# АНАЛИЗ КРИПТОСТОЙКОСТИ СИСТЕМ ШИФРОВАНИЯ НА ОСНОВЕ ДИНАМИЧЕСКОГО ХАОСА

*А.В. Сидоренко, К.С. Мулярчик*

Белорусский государственный университет, факультет радиофизики и электроники
г. Минск, Республика Беларусь
телефон: (+375 17) 2 78 77 42; факс: (+375 17) 209 58 18; e-mail: SidorenkoA@bsu.by
web: www.bsu.by

**В данной статье рассматриваются вопросы построения системы шифрования на основе динамического хаоса. В основе системы лежит явление самосинхронизации двух хаотических систем, схема с нелинейным подмешиванием информационного сигнала к хаотическому, а также несколько видов хаотических отображений. С помощью разработанного программного обеспечения проводится анализ криптостойкости данной схемы шифрования.**

**Ключевые слова - динамический хаос, криптография, криптостойкость.**

## 1 ВВЕДЕНИЕ

Одним из актуальных направлений в развитом информационном обществе является разработка методов и средств защиты информации, что обусловлено необходимостью обеспечения конфиденциальности передаваемой информации. Развитие теории динамического хаоса в последнее десятилетие способствовала разработке на ее основе новых методов защиты информации. Хаотический сигнал может быть использован в качестве носителя информации, контейнера для передачи информации с помощью стеганографических систем. Хаотический сигнал, внешне похожий на шум, может потенциально обеспечить передачу полезной информации, скрывая при этом сам факт ее передачи.

В криптографии полагается, что внутренняя структура криптосистемы хорошо известна, а каналы передачи и синхронизации доступны, что обеспечивает ее работоспособность. Правомочность реализации систем на основе динамического хаоса в криптографии будет доказана при наличии корректных аналогий таких криптографических понятий как: полиномиальная и экспоненциальная вычислительная сложность. Наличие данных аналогий позволит:

1) унифицировать принципы и методы определения криптостойкости для шифров на основе дифференциальных уравнений и дискретных отображений с таковыми для традиционных шифров;

2) разработать методы генерации шифртекста с заданной сложностью.

## 2 ТРЕБОВАНИЯ К СИСТЕМЕ ШИФРОВАНИЯ НА ОСНОВЕ ДИНАМИЧЕСКОГО ХАОСА

К настоящему времени выполнен ряд исследований по разработке стойких систем шифрования на основе динамического хаоса. Сформулированы критерии, которым должен удовлетворять криптографически стойкий алгоритм шифрования: при отображении исходного сообщения в зашифрованное в последнем наличие структур не предполагается; схема кодирования должна быть чувствительной по отношению к открытому тексту и ключу; схема кодирования должна быть симметричной относительно времени кодирования/декодирования; объемы зашифрованного и исходного сообщений не должны сильно отличаться; следует обеспечить простоту и скорость алгоритма кодирования; необходимость обеспечения возможности адаптации схемы кодирования к различным видам информационных сигналов; следует обеспечить возможность изменения длины ключа; схема должна быть устойчивой к основным видам криптоатак (атака "грубой силой", т.е. перебором, и атака на основе известного шифртекста).

Рассматривая системы на основе динамического хаоса для криптографических применений, было отмечено с одной стороны, что такие свойства как чувствительность к начальным условиям, асимптотическая независимость начального и конечного состояний, возможность самосинхронизации передатчика и приемника присущи динамическому хаосу, а с другой – являются характерными для криптографических алгоритмов.

Большинство предлагаемых в литературе методик производят криптографически слабые и медленные алгоритмы. Одна из причин такого положения заключается в необоснованном выборе хаотического отображения для схемы шифрования.

Дело в том, что двумя основными принципами, которыми необходимо руководствоваться при построении алгоритмов, являются чувствительность к открытому тексту и чувствительность к ключу. Малейшие изменения в одном из них должны значительно изменять результаты шифрования. В хаотических алгоритмах шифрования роль открытого текста могут играть начальные условия, в роль ключа – параметры отображения. Это означает, что если мы хотим использовать в качестве основного элемента схемы некоторое хаотическое отображения, то оно должно обладать чувствительностью не

только к начальным условиям, но и к любым возмущениям в пространстве параметров. Однако известно, что большинство хаотических аттракторов структурно неустойчиво по отношению к изменению параметров. Поэтому алгоритмы на их основе могут уметь слабые ключи. В этой связи, необходимо осторожно и обоснованно выбирать тип хаотических отображений. Так, например, устойчивый хаос не может встречаться в гладких системах. С другой стороны, структурно устойчивый хаос может наблюдаться в кусочно-линейных отображениях.

