Инженерный вестник Дона, №10 (2023)
ivdon.ru/ru/magazine/archive/n10y2023/8718

Исследование аппаратной реализации нейронных сетей при обработке информации в системе остаточных классов

А.А. Евдокимов, А.И. Колдаев

Северо-Кавказский федеральный университет, г. Невинномысск

Аннотация: В данной статье исследованы модели арифметических устройств нейронных сетей конечного кольца второго и третьего порядков. Исследуемые арифметические устройства были синтезированы на программируемой логической интегральной схеме. Получены оценки аппаратных затрат и быстродействия вычислителей для модулей системы остаточных классов разной разрядности. Предложена структура нейронной сети конечного кольца с динамическими связями, эффективность которой в части аппаратных затрат наблюдается с ростом разрядности модуля системы остаточных классов. Преимущество нейронной сети конечного кольца с динамическими связями установлено для модулей разрядностью равной 64 бита и выше.
Ключевые слова: нейронные сети, система остаточных классов, группа точек эллиптической кривой, ПЛИС, умножитель, сумматор.

Введение

Развитие методов обработки данных направлено на обеспечение вычислительных систем, требуемым уровнем пользовательской производительности. Обработка информации с высокой скоростью над группой точек эллиптической кривой нашла применение в задачах информационной безопасности [1], эллиптического кодирования в системах многоканальной связи, распознавания образов, построения плана эксперимента [2], теории чисел при выполнении факторизации [3] и др.

Пути снижения вычислительной сложности алгоритмов эллиптической арифметики сводятся к выбору оптимальных координат (аффинные, проективных, Якоби) представления точек эллиптической кривой, обеспечивающих минимум операций над конечным полем (сложение, умножение) и исключение мультипликативной инверсии [4].

Альтернативным подходом к ускорению выполнения операций над числами большой разрядности является модулярная арифметика, реализованная в нейросетевом логическом базисе [5]. Поэтому разработка структурных моделей искусственных нейронных сетей, используемых для

вычислений на эллиптических кривых, и отдельных вычислительных узлов нейронных сетей, позволяющих уменьшить время выполнения базовых операций над точками эллиптической кривой и аппаратные ресурсы арифметического устройства специализированного процессора, относится к актуальным задачам.

Цель исследования

Эффективная реализация базовых операций в группе точек эллиптической кривой посредством нейронных сетей высоких порядков отличается относительно малым числом межслойных связей [6]. Усложнение отдельного нейрона при переходе к сетям высокого порядка является сдерживающим фактором использования таких сетей.

Во-первых, для аппаратной реализации нейронных сетей конечного кольца (НСКК) в соответствии с моделью из [5]:

$$A(j+1)=\sum_{i=0}^{\left[\log_2 A(j)\right]}\left|2^i\right|_p\left\{A(j)\right\}^{[i]},$$

где $\{A(j)\}^{[i]}$ – оператор извлечения i-го разряда двоичного представления числа $A(j)$, потребуется многоместный сумматор для операндов разной разрядности: от 1 бита, соответствующего $\left|2^0\right|_p$, до $\left[\log_2(p-1)\right]+1$, соответствующего $\left|2^x\right|_p=p-1$, где x – целое положительное число, $x>0$.

Во-вторых, немодульные процедуры системы остаточных классов (СОК) на базе Китайской теоремы об остатках (КТО) $X=\sum_{i=1}^{n}\alpha_i B_i-r_X P$, обобщенной позиционной системы счисления (ОПСС) $X=\sum_{i=1}^{n}a_i\prod_{j=1}^{i-1}p_j$, при $\prod_{j=1}^{0}p_j=1$, и их комбинирования (например, КТО с базисами в ОПСС), при аппаратной реализации также нуждаются в многоместных сумматорах [7, 8].

Разрядность операндов и результата сложения определяются диапазоном СОК: $\prod_{i=1}^{n} p_i$.

В-третьих, в алгоритмах преобразования точек эллиптической кривой при переходе к проективным координатам присутствует многоместное умножение по модулю эллиптической кривой [9]. Эффективная реализация многоместного умножителя операндов большой разрядности с использованием индексной арифметики на базе программируемых логических интегральных схем (ПЛИС) является актуальной задачей разработки арифметического ускорителя преобразования точек кривой в проективных координатах. Известные решения на базе индексной арифметики представляют собой двухоперандные устройства по модулям разрядности 7-8 бит для покрытия диапазона в 32 бит [10]. Рост разрядности оснований и числа операндов арифметического узла приводит к снижению эффективности табличной арифметики, что продемонстрировано на рис. 1. Экспоненциальный рост емкости табличного вычислителя с ростом разрядности и числа операндов ограничивает использование табличной арифметики на базе конфигурируемых логических блоков (КЛБ) ПЛИС.

Следовательно, для систем обработки данных эффективный подход к использованию ресурсов ПЛИС заключается в применении комбинационной логики и специализированных ресурсов микросхемы (умножители, DSP-блоки) для арифметических устройств по модулю $P = \prod_{i=1}^{n} p_i$, или для оснований СОК большой разрядности. Использование комбинационной логики, как это следует из результата на рис. 1, целесообразно для многоместных арифметических устройств (умножителей и сумматоров).

Снижение разрядности оснований эффективно решается в рамках иерархически организованной СОК [5]. Использование иерархической СОК для сокращения аппаратных затрат модулярного нейропроцессора требует

проведения дополнительных исследований, поскольку введение уровней и соответствующих им преобразований чисел из СОК в позиционную систему счисления (ПСС) могут привести к снижению производительности системы обработки данных.

