АНОТАЦІЯ

Дипломний проєкт включає у себе пояснювальну записку (51 ст., 27 рис., 3 додатки).

Об'єктом розробки – створення криптостійкої системи шифрування даних на базі алгоритму Salsa20.

Система шифрування дозволяє: шифрувати та дешифрувати інформацію, здійснювати швидку передачу даних з перевіркою на їх цілісність, генерувати криптостійкий нонс та швидкий псевдовипадковий ключ. У процесі розробки було використано програмне середовище QT для створення інтуїтивно-зрозумілого інтерфейсу.

У ході розробки:

* проведено аналіз існуючих алгоритмів шифрування;
* проведено аналіз основних кібератак на конфіденційні дані;
* дослідження технологій розробки для відповідних систем;
* сформульовані вимоги для криптостійкої системи;
* розроблено та протестовано систему для кодування та декодування інформації на базі існуючого алгоритму.

Упровадження цієї системи дозволить збільшити швидкість обробки даних для шифрування із забезпеченням захисту від зловмисників.

Ключові слова: криптостійка система, Salsa20, цілісність даних, нонс, пседовипадковий ключ, QT.

ABSTRACT

Diploma project includes an explanatory note (51 p., 27 fig. 3 appendices).

The object of development is to create a сryptographically strong algorithms for data encryption systems based on the Salsa20 algorithm.

The encryption system allows: to encrypt and decrypt information, to perform fast data transfer with verification of their integrity, generate a a сryptographically strong nonce and a fast pseudorandom key. The QT software environment was used in the development process to create an intuitive interface.

During development:

* the analysis of existing encryption algorithms is carried out;
* the analysis of the main cyber attacks on confidential data is carried out;
* research of development technologies for the corresponding systems;
* the requirements for a сryptographically strong system are formulated;
* developed and tested a system for encoding and decoding information based on the existing algorithm.

Implementation of this system will increase the speed of data encryption to protect against intruders.

Keywords: strong cryptography, Salsa20, data integrity, nonce, pseudorandom key, QT.