

# СОДЕРЖАНИЕ

## Секция 1

### ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

<b>Аборнев А. В.</b> Разрядно-инъективные преобразования модуля над кольцом Галуа .....	6
<b>Бондаренко Л. Н.</b> Свойства статистики $\text{var}$ на группе перестановок .....	7
<b>Былков Д. Н.</b> Вторая координатная последовательность линейной рекурренты максимального периода над кольцом $\mathbb{Z}_8$ .....	9
<b>Волгин А. В.</b> Оценка скорости сходимости в многомерной центральной предель- ной теореме .....	11
<b>Геут Кр. Л., Титов С. С.</b> О поликвадратичном расширении бинарных полей .....	12
<b>Заец М. В.</b> Классы полиномиальных и вариационно-координатно полиномиаль- ных функций над кольцом Галуа .....	13
<b>Коломеец Н. А.</b> Об аффинности булевых функций на подпространствах и их сдвигах .....	15
<b>Курганский А. Н.</b> Об алгоритмических и топологических свойствах орбит кусочно-аффинных отображений .....	16
<b>Мироненко О. Л.</b> О статистической независимости произвольной суперпозиции булевых функций .....	18
<b>Филюзин С. Ю.</b> Верхняя оценка алгебраической иммунности некоторых бент- функций Диллона .....	19
<b>Фомичев В. М.</b> Эквивалентность примитивных множеств .....	20
<b>Фролова А. А.</b> Итеративная конструкция APN-функций .....	24
<b>Черемушкин А. В.</b> К определению степени нелинейности дискретной функции на циклической группе .....	26
<b>Шоломов Л. А.</b> Экономное представление недоопределённых данных и дизъ- юнктивные коды .....	27

## Секция 2

### МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

<b>Виткуп В. А.</b> О представлении S-блоков при реализации в блочных шифрах .....	30
<b>Калужин А. К., Чижов И. В.</b> Алгоритм восстановления открытого текста по шифртексту в криптосистеме Мак-Элиса .....	32
<b>Карпунин Г. А.</b> О вероятностных характеристиках случайных графов, поро- даемых алгоритмами поиска коллизий криптографических хэш-функций .....	33
<b>Катеринский Д. А.</b> Об обратимости конечных автоматов с конечной задержкой .....	35
<b>Ковалев Д. С.</b> Реализация на ПЛИС симметричного аналога FAPKC .....	36
<b>Коренева А. М.</b> О блочных шифрах, построенных на основе регистров сдвига с двумя обратными связями .....	39
<b>Медведев Н. В., Титов С. С.</b> Конструкции идеальных схем разделения секрета .....	41
<b>Медведева Н. В., Титов С. С.</b> О неминимальных совершенных шифрах .....	42
<b>Пестунов А. И.</b> О связях между основными понятиями разностного анализа итеративных блочных шифров .....	44
<b>Чижов И. В., Бородин М. А.</b> Уязвимость криптосистемы Мак-Элиса, постро- енной на основе двоичных кодов Рида — Маллера .....	48

## Секция 3

# МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ И НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

<b>Алехина М. А., Барсукова О. Ю.</b> Об оценках ненадёжности схем при инверсных неисправностях и отказах функциональных элементов.....	50
<b>Анисеня Н. И., Стефанцов Д. А., Торгаева Т. А.</b> Сервис BlackBox для проведения соревнований по защите компьютерной информации Capture The Flag .....	52
<b>Васин А. В.</b> О базисах с коэффициентом ненадёжности 1.....	56
<b>Девянин П. Н.</b> Корректность правил преобразования состояний системы в рамках мандатной сущностно-ролевой ДП-модели ОС семейства Linux .....	58
<b>Зайцев Г. Ю., Потапкин А. И., Стефанцов Д. А.</b> Модификация скомпилированных приложений для платформы Android методом аспектно-ориентированного программирования .....	60
<b>Колегов Д. Н., Ткаченко Н. О., Чернов Д. В.</b> Разработка и реализация мандатных механизмов управления доступом в СУБД MySQL .....	62
<b>Щерба Е. В., Волков Д. А.</b> Разработка системы обнаружения распределённых сетевых атак типа «отказ в обслуживании» .....	68

