РЕФЕРАТ

Актуальність. Широке впровадження інформаційних технологій робить закономірною та актуальною проблему захисту інформації. Дослідження показують, що лишеполовина фахівців з інформаційної безпеки вважають свою компанію чи установу такою, що готова протистояти сучасним інформаційним загрозам, зокрема і таким, що можуть призвести до неконтрольованого поширення інформації за межі інформаційних систем, у яких вона обробляється

Зв'язок роботи з науковими програмами, планами, темами. Однією з важливих галузей досліджень в системах, мережах і пристроях ІТ є дослідження та розробка нових методів захисту інформації та забезпечення інформаційної безпеки систем, мереж і пристроїв. Захист інформації значною мірою базується на використанні криптографічних методів, пов'язаних з шифруванням даних. У зв’язку з цим удосконалення існуючих методів шифрування та дешифрування є актуальною, що дозволить компаніям та установам підвищити надійсність зашифрованої інформації (підвищити криптостійкість), підвищити безпеку обміну інформації.

Робота виконана на філії кафедри автоматизованих систем обробки інформації та управління в Інституті кібернетики ім. В.М. Глушкова НАН України в рамках науково-дослідної теми «Розробити оптимальні за точністю та швидкодією алгоритми розв’язання задач: інтегрування швидкоосцилюючих функцій, цифрової обробки сигналів та зображень, дистанційного моніторингу об’єктів, інформаційної безпеки» (В.Ф. 140.14, номер державної реєстрації: 0114U000357).

Мета підвищити швидкість шифрування та дешифрування інформації

Для досягнення мети необхідно виконати наступні **завдання**:

– виконати огляд існуючих методів та засобів шифрування та дешифрування інформації;

– здійснити порівняльний аналіз різних алгоритмів шифрування та дешифрування інформації;

– розробити алгоритми шифрування та дешифрування на основі існуючих рішень з використанням методу швидкого обчислення багаторозрядних чисел;

– розробити програмну реалізацію розробленого алгоритму;

– виконати аналіз отриманих результатів.

Об’єкт дослідження – процес шифрування та дешифрування інформації.

Предмет дослідження – алгоритми шифрування та дешифрування інформації, методи швидкого обчислення багаторозрядних чисел.

Наукова новизна одержаних результатів полягає у використанні швидких методів обчислення багаторозрядних чисел для шифрування та дешифрування інформації, що дозволить прискорити існуючі алгоритми шифрування та дешифрування інформації.

Публікації. Матеріали роботи опубліковані в Міжнародної наукової конференції “iScience” та в Міжнародній конференції “ΛΌГОΣ”.

ОБЧИСЛЕННЯ БАГАТОРОЗРЯДНИХ ЧИСЕЛ, АЛГОРИТМИ ШИФРУВАННЯ ТА ДЕШИФРУВАННЯ ІНФОРМАЦІЇ, КРИПТОСТІЙКІСТЬ