Volodymyr SOKOLOV[1], Artem PLATONENKO[2], Lidiia KUZMENKO[3]

Scientific supervisor: Volodymyr BURIACHOK[4]

OPRACOWANIE NISKOBUDŻETOWYCH ANALIZATORÓW WIDMA DLA IoT I SIECI CZUJNIKÓW

Streszczenie: W artykule opisano rozwój, wdrożenie i badania pracy analizatorów widma dla sieci czujników i Internetu Rzeczy (IoT). Jako pasmo robocze wybrano pasmo ISM 2,4–2,5 GHz. Analiza porównawcza istniejących dostępnych mikrokontrolerów do analizy widma, wybór interfejsów sprzętowych, zamawianie wymaganych modułów i komponentów elektrycznych. Podczas opracowywania zaimplementowano kilka wariantów analizatorów widma.

Słowa kluczowe: analiza widma, sieć bezprzewodowa, nadajnik-odbiornik, zakres ISM

DEVELOPMENT OF LOW-BUDGET SPECTRUM ANALYZERS FOR IoT AND SENSOR NETWORKS

Summary: The article describes the development, implementation and research of the work of spectrum analyzers for sensor networks and IoT (2.4 GHz). Comparative analysis of existing available microcontrollers for spectrum analysis, selection of hardware interfaces, ordering of required modules and electrical components have been described in the paper. Several variants of spectrum analyzers were implemented during development

Keywords: spectrum analysis, wireless network, transceiver, ISM range

1. Introduction

In Ukraine, more and more new home and industrial networks are being built with full or partial use of wireless technologies. Over the past few years, such technologies

[1] Ph.D. in IT, Borys Grinchenko Kyiv University, associate professor of Information and Cyber Security Department, OrcID: 0000-0002-9349-7946, v.sokolov@kubg.edu.ua
[2] Ph.D. in IT, Borys Grinchenko Kyiv University, associate professor of Information and Cyber Security Department, OrcID: 0000-0002-2962-5667, a.platonenko@kubg.edu.ua
[3] Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Postgraduate student, OrcID: 0000-0001-7392-0324, lido4ok@gmail.com
[4] Prof., D.Sc., Borys Grinchenko Kyiv University, head of Information and Cyber Security Department, OrcID: 0000-0002-4055-1494, v.buriachok@kubg.edu.ua

have become the defacto standard. The number of networks is increasing due to their affordability and ease of use, the emergence of industrial roaming systems, a wide range of antenna equipment, and the use of licenses fixed at the legislative level.
This article addresses the main issue of securing information transmission in wireless systems: its accessibility. When designing a wireless network, it is not possible to anticipate all the nuances: re-reflection, shading, the directionality of the antennas of the receivers, etc., so after the construction of a real system, you need to check it and reduce the impact of negative factors. Spectrum analyzers help solve this problem.
Spectrum analyzers do not increase the availability of information on the network, but contribute to its improvement, through the identification of weaknesses, occupancy of the spectrum by other networks (collision avoidance/interference). Unlike the standard tools available on network cards, the spectrum analyzer collects noise levels such as magnetrons (in microwave ovens), can detect stationary interference and other equipment (Bluetooth, ZigBee, radios, toys, video transceivers, video transceivers) medical sensors, etc.). Also, the spectrum analyzer "sees" not only service packets, which assess the signal level in network cards, but also all other packets. Therefore, the topic of the article is important and very relevant. Previous versions of the Pololu Wixel industrial spectrum analyzers have been used by the authors as sensors in conducting antenna research [1] and building sensor networks [2].
The diagram (Fig. 1) shows the classification of modern types of spectrum analyzers. The spectrum analyzers considered in the article are related to Fourier analyzers.

