The substitution of concepts in the TSCM

Now there are many radio monitoring systems on the market. They all have many different technical parameters but all of them can do just one thing – to display spectrum of radio signals and (in the best case) retain panoramas in DB.

These programs are not able to solve tasks of analyzing of legal communication channels at all or just simulate that work. There are many different reasons: poor input channel, impossibility to connect device with computer or even unwillingness to accept this problem! Why should we change anything if customer is ready to pay for outdated decisions? However, customer often even does not know that producer offers him moth-eaten devices, which are not able to give him an effective counteraction to up-to-date threats.

But the problem is real!

Let's talk a bit about "classic radio monitoring" which does not solve problems of analysis and protection of digital information transmitted via radio channels. The question is: do we need such monitoring against up-to-date digital clandestine devices of interception of information?

To understand the problem we need to imagine, what is it typical object, which needs protection.

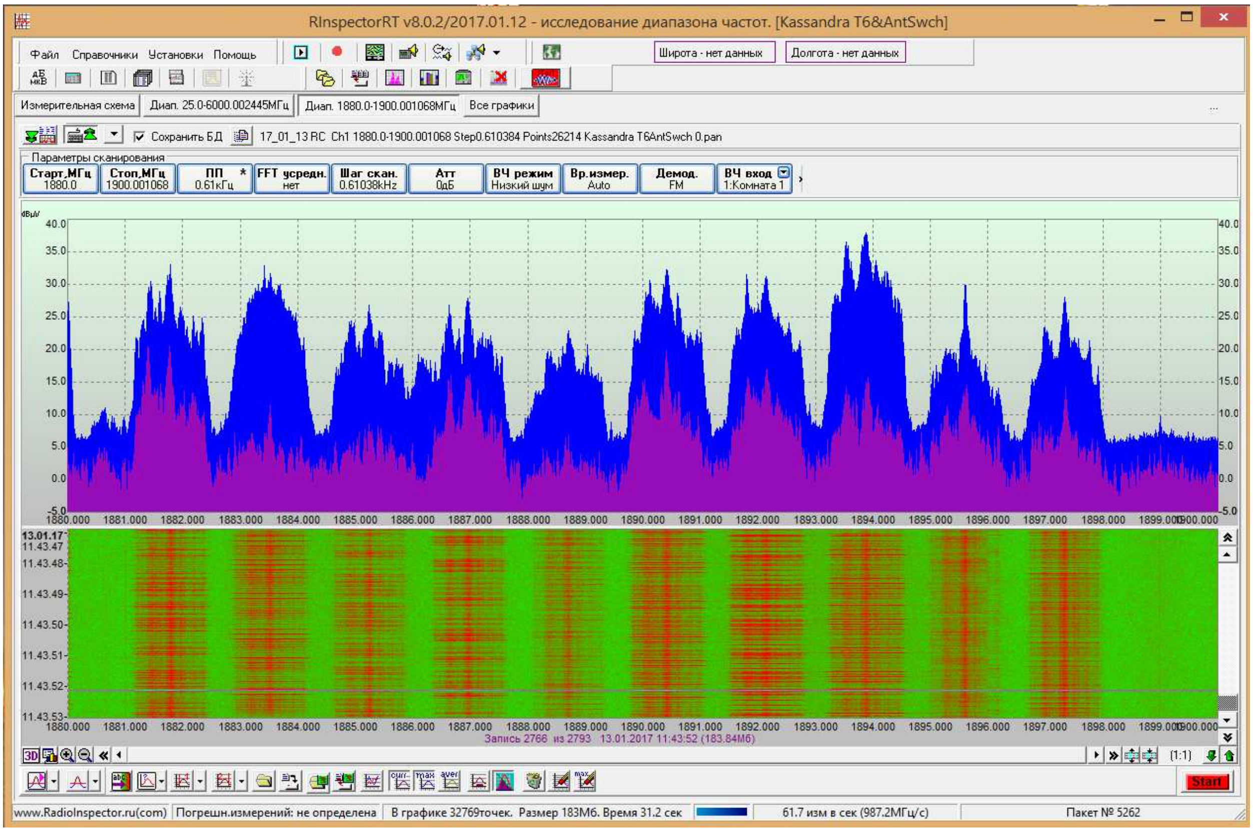
Not necessary to talk about standalone objects somewhere in the middle of a desert. There is very simple decision of the problem – any new radio source or physical object is a threat. We would like to talk about object placed in the center of city, among administrative and private buildings with old and new electronic devices, analog and digital phones, WLANS and so on. In the city where work GSM 2G/3G/4G and UMTS operators, DECT phones, different type of emergency alarms and radio networks etc.