## 3 СИСТЕМА ШИФРОВАНИЯ С НЕЛИНЕЙНЫМ ПОДМЕШИВАНИЕМ ИНФОРМАЦИОННОГО СИГНАЛА К ХАОТИЧЕСКОМУ

В основе построения системы шифрования на основе динамического хаоса лежит схема "хаотический передатчик – хаотический приемник", работающая на эффекте "хаотического синхронного отклика". Особенностью такой схемы является то, что в нем не требуется внешней синхронизации, т.е. для принимающей стороны не требуется знания начальных условий.

Важная роль в процессе построения системы шифрования отводится выбору способа передачи информации, структуре и параметрам схемы передачи информации на основе синхронного хаотического отклика. На основе анализа различных вариантов схем построения была выбрана схема кодирования с нелинейным подмешиванием информационного сигнала к хаотическому. Данная схема рассматривается как простая и, в то же время, эффективная схема защиты информации. Важными особенностями данной схемы по отношению к другим возможным схемам передачи информации на основе динамического хаоса являются: свойства точного извлечения информации из смеси с хаотическим сигналом, самосинхронизация передатчика и приемника, простота аппаратной и программной реализации.

Структурная схема системы шифрования приведена на рис.1:

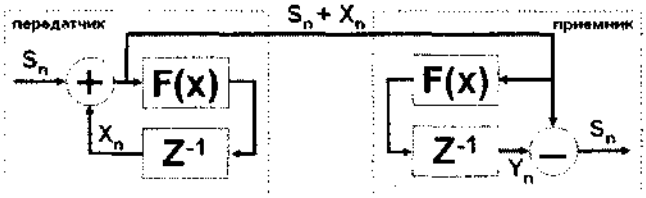


Рис.1. Структурная схема системы шифрования.

Кодер и декодер данных состоят из следующих структурных элементов:

– нелинейный преобразователь (НП) – хаотическое отображение F(X);

– фильтр (Ф) – единичная задержка $Z^{-1}$

– сумматор (вычитатель)

В данной схеме используются следующие типы хаотических отображений:

– tent-отображение

– отображение сдвига Бернулли

Для каждого из данных отображений показатели Ляпунова положительны, что говорит о том, что хаотическое поведение отображения сдвига Бернулли наблюдается также на всем промежутке допустимых значений параметра $\mu$, где $\mu$ – параметр отображения .

## 4 АНАЛИЗ КРИПТОСТОЙКОСТИ

Для практического осуществления криптографических преобразований информации на основе разработанной схемы кодирования, а также анализа криптостойкости данной схемы было разработано программное обеспечение, которое осуществляет кодирование и декодирование информации. Для экспериментов в качестве открытого текста выбран фрагмент текста на русском языке.

Проведен статистический анализ открытого текста, а также соответствующих ему шифртекстов, полученных с помощью программы на основе одного из перечисленных выше хаотических отображений. Произведенный анализ позволяет сделать вывод о том, что данная схема производит надежное сокрытие факта передачи информации.

Для определения криптостойкости данной схемы шифрования проводилось расшифрование зашифрованного исходного текста, при этом ключ для расшифрования выбирался близким к ключу шифрования.

## 5 ВЫВОДЫ

В данной работе рассмотрены вопросы, связанные с применением методов хаотической динамики для решения криптографических задач. Основным компонентом схемы шифрования на основе динамического хаоса является хаотическое отображение, выбор которого определяет криптостойкость схемы шифрования. Криптостойкость схемы шифрования оценивалась путем расшифрования зашифрованного исходного текста ключом, близким к ключу шифрования.

## ЛИТЕРАТУРА


[1] Nonlinear–dynamic systems of confidential communication: classification, simulation, experiment / Igor Izmailov [и др.] // ENOC 2008, Saint Petersburg, Russia June, 30–July, 4 2008

[2] Кодирование и передача информации на основе хаотических динамических систем с дискретным временем / А.А. Дмитриев // М., 2003

[3] Динамический хаос. / А.П. Кузнецов // М.: Физматлит, 2005