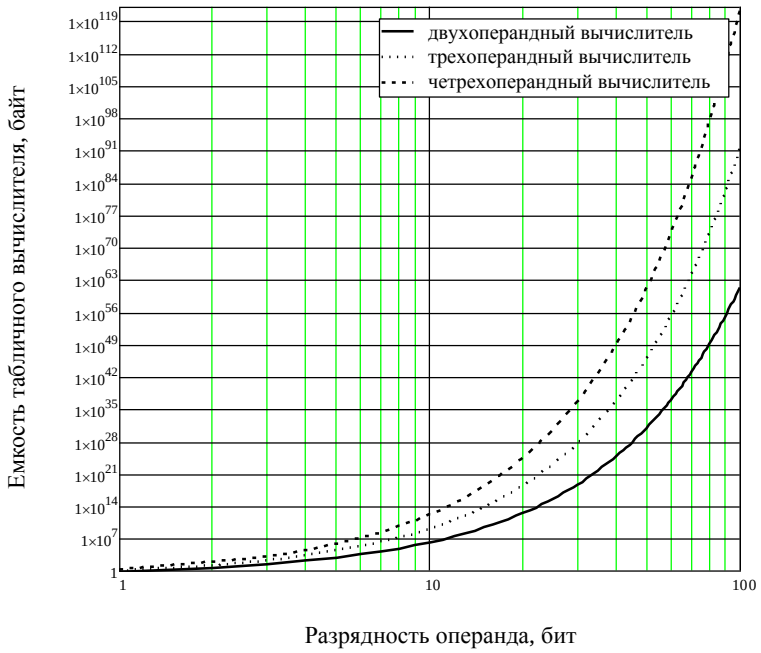

Рис. 1. – Емкость таблиц арифметических устройств по модулю системы остаточных классов

Целью работы является исследование моделей арифметических устройств нейронных сетей конечного кольца второго и третьего порядков с позиции использования ресурсов ПЛИС и быстродействия, а также разработка эффективной структуры НСКК.

Материалы и методы исследования

Производители ПЛИС в целях оптимизации своего продукта для высокопроизводительных систем традиционные ресурсы своих микросхем (секции Slices, логические ячейки Logic Cells, триггеры конфигурируемых логических блоков CLB Flip-Flops) дополняют блочной памятью (Block

RAM/FIFO), ячейками DSP, блоками обработки аналоговых сигналов (AMS/XADC), блоками шифрования AES/HMAC, высокоскоростными приемопередатчиками. Выбор серии ПЛИС зависит от требуемого для проекта объема перечисленных ресурсов.

Аппаратная реализация математических моделей обработки данных, представленных точками эллиптической кривой, в базисах системы остаточных классов имеет архитектурные особенности, несвойственные известным решениям. В основе данных особенностей лежат многооперандные арифметические операции нейросетевого логического базиса и процедуры перевода чисел из СОК в ПСС, а также обработка сверхдлинных чисел, затрудняющая использование табличной арифметики.

Для реализации многооперандных операций необходимо исследовать оптимизацию многоместных арифметических устройств на базе ПЛИС с использованием доступных для разработчика инструментов проектирования. Операции группы точек эллиптической кривой (сложение, удвоение, утроение точек) в базисе СОК отличаются вычислительными устройствами разной сложности исполнения: сумматоры двух и трех операндов по модулю СОК, умножители двух и трех операндов по модулю СОК.

Перевод чисел из СОК в двоичную систему счисления для иерархической СОК должен быть обеспечен сумматорами

- с двумя операндами разрядностью 64 и 96 бит,
- с тремя операндами разрядностью 64, 97 и 144 бит,
- с четырьмя операндами разрядностью 64, 97, 145 и 216 бит,
- с пятью операндами разрядностью 64, 97, 145, 217 и 324 бит,
- с шестью операндами разрядностью 64, 97, 145, 217, 325 и 486 бит,
- с семью операндами разрядностью 64, 97, 145, 217, 325, 487 и 728 бит.

Производители ПЛИС предлагают библиотеки арифметических компонент (например, IEEE.STD_LOGIC_ARITH.ALL, IEEE.NUMERIC_STD.ALL от Xilinx), оптимизированные под структуру определенной серии микросхем для различных типов данных. Использование данных библиотек сокращает время разработки, поскольку не требует создания с нуля описания отдельных арифметических устройств.

Таким образом, аппаратная реализация моделей на базе ПЛИС должна быть обеспечена двумя типами VHDL-библиотек:

- с описаниями двух- и трехоперандных сумматоров и умножителей с настраиваемыми параметрами по модулям одноуровневой СОК;
- с описаниями многоместных сумматоров операндов разной разрядности с фиксированными параметрами для иерархической СОК.

На рис. 2-6 представлены модели сумматоров и умножителей НСКК второго и третьего порядков. Для описания умножителей используются операции умножения «*» и вычисление вычета «mod», входящие в стандартную библиотеку IEEE.NUMERIC_STD.ALL для типа данных unsigned (целые числа без знака). В структуру сумматоров включены схема сравнения (СхС) и мультиплексор (mux) для выбора подходящего вычета в качестве конечного результата.

