УДК 621.391

М.В. ВАСИЛЬКІВСЬКИЙ, Р.П. ПАЛАМАРЧУК
Вінницький національний технічний університет

ЗАХИСТ ІНФОРМАЦІЇ У ВОЛОКОННО-ОПТИЧНИХ ЛІНІЯХ ЗВ'ЯЗКУ

Розглянуто способи несанкціонованого доступу до інформаційних потоків у волоконно-оптичних лініях зв'язку та способи їх захисту. Проаналізовано можливі варіанти реалізації захисту від несанкціонованого доступу. Запропоновано структурні схеми апаратної реалізації керуючих пристроїв для захисту волоконно-оптичної лінії зв'язку. Запропоновано апаратно-програмний метод захисту інформації у волоконно-оптичних лінійних трактах багатоканальних ВОСП-СРК. Запропонований засіб захисту волоконно-оптичної лінії зв'язку показав, що його використання підвищує інформаційну безпеку волоконно-оптичної лінії зв'язку.

Ключові слова: волоконно-оптична лінія зв'язку, захист інформації, несанкціонований доступ.

M.V. VASYLKIVSKYI, R.P. PALAMARCHUK
Vinnytsia National Technical University

INFORMATION PROTECTION IN FIBER-OPTIC COMMUNICATION LINES

The analysis of possible ways of unauthorized access in fiber optic communication lines and means of their protection was made. Also was analyzed are the basic methods of protecting the fiber-optic communication line from unauthorized access, which eliminate the ability to intercept information. Possible options for implementation of protection against unauthorized access are analyzed. The structural schemes of the hardware implementation of control devices for the protection of the fiber optic communication line are proposed. The proposed remedy of protection for fiber-optic communication line showed that its use enhances the security of the fiber-optic communication line. The modified method for controlling the security of a multichannel fiber-optic communication line (FOCL) is considered in the article, which allows determining the time and place of unauthorized access (UA). At the heart of this method is the technology of measurement reflectometry and the method of statistical analysis of quantitative indicators of the quality of the operation of the fiber optic communication line with the use of error criterion. The proposed method of FOCL control is based on the simultaneous use of hardware and software, which allows to improve the efficiency of the protection of information flows through the additional processing of information signals transmitted by the FOCL and to increase compliance indicator and accuracy of determining the location of unauthorized access to optical channels. An overview of the main types of hardware and software protection fiber optic communication lines showed a number of objective shortcomings of existing methods and created the prerequisites for the use of combined information security tools in the fiber optic transmission systems. The proposed method makes it possible to effectively determine the presence of unauthorized access. The advantage of this method is that this method can be implemented as in simple networks and in expanding networks. Additional computer use allows you to analyze and predict possible changes in the power of optical signals and to set the location of unauthorized access using reflectometer that can work by using PC according to the proposed algorithm.

Keywords: fiber-optic communication lines, information protection, unauthorized access.

Вступ

В сучасних телекомунікаційних мережах на базі волоконно-оптичних ліній зв'язку (ВОЛЗ) існує проблема несанкціонованого доступу (НД) в лінійний тракт [1, 2]. Способи несанкціонованого підключення до волоконно-оптичного кабелю (ВОК), що відомі як «fiber tapping», можна поділити на дві категорії. До першої категорії відносяться способи, які передбачають переріз оптичного волокна для подальшого підключення за допомогою спеціального пристрою зчитування (перехоплення) інформації [3]. До другої категорії відносяться способи, що передбачають порушення розповсюдження хвилі в оптичному волокні (ОВ), а отже втручання в інформаційний потік даних без перерізу ОВ [4].

Існуючі методи захисту або мінімізації можливостей здійснення несанкціонованих підключень в певній мірі дозволяють підвищити захищеність інформаційних потоків у ВОЛЗ. При цьому розрізняють три групи методів, а саме [5]: моніторинг цілісності кабелю та контроль рівня потужності оптичних сигналів; використання волокна з підвищеним коефіцієнтом гнучкості; шифрування інформаційних сигналів за допомогою криптографічних методів.