The difficulty of contemporary monitoring is based on such problem that up-to-date illicit "bugs" use the same standards as legal devices placed in the buildings and around them.

Let's look what can do an operator with standard equipment without software for digital analysis.

Here are some examples:

1. What shall you do, when intercept such spectrum diagram like on the Figure 1?
   Figure 1.



RInspectorRT v8.0.2/2017.01.12 - исследование диапазона частот. [Kassandra T6&AntSwch]

Широта - нет данных

Долгота - нет данных

Измерительная схема | Диап. 25.0-6000.002445МГц | Диап. 1880.0-1900.001068МГц | Все графики

☑ Сохранить БД 17_01_13 RC Ch1 1880.0-1900.001068 Step0.610384 Points26214 Kassandra T6AntSwch 0.pan

Параметры сканирования

Старт,МГц 1880.0 | Стоп,МГц 1900.001068 | ПП 0.61кГц | FFT усредн. нет | Шаг скан. 0.61038kHz | Атт 0дБ | ВЧ режим Низкий шум | Вр.измер. Auto | Демод. FM | ВЧ вход 1:Комната 1

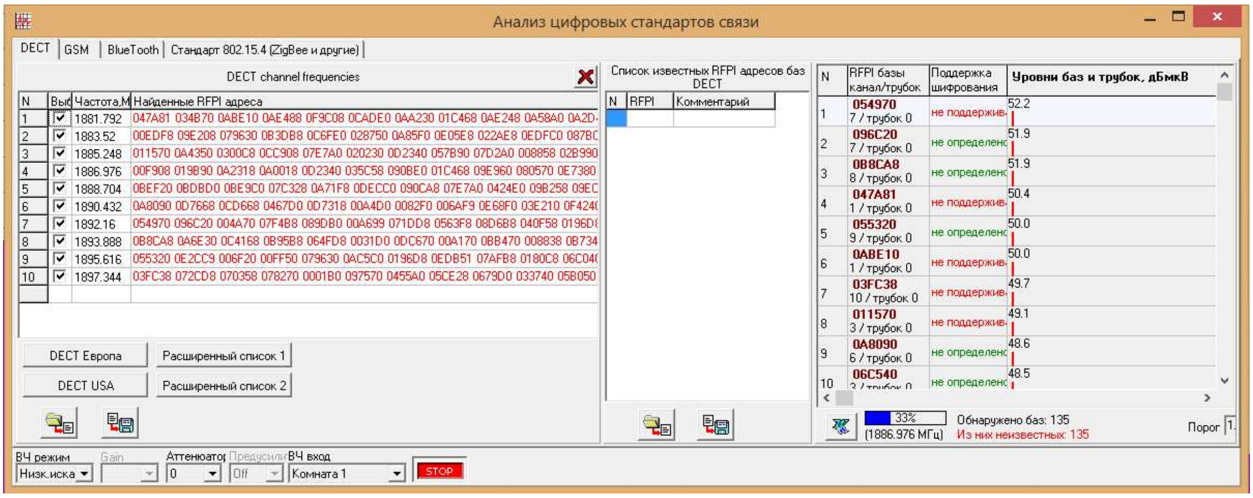
Запись 2766 из 2793 13.01.2017 11:43:52 (183.84Мб)

www.RadioInspector.ru(com) | Погрешн.измерений: не определена | В графике 32769точек. Размер 183Мб. Время 31.2 сек | 61.7 изм в сек (987.2МГц/с) | Пакет № 5262

How can you identify an illicit device, which works on the same frequencies like up to 24 legal devices – 12 DECT bases and phones? DECT standard allows using 10 frequencies like this. It means we can detect up to 240 devices simultaneously! In the vast business centers, very often all 10 channels are busy.

On the Figure 2 you can see an example of detection of 15 DECT bases.

Figure 2.



