ABSTRACT

The relevance. Wide implementation of information technology makes a logical and topical problem of information security. Studies show that only half of the information security specialists consider their company or institution to be ready to withstand modern information threats, including those that can lead to uncontrolled dissemination of information beyond the information systems in which it is processed. One of the important areas of research in IT systems, networks and devices is the research and development of new methods for protecting information and providing information security for systems, networks and devices. The protection of information is largely based on the use of cryptographic methods related to data encryption. In this regard, the improvement of existing encryption and decryption methods is relevant, which will allow companies and institutions to increase the validity of encrypted information (increase cryptographic stability), increase the security of information exchange.

Relationship with academic programs, plans, themes. Master's thesis is executed according to plan in processes managed optimization department at Institute of Cybernetics of V.M. Glushkov NAS of Ukraine within the research theme «To develop algorithms optimal for accuracy and speed of solving problems: integration of fast-sensing functions, digital processing of signals and images, remote monitoring of objects, information security» (state registration number 0114U000357).

The purpose and objectives of the study. The aim is to increase the speed of encryption and decryption of information

To achieve the aim, we must accomplish the following **tasks**:

– perform an overview of existing methods of encryption and decryption of information;

– perform a comparative analysis of various algorithms for encryption and decryption of information;

– develop algorithms of encryption and decryption based on existing solutions using the method of rapid calculation of multi-digit numbers;

– develop software implementation of the developed algorithm;

– perform the analysis of the obtained results.

The object of research is the process of encryption and decryption of information.

The subject of research - algorithms of encryption and decryption of information, methods of fast calculation of multi-digit numbers.

The scientific novelty of the results is to use fast methods for calculating multi-digit numbers for encryption and decryption of information, which will accelerate existing algorithms for encryption and decryption of information**.**

Publications. The materials of the work are published in the International scientific conference "iScience" and in the International conference “ΛΌΓΟΣ”.

FAST CALCULATION OF MULTI-DIGIT NUMBERS, ALGORITHMS FOR ENCRYPTION AND DECRYPTION INFORMATION, CRYPTOGRAPHY