# МОДЕЛЮВАННЯ АЛГОРИТМУ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ AES НА МОВІ VHDL

**КАРАМАН Д. Г., ШЕВЧЕНКО Д. А.**
**Національний технічний університет "Харьківський політехнічний інститут", м.Харків**

Криптографічні методи відіграють важливу роль у зберіганні та передаванні конфіденційних даних. Потреба у захисті інформації відображається широким вибором існуючих алгоритмів і стандартів шифрування.

AES – новітній стандарт криптографічного захисту інформації, який було прийнято Національним Інститутом Стандартів та Технологій США (NIST) у 2001 році для використання у комерційних та державних установах. Стандарт описує блоковий симетричний алгоритм шифрування, адаптований для програмної та апаратної реалізації. Апаратні рішення мають ряд переваг над програмними, чим пояснюється численна кількість публікацій з пошуку найбільш ефективних апаратних реалізацій цього алгоритму.

Останні тенденції розвитку цифрової техніки відмічають активний інтерес до архітектур типу «Система на кристалі» (SoC), для реалізації яких використовують програмовані логічні інтегральні схеми (ПЛІС) типу FPGA. Для забезпечення функцій криптографічного захисту у таких пристроях алгоритми шифрування виконують у вигляді окремих функціональних модулів (IP-cores) з гнучким налаштуванням.

Проведено аналіз існуючих рішень апаратних реалізацій алгоритму криптографічного захисту інформації за стандартом AES. Розглянуто різні варіанти схемних рішень перетворень алгоритму на мові VHDL, виконано моделювання та верифікацію їхніх динамічних та функціональних характеристик з метою вибору найбільш ефективних рішень.