Вказані методи запобігають основним способам несанкціонованого підключення до оптичного волокна, але характеризуються низькою точністю встановлення місця НД у ВОЛЗ.

Наведена аргументація підтверджує своєчасність та актуальність поставленої науково-практичної задачі, розв'язання якої потребує розвитку методів та практичних положень для побудови засобів контролю НД у ВОЛЗ.

Метою роботи є підвищення точності засобів встановлення місця НД у ВОЛЗ за рахунок додаткового оброблення інформаційних сигналів, що передаються у ВОЛЗ.

Для досягнення заданої мети необхідно розв'язати такі задачі:

- виконати аналіз особливостей апаратного та програмного підходу при реалізації методів захисту ВОЛЗ від НД;
- здійснити розробку методу захисту ВОЛЗ від НД;
- розробити структури засобів контролю захищеності ВОЛЗ.

Аналіз особливостей апаратного та програмного підходу при реалізації методів захисту ВОЛЗ від НД

Основним апаратним методом виявлення несанкціонованого доступу є метод контролю рівня потужності оптичних сигналів на вході оптичного приймача. При зменшенні рівня потужності оптичних сигналів, що відповідає виникненню НД приймається рішення про перенаправлення інформаційних потоків на інші маршрути передавання. При цьому, для забезпечення точності методу необхідно забезпечити

постійний рівень потужності оптичних сигналів у ВОЛЗ за умови задіяного типу кодування, який не залежить від виду інформаційних сигналів, що передаються [4]. Отже, зменшення контрольованого значення рівня потужності оптичних сигналів зумовлює спрацювання аварійної сигналізації. Ефективним способом виявлення підключень до ВОЛЗ є використання оптичних рефлектометрів, оскільки інші варіанти контролю передбачають додаткові під'єднання до волокна, які спричиняють додаткове затухання потужності оптичних сигналів. Сутність рефлектометричного методу полягає в тому, що в досліджуване ОВ подається потужний короткий імпульс та реєструється випромінювання, що розсіюється в зворотному напрямку на всіх неоднорідних ділянках ОВ, за інтенсивністю якого можна аналізувати розподілені втрати потужності оптичного сигналу на всій довжині ВОЛЗ до 120 км. Порівняння записаних еталонних рефлектограм в пам'яті комп'ютера, що виконані при різних параметрах зондуючого сигналу з відповідними поточними рефлектограмами може забезпечити контроль захищеності ВОЛЗ з точністю по локальному відхиленню рефлектограм не більше ніж на 0,1 дБ. Перевищення порогу відхилення рефлектограми свідчить про присутність НД до ОВ у визначеній точці тракту. Отже, за допомогою рефлектометрів можна встановити відстань до точки несанкціонованого підключення в тракті передачі інформаційних потоків [4].

Крім апаратних методів також використовуються програмні методи захисту оптичних інформаційних сигналів у ВОЛЗ. В основі переважної більшості програмних методів захисту використовуються протоколи шифрування третього та другого рівнів. Реалізація протоколу шифруванням третього рівня (IPSec) здійснюється на приймальному абонентському обладнанні, що створює додаткові затримки в роботі телекомунікаційного обладнання. Через те, що виконання протоколу розпочинається на початку сесії та з використанням великої кількості мережевих елементів, його загальна реалізація може бути досить складною. Використання другого рівня шифрування звільняє елементи третього рівня від функції шифрування. В основі методу шифрування другого рівня використовується технологія оптичного кодового мультиплексування CDMA. При цьому ймовірність перехоплення інформації є функцією декількох параметрів, включаючи відношення сигнал-шум, дроблення (Fraction) доступної системної ємності [5].

Таким чином, для ефективного захисту ВОЛЗ необхідно використовувати комбіновані (апаратно-програмні) методи захисту оптичних інформаційних потоків. Один з цих методів базується на моніторингу контрольних сигналів, що передаються по додаткових ОВ навколо робочого оптичного волокна. Для цього має бути зарезервовано додатковий ВОК, що підвищує вартість ВОЛЗ. Такий підхід дає змогу здійснювати моніторинг рівня потужності оптичного сигналу та відслідковувати спроби згинання контрольованого ВОК, при яких відбудеться фіксування додаткових втрат потужності оптичних сигналів в ОВ, що зумовить спрацювання сигналу тривоги.

