УДК 621.396

М. В. Васильківський [1]
Р. П. Паламарчук [1]

МЕТОДИ ЗАХИСТУ ВОЛОКОННО-ОПТИЧНИХ ЛІНІЙ ЗВ'ЯЗКУ

[1] Вінницький національний технічний університет;

Анотація

У роботі розглянуто способи несанкціонованого доступу до інформаційних потоків у волоконно-оптичних лініях зв'язку та способи їх захисту. Запропоновано використовувати модифікований апаратно-програмний метод захисту інформації у волоконно-оптичних лінійних трактах.

Ключові слова: волоконно-оптична система передачі, несанкціонований доступ, захист інформації.

Abstract

The analysis of possible ways of unauthorized access in fiber optic communication lines and means of their protection was made. It is proposed to use the modified hardware-software method of information protection in fiber-optic communication line.

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

Вступ

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, що забезпечує зчитування (перехоплення) інформації. До другої категорії відносяться способи, що передбачають порушення розповсюдження хвилі в оптичному волокні (ОВ), а отже порушення потоку даних без перерізу ОВ.

Аналіз основних існуючих способів несанкціонованого доступу в ВОЛЗ визначив необхідність розробки та впровадження методів протидії та захисту інформації від НД, що є актуальною науковою задачею.

Метою роботи є визначення можливостей використання апаратного та програмного захисту, а також доведення високої продуктивності комбінованих засобів захисту інформації у ВОЛЗ.

Основна частина

Методи захисту, або мінімізації можливостей здійснення несанкціонованих підключень, які дозволяють підвищити захищеність інформаційних потоків у ВОЛЗ можна поділити на три групи, а саме:

- спостереження за цілісністю кабелю та моніторинг рівня потужності оптичних сигналів;
- використання волокна з підвищеним коефіцієнтом гнучкості;
- шифрування на основі криптографічних методів.

Вказані методи запобігають основним способам несанкціонованого підключення до оптичного волокна. Розглянемо більш детально процес реалізації класифікованих методів захисту ВОЛЗ від НД.

Основним апаратним методом виявлення несанкціонованого доступу є метод контролю рівня потужності оптичних сигналів на вході оптичного приймача. При виявленні зменшення рівня потужності оптичних сигналів, що відповідає виникненню НД приймається рішення про перенаправлення інформаційних потоків на інші маршрути передавання [1]. При цьому, для забезпечення точності методу необхідно забезпечити постійний рівень потужності оптичних сигналів у ВОЛЗ за умови заданого типу кодування, який не залежить від виду інформаційних сигналів, що передаються [2]. 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 розсіяне в зворотному напрямку на різних неоднорідних ділянках ОВ, за інтенсивністю якого можна визначати розподілені втрати потужності оптичного сигналу в ОВ на

всій його довжині до 120 км. Порівняння еталонних рефлектограм, що виконані при різних параметрах зондуючого сигналу та записаних в пам'яті комп'ютера з відповідними поточними рефлектограмами може забезпечити контроль захищеності ВОЛЗ з точністю по локальному відхиленню рефлектограм не більше ніж на 0,1 дБ.

Ще один варіант захисту інформації у ВОЛЗ базується на використанні волокна із підвищеним коефіцієнтом гнучкості. Захист ОВ з низькими втратами і великим допустимим радіусом вигину, полягає у обмеженні високих втрат, що виникають під час згинання або проколювання волокна. Використання такого волокна також зменшує вплив витягування, перекручування та інші фізичних видів впливу на оптичне волокно [3].

Крім апаратних методів існують програмні методи захисту оптичних інформаційних потоків у ВОЛЗ. Розглянемо їх більш детально. В основі програмного методу захисту використовуються протоколи шифрування третього та другого рівнів. Протокол IPSec є шифруванням третього рівня, реалізація якого виконується на приймальній стороні (стороні користувача), що створює додаткові затримки в роботі телекомунікаційного обладнання. Використання другого рівня шифрування звільняє елементи третього рівня від функції шифрування. Одним із джерел шифрування другого рівня є технологія оптичного кодового мультиплексування CDMA [4-6]. При цьому шанс перехоплення інформації є функцією декількох параметрів, включаючи відношення сигнал-шум, дроблення (Fraction) доступної системної ємності. Також варто відмітити метод на основі використання режиму динамічного (детермінованого) хаосу, який дозволяє забезпечити передачу інформації з псевдовипадковою зміною частоти та амплітуди носійної. В результаті вихідний сигнал є шумоподібним, що в свою чергу ускладнює його розшифрування.

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 додатковим ОВ навколо робочого оптичного волокна. Для цього має бути зарезервовано додатковий ВОК, що підвищує вартість ВОЛЗ. Але це дає змогу вести моніторинг рівня потужності оптичного сигналу та при спробі зігнути даний ВОК відбудеться втрата потужності контрольного сигналу, що зумовить спрацювання сигналу тривоги [7].

Висновки

Перевагою комбінованих (апаратно-програмних) методів захисту є те, що їх 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 запропонованого алгоритму.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Спосіб контролю ліній зв'язку телекомунікаційної системи хмарного антивірусу О.А. Смірнов, А.К. Дідик, А.М. Дрєєв, С.А. Смірнов, Кіровоградський національний технічний університет, 2016 р – 7с.
2. All Optical Networks (AON), National Communication System, NCSTIB 00-7, August 2000
3. Draka Elite, Bend Bright-Elite Fiber for Patch Cord, Draka Communications, July 2010
4. W. Ford, «Computer Communications Security», Upper Saddle River, NJ: Prentice-Hall, 1994.
5. D. R. Stinson, «Cryptography», Boca Raton, FL: CRC, 1995.
6. N. Ferguson and 8. Schneier, «Practical Cryptography», Indianapolis, IN: Wiley, 2003.
7. «Optical Fiber Design for Secure Tap Proof transmission», US Patent No. 6801700 B2, Oct. 5, 2004.

Васильківський Микола Володимирович – канд. техн. наук, доцент кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університет, м. Вінниця, e-mail: mvasylkivskyi@gmail.com.

Паламарчук Роман — студент групи ТКП-15б, факультет інфокомунікацій, радіоелектроніки та наносистем, Вінницький національний технічний університет, Вінниця, e-mail: rporitskiy@gmail.com

Vasylkivskyi Mikola V. – Ph.D., Senior lecturer of the Chair of Telecommunication Systems and Television, Vinnytsia National Technical University, Vinnytsia, e-mail: mvasylkivskyi@gmail.com

Palamarchuk Roman P. — Department of Infocommunication, Electronics and Nanosystems, Vinnytsia National Technical University, Vinnytsia, e-mail: rporitskiy@gmail.com