.893 нс. По остальным критериям оценки функциональных устройств получены следующие результаты: занято 113 Les; потребляемая мощность 0,116952157113843 Вт.

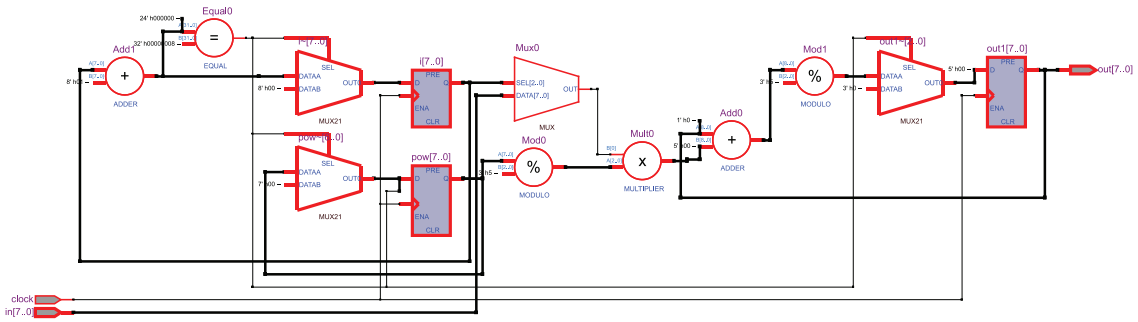

Рис. 1. Модель функционального устройства вычисления остатка от деления последовательным методом

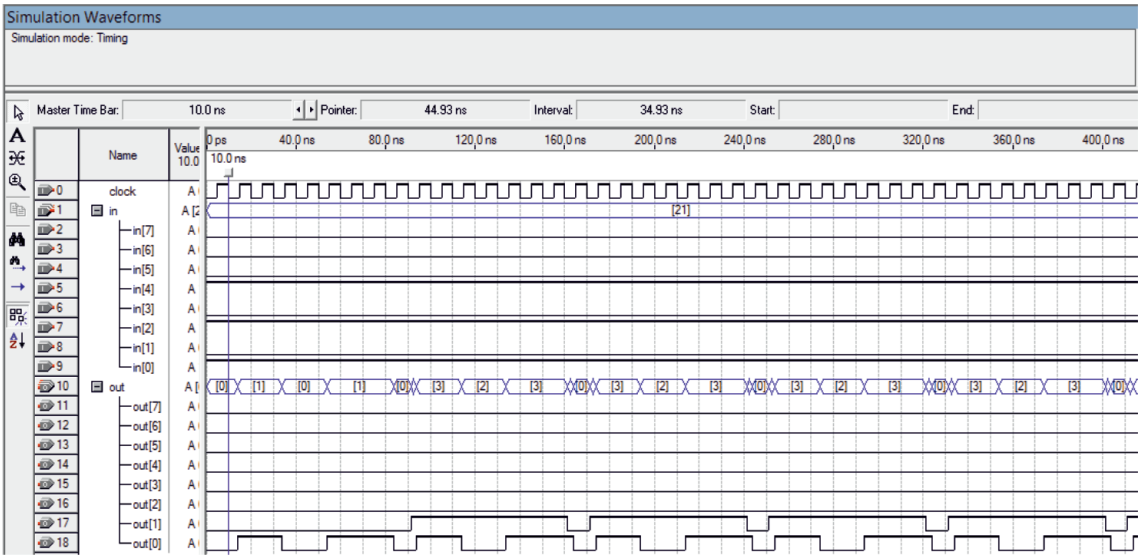

Рис. 2. Временная диаграмма функционального устройства вычисления остатка от деления последовательным методом

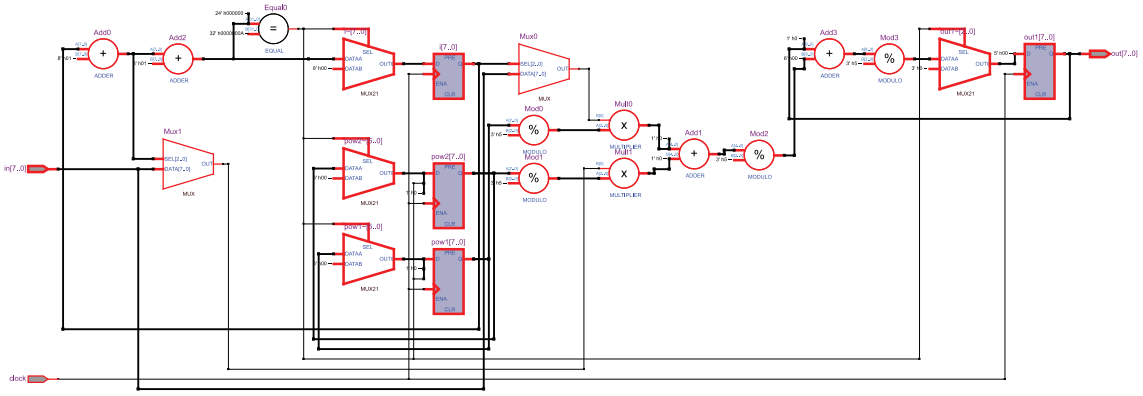

Рис. 3. Модель функционального устройства вычисления остатков с применением двух потоков

