УДК 004.056 DOI: 10.31673/2412-4338.2019.015561

Лаптєв О.А., Барабаш О.В., Зозуля С.А.
Державний університет телекомунікацій, Київ

ВЕКТОРНІ АНАЛІЗАТОРИ СИГНАЛІВ ДЛЯ УДОСКОНАЛЕННЯ МЕТОДИКИ ПОШУКУ ЗАСОБІВ НЕГЛАСНОГО ОТРИМАННЯ ІНФОРМАЦІЇ

У статті коротко розглянуті тенденції розвитку засобів негласного отримання інформації. Основні з них застосування все більш заплутаних алгоритмів приховування випромінювання цифрових радіозакладок, застосовуються спеціальні методи маскування, може створюватися канал знімання інформації під прикриттям випромінювання що працює поблизу об'єкта легальних радіозасобів, що заважають роботі пошукової техніки. Наступним важливим фактором є продовження застосування частот радіоефіру для організації зв'язку, передачі даних, різних команд управління. Практично весь радіочастотний діапазон залучений під роботу легальних радіопередавачів. Це викликає істотне ускладнення радіо ефірної обстановки, виявити цифрові радіозакладки в таких умовах вкрай важко. Зробити це без застосування спеціальних засобів аналізу цифрових пакетів в реальному маштабі часу, неможливо. В якості спеціального вимірювального пристрою, з метою поліпшення методики виявлення цифрових радіозакладок запропонований векторний аналізатор. Вибір обґрунтовується на основі детального аналізу технічних характеристик і принципів роботи аналізатора. Відзначено, що в частотної області для дослідження радіосигналу, вимірювання його рівня та опорних частот використовуються два типи аналізаторів спектра: послідовні та паралельні аналізатори спектра. Важливою перевагою паралельного аналізу в порівнянні з послідовним – є відносне підвищення швидкості побудови спектра, яке стає особливо значним при малих смугах аналізу. Звернено увагу на те, що аналіз спектра – це важлива, але далеко не єдина процедура, яка використовується при виявленні та дослідженні сигналів в системах радіомоніторингу. Дуже важливий зараз аналіз зміни параметрів радіосигналу в часі. Саме ця можливість роботи векторного аналізатора і закладена в удосконаленні методики пошуку цифрових радіозакладок, що працюють в імпульсному режимі.

Для кожної обраної на спектрограмі смуги частот векторний аналізатор може одночасно показувати її спектр, тимчасову або векторну діаграму. Це дозволяє знайти моменти появи та закінчення передачі імпульсного короткочасного сигналу, визначити за спектром інтервали передачі, розпізнати вид модуляції та на основі отриманих даних виконати аналіз і визначити з високою ймовірністю походження радіосигналу – визначити радіозакладку. Показано, що векторний аналізатор являє собою потужний інструмент дослідження і вимірювання характеристик радіосигналів у всьому використовуваному діапазоні частот від декількох кГц до десятків і сотень ГГц. Застосування векторних аналізаторів дозволяє, зокрема, розв'язувати серйозні проблеми виявлення сигналів сучасних цифрових засобів негласного знімання інформації, що використовують тимчасове і кодове розділення каналів, випадкову перебудову частоти, багатопозиційну аплітудно-фазову модуляцію та інші перспективні методи передачі інформації.

Ключові слова: векторні аналізатори, аналіз цифрових пакетів, спектр, параметри радіосигналу в часі, інтервали передачі.

