РЕФЕРАТ

Метою даної дипломної роботи є аналіз, уточнення та застосування методів дослідження марковських SP-мереж на стійкість до диференціального криптоаналізу. Об’єктом дослідження є інформаційні процеси в системах криптографічного захисту. Предметом дослідження є алгоритми оцінювання SP-мереж на стійкість до диференціального криптоаналізу. В роботі проводиться уточнення та застосування методів для оцінки стійкості SP-мереж до диференціального криптоаналізу на прикладі шифру ДСТУ 7624:2014. Основні результати роботи представлено у вигляді тез доповіді на XVIII Міжнародній науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах» (Київ, 25-26 травня 2016 р.) та XIV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (Київ, 26-28 травня 2016 р.).

Ключові слова: SP-мережа, диференціальний криптоаналіз, шифр ДСТУ 7624:2014, диференціальна ймовірність.