УДК 004.056
DOI: 10.31673/2409-7292.2020.043340

Kikot O.M., Pravdyvyi A.M., Kornienko S.V., Ozerinin F.O., Zozulia S.A.

ANALYSIS AND DEVELOPMENT TRENDS OF DEVICES FOR FINDING ILLEGAL MEANS OF OBTAINING INFORMATION

This article raises the issue of leakage or loss of information, which can lead to material damage or catastrophic consequences. The analysis of search devices of secret reception means of information different on the principle of work, and methods of search of secret reception means of information is carried out. According to the analysis, we can conclude that the process of finding means of covert receipt of information at the present stage of society qualitatively development goes to another level. Therefore, the search methods and equipment used for this need to be improved, and the problem of analyzing the means of finding means of covert information in order to identify trends and develop modern requirements for them becomes relevant. Methods of concealing the work of secret means of obtaining information used in their development are studied. It should be noted that today it is much easier to make a digital transmitter, using the modern element base of standard means of communication, than to create and configure an "analog" bookmark on a transistor with positive feedback. That is why the possibilities of modern means of obtaining information secretly are influenced by the latest and promising technologies. The latest means of covert information retrieval (radio bookmarks) have the ability to use a variety of methods to hide the data channel, which significantly complicates the process of finding them. In particular, in the case of their use of combined methods of hiding the data channel. Taking into account the latest developments in the field of hidden information, a complete methodological set of requirements for regional design and creation of modern automated search systems, which, in turn, fully meet the process of modern automated search of digital radio bookmarks. These requirements can be used as a technical task in the design of automated software for searching digital radio bookmarks.

Key words: information, radio monitoring, analysis, automated software package, search devices.

Introduction

As the importance and value of information grows, so does the need to protect it. We can approach this question from two aspects. In one aspect, the information has a material value, respectively, its leakage or loss can cause material damage. Approaching this question from the second aspect of information is management. Unauthorized interference with management can have dire consequences. As of today, the issue of information security is extremely relevant. The number of used equipment continues to grow, and hence the importance of organizational work and software and hardware protection against information leakage.

The leakage of information from the technical channel means the uncontrolled spread of information from the information carrier, which is protected through the physical environment, to the technical means that intercepts information.

Depending on the physical nature of information signals and the environment of their propagation, technical channels of acoustic (speech) information can be divided into direct acoustic (air), acousto-vibration (vibration), acousto-optical (laser), acoustoelectric (parametric) [1]. Moreover, most often the leakage of information occurs during its transmission over the radio channel. That is why the methods of neutralization and search of radio channels of means of covert receipt of information (MCRI) at the present stage of development are becoming more relevant.

Analysis of literature data and problem statement.

A significant number of publications are devoted to the search for MCRI radio channels and their localization.

Thus, in [2] the issues of search and localization of radio bookmarks by the ‘classical’ method with the help of universal devices, field indicators and more are considered. This technique has previously met the needs of MCRI search. The devices described in this technique are very, very difficult to detect and localize MCRIs that operate in the digital range. Therefore, it is necessary to improve the methodology and use other search techniques.

In [3] the tendencies of development of radio bookmarks are considered. Technical developments are becoming more sophisticated, algorithms for transmitting information (mostly digital) allow you to create stable, unobstructed communication channels at much higher frequencies than before. Conditions for the propagation of radio waves do not seem to be such a big obstacle. Radio relay stations, for example, use a range close to hundreds of gigahertz, and in the

range of 5 GHz organized broadband access with gigahertz traffic. Based on this, search engines operating in the range up to 3 GHz no longer meet modern needs and need improvement or replacement.

[4] discusses the Wi-Fi technology used in various wireless telemetry systems in transport. Virtually all wireless camcorders and speed recorders installed on highways use Wi-Fi. This technology is also used to organize local area networks between buildings and industrial facilities. It should be emphasized that the Wi-Fi band of 5 GHz is the best for the organization of industrial local area networks in the presence of high-level interference. It is proved that it is impossible to analyze this frequency range by the 'classical' search method. That is, to search for MCRI, you need to use other methods. The method of localization of radio bookmarks in the range of Wi-Fi works is considered. But it is used separately and is not part of the search engine.

[5] analyzes the complexity of modern radio monitoring in the interests of information protection. The problem is that modern embedded devices with the transmission of information over the air channel increasingly use the same standards for the transmission of information as devices that are legally in the premises. Therefore, the former methods of radio monitoring are not able to identify embedded devices operating under the guise of legally operating devices. New devices and techniques need to be developed to search for MCRIs operating in the legal frequency bands.

The above factors allow us to conclude that at the present stage of development of society, the process of finding MCRI goes to a qualitatively different level. Therefore, the search methods and equipment used for this need to be improved, and the problem of analyzing the search tools of digital radio bookmarks in order to identify them, trends and development of modern requirements for them is very relevant.

Presenting main material

At the present stage, the search for MCRI radio channels is complicated by several factors.

First, MCRI developers are using increasingly sophisticated methods and algorithms to hide the radiation of their products. At the stage of MCRI installation, special masking methods are used, for example, a channel is created to capture information taking into account the radiation of legal means working near the object, which interfere with the search equipment.

Secondly, the use of radio for communication, data transmission and control commands continues to increase. Now almost the entire radio frequency spectrum is involved in the work of legal radio transmitters. This complicates the air situation, especially in large cities.

Based on the above, it is possible to conclude that the developers of modern MCRI with the transmission of information over the air are moving to digital standards that are very close to legal or in the legal range of radio.

You can give an example of a typical institution where inspections are conducted. Dozens of computers, DECT cordless phones, mobile phones of various standards (only in Kyiv there are 5: CDMA-2000, GSM-900/1800, 3G (UMTS), 4G (WiMax)), mobile communication amplifiers (in some buildings) amplifiers of all standards are already found), legal radio microphones, wireless headsets, Wi-Fi devices, various electronic readers of access control and management systems, leading security video cameras (which often have EMPI levels commensurate with the radiation of radio bookmarks), etc. We must not forget about the 'quality' of modern electronic equipment, some switching power supplies, which are 'visible' on the air sometimes up to 500 MHz. Add to all this diversity all that "arrives" in the room from the outside - TV and radio (including digital TV DVB), aviation negotiations, radio babysitters, amateur radio, departmental communication channels, all more active goes to digital standards (example - APCO P25, TETRA, DMR), data transmission, telemetry, even astronauts and satellites, transmit meteorology. You can even accept them while on the premises. As an example, in Kyiv in the range up to 3000 MHz, depending on the area and reception conditions, you can detect more than 3500 radio signals.

Conducting an abbreviated analysis of MCRI search tools in the current literature, the search tools data are shown in Table 1.

It can be concluded that the main frequency bands of these tools are ELF (30-300 MHz) plus ULF (300-3000 MHz), ie they can not fully analyze the digital packets in relation to the tasks of

search radio control. This proves that the range of technical devices has already gone beyond analog radio signals. The current trend of technology proves that the range of work is moving to the digital range.

Table 1.

Frequency range of search tools MCRI

MCRI search tools	Basic search range	The presence of the device to increase the frequency range
Field detectors		
NR-D	50-3500 MHz	
ST-110	50-2500 MHz	Antenna-converter into 7 GHz
SEL SP-75 Black Hunter	100-3000 MHz	
Universal search devices		
ST-033 ‘Piranha‘	30 kHz -2500 MHz	ST 03.SHF до 10 GHz
ST-131 ‘Piranha -2’	30 kHz -4100 MHz	ST 131.SHF до 18 GHz
CPM-700	200 Hz - 3 GHz	BMP-1200 до 12 GHz
Scanning receivers		
AOR 8200	30 kHz -3000 MHz	
Scorpion-XL	30 kHz -2500 MHz	
Contour	30 kHz -2500 MHz	
Hardware and software complexes of radio monitoring		
‘Kassandra-M’	24 kHz -3000 MHz	UHF-converter up to 18 GHz
OMEGA	25 kHz -3000 MHz	OMEGA-K18 to 18 GHz
OSC-5000	10 kHz - 3 GHz	MDC-2100 to 21 GHz
KRONA	30 kHz -3000 MHz	UHF-converter to 18 GHz
RS digital Mobile	50 kHz -2000 MHz	UHF-converter RS/DC to 12 GHz
Delta 2000/6 Real-time	40 kHz -6000 MHz	

To determine the requirements for MCRI search engines, we will briefly consider the methods of hiding the work of radio bookmarks used in the development of such devices. At once we will note that now it is much easier to make the digital transmitter, using a modern element base of standard means of communication, than to design and adjust ‘analog’ bookmark on the transistor with positive feedback. Therefore, modern and promising requirements for the complexes of search for means of covert recording of information follow from the analysis of the capabilities of modern digital data transmission.

Modern radio bookmarks can use the following methods of hiding the data channel:

methods of information accumulation and its discrete transmission in short periods of time (up to several milliseconds);

methods of accumulation of information for a long time with the subsequent transfer at the appointed time or upon receipt of an external command;

periodic or chaotic adjustment of the frequency of the radiation channel;

use of broadband signals, when the signal energy is distributed in a wide frequency band and the signal does not have a pronounced excess over noise;

implementation of noise-like bookmarks, which use special coding algorithms that allow stable reception of information with a negative signal-to-noise ratio at the location of the receiver;

selection of radiation frequency along with powerful sources of legal signals that overload the receiving paths of search equipment with insufficient dynamic range or masked by the spectrum of the legal signal with insufficiently low phase noise of radio paths of search complexes;

masking under standard communication channels and / or operation of narrowband radiation within the spectrum of legal broadband signals;

use of standard communication channels such as GSM, CDMA, WiFi, BlueTooth.

The methods used can be combined with each other. For example, the use of signals from over a wide bandwidth can be combined with the method of information accumulation and discrete transmission, etc.

Radio bookmarks that use methods of information accumulation and discrete transmission, radiation frequency adjustment and remote control can be reliably identified only by unmasking features in the space amplitude-frequency-time. No matter how complex algorithms for hiding the data channel are not used in bookmarks, they still unmask themselves with a certain pattern (frequency) of broadcasting. These unmasking features of radio bookmarks are detected by the operator when performing a temporary analysis of the radio frequency spectrum. It is the frequency and time regularity of bookmarks that differ from random bursts of industrial noise in the radio, which an inexperienced operator can take for a bookmark. When searching for such radio bookmarks, it is not a question of instant detection. For their reliable detection, radio monitoring is required for a long time: up to a day or more, followed by analysis of all measured panoramas in the time plane in the presentation of the spectrogram ('waterfall'). Based on these considerations, there are requirements for algorithms that must be implemented in the software of the automated complex.

Regarding the detection of broadband and noise-like bookmarks, we note the following: the method of their detection is based on the fact that in the near zone the signal-to-noise ratio even at such transmitters will be above zero, From this it is possible to formulate requirements for receiving means of radio monitoring complexes: in order to monitor the change of noise level against the background of strong signals, the receiving means must have good sensitivity and a wide dynamic range (not less than 80-90 dB). The thesis that the dynamic range in radio monitoring systems is not so important, as the bookmarks in the near zone have a high signal power and therefore you can use an attenuator, which is unacceptable in the case of searching over broadband and noise signals. The situation when a legal means of communication works together with a bookmark in the preselector band, the signal level of which exceeds the bookmark level by 70-90 dB, is not uncommon at present. The 70-90 dB level is a very high signal level that can overload many radios. If the signal exceeds the level of the dynamic range of the receiving path, the panorama of the signals will display many false side and combination signals, which are extremely unstable in frequency, amplitude and time. The experience of acquaintance with a number of radio monitoring systems presented on the market, with the formal compliance of the parameters of their dynamic range with the search requirements, revealed that they are easily overloaded by a simple transmitter such as 'Walkie-Talkie'. Naturally, in the presence of a large number of erroneous signals, it is not necessary to speak about quality of search of embedded devices.

To search for 'tricky' bookmarks that are disguised as a spectrum of legal signals or to search for narrowband signals that can hide in the spectrum of legal signals, the radio monitoring system must have the means to study the spectra of signals with resolution in Hertz. Of course, the experience of the operator and his intuition are crucial here. However, the hardware and software of the complex must allow the operator to perform such tasks.

Finally, for identification when searching for embedded radio devices using standard communication channels, such as DECT, GSM, CDMA, WiFi, BlueTooth, in addition to work on the identification of these transmitters by analyzing the appropriate frequency bands, the radio monitoring system must have additional network analysis that allow you to detect 'foreign' MAC addresses or identify 'foreign' subscriber devices for those networks for which this is possible.

It should be noted that there are no separate devices for the analysis of digital packets in relation to the task of search radio control. The first attempt to create a software tool (ST) for demodulation and analysis of digital radio communication devices can be considered a digital signal processing package in ST DigiScan software and in ST 'Radio Inspector Soft ™'.

ST 'Radio InspectorSoft ™' has found its further application in the automated search complex (ASE) 'Kassandra'.

ASE ‘Kassandra’ with ST RadioInspector provides the operator with the following opportunities:

long-term control of the frequency range (s), collection, storage and display of data on the state of the radio frequency spectrum for the entire measurement time (spectrogram or ‘waterfall’ without restrictions on the size of the measurement data);

use of the database of frequency assignments, threshold line, list of signals exceeding the threshold line;

recording and analysis of demodulated audio signal, forming a task to record demodulated audio signal when the threshold line is exceeded;

control of another scanning receiver as a means of audio control without stopping scanning by the main receiver (tuning to frequency, listening and recording of demodulated audio signal without stopping scanning);

control of the scanning receiver over the network, transmission of demodulated audio signal over the network in real time;

control of Wi-Fi wireless communication devices;

monitoring of devices of Wi-Fi networks in the 2.4 / 5 GHz bands with the possibility of autonomous, round-the-clock collection of information with subsequent transmission of the accumulated information over the LAN;

real-time operation with signal analysis DECT, GSM, Bluetooth, TETRA, APCO 25, DMR, IEEE 802.15.4 (ZigBee), UMTS (3G).

The appearance of the hardware search complex ‘Kassandra’ is shown in Figure 1.

Fig.1. Appearance of search ASE Kassandra with ST ‘RadioInspektorSoft ™’

As you can see from the description, the complex with ST ‘RadioInspectorSoft ‘ allows you to perform almost all tasks of searching for digital radio bookmarks, but the disadvantage of this complex and ST is its modularity, which does not allow searching in full, you must optionally purchase additional modules such as RadioInspectorWI-FI, DTest (Digital Test), etc. The operator needs to work in different software environments, there is no so-called ‘single window’ for finding radio bookmarks. ASE DeltaX, which is an extension of ASE from ST DigiScan, is devoid of this drawback.The developer has improved ST DigiScan, supplemented by its ability to demodulate and analyze signals operating in the standards DECT, GSM, Bluetooth, Wi-Fi, TETRA, perform demodulation and display of analog TV signal, including using the method of inversion of clock pulses, demodulate analog AM and FM signals in the frequency band from tens of hertz to several megahertz, trying to meet the above requirements in full. The result of these improvements was ASE with ST ‘Delta 2000/6 Real-time X Advanced’. [6] The appearance of the complex is presented in Figure 2.

Fig.2. Appearance searchable ASE with PM ‘Delta 2000/6 Real-time X Advanced’.

Today, the automated search complex based on ST DeltaX is the most advanced complex, it allows you to search for digital radio bookmarks, demodulate, analyze, identify and locate base stations and mobile devices. This ASE is close to optimal, but its ST does not use vector analysis to search in full. That is, not enough attention is paid to vector analysis and automatic direction finding of digital radio bookmarks.

The analysis would not be complete without considering the AKOR complex.

AKOR-2PK (Fig. 3) is the second generation of universal professional search and measuring systems of the AKOR series and is intended for MCRI search, it is characterized by the following features: use as a computer modern ST allows to improve the software of the complex and expand its functionality for radio monitoring; detection of low-power digital devices; detection of technical channels of information leakage from personal electronic computers; high automation of all processes of detection of technical channels of information leakage on parasitic electromagnetic radiation (PEMR); the presence of a sound correlator to detect parasitic modulation of PEMR by a speech signal; the presence of a set of filters with a bandwidth of up to 1 Hz, which allows you to measure signals below the noise level; universality, because it combines the functions of two complexes: search - for radio monitoring and search of radio interception devices and measuring - for detection and measurement of PEMR (two in one!); ease of control and switching from the search mode of the complex to the measuring and back.

Fig.3. Appearance of search engine ASE AKOR-2PK

This ASE is superior to the above-described complexes for detecting technical channels of information leakage by PEMR, but is inferior to them in spectral analysis and localization of digital radio bookmarks.

Summarizing the above considerations, we can formulate requirements for a modern and promising complex of radio monitoring.

1. The modern ASE complex must have sufficiently high-quality analog and digital signal processing paths, so that the presence of extraneous powerful signals does not prevent it from detecting over broadband and noise-like signals. In the tactical and technical characteristics of radio receivers, compliance with these requirements is reflected in such characteristics as sensitivity and dynamic range.

With the development of technology, these characteristics will improve. The starting point can now be taken as the characteristics of modern measuring receivers with a sensitivity of at least 160dBt (1 Hz) and a dynamic range of at least 85 dB at a frequency of 1 GHz.

2. The modern complex of radio monitoring should have rather high-quality and multipurpose software which should allow to carry out the following functions:

perform round-the-clock radio monitoring of the specified frequency bands and store all the results of panorama measurements for further temporal analysis;

provide analysis of amplitude-frequency-time representation of radio monitoring results in real time and in deferred mode;

allow detailed analysis of signal spectra with resolution in Hertz units;

examine the radiation of standard, open Wi-Fi and BlueTooth communication channels for the presence of "foreign" subscriber stations;

perform analysis of signals on a vector diagram;

carry out direction finding of unknown sources of radio signals.

In addition, the software must support search methods that have become "traditional" and widely used in practice:

spaced antenna method;

method of comparison with the reference panorama;

use of a selective threshold line and formation of the list of signals which have exceeded a threshold line;

detailed analysis of the characteristics of the spectra of received signals up to 6 GHz;

automatic recording of phonograms and low-frequency analysis of the demodulated audio signal.

Unctionality, ergonomic characteristics and software development of all MCRI search systems are the most relevant today, because, of course, the search for modern radio bookmarks is an intellectual struggle between the developer of such tools and the operator that performs bookmark search. Software is a search tool and how functional and convenient it is largely determines the result of work.

Summary

The analysis of devices and software complexes of search of means of secret reception of the information which has shown absence in the market of the automated software complexes which allow to solve problems of the automated search of digital radio bookmarks in full is carried out.

Taking into account the peculiarities of modern developments of means of secret information retrieval, a complete methodological set of requirements for the design and creation of modern automated search systems that meet the process of modern automated search of digital radio bookmarks in full. These requirements can be used as a technical task in the design of automated software for searching digital radio bookmarks.

Further research should focus on improving the software for automated software, studying the positive aspects and improving the methodology of their use.

References

1. Anansky E.V.chto such radio tabs and how to find them? (part2) / Journal "Security Service" [Electronic resource] access mode: http://www.kvirin.com/articles/267/
2. Krivtsun A.V. The use of new possibilities of the radio monitoring and digital analysis complex of "Kassandra-M" signals for the detection of modern special technical means with the transmission of information over the radio channel [Electron resource] / A. V. Krivtsun, A. V. Zakharov // access mode: http://www.inspectorsoft.ru/article.php?id=388
3. Zakharov AV Requirements for a prospective analyzer of Wi-Fi networks [Electronic resource] - Access mode: http://www.analitika.info/stati3.php?page=1&full=block_article241 (25.05.2019).
4. Vlasov A. Wireless office communication: DECT and Wi-Fi. [Electronic resource]. - Access mode: http://www.dect.ru/dect.html (05.05.2016)
5. Search complexes. [Electronic resource]. https://www.das-ua.com/documents/catalog/search-appliances/search-complexes/page-01.php (05.03.2019)
6. Laptiev O.A., Musienko A.P., Sobchuk V.V., Borsuk B.M. Method of selecting the optimal radio monitoring input signal for Fourier transform-based software. Scientific periodical of the Control, Navigation and Communication System, Poltava: PNTU,4(56),2019, C.135 – 141.
7. Laptiev O.A., Fedorenko R.M., Berestov D.S. Improving the technique of searching for digital radio bookmarks in the Wi-Fi range. Collection of scientific works of the Center for Military Strategic Studies of Ivan Chernyakhovsky NUOU, №2(66),2019., C102 – 10.
8. Laptiev O.A. Methods of detection and localization of means of covert receipt of information working in the digital range. Modern information protection: scientific and technical journal. K .: DUT, 2019. № 2(38)., C 25 – 31.
9. Oleksandr Laptiev, Anatoliy Biehun, Spartak Hohoniants, Rostyslav Lisnevskyi, Andrii Pravdyvyi, Serhii Lazarenko. Method of detecting signals of means of covert obtaining of information on the basis of approximation of T-spectrum. The Intelligent Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 10, Oktober 2020, pp 6835-6841 Scopus.
10. Oleksandr Laptiev, Vitalii Savchenko, Ivan Ablazov, Rostyslav Lisnevskyi, Oleksandr Kolos, Viktor Hudyma. Method of detecting random signals based on determining the deviations of the main parameters of radio signals. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE). Volume 9 No. 5 . September-Oktober 2020. pp.9204 – 9209. Scopus.

Надійшла: 11.11.2020 Рецензент: д.т.н., професор Гайдур Г.І.