СОДЕРЖАНИЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

Денисов О. В. Статистические методы поиска набора координат, на котором случайный вектор имеет запреты 5

Минаков А. А. Аппроксимация распределения числа монотонных цепочек заданной длины в случайной последовательности сложным распределением Пуассона 21

Фролова Ю. Ю., Шулежко О. В. Почти нильпотентные многообразия алгебр Лейбница 30

Шурупов А. Н. Критерии функциональной разделимости квадратичных булевых пороговых функций 37

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Горнова М. Н., Кукина Е. Г., Романьков В. А. Криптографический анализ протокола аутентификации Ушакова — Шпильрайна, основанного на проблеме бинарно скрученной сопряжённости 46

Рыбалов А. Н. О генерической сложности проблемы распознавания квадратичных вычетов 54

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Анисеня Н. И. Разработка безопасного протокола распределённой системы проведения соревнований CTF 59

Колегов Д. Н., Брославский О. В., Олексов Н. Е. Скрытые каналы по времени на основе заголовков кэширования протокола HTTP 71

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Фомичев В. М. Свойства минимальных примитивных орграфов 86

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

Николаев М. В. О сложности задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием 97

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

Алексеев Д. В., Казунина Г. А., Чередниченко А. В. Клеточно-автоматное моделирование процесса разрушения хрупких материалов 103

СВЕДЕНИЯ ОБ АВТОРАХ 118

CONTENTS

THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

Denisov O. V. Statistical methods of search for coordinate set on which a random vector has bans 5

Minakov A. A. Compound Poisson approximation of the number distribution for monotone strings of fixed length in a random sequence 21

Frolova Yu. Yu., Shulezhko O. V. Almost nilpotent varieties of Leibniz algebras 30

Shurupov A. N. Functional decomposability criteria for quadratic threshold Boolean functions 37

MATHEMATICAL METHODS OF CRYPTOGRAPHY

Gornova M. N., Kukina E. G., Romankov V. A. Cryptanalysis of Ushakov — Shpilrain's authentication protocol based on the twisted conjugacy problem 46

Rybalov A. N. On generic complexity of the quadratic residuosity problem 54

MATHEMATICAL BACKGROUNDS OF COMPUTER SECURITY

Anisenya N. I. Developing safe protocol for distributed task-based CTF holding system 59

Kolegov D. N., Broslavsky O. V., Oleksov N. E. Covert timing channels over HTTP cache-control headers 71

APPLIED GRAPH THEORY

Fomichev V. M. Properties of minimal primitive digraphs 86

COMPUTATIONAL METHODS IN DISCRETE MATHEMATICS

Nikolaev M. V. On the complexity of discrete logarithm problem in an interval in a finite cyclic group with efficient inversion 97

DISCRETE MODELS FOR REAL PROCESSES

Alekseev D. V., Kazunina G. A., Cherednichenko A. V. Cellular automaton simulation of the fracture process for brittle materials 103

BRIEF INFORMATION ABOUT THE AUTHORS 118