ПРИСТРІЙ ВИЯВЛЕННЯ РАДІОАКУСТИЧНИХ ЗАКЛАДНИХ ПРИСТРОЇВ

Коробка С.В.

Харківський національний університет радіоелектроніки,
Україна.

E-mail: stanislav.korobka@nure.ua

Abstract

The focus of qualifying work is technical protection of acoustic information. The objective of qualifying work is design a scanning receiver for location of secret intelligence devices.In theoretical part of qualifying work the methods and technologies of information protection via scanning receivers were considered. In practical part of qualifying work were developed: the structural scheme of scanning receiver; circuit realization of the active Chebyshev band-pass filter, frequency mixers, intermediate-frequency amplifier and crystal oscillator. Numerical analysis methods of linear and nonlinear circuits and MathCAD software environment were used.

Промислове шпигунство в сучасному світі набуває все більшого поширення і для захисту від нього підприємства та фірми затрачують великі ресурси, бо цінність конфіденційної інформації і важкі наслідки в разі незаконного ознайомлення з нею сторонніх осіб давно вже стали очевидні всьому розвиненому суспільству.Один із шляхів негласного отримання комерційної інформації заснований на застосуванні так званих закладних пристроїв, що таємно встановлюються в місцях можливого знаходження об'єктів спостереження або підключаються до використовуваних ними каналів зв'язку. В наш час розроблено велику кількість типів таких пристроїв, що розрізняються принципом функціонування, способом передачі інформації, дальністю дії, а також розміром і зовнішнім оформленням.

У радіозакладних пристроях для передачі інформації використовується енергія електромагнітних хвиль, які не впливають на органи чуття людини, здатні поширюватися на значні відстані, долаючи природні та штучні перешкоди. Завдяки цим двом властивостям радіозакладні пристрої дозволяють за допомогою спеціальної приймальної апаратури вести скритне спостереження за об'єктом, який цікавить, практично з будь-якої віддаленої точки.

Останнім часом з'являються радіозакладні пристрої, що використовують надвисокочастотний діапазон (понад 10 ГГц), а також радіозакладні пристрої, які постійно змінюють частоту носійного сигналу або використовують шумоподібні сигнали.

Ефективним засобом протидії несанкціонованому зніманню інформації за допомогою радіозакладних пристроїв є панорамні (скануючі) радіоприймальні пристрої. Сучасний скануючий приймач дозволяє здійснювати:

– панорамний спектральний аналіз радіосигналів при спільній роботі всіх каналів від однієї антени – накопичення панорами спектрів в заданому діапазоні частот;

– збереження спектральної панорами для подальшого аналізу;

– панорамний спектральний аналіз радіосигналів по кожному каналу, накопичення панорами спектрів в заданому діапазоні частот;

– відкладену обробку результатів панорамного аналізу;

– когерентну багатоканальну обробку радіосигналів;

– покроковий перегляд списку діапазонів частот з автоматичною постановкою знайдених джерел на реєстрацію;

– пошук працюючих джерел радіовипромінювань за списком частот;

– запис радіосигналів по проміжній частоті в векторній формі на ЕОМ;

– технічний аналіз, визначення виду модуляції і вимірювання параметрів радіосигналів;

– запис де модульованих сигналів на ЕОМ;

– відтворення записаної на ЕОМ звукової інформації, прослуховування працюючих джерел радіовипромінювань в реальному часу;

– формування звітів за результатами моніторингу радіоканалів і аналізу сигналів.

В даній кваліфікаційній роботі проведено проектування та розрахунок основних функціональних вузлів скануючого цифрового радіоприймального пристрою.

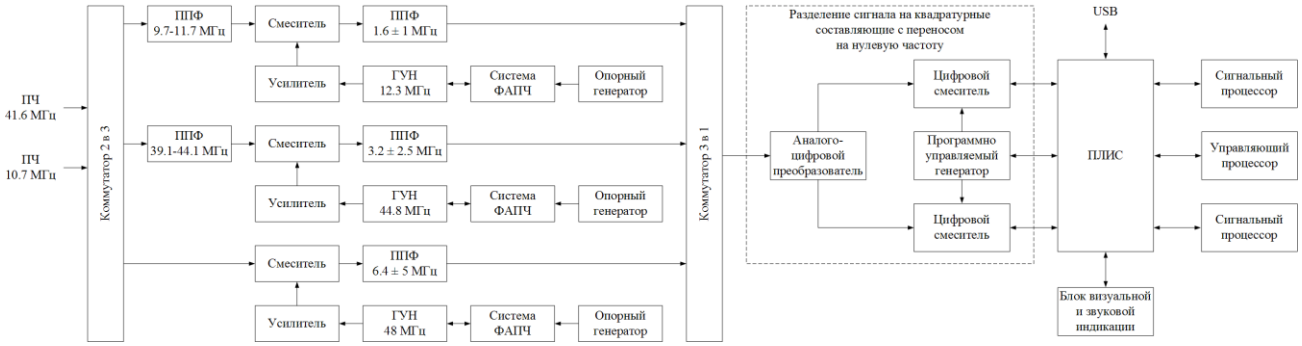

Рис. 1. Загальна схема програмного комплексу Osmocom для побудови БС LTE

Література

1. Торокин А.А. Инженерно-техническая защита информации – М.: Гелиос АРВ, 2005. – 960

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

3. Петраков А.В. Охрана и защита современного предприятия / Петраков А.В., Дорошенко П.С., Савлуков Н.В. – М.: Энергоатомиздат, 1999. – 568 с.

4. Абалмазов Э.И. Методы и инженерно-технические средства противодействия информационным угрозам. – М.: Изд-во "Компания "Гротек", 1997. – 248 с.

5. Методы и средства защиты информации / [Хорошко В.А., Чекатов А.А.]; под ред. Ю.С. Ковтанюка – К.: Издательство Юниор, 2003. – 504 с.

6. Большая энциклопедия промышленного шпионажа / [Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н.]. – СПб.: ООО "Изд-во "Полигон", 2000. – 896 с.

7. Герасименко В.А. Основы защиты информации / Герасименко В.А., Малюк А.А. – М.: МГИФИ, 1997. – 538 с.

8. Петраков А.В. Основы практической защиты информации – М.: Радио и связь, 1999. – 368с.

9. Лагутин В.С. Утечка и защита информации в телефонных каналах / Лагутин В.С., Петраков А.В. – М.: РадиоСофт, 2009. – 324 с.

10. Зааль Р., Справочник по расчетам фильтров. – М.: Радио и связь, 1983. – 753 с.

11. Демин В.П. Радиоэлектронная разведка и радиомаскировка / Демин В.П., Куприянов А.И., Сахаров А.В. – М.: Изд-во МАИ, 1997. – 156 с