Метод контролю захищеності багатоканальної волоконно-оптичної лінії зв'язку

В роботі розглянуто модифікований метод контролю захищеності багатоканальної волоконно-оптичної лінії зв'язку (ВОЛЗ), який дозволяє визначити час та місце несанкціонованого доступу (НД). В основі даного методу використовується технологія рефлектометричного вимірювання та методика статистичного аналізу кількісних показників якості функціонування ВОЛЗ з використанням критерію коефіцієнта помилок.

Запропонований метод контролю ВОЛЗ базується на одночасному використанні апаратного та програмного забезпечення, що дозволяє підвищити ефективність захисту інформаційних потоків за рахунок додаткового оброблення інформаційних сигналів, що передаються у ВОЛЗ та підвищити достовірність і точність визначення місця несанкціонованого доступу до оптичних каналів.

Згідно з запропонованим методом обладнання, яке розміщено на приймальній стороні, має у своєму складі систему контролю та виявлення НД. Завданням цієї системи є спостереження за станом лінії, контроль вхідного сигналу та прийняття рішення про наявність або відсутність НД. Для такої системи введемо такі показники якості: $P_в$ – ймовірність виявлення НД; $P_х$ – ймовірність хибного спрацювання; k – перехоплений об'єм інформації; $P_{проп}$ – ймовірність пропуску факту НД.

Якщо значення цих показників знаходяться у межах допустимих значень, то дана система контролю є ефективною. Для того, щоб проаналізувати роботу такої системи, позначимо через S_0 стан ВОЛЗ, в якому відсутній НД, а через S_1 – стан ВОЛЗ за наявності НД. Завдання системи контролю полягає у виявленні моменту зміни стану ВОЛЗ.

Сигнал, що надходить на вхід оптичного приймача ВОСП є послідовністю біт, які виражені у вигляді імпульсів світла з параметрами: тривалістю, рівнем оптичної потужності, функцією розподілу потужності. Підключення до лінії зв'язку (ЛЗ) засобів здійснення НД зумовлює зміну цих параметрів, зокрема зменшиться значення потужності оптичних сигналів а також її закон розподілу [6].

Враховуючи, що фотодетектор в оптичному приймачі ВОСП працює із достатньо потужним оптичним сигналом, тому відношення сигнал/шум для нього буде великим. Проведемо аналіз його роботи для визначення залежності між зміною прийнятої оптичної потужності та ймовірністю виявлення НД або хибного спрацювання.

Введемо величину y_i – параметр рівня сигналу в і-й момент часу, який буде розподілятись за нормальним законом:

$$P(y_i) = \frac{1}{\sqrt{2\pi\sigma_i}} e^{\frac{-(y-\lambda_i)^2}{2\sigma_i}}, \quad (1)$$

де λ_i – математичне сподівання випадкової величини y_i;

σ_i – дисперсія випадкової величини y_i.

Сума величин y_i, яка розраховується в системі контролю для всіх y_i, що відповідають додатнім імпульсам, позначається через Z і порівнюється з порогом γ:

$$Z = \frac{1}{N} \sum_{j=0}^{N} y_j, \quad (2)$$

де N – інтервал аналізу.

За результатами такого порівняння приймається рішення про виникнення НД. Якщо НД відсутній, то цей процес повторюється для наступного інтервалу N. Послідовність біт , що приймаються розбивається на рівні інтервали аналізу з тривалістю N біт. Припустимо, що в певний момент часу починається перехоплення інформації. Цей момент припадає на деякий біт інтервалу N_n. Починаючи з цього біту всі решта біт мають уже змінені параметри через вплив процесу НД. Контроль цих параметрів призводить до того, що на певному інтервалі N_i, який знаходиться від інтервалу N_n на відстані в T інтервалів, система виявить НД. Знаючи це, можна знайти втрати у інформаційних бітах. Якщо m – кількість втрачених біт на першому після появи НД інтервалі (в нашому випадку це N_n), то загальну кількість втрат в бітах можна визначити:

$$L_i = m_i + N \times T + t, \quad (3)$$

де t – час, необхідний для поширення інформації про сигнал НД.