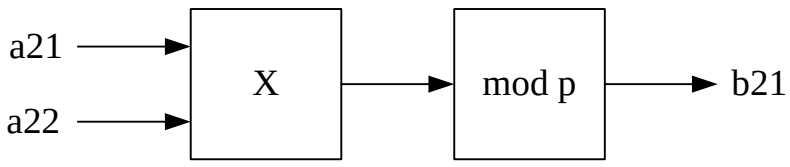

Рис. 2. – Двухоперандный умножитель НСКК второго порядка

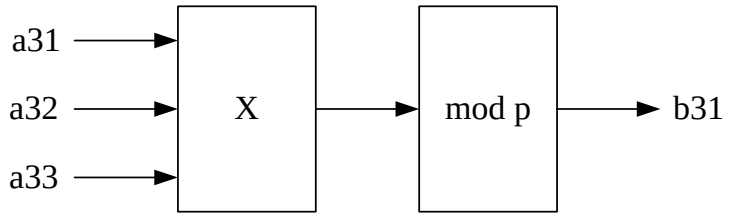

Рис. 3. – Трехоперандный умножитель первого типа НСКК третьего порядков

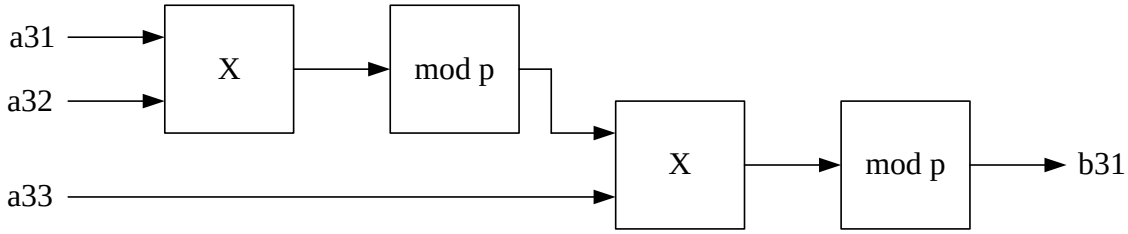

Рис. 4. – Трехоперандный умножитель второго типа НСКК третьего порядков

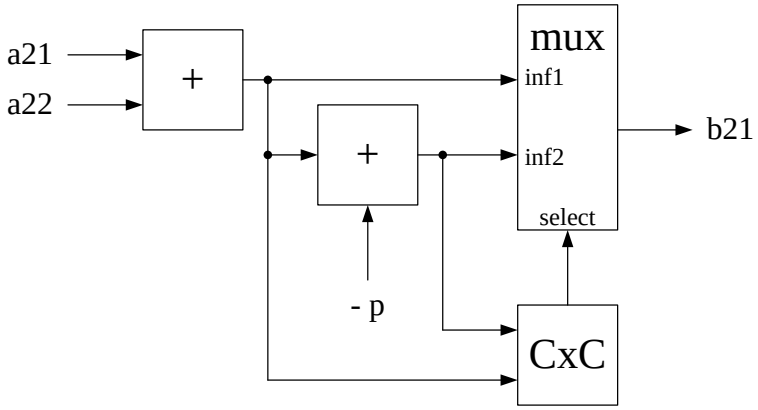

Рис. 5. – Сумматор двух операндов по модулю p НСКК второго порядка

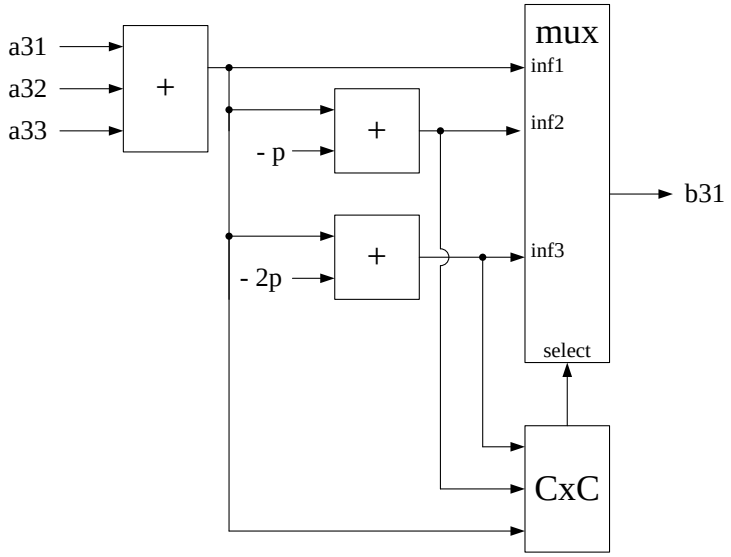

Рис. 6. – Сумматор трех операндов по модулю p НСКК третьего порядка

Каждый вычислительный блок НСКК был реализован стандартными программными компонентами Xilinx. Основной критерий для оптимизации – минимальные аппаратные затраты при однотактной реализации вычислителя. Выбор в пользу нерекурсивного подхода к построению умножителей и сумматоров НСКК сделан с целью получения точной оценки быстродействия схемы.

В процессе перевода чисел из СОК в ПСС для иерархической системы можно выделить следующие виды преобразований: для двух оснований $\left(2^{64}, p_1\right)$ выполняется 16 раза; для трех оснований $\left(2^{64}, p_1, p_2\right)$ выполняется 8 раза; для четырех оснований $\left(2^{64}, p_1, p_2, p_3\right)$ выполняется 4 раз; для пяти оснований $\left(2^{64}, p_1, p_2, p_3, p_4\right)$ выполняется 2 раз; для шести оснований $\left(2^{64}, p_1, p_2, p_3, p_4, p_5\right)$ выполняется 1 раз; для шести оснований $\left(2^{64}, p_1, p_2, p_3, p_4, p_5, p_6\right)$ выполняется 1 раз.

С ростом разрядности оснований СОК минимальные вычислительные ресурсы характерны преобразованию чисел из СОК в ПСС через полиадическую систему счисления [5]. В этом случае, для СОК с основаниями $\left(2^{64}, p_1\right)$ коэффициенты ОПСС определяются, как:

$$a_1 = |A|^{+}_{2^{64}},\ a_2 = \left|\left(|A|^{+}_{p_1} - |A|^{+}_{2^{64}}\right)\Big/ 2^{64}\right|^{+}_{p_1}.$$

Необходимо отметить, что $|A|^{+}_{2^{64}}$ является младшими 64 разрядами числа А. Кроме того $2^{64} > p_1 \le 2^{32}$, а вычет $|A|^{+}_{p_1}$ представим в 64-разрядном вычислительном канале. Операция деления $\left|\left(|A|^{+}_{p_1} - |A|^{+}_{2^{64}}\right)\Big/ 2^{64}\right|^{+}_{p_1}$ соответствует произведению $\left|\left(|A|^{+}_{p_1} - |A|^{+}_{2^{64}}\right)\left|\frac{1}{2^{64}}\right|^{+}_{p_1}\right|^{+}_{p_1}$.

Таким образом, для четырех преобразований СОК-ПСС понадобится одно двухоперандное умножение и одно двухоперандное сложение чисел с результатами не превышающих 64 бита.

Следовательно, НСКК по модулю 2^{64} является базовой не только для арифметического устройства модулярного нейропроцессора, но и для преобразователя чисел из СОК в ПСС.

Результаты исследования и их обсуждение

Эффективность разработанных вычислительных устройств оцениваться с позиции аппаратных затрат (ресурсы ПЛИС) и быстродействия схемы. Для оценки быстродействия использована максимальная задержка распространения сигнала в схеме. Для эксперимента была выбрана ПЛИС Xilinx семейства Virtex.

При сравнении аппаратных затрат НСКК с двухместными и трехместными арифметическими узлами можно сделать следующие выводы.

Для построения сумматоров используются только генераторы логических функций (LUTs). Аппаратные затраты трехопреандного сумматора по модулю почти в 2 раза выше затрат двухоперандного сумматора (рис. 7). Затраты на сумматоры относительно затрат на умножители незначительны: ресурсы двухместного сумматора по модулю составляют приблизительно 2,9 % от затрат на двухместный умножитель по модулю, а трехместного сумматора – приблизительно 2,3% от затрат на трехместный умножитель по модулю второго типа.

Ресурсы, требуемые для построения умножителей по модулю, складываются из генераторов LUTs и ячеек DSP. Затраты на двухместные умножители по модулю более чем в 2 раза меньше затрат на трехместные умножители двух исполнений.