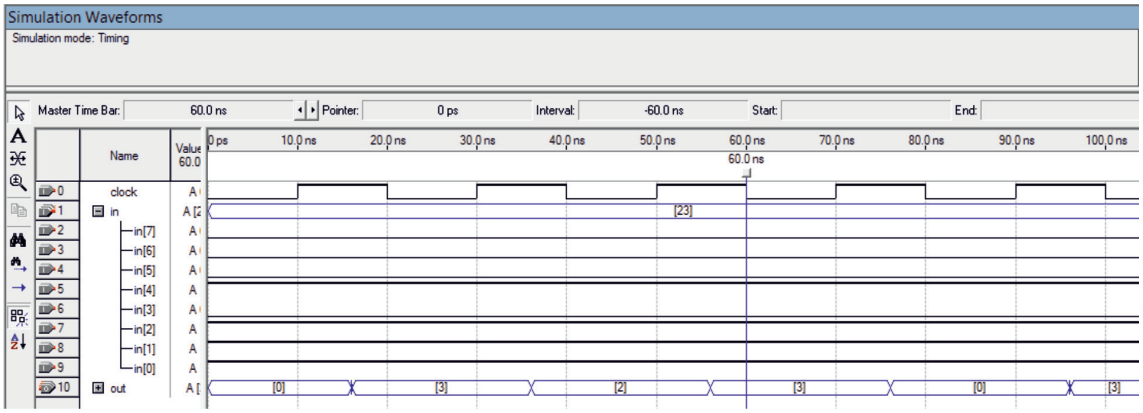

Рис. 4. Временная диаграмма функционального устройства вычисления остатка от деления с применением двух потоков

Для увеличения скорости нахождения остатков вычисления производятся в несколько потоков. На рис. 3 представлена модель функционального устройства вычисления остатков от деления с применением двух потоков, реализующая метод (7).

На рис. 4 представлена временная диаграмма разработанной модели функционального устройства вычисления остатка от деления с применением двух потоков. Из временной диаграммы видно, что для вычисления требуется в два раза меньше импульсов генератора тактовой частоты. Вычисления при каждом импульсе происходят примерно за 6 нс. По остальным критериям оценки функциональных устройств получены следующие результаты: занято 165 Les; потребляемая мощность 0.116952157113843 Вт.

При использовании метода понижения разрядности и разделении процесса вычисления остатка на n потоков нет необходимости подключать внешний генератор для вычисления каждого бита входной шины. На рис. 5 представлена модель функционального устройства вычисления остатков от деления с применением n потоков.

На рис. 6 представлена временная диаграмма разработанной модели функционального устройства вычисления остатка от деления с применением n потоков. Из временной диаграммы видно, что для вычисления требуется 15 нс. По остальным критериям оценки функциональных устройств получены следующие результаты: занято 82 Les; потребляемая мощность 0,116858249665486 Вт.

Из рассмотренных моделей функциональных устройств прямого преобразования из ПСС в СОК можно сделать вывод, что для вычисления остатков от целочисленного деления на произвольный набор модулей предпочтительно использовать параллельный метод нахождения остатков с применением дерева сумматоров.

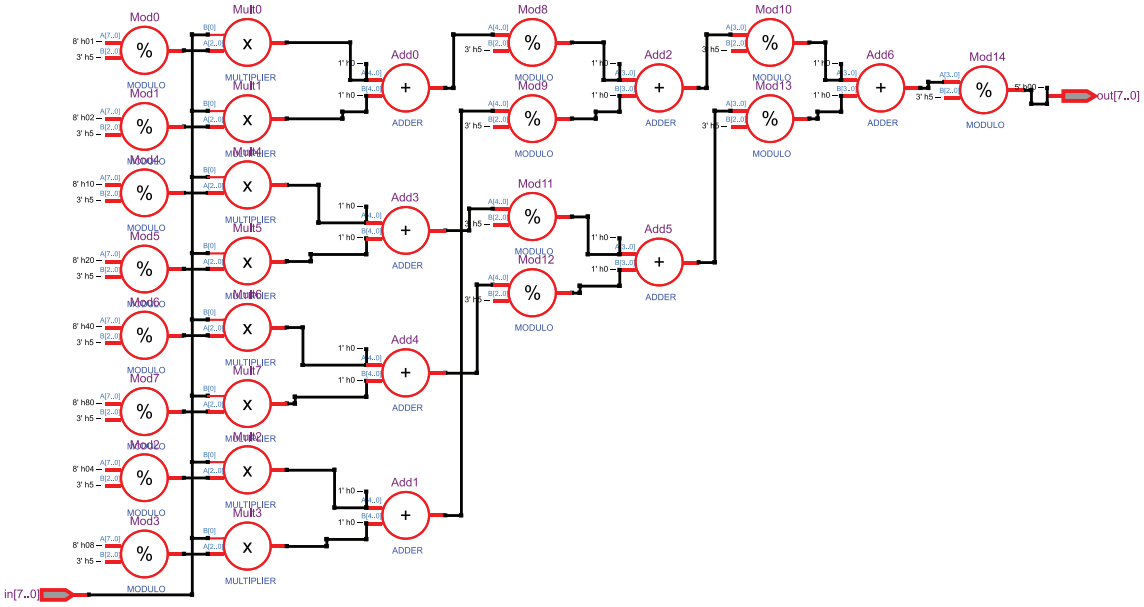

Рис. 5. Модель функционального устройства вычисления остатков от деления с применением n потоков