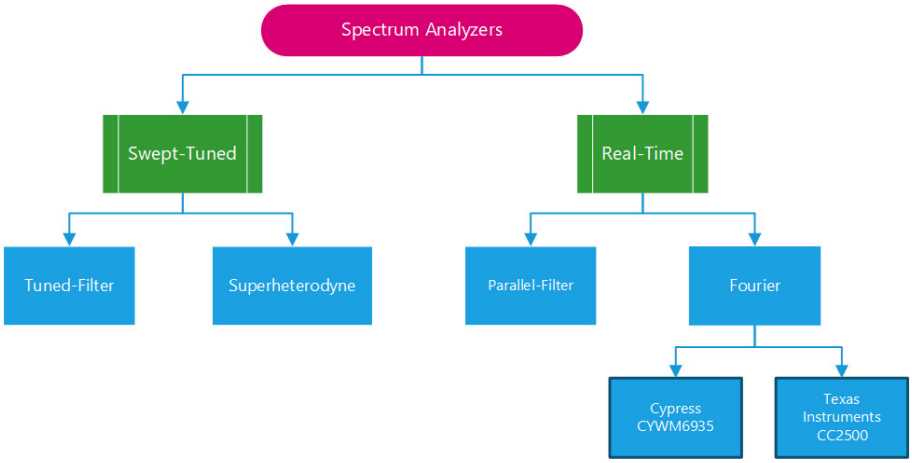

Figure 1. Spectrum analyzer classification

2. Comparisons of Radio Frequency Transfers

Spectrum analyzer is a device for scanning and analyzing a specific frequency band, allowing you to detect and communicate wireless capabilities of wireless networks, access points, and client devices. For example, using a frequency scanner allows you to identify the names of detected radio networks, their signal level, the type of data encryption used, and other parameters. The most common spectral Wi-Fi analyzers

can be found in an arsenal of professionals whose professional activity is related to the deployment and setup of 802.11 a/b/g/n/ac wireless data networks.
Using a frequency scanner during the construction phase of a Wi-Fi network allows the engineer to quickly determine the presence and level of interference on the airwaves, to choose the optimal frequency for WLAN operation, as well as to calculate the number and location of access points to provide a complete coverage area. In the event of a network failure, the spectrum analyzer can assist in the diagnosis and detection of the cause of the problem, including assessing network congestion, detect unauthorized connections and devices, identify and locate radio interference in channels [3] and [4]. In this paper, only low-cost circuits were selected so that they could be used in sensor networks such as those given in [2]. Table 1 summarizes the six most successful transceivers in this class from the manufacturers Nordic, Texas Instruments, and Cypress. The comparison shows that Texas Instruments are the most successful transceivers. The following are experiments to compare the performance of the tracers of only two firms (TI and Cypress) since the Nordic nRF24L01 module has a very small range of signal power measurement and therefore its limits of use are quite small. Four hardware implementations of analyzers are considered:

- CC2500 microcontroller (with USB interface).
- CC2500 module (USB).
- CYWUSB6935 module (LPT).
- CYWUSB6935 module (USB).

Table 1. Basic characteristics of transceivers

Microcircuit	Frequency range, MHz	Resolution, kHz	Power range, dBm	Resolution, dBm
Nordic nRF24L01	2400–2525	977	–(85..42)	1.0
TI Chipcon CC2500	2400–2483.5	58–812	–(104..13)	0.8
TI Chipcon CC2511-F32	2400–2483.5	58–812	–(110..6.5)	0.5
Cypress CYRF6934	2400–2483	1000	–(90..40)	~4.1
Cypress CYRF6935	2400–2483	1000	–(95..40)	~3.1
Cypress CYRF6936	2400–2497	1000	–(97..47)	~1.3

3. CC2500-Based Analyzer

To analyze the integrity of the data transfer, we will use a hardware spectrum analyzer built on a radio transceiver, namely the Chipcon CC2500. The scheme of the device is shown in Fig. 2.
An example of such a double-sided board is shown in Fig. 3a. This project is transferred on thermal paper, which is ironed until the color changes from white to gray. Then we take this thermal paper and print a card on it with the help of a laser printer. Fig. 3b shows printed paper with the printed circuit board. The board is made on fiberglass size 96×71 mm and a thickness of 1 mm. Printed circuit boards are attached to the fiberglass and are ironed for about 5 minutes on each side. The board is cooled and transferred to a container of warm water, and the paper is removed within half an hour. The board is transferred to a container with chlorine iron and the

board is etched. (On the first attempt, it failed to make a circle of the transceiver through the thin tracks, which began to “fly away” immediately when the board was etched). Sandpaper is used to process the workpiece, drill holes with 0.5 and 2 mm drill bits. As a result, we get a ready fee for mounting the elements (Fig. 3c).