Анализ цифровых стандартов связи

DECT | GSM | BlueTooth | Стандарт 802.15.4 (ZigBee и другие)

DECT channel frequencies

N	Выб	Частота,М	Найденные RFPI адреса
1	☑	1881.792	047A81 034B70 0ABE10 0AE488 0F9C08 0CADE0 0AA230 01C468 0AE248 0A58A0 0A2D
2	☑	1883.52	00EDF8 09E208 079630 0B3DB8 0C6FE0 028750 0A85F0 0E05E8 022AE8 0EDFC0 087BC
3	☑	1885.248	011570 0A4350 0300C8 0CC908 07E7A0 020230 0D2340 057B90 07D2A0 008858 02B990
4	☑	1886.976	00F908 019B90 0A2318 0A0018 0D2340 035C58 090BE0 01C468 09E960 080570 0E7380
5	☑	1888.704	0BEF20 0BDBD0 0BE9C0 07C328 0A71F8 0DECC0 090CA8 07E7A0 0424E0 09B258 09EC
6	☑	1890.432	0A8090 0D7668 0CD668 0467D0 0D7318 00A4D0 0082F0 006AF9 0E68F0 03E210 0F424
7	☑	1892.16	054970 096C20 004A70 07F4B8 089DB0 00A699 071DD8 0563F8 08D6B8 040F58 0196D
8	☑	1893.888	0B8CA8 0A6E30 0C4168 0B95B8 064FD8 0031D0 0DC670 00A170 0BB470 008838 0B734
9	☑	1895.616	055320 0E2CC9 006F20 00FF50 079630 0AC5C0 0196D8 0EDB51 07AFB8 0180C8 06C04
10	☑	1897.344	03FC38 072CD8 070358 078270 0001B0 097570 0455A0 05CE28 0679D0 033740 05B050

Список известных RFPI адресов баз DECT

N	RFPI	Комментарий

N	RFPI базы канал/трубок	Поддержка шифрования	Уровни баз и трубок, дБмкВ
1	054970 7 / трубок 0	не поддержив	52.2
2	096C20 7 / трубок 0	не определено	51.9
3	0B8CA8 8 / трубок 0	не определено	51.9
4	047A81 1 / трубок 0	не поддержив	50.4
5	055320 9 / трубок 0	не определено	50.0
6	0ABE10 1 / трубок 0	не поддержив	50.0
7	03FC38 10 / трубок 0	не поддержив	49.7
8	011570 3 / трубок 0	не поддержив	49.1
9	0A8090 6 / трубок 0	не определено	48.6
10	06C540 3 / трубок 0	не определено	48.5

33%
(1886.976 МГц)
Обнаружено баз: 135
Из них неизвестных: 135
Порог 1.

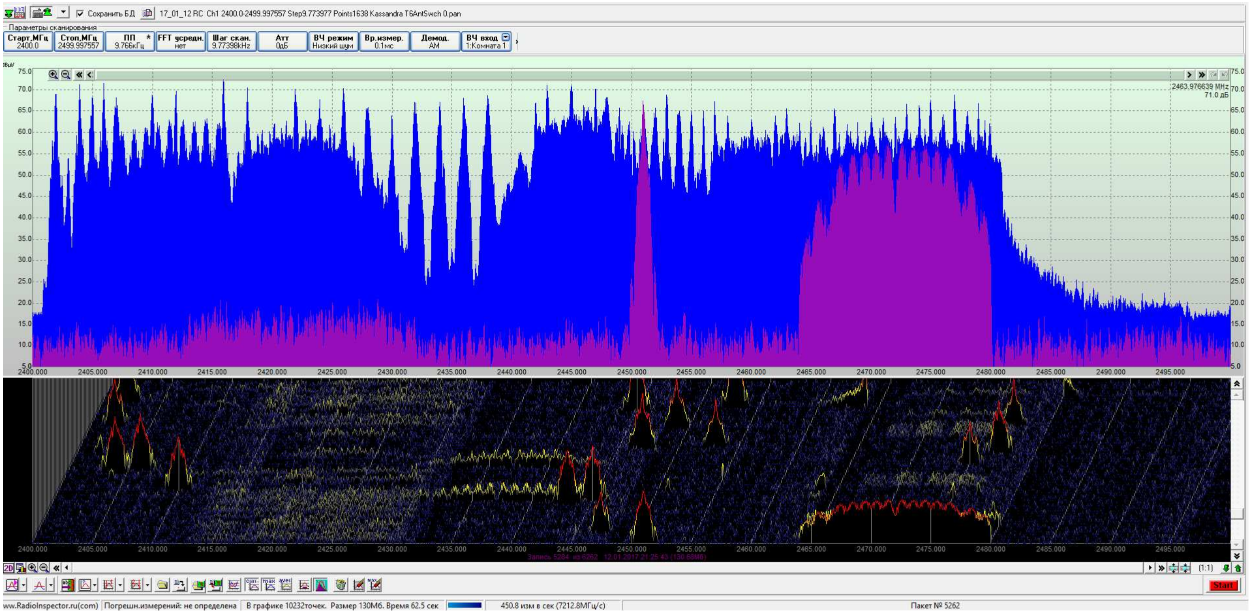
ВЧ режим: Низк.иска
Gain:
Аттенюатор: 0
Предусилитель: Off
ВЧ вход: Комната 1