Laptev O.A., Barabash O.V., Zozulia S.A.
State University of Telecommunications, Kyiv

VECTOR ANALYZERS OF SIGNALS FOR IMPROVING METHODS OF SEARCH OF MEANS OF OUTPUT RECEIVING OF INFORMATION

The article briefly discusses the development trends of the means of secretly collecting information. The main of them are the use of more and more entangled algorithms for hiding the radiation of digital radio bookmarks, special masking methods are used, a channel can be created for retrieving information under the cover of radiation of legal radio tools working near the object that interfere with the search technology. The next important factor is the continuation of the use of radio frequencies for communication, data transmission, and various control commands. Almost the entire radio frequency range is involved in the work of legal radio transmitters. This causes significant complications of the radio broadcasting environment, to identify digital radio tabs in such conditions is extremely difficult. To do this without the use of special tools for analyzing digital packets in real time is impossible. A vector analyzer has been proposed as a special measuring tool in order to improve the technique of detecting digital radio bookmarks. The choice is based on a detailed analysis of the technical characteristics and principles of the analyzer. It is noted that in the frequency domain for the study of the radio signal, measuring its level and carrier frequencies, two types of spectrum analyzers are used: serial and parallel spectrum analyzers.

An important advantage of parallel analysis as compared to sequential is a relative increase in the speed of spectrum construction, which becomes especially significant with small analysis bands. Attention is drawn to the fact that spectrum analysis is an important, but not the only procedure that is used to identify and study signals in radio monitoring systems. It is very important now to analyze changes in the parameters of a radio signal over time. It is this ability to work vector analyzer and laid in the improvement of the search method of digital radio tabs operating in pulsed mode.

For each frequency band selected on the spectrogram, the vector analyzer can simultaneously display its spectrum, time or vector diagram. This allows you to find the moments of the appearance and end of the transmission of a pulsed short-term signal, determine the transmission intervals from the spectrum, recognize the type of modulation and, based on the data received, perform an analysis and determine the radio signal origin with a high probability. It is shown that the vector analyzer is a powerful tool for studying and measuring the characteristics of radio signals in the entire frequency range used from a few kHz to tens and hundreds of GHz. The use of vector analyzers allows, in particular, to solve the serious problems of detecting signals from modern digital means of secretly picking up information using time and code division channels, pseudo-random frequency tuning, multipositional-phase-amplitude modulation and other promising methods of information transfer.

Keywords: vector analyzers, digital packet analysis, spectrum, radio signal parameters in time, transmission intervals.

Вступ. У сучасному світі з підвищенням значущості та цінності інформації істотно зростає важливість її цілісності та захисту. Інформація – це засіб управління. Несанкціоноване втручання в управління може привести до катастрофічних наслідків на об'єкті управління – в першу чергу на транспорті та військовій справі. Тому питання збереження цілісності інформації сьогодні стають актуальними як ніколи раніше. Для ефективного вирішення завдань захисту інформації необхідний якісний аналіз радіоефіру і

виявлення можливих каналів витоку інформації. Якісний аналіз радіоефіру, з одного боку, обумовлений можливостями вимірювальної контрольної апаратури, з іншого – можливістю ефективно цю інформацію обробити. Стосовно апаратури контролю радіоефіру, ефективність одержуваної інформації визначається, перш за все, її якістю. Виходячи з цього, питання отримання якісного аналізу радіоефіру за допомогою сучасної апаратури стоїть як ніколи актуально.

Питанням пошуку і виявлення до радіоканалів цифрових радіозакладок присвячено значну кількість публікацій. Так, у [1] розглядаються питання пошуку і локалізації радіо закладок «класичним» методом за допомогою універсальних приладів, індикаторів поля та іншої допоміжної апаратури. Ця методика задовольняла потреби пошуку засобів негласного отримання інформації (ЗНОІ) раніше. Приладами, наведеними в цій методиці, виявити та локалізувати ЗНОІ, які працюють в цифровому діапазоні дуже і дуже важко. Тому потрібно вдосконалювати як методику пошуку, так і розглядати використання більш чутливої вимірювальної пошукової апаратури. У [2] розглянуті тенденції розвитку радіозакладок, технічні розробки стають все більш досконалими, канали передачі даних працюють на набагато вищих частотах, ніж раніше. Умови передачі та приймання на високих частотах радіохвиль вже не виглядають настільки великою перешкодою. Радіорелейні станції, наприклад, використовують діапазон, близький до сотні гігагерц, а в діапазоні 6 ГГц організований широкосмуговий доступ з гігагерцевим трафіком. Виходячи з цього, пошукові засоби, що працюють в діапазоні до 3 ГГц, вже не задовольняють сучасним вимогам і потребують удосконалення або заміни на більш сучасні, що працюють з іншими частотними параметрами. У [3] аналізується складність сучасного радіомоніторингу в інтересах забезпечення захисту інформації.