На практиці зазвичай $t << N \times T$, тому можна використовувати співвідношення:

$$L_i = m_i + N \times T. \quad (4)$$

Однак, якщо при заданій ймовірності хибного спрацювання тривоги ймовірність пропуску на одному інтервалі досить мала, то на практиці можна обмежитись одним інтервалом аналізу. Якщо ж ця ймовірність велика, то достатньо збільшити значення N, тобто довжину інтервалу, при тому не виходячи за його межі. При мінімізації значення N, яке буде забезпечувати задані P_x, $P_в$. В цьому випадку, навіть якщо НД розпочнеться посередині попереднього інтервалу і не буде виявленим, то НД буде виявлено на наступному інтервалі при чому втрати інформації не будуть перевищувати величину:

$$L_i = m_i + N. \quad (5)$$

В цьому випадку для розрахунку значень P_x і $P_в$ можна використовувати вирази, які були отримані в роботі [7], оскільки величина Z так само має гаусовий закон розподілу з дисперсією σ_1^2/N і математичним сподіванням λ_1. При появі НД оптична потужність зменшиться та математичне сподівання величини Z стане рівним λ_1^H, а її дисперсія – $\sigma_1 H^2/N$.

Система виявлення НД хибно спрацює тоді, коли при відсутності НД рівень оптичної потужності стане меншим за порогове значення γ. Аналогічно, факт НД може бути пропущений через перевищення рівня потужності за прийняте порогове значення. Звідси можна записати вирази для ймовірностей хибного спрацювання тривоги та виявлення НД:

$$P_x = \frac{1}{\sqrt{2\pi}\frac{\sigma_1}{\sqrt{H}}} \int_{-\infty}^{\gamma} e^{\frac{-(z-\lambda_1)^2}{2\sigma_1^2/N}} dz;$$

$$P_{прол} = \frac{1}{\sqrt{2\pi}\frac{\sigma_1^H}{\sqrt{H}}} \int_{-\infty}^{\gamma} e^{\frac{-(z-\lambda_1^H)^2}{2(\sigma_1^H)^2/N}} dz, \quad (6)$$

де λ_1^H – математичне очікування випадкових величин y_i при наявності НД;

σ_1^H – дисперсія випадкових величин y_i за наявності НД.

Врахуємо, що:

$$P_x \approx 1 - P_в. \tag{7}$$

Вираз (7) записаний із міркувань того, що всі спрацювання системи контролю, які не є результатом НД – хибні. Але:

$$1 - P_в = P_{проп}. \tag{8}$$

Тому, порівнюючи P_x і $P_{проп}$, можна розрахувати їх як функції від N, λ_1 та λ_1^H. При цьому ймовірності будуть поступово зменшуватись при збільшенні N та при збільшенні різниці $\lambda_1 - \lambda_1^H$, яка відповідає зміні рівня оптичної потужності внаслідок НД.

Перепишемо рівняння (6) спростивши їх:

$$P_X = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{(\gamma-\lambda_1)\sqrt{N}}{\sigma_1}} e^{-\frac{y^2}{2}} dy,$$
$$\text{де } y = \frac{(Z-\lambda_1)\sqrt{N}}{\sigma_1}; \tag{9}$$
$$dz = dy\sigma_1\sqrt{N}.$$

Аналогічно для ймовірності пропуску:

$$P_X = \frac{1}{\sqrt{2\pi}} \int_{\frac{(\gamma-\lambda_1^H)\sqrt{N}}{\sigma_1^H}}^{+\infty} e^{-\frac{y^2}{2}} dy,$$
$$\text{де } y = \frac{(Z-\lambda_1^H)\sqrt{N}}{\sigma_1^H}; \tag{10}$$
$$dz = dy\sigma_1^H\sqrt{N}.$$

