

# ДОСЛІДЖЕННЯ МЕТОДІВ КОДУВАННЯ В ЕЛЕКТРОННИХ СИСТЕМАХ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Гордієнко В.О.

Науковий керівник д.т.н., доц. Стрілкова Т.О.

Харківський національний університет радіоелектроніки  
(61166, Харків, просп. Науки, 14, каф. МЕПП, тел. (057) 702-13-62)

E-mail: [gord11@ukr.net](mailto:gord11@ukr.net)

In this work various coding algorithms were collected. To improve cryptographic stability XOR is used. Next this is a ciphertext that should not substantially exceed the amount of initial information. The solution to this problem is to use the Huffman algorithm which allows us to compress data losslessly. The last problem is the noise immunity for this we apply the Hemminga code and will transmit information through the fiber-optic communication line. Fiber-optic communication lines (FOCL) are used for transmission of (coded) information this concerns both the construction of long telecommunication highways and local area networks (LANs).

**Актуальність.** Актуальність теми полягає в тому, що конфіденційність і недоступність інформації грає дуже велику роль, і тому одним з надійних способів її захисту є шифрування.

Криптографія сьогодні - це найважливіша частина усіх інформаційних систем: від електронної пошти до стільникового зв'язку, від доступу до мережі Internet до електронної готівки. Криптографія забезпечує підзвітність, прозорість, точність і конфіденційність. Вона запобігає спробам шахрайства в електронній комерції і забезпечує юридичну силу фінансових транзакцій. Криптографія допомагає встановити вашу особу, але і забезпечує вам анонімність. [1].

Криптографічні методи захисту інформації забезпечують неможливість несанкціонованого доступу, зміни або видалення важливих комерційних і особистих даних, які зберігаються на вашому комп'ютері. У світі сучасної комерції інформація є одним з найважливіших елементів, і основна частина цієї важливої інформації зберігається і обробляється в електронному вигляді, тому надійні методи захисту комп'ютерної інформації – це самий кращий спосіб перешкодити умисному або випадковому її витоку.

**Метою роботи є розробка** різних методів кодування, які дозволять нам поліпшати криптографічну стійкість, завадостійкість, а також стиснути дані без втрат. Розглянути передачу закодованих даних по волоконно-оптичному зв'язку. Визначити та розрахувати втрати в ВОЛЗ

**Основна частина.** На мою думку, потрібно зібрати різні алгоритми кодування. Для поліпшення криптографічної стійкості використовується

Шифр XOR. Наступне, це шифр-текст, який не повинен істотно перевершувати за об'ємом початкову інформацію. Рішення цієї проблеми є використання алгоритму Хаффмана, що дозволить нам стиснути дані без втрат. Остання проблема це завадостійкість, для цього ми застосуємо код Хеммінга та будемо передавати інформацію по волоконно-оптичній лінії зв'язку. Для передачі (кодованої) інформації використовуються волоконно-оптичні лінії зв'язку (ВОЛЗ), це стосується як побудови протяжних телекомунікаційних магістралей, так і локальних обчислювальних мереж (ЛВС). Цей факт викликаний збільшенням числа користувачів Internet, а також зі зростаючим взаємодією міжнародних операторів і збільшенням обсягів переданої інформації. [2].

**В докладі обговорюються** класифікація методів криптографічного захисту, їх переваги та недоліки. Обговорюються різні методи кодування, та обираються найбільш оптимальні для передачі інформації в електронних системах. Застосування обраних алгоритмів кодування для передачі даних по лініях зв'язку оптичних сигналів та виконання процесу перетворення інформації на Python.

**Запропоновані алгоритми дозволили** поліпшити криптографічну стійкість, завадостійку, а також стиснути дані без втрат. Передача закодованих даних по волоконно-оптичному зв'язку дозволить нам передавати інформацію на високій швидкості, недосяжній для інших систем зв'язку.

Для передачі даних по ВОЛЗ, а саме зменшення кількості ділянок регенерації ми збільшили довжину ділянки регенерації. Так як довжина ділянки регенерації в даному випадку визначається довжиною ділянки, обмеженої дисперсією, то збільшити довжину можна або зменшенням швидкості передачі інформації, що небажано, або збільшенням інформаційної ємності, що є корисним фактором. Тому було збільшено інформаційну ємність за рахунок зменшення дисперсії (в нашому випадку в основному межмодовою дисперсією, так як при даних параметрах волокна (ступінчаста Багатомодові ВОЛЗ) переважає межмодова дисперсія над матеріальною). Для зменшення межмодовою дисперсії використовували градієнтне волокно. Смуга частот оцінюється параметром, який називається інформаційною ємністю ВОЛЗ. Зі зменшенням дисперсії, зростає інформаційна ємність.

#### **Література:**

1. Zhichao Yu, Willen Lao System and method for executing Advanced Encryption Standard (AES) algorithm, US7106860B1 2006-09-12 2. John M. Zelle, Ph.D. Python Programming: An Introduction to Computer Science 2013.