**Ахметзянова Лилия Руслановна Комбинаторные свойства схем обеспечения конфиденциальности и целостности информации**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Ахметзянова Лилия Руслановна

Введение

Обозначения, определения и общие сведения

Свойства безопасности ЛЕЛБ-схем

Глава 1. Комбинаторные свойства ЛЕЛБ-режимов

1.1. Режим «8 бит»

1.2. Режим ЫСЫ

Выводы

Глава 2. Устойчивость к повтору вектора инициализации

2.1. Режим ЫСЫ2

Выводы

Глава 3. Методы улучшения свойств ЛЕЛБ-режимов

3.1. Режим OMAC-ACPKM-Masteг

3.2. Режим GCM-ACPKM

Выводы

Заключение

Список литературы

Приложение

1. Оценка вероятности коллизий в атаке на режим «8 бит»