ABSTRACT

Master's thesis: 94 pp., 30 fig., 22 tab., 1 app., 24 sources.

The relevance. The cumbersome implementation of IT makes it an urgent problem to protect information. Statistics show that only some business owners in this industry consider their company to be able to withstand today's information threats.

This study addresses the issue of improving the efficiency of encryption and decryption algorithms. Increasing numbers of digital documents and commercial transactions create an urgent need for encryption algorithms. Secure cryptographic algorithms are very time consuming and their effective implementation is necessary for programs. This study presents the parallel implementation and analysis of various encryption algorithms such as: AES (Advanced Encryption Standard), Blowfish, Twofish, DES (Data Encryption Standard), Serpent, Triple DES and RSA. Parallel implementation of algorithms is created to increase the efficiency of algorithms. Experiments show that a consistent implementation is significantly inferior to a parallel one at run time. The algorithms are compared based on the time of encryption and decryption of information and their acceleration. The results show that Triple DES is a more efficient algorithm among the studied algorithms.

Relationship with working with scientific programs, plans, topics. The work was performed at the branches of the Department of Automated Information Processing and Control Systems of the National Technical University of Ukraine «Kyiv Polytechnic Institute. Igor Sikorsky» within the theme «Develop optimal cryptographic algorithms for accuracy and speed, parallelize them and make their comparative analysis».

Objective: To increase the acceleration of information encryption and decryption algorithms.

To achieve the desired goal, you must perform the following tasks:

– review existing solutions;

– to develop algorithms on the basis of existing means of encryption and decryption of information, to parallelize each of the proposed algorithms;

– to develop software implementation of the given algorithms;

– to perform comparative analysis of sequential and parallel execution of different algorithms.

The object of the study is to encrypt information and decrypt it.

The subject of the study - algorithms by which you can perform encryption and decryption of information.

The scientific novelty of the obtained results is the parallelization of existing cryptographic algorithms and their comparative analysis.

Publications. The materials have been published in the International Scientific Conference “iScience”, in the International Conference “UKRLOGOS”, in the All-Ukrainian Scientific and Practical Conference of Young Scientists and Students “Information Systems and Technologies of Management” and in the International Scientific Internet Conference “Information Society: Technological, Economic and technical aspects of becoming".

EFFECTIVE ALGORITHMS FOR CALCULATING CRYPTO PRIMITIVES IN A PARALLEL COMPUTING SYSTEM.