Вестник Воронежского государственного университета www.vestnik.vsu.ru
Серия: Системный анализ и информационные технологии, 2006, № 2

ЗАЩИЩЕННАЯ СВЯЗЬ В СТАНДАРТЕ GSM

Ю.Б. Нечаев, Б.Н. Воронков, Е.А. Долбилова,
А.В. Дудченко

В связи с недостаточной криптостойкостью алгоритма шифрования A5/1 стандарта GSM предлагается его модификация, позволяющая расширить ключевое пространство и обеспечить защиту от атаки на основе известного или подобранного исходного текста. С этой целью, на основе теории конечных полей, осуществляются дополнитбельные криптографические преобразования открытого текста и вырабатываемой псевдослучайной последовательности.