

## ОГЛАВЛЕНИЕ

Предисловие . . . . .	7
<b>I. Теоретические основы и принципы применения модулярной арифметики</b>	
<b>Глава 1. Базовые элементы теории модулярных вычислительных структур . . . . .</b>	<b>12</b>
1.1. Теоретические основы систем счисления с параллельной кодовой структурой . . . . .	12
1.2. Модулярные системы счисления. . . . .	19
1.2.1. Модулярная кодификация конечных коммутативных колец (19). 1.2.2. Модулярные системы счисления с целочисленными диапазонами (22).	
1.3. Технология вычисления интегральных характеристик модулярного кода на диапазонах неотрицательных целых чисел . . . . .	28
1.4. Интервально-индексный метод четного модуля для расчета интегральных характеристик кода неизбыточной МСС с симметричным диапазоном. . . . .	40
1.5. Минимально избыточные модулярные системы счисления. . . . .	47
<b>Глава 2. Функциональные особенности, принципы построения, методологические и инструментально-программные основы реализации базы модулярной вычислительной технологии. . .</b>	<b>55</b>
2.1. Особенности и принципы организации модулярных вычислений. . .	55
2.2. Табличная реализация операций модульного умножения. . . . .	59
2.3. Умножение по модулям специального вида на позиционных процессорах. . . . .	64
2.4. Аккумулятивно-табличный метод суммирования вычетов по модулям МСС . . . . .	68
<b>Глава 3. Методы и алгоритмы выполнения немодульных операций в МИМСС . . . . .</b>	<b>73</b>
3.1. Расширение модулярного кода . . . . .	73
3.2. Методологические и алгоритмические средства преобразования кодов позиционной и модулярной систем счисления . . . . .	81
3.2.1. Перевод чисел из позиционной в модулярную систему счисления по схеме Горнера (82). 3.2.2. Метод деления на двоичную	

экспоненту для преобразования МИМК в ПК (86). 3.2.3. Интервально-индексная технология синтеза параллельных алгоритмов модулярно-позиционного кодового преобразования с таблично-сумматорной конфигурацией (97).	
3.3. Масштабирование диапазона МИМСС . . . . .	103
3.3.1. Методология синтеза универсальных алгоритмов масштабирования в МИМСС (103). 3.3.2. Анализ эффективности универсального МИМА-алгоритма масштабирования (107). 3.3.3. Масштабирование в МИМСС на масштабы мультипликативной структуры (110). 3.3.4. Оценки эффективности МИМА-алгоритма масштабирования на мультипликативные масштабы (117).	
3.4. Синтез МИМА-алгоритма деления больших чисел на основе схемы спуска Ферма . . . . .	118
3.4.1. Минимально избыточная модулярная алгоритмизация метода деления на основе схемы спуска Ферма (118). 3.4.2. Исследование корректности алгоритма деления (124). 3.4.3. Оценки эффективности МИМА-процедуры умножения по модулю на основе схемы деления спуска Ферма (129).	
<b>Глава 4. Методологические, компьютерно-алгоритмические и реализационные средства для быстрого умножения Монтгомери по большому модулю с применением вычислительной МИМА-технологии . . . . .</b>	<b>132</b>
4.1. Метод Монтгомери для умножения по большому модулю . . . . .	132
4.2. Минимально избыточная модулярная схема Монтгомери для умножения по большим модулям . . . . .	135
4.3. Таблично-сумматорная технология компьютерной реализации мультипликативной МИМА-схемы Монтгомери . . . . .	141
4.3.1. Формирование базисов МСС для схемы умножения Монтгомери (142). 4.3.2. Алгоритм расчета системных констант для мультипликативной МИМА-схемы Монтгомери (144). 4.3.3. Генерирование и функционально-структурная оптимизация базового комплекта таблиц для мультипликативной МИМА-схемы Монтгомери (146).	
4.4. Алгоритмы умножения по большим модулям на основе МИМА-схемы Монтгомери . . . . .	154
<b>Глава 5. Криптомодуль RSA на основе мультипликативных МИМА-алгоритмов типа Монтгомери . . . . .</b>	<b>163</b>
5.1. Криптографическая система RSA с модулярной кодовой организацией . . . . .	163
5.2. Базовый алгоритм возведения в степень по большому модулю . . . . .	171
5.3. Методологические и алгоритмические средства позиционно-модулярного интерфейса криптомодуля RSA . . . . .	180
5.3.1. Принцип модулярной интерпретации сообщений в криптосистеме RSA (182). 5.3.2. Алгоритмическое обеспечение модулярной интерпретации сообщений в СЗИ (186).	
Список литературы . . . . .	190