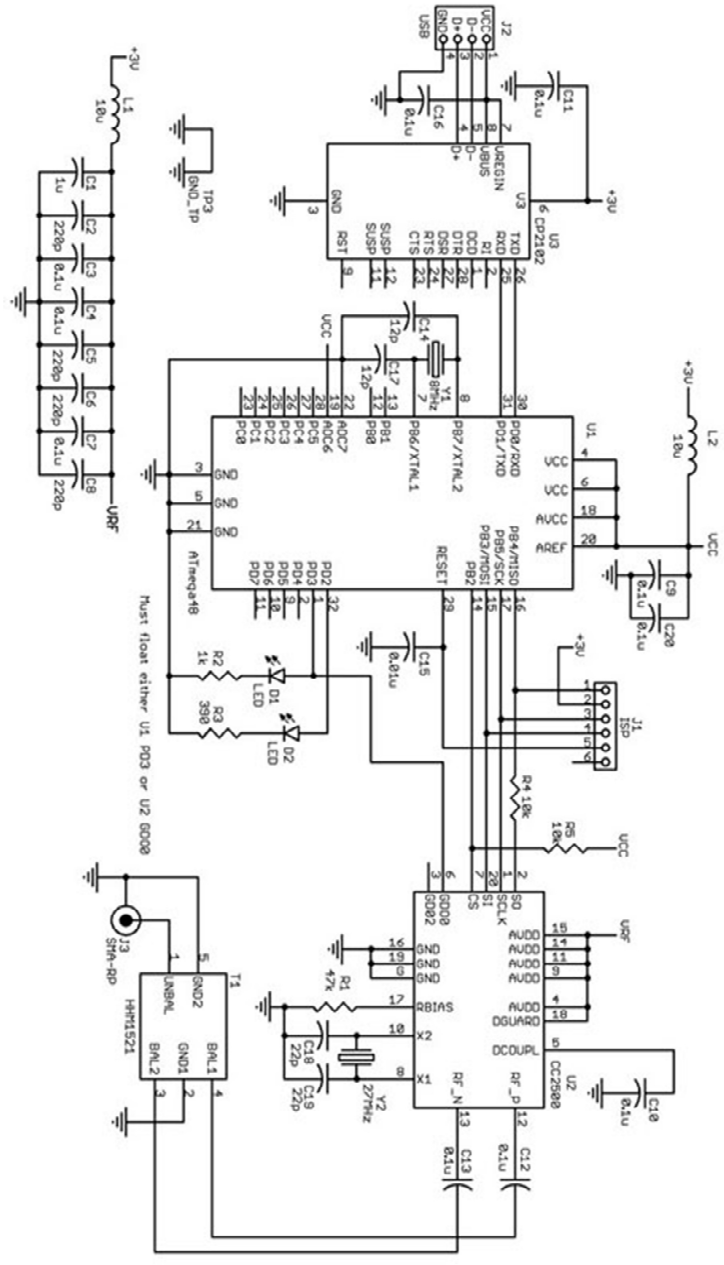

Figure 2. Schematic diagram of a spectrum analyzer on the Chipcon CC2500

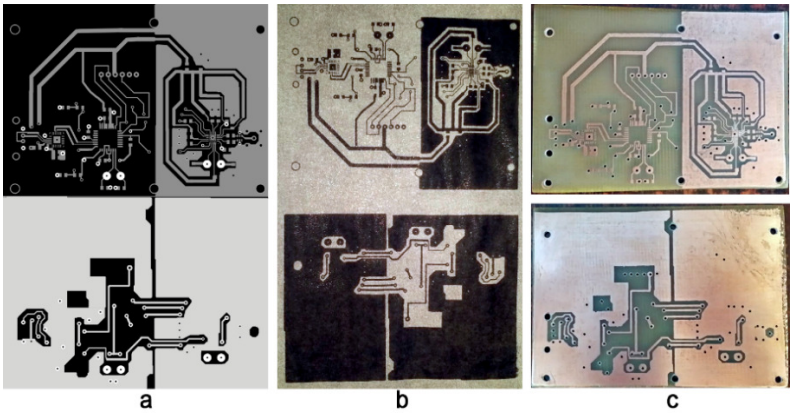

Figure 3. Spectrum analyzer PCB on Chipcon CC2500: in the graphic editor (a); thermal paper with the printed circuit board (b); finished board (c)