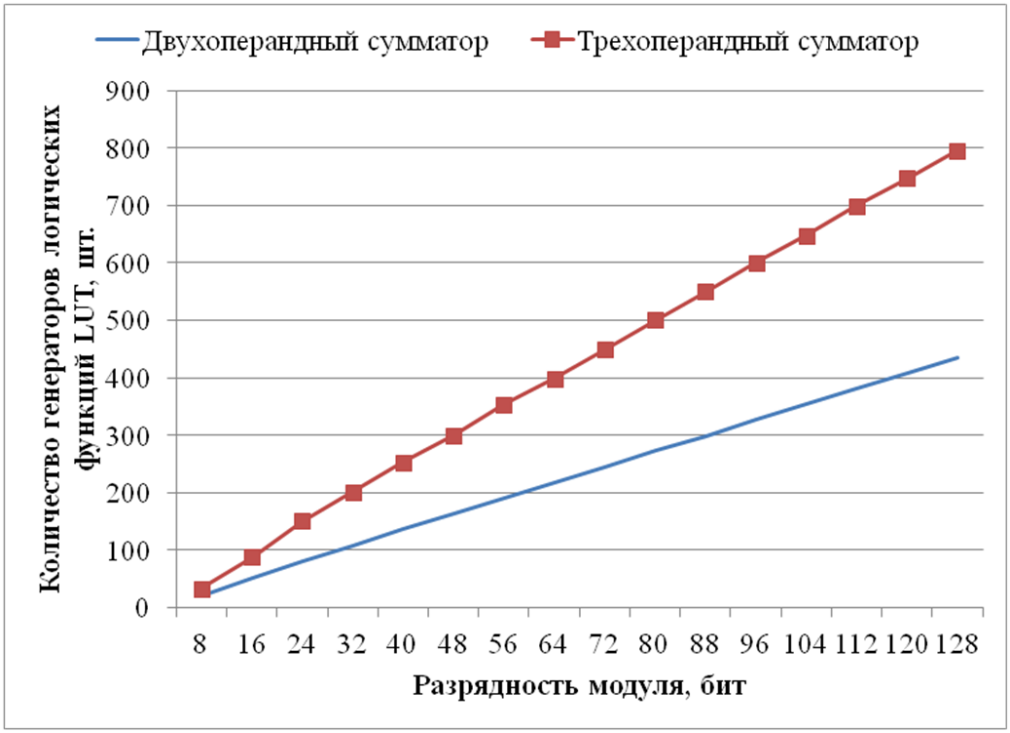

Рис. 7. – Ресурсы ПЛИС, требуемые для реализации сумматоров по модулю

На рис. 8 и рис. 9 представлены результаты синтеза умножителей по модулю в сравнении с умножителями без операции модулярной редукции. Исходя из данных рисунков видно, что аппаратные затраты умножителя без модулярной редукции малы и большей частью определяются числом ячеек DSP. Большое число генераторов LUTs можно объяснить затратами на операцию сокращения по модулю. Трехоперандный умножитель первого типа имеет большие аппаратные затраты, чем умножитель второго типа (рис. 8 и рис. 9), но и более высокое быстродействие (рис. 10).

Сравнение умножителей по быстродействию (рис. 10) позволило заключить, что умножители двухоперандные по модулю имеют преимущество перед трехоперандными умножителями по модулю. При этом быстродействие умножителей без модулярной редукции на порядок выше быстродействия умножителей по модулю.

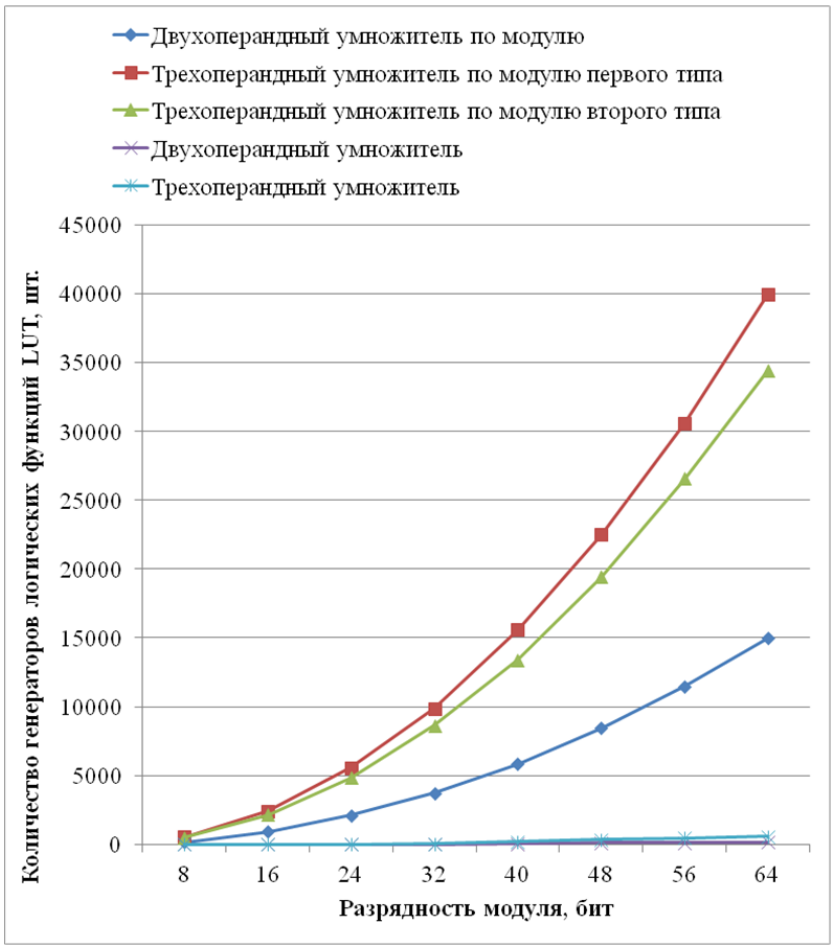

Рис. 8. – Ресурсы ПЛИС, требуемые для построения умножителей

Полученные результаты демонстрируют преимущество двухместных вычислителей. Однако представленные модели НСКК третьего порядка отличаются меньшим числом слоев, а, следовательно, меньшим числом операций в конвейере. Для оценки эффективности нейронных сетей третьего порядка в сравнении с сетями второго порядка рассмотрим быстродействие НСКК сложения точек эллиптической кривой для 32-хразрядного модуля. Время задержки сигнала двухоперандным сумматором по модулю составило t_C = 3,361 нс, а трехоперандного – t_C = 4,091 нс. Время задержки умножителя по 32-хразрядному модулю: для двухоперандного умножителя по модулю $t_П$ = 80,026 нс, для трехоперандного – $t_П$ = 160,397 нс. Результаты расчетов представлены в таблице № 1.

