

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ВОЛОКОННО-ОПТИЧНИХ СИСТЕМАХ ПЕРЕДАЧІ

Вінницький національний технічний університет

Анотація

Здійснено обґрунтований аналіз способів несанкціонованого доступу в лінійний тракт сучасних телекомунікаційних мереж на базі волоконно-оптичних ліній передачі. Запропоновано метод контролю потужності оптичного сигналу та коефіцієнту помилок у ВОЛТ, який базується на порівнянні коефіцієнту помилок BER в оптичному каналі.

Ключові слова: волоконно-оптична лінія зв'язку, несанкціонований доступ, коефіцієнт помилок.

Abstract

A substantiated analysis of methods of unauthorized access to the line link of modern telecommunication networks based on fiber-optic communication lines is carried out. The method of control the power of the optical signal and the error coefficient in fiber-optic communications line is proposed, which is based on comparison of the bit error rate in the optical channel.

Keywords: fiber-optic communication line, unauthorized access, bit error rate.

Вступ

Аналіз основних існуючих способів несанкціонованого доступу в ВОЛЗ визначив необхідність розробки та впровадження методів протидії та захисту інформації від НД [1, 2]. Методи захисту, або мінімізації можливостей здійснення несанкціонованих підключень до ВОЛЗ можна поділити на три групи, а саме: моніторинг рівня потужності оптичних сигналів; використання волокна з підвищеним коефіцієнтом гнучкості; шифрування на основі криптографічних методів. Вказані методи запобігають основним способам несанкціонованого доступу (НД) до оптичного волокна (ОВ), але характеризуються низькою точністю встановлення місця НД у ВОЛЗ, тому 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 НД до оптичних каналів.

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

Модифікований метод підвищення інформаційної захищеності ВОЛЗ

Для підвищення ефективності захисту ВОЛЗ від НД пропонується здійснювати порівняльний контроль рівнів потужності оптичних сигналів на виході оптичних мультиплексорів та демультиплексорів у ВОЛТ та коефіцієнту помилок на виході оптичних приймачів ВОСП. 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 двоканалний BER-тестер, який одночасно визначає значення коефіцієнта помилок для двох оптичних каналів: робочого (опорного) та контрольованого [3]. 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). Для мереж, які поступово розширюються,

чи мають перспективу на розширення, застосування такого методу є не доцільним, тому для таких мереж для адаптивного налаштування блоку порівняння результатів необхідно додати в структуру ПКЗ ще один ОП 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.

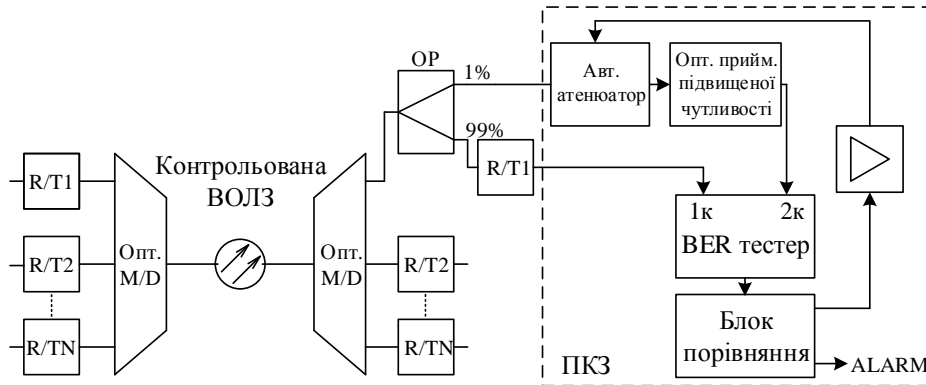


Рисунок 1 - Узагальнена структура пристрою контролю захищеності ВОЛЗ

Реалізація програмного забезпечення апаратно-програмного засобу контролю інформаційної захищеності ВОЛЗ

