

## 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 обгрунтовано 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 обгрунтовано 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.

					<b>ДП ІС-2202. 1448-с.ПЗ</b>			
		<i>Прізвище</i>	<i>Підпис</i>	<i>Дата</i>				
<i>Розроб.</i>	<i>Борисенко І.В.</i>				Система обміну персональними даними групи учасників на баз іпорогової криптосистеми в хмарних середовищах та однорангових мережах портативних пристроїв	<i>Літ.</i>	<i>Арк.</i>	<i>Аркушів</i>
<i>Перевірів.</i>	<i>Шевченко К.Ю.</i>						2	
<i>Н. кон.</i>	<i>Халус О.А.</i>				<i>КПІ ФІОТ кафедра АСОІУ гр. ІС-22</i>			
<i>Затв.</i>	<i>Шевченко К.Ю.</i>							