ЦЕЛОЧИСЛЕННЫЕ ХАОТИЧЕСКИЕ ОТОБРАЖЕНИЯ, ИХ СВОЙСТВА И ОСОБЕННОСТИ ПРИМЕНЕНИЯ В АЛГОРИТМАХ ШИФРОВАНИЯ ДАННЫХ НА ОСНОВЕ ДИНАМИЧЕСКОГО ХАОСА

А.В. Сидоренко, К.С. Мулярчик

Развитие теории динамического хаоса в последнее десятилетие способствовало разработке на ее основе новых методов защиты информации. Было установлено, что хаотический сигнал, внешне похожий на шум, может быть потенциально использован в качестве контейнера для передачи информации, скрывая при этом сам факт ее передачи.

В данной работе рассматривается модификация системы шифрования на основе динамического хаоса, заключающаяся в применении дискретного (цифрового, целочисленного) хаотического отображения вместо непрерывного.

Система шифрования представляет собой систему, базирующуюся на явлении самосинхронизации хаотических систем, Используемый в системе алгоритм шифрования основан на применении схемы с нелинейным подмешиванием информационного сигнала к хаотическому. Одной из составных частей данной схемы является хаотическое отображение.

Реализация подобной системы шифрования на практике с помощью персонального компьютера сталкивается с существенной проблемой. Дело в том, что во всех структурных элементах системы шифрования фигурируют действительные числа, представление которых в памяти компьютера неизбежно сопряжено с погрешностью данного представления ввиду ограниченности объема памяти для хранения данных.

Для снятия данного принципиального ограничения предложена модификация системы шифрования, которая заключается в применении дискретного (цифрового, целочисленного) хаотического отображения вместо оперирующего действительными числами непрерывного отображения. Под дискретным отображением здесь понимается отображение, оперирующее целыми числами, представление которых в памяти компьютера не связано с погрешностями.

В данной работе представлен целочисленный аналог tent-отображения. Проведен его анализ, определены и исследованы показатели Ляпунова. Проведен анализ программной реализации модифицированной таким образом системы шифрования на стойкость к атаке методом грубой силы. На основании результатов анализа криптостойкости были выявлены условия, при которых система шифрования является стойкой к атаке методом грубой силы.