After mounting the elements, the Atmega48 microcontroller is programmed using a USB programmer for AVR [5], [6]. Fig. 4a shows a ready-made board, but with a soldered microcontroller. After flashing the microcontroller, we solder it back to the board and connect it to the computer, install the drivers for the device, and run the spectrum analysis program, but the device did not work the first time. Checked all tracks on the board with a multimeter and found that there was a break on one track, it was successfully removed with a soldering iron and tin. After that, the board was installed in the housing (Fig. 4b). Raising a hand or other object to the device creates a tip, so we decided to put a screen to reduce interference in the area where the transceiver is located. The screen we made of copper (Fig. 4c).

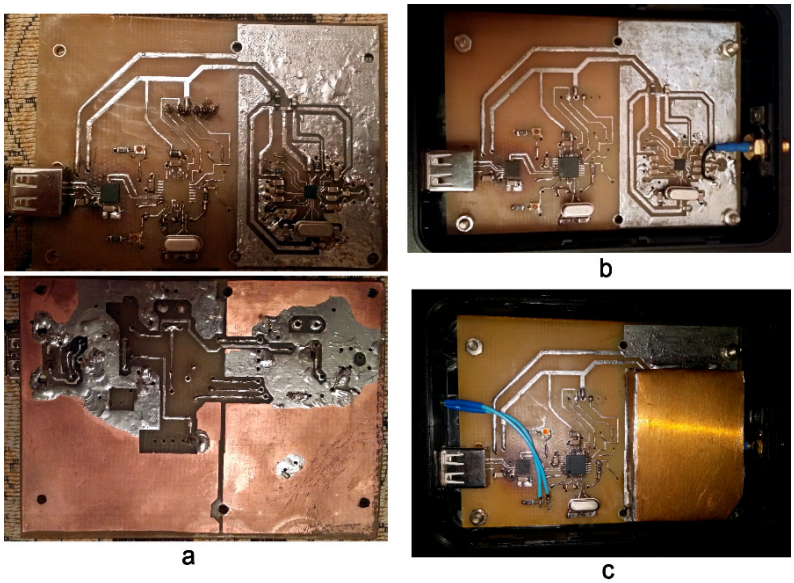

Figure 4. Chipcon CC2500 spectrum analyzer board: with mounted elements (a); installed in the housing (b); with a soldered screen (c)

The results of the spectrum analyzer are presented in Fig. 5.

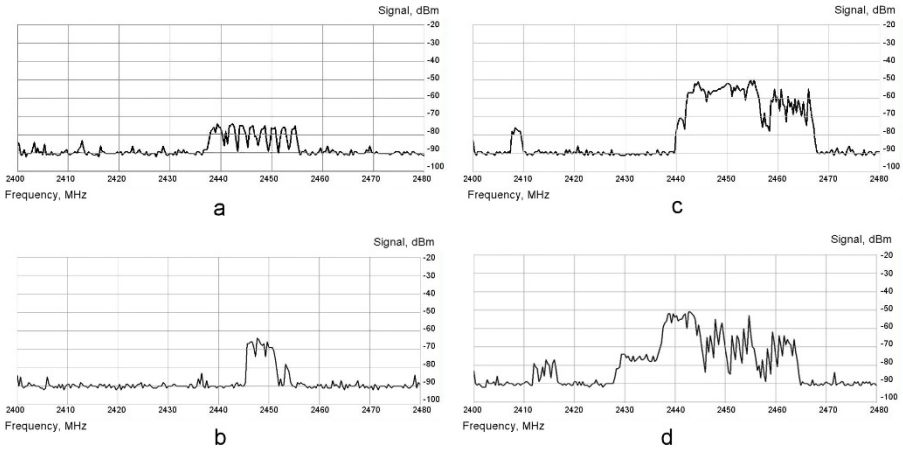

Figure 5. Analysis of the spectrum obtained from Chipcon CC2500:
without the use of antenna and screen (a);
using the screen, but without the antenna (b);
using the antenna, but without the screen (c);
using antenna and screen (d)

During the experiments, the microcontroller burned down due to insufficient heat sink, so it was decided to leak a new board, replace the microcontroller and antenna.