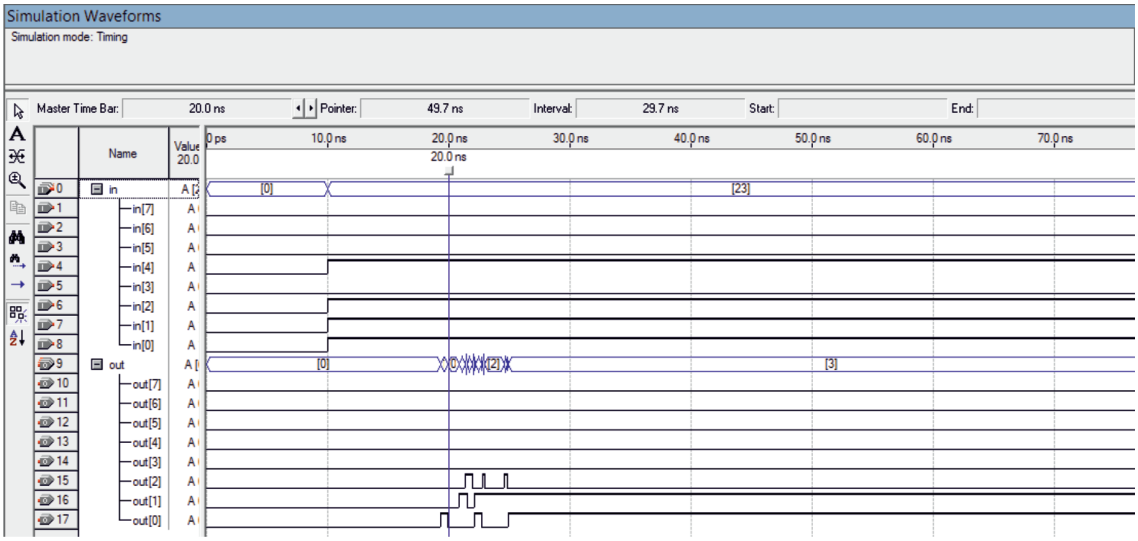

Рис. 6. Временная диаграмма функционального устройства вычисления остатка от деления с применением двух потоков

Заключение

В статье рассмотрены вопросы разработки моделей прямого преобразователя из позиционного кода в модулярный код для отказоустойчивой системы аутентификации спутника. Данные преобразователи являются необходимой частью отказоустойчивой системы опознавания «свой-чужой», функционирующей в модулярном коде. Проведенные исследования разработанных моделей показали, что применение параллельных методов вычисления остатков позволяет сократить в 1,3–2 раза число используемых LEs; а также в 1,000803 потребляемую мощность, что окажет положительное влияние на надежность работы запросно-ответной системы.

Список литературы

1. Калмыков И.А., Вельц О.В., Калмыков М.И. Алгоритм имитозащиты для системы удаленного мониторинга и управления критическими технологиями // Известия ЮФУ. Технические науки. – Таганрог: ТРТУ, 2014. – № 2 (151). – С. 181–187.

2. Калмыков И.А., Ляхов А.В., Пашинцев В.П. Применение помехоустойчивого протокола аутентификации космического аппарата для низкоорбитальной системы спутниковой связи // Инфокоммуникационные технологии. – 2015. – Т. 13, № 2. – С. 183–190.

3. Кочеров Ю.Н., Жирный А.В. Сравнительный анализ методов преобразования из системы остаточных классов в позиционную систему счисления на ПЛИС // Мир науки глазами современной молодежи: материалы Всероссийской научной конференции. – 2014. – С. 148–152.

4. Угрюмов Е.П. Глава 7. Программируемые логические матрицы, программируемая матричная логика, базовые матричные кристаллы / Цифровая схемотехника. Учеб. пособие для вузов. Изд.2, БХВ-Петербург, 2004. – С. 357.

5. Ananda Mohan Residue Number Systems. Theory and Applications. Springer International Publishing Switzerland. 2016.

6. Cyclone III Device Family Overview. https://www.altera.com/content/dam/altera-www/global/en_US/pdfs/literature/hb/cyc3/cyc3_ciii51001.pdf (дата обращения 22.05.17).

7. Kalmykov I., Katkov K., Naumenko D., Sarkisov A., Makarova A. (2014). Parallel Modular Technologies in Digital Signal Processing. Life Science Journal, 11(11s), 435–438.

8. Mohan P.V. Residue Number Systems. Algorithms and Architectures. Springer. 2002.

9. Omondi A. and Premkumar B. 2007. Residue Number Systems: Theory and Implementation. Imperial College Press. UK 2007.