Проблема полягає в тому, що сучасні цифрові закладні пристрої з передачею інформації радіоканалом все частіше використовують для передачі інформації ті ж стандарти, що і пристрої, які легально перебувають на об’єктах. Тому колишні «класичні» методи радіомоніторингу не в змозі визначити закладні пристрої, що працюють під прикриттям легальних засобів. Це підштовхує до розробки нових вимірювальних пристроїв і методик для пошуку ЗНОІ, які працюють в легальних частотних діапазонах. Перераховані вище фактори дозволяють зробити висновок, що на сучасному етапі розвитку суспільства процес пошуку ЗНОІ виходять якісно на інший рівень. Тому методи пошуку та обладнання, які використовуються для цього, вимагають серйозного вдосконалення, а проблема високоякісного аналізу радіоефіру за допомогою різних вимірювальних приладів стоїть як ніколи актуальною.

Виклад основного матеріалу. На сучасному етапі розвитку технічних засобів пошук цифрових радіо закладок ускладнюється декількома факторами. Основним з них є те, що розробники цифрових ЗНОІ застосовують все більш заплутані алгоритми «камуфлювання» випромінювання цифрових радіозакладок. Наступним важливим фактором є те, що зараз практично весь радіочастотний діапазон залучений під роботу легальних радіопередавачів. Це викликає істотне ускладнення радіо ефірної обстановки. Можна зробити припущення, що розробники сучасних ЗНОІ з передачею інформації радіоканалом переходять на цифрові стандарти дуже близьких до легальних або в легальному діапазоні радіоефіру. Вимоги до сучасних та перспективних вимірювальних пристроїв автоматизованих комплексів пошуку цифрових радіо закладок випливають з аналізу можливостей сучасних цифрових засобів передачі даних. Розглянемо деякі з них, спираючись безпосередньо на аналізі методів приховування роботи цифрових радіозакладок та способів приховування самих каналів

передачі даних. Сучасні цифрові радіозакладки використовують такі методи приховування своєї роботи і роботи каналів передачі перехоплених даних:

- найпоширеніший метод – накопичення отриманої інформації з дискретною передачею її за короткі проміжки часу, причому, час передачі інформації може бути заздалегідь запрограмований, або передача здійснюється по команді із зовні;
- наступний метод – це спосіб періодичної або хаотичної перебудови частоти каналу радіопередачі;
- використання широкосмугових сигналів, метод, коли спектр сигналу розподілений в широкій смузі частот і сигнал не має яскраво вираженого піку перевищення над шумами;
- складним для визначення – це метод вибору частоти передавача поруч з потужними джерелами легальних сигналів, які перевантажують приймальні тракти пошукової апаратури при недостатньому динамічному діапазоні;
- маскують цифрові радіозакладки під стандартні канали зв'язку, маючи у своєму розпорядженні частоту радіозакладки в безпосередній близькості від легального джерела або ж використовуючи вузькосмугове випромінювання всередині спектра легальних широкосмугових сигналів [4].

Використовувані методи та способи можуть успішно комбінуватися один з одним. Цифрові радіозакладки, що використовують методи накопичення інформації з наступною її передачею в короткий проміжок часу надійно можна ідентифікувати тільки за двома демаскуючими ознаками, перша ознака – побічне електромагнітне випромінювання (дуже складно виявити через дуже низький сигнал) і друга ознака – визначення перевищення амплітуди на певній частоті з коротким проміжком часу роботи цифрової радіозакладки.