4. CYWUSB6935-Based LPT Analyzer

The Cypress CYWUSB6935 micro-assembly was used to implement the superheterodyne spectrum analyzer. In Fig. 6 is a schematic diagram, and in Fig. 7 is an adapter assembled on the circuit board.

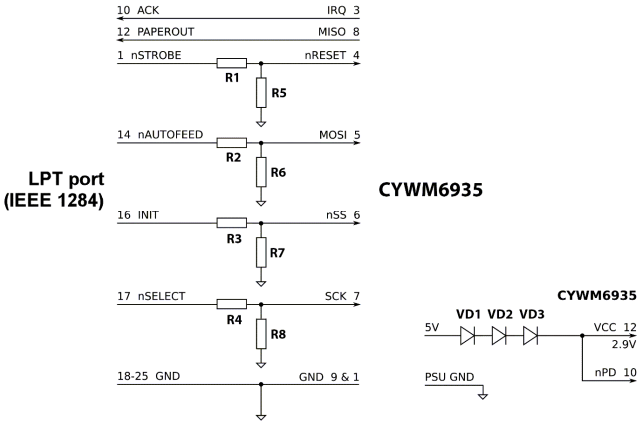

Figure 6. Circuit diagram for connecting the CYWUSB6935 module

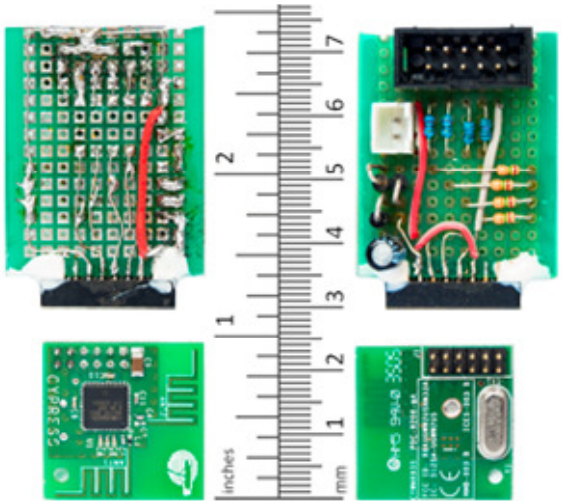

Figure 7. Appearance of the LPT spectrum analyzer on the CYWUSB6935 module

When reading via console directly from the LPT port, RSSI levels are obtained:

```
frame: [0,0,1,1,0,0,2,1,0,2,0,0,4,31,30,2,0,0,0,0,0,3,0,0,0,
0,0,0,0,0,0,0,1,1,0,0,0,1,0,2,0,0,0,0,0,0,0,1,0,0,2,0,0,0,2,
0,0,0,1,0,4,5,1,1,0,0,1,1,0,1,1,1,0,0,0,0,3,2,1,0,0,0,0,1,]
frame: [1,1,0,3,0,0,0,0,1,0,0,2,3,1,0,0,0,0,0,0,0,27,19,1,0,
0,0,0,0,0,0,0,1,0,1,0,1,2,3,0,0,0,0,1,0,0,1,0,0,1,0,2,1,0,0,
3,3,1,0,0,0,0,0,0,0,0,0,0,2,4,4,0,0,0,0,0,1,0,3,2,0,0,0,0,]
frame: [0,0,0,2,0,1,0,2,0,31,31,0,3,0,1,0,0,0,1,0,1,0,0,0,1,
0,0,0,0,1,1,0,1,0,0,0,0,0,2,0,0,0,0,0,1,0,1,0,0,0,0,0,1,1,1,
1,0,0,1,2,0,3,3,0,0,2,0,2,1,1,0,1,0,0,0,1,0,0,0,2,1,1,0,0,]
```

After collecting the data, the resulting picture of the spectrum is shown in Fig. 8.

