**Матвеев Евгений Анатольевич Применение квантовомеханических эффектов в системах защиты информации**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Матвеев Евгений Анатольевич

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

ГЛАВА 1. Квантовые ресурсы, используемые в криптографических 21 приложениях

§ 1.1. Теорема о невозможности клонирования

§ 1.2. Несепарабельные состояния квантовых систем

§ 1.3. Математическое определение несепарабельности состояния п- 34 кубитной квантовой системы

§ 1.4. Состояние спиновый синглет

§ 1.5. Состояния квантовых систем, близкие по своим свойствам к 51 состоянию спиновый синглет

Выводы по главе

ГЛАВА 2. Достаточные признаки несепарабельности состояний 67 многокубитных квантовых систем

§ 2.1. Булевы маски состояний квантовых систем

§ 2.2. Нумераторы весов состояний квантовых систем

§ 2.3. Алгоритм определения неразложимости состояния квантовой 82 системы в тензорное произведение состояний меньшей размерности с использованием редукций булевых функций

Выводы по главе

ГЛАВА 3. Квантовые криптографические системы

§ 3.1. Квантовые криптографические системы на основе ресурса 90 невозможности клонирования неизвестного квантового состояния

§ 3.2. Квантовые криптографические системы на основе двух

ресурсов: невозможности клонирования неизвестного квантового состояния и несепарабельности

§ 3.3. Квантовая криптографическая система АКМ2017 на основе

ресурса несепарабельности состояния спиновый синглет

§ 3.4. Сеансовый ключ квантовой криптографической системы

АКМ2017 как еще одна степень усиления криптографической стойкости

§ 3.5. Восстановление состояний носителей-кубитов для

формирования ключевой информации квантовой криптографической системы АКМ2017

Выводы по главе

1

ЗАКЛЮЧЕНИЕ

СПИСОК ЛИТЕРАТУРЫ

Приложение А

Приложение Б

Приложение В

Приложение Г

Приложение Д