СИНТЕЗ И АНАЛИЗ ХАОТИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ЛИНЕЙНЫХ И НЕЛИНЕЙНЫХ МЕТОДОВ

А.А. БОРИСКЕВИЧ, А.А. МЕРКУШОВ

В настоящее время отсутствуют средства для эффективной оценки и улучшения параметров генераторов криптографических последовательностей на основе динамических хаотических систем, основной особенностью которых является существенная зависимость от начальных условий. Оценка параметров хаотических последовательностей имеет ряд особенностей, заключающихся в необходимости использования сочетания линейных и нелинейных методов тестирования. Предлагаются алгоритмы модификации для улучшения свойств хаотических последовательностей и набор взаимосвязанных тестов для анализа их параметров. Тестирование заключается в использовании дополняющих друг друга трех классов оценок. На основе результатов первого класса оценок, основанного на построении бифуркационной диаграммы, показателя Ляпунова, фрактальных размерностей, осуществляется синтез и выбор хаотических последовательностей с требуемыми криптографическими свойствами. Второй класс оценок, определяющий параметры синтезированных последовательностей в частотной, временной и пространственной областях., предназначен для принятия окончательного решения о возможности использования синтезированных последовательностей в задачах передачи и защиты данных. Третий класс, определяющий временную динамику изменения параметров последовательностей, прошедших два предыдущих уровня тестирования, позволяет оценить непредсказуемость структуры последовательности по ее сегменту ограниченной длинны.