Додатково хотілося відзначити, що які б складні алгоритми, методи та способи приховування каналу передачі даних не застосовувалися в цифрових радіозакладках, вони все одно себе демаскують, виходячи з певної закономірності, наприклад, періодичністю виходу в радіоефір. Ці характерні ознаки радіозакладок визначаються в основному, оператором пошукового комплексу при виконанні тимчасового аналізу радіочастотного спектра. Але, для виконання цього аналізу необхідна вимірювальна апаратура, яка дозволяє це зробити. Найсучасніша на сьогодні вимірювальна апаратура – це векторні аналізатори сигналів, які створювалися для досліджень радіосигналів складної форми. Вони успішно вирішують завдання дослідження двокомпонентного векторного процесу, що показує зміни в часі амплітуди та фази вихідного сигналу. Для вимірювання всієї сукупності параметрів для системи радіомоніторінгу раніше доводилося використовувати кілька спеціалізованих приладів: аналізатори спектру, приймачі що сканують радіодіапазон та аналізатори модуляції. Зараз на зміну прийшов векторний аналізатор.

Принципово векторні аналізатори діляться на два типи: послідовні і паралельні аналізатори спектра. Послідовний формує спектральну картину послідовно. Паралельний аналізатор оцінює весь спектр відразу, оскільки містить групу налаштованих на суміжні частоти смугових фільтрів. Основою роботи є перетворення аналогового сигналу в цифровий, який обчислюється за допомогою алгоритмів швидкого перетворення Фур'є (далі ШПФ). Для подання будь-якого радіосигналу в цифровому вигляді досить знати його опорну частоту та комплексну складову сигналу. З огляду на те, що цифрові радіозакладки працюють в широкому діапазоні, на вході векторного аналізатора включається перетворювач, що понижує або підвищує частоти, який переносить спектр вхідного сигналу на фіксовану проміжну частоту. Далі квадратурний демодулятор працює на проміжній частоті та виділяє справжню (I) і уявну (Q) частини комплексної огинаючої сигналу в смузі частот, яка

називається смугою паралельної обробки. Після аналого-цифрового перетворення цифрові реалізації I та Q реєструються в пам'яті обчислювального обладнання. Маючи у своєму розпорядженні I/Q - реалізації, процесор обчислює спектр вхідного сигналу, а також функції, які описують поведінку в часі амплітуди, частоти та фази сигналу [5].

Особливу увагу треба звернути на характерні фактори роботи векторних аналізаторів, які відрізняють їх від всіх вимірювальних приладів, які передають виміряний і перетворений сигнал в АПК для його аналізу:

- векторний аналізатор обробляє комплексні огинаючі, що представляють амплітуду і фазу радіосигналу, що дозволяє досліджувати амплітудні та фазові спектри, і показує їх у вигляді спектральних, тимчасових або векторних діаграм;
- завдяки програмно-цифровій обробці сигналу, векторний аналізатор виконує паралельний аналіз спектра в реальному часі.

Цифрова реєстрація і зберігання в пам'яті наступних один за одним цифрових перетворень радіосигналу дає можливість виявити імпульсні одноразові радіосигнали. Залежно від смуги паралельного аналізу векторні аналізатори виконують вимірювання потужності спектральних компонент з динамічним діапазоном від 60 до 90 дБ. Фахівці компанії Tektronix (США) називають подібні прилади аналізаторами спектра у реальному часі (RTSA - Real Time Spectrum Analyzer). Паралельний аналіз виконується в смузі до 5 МГц з частотним діапазоном до 5 кГц. Вимірювання рівнів від -50 до +30дБм. Рівень власних шумів на вході становить -140дБм/Гц. Ці параметри значно перевершують інші вимірювальні пристрої радіосигналів. Тобто векторні аналізатори сьогодні є найбільш високоякісними приладами вимірювання вхідного сигналу.