Якщо $P_x = P_{проп}$, то прирівнявши отримані вирази, можна прирівняти і граничні значення:

$$\frac{\lambda_1 - \gamma}{\sigma_1 / \sqrt{N}} = \frac{\gamma - \lambda_1^H}{\sigma_1^H / \sqrt{N}}. \tag{11}$$

Із виразу (11) знайдемо значення порогу:

$$\gamma = \frac{\lambda_1\sigma_1^H - \lambda_1^H\sigma_1}{\sigma_1 + \sigma_1^H}. \tag{12}$$

Якщо вираз (12) підставити у вираз для ймовірностей P_x та $P_{проп}$, попередньо спростивши його, отримаємо:

$$P_X = P_{прop} = \frac{1}{\sqrt{2\pi}} \int_{\frac{\left(\lambda_1-\lambda_1^H\right)\sqrt{N}}{\sigma_1+\sigma_1^H}}^{+\infty} e^{-\frac{y^2}{2}} dy. \tag{13}$$

Введемо наступне позначення:

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} e^{-\frac{y^2}{2}} dy. \tag{14}$$

Тоді ймовірність хибного спрацювання можна записати:

$$P_x = \Phi\left(\frac{\lambda_1 - \lambda_1^H}{\sigma_1 + \sigma_1^H}\sqrt{N}\right). \tag{15}$$

Величини λ_1, λ_1^H в цьому виразі є математичним сподіванням розподілення оптичної потужності вхідного сигналу. Оскільки дисперсія характеризується шумом, то її зміна залежно від наявності або відсутності НД незначна, тоді вираз (15) можна записати:

$$P_x = \Phi\left(\frac{\lambda_1 - \lambda_1^H}{2\sigma_1}\sqrt{N}\right). \tag{16}$$

Отриманий вираз пов'язує між собою ймовірність хибного спрацювання (яка рівна ймовірності пропуску НД), величину відведеної при НД оптичної потужності, а також величину інформаційних втрат при виявленні НД.

Засоби контролю НД у ВОЛЗ

Для підвищення ефективності захисту ВОЛЗ від НД пропонується здійснювати порівняльний контроль рівнів потужності оптичних сигналів на виході оптичних мультиплексорів/демультиплексорів у ВОЛТ та коефіцієнту помилок на виході оптичних приймачів ВОСП. Для контролю обирається канал з найменшим рівнем потужності оптичних сигналів (найбільший коефіцієнт затухання) [7].

Узагальнена структура пристрою контролю захищеності ВОЛЗ представлена на рис. 1. За допомогою несиметричного оптичного розгалужувача (ОР) виконується підключення до оптичного каналу ВОЛТ пристрою контролю захищеності (ПКЗ). При виникненні несанкціонованого підключення до контрольованої ВОЛЗ зменшується рівень потужності оптичних сигналів у лінійному тракті. При цьому, відбувається зменшення рівня потужності, яку фіксує оптичний приймач з підвищеною чутливістю та передає результат у вигляді електричного сигналу на двоканальний BER-тестер, який одночасно визначає значення коефіцієнта помилок для двох оптичних каналів: робочого (опорного) та контрольованого. Після цього значення коефіцієнта помилок надходять на блок порівняння та визначення різниці, до складу якого входять пристрій порівняння з еталонними значеннями та пристрій формування сигналу про прийняття рішення про присутність або відсутність НД. Даний пристрій контролю доцільно використовувати у невеликих мережах, оскільки блок порівняння результатів потребує ручного налаштування (калібрування) [8]. Для мереж, які поступово розширяються, чи мають перспективу на розширення, застосування такого методу є не доцільним, адже після кожного розширення мережі необхідно здійснювати повторне калібрування блоку порівняння результатів.

