

## Аннотация дипломной работы

**Тема:** Методы шифрования с дополнительными возможностями

**ФИО студента:** Чудовская Наталья Игоревна

**Научный руководитель:** Заведующий кафедрой НИИ ППМИ БГУ, кандидат физико-математических наук Агиевич Сергей Валерьевич

**Кафедра (специальность, специализация):** Кафедра математического моделирования и анализа данных, специальность – компьютерная безопасность, специализация – математические методы защиты информации

**Дипломная работа:** 52 страницы, 13 рисунков, 7 использованных источников литературы

### Структура дипломной работы:

Введение

#### 1. Шифрование на основе атрибутов

- 1.1. Общая схема шифрование на основе атрибутов
- 1.2. Описание схемы шифрования на основе атрибутов
- 1.3. Разновидности шифрования на основе атрибутов

#### 2. Широковещательное шифрование

- 2.1. Ассиметричное шифрование
- 2.2. Широковещательное шифрование
- 2.3. Первоначальная схема широковещательного шифрования
- 2.4. Сравнение широковещательного шифрования с ассиметричным шифрованием

#### 3. Гомоморфное шифрование

- 3.1. Определение гомоморфного шифрования
- 3.2. Схема полностью гомоморфного шифрования

#### 4. Шифрование, сохраняющее порядок

- 4.1. Схемы шифрования, сохраняющего порядок
- 4.2. Прототип защищенной базы данных

#### 5. Шифрование с возможностью поиска

- 5.1. Задача поиска в зашифрованных данных
- 5.2. Последовательный просмотр
- 5.3. Базовая схема
- 5.4. Схема контролируемого поиска
- 5.5. Схема скрытого поиска
- 5.6. Финальная схема
- 5.7. Конфиденциальная обработка данных

#### 6. Реализация шифрования с поиском

- 6.1. Схема шифрования с поиском
- 6.2. Работа с приложением “Searchable Encryption”

Заключение

Список использованной литературы

Приложение

**Ключевые слова:** ШИФРОВАНИЕ, НАБОР АТТРИБУТОВ, ШИРОКОВЕЩАТЕЛЬНЫЙ, ГОМОМОРФНЫЙ, ШИФРОВАНИЕ С ВОЗМОЖНОСТЬЮ ПОИСКА

**Цель работы (постановка задачи):** исследовать существующие методы шифрования с дополнительными возможностями, реализовать метод шифрования с поиском.

**Результаты работы:** проведен аналитический обзор публикаций по методам шифрования с дополнительными возможностями, предложена схема шифрования с поиском на основании “шифрования наполовину”, реализовано приложение, демонстрирующее возможности разработанной схемы поиска по зашифрованным данным.