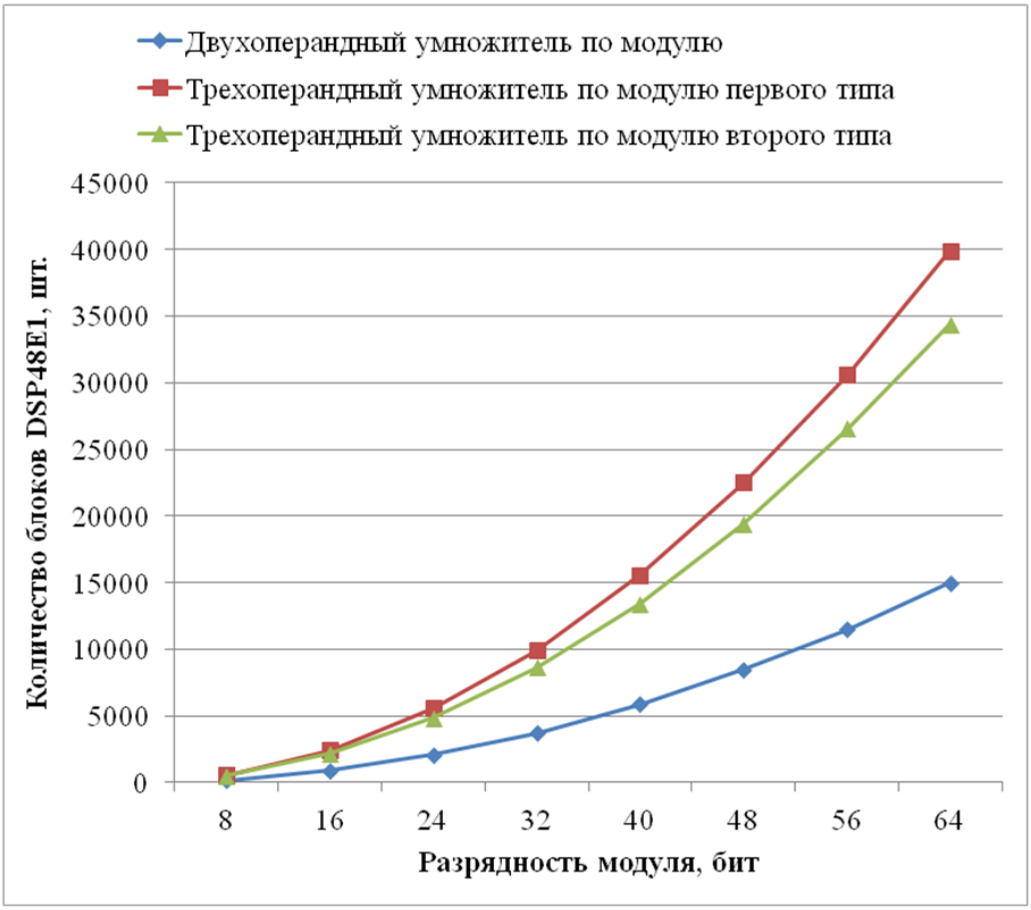

Рис. 9. – Ресурсы ПЛИС, требуемые для реализации умножителей по модулю

Из таблицы № 1 видно, что двухоперандные арифметические устройства НСКК имеют преимущество по быстродействию при аппаратной реализации на базе ПЛИС. Операция сложения точек эллиптической кривой в проективных координатах $\left(X/Z^2, Y/Z^3\right)$ на НСКК второго порядка выполняется в 1,15 раз быстрее, чем на НСКК третьего порядка. Операция сложения точек эллиптической кривой в проективных координатах $\left(X/Z, Y/Z\right)$ на НСКК второго порядка выполняется в 1,66 раз быстрее, чем на НСКК третьего порядка. Таким образом, для реализации сложения, удвоения и утроения точек эллиптической кривой на базе ПЛИС предпочтительным является использование НСКК второго порядка с двухместными сумматорами и умножителями.

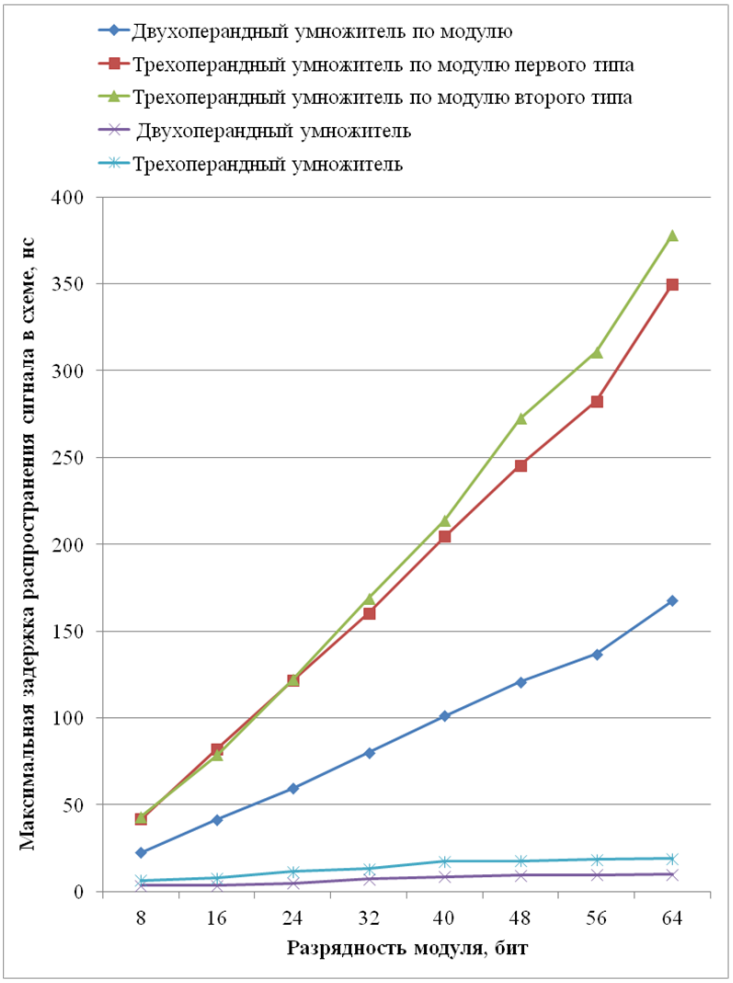

Рис. 10. – Быстродействие умножителей

Таблица № 1

Быстродействие НСКК сложения точек эллиптической кривой для 32-разрядного модуля СОК