An operator with big experience can say:

"To localize a clandestine illicit source, I will switch off all DECT devices in the office and look for a source with the most strong signal around me". It is a good idea, but how can you switch off a phone and base in the office near yours, which belongs to another company? In many offices, we have seen stuff continuously moving and speaking by DECT phones throughout many rooms in the building. The strength of signals changed every time. In the night, the situation does not change, because DECT bases work always. As you can see, in this case we should be able to receive, decode and read headers of DECT packets.

Here is another one example – the frequency range 2,4 – 2,5 GHz. WiFi, ZigBee, Bluetooth, quadrocopters (UAV) control, digital and analogue camcorders here they are! There is no better frequency range to hide an illicit radio device! Just look at spectrum on the Figure 3.

Figure 3.



☑ Сохранить БД   17_01_12 RC Ch1 2400.0-2499.997557 Step9.773977 Points1638 Kassandra T6AntSwch 0.pan

Параметры сканирования

Старт,МГц	Стоп,МГц	ПП	FFT усредн.	Шаг скан.	Атт	ВЧ режим	Вр.измер.	Демод.	ВЧ вход
2400.0	2499.997557	9.766кГц	нет	9.77398kHz	0дБ	Низкий шум	0.1мс	AM	1:Комната 1

ww.RadioInspector.ru(com) | Погрешн.измерений: не определена | В графике 10232точек. Размер 130Мб. Время 62.5 сек | 450.8 изм в сек (7212.8МГц/с) | Пакет № 5262

Can you say where a "bug" is? We can't, but it is! The digital analysis only can help us to solve this problem successfully.

Briefly, we can say – nowadays, contemporary TSCM is impossible without a digital analysis of intercepted signals.

The situation like this is actual for a long time and in some cases operators try to solve problem by using digital devices connected to computers via USB. Devices, which are not especially designed for radio interception and does not have a proper sensitivity and selectivity.

In case of radio interception and intelligence, radio-monitoring systems should be developed as all-in-one system. Just try to find in Google “high-power Bluetooth system” and you will find Bluetooth modules with range up to 2 km. This example is for readers, who thinks that Bluetooth is a short range standard.

So, what kind of difficulties are waiting for an operator, who is trying to find a clandestine Bluetooth device? There are more than 10-15 Bluetooth devices can work simultaneously in the premise. The worse situation is in the offices, where people like to use products Apple’s products. These devices often use Bluetooth for interconnection, because it is very convenient for users. In the same room can work many other Bluetooth gadgets. Even security can use Bluetooth garniture connected to portable radio stations. How can we differentiate legal and illicit sources? Furthermore, “bug” can be placed in the same place where works a legal source, has the same strength of signal, and receiver is mounted in an adjacent premise, but owner of this room is another company.

The implication is one – without analysis of headers of Bluetooth packets and collecting LAP-addresses of devices which work in the controlled area, it’s practically impossible to find illegal source.

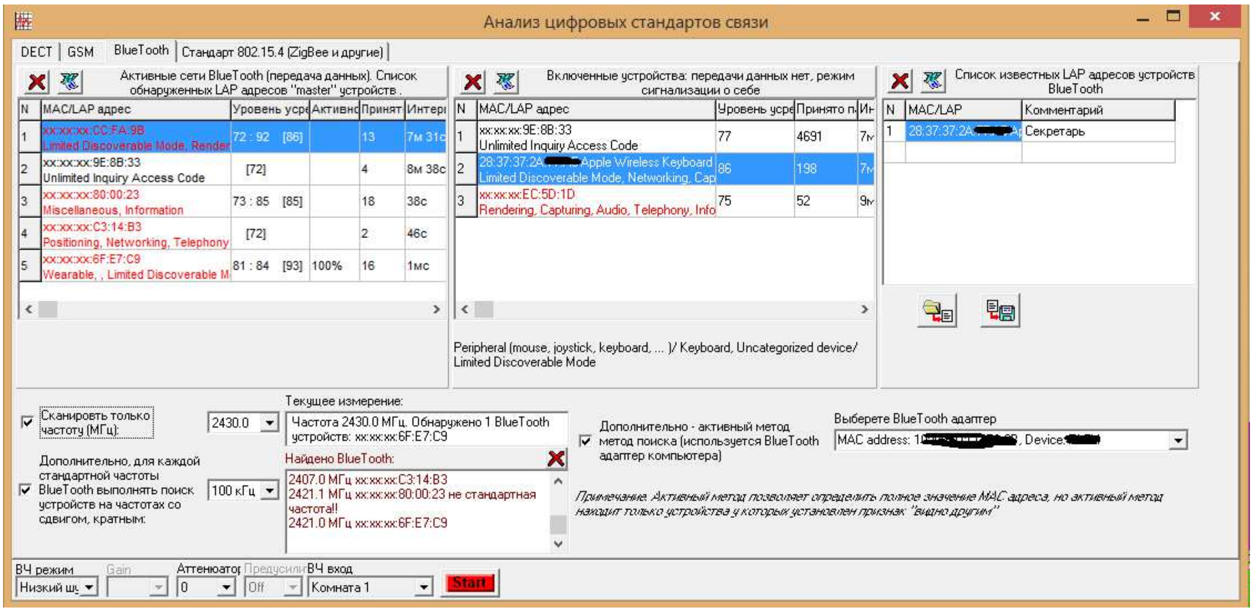
Why LAP, not MAC address?

Here is an important moment – the substitution of concepts. To understand this case we should to remember, that Bluetooth devices which has been interconnected with each other once and do not work in discoverable mode, don’t broadcast their MACs. For example, if your Bluetooth keyboard was connected to the laptop or Bluetooth headset was connected to the mobile phone, they will not broadcast MACs. If your spectrum analyzer is able to detect MACs only, you will not detect such devices as above. It means you will not find a bug connected to the receiver that is located in another room or even in another building.

Here is a worse situation - a year ago, we have found a Bluetooth device did not founded by Bluetooth analyzer. Only RadioInspector with spectrum analyzer Kassandra have detected device by it’s spread spectrum emission in Bluetooth frequency range. This problem forced us to study intercepted signal deeper. The implication was unpredictable and very unpleasant for users of standard Bluetooth analyzers – the frequency of work this device was shifted more than 100 KHz and this device now is invisible for standard analyzers of digital channels.

We revised algorithms of work of our digital analyzer – DTest. Now it able to work in different modes and detects devices with standard frequency range, with arbitrary frequency range and with shifted frequency relatively to standard frequency range.

Figure 4.



Анализ цифровых стандартов связи

DECT | GSM | BlueTooth | Стандарт 802.15.4 (ZigBee и другие)

Активные сети BlueTooth (передача данных). Список обнаруженных LAP адресов "master" устройств .

N	MAC/LAP адрес	Уровень усре	Активно	Принят	Интер
1	xx:xx:xx:CC:FA:9B Limited Discoverable Mode, Render	72 : 92 [86]		13	7м 31с
2	xx:xx:xx:9E:8B:33 Unlimited Inquiry Access Code	[72]		4	8м 38с
3	xx:xx:xx:80:00:23 Miscellaneous, Information	73 : 85 [85]		18	38с
4	xx:xx:xx:C3:14:B3 Positioning, Networking, Telephony	[72]		2	46с
5	xx:xx:xx:6F:E7:C9 Wearable, , Limited Discoverable M	81 : 84 [93]	100%	16	1мс

Включенные устройства: передачи данных нет, режим сигнализации о себе

N	MAC/LAP адрес	Уровень усре	Принято п	Ин
1	xx:xx:xx:9E:8B:33 Unlimited Inquiry Access Code	77	4691	7м
2	28:37:37:2A[redacted]Apple Wireless Keyboard Limited Discoverable Mode, Networking, Cap	86	198	7м
3	xx:xx:xx:EC:5D:1D Rendering, Capturing, Audio, Telephony, Info	75	52	9м

Peripheral (mouse, joystick, keyboard, ...)/ Keyboard, Uncategorized device/ Limited Discoverable Mode

Список известных LAP адресов устройств BlueTooth

N	MAC/LAP	Комментарий
1	28:37:37:2A[redacted]Ap	Секретарь

☑ Сканировть только частоту (МГц): 2430.0

Текущее измерение:
Частота 2430.0 МГц. Обнаружено 1 BlueTooth устройств: xx:xx:xx:6F:E7:C9

Дополнительно, для каждой стандартной частоты
☑ BlueTooth выполнять поиск устройств на частотах со сдвигом, кратным: 100 кГц

Найдено BlueTooth:
2407.0 МГц xx:xx:xx:C3:14:B3
2421.1 МГц xx:xx:xx:80:00:23 не стандартная частота!!
2421.0 МГц xx:xx:xx:6F:E7:C9

☑ Дополнительно - активный метод метод поиска (используется BlueTooth адаптер компьютера)

Выберете BlueTooth адаптер
MAC address: 1[redacted], Device:[redacted]

Примечание: Активный метод позволяет определить полное значение MAC адреса, но активный метод находит только устройства у которых установлен признак "видно другим"

ВЧ режим: Низкий шу | Gain | Аттенюатор: 0 | Предусили: Off | ВЧ вход: Комната 1

Pay your attention to one of MAC addresses in the middle column of the table, it is the only one device which could be detected by contemporary digital spectrum analyzers of the most developers. In this case we can see

an Apple's keyboard. In the left table we can see "invisible" devices. They don't broadcast full MAC addresses to the network because they already established interconnection: a keyboard, mobile phone and headset and proverbial device with shifted RF beyond standard Bluetooth frequency range.
Operators, who practices TSCM, should to take note, that LAP address 9E:8B:33 which is displayed at the end of string is just a broadcast request "give me your address" for any devices around. In our case, this request have sent by notebook's Bluetooth adaptor of radio monitoring system Kassandra especially for clandestine devices detection. If you don't use an active search mode, but request like this is present in the table, it means there is any other device is looking for connection in your premise. For example, two men are trying to send a file to via Bluetooth from one device to another.

Digital analysis by spectrum?
Another one example of substitution of concepts – in some TSCM systems the digital analysis is presented by signal detection in a specific frequency range only. For instance, we can't understand, how the signal intercepted on the frequency range 1920 – 1980 MHz is recognized like UMTS2100 or signal intercepted on the FR 3400 – 3700 MHz is Wi-Fi?
Where is such confidence from?
In fact, it is impossible to decide what kind signal was intercepted without real digital analysis of I/Q data.

DMR, Tetra, APCO…
Very important channel of information leakage is trunked radio used by security stuff. It seems strange, what kind of influence has trunked radio onto information confidence? What about password interception or eavesdropped part of confident conversation?
How does it become possible? Nowadays radio uses digital channels for interconnection! Yes, and here is the newest problem! Digital standards have many good decisions, but they have vulnerabilities too.
The first and the most important problem is drivers inside radios – you never be assure what kind of "surprises" has software installed into your mobile station. Nowadays the most popular digital standard is DMR. Very convenient digital standard allows interconnect two groups of speakers simultaneously in direct (DMO) and/or trunked (TMO) modes. An encryption and SMS are supported too. The "police mode" realized by using DMO, this function is very interesting for us, because it allows switching on needed radio station and forcing it to transmit eavesdropped information. Meanwhile drivers allow switching off any indicators on the radio to hide this mode. Duration of "police mode" of Motorola mobile radio can be up to 2 minutes.
The most interesting case we encountered in our work was "police mode" on the one of the Motorola's radio placed in the car of one important person of a big company. It was impossible to understand which of stations transmits information and localize it. Only digital analysis helped us to determine that one of radios uses second timeslot to transmit eavesdropped information.
That is why we work hard to improve DTest to analyze security radio channels:
- the possibility to demodulate APCO, TETRA, DMR without encryption;
- the IDs of radio stations.
We insist that radio channels of security forces must be under control 24-hours a day not only for radio exchange tracking. Impossibility to analyze the whole structure of radio exchange by contemporary radio control system, from our point of view, is unforgivably carefree.