

УДОСКОНАЛЕНИЙ СПОСІБ ТА ПРИСТРІЙ МАСКУВАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

*Карпуков Л. М., д.т.н., проф.; Щекотихін О. В., к.т.н., доцент;
Савченко Д. К., аспірант
ЗНТУ, м. Запоріжжя, Україна*

Метою навчальної роботи є розробка способу захисту інформації у волоконно-оптичних лініях зв'язку від несанкціонованого доступу з поліпшеними характеристиками, тобто з підвищеною захищеністю, надійністю та з покращеною якістю інформаційного сигналу на приймальній стороні.

Поставлена задача вирішується тим, що виконується маскування інформаційного сигналу перед передачею по волоконно-оптичній лінії зв'язку, тобто забезпечується однакова форма заповнення кожної частини тактового інтервалу T як при передачі двійкового нуля, так і при передачі двійкової одиниці, а на приймальній стороні виконуються зворотні перетворювальні дії [1,2].

При цьому виконують наступні перетворювальні дії. Перед передаванням інформації вона проходить етап маскування, а саме, інформацію, яку треба захистити, розподіляють за кодом RZ-1/4, тобто на чотири частини тактового інтервалу T , причому двійкова одиниця передається однією чвертю тактового інтервалу T на його початку, затримується на час, рівний $1/2$ частині тактового інтервалу, та передається як на початку тактового інтервалу, так і у третій його чверті разом протягом кожного тактового інтервалу T . Маскування інформації виконується також при передачі двійкового нуля, передавання якого відбувається заміною відсутнього в тактовому інтервалі T нульового посилення на посилення імпульсів відповідних двійковій одиниці, та виконуються такі ж перетворювальні дії як для двійкових одиниць. Передача замаскованих двійкових одиниць та нуля відбувається на двох обов'язково сусідніх довжинах хвиль стандартного частотного плану WDM, які мультиплексуються і передаються одночасно. На приймальному боці після демультимплексування інформація маскованих двійкових нулів відкидається. Інформація двійкових одиниць передається для подальшої обробки, в процесі якої інформація на $1/4$ та $3/4$ частинах кожного тактового інтервалу T коду RZ-1/4 затримується на час, що дорівнює $1/4$ частині тактового інтервалу. Відповідно інформація відображається на $2/4$ та $4/4$ частинах у кожному тактовому інтервалі при передаванні двійкової одиниці, а на виході приймача отримується інформація в коді NRZ [1].

На рис.1 показані кодограми спектрального способу маскування інформаційних сигналів при передачі інформації у волоконно-оптичних лініях зв'язку.

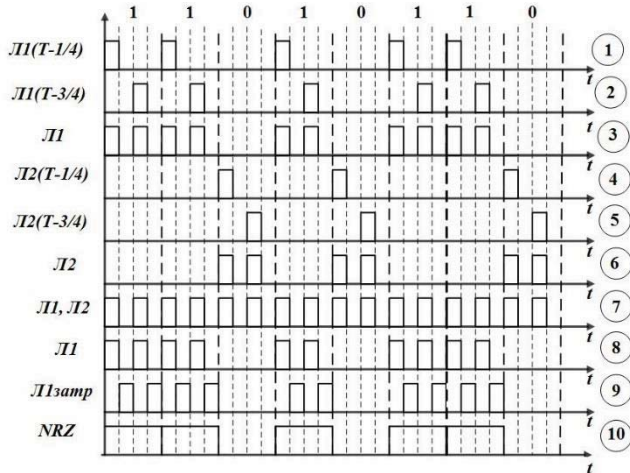


Рисунок 1. Кодограми спектрального способу маскуванню інформаційних сигналів при передачі інформації у волоконно-оптичних лініях зв'язку.

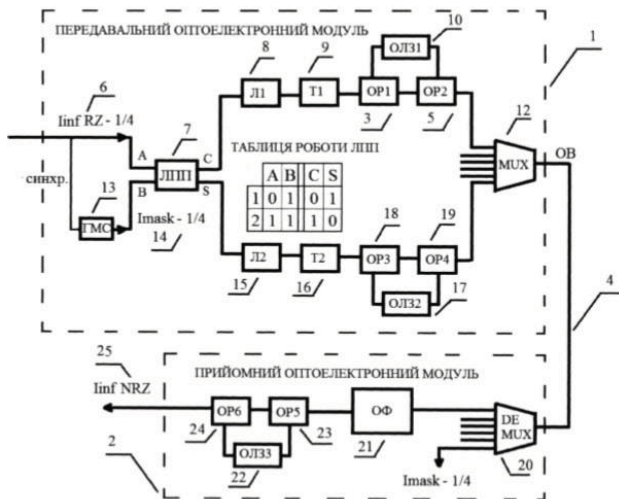


Рисунок 2. Пристрій захисту інформації у волоконно-оптичних лініях зв'язку від несанкціонованого доступу.