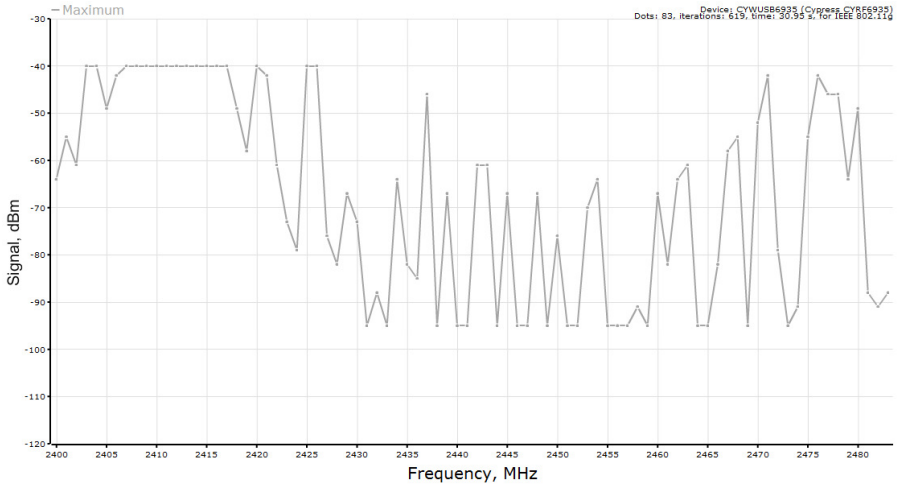

Figure 8. Analysis of the spectrum obtained from CYWUSB6935

The design has a major drawback—working on an outdated LPT interface that is rarely found in modern computers. Also, extra power is required. In this case, we used power from the USB port in series with three diodes connected to reduce the voltage.

5. CYWUSB6935-Based USB Analyzer

The schematic diagram of the spectrum analyzer is shown in Fig. 9.

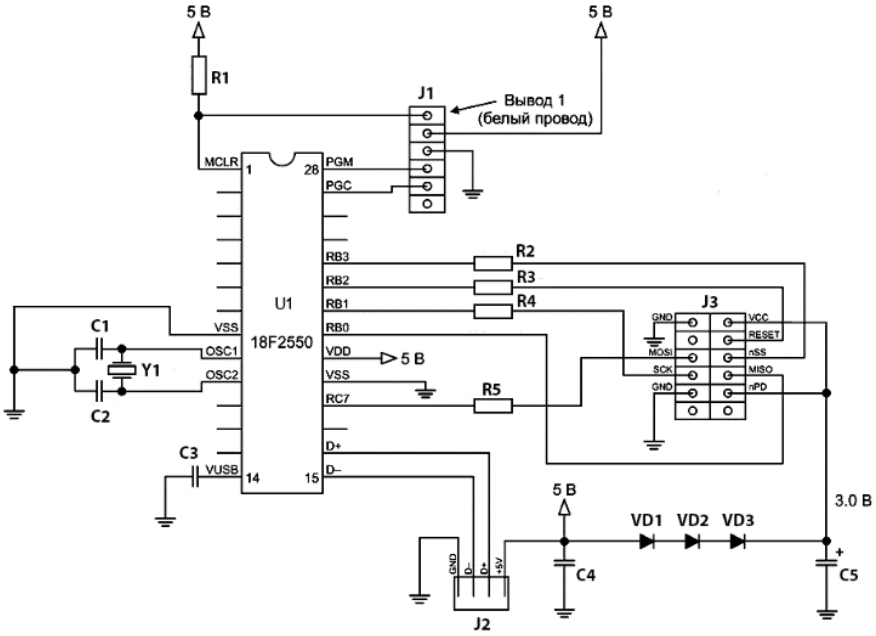

Figure 9. Schematic diagram of the control module CYWUSB6935

The microcontroller is clocked by a 20 MHz quartz resonator with two 15 pF load capacitors. The internal divider of the microcontroller divides the clock frequency by 5 to obtain a frequency value of 4 MHz, which will be used for phase auto frequency tuning at a frequency of 48 MHz. This is the main clock on which the USB interface and the kernel work. A 10 kΩ resistor connected to pin 1 of the microcontroller pulls the MCLR (reset) output to high. The scanner receives power from the USB interface as the circuit consumes little current. To power the radio module requires a voltage of 2.7 to 3.6 V. Voltage of the order of 3.0 V, we can get from the bus 5 V, including a series of 3 diodes type IN4001 (for each diode voltage drop of about 0.7 V). This, of course, is the simplest and cheapest, but quite reliable way. CYWUSB6935 has protection diodes at the inputs. This means that you can use 5-volt logic signals from the microcontroller to control it, including serial resistors to limit the current.

Since our scheme is not too complicated, the easiest way was to assemble the device: a circuit board (Fig. 10). A special multi-pin connector was used to connect the radio module. A standard USB connector was used [6].

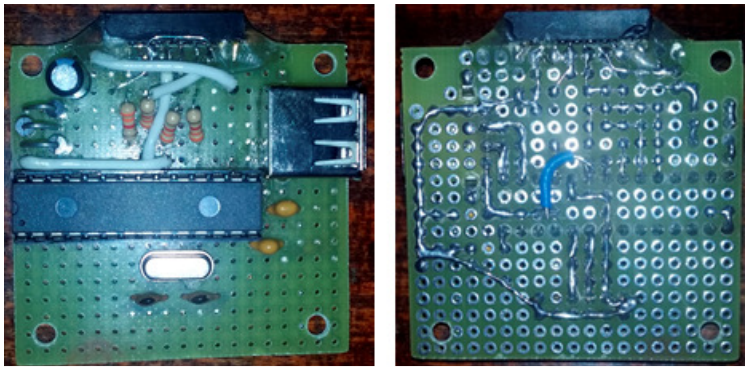

Figure 10. The appearance of the control module

6. Comparison of Spectrum Analyzers

Fig. 11a and 11b present the results of reception at the location of the spectrum analyzer in the near area of the transmitter to transmit data over a wireless Bluetooth channel, and Fig. 11c and 11d are 2.4 GHz Wi-Fi. It is easy to see that the solid assembly showed much better results because the assembly, the screen, and the external antenna were used better.

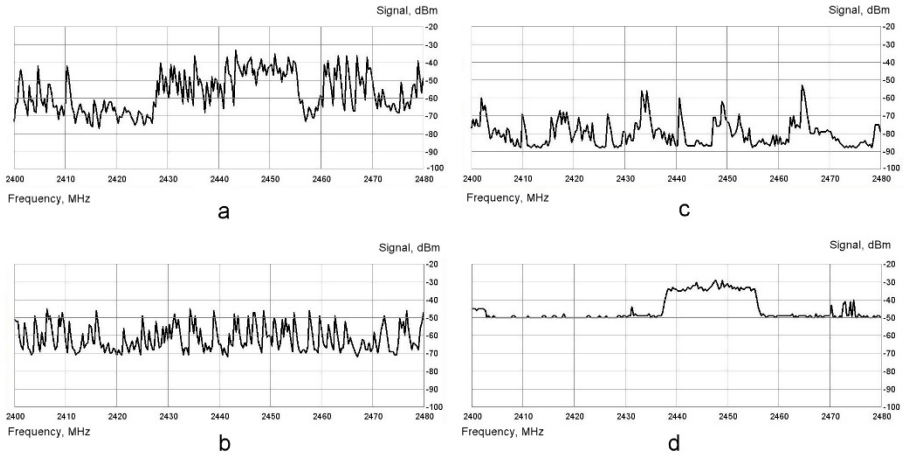

Figure 11. Examples of spectra for different devices:
Bluetooth with external modular (a); Bluetooth with internal modular (b);
Wi-Fi with external modular (c); Wi-Fi with internal modular (d)

After assembly, testing, and debugging, the device is ready for use in both technical and scientific applications. The general view of all three devices is shown in Fig. 12.

Figure 12. General view of all spectrum analyzers

7. Spectrum Analyzer Calibration

Fig. 13 shows the calibration scheme for hardware spectrum analyzers. The generator was Software-defined radio (SDR) Great Scott Gadgets HackRF One with software GNU Radio v. 3.8, which simulated various wireless data transfer protocols. The spectrograms of the spectrum analyzers described earlier were compared [5, 6] with a Nuand bladeRF x40 SDR verification receiver with software HDSDR v. 2.80.

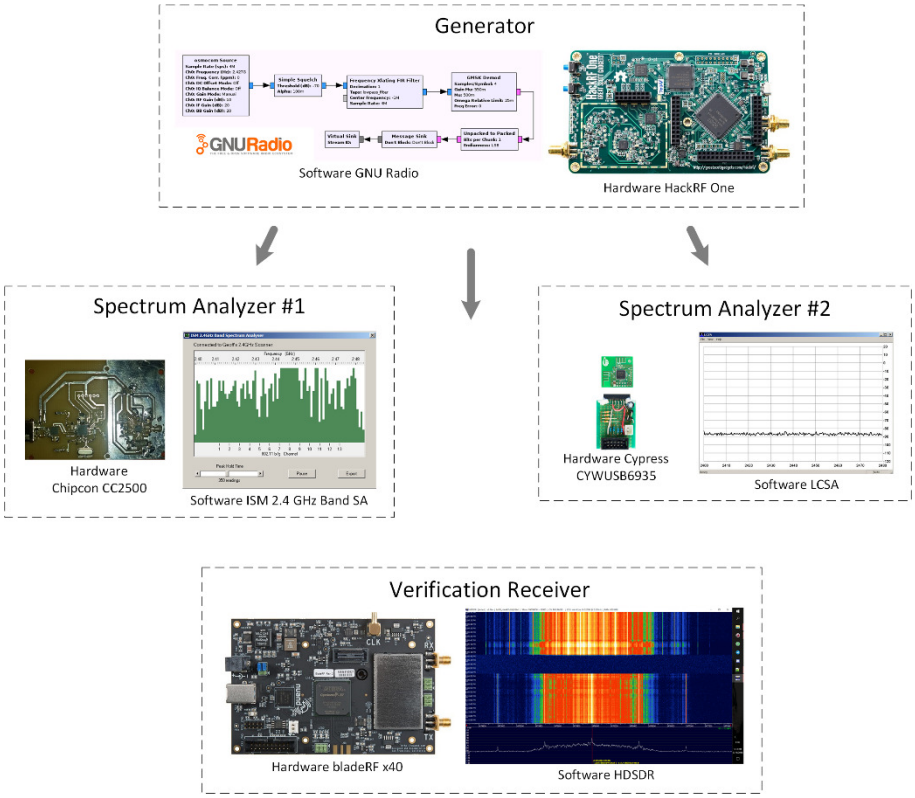

Figure 13. Calibration scheme for hardware spectrum analyzers

8. Conclusions and Further Research

The article presents the results of designing and manufacturing spectrum analyzers on pre-made components (ICs for IEEE 802.15.4/ZigBee). The process of designing, manufacturing printed circuit boards, collecting devices, and programming microcontrollers are described in detail. Testing and improvement of existing devices were carried out. The wiring of the board revealed the dependence of the quality of work of the device on the quality of its assembly, the presence of an electromagnetic screen, and the type of antenna.

The article uses third-party software, as well as software developed at the Department of Information and Cyber Security to analyze data collected from different spectrum analyzers. After detailed testing and testing of the devices, we concluded that a more compact solution for serial production of devices could be made.

Possible areas for further research include deeper statistical analysis, improved approaches to information measurement, and forecasting. In the future, these devices can be integrated into the software complex of the situational center, which consolidates the work with various low-budget models of analyzers of the spectrum of a given frequency range.

REFERENCES

1. ASTAPENYA V., SOKOLOV V.: Experimental evaluation of the shading effect of accelerating lens in azimuth plane. Proc. XI Intet. Conf. on Antenna Theory and Techniques (ICATT), Kyiv 2017, 389–391. DOI: 10.1109/icatt.2017.7972671.
2. SOKOLOV V., CARLSSON A., KUZMINYKH I.: Scheme for dynamic channel allocation with interference reduction in wireless sensor network. Proc. IV Inter. Conf. Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv 2017, 564–568. DOI: 10.1109/infocommst.2017.8246463.
3. RAUSHER K.: Basics of spectral analysis: Rohde & Schwarz. Goryachaya Liniya-Telekom, 2006.
4. VARGAUZIN V.: Radio networks for data collection from sensors, monitoring and control based on the IEEE 802.15.4 standard: RFID. Telecommunications, **6**(2005), 23–27.
5. ARMITAGE S.: Low-Cost 2.4-GHz spectrum analyzer. Circuit Cellar, **189**(2006), 18–22.
6. Website of Geoff Graham—2.4 GHz WiFi & ISM band scanner: *http://geoffg.net/ISM_Scanner.html*, 16.01.2020.