ДИНАМИЧЕСКИЙ ХАОС ПРИ ЗАЩИТЕ ИНФОРМАЦИИ

А.В. СИДОРЕНКО

При решении задач защиты информации методология динамического хаоса используется в двух направлениях: 1) при скрытой передаче информации, 2) при криптографической защите данных для обеспечения конфиденциальности, целостности и подлинности информации.

Принципиальным достоинством методов на основе динамического хаоса по сравнению с традиционными являются значительное повышение устойчивости к шумам и искажениям в канале передачи, а также увеличение скорости при скрытой передаче информации.

При использовании динамического хаоса для решения криптографических задач принципиальным является наличие общих фундаментальных свойств между хаосом и криптографией. Среди таких свойств выделяются чувствительность к начальным условиям и апериодичность траекторий в фазовом пространстве хаотических динамических систем, которые обеспечивают такие свойства криптографических систем, как запутывание и рассеяние.

Рассмотрены и охарактеризованы схемы реализации скрытой передачи данных с использованием синхронного хаотического отклика: хаотическая маскировка, переключение хаотических режимов, нелинейное подмешивание информационного сигнала к хаотическому, фазовая автоподстройка частоты, адаптивные методы приема.

Показаны особенности и приведены собственные результаты применения систем с нелинейным подмешиванием информационного сигнала к хаотическому при шифровании данных в криптографии. Отмечаются преимущества схем на основе динамического хаоса для поточных и блочных шифров.