

## ЗАГРОЗИ ВИТОКУ АКУСТИЧНОЇ ІНФОРМАЦІЇ ЧЕРЕЗ ЛІНІЇ ВОЛОКОННО-ОПТИЧНОГО ЗВ'ЯЗКУ

Вінницький національний технічний університет

### Анотація

У даній роботі розглядаються можливості витоку акустичної інформації через лінії волоконно-оптичного зв'язку. Загрозу витоку інформації може створювати модуляція звуковими частотами оптичних сигналів шляхом впливу акустичних хвиль на оптичне волокно або на обладнання, що використовується в даних системах зв'язку. Проаналізовано особливості реалізації даного каналу витоку інформації та методи захисту від нього, зокрема, звукоізоляція, фільтрація та шумлення. Також, розглянуто технічні можливості протидії загрозам, шляхом моніторингу оптичного випромінювання в лініях для виявлення факту несанкціонованого підключення.

**Ключові слова:** витік, інформація, лінії, загрози, виявлення, зв'язок, волоконно-оптичний зв'язок, фільтрація, шумлення.

### Abstract

*This paper considers the possibilities of leakage of acoustic information through fiber-optic communication lines. The threat of information leakage can be created by audio frequency modulation of optical signals by impact of acoustic waves on the optical fiber or on the equipment used in these communication systems. The peculiarities of the implementation of this channel of information leakage and methods of protection against it are analyzed, in particular, sound insulation, filtering and noise reduction. Also, the technical possibilities of countering threats, by monitoring optical radiation in lines to detect the fact of unauthorized connection, were considered.*

**Keywords:** leak, information, lines, threats, detection, communication, fiber optic, filtering, noise.

### Вступ

Сучасні технології глобальних і локальних систем зв'язку нерозривно пов'язані з оптичними системами передачі даних, в першу чергу це обумовлено чисельними перевагами волоконно-оптичного кабелю в порівнянні зі звичайним коаксіальним електричним кабелем, зокрема, більша пропускна спроможність, стійкість до радіозавад, менші втрати при поширенні сигналу на великі відстані і т.д. Таким чином, все більше пристроїв, що використовуються у повсякденному житті, мають оптоволоконне підключення: інтернет модеми, локальні мережі, IP телефонія, тим самим, все більше і більше оптоволоконні лінії замінюють собою звичайні провідні технології в найближчому оточенні користувача в офісах, кабінетах, конференц-залах тощо. Таке поширення оптичних систем створює нові загрози для інформаційної безпеки, один з ризиків, що вони несуть, пов'язаний з можливістю перехоплення перетвореної мовної інформації, за рахунок використання впливу акустичних полів на передачу світла через волоконно-оптичну лінію.

### Результати дослідження

Несанкціоноване отримання акустичної (мовної) інформації з допомогою волоконно-оптичних комунікацій є одним з нових методів акустичної розвідки, який називається акустооптичним каналом витоку інформації, який по своїй суті є аналогічним до акустоелектричного каналу, з тією лише відмінністю, що в даному випадку вплив акустичного поля викликає зміни не в електричних, а в оптичних сигналах. Формування даного каналу витоку пов'язане з тим, що акустичне поле, яке містить інформацію впливає на волокна кабельних систем, що знаходяться у приміщенні і тим самим викликає модуляцію світла, яке проходить через дану лінію або елементи оптичного устаткування [1]. Модуляція відбувається звуковими частотами і може реалізовуватись за амплітудою, фазою, частотою і поляризацією випромінювання в результаті впливу мовного сигналу.

Далі, промодульоване світло може поширюватись лініями далеко за межі приміщення та контрольованої зони, де немає можливості запобігти фізичному доступу до даних комунікацій стороннім особам. У випадку, якщо зловмисник, зможе непомітно підключитись до волоконнооптичної лінії, в нього з'явиться можливість отримати доступ до мовної інформації, яка циркулює в середині приміщення за допомогою демодуляції оптичного сигналу. Спрощена модель утворення даного каналу витоку інформації наведено на рисунку 1.

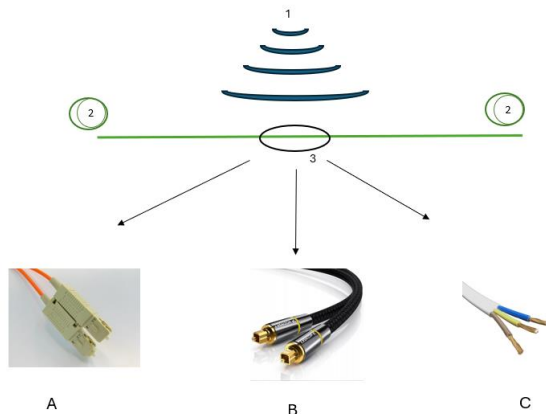


Рисунок 1. Спрощена модель акустооптичних каналів витоку інформації.

1- джерело звуку, 2 - оптичний кабель, 3 - елемент оптичної кабельної системи, що підлягає впливу звуку в тому числі оптичний роз'єм (А), оптичний кабель (В), кабель, що проходить в конструкціях будівлі (С).

Як зазначалось вище, акустооптичний канал багато в чому подібний до акустоелектричного каналу витоку інформації, зокрема, схожість спостерігається і у процесі виділення інформації із перехоплених сигналів. При перехопленні акустоелектричних сигналів у лініях зв'язку зловмисник може скористатись «штатними» сигналами, які з'являються у лінії при нормальному функціонуванні пристроїв, що до неї підключені, але які під впливом акустичного поля модулюються і починають містити мовний інформаційний сигнал. А також, у випадку, коли «штатні» сигнали мають малий рівень або ступінь модуляції у них досить низький і їх перехоплення у лінії є складним то зловмисник може скористатись спеціальним зондуючим ВЧ сигналом, який з допомогою генератора подається у лінію (ВЧ-навізування), після чого вже він потрапляє на пристрої у середині приміщення де модулюється і через неузгодженість опорів відбивається у зворотному напрямку [2]. Відповідно, і у випадку волоконно-оптичних ліній всі світлові сигнали, що може використати зловмисник можна поділити на штатні, тобто ті які пов'язані з технічною реалізацією протоколу передачі даних, і штучні - спеціально сформовані зловмисником для несанкціонованого перехоплення мовної інформації, по аналогії з ВЧ навізуванням.

