АНОТАЦІЯ

Пояснювальна записка дипломного проекту складається з п’яти розділів, містить 64 сторінки, 13 рисунків, 6 таблиць, 1 додаток, 18 джерел.

Дипломний проект присвячений розробці системи на базі порогової криптосистеми для надійного захисту даних користувачів.

В дипломному проекті були розглянуті: шифрування з відкритим ключем RSA, схема Шаміра, симетричне шифрування методом AES+CBC-MAC(CCB), підпис Шнора.

У розділі з інформаційного забезпечення були визначені вхідні та вихідні дані до комплексу задач.

У розділі з математичного забезпечення було обґрунтовано доцільність використання обраних криптографічних алгоритмів та методів.

У розділі з програмного забезпечення описані основні засоби розробки комплексу задач, висунуті вимоги до технічного забезпечення, обрано та обґрунтовано архітектуру програмного забезпечення.

У технологічному розділі описана інструкція користувача та проведене тестування комплексу задач.

КРИПТОСИСТЕМА, RSA, AES-CBC, ГРУПОВИЙ КЛЮЧ, ВЕРИФІКАЦІЙНИЙ КЛЮЧ, СХЕМА ШАМІРА, ПІДПИС ШНОРА, СХЕМА ШАМІРА, ОДНОРАНГОВА МЕРЕЖА.