## Секция 4

# ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

<b>Абросимов М. Б., Моденова О. В.</b> О нижней оценке числа дополнительных дуг минимального вершинного 1-расширения ориентации цепи .....	71
<b>Батуева Ц. Ч.-Д.</b> Свойства генных сетей циркулянтного типа с пороговыми функциями .....	72
<b>Бондаренко П. П.</b> К вопросу о верхней оценке числа дополнительных рёбер минимальных вершинных расширений цветных циклов .....	73
<b>Евдокимов А. А., Кочемазов С. Е., Отпущенников И. В., Семенов А. А.</b> Исследование динамических свойств некоторых дискретно-автоматных отображений, заданных случайными графами.....	75
<b>Жаркова А. В.</b> О ветвлении и непосредственных предшественниках состояний в конечной динамической системе всех возможных ориентаций графа .....	76
<b>Комаров Д. Д.</b> О минимальных рёберных расширениях палъм специального вида .....	78
<b>Корниенко А. С.</b> Деревья функциональных графов для циркулянтов с линейными булевыми функциями в вершинах .....	80
<b>Кяжин С. Н.</b> О локальной примитивности графов и неотрицательных матриц.....	81
<b>Нажмиденова А. М.</b> Дискретная динамическая система на двойном циркулянте с разными функциями в вершинах .....	84
<b>Осипов Д. Ю.</b> О Т-неприводимых расширениях сверхстройных деревьев .....	85
<b>Салий В. Н.</b> Об упорядоченном множестве связных частей многоугольного графа .....	87
<b>Токарева Н. Н.</b> Простое доказательство сильной регулярности графа Кэли бент-функции.....	89
<b>Цициашвили Г. Ш., Осипова М. А., Лосев А. С.</b> Асимптотики вероятностей связности пар вершин графа .....	90

## Секция 5

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ  
И ПРОГРАММИРОВАНИЯ

Agibalov G. P., Lipsky V. B., Pankratova I. A. Cryptographic extension of Russian programming language .....	93
Agibalov G. P., Lipsky V. B., Pankratova I. A. Project of hardware implementation of Russian programming language .....	98
Broslavskiy O. V. AES in LYaPAS .....	102

## Секция 6

## ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

Анашкина Н. В. О возможности сокращения перебора в алгоритме Балаша .....	105
Арбузов Д. С., Туктарова Л. И. Сравнительный анализ некоторых алгоритмов распознавания гладких чисел .....	107
Булавинцев В. Г., Семенов А. А. О GPU-реализации ограниченной версии нехронологического алгоритма DPLL .....	111
Быкова В. В. Об асимптотике решений рекуррентных соотношений в анализе алгоритмов расщепления для пропозициональной выполнимости .....	112
Жуков К. Д., Рыбаков А. С. К решению больших систем сравнений .....	116
Климина А. С. Оптимизация $(p - 1)$ -алгоритма Полларда .....	118
Кузнецова А. С., Кузнецов А. А., Сафонов К. В. Параллельный алгоритм вычисления функций роста в конечных дупорождённых группах периода 5 .....	119
Поттосин Ю. В., Кардаш С. Н. Конвейеризация комбинационных схем .....	121
Рябоконь Д. В. Алгоритм поиска запретов булевых функций .....	123
Семенов А. А. Об эффективном представлении дизъюнктивных нормальных форм диаграммами специального вида .....	125
Усатюк В. С. Реализация параллельного алгоритма поиска кратчайшего вектора в блочном методе Коркина — Золотарева .....	130
Черняк Р. И. Распараллеливание алгоритма декодирования стандарта сжатия видеоданных H.265/HEVC .....	131
Шангин Р. Э. Точный алгоритм для решения одного частного случая задачи Вебера в дискретной постановке .....	136
СВЕДЕНИЯ ОБ АВТОРАХ .....	138
АННОТАЦИИ ДОКЛАДОВ .....	143