**Коренева Алиса Михайловна Оценки экспонентов перемешивающих орграфов регистровых преобразований, используемых в системах защиты информации**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Коренева Алиса Михайловна

ВВЕДЕНИЕ

Глава 1. Характеристики перемешивающего орграфа преобразования регистра сдвига с одной обратной связью над пространством двоичных векторов

§ 1.1 Обзор известных оценок экспонентов примитивных орграфов

§ 1.2 Определяющие свойства перемешивающего орграфа регистрового преобразования с одной обратной связью над пространством двоичных векторов

§ 1.3 Описание множеств путей и контуров в перемешивающем орграфе регистрового преобразования с одной обратной связью над пространством двоичных векторов

§ 1.4 Условия примитивности и оценки экспонентов перемешивающего орграфа регистрового преобразования с одной обратной связью над пространством двоичных векторов

§ 1.5 Выводы

Глава 2. Характеристики перемешивающего орграфа регистрового преобразования, построенного на основе модифицированного аддитивного генератора (МАГ)

§ 2.1 Уравнения функционирования и определяющие свойства МАГ

§ 2.2 Описание множеств путей и контуров в перемешивающем орграфе преобразования множества состояний МАГ

§ 2.3 Примитивность и оценки экспонента перемешивающего орграфа МАГ

§ 2.4 О приложениях МАГ в системах защиты информации

2.4.1 Перемешивающие свойства генератора ключевого расписания на основе МАГ

2.4.2 Перемешивающие свойства нелинейных узлов замены, построенных с использованием МАГ

§ 2.5 Выводы

Глава 3. Характеристики перемешивающего орграфа преобразования регистра сдвига с двумя обратными связями над пространством двоичных векторов

§ 3.1 Биективность преобразования регистра сдвига с несколькими обратными связями над пространством двоичных векторов и определяющие свойства перемешивающего орграфа

§ 3.2 Примитивность перемешивающего орграфа преобразования регистра сдвига на основе МАГ с двумя обратными связями

§ 3.3 Оценки экспонентов перемешивающего орграфа преобразования регистра сдвига на основе МАГ с двумя обратными связями

§ 3.4 Сравнение экспонентов перемешивающих орграфов регистровых преобразований с одной и двумя обратными связями и рекомендации по выбору параметров

§ 3.5 Выводы

ЗАКЛЮЧЕНИЕ

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

СПИСОК ЛИТЕРАТУРЫ