Порядок НСКК	Проекционные координаты	Выражение для расчета оценки быстродействия	Максимальная задержка распространения сигнала в схеме, нс
Второй порядок	$(X/Z^2, Y/Z^3)$	$7t_П + 2t_С$	565,543
	$(X/Z, Y/Z)$	$6t_П + 2t_С$	486,878
Третий порядок	$(X/Z^2, Y/Z^3)$	$4t_П + 3t_С$	653,861
	$(X/Z, Y/Z)$	$5t_П + 2t_С$	810,167

Сокращение аппаратных затрат умножителя по модулю возможно посредством оптимизации устройства модулярной редукции, поскольку основные аппаратные и временные затраты умножителей формируются данным устройством, что видно при сопоставлении зависимостей на рис. 11 с зависимостями на рис. 8. На рис. 11 представлены аппаратные затраты на нерекурсивные устройства сокращения числа по модулю, синтезированные системой проектирования и описываемые одним оператором «mod» на языке VHDL. При сравнении зависимостей на рис. 10 и рис. 12 можно установить, что быстродействие умножителя по модулю в большей степени зависит от быстродействия модулярной редукции.

С целью повышения эффективности устройства сокращения по модулю была разработана НСКК с динамическими связями, представленная на рис. 13.

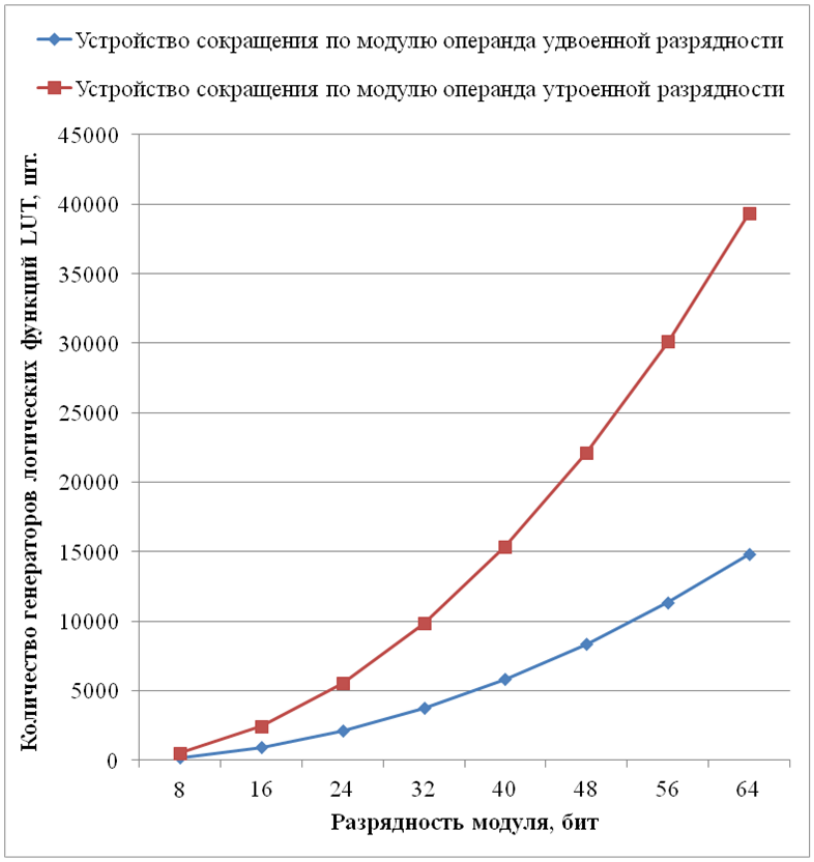

Рис. 11. – Ресурсы ПЛИС, требуемые для реализации нерекурсивных устройств сокращения чисел по модулю

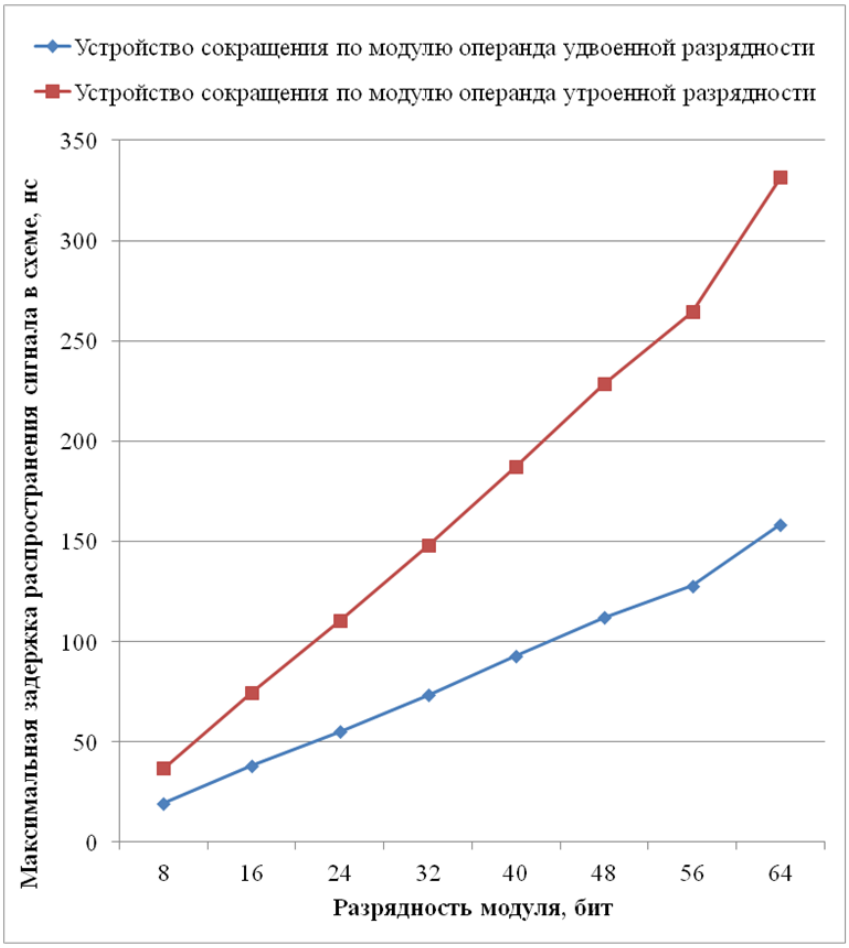

Рис. 12. – Быстродействие нерекурсивных устройств сокращения по модулю

НСКК на рис. 13 предназначена для сокращения 16-тиразрядного входного операнда по модулю разрядности 8 бит. Входной операнд делится на две группы разрядов: младшая группа $[A_0 : A_7]$ поступает без изменений на сумматор НСКК, старшая группа $[A_8 : A_{15}]$ поразрядно поступает на селективные входы мультиплексоров mux, которые переключают на вход сумматора либо нулевой сигнал, либо значение весового коэффициента НСКК, соответствующего биту старшей группы. Многоместный сумматор формирует сигнал на выходе НСКК. В отличие от известных решений модель НСКК на рис. 13 допускает изменение весовых коэффициентов, адаптируя вычислитель к вычислительному тракту СОК.