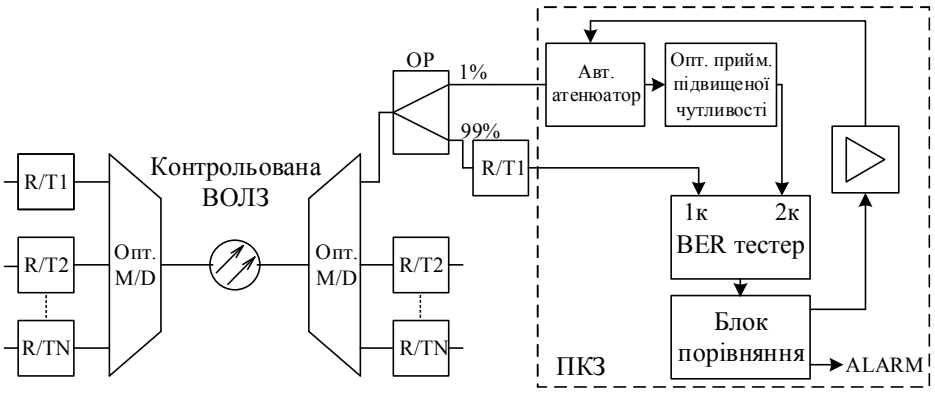

Рис. 1. Узагальнена структура пристрою контролю захищеності ВОЛЗ

Для інфокомунікаційних мереж, що розширяються з динамічним налаштуванням конфігурації обладнання, запропоновано модифікований варіант схеми пристрою (рис. 2).

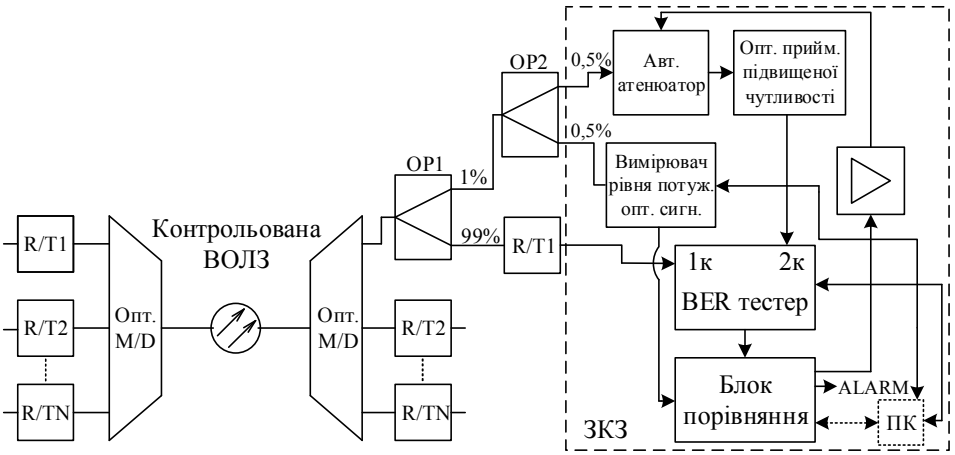

Рис. 2. Узагальнена структура адаптивного пристрою контролю захищеності ВОЛЗ

Для адаптивного налаштування блоку порівняння результатів необхідно додати в структуру ПКЗ ще один ОР та вимірювач рівня потужності оптичних сигналів. Використання ПК у складі ПКЗ дає можливість побудувати адаптивний засіб контролю захищеності (ЗКЗ) ВОЛЗ на базі запропонованого апаратно-програмного методу. Даний ЗКЗ забезпечить ведення статистики функціонування, на базі якої можна буде виконувати прогнозування функціональних характеристик ВОЛЗ в умовно-реальному часі.

Висновки

Огляд основних типів апаратного та програмного захисту ВОЛЗ показав ряд об'єктивних недоліків існуючих методів та створив передумови до використання комбінованих засобів захисту інформації у ВОСП. Запропонований метод дає можливість ефективно визначати наявність НД. Перевагою даного методу є те, що його можливо реалізувати як і в простих мережах, так і у мережах, що розширюються. Додаткове використання комп'ютера дає змогу аналізувати та прогнозувати можливі зміни потужності оптичних сигналів та встановлювати місце НД за допомогою рефлектометрів, які можуть працювати при керуванні з ПК згідно з запропонованим алгоритмом.