Програмне забезпечення у складі обладнання, яке розміщено на приймальній стороні, дозволить 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. Це відбувається за рахунок виконання програмою алгоритму [4]. Відповідно до алгоритму відбувається постійне вимірювання рівня потужності оптичних сигналів (ПОС), та порівняння його із пороговим значенням (допуском), яке в свою чергу формується протягом певного часу роботи системи, при якому несанкціоноване підключення (НП) точно відсутнє. Або його формування забезпечується за рахунок задання певного відсотку від ПОС. В ході роботи системи за наявності НД передача інформації припиняється, та на робочу станцію і до системи надсилається повідомлення про його наявність. Після чого за допомогою рефлектометра встановлюється місце НП, та відбуваються подальші дії по виявленню та виправленню причин НД/НП. На рис. 2 зображено частину коду, який виконує вимірювання ПОС у циклічному режимі, програми контролю ПОС у ВОЛЗ та приймає рішення про наявність НД/НП.

```

1  [ ] while(true){
2
3
4
5  [ ]     n_diff = diff_W - delta;
6
7         if(n_diff < (diff_W - percent)){
8
9             cout<<"Unauthorized access detected\n";
10
11         }
12     else{
13         cout<<"System work\n";
14     }
15
16 }

```

Рисунок 2 – Блок прийняття рішення про наявність НД/НП

Відповідно до рис. 2: 1 – 16 стрічки – тіло циклу, в якому відбувається постійне вимірювання ПОС; 3 стрічка – розрахунок потужності сигналу із врахуванням НД (в реальному пристрої розрахунок не відбувається, значення ПОС із НД отримується напряму із приймача); 5 – 14 стрічки – тіло умови, яка порівнює значення ПОС: при істинній умові, тобто, коли нове значення потужності ОС менше за порогове (у випадку симуляції) на екран виводиться повідомлення про наявність НД (стрічка 7) (в реальному пристрої додатково надходить повідомлення про нове значення ПОС. Усі повідомлення надходять до системи та робочих станцій); При хибній умові, тобто при дотриманні допустимого відхилення на екран виводиться повідомлення про нормальне функціонування системи, стрічка 12 (в реальному пристрої, при нормальному функціонуванні системи передачі ніяких повідомлень до системи не надходить).

Висновки

Запропоновано узагальнену структуру пристрою контролю захищеності ВОЛЗ, яка представлена на рис. 1. Даний метод та наведений варіант його реалізації мінімізує можливість здійснення несанкціонованих підключень до мережі та дозволить виявляти спроби реалізації пасивних атак, відомих як «sniffing», на мережі доступу. 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 запропонованого алгоритму.

Наведено алгоритм реалізації програмного забезпечення для пристрою контролю захищеності ВОЛЗ, на основі блок схеми [4]. Наведено частину програмного коду, зображеного на рис. 2, який виконує циклічне вимірювання ПОС та перевірку умови присутності або відсутності НД/НП.

Тому 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.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Васильківський М.В., Паламарчук Р.П. Методи захисту волоконно-оптичних ліній зв'язку: тези XLVII Науково-технічної конференції факультету інфокомунікацій, радіоелектроніки та наносистем (м. Вінниця, 21.03.2018 – 23.03.2018) Вінниця, 2018.
2. М.В. Васильківський, Р.П. Паламарчук Захист інформації у волоконно-оптичних системах зв'язку / Вісник Хмельницького національного університету. Технічні науки №3 2018р. с. 202-207.
3. М.В. Васильківський, Р.П. Паламарчук Оцінювання енергетичних характеристик волоконно-оптичних ліній зв'язку за критерієм коефіцієнта помилок / Вісник Хмельницького національного університету. Технічні науки №1 2019р. с. 216-220.
4. Васильківський М.В. Захист інформації у волоконно-оптичних лініях зв'язку/ М.В. Васильківський, Р.П. Паламарчук // Вимірювальна та обчислювальна техніка в технологічних процесах (ВОТТП_18_2018) XVIII міжнародної науково-технічної конференції, 8-13 червня 2018 р. – Матеріали – Одеса. – 2018 с. 209.

Паламарчук Роман Петрович — студент групи ТКП-156, факультет інфокомунікацій, радіоелектроніки та наносистем, Вінницький національний технічний університет, Вінниця.

Науковий керівник: **Васильківський Микола Володимирович** – канд. техн. наук, доцент кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університет, Вінниця.

Palamarchuk Roman P. — Department of Infocommunication, Electronics and Nanosystems, Vinnytsia National Technical University, Vinnytsia.

Supervisor: **Vasykivskyi Mikola V.** – Ph.D., Senior lecturer of the Chair of Telecommunication Systems and Television, Vinnytsia National Technical University, Vinnytsia.