УДК 621.373
Д.И. Ганзина, Т.А. Левицкая, канд. техн. наук, доц.
ГВУЗ «ПГТУ», Украина

ПРИМЕНЕНИЕ КРИПТОСИСТЕМЫ НА ГЕНЕРАТОРЕ ХАОСА «СХЕМА ЧУА» ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

D.I. Ganzina, T.A. Levitskaya, Ph.D, Assoc. Prof.

APPLICATION CRYPTOSYSTEM ON THE GENERATOR CHAOS "CHUA CIRCUIT" PROTECTION OF INFORMATION

Защита информации от нарушения её конфиденциальности, целостности, а также доступности является одной из важнейших проблем нынешнего времени, когда для передачи каких-либо данных используются технические средства, которые могут быть подвержены атаке злоумышленника или воздействию среды. Защита информации с помощью шифрования позволяет подтвердить целостность, обеспечить конфиденциальность и доступность данных для конечного получателя.

Данная работа посвящена обоснованию применения криптосистемы, основанной на математической модели генератора хаоса (электрической цепи, демонстрирующей режимы хаотических колебаний), предложенного Леоном Чуа в 1983 году, описанию принципов реализации криптоалгоритма и перспективам применения. Благодаря тому, что схема Чуа является одним из простейших генераторов хаоса (описывается всего тремя дифференциальными уравнениями и при этом обладает достаточно сложным поведением, свойственным генераторам хаоса), она была выбрана для реализации системы шифрования информации[1-2].

Криптосистемы на генераторах хаоса обладают рядом преимуществ над симметричными системами и системами с открытым ключом (последние при шифровании информации используются в форме гибридных криптосистем), главной проблемой которых является длина ключа, а в результате – его повторяемость.

К особенностям криптосистем на генераторах хаоса относятся [3]:

- структурная сложность и нерегулярность хаотического сигнала;
- практически неограниченная длина генерируемого ключа.

В работе приведены требования к криптосистемам и алгоритмами, а также их проблемы, принципы применения генераторов хаоса, как компонентов криптосистемы, описание схемы Чуа и её уравнений, результаты и перспективы применения генераторов хаоса, в частности, схемы Чуа для шифрования передаваемой информации.

Литература

1. Бугаевский М. Ю. Исследование поведения цепи Чуа. Учебно-методическое пособие /М. Ю. Бугаевский, В. И. Пономаренко. — Саратов: Издательство ГосУНЦ «Колледж», 1998. — 29 с.
2. Баричев С. Г. Основы современной криптографии /С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. — М.: Горячая линия — Телеком, 2002. — 175 с.
3. Кузнецов А. П. Наглядные образы хаоса /А. П. Кузнецов //Соросовский образовательный журнал. – 2000. – № 11. – С. 104-110.