Література

1. Бортник Г.Г. Методи та засоби оцінювання параметрів абонентських ліній зв'язку / Г.Г. Бортник, В.М. Кичак, В.Ф. Яблонський. – Вінниця : УНІВЕРСУМ-Вінниця, 2006. – 139 с.

2. Бортник Г.Г. Системи передавання в електрозв'язку : навчальний посібник / Г.Г. Бортник, О.А. Семенюк, О.В. Стальченко. – Вінниця : ВНТУ, 2006. – 138 с.

3. Warwick Ford, Computer communications security: principles, standard protocols and techniques. Englewood Cliffs, N.J.: PTR Prentice Hall, 1994, 494 p.

4. Douglas R. Stinson Cryptography: Theory and Practice. CRC Press, Inc. Boca Raton, FL, USA, 1995, 434 p.

5. Niels Ferguson, Bruce Schneier, Practical Cryptography. Wiley Publishing, Inc., Indianapolis, Indiana, 2003, 432 p.

6. Бортник Г.Г. Метод оцінювання детермінованих складових фазового дрижання у цифрових системах передавання / Г.Г. Бортник, М.В. Васильківський, О.Г. Бортник // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2012. – № 3. – С. 45–48.

7. Бортник Г.Г. Аналіз методів оцінювання джитеру в телекомунікаційних системах / Г.Г. Бортник, М.В. Васильківський, М.Л. Мінов // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2007. – № 1. – С. 169–175.

8. Бортник Г.Г. Методи та засоби підвищення ефективності оцінювання фазового дрижання сигналів у телекомунікаційних системах : монографія / Г.Г. Бортник, М.В. Васильківський, В.М. Кичак. – Вінниця : ВНТУ, 2015. – 140 с.

References

1. Bortnyk H.H. Metody ta zasoby otsiniuvannia parametriv abonentskykh linii zviazku / H.H. Bortnyk, V.M. Kychak, V.F. Yablonskyi. – Vinnytsia : UNIVERSUM-Vinnytsia, 2006. – 139 s.

2. Bortnyk H.H. Systemy peredavannia v elektrozviazku : navchalnyi posibnyk / H.H. Bortnyk, O.A. Semeniuk, O.V. Stalchenko. – Vinnytsia : VNTU, 2006. – 138 s.

3. Warwick Ford, Computer communications security: principles, standard protocols and techniques. Englewood Cliffs, N.J.: PTR Prentice Hall, 1994, 494 p.

4. Douglas R. Stinson Cryptography: Theory and Practice. CRC Press, Inc. Boca Raton, FL, USA, 1995, 434 p.

5. Niels Ferguson, Bruce Schneier, Practical Cryptography. Wiley Publishing, Inc., Indianapolis, Indiana, 2003, 432 p.

6. Bortnyk H.H. Metod otsiniuvannia determinovanykh skladovykh fazovoho dryzhannia u tsyfrovykh systemakh peredavannia / H.H. Bortnyk, M.V. Vasylkivskyi, O.H. Bortnyk // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh. – 2012. – № 3. – S. 45–48.

7. Bortnyk H.H. Analiz metodiv otsiniuvannia dzhyteru v telekomunikatsiinykh systemakh / H.H. Bortnyk, M.V. Vasylkivskyi, M.L. Minov // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh. – 2007. – № 1. – S. 169–175.

8. Bortnyk H.H. Metody ta zasoby pidvyshchennia efektyvnosti otsiniuvannia fazovoho dryzhannia syhnaliv u telekomunikatsiinykh systemakh : monohrafiia / H.H. Bortnyk, M.V. Vasylkivskyi, V.M. Kychak. – Vinnytsia : VNTU, 2015. – 140 s.

Рецензія/Peer review : 18.04.2018 р. Надрукована/Printed :22.05.2018 р.
Рецензент: к.т.н., проф. Бортник Г.Г.