Для НДІ необхідне використання спеціального спектрального обладнання, яке дозволило б визначити довжини хвиль переданих оптичних сигналів.

Далі наведено пристрій, що реалізує запропонований спосіб (рис. 2).

Пристрій працює наступним чином. Наприклад, необхідно безпечно, швидко та якісно передати конфіденційну інформацію від мікрофона, що являє собою сигнал в аналоговій формі. В такому випадку виконуються наступні перетворювальні дії. В передавальному оптоелектронному модулі (1) перш за все отримуємо інформацію у вигляді інформаційних сигналів $I_{inf} RZ-1/4$ (6), що являються наслідком перетворення сигналів з аналогової форми в цифрову, та представляють собою набір двійкових одиниць і нулів. Одночасно в лінію за допомогою генератора маскувальних сигналів ГМС (13) подаються маскувальні сигнали $I_{mask-1/4}$ (14). Обидва сигнали подаються відповідно

на перший та другий входи логічного перемикаючого пристрою (7А, 7В), та мають вихід з першого та другого виходів (7С, 7S) згідно з таблицею роботи логічного перемикаючого пристрою (7). Далі інформаційний сигнал $I_{inf} RZ-1/4$ (6) надходить на лазерний перетворювач оптичних сигналів Л1 (8), потрапляє на транспондер Т1 (9), затримується в оптичній лінії затримки ОЛЗ1 (10) через два оптичні розгалужувачі ОР1 (3) та ОР2 (5), потім інформаційний сигнал потрапляє до мультиплектора. В свою чергу маскувальний сигнал $I_{mask-1/4}$ (14) має такі самі перетворювальні дії через лазерний перетворювач оптичних сигналів Л2 (15), транспондер Т2 (16), оптичну лінію затримки ОЛЗ2 (17), що включає в себе два оптичні розгалужувачі ОР3 (18) та ОР4 (19). Після цих дії маскувальний сигнал $I_{mask-1/4}$ (14) потрапляє на мультиплексор, де сумується разом з інформаційним сигналом $I_{inf} RZ-1/4$,

а потім отриманий сигнал через волоконно-оптичну лінію ОВ (4) потрапляє на прийомний оптоелектронний модуль (2). В цьому модулі отриманий сигнал перш за все потрапляє на демультіплексор (20), де знову розділяється на два окремих сигнали - інформаційний та маскувальний. Одразу після проходження демультіплексора маскувальний сигнал $I_{mask-1/4}$ (14) відкидається, а інформаційний сигнал $I_{inf RZ-1/4}$ (6) потрапляє на оптичний фільтр ОФ (21), після чого затримується в затримується в оптичній лінії затримки ОЛЗЗ (22) через два оптичні розгалужувачі ОР5 (23) та ОР6 (24). На виході отримуємо інформаційний сигнал в коді NRZ $I_{inf NRZ}$ (25). [2]

Перелік посилань

1. Пат. 123836 Україна, МПК Н 04 К 1/10 Н 04 В 10/25. Спосіб захисту інформації у волоконно-оптичних лініях зв'язку від несанкціонованого доступу [*Електронний ресурс*] / О. В. Щекотихін, Л.М. Карпуков, Д.К. Савченко, Т.В Литовка ; заявл. 26.09.2017; опубл. 12.03.2018, Бюл. № 5. – Режим доступу: <http://base.uipv.org/searchINV/search.php?action=viewdetails&IdClaim=245125>.

2. Пат. 132701 Україна, МПК Н 04 К 1/10 Н 04 В 10/25. Пристрій захисту інформації у волоконно-оптичних лініях зв'язку від несанкціонованого доступу [*Електронний ресурс*] / О. В. Щекотихін, Л.М. Карпуков, Д.К. Савченко, Т.В Литовка ; заявл. 30.08.2018 ; опубл. 11.03.2019, Бюл. № 5. – Режим доступу: <http://base.uipv.org/searchINV/search.php?action=viewdetails&IdClaim=256383>.

Анотація

Пропонується удосконалений спосіб шифрування лінійного коду в волоконно-оптичних лініях зв'язку шляхом додаткового маскуванню довічного «нуля». Також наводиться опис роботи пристрою захисту інформації, заснований на запропонованому способі.

Ключові слова: волоконно-оптичні лінії зв'язку, маскуванню лінійного коду, лінійний тракт, несанкціонований доступ.

Аннотация

Предлагается усовершенствованный способ шифрования линейного кода в волоконно-оптических линиях связи путем дополнительного маскирования двоичного «нуля». Также приводится описание работы устройства защиты информации, основанного на предложенном способе.

Ключевые слова: волоконно-оптические линии связи, маскирование линейного кода, линейный тракт, несанкционированный доступ.

Abstract

An improved method for encrypting a linear code in fiber-optic communication lines by additional masking of binary “zero” is proposed. A description is also given of the operation of an information protection device based on the proposed method.

Keywords: fiber-optic communication lines, masking of a linear code, linear path, unauthorized access.