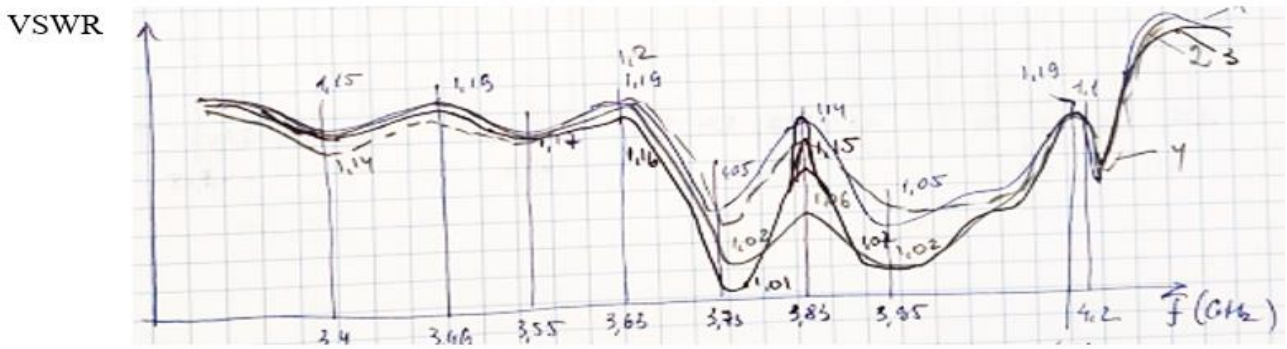


Рисунок 5. КСХН (VSWR) смуго- пропускних фільтрів.

**Література**

1. Безбородов Ю. М. Фільтри НВЧ на діелектричних резонаторах / Ю. М. Безбородов, Т. Н. Нариткін, В. Б. Федоров. – Київ. Техніка, 1989.

2. В. В. Козловський. Синтез пристроїв НВЧ на неоднорідних лініях. В. І. Сошніков, В. А. Бичковський, – Київ. Техніка, 1991.

3. Місюра А.О. Електромагнітне поле хвилеводів з фрактальними властивостями перерізів: автореф. дис. на наук. ступінь к.ф.-м.н. Харків. нац. ун-т радіоелектроніки 2006.

**4.** Чухов В. В. Радіочастотні методи та засоби вимірювань параметрів хвилеводів із діелектричним заповненням: автореф. дис. на наук. ступінь к.т.н. Вінниц. нац. техн. ун-т. 2007.

УДК 004.056.5:004.8

**О.В. Цвірла, І. В. Мудрий, Н. С. Луцик, доктор філософії, доц.**
Тернопільський національний технічний університет імені Івана Пулюя, Україна

## ІНТЕЛЕКТУАЛЬНИЙ ПІДХІД ДО ВИЯВЛЕННЯ ВРАЗЛИВИХ ХЕШ-СТРІЧОК У КОМП'ЮТЕРИЗОВАНИХ СИСТЕМАХ

**O.V. Tsvirla, I. V. Mudryi, N. S. Lutsyk, Ph.D., Assoc. Prof.**

## INTELLIGENT APPROACH TO DETECTING VULNERABLE HASH STRINGS IN COMPUTERIZED SYSTEMS

Стрімке зростання обсягів цифрових даних та ускладнення інформаційних інфраструктур посилюють вимоги до механізмів забезпечення криптографічної стійкості. Одним із критичних елементів таких систем є хеш-функції, що застосовуються для автентифікації, контролю цілісності та зберігання конфіденційних записів. Проте у практиці експлуатації інформаційних систем нерідко виявляються хеші, сформовані застарілими або надійно непараметризованими алгоритмами, що створює реальні передумови для компрометації даних через перебір, колізії або атаки на слабкі криптографічні конструкції [1].

Традиційні засоби аудиту хешів орієнтовані переважно на сигнатурне розпізнавання типу алгоритму або на застосування brute-force методів. Подібні рішення не дозволяють оцінити структурну і статистичну уразливість конкретного хеш-значення без виконання реальної атаки, що значно знижує їх ефективність у масштабних системах. У сучасних умовах виникає потреба у методах, здатних проактивно визначати рівень небезпеки хеш-стрічок на основі їх внутрішніх властивостей [2-4].

Перспективним напрямком є інтелектуальний підхід, заснований на машинному навчанні та векторному описі хеш-даних. У межах такого підходу хеш-рядок розглядається як об’єкт із низкою параметрів: довжиною, алфавітною структурою, ентропією, наявністю сольового компоненту, сигнатурними характеристиками алгоритму та поведінковими патернами. На основі цих ознак формується багатовимірний простір, у якому класифікаційна модель визначає рівень криптографічного ризику без необхідності здійснення перебору або криптографічного зламу.

Підвищення ефективності аналізу хеш-даних можливе за умови поєднання інтелектуальних методів із комплексним урахуванням контексту їх використання. Це включає аналіз частоти появи певних типів хешів у корпоративних системах, оцінку відповідності політикам автентифікації, виявлення системних аномалій у структурі даних та зіставлення їх з чинними стандартами криптографічного захисту. Такий підхід дозволяє оцінювати не лише стійкість конкретного значення, а й прогнозувати потенційні маршрути атак, зумовлені слабкими ланками інфраструктури або помилками адміністрування.

Подальший розвиток інтелектуального аналізу хеш-функцій пов’язаний із впровадженням адаптивних моделей, здатних оновлювати правила класифікації відповідно до появи нових алгоритмів, технік обходу криптографічних бар’єрів та шаблонів атак. Важливим напрямом є також інтеграція таких систем із платформами моніторингу подій безпеки (SIEM), що забезпечує оперативне виявлення відхилень та підвищує рівень кіберстійкості. Застосування інтелектуальних технологій у поєднанні зі структурним криптоаналізом формує підґрунтя для створення проактивних інструментів захисту, які здатні запобігати інцидентам ще на етапі їх формування.

**Література**

1. Stallings W. 2023. Cryptography and Network Security: Principles and Practice. Pearson. P. 145–200.

2. Aghaei A., Homayoun H., Sasan A. 2020. Hash Function Security Evaluation via Machine Learning-Based Structural Analysis. ACM. P. 1–10.

3. Hindy H., Brosset D., Bayne E. et al. 2020. A Taxonomy and Survey of Intrusion Detection Systems Using Machine Learning. ACM Computing Surveys. P. 1–41.

4. Zhang Y., Wang L., Sun Q. 2021. A Survey on Deep Learning-Based Hashing Methods. IEEE Transactions on Knowledge and Data Engineering. P. 1–20.

УДК 004.056: 004.738.5

**І. М. Чепіль, В.Д. Тимощук**
(Тернопільський національний технічний університет імені Івана Пулюя)

## МОДЕЛЬ НАДАННЯ МЕРЕЖЕВИХ СЕРВІСІВ У SDN З ПІДТРИМКОЮ BRING YOUR OWN CONTROL

**I. Chepil, V. Tymoshchuk**

## A NETWORK SERVICE PROVISIONING MODEL IN SDN WITH BRING YOUR OWN CONTROL

Програмно-визначені мережі (SDN) дедалі частіше стикаються з обмеженнями традиційної моделі централізованого керування, яка ускладнює швидку адаптацію мережевих сервісів безпеки до динамічних загроз та індивідуальних потреб