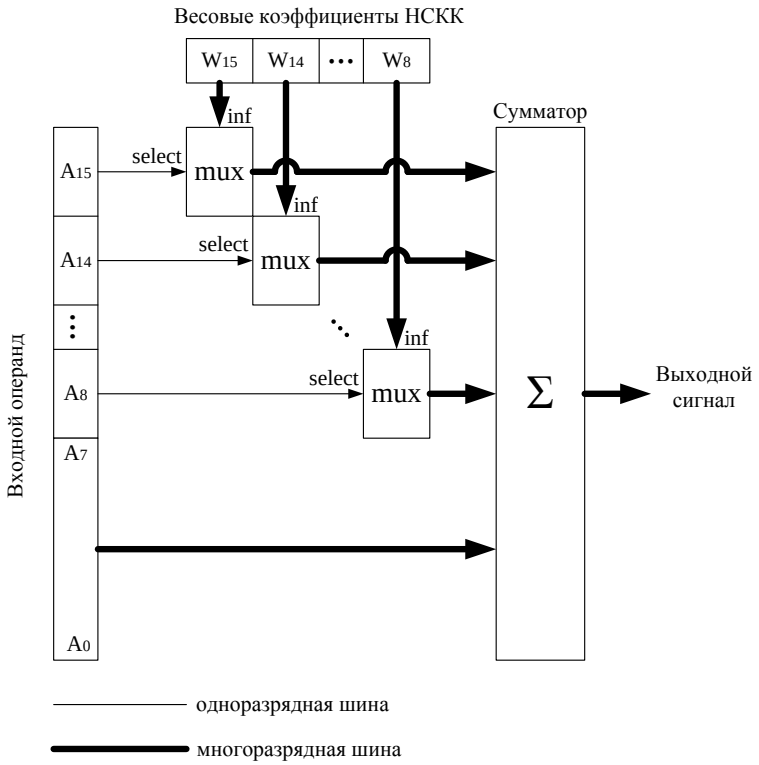

Рис. 13. – Структура нейронной сети конечного кольца с динамическими связями

Сравнение аппаратных затрат нерекурсивного устройства модулярной редукции операнда удвоенной разрядности с разработанной НСКК показало, что нейронная сеть требует генераторов логических функций LUTs приблизительно в 2 раза меньше, чем стандартный компонент (рис. 14).

Сравнение быстродействия НСКК с нерекурсивным устройством модулярной редукции (рис. 15) показало, что для модулей разрядностью до 64 бит максимальное время задержки распространения сигнала в НСКК выше, чем в схеме стандартного компонента.

Однако, для модулей разрядностью более 64 бит, время задержки распространения сигнала в НСКК более чем в 2 раза ниже по сравнению со стандартным устройством сокращения по модулю (рис. 15). Этот эффект объясняется оптимальным использованием ресурсов ПЛИС для вычислителей, обрабатывающих операнды разрядностью 64 бита и выше.

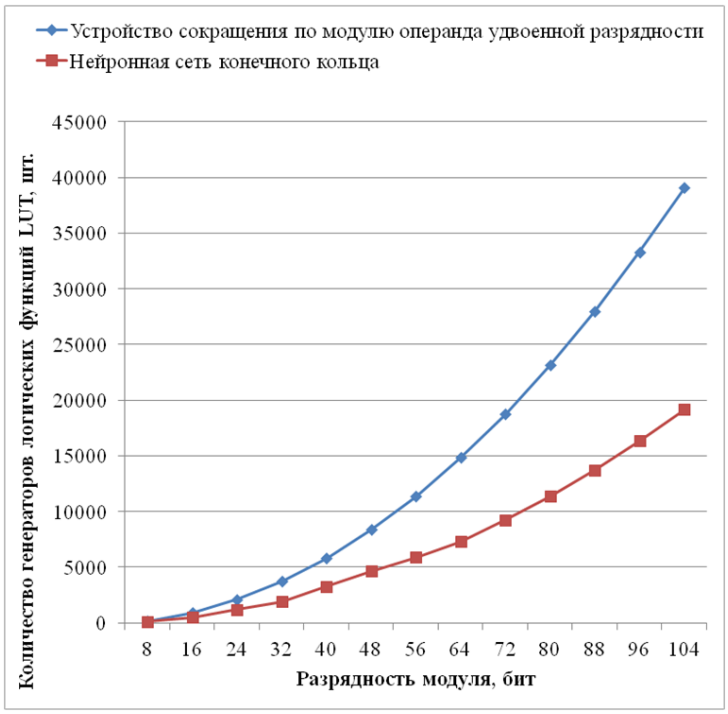

Рис. 14. – Сравнение аппаратных затрат на реализацию нерекурсивного устройства сокращения по модулю и нейронной сети конечного кольца

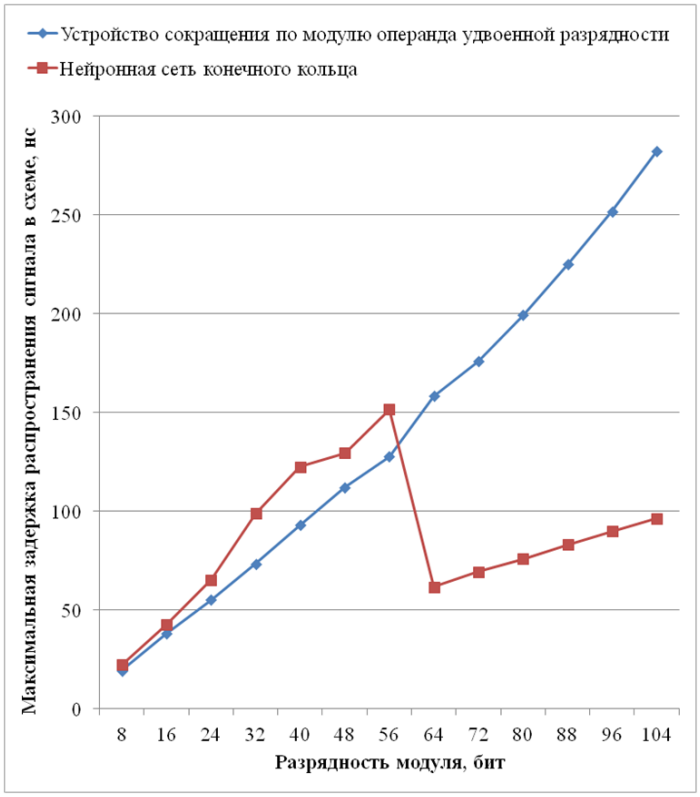

Рис. 15. – Сравнение быстродействия нерекурсивного устройства сокращения по модулю и нейронной сети конечного кольца

