

СОДЕРЖАНИЕ

Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

Бондаренко Л. Н., Шарапова М. Л. Свойства статистик Мак-Магона на множествах слов	6
Дорохова А. М. О примитивности перемешивающих графов преобразований регистров сдвига с двумя обратными связями	8
Кяжин С. Н., Фомичев В. М. О локальных экспонентах перемешивающих графов функций, реализуемых алгоритмами типа А5/1	11
Облаухов А. К. О некоторых метрических свойствах линейных подпространств булева куба	13
Погорелов Б. А., Пудовкина М. А. Свойства группы, порождённой группами сдвигов векторного пространства и кольца вычетов	15
Погорелов Б. А., Пудовкина М. А. $\otimes \mathbf{W}_{ch}$ -марковские преобразования	17
Фомичев В. М. О степенной структуре графов	20

Секция 2

ДИСКРЕТНЫЕ ФУНКЦИИ

Виткуп В. А. О числе симметрических координатных функций APN-функции	23
Городилова А. А. О пересечении множеств значений производных APN-функций	25
Ивачев А. С. Исследование группы биективных дифференцируемых по модулю p^n функций	27
Карпов А. В. Обращение дифференцируемых перестановок над группой	30
Коломеец Н. А. О связности графа минимальных расстояний множества бент-функций	33
Куценко А. В. О самодуальных булевых бент-функциях	34
Панкратова И. А. Об обратимости векторных булевых функций	35
Покрасенко Д. П. Об алгебраической иммунности векторных булевых функций	37
Потапов В. Н. Свойства p -ичных бент-функций, находящихся на минимальном расстоянии друг от друга	39
Черемускин А. В. Перечисление функций, имеющих заданное число аффинных сомножителей	43
Шурупов А. Н. Некоторые структурные свойства квадратичных булевых пороговых функций	48
Шушуев Г. И. О свойствах множества значений произвольной векторной булевой функции	51

Секция 3

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Агибалов Г. П. Шифры с водяными знаками	54
Егорова В. В., Чечулина Д. К. Построение криптосистемы с открытым ключом на основе полностью гомоморфного шифрования	59
Карондеев А. М. Сложение по модулю 2^n в блочном шифровании	62

Медведева Н. В., Титов С. С. Неэндоморфные совершенные шифры с двумя шифрвеличинами	63
Пестунов А. И. Предварительная оценка минимального числа раундов легких шифров для обеспечения их удовлетворительных статистических свойств	66
Погорелов Б. А., Пудовкина М. А. $\otimes_{W, ch}$ -марковость и импримитивность в блочных шифрсистемах	69
Рыбалов А. Н. О генерической сложности проблемы распознавания квадратичных вычетов	71
Токарева Н. Н. NSUCRYPTO — студенческая олимпиада по криптографии: идея, воплощение, результат	74
Трепачева А. В. Атака по шифртекстам на одну линейную полностью гомоморфную криптосистему	75

Секция 4

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Анисеня Н. И. О защищённом распределённом протоколе в конкурентной среде на примере проведения соревнований СТФ	79
Девянин П. Н. Необходимые условия нарушения безопасности информационных потоков по времени в рамках МРОСЛ ДП-модели	81
Колегов Д. Н., Брославский О. В., Олексов Н. Е. О возможности реализации скрытых каналов по времени на основе заголовков кэширования протокола HTTP в облачных сервисах хранения файлов	83
Колегов Д. Н., Брославский О. В., Олексов Н. Е. Неинвазивный метод контроля целостности cookie в веб-приложениях	85
Колегов Д. Н., Ткаченко Н. О. Неинвазивная реализация мандатного управления доступом в веб-приложениях на уровне СУБД	89
Милованов Т. И. Реализация атаки DNS Rebinding	92
Овсянников С. В., Тренькаев В. Н. Атрибутное управление доступом к хранилищу данных типа «ключ — значение»	95
Epishkina A. V., Kogos K. G. The capacity of a packet length covert channel	96

Секция 5

МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

Алехина М. А. Ненадёжность схем при константных неисправностях на входах и выходах элементов	100
Алехина М. А., Барсукова О. Ю. Нижняя оценка ненадёжности схем в базисе, состоящем из функции Вебба	102
Алехина М. А., Каргин С. П. Нижние оценки ненадёжности схем в базисе Россера — Туркетта (в P_4)	104
Грабовская С. М. Верхняя оценка ненадёжности неветвящихся программ с ненадёжным стоп-оператором	106
Рыбаков А. В. О длине, высоте и надёжности схем, реализующих функции выбора v_{2i}	108

Секция 6

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ, АВТОМАТОВ И ГРАФОВ

Абросимов М. Б., Моденова О. В. О точных оценках числа дополнительных дуг минимального вершинного 1-расширения турнира	111
Авезова Я. Э., Фомичев В. М. Условия примитивности системы двух графов	113
Жаркова А. В. О количестве недостижимых состояний в конечных динамических системах двоичных векторов, ассоциированных с ориентациями палым	115
Малюгин С. А. Совершенные двоичные коды бесконечной длины	117
Поттосин Ю. В. Энергосберегающее противогоночное кодирование состояний асинхронного автомата	120
Салий В. Н. Шпернеровы деревья	124
Федоряева Т. И. О разнообразии шаров графа заданного диаметра	127

Секция 7

**МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ
И ПРОГРАММИРОВАНИЯ**

Гречнев С. Ю., Стефанцов Д. А. Модификация ЛЯПАСа для разработки ОС	129
Жуковская А. О., Стефанцов Д. А. Операционная семантика ЛЯПАСа	131
Сафонов В. О. Система управления библиотеками для ЛЯПАСа	133
Стефанцов Д. А., Томских П. А. Разработка ОС на языке ЛЯПАС	134

Секция 8

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

Анашкина Н. В., Шурупов А. Н. Применение алгоритмов локального поиска к решению систем псевдобулевых линейных неравенств	136
Богачкова И. А., Заикин О. С., Кочемазов С. Е., Отпущенников И. В., Семёнов А. А. Применение алгоритмов решения проблемы булевой выполнимости к криптоанализу хэш-функций семейства MD	139
Быкова В. В., Кириллов Ю. И. Вычисление верхней оценки вершинной целостности графа на основе минимальных сепараторов	142
Кожушко О. А. Построение функции ошибки для решения задачи идентификации алгоритма ранжирования	144
Кузнецов А. А., Сафонов К. В. Полиномы Холла бернсайдовых групп периода 3	147
Николаев М. В. О сложности задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием	149
Тарков М. С. Реализация нейронной WTA-сети на мемристормом кроссбаре	151
СВЕДЕНИЯ ОБ АВТОРАХ	155
АННОТАЦИИ ДОКЛАДОВ НА АНГЛИЙСКОМ ЯЗЫКЕ	159