## II. Синтез функциональных модулярных устройств в базе искусственных нейронных сетей

Глава 6. Методы и алгоритмы прямого и обратного преобразования кодов системы остаточных классов с использованием искусственных нейронных сетей . . . . .	202
6.1. Системный анализ различных форм представления данных в модулярных нейрокомпьютерах и обоснование необходимости перехода от одной формы к другой при позиционно-остаточной обработке данных. . . . .	202
6.2. Метод и алгоритм определения вычета числа на основе использования множеств классов чисел по модулю и синтеза на его основе иерархической нейронной сети конечного кольца. . . . .	205
6.3. Метод и алгоритм параллельного определения вычета числа на основе использования распределенной арифметики и синтеза на его основе параллельной нейронной сети конечного кольца. . . . .	209
6.4. Развитие метода параллельного определения вычета числа с целью синтеза на его основе конвейерной нейронной сети конечного кольца . . . . .	213
6.5. Связность кода системы остаточных классов и кода обобщенной позиционной системы счисления. . . . .	216
6.6. Метод ускоренного перехода от кортежа вычетов числа, представленного по модулям системы остаточных классов, к его позиционному представлению. . . . .	222
Глава 7. Анализ и синтез многофункциональных модулярных устройств с использованием нейронных сетей конечного кольца . . . . .	226
7.1. Метод и алгоритм расширения кортежа вычетов по вновь введенным модулям СОК . . . . .	226
7.2. Методы и алгоритмы масштабирования модулярных чисел, применяемых в модулярных нейрокомпьютерах. . . . .	230
7.3. Ускоренный метод масштабирования чисел и синтез на его основе устройства масштабирования с использованием нейронных сетей конечного кольца. . . . .	239
7.4. Развитие теории корректирующих свойств модулярных кодов, используемых при обработке данных . . . . .	248
7.5. Особенности коррекции ошибок в минимально-избыточной симметричной системе остаточных классов . . . . .	258
7.6. Синтез структуры адаптивной нейронной сети для коррекции ошибок . . . . .	262
Список литературы . . . . .	270

### III. Применение модулярной арифметики в задачах обеспечения безопасности передачи данных

Глава 8. Схемы разделения секрета в задачах обеспечения безопасности беспроводных сетей . . . . .	280
8.1. Схемы разделения секрета на точках эллиптической кривой в системе остаточных классов . . . . .	280
8.2. Схемы множественного разделения секрета с использованием системы остаточных классов . . . . .	289
8.3. Нейросетевые схемы разделения секрета . . . . .	308
Глава 9. Генераторы псевдослучайных чисел в системе остаточных классов . . . . .	315
9.1. Линейные рекуррентные последовательности на эллиптической кривой . . . . .	315
9.2. Построение генератора псевдослучайных чисел на базе криптосистемы XTR . . . . .	320
Глава 10. Применение концепции активной безопасности для обеспечения безопасности беспроводных сетей и облачных технологий . . . . .	325
10.1. Разработка системы передачи данных для сетей MANET на основе системы остаточных классов . . . . .	325
10.2. Развитие теоретических аспектов защиты информации в облачных технологиях с использованием пороговых структур . . . . .	331
Список литературы . . . . .	335

### IV. Применение модулярной арифметики в цифровой обработке сигналов

Глава 11. Модели и методы цифровой фильтрации в системе остаточных классов . . . . .	342
11.1. Принципы проектирования цифровых фильтров с использованием системы остаточных классов . . . . .	342
11.2. Методы организации параллельной фильтрации . . . . .	359
Глава 12. Методы цифровой обработки изображений в системе остаточных классов . . . . .	368
12.1. Реализация алгоритмов вейвлет-анализа в модулярном базисе . . . . .	368
12.2. Методы цифровой фильтрации с использованием вейвлетов конечного поля . . . . .	377
12.3. Применение модулярной арифметики в цифровой обработке изображений . . . . .	386
Список литературы . . . . .	396