УДК 681.3.06

О. М. Бевз, к.т.н., доц., К. В. Деревенько

СИСТЕМА ПЕРЕДАЧИ ДАННЫХ С БЫСТРЫМ ДЕКОДИРОВАНИЕМ И ВЫСОКОЙ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТЬЮ

Современные оптоэлектронные системы обладают рядом преимуществ по сравнению с другими системами передачи информации. Вместе с тем, существует ряд проблем, которые снижают эффективность процесса передачи информации. Одними из таких главных и важных проблем являются проблема искажения данных во время передачи и проблема возможности несанкционированного доступа со стороны постороннего участника.

Искажение информации приводит к ошибкам в работе оптоэлектронной системы и возникает в результате помех, которые влияют на передаваемые в оптоэлектронных системах данные. Наиболее часто искажаются два информационных символа – возникают две ошибки. Несанкционированный доступ (НСД) участников возможен по причине открытости каналов связи, на основе которых работают оптоэлектронные системы. Современные методы исправления двух ошибок и методы защиты от несанкционированного доступа, которые используются в оптоэлектронных системах, характеризуются рядом недостатков. Самые критические из них – низкая скорость работы оптоэлектронной системы, которая приводит к снижению эффективности работы оптоэлектронной системы.

Цель данной статьи – повышение эффективности работы оптоэлектронной системы, в которой реализовано исправление двух ошибок и информационная защита от несанкционированного доступа.

Методы. Наиболее распространенный метод исправления двух ошибок, которые возникают при передаче данных , в системах основывается на использовании семейства кодов Боуза - Чоудхури – Хонквингема. Преимуществом данных кодов является возможность индикации наличия трех ошибок . Декодирования кодовой последовательности, которая будет получена из системы передачи данных с быстрым декодированием и высокой криптографической стойкостью , базируется на решении системы двух уравнений в конечном поле . Нахождение корней этой системы выполняется приведением системы к квадратному уравнению:

$$\left.\begin{aligned} i &+ j = z_1 \\ i^3 &+ j^3 = z_2 \end{aligned}\right\} \qquad (1)$$

Результаты. В результате выполненного исследования разработана оптоэлектронная система, в которой используется метод исправления двух ошибок при передачи данных и метод защиты информации от несанкционированного доступа.

Выводы. Метод исправления двух ошибок основанный на обобщении кода Хемминга, реализация которого в оптоэлектронной системе повысит скорость работы на 26%, по сравнению с существующими методами. Метод защиты информации основанный на двухуровневой подстановочно-перестановочной сети. Реализация данного метода в оптоэлектронной системе передачи данных повысит эффективность работы по сравнению с существующими методами на 35%.

Список литературы:

1. Ф. Дж. Мак - Вильямс. Теория кодов исправляющих ошибки / Ф. Дж. Мак – Вильямс, Н. Дж. А. Слоэн // Связь. – 1979. – 743 с.

2. Daemen J. The Design of Rijndael. AES: The Advanced Encryption Standard / Joahn Daemen, Vincent Rijmen // Springer – Berlin. – 2002. – V.234. – P. 24 – 28.

3. O'Connor L. On the distribution of characteristics in bijective mappings / O'Connor L. // Advances in Cryptology – EUROCRYPT '93. – Springer-Verlag. – 1994. – Vol.678. – P. 360 – 370.

4. The block cipher Hierocrypt / [Ohkuma K., Muratani H., Sano F., Kawamura S]. // Proceedings of Selected Areas in Cryptography – SAC 2000, Lecture Notes in Computer Science. – Springer-Verlag. – 2001. – Vol. 2012. – P. 72 – 88.

5. Kanda M. Practical security evaluation against differential and linear cryptanalysis for Feistel ciphers with SPN round function. / Kanda M. // Seventh Annual International Workshop on Selected Areas in Cryptography-SAC`00, Lecture Notes in Computer Science – Springer-Verlag. – 2001. -Vol. 2012. – P.324 – 338.