Заключение

В работе исследованы модели арифметических устройств нейронных сетей конечного кольца второго и третьего порядков с позиции использования ресурсов ПЛИС и быстродействия, а также разработана структура НСКК с динамическими связями. Разработанная НСКК с динамическими связями может быть использована, как компонент в умножителе по модулю или в устройстве перевода чисел из иерархической СОК в ПСС для сокращения результатов многооперандного сложения.

Анализ эффективности построения на ПЛИС НСКК высокого порядка показал, что нейронная сеть второго порядка имеет меньшие аппаратные затраты (минимум в 2 раза) в сравнении с сетью третьего порядка. Операция сложения точек эллиптической кривой в проективных координатах $\left(X/Z^2, Y/Z^3\right)$ на НСКК второго порядка выполняется в 1,15 раз быстрее, а в координатах $\left(X/Z, Y/Z\right)$ – 1,66 раз быстрее, чем на НСКК третьего порядка. Установлено, что при использовании стандартных программных компонент ПЛИС для сокращения результата умножения двух и трех операндов по модулю большая доля аппаратных и временных затрат (от 85% и выше в зависимости от разрядности модуля) приходится на блок модулярной редукции.

Для арифметических устройств сложения или умножения по модулю разрядностью меньше 64 бит в случае отсутствия необходимости в адаптации НСКК к новому основанию СОК рекомендуется использовать стандартные компоненты ISE Xilinx для модулярной редукции. Для модулей разрядностью равной 64 бит и выше, рекомендуется использование НСКК с динамическими связями даже в случае неиспользования адаптивных возможностей нейронной сети.

Литература

1. VenkataGiri J., Murty ASR. Elliptical Curve Cryptography Design Principles // Proceedings of 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), 27-28 August 2021, pp. 889-893. DOI: 10.1109/RTEICT52294.2021.9573662.

2. Степанов М.В., Беззатеев С.В. Алгебро-геометрические коды на границе Грайсмера // Информационно-управляющие системы. Т.16. №3. 2005. С. 47-50.

3. Vostrov G., Dermenzhy I. The Concept of Machine Learning and Elliptic Curves United Approach in Solving of the Factorization Problem // Proceedings of 2019 XIth International Scientific and Practical Conference on Electronics and Information Technologies (ELIT), 16-18 September 2019, pp. 87-91. DOI: 10.1109/ELIT.2019.8892318.

4. Chatterjee K., De A., Gupta D. Software implementation of curve based cryptography for constrained devices // International Journal of Computer Application, Vol.24, No.5, 2011, pp. 18-23.

5. Червяков Н.И., Коляда А.А., Ляхов П.А. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. – М.: ФИЗМАТЛИТ, 2017. 400 с.

6. Червяков Н.И., Афонин М.С., Бабенко М.Г., Ляхов П.А. Аналитический обзор методов и алгоритмов распараллеливания арифметических операций с точками эллиптической кривой на основе нейросетевого подхода // Информационные технологии. – М.: Новые технологии. 2013. № 2. С. 51-55

7. Ефременков И.Д., Калмыков И.А. Исследование корректирующих способностей помехоустойчивого кода системы остаточных классов // Инженерный вестник Дона, 2023, № 9. URL: ivdon.ru/ru/magazine/archive/n9y2023/8702/.

8. Эрдниева Н.С. Использование системы остаточных классов для маломощных приложений цифровой обработки сигналов // Инженерный вестник Дона, 2013, № 2. URL: ivdon.ru/ru/magazine/archive/ n2y2013/1621/.

9. Turki F. Al-Somani. Performance Evaluation of Elliptic Curve Projective Coordinates with Parallel GF(p) Field Operations and Side-Channel Atomicity // Journal of Computers. vol. 5, no. 1, 2010. pp. 99-109.

10. Стемпковский А.Л., Корнилов А.И., Семенов М.Ю. Особенности реализации устройств цифровой обработки сигналов в интегральном исполнении с применением модулярной арифметики // Информационные технологии, № 2, 2004. С.2-9.

References

1. VenkataGiri J., Murty ASR. 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), 27-28 August 2021, pp. 889-893. DOI: 10.1109/RTEICT52294.2021.9573662.

2. Stepanov M.V., Bezzateev C.V. Informatsionno-upravlyayushchie sistemy. T.16. №3. 2005. pp. 47-50.

3. Vostrov G., Dermenzhy I. 2019 XIth International Scientific and Practical Conference on Electronics and Information Technologies (ELIT), 16-18 September 2019, pp. 87-91. DOI: 10.1109/ELIT.2019.8892318.

4. Chatterjee K., De A., Gupta D. International Journal of Computer Application, Vol.24, No.5, 2011, pp. 18-23.

5. Chervyakov N.I., Kolyada A.A., Lyakhov P.A. Modulyarnaya arifmetika i ee prilozheniya v infokommunikatsionnykh tekhnologiyakh. [Modular arithmetic and its applications in info-communication technologies]. M.: FIZMATLIT, 2017. 400 p.

6. Chervyakov N.I., Afonin M.S., Babenko M.G., Lyakhov P.A. Informatsionnye tekhnologii. M.: Novye tekhnologii. 2013. № 2. pp. 51-55.

7. Efremenkov I.D., Kalmykov I.A. Inzhenernyj vestnik Dona, 2023, № 9. URL: ivdon.ru/ru/magazine/archive/n9y2023/8702/.

8. Erdnieva N.S. Inzhenernyj vestnik Dona, 2013, № 2. URL: ivdon.ru/ru/magazine/archive/ n2y2013/1621/.

9. Turki F. Al-Somani. Journal of Computers. vol. 5, no. 1, 2010. pp. 99-109.

10. Stempkovskiy A.L., Kornilov A.I., Semenov M.Yu. Informatsionnye tekhnologii, № 2, 2004. pp.2-9.