

# ПДМ. 2012. № 4(18).

## ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

5–13

*Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // ПДМ. 2012. № 4(18). С. 5–13.

14–30

*Панков К. Н.* Оценки скорости сходимости в предельных теоремах для совместных распределений части характеристик случайных двоичных отображений // ПДМ. 2012. № 4(18). С. 14–30.

## МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

31–52

*Марков В. Т., Михалёв А. В., Грибов А. В., Золотых П. А., Скаженик С. С.* Квазигруппы и кольца в кодировании и построении криптосхем // ПДМ. 2012. № 4(18). С. 31–52.

53–60

*Пестунов А. И.* О вероятности протяжки однобитовой разности через сложение и вычитание по модулю // ПДМ. 2012. № 4(18). С. 53–60.

## ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

61–72

*Емеличев В. А., Коротков В. В.* Исследование устойчивости решений векторной инвестиционной булевой задачи в случае метрики Гельдера в критериальном пространстве // ПДМ. 2012. № 4(18). С. 61–72.

73–81

*Тимчук Г. Д., Жихаревич В. В.* Развитие метода непрерывных асинхронных клеточных автоматов для моделирования турбулентных потоков // ПДМ. 2012. № 4(18). С. 73–81.

## ИСТОРИЧЕСКИЕ ОЧЕРКИ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЁ ПРИЛОЖЕНИЯМ

82–107

*Токарева Н. Н.* Об истории криптографии в России // ПДМ. 2012. № 4(18). С. 82–107.

## АНАЛИТИЧЕСКИЕ ОБЗОРЫ

*Агибалов Г. П., Панкратова И. А.* Sibescrypt'12. Обзор докладов // ПДМ. 2012. № 4(18). С. 108–122.

## ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.6

### ПОЛОЖИТЕЛЬНЫЕ СВОЙСТВА НЕОТРИЦАТЕЛЬНЫХ МАТРИЦ

К. Г. Когос\*, В. М. Фомичев\*\*

\* *Национальный исследовательский ядерный университет (МИФИ), г. Москва, Россия*

\*\* *Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия*

**E-mail:** fomichev@nm.ru

Дан обзор результатов исследования примитивности графов (неотрицательных матриц) и некоторых направлений обобщения. Приведены оценки экспонентов различных классов графов и систем графов (матриц и систем матриц).

**Ключевые слова:** *примитивный граф, примитивная матрица, экспонент, суб-экспонент.*

Одним из положительных криптографических свойств преобразований векторных пространств является хорошее перемешивание, то есть зависимость каждой координатной функции от всех переменных. Перемешивающие свойства преобразования  $g$  пространства  $P^n$  над полем  $P$ , заданного системой координатных функций  $\{g_1(x_1, \dots, x_n), \dots, g_n(x_1, \dots, x_n)\}$ , определяются системой множеств  $\{S(g_1), \dots, S(g_n)\}$ , где  $S(g_j)$  — множество номеров существенных переменных координатной функции  $g_j(x_1, \dots, x_n)$ ,  $j = 1, \dots, n$ . Наилучшее перемешивание достигается, если каждая из координатных функций преобразования  $g$  зависит от всех переменных, то есть  $S(g_j) = \{1, \dots, n\}$ ,  $j = 1, \dots, n$ . Такие преобразования принято называть совершенными. Обобщениями свойства совершенности функций являются такие свойства, как строгий лавинный критерий, критерии распространения, свойство «бент».

Почти все преобразования векторного пространства  $P^n$  над конечным полем  $P$  являются совершенными при  $n \rightarrow \infty$ . Однако подобный вывод неприменим к функциям, используемым в криптографических системах, так как они выбираются не случайно, а из отображений с рядом заданных свойств. Поэтому изучение перемешивающих свойств криптографических функций — актуальная задача криптографического анализа.

Некоторые функции с полным перемешиванием обладают свойством распространения искажений входных данных, что позволяет использовать их в криптосистемах аутентификации. С другой стороны, к функциям шифрования с неполным перемешиванием входов применимы методы определения ключа типа последовательного опробования, что делает привлекательным использование в криптосистеме шифрования совершенных преобразований.

Аппаратная или программная реализация совершенных преобразований затруднена в связи с необходимостью реализации функций от большого числа переменных. Поэтому для хорошего перемешивания используются итерации (возведение в степень) преобразования с относительно слабыми перемешивающими свойствами. Показатель степени преобразования, при которой достигается хорошее перемешивание, является