Ще більше перевагу дає паралельний векторний аналізатор спектру, котрий на відміну від послідовного (якій використовує аналогові фільтри) використовує цифрові методи обробки радіосигналів. Паралельні векторні аналізатори можуть змінювати роздільну здатність програмно, а реалізація вузьких смуг аналізу не викликає проблем, таких, як в аналізаторах з дискретними фільтрами. Частотний діапазон векторного аналізатора залежить тільки від розмірності (числа точок) алгоритму швидкого перетворення Фур'є: $f_r = \frac{f_p}{R_f}$, де f_r - частотний діапазон, f_p - смуга частот паралельної обробки, R_f - розмірність ШПФ. Нескладно порахувати, що при смузі частот 400 кГц і розмірності 2048 частота складе біля 200 Гц при розмірності 4096-100Гц відповідно.

Цей принцип роботи паралельних аналізаторів спектра значно підвищує шанси знайти цифрову радіозакладку, користуючись можливістю програмно скорочувати смугу аналізу, що призводить до підвищення чутливості. Зменшення смуги частоти аналізу в три рази призводить до підвищення чутливості в середньому на 20 дБ. Однак, недоліком паралельного аналізу є порівняно вузька смуга частот, яка, зазвичай, не перевищує декількох МГц. Тому при застосуванні векторного аналізатора в якості основного вимірювального пристрою для АПК використовують послідовно-паралельний векторний аналізатор. При такому режимі роботи ШПФ обчислюється за частотними смугами, які потім перетворюються в безперервний сигнал. Наочний приклад наведено на рис.1.

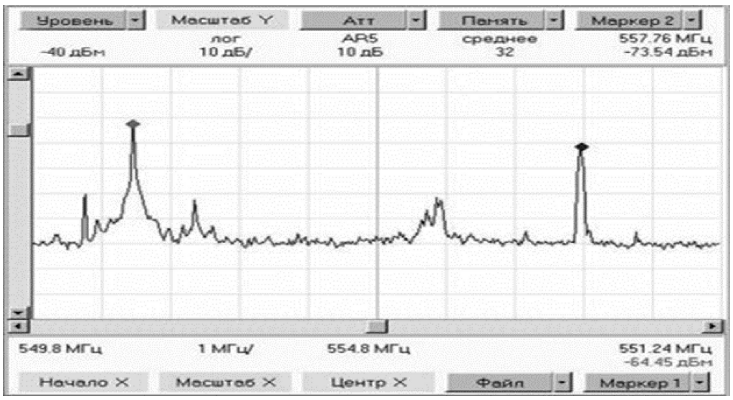

Рис. 1. Спектр повного телевізійного сигналу побудований в смузі огляду 10 МГц в режимі послідовно-паралельного аналізу

На цьому рисунку на кожному з 50 послідовних 200-кГц кроків перебудови виконується 16-точкова ШПФ [5]. Як зазначалося вище, крім частотних характеристик, які відіграють важливу роль при пошуку цифрових радіозакладок, дуже важливо аналізувати зміну радіосигналів в часі, саме ґрунтуючись на цьому факті, що векторний аналізатор розглядає комплексну огинаючу (криву) радіосигналу, можливо бачити зміни параметрів радіосигналу в часі, тож то і буде проходить тимчасовий аналіз радіосигналів. Саме на цьому принципі роботи будується принцип поліпшення методики пошуку радіозакладок, саме часовий аналіз в сукупності з раніше використовуваним у всіх методиках пошуку - амплітудний з частотним методом, дозволяє вірогідно виявляти цифрові радіозакладки, що працюють з імпульсною передачею інформації. Виходячи з детального аналізу роботи, та відмінних рис, також з застосовуваних алгоритмів обробки радіосигналів, використання у якості вимірювального пристрою, векторного аналізатора для автоматизованого програмного комплексу дозволяє значно збільшити ймовірність знаходження цифрових радіозакладок.

Висновки.

1. Коротко розглянуто тенденції розвитку цифрових радіозакладок, виявлені основні умови приховування їх роботи. Визначили, що найбільш складним є виявлення цифрової радіозакладки, що працює з накопиченням аудіо інформації та передачею її в короткий проміжок часу.

