*Гормакова І.В., Україна, Харків*

## СИСТЕМА БЛОЧНОГО ШИФРУВАННЯ НА МЕРЕЖАХ КЛІТИННИХ АВТОМАТІВ

У доповіді представлено метод побудови системи блочного симетричного шифрування на мережах клітинних автоматів (МКА). Основою метода є використання алгебри груп, які властиві окремим класам МКА. Проведено порівнювальний аналіз криптосистем, побудованих на основі стандартів DES та AES, і криптосистеми на МКА. Показано, що програмно - апаратна реалізація криптосистем на основі МКА забезпечує підвищення швидкодії системи та зменшення апаратних витрат.

*Гормакова И.В., Украина, Харьков*

## СИСТЕМА БЛОЧНОГО ШИФРОВАНИЯ НА СЕТЯХ КЛЕТОЧНЫХ АВТОМАТОВ

В докладе представлен метод построения системы блочного симметричного шифрования на сетях клеточных автоматов (СКА). Метод основан на использовании алгебры групп, присущих отдельным классам СКА. Проведен сравнительный анализ криптосистем, построенных на основе стандартов DES и AES, и криптосистемы на СКА. Показано, что программно-аппаратная реализация криптосистем на основе СКА обеспечивает повышение быстродействия системы и уменьшение аппаратных затрат.

*Gormakova I.V., Ukraine, Kharkiv*

## BLOCK ENCRYPTION SYSTEM BASED ON CELLULAR AUTOMATA

In the report the method of building of block encryption system based on cellular automata (CA) is presented. The method is based on using of group algebra, which is attached to particular class of CA. Comparative analysis of cryptosystems based on DES and AES standards and CA based cryptosystem is carried out. It is shown that hardware-software implementation of CA based cryptosystem ensures increasing system operation speed and decreasing of hardware costs.