Таким чином, головною умовою для формування даного каналу витоку є фізичне підключення до оптичного кабелю, при чому підключення повинно відбуватись на ділянці лінії де відсутні активні засоби підсилення та передачі оптичних сигналів, це пов'язано з тим що у даному обладнанні відновлюється нормальна форма сигналу і придушуються шуми накладені на випромінювання. Відповідно між зловмисником і джерелом акустичної інформації повинні бути розміщені тільки пасивні оптичні елементи, які значно не змінюють модуляцію світла, до таких елементів, окрім оптичного кабелю, відносяться ще роз'єми, адаптери, розгалужувачі, з'єднувачі та подовжувачі. Для технічної реалізації каналу витоку потрібне застосування технічних засобів для підключення до кабелю і запису оптичного випромінювання, підключення здійснюється за допомогою звичайних контактів, які використовуються для підключення частин мережі між собою або для приєднання до оптичних мережевих терміналів [3]. Також, можливе підключення у розрив кабелю з подальшою вставкою перехідника на місці зварювання волокон кабелю.

Враховуючи, сказане вище, загрози, що створюють даний канал витоку інформації є більш ніж реальними і потребують вирішення з точки зору технічного захисту інформації, а подальше поширення волоконно-оптичних систем зв'язку буде тільки актуалізувати дану проблему. Тому, необхідним є визначення доступних методів захисту від даного каналу. Його спорідненість з

акустоелектричним каналом, де що спрощує дану задачу, оскільки методи та засоби захисту будуть ефективними одразу для обох випадків. Таким чином всі основні способи протидії витoku мовної інформації через волоконнооптичні лінії зв'язку можна розділити на:

- звукоізоляція оптичної лінії, пасивний метод для зменшення впливу акустичного поля на навколишнє середовище каналу;
- фільтрація носія даних в каналі передачі, метод полягає в тому, що через оптичну лінію не проходять штучні (зондуючі) і промодульовані мовною інформацією сигнали;
- маскування носія даних в каналі передачі, метод полягає у приховуванні сигналу додаванням спеціальної маски і модуляцій;
- зашумлення середовища каналу, активний метод, що полягає в створенні штучної завади і шуму на акустичних частотах.

Кожен метод має свої переваги і недоліки, але в цілому ефективність будь-якого засобу захисту багато в чому залежить і від технічних можливостей виявлення загроз для інформації. Технічні засоби для виявлення факту підключення до лінії або застосування обладнання для реалізації підключення, безсумнівно, підвищить надійність системи захисту. У випадку волоконно-оптичних комунікацій слід враховувати фізичні характеристики каналу волоконно-оптичного зв'язку, такі як напрямок випромінювання та відсутність побічних світлових пучків. Відповідно, аналіз та моніторинг оптичної лінії на наявність аномальних параметрів чи сигналів дозволить виявляти факт підключення та «прослуховування» і реагувати на це.

### Висновки

Підсумовуючи сказане, стає зрозумілим, що оптичні системи зв'язку, які надають значні переваги у порівнянні з електричними аналогами, це невід'ємна частина сучасної діяльності людини, і у перспективі їх роль буде тільки зростати. А це в свою чергу буде створювати нові виклики у сфері інформаційної безпеки. Тому важливим є розуміння суті загроз для інформації, що вони створюють та шляхів їх усунення. Розглянутий новий метод акустичної розвідки - акустооптичний канал витoku інформації, який може використовуватися для отримання конфіденційних розмов через волоконно-оптичні комунікації, повинен обов'язково враховуватись при проектуванні систем захисту інформації на об'єктах інформаційної діяльності із застосуванням відповідних методів захисту, які були проаналізовані в даній роботі.

### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. V. V. Grishachev, D. B. Khalyapin and N. A. Shevchenko, "Methods and Devices for Actively Protecting Spoken Information against Eavesdropping via an Acousto-Optic Fibre Leakage Channel," 2010. – URL: <http://www.wipo.int/patentscope/search/en/WO2010126401>
2. Методи та засоби технічного захисту інформації. [Електронний ресурс] : навч. посіб. для здобувачів ступеня бакалавра за освітньою програмою «Системи технічного захисту інформації» спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: В. М. Луценко, Д. О. Прогонов., 2021 – URL: <https://ela.kpi.ua/handle/123456789/42397>
3. R. Hui and M. S. O'Sullivan, "Fiber Optic Measurement Techniques," Elsevier Academic Press, Waltham, 2009.

**Москаленко Аліна Євгенівна**- студентка групи 1БКС-22б, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: [moskalenkoalina56@gmail.com](mailto:moskalenkoalina56@gmail.com)

**Moskalenko Alina Evgeniivna**- student of group 1BKS-22b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: [moskalenkoalina56@gmail.com](mailto:moskalenkoalina56@gmail.com)

**Катаєв Віталій Сергійович** – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, [kataev@vntu.net](mailto:kataev@vntu.net).

**Vitalii Kataiev** – assistant of the Department of Management and Security of Information Systems; Vinnytsia National Technical University, Vinnytsia, [kataev@vntu.net](mailto:kataev@vntu.net).