2. Векторний аналіз являє собою потужний інструмент дослідження та вимірювання характеристик радіосигналів у всьому використовуваному діапазоні частот від декількох кГц до десятків і сотень ГГц. Значний потенціал мають ці прилади у сфері радіоконтролю і радіорозвідки

3. Детально розглянуто аналіз роботи векторних аналізаторів, виявлені основні його відмінні характеристики, які полягають в обробці комплексних огинаючих, що представляють амплітуду і фазу радіосигналу. Це дозволяє досліджувати амплітудні та фазові спектри, і показувати їх у вигляді спектральних, тимчасових або векторних діаграм. Використання у векторних аналізаторів алгоритму ШПФ дозволяє істотно збільшувати роздільну здатність приладу і скоротити час аналізу радіосигналів.

4. Запропоноване удосконалення методики пошуку цифрових радіозакладок, яка ґрунтується на використанні у якості вимірювального приладу для аналізу радіоефіру векторного аналізатора, котрий за своїм принципом роботи та характеристиками дозволяє виявляти цифрові засоби негласного знімання інформації з високою ймовірністю.

Список використаної літератури

1. Ананский Е. В. Что такое радиозакладки и как их обнаружить? (часть2) / Е. В. Ананский // Журнал «Служба безопасности». [Електронний ресурс]. Режим доступу: http://www.kvirin.com/articles/267/

2. Кривцун А. В. Использование новых возможностей комплекса радиомониторинга и цифрового анализа сигналов «Кассандра-М» для обнаружения современных специальных технических средств с передачей информации по радиоканалу /А.В. Кривцун, А.В.Захаров. [Електронний ресурс]. Режим доступу :http://www.inspectorsoft.ru/article.php?id=388

3. Поисковые комплексы . [Електронний ресурс]. Режим доступу: https://www.das-ua.com/documents/catalog/search-appliances/search-complexes/page-01.php

4. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации: учебное пособие / А.А. Хорев. – М.: Гостехкомиссия России, 1998. – 320 с.

5. Силантьев В.А. Применение векторных анализаторов в системах радиоконтроля / В.А. Силантьев// "Специальна техника". – 2002 – №5. – С. 25-37.

References

1. Ananskyi E. V. “What are radio tabs and how to detect them? (part 2)”. *Security Service Magazine*, http://www.kvirin.com/articles/267/ Web.

2. Kryvtsun A. V. “Using the new features of the radio monitoring and digital signal analysis complex "Kassandra-M" for the detection of modern special technical means with the transfer of information over the air”, http://www.inspectorsoft.ru/article.php?id=388 Web.

3. “Search complexes”, https://www.das-ua.com/documents/catalog/search-appliances/search-complexes/page-01.php Web.

4. Khorev A.A. *Protection of information from leakage through technical channels. Part 1: Technical information leakage channels: Tutorial*. State Technical Commission of Russia, 1998. Print.

5. Sylantev V.A. “Application of vector analyzers in radio monitoring systems”. *Special machinery* 5 (2002): 25-37. Print.

Автори статті (Authors of the article)

Лаптєв Олександр Анатолійович – к.т.н., с.н.с., доцент кафедри систем інформаційного та кібернетичного захисту (Laptev Oleksandr Anatoliiovych – Ph.D in Technics, Senior Researcher, Associate Professor of the Department of Information and Cybernetic Protection Systems). Phone: +38(067) 434 80 01. E-mail: Alaptev64@ukr.net.

Барабаш Олег Володимирович – д.т.н., професор, завідувач кафедри вищої математики (Barabash Oleh Volodymyrovych – D.Sc. in Technics Professor, Head of the Department of Higher Mathematics). Phone: +38(095) 870 24 90. E-mail: bar64@ukr.net

Зозуля Сергій Анатолійович – асистент кафедри кафедри систем інформаційного та кібернетичного захисту (Zozulia Serhii Anatoliiovych – Professor Assistant of the Department of Information and Cybernetic Protection Systems). Phone: +38(067) 439 40 04. E-mail: zozulyas@gmail.com

Рецензент: доктор техн. наук, професор **К. С. Сундучков**, НТУУ "КПІ", Київ.