

СОДЕРЖАНИЕ

Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

Алексеев Е. С. Алгоритм вычисления D -пробельных чисел и D -вейерштрассовых точек	6
Евдокимов А. А. Кодирование конечной целочисленной решетки в классе отображений ограниченного искажения	8
Коломеев Н. А. Количество бент-функций на минимальном расстоянии от квадратичной бент-функции	9
Колчева О.Л., Панкратова И. А. О статистической независимости суперпозиции булевых функций	11
Корсакова Е. П. Классификация графов АНФ квадратичных бент-функций от шести переменных	13
Парватов Н. Г. Слабоцентральные клоны и проблема полноты в них	14
Пичкур А. Б. Описание класса подстановок, представимых в виде произведения двух подстановок с фиксированным числом мобильных точек	16
Погорелов Б. А., Пудовкина М. А. О приближении подстановок импримитивными группами	17
Потапов В. Н. О совершенных 2-раскрасках q -значного гиперкуба	18
Пряничникова Е. А. Алгебры языков, ассоциированные с отмеченными графами	20
Токарева Н. Н. Гипотезы о числе бент-функций	21

Секция 2

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Аборнев А. В., Былков Д. Н. Многочлены над примарными кольцами вычетов с малым расстоянием единственности	24
Андреева Л. Н. О расширениях отображений, сохраняющих свойство идентифицируемости	26
Артамонов А. В., Васильев П. Н., Маховенко Е. Б. Доказуемо безопасная динамическая схема групповой подписи	27
Воронин Р. И. Алгебраический криптоанализ однораундового S-AES	29
Ерофеев С. Ю. Диофантовость дискретного логарифма	31
Ерофеев С. Ю., Романьков В. А. Построение односторонних функций на основе неразрешимости проблемы эндоморфной сводимости в группах	32
Ковалев Д. С., Тренькаев В. Н. Реализация на ПЛИС шифра FAPKC	33
Кукало И. А. Безопасность режимов шифрования ГОСТ 28147-89	34
Лебедева О. Н. О выборе слайдовых пар в корреляционном методе криптоанализа шифра KeeLoq	36
Пудовкина М. А. О невозможных усечённых разностях XSL-алгоритмов блочного шифрования	38

Секция 3

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Абросимов М. Б., Маторин А. А. Анализ надежности графических САПРТСНА-систем на примере проекта КСАПРТСНА	40
Девянин П. Н. О результатах разработки ролевой ДП-модели для операционных систем семейства Linux	42
Качанов М. А. Разработка ролевой модели безопасности управления доступом и информационными потоками компьютерной системы <i>SELinux</i>	44
Колегов Д. Н. Особенности разработки ДП-моделей сетевого управления доступом	46
Кононов Д. Д., Исаев С. В. Модель безопасности кросс-платформенных веб-сервисов поддержки муниципальных закупок	48
Милошенко А. В., Соловьёв Т. М., Черняк Р. И., Шумская М. В. Разработка комплексной обучаемой системы защиты информационных ресурсов от фишинговых атак	50
Проскурин В. Г. Подходы к разработке дискреционной ДП-модели современных защищенных операционных систем	55

Секция 4

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ
И ПРОГРАММИРОВАНИЯ

Быкова В. В. FRT-алгоритмы и их классификация на основе эластичности.....	58
Сафонов К. В., Калугин-Балашов Д. А. О свойстве формальных языков непосредственно составляющих	60
Стефанцов Д. А., Крюкова А. Е. Денотационное описание языка AspectTalk	61
Стефанцов Д. А., Ткаченко Н. О., Чернов Д. В., Шмакова Р. В. Разработка и реализация библиотеки ORM на языке C++	62

Секция 5

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

Заикин О. О. Решение задач криптоанализа в грид-системах (на примере BOINC)	66
Коломеец Н. А., Павлов А. В. Boolean Functions — система для работы с булевыми функциями	67
Семенов А. А., Отпущенников И. В., Кочемазов С. Е. Применение SAT-подхода в решении комбинаторных задач	68
Фомичев В. М. О параллельных вычислениях при реализации метода согласования в криптоанализе.....	69

Секция 6

ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ

Березовская Ю. В., Воробьев В. А. К-модель хищник — жертва в экологической нише	74
Салий В. Н. О скелетных автоматах	76
Тренькаев В. Н. Атака аппаратного сбоя на реализацию шифра Закревского на основе перестраиваемого автомата	78

Секция 7

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Абросимов М. Б., Бондаренко П. П. О минимальных вершинных 1-расширениях циклов с вершинами двух типов	80
Абросимов М. Б., Долгов А. А. К вопросу о единственности точных вершинных расширений	81
Абросимов М. Б., Комаров Д. Д. О минимальных реберных 1-расширениях двух семейств деревьев	83
Абросимов М. Б., Моденова О. В. О некоторых свойствах минимальных вершинных расширений орграфов.....	84
Быкова В. В. Вычислительные аспекты древовидной ширины графа	85
Власова А. В. Об аттракторах динамических систем, ассоциированных с циклами.....	88
Грунский И. С., Сапунов С. В. О самолокализации мобильного агента с использованием топологических свойств среды	90
Карманова Е. О. О конгруэнциях цепей	91
Кочкаров А. А., Сенникова Л. И., Болуров Н. Н. О некоторых свойствах предфрактальных графов	93
Мелентьев В. А. Компактные графы и детерминированный алгоритм их синтеза	94
Мелентьев В. А. Ограничения на обхваты в компактных графах	96
Фомичев В. М. Уточнение оценок экспонентов примитивных графов	98
СВЕДЕНИЯ ОБ АВТОРАХ	101
АННОТАЦИИ ДОКЛАДОВ НА АНГЛИЙСКОМ ЯЗЫКЕ	105