# Hardware and Software Complex for Analysis of Radio-Electronic Environment in Radio Communication Networks of GSM/UMTS/LTE Standards

Sergey Blinov
UrFU
Yekaterinburg, Russia
drs-slam@yandex.ru

Vladimir Shkitenkov
UrFU
Yekaterinburg, Russia
sun1605@mail.ru

## Abstract

The article describes the hardware and software complex for analyzing the radio-electronic environment in the radio communication networks of the GSM / UMTS / LTE standards, which was developed in the final qualification work. The developed device performs the tasks set for analyzing the radio-electronic situation in real time, including in the premises.

## 1 Introduction

The number of radio frequency means that operate in GSM, UMTS and LTE radio communication networks is growing every day. To maintain and improve the quality of services provided, cellular operators increase the number of base stations (BS). But the frequency resource is limited and controlled by the state. The control is carried out by the "General Radio Frequency Center" and the Federal Service for Supervision in the Communication and Information Technologies "Roskomnadzor".

When installing the BS, an operator is obliged to keep within the law in force in the territory of Russia and have permission to use frequencies. At the same time, Roskomnadzor identified over 13,000 illegally operating BSs from the "big four" by September 2016 (MTS, Megafon, Beeline, Tele2) [1].

To detect violations, the radio frequency service conducts periodic monitoring of the parameters of radio electronic means for deviating from the parameters specified in the frequency permission.

## 2 The problem of monitoring the radio-electronic environment indoor the premises

The Radio Frequency Service is a specially authorized service that ensures the regulation of the use of radio frequencies and radioelectronic means in the Federal Service for Supervision in the Communication Sphere and Information Technologies.

The radio frequency service performs the following functions:

- controls emissions of radio electronic means and high-frequency devices (radio monitoring);
- ensures the correct use of radio frequencies or radio frequency channels by radio electronic means and high-frequency devices

To monitor the radio-electronic situation, the Radio Frequency Center uses mobile complexes. Today, to use almost any of these complexes, it is required to re-equip a car. In addition, such complexes require diesel generators as power. An example of a mobile radio monitoring system can be seen in Figure 1.

Figure 1: Example of a radio monitoring complex

Such complexes cannot be called portable. Also, They cannot be used to monitor the electronic environment in the premises, which is especially relevant with the development of indor-cover recently.

The developed device has the following advantages: small dimensions, built-in GPS-receiver, requires only a laptop with Windows 7 and most importantly - with it you can monitor in premises. The developed device does not have direct analogues. Similar portable competitors solve other tasks and do not have the ability to monitor the electronic environment in real time for several operators.

## 3 The concept and tasks that the hardware-software complex solves

The developed hardware and software complex was called the "Enot". It is the decoder of the system information of the wireless communication standards GSM, UMTS and LTE. Structurally it is made in the form of a portable monoblock. Can be installed on a mobile radio monitoring system (on the basis of any vehicle, including unequipped vehicles) or be used by a specialist without a car to measure the radioelectronic situation in open areas and indoors (assessing the indoor radio-electronic environment). The complex has hardware and software parts. The hardware includes a monoblock with a telecommunications module, antennas for diversity reception, a GPS module with an antenna, and an integrated battery with a power management board. The software part includes drivers for pairing a monoblock with a laptop on Windows 7 and the application “Enot” for input / output of information provided by the complex's functionality.

Identification/decoding of monitored signals from the BSs of radio communications of GSM, UMTS and LTE standards:

- Frequency of transmission in the direction of downlink and uplink (determined by the frequency channel number) [2][3][4];
- The power of the signal detected in the channel;
- Carrier identifier;
- Base station identifier (BS);
- Registration of information (recording "logs" in LOG format and generating a report in HTML format) for post-processing and preparation of reporting materials on identified signs of violations by cellular operators
- Coordinate information on the route;

Events of radio control:

- Determination of the load of frequencies and frequency bands, the formation of a report in the established form (in HTML format).

# 4 The hardware part of the analyzer of radio-electronic environment the "Enot"

## 4.1 Telecommunication module SIM7100E EVB

The LTE module SIM7100E from SIMCom Wireless Solutions was selected as the hardware part of the radio-electronic environment the "Enot".

This module is designed as a debugging board and meets the following requirements:

- Version "E" works in the Russian frequency band LTE (There are versions for other countries, including Europe, America and China);
- There is a built-in GLONASS / GPS-receiver;
- It is possible to connect up to two external antennas GSM, UMTS and LTE with the possibility of diversity reception [5] and one GLONASS / GPS antenna;
- A wide range of operating temperatures (-30 ... +80) and storage range (-45 ... + 90), which is actual in the climatic conditions of Russia.

## 4.2 Power supply circuit for the analyzer of electronic environment

The telecommunications module can consume current up to 2A in peaks. Therefore, the device was equipped with rechargeable batteries Samsung ICR18650-26F (type - 18650), which can be given in the peak 2A and a control board to them. The batteries provide a stable power supply of 3.7V, and the capacity of each of them is 2600mAh[6]. It turns out that one 18650 battery should "keep" the peak load for at least an hour. The power circuit for the hardware and software was designed in the program sPlan 7.0.0.9 and is shown in Figure 2.

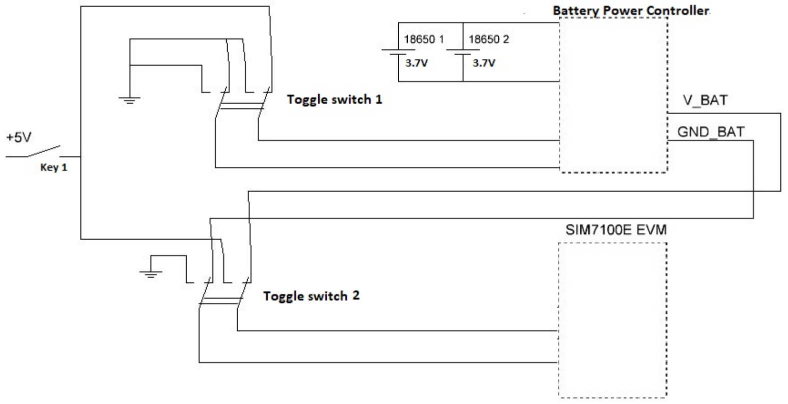


Рисунок 2: Power circuit for the “Enot”

## 4.3 The case for the hardware-software complex

As the case for the analyzer the "Enot" was selected Gainta G768, which has an overall dimension of 190 * 140 * 80mm. It is made of light gray ABS plastic. In addition, toggle switches, buttons, wires and other parts necessary for assembly were selected. The location of the components of the device can be seen in Figure 3 on the left. The general view of the case is shown in Figure 3 on the right Omni-directional receiving and transmitting antenna, located in the device case and has a gain of 2.5 dB (operating range 700 ... 960MHz / 1710 ... 2700MHz). It is located there, because in severe conditions the use of an external antenna can be difficult, it can be accidentally broken or torn from the body of the device [7].

As an external antenna, you can use any antenna that works in the GSM, UMTS and LTE standards. Now an antenna with a gain of 5 dBi is used (operating range is 700 ... 960MHz / 1710 ... 2700MHz), but instead it can be connected to the active log-periodic directional antenna ROHDE & SCHWARZ HE300 (operating range 500MHz ... 7.5GHz) [8].

The GPS / GLONASS antenna is active with a supply voltage of 3 ... 5V. The initial search for satellites takes about 5 ... 15 minutes.

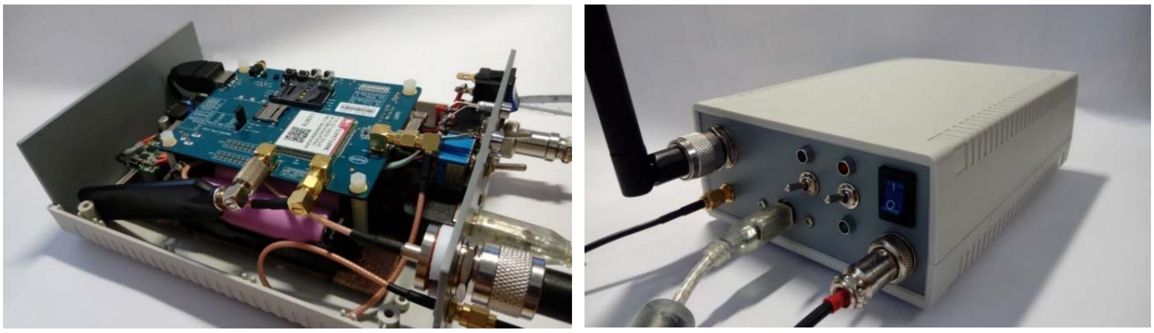
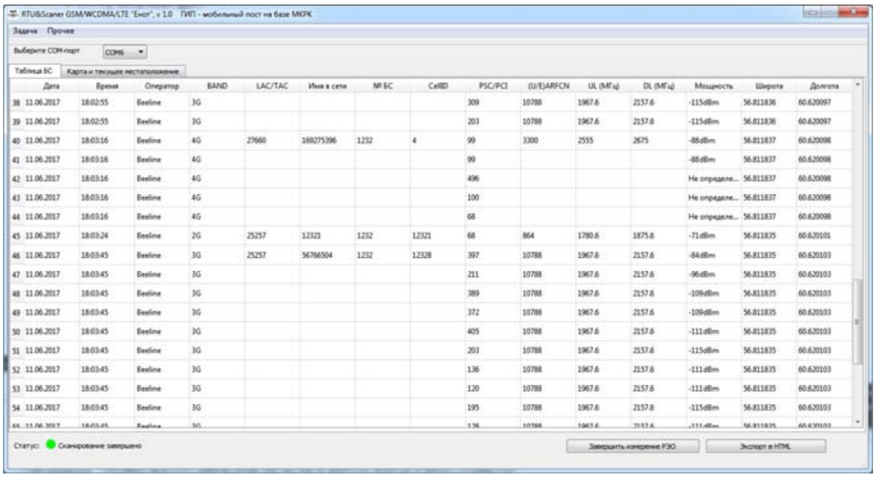


Figure 3: Location of components in the case (left) and the appearance of the device (right)

## 5 The software part of the analyzer of radio-electronic environment "Enot"

The main part of the program was written in C++ using the Qt library, generating a report using HTML markup language, and displaying offline maps in JavaScript. The program has the function of recording logs. The program is distributed in the form of an executable file (*.exe). The main window of the program can be seen in Figure 5, and the example of the map in Figure 6.



RTU&Scaner GSM/WCDMA/LTE "Енот", v 1.0   ГИП - мобильный пост на базе МКРК

Задача   Прочее

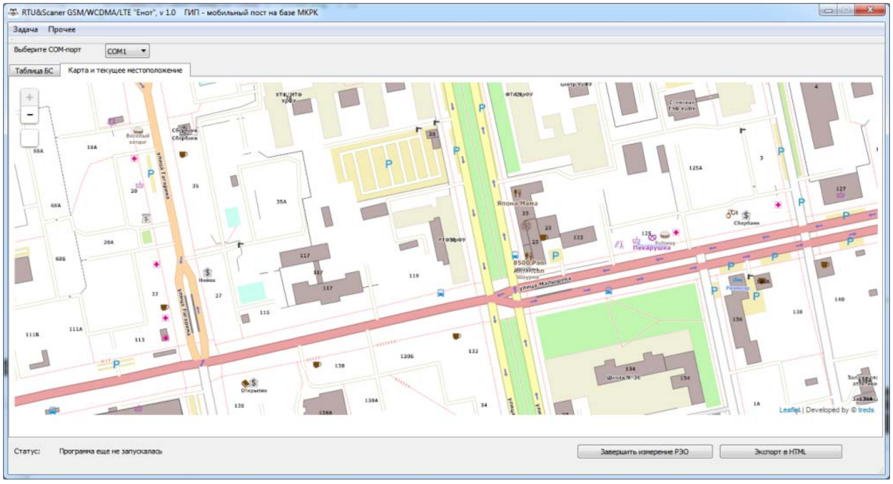
Выберите COM-порт: COM6

Таблица БС | Карта и текущее местоположение

| | Дата | Время | Оператор | BAND | LAC/TAC | Имя в сети | № БС | CellID | PSC/PCI | (U/E)ARFCN | UL (МГц) | DL (МГц) | Мощность | Широта | Долгота |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 38 | 11.06.2017 | 18:02:55 | Beeline | 3G | | | | | 309 | 10788 | 1967.6 | 2157.6 | -115dBm | 56.811836 | 60.620097 |
| 39 | 11.06.2017 | 18:02:55 | Beeline | 3G | | | | | 203 | 10788 | 1967.6 | 2157.6 | -115dBm | 56.811836 | 60.620097 |
| 40 | 11.06.2017 | 18:03:16 | Beeline | 4G | 27660 | 169275396 | 1232 | 4 | 99 | 3300 | 2555 | 2675 | -88dBm | 56.811837 | 60.620098 |
| 41 | 11.06.2017 | 18:03:16 | Beeline | 4G | | | | | 99 | | | | -88dBm | 56.811837 | 60.620098 |
| 42 | 11.06.2017 | 18:03:16 | Beeline | 4G | | | | | 496 | | | | Не определе... | 56.811837 | 60.620098 |
| 43 | 11.06.2017 | 18:03:16 | Beeline | 4G | | | | | 100 | | | | Не определе... | 56.811837 | 60.620098 |
| 44 | 11.06.2017 | 18:03:16 | Beeline | 4G | | | | | 68 | | | | Не определе... | 56.811837 | 60.620098 |
| 45 | 11.06.2017 | 18:03:24 | Beeline | 2G | 25257 | 12321 | 1232 | 12321 | 68 | 864 | 1780.6 | 1875.6 | -71dBm | 56.811835 | 60.620101 |
| 46 | 11.06.2017 | 18:03:45 | Beeline | 3G | 25257 | 56766504 | 1232 | 12328 | 397 | 10788 | 1967.6 | 2157.6 | -84dBm | 56.811835 | 60.620103 |
| 47 | 11.06.2017 | 18:03:45 | Beeline | 3G | | | | | 211 | 10788 | 1967.6 | 2157.6 | -96dBm | 56.811835 | 60.620103 |
| 48 | 11.06.2017 | 18:03:45 | Beeline | 3G | | | | | 389 | 10788 | 1967.6 | 2157.6 | -109dBm | 56.811835 | 60.620103 |
| 49 | 11.06.2017 | 18:03:45 | Beeline | 3G | | | | | 372 | 10788 | 1967.6 | 2157.6 | -109dBm | 56.811835 | 60.620103 |
| 50 | 11.06.2017 | 18:03:45 | Beeline | 3G | | | | | 405 | 10788 | 1967.6 | 2157.6 | -111dBm | 56.811835 | 60.620103 |
| 51 | 11.06.2017 | 18:03:45 | Beeline | 3G | | | | | 203 | 10788 | 1967.6 | 2157.6 | -115dBm | 56.811835 | 60.620103 |
| 52 | 11.06.2017 | 18:03:45 | Beeline | 3G | | | | | 136 | 10788 | 1967.6 | 2157.6 | -111dBm | 56.811835 | 60.620103 |
| 53 | 11.06.2017 | 18:03:45 | Beeline | 3G | | | | | 120 | 10788 | 1967.6 | 2157.6 | -111dBm | 56.811835 | 60.620103 |
| 54 | 11.06.2017 | 18:03:45 | Beeline | 3G | | | | | 195 | 10788 | 1967.6 | 2157.6 | -115dBm | 56.811835 | 60.620103 |
| 55 | 11.06.2017 | 18:03:45 | Beeline | 3G | | | | | 136 | 10788 | 1967.6 | 2157.6 | -111dBm | 56.811835 | 60.620103 |

Статус: ● Сканирование завершено

Figure 5: The main program window with the table



RTU&Scaner GSM/WCDMA/LTE "Енот", v 1.0   ГИП - мобильный пост на базе МКРК

Задача   Прочее

Выберите COM-порт: COM1

Таблица БС | Карта и текущее местоположение

Статус: Программа еще не запускалась

Figure 6: Displaying an offline map of the area

## 6 Conclusion

At the moment, the hardware and software complex the "Enot" is used to analyze the radio-electronic environment in the networks of GSM, UMTS and LTE standards. In conclusion I would like to note the advantages and disadvantages of the developed device, as well as development prospects.

Advantages of the “Enot“:

- Ability to work without an external power source;
- Small size and weight;
- The possibility of assessing the radio-electronic environment in the premises
- The software is modular, portable and universal;
- The software records "logs" in the background, which eliminates the complete loss of measurements;
- The software forms a report in HTML format for further processing without using the “Enot”.

Disadvantages of the “Enot“:

- At the same time, it is possible to analyze the radio-electronic situation in the mobile communication network of only one operator with the SIM card installed. Without a SIM card, the functionality is limited.

Development prospects of the “Enot”:

- Smaller overall dimensions and weight, because a new, more compact board will be designed and batteries with a higher specific capacity will be used;
- Work with all mobile operators at the same time;
- Displays the current location on the map;
- Displays BSs on the map of the area;
- DB with Cell ID of all operators to identify the BS, which are installed with violations of the legislation of the Russian Federation;
- DB with the allowed frequencies of each of the cellular operators to exclude the use of spectrum with violations of the legislation of the Russian Federation;
- Work software in other operating systems (including not only the Windows family)

## References

1. Роскомнадзор – В России на 55% выросло количество базовых станций стандарта LTE [Электронный ресурс] – URL: http://rkn.gov.ru/news/rsoc/news43427.htm (access date: 18.11.2017).
2. Digital cellular telecommunications system (Phase 2+) (GSM); GSM/EDGE Radio transmission and reception (3GPP TS 45.005 version 14.0.0 Release 14) / 3GPP, 2017. – 307c.
3. Universal Mobile Telecommunications System (UMTS); User Equipment (UE) radio transmission and reception (FDD) (3GPP TS 25.101 version 10.1.0 Release 10) / 3GPP, 2011. – 273c.
4. LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception (3GPP TS 36.104 version 13.3.0 Release 13) / 3GPP, 2016. – 183c.
5. Вымпелком. Обзор системы GSM, 2004.
6. SPECIFICATION OF PRODUCT for Lithium-ion Rechargeable Cell Model: ICR18650-26F / SAMSUNG SDI Confidential Proprietary, 2009.
7. G7XX, type b series. new plastic instrument cases / Gainta Industries, 2014.
8. ROHDE&SCHWARZ. Technical information. Active directed antenna from 9 kHz to 7,5 GHz R&S®HE300.