Threats and risks to information security: A practical analysis of free access wireless networks

Daniel I. Quirumbay*[a], Iván A. Coronel [a], Marcia M. Bayas [a], Ronald H. Rovira [a], Konrad Gromaszek[b], Akmaral Tleshova [c], Ainur Kozbekova[d]
[a]Universidad Estatal Península de Santa Elena, Ave La Libertad, Libertad, EC240250, Ecuador; [b]Lublin University of Technology, ul. Nadbystzrycka 38D, 20-618 Lublin, Poland; [c]M.Kh. Dulaty Taraz State University, Taraz, Kazakhstan; [d]Institute of Information and Computational Technologies, 125, Pushkin St., 050010, Almaty, Kazakhstan

ABSTRACT

Nowadays, there is an ever-growing need to investigate, consult and communicate through the internet. This need leads to the intensification of free access to the web in strategic and functional points for the benefit of the community. However, this open access is also related to the increase of information insecurity. The existing works on computer security primarily focus on the development of techniques to reduce cyber-attacks. However, these approaches do not address the sector of inexperienced users who have difficulty understanding browser settings. Two methods can solve this problem: first the development of friendly browsers with intuitive setups for new users and on the other hand, by implementing awareness programs on essential security without deepening on technical information. This article addresses an analysis of the vulnerabilities of wireless equipment that provides internet service in the open access zones and the potential risks that could be found when using these means.

Keywords: Computer security, IT audit, ethical hacking, cybercrime, 802.11 protocol, pentesting

1. INTRODUCTION

In the last decade, the use and supply of wireless networks have experienced a substantial increase throughout Ecuador. Public and private organizations provide the Internet service in different places. One can find free access to the web in shopping centers, dance clubs, hairdressers, and even in public transport. Such an increase means a technological progress, which has a dual effect on society. On the one hand, wireless networks contribute significantly to improving the welfare and standard of living, but on the contrary, lack of security policies exposes users to risks, that might affect the physical and logical integrity.

Establishing a system of security measures in communication by radio waves is a difficult task. Today, organizations cannot find reliable means of transmitting information in a wireless network. Thus, the probability that an unauthorized person, even without being an expert, of intercepting the information or access personal data is also increasing.

A protocol such as Wireless Protected Access (WPA or WPA2) allows improving accessibility parameters. However, some reports suggest the presence of vulnerability of these protocols. Ijeh[1] suggested that the WEP protocol, based on the encryption algorithm RC4, is not safe[2]. Since this protocol is one of the most widely used in open access wireless networks, then data security is compromised. On the other hand, despite the fact that engineers of WPA have adopted a system of key management or Temporal Key Integrity Protocol (TKIP) and the keys are generated by a server there is still an opened gap for cyber-attacks.

Based on technical criteria, some authors argue that wireless communication protocols based on the 802.11 standards are not safe. This situation creates an atmosphere of uncertainty among this protocol users. By an authentication server with a string of 256 bits or a sentence of 8 to 63 characters, PSK provides an alternative to 802.1x PMK generation[3]. However, the most glaring weakness of the 802.11 standards is revealed by frequent attacks on the key PSK of WPA / WPA2. Even though, the new protocols do not yet show a good mechanism to protect information, some researchers [3-4] have suggested that there may be the feasibility of improving security with the WPA2 protocol in combination with the Advanced Encryption Standard encryption process (AES) to avoid cyber-attacks in wireless networks[5].

Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2017, edited by Ryszard S. Romaniuk, Maciej Linczuk, Proc. of SPIE Vol. 10445, 104452R
 · doi: 10.1117/12.2281227

The overall increase in the use of mobile devices, especially the smart ones, is an undeniable fact today. This trend will only continue to grow. According to forecasts by researchers from Cisco Visual Networking Index (VNI), in 2020, 50 billion smart objects can be connected to wireless networks[6]. Therefore, the number of users who remain permanently online also increases. Such continuous connectivity leads to both positive as well as negative aspects to the analysis of computer security.

According to the Internet Crime Complaint Center (IC3), in its report Internet crime 2015, they received 7,838 complaints of fraud through social engineering and interception of emails from people working with suppliers and transactions line. These crimes generated losses greater than $ 263 million[7]. In Latin America about cybercrimes, according to information provided by the Computer Crime Observatory Latin American ODILA 83% of reports of attacks come from individuals. According to the number of complaints, Ecuador is in the fifth place with 4.76%[8]. These statistics motivate further study.

Cybercrimes reported in the different departments of the Public Prosecution in Ecuador include the illegal transfer of funds, theft of personal data, data interception and sexual harassment. The Criminal Policy of the Public Prosecutor's Office recorded 626 complaints of cyber-crime since August 10th, 2014, when entered into force the Code of Criminal Integral Protection (COIP), until May 31st, 2015. Ecuadorian provinces with highest rates of cyber-crime reported until 2015 were Pichincha, Guayas, and El Oro. On the contrary, there are no reports of cyber-crime in the province of Santa Elena[9].

Computer crime and the damage they can cause are issues which should create awareness in the community. In open wireless networks, the user sees only the network identifier (SSID), that is, the name of the WiFi network he wants to connect. However, he is not aware that anyone with little computer knowledge can access to these networks. For this purpose, it only takes a wireless antenna connected to a laptop and free software to capture any information traveling on the network. People who access networks with an economic motivation are considered computer criminals. The computer criminals are also known as black hat hackers. There are also gray hat hackers who act according to personal interests. These gray hat hackers can also access long distance links and test free access WiFi networks to capture authorized or unauthorized personal information. Additionally, also exist white hat hackers who use their knowledge to correct the errors of systems or computer platforms and prevent the attack of black hat and gray hat hackers. In the development of this work, the specialist who performed the analysis of the hacked networks is considered as white hat hacker as shown in the Figure 1[9].

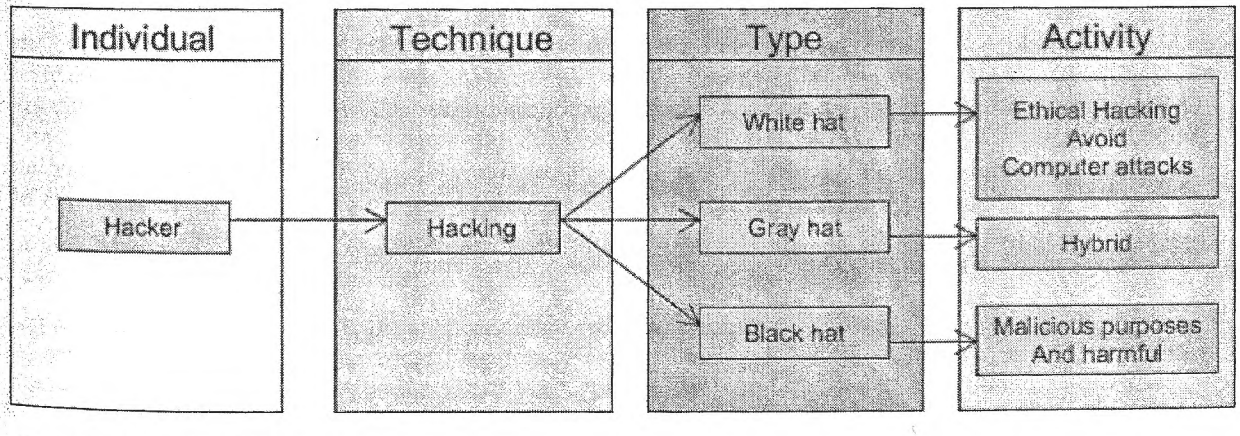

Figure 1. The types of hackers.

2. METHOD

The analysis of the objects of this study required the execution of several activities. First, the connection points with open access to the web within the province of Santa Elena were found then the devices connected to these networks were

scanned with the authorization of the chief of ICT's department. Second, the technical conditions of each network were identified. Finally, we identified and analyzed the AP-ROUTER device, objective of this audit. Also, the bandwidth of the network, the average number of connected devices and the identification of trends of user´s navigation in the chosen places were identified.

The networks search techniques: Wi-Fi wardriving and warwalking allowed the identification of risks in wireless networks. In addition to these methods, Ethical Hacking was used. It worths noting that criminals can use each of these techniques to obtain information illegally. Network Scanner, Kali Linux y Nmap tools allowed the analysis and the identification of vulnerabilities in the network. The adapters ALFA AWUS036H and TP-LINK TL-WN722N were used for detecting wireless signals.

Figure 2 shows the schematic analysis of pentesting performed on the wireless equipment of selected sites in different locations in the province of Santa Elena. The vulnerabilities investigated in this device were the type of power and quality of the signal. In addition to this, we also studied opened working channels and the degree of safety of the equipment.

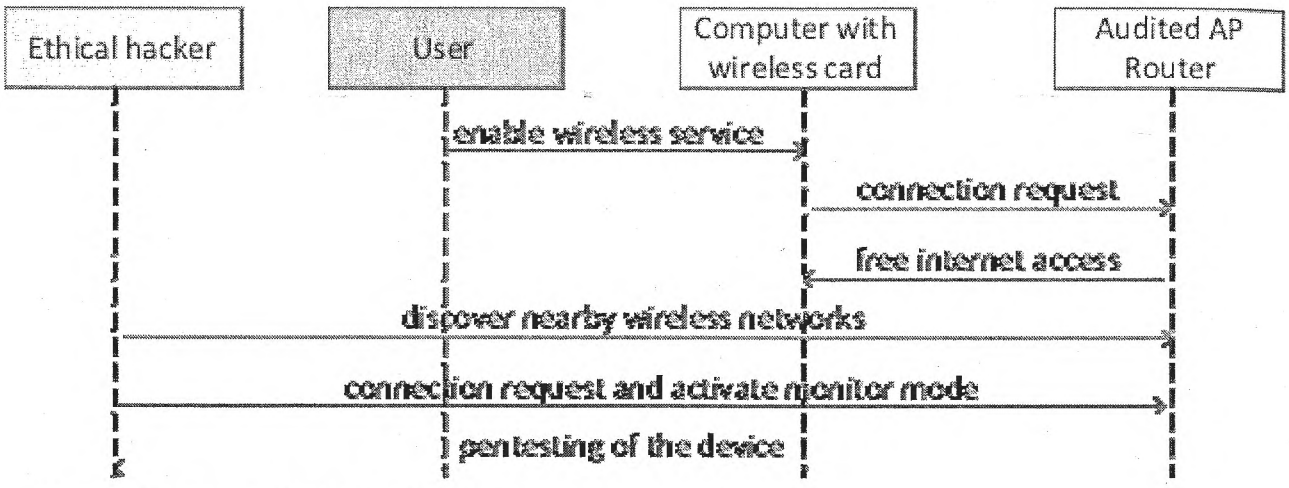

Figure 2. Schematic analysis of the selected city places.

3. RESULTS

From the search of networks with open access several public places were selected. It was considered of greater interest the following: a) a food court of a commercial center, b) the network of the sea promenade, c) the WiFi area of the terrestrial bus terminal station and d) several Points Wi-Fi of the State University Santa Elena Peninsula (UPSE). In all these cases, it was found that commonly all networks use the same logical architecture as shown in Figure 3.

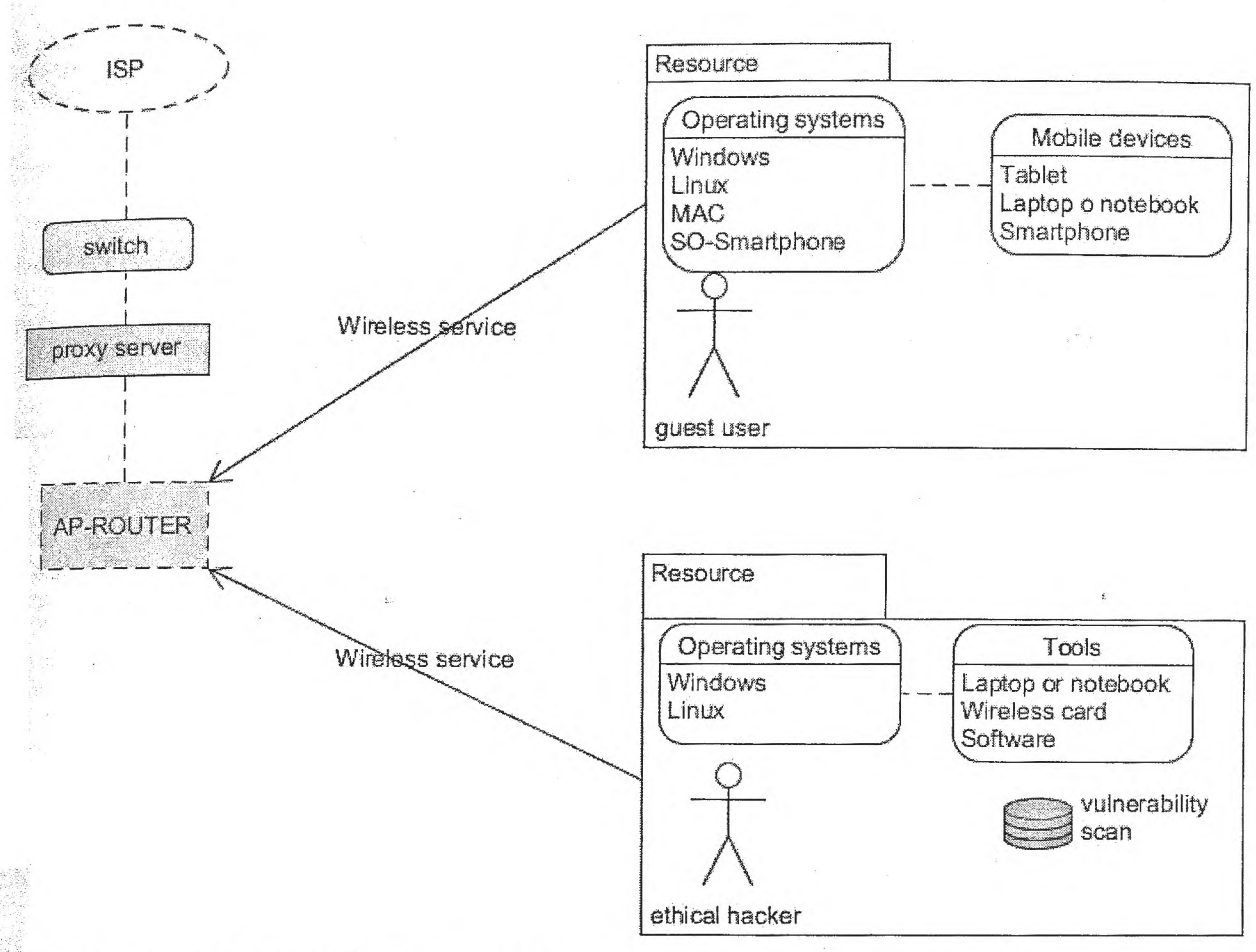

Figure 3. Common Network topology in the studied places.

In wireless network analysis, it was found, that the network, located in the food court of the shopping center, had enough intensity concerning its coverage, but apparently does not support many devices connected at once, which in sometimes creates difficulties when connecting. The sea promenade network, although, has good coverage and good bandwidth has the disadvantage of only allowing connections of half an hour per day.

The UPSE networks have a good wireless signal strength and campus-wide coverage. Each device supports 40 connections at the same time with a frequency of 2.4 GHz, allowing navigation all day. The bus terminal has two free connection areas: one in the food court and the other in the waiting room. The second area has better coverage than the first and allows a good internet connection continuously throughout the day.

During assessments of the networks, the average number of users connected to the wireless access point in the shopping center and the sea promenade was 20 users. The pentesting in the bus terminal station revealed that the average number of hosts connected during three days was about 70 users. And an average of 476 people use the UPSE networks.

Traffic can vary depending on the time, but on average, the value for data download and upload in the food court of the shopping center is 1 Mbps, while for the sea promenade, it was 3.95 Mbps. In the case of the bus terminal station network, the download and upload data at certain times is 1 Mbps for information upload and 3 Mbps for download, and for UPSE it was 1 Mbps for information upload and 0.90 Mbps for download.

The descriptive analysis of the wireless equipment was carried out using the NMAP tool and the Kali Linux software. Figure 4 and Figure 5 show the results found and the vulnerable ports. The router, employed at the bus terminal station, is a Mikrotik. It offers free internet service and works with the protocols and ports shown in the Figure 4. The figure indicates that the TCP port 23 is enabled. In the wireless coverage area of the shopping center, it is observed that the

most used channels are 1, 6 and 11, working at the 2.4 GHz frequency and only detect 80 port enabled (see Figure 6). And in the Wifi coverage area of the sea promenade, the most used channels are 1, 6 and 9 (see Figure 6), operating at the frequency of 2.4 GHz without active vulnerable ports.

Port	Protocol	State	Service	Version
21	tcp	open	ftp	MikroTik router ftpd 6.35.4
22	tcp	open	ssh	MikroTik RouterOS sshd (protocol 2.0)
23	tcp	open	telnet	Linux telnetd
53	tcp	open	domain	MikroTik RouterOS named or OpenDNS Updater
80	tcp	open	http	MikroTik router config httpd
2000	tcp	open	bandwidth-test	MikroTik bandwidth-test server
8291	tcp	open	unknown	

Figure 4. Port scans in the bus terminal station.

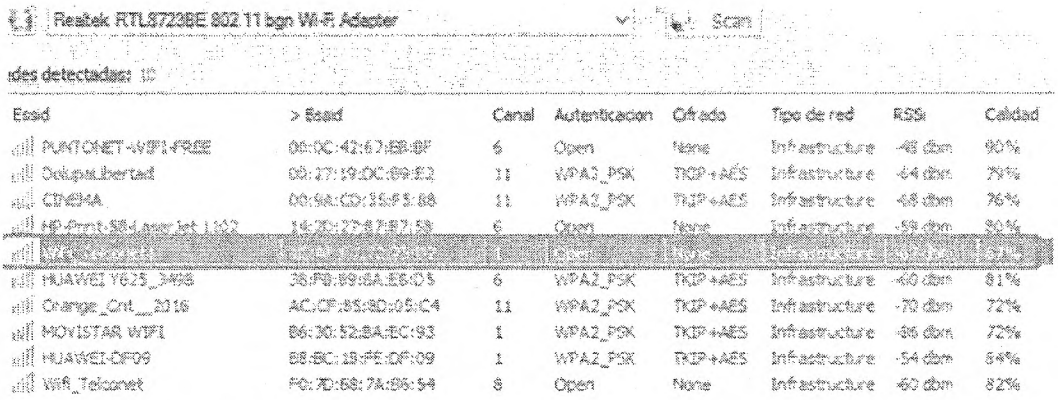

Figure 5. Port scans in the Shopping center.

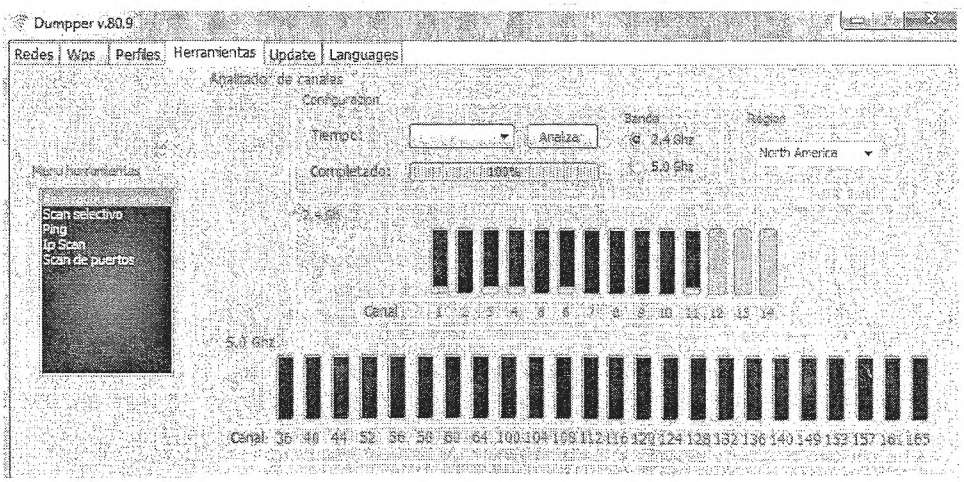

Figure 6. Wireless channels.

Also, a survey was conducted among visitors to the chosen places. The study intended to clarify the knowledge about the dangers of using open access networks and the necessary steps to avoid becoming a victim of cybercrime. The result showed that 57% were not aware of the vulnerability factors.

4. ANALYSIS AND DISCUSSION

The present study was carried out observing the following norms and laws of data protection in Ecuador. These statutes include the law of the national public data system, the law of electronic commerce, signatures and data messages, the organic law of transparency and access to public information and the article 230 of the Integrated Criminal Code[10]. Also, the tests were performed with the consent of the service providers within the places chosen to audit. Therefore, the study was carried out within the legal framework.

Detecting opened wireless connecting ports reveals the vulnerability of user information. These opened ports allow connecting to other computers and control them remotely as if the user were sitting in front of the computer. Therefore, precautions and corrections must be taken. We assume that ports stay opened because when configuring the AP-routers, technicians choose the default options sloppily[13-15].

The increase in complaints and amounts of financial damage creates the need for better understanding of the potential vulnerabilities of wireless networks. Easy access to the information about hacking and malicious attacks techniques found on the web, coupled with the lack of knowledge of users of free networks exposes users to cyber-attacks. Therefore, insecurity arises specifically due to users' lack of knowledge of technological tools, as evidenced by the results of the survey. Due to the high tendency of navigation by social networks and emails, which are the most used sites for navigation. It is deduced that the attacker can get the Facebook password by repeated attempts at hacking, intuition or luck, and in this way, can automatically enter the rest of the platforms.

CONCLUSIONS

This work is focused on a study of places with free access to the Internet to evaluate information security factors. The results showed, that places with free Internet access could be hacked with few technical resources and little knowledge of computer networks. It also showed, that these places are in high demand among users which could encourage unscrupulous people to commit cybercrimes. A large number of individuals, who are not aware of the dangers to which they are exposed when using free networks leads to the need for higher education institutions to create training programs for safe use of mobile devices when accessing the free internet service in public places. In the development of this work, it was shown that 70% of the people who access the open access points are potential victims of computer criminals. Therefore, it is recommended that people take preventive and corrective actions, in case they are threatened by cyber criminals or by content voluntarily or involuntarily accessed on the Internet. The society must be able to identify, respond to and denounce threats of computer crime.

REFERENCES

[1] Ijeh, A. C., Brimicombe, A. J., Preston, D. S., Imafidon, C. O., "Security Measures in Wired and Wireless Networks," Annual Report on the ERC activities and achievements in 2015, 113–121 (2009).

[2] Borisov, N., Goldberg, I., Wagner, D., "Intercepting mobile communications," Proc. 7th Annu. Int. Conf. Mob. Comput. Netw. - MobiCom'01, 180–189 (2001).

[3] Lehembre G., "W. P. A. Seguridad Wi-Fi – WEP, WPA y WPA2," Hakin9, 1, 12–26 (2006).

[4] Kumar, U., Gambhir, S., "A Literature Review of Security Threats to Wireless Networks," Int. J. Futur. Gener. Commun. Netw. 7, 25–34 (2014).

[5] Buttyán, L., Dóra, L., "WiFi Security–WEP and 802.11" Híradástechnika, 1–13 (2006).

[6] Cisco White paper, "Cisco Visual Networking Index (VNI) Forecast and Methdology 2015–2020", 1 June 2016, <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html> (19 March 2016).
[7] Internet Crime Report. (2015). at <https://www.ic3.gov/media/annualreports.aspx>
[8] ODILA. ODILA (Observatorios de delitos Informáticos de Latinamerica), "Reporte 2016". 28 July 2016, <www.odila.org> (19 Janary 2017).
[9] Los delitos informáticos van desde el fraude hasta el espionaje. at <http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html> (19 March 2016).
[10] Ministerio de Justicia, D. H. y C. Código Orgánico Integral Penal. (2014).
[11] Vassilenko, S., Valtchev, J.P., Teixeira, S., Pavlov., "Energy harvesting: an interesting topic for education programs in engineering specialities," Internet, Education, Science (IES-2016), 149-156 (2016).
[12] Romanyuk, N., Pavlov, S. V., Dovhaliuk, R. Yu., Babyuk, N. P., Obidnyk, M. D., "Microfacet distribution function for physically based bidirectional reflectance distribution functions," Proc. SPIE 8698, Optical Fibers and Their Applications 2012, 35-47 (2013).
[13] Kostishyn, S., Tymchyk, S., Vyrozyb, R., Zlepko, A., Pavlov, V., "Design features of automated diagnostic systems for family medicine," Proc. of 13th International Conf. on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), 109-131 (2016).
[14] Sawicki D. and Kotyra A., "Monitoring combustion process using image classification,", Przegląