МЕТОДИКА СИНТЕЗА И ТЕСТИРОВАНИЯ КАСКАДНЫХ И КОЛЬЦЕВЫХ ХАОТИЧЕСКИХ ГЕНЕРАТОРОВ ДЛЯ СИСТЕМ ПОТОЧНОГО ШИФРОВАНИЯ

А.А. Борискевич

Одним из эффективных средств для генерирования хаотических псевдослучайных последовательностей (ХПСП) для систем поточного шифрования являются динамические системы детерминированного хаоса. Большинство ХПСП основываются на одной хаотической системе. В этом случае подобные хаотические генераторы потенциально небезопасны, так как выходная последовательность может нести некоторую информацию о структуре хаотической системы. Одним из эффективных средств улучшения свойств генераторов ХПСП основан на двух хаотических системах и обладает большей безопасностью, так как извлечение информации об обеих хаотических системах (о ключах и структуре хаотического отображения) представляет собой более сложную задачу. Целью работы является разработка методики синтеза генератора, обеспечивающего приблизительно одинаковые в понятии выбранной основной характеристики ХПСП вне зависимости от используемых типов хаотических функций в генераторе.

Предложены и проанализированы четыре типа генераторов ХПСП с различными принципами построения, использующие простые хаотические функции: пороговый составной генератор, каскадные генераторы без и с внешними обратными связями и генератор с кольцевой структурой. Разработана система оценки качества генераторов ХПСП на основе количественных и качественных характеристик. В качестве количественных характеристик используются 10 оценок: коэффициенты пологости Фурье-спектра и гистограммы, диапазон значений ХПСП, среднее арифметическое ХПСП, медиана, коэффициент асимметрии, эксцесс, нормированная дисперсия и энтропия, аппроксимационная энтропия (АпЭн). В качестве графических характеристик используются четыре метрики: 2D аттрактор, гистограмма, чувствительность к начальным параметрам и взаимная корреляция последовательностей. Качественные характеристики в данной методики характеризуют интегральную статистику, которая отражает наиболее важные свойства синтезируемых ХПСП.

На основе предложенной методики протестировано 13 различных хаотических функций: отображение Бернулли, рекурсивное отображение, логистическое отображение и три его модификации, четыре функции класса PWAM, отображение Tent и две его модификации.

Установлено, что генератор с кольцевой структурой обеспечивает приблизительно одинаковые по АпЭн значения ХПСП независимо от типа используемой хаотической функции. Данный генератор позволяет добиться самых малых отклонений величины АпЭн при использовании 13 различных хаотических функций по сравнению с генераторами с одной и несколькими хаотическими функциями; различие между максимальным и минимальным значениями АпЭн составляет около одной десятой. Кроме того, предложенный кольцевой генератор обладает гибкой структурой для управления качеством генерируемой ХПСП.