УДК 618.3.06

СИСТЕМА ПЕРЕДАЧІ ДАНИХ ЗІ ШВИДКИМ ДЕКОДУВАННЯМ І ВИСОКОЮ КРИПТОГРАФІЧНОЮ СТІЙКІСТЮ.

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

Спотворення інформації призводить до помилок в роботі системи передавання даних і виникає внаслідок перешкод, які впливають на передані в оптоелектронних системах дані. Найбільш часто спотворюються два інформаційних символи - виникають дві помилки. Несанкціонований доступ (НСД) учасників можливий унаслідок відкритості каналів зв'язку, на основі яких працює система передавання даних.

Сучасні методи виправлення двох помилок і методи захисту від несанкціонованого доступу, які використовуються в системах передавання інформації, характеризуються рядом недоліків. Найкритичніші з них - низька швидкість роботи системи, яка призводить до зниження ефективності роботи системи передавання даних. Ціль - підвищення ефективності роботи системи, в якій реалізовано виправлення двох помилок та інформаційний захист від несанкціонованого доступу.

Задача вирішується в два кроки. На першому кроці розробляється код, що виправляє дві помилки, з високою швидкістю роботи в системі передачі даних. На другому кроці формується метод шифрування з високою ефективністю работи в системі передачі даних. Перший крок складається з двох етапів. На першому етапі формується код, що виправляє дві помилки, а на другому – розроблюється система декодування, в якій враховані покращені характеристики сучасних методів.

На другому кроці у відповідності з описаною вище ціллю забезпечується висока швидкість роботи і стійкість метода захисту інформації (криптографічного перетворення) в системі передачі даних. Криптографічна стійкість приведення до лінійного і диференціального криптаналізу являється функцією кількості активних S-боксів, яку збільшуємо за допомогою дворівневої підстановлювально-перестановлювальної мережі.

В результаті виконаного дослідження розроблена система передачі даних, в якій використовується метод виправлення двох помилок при передачі даних і метод захисту інформації від несанкціонованого доступу. Метод виправлення двох помилок заснований на узагальненні коду Хеммінга, реалізація якого в системі передачі даних підвищить швидкість роботи на 20%, порівняно з існуючими методами. Метод захисту інформації заснований на дворівневій підстановлювально-перестановлювальній мережі. Реалізація даного методу в системі передачі даних підвищить ефективність роботи в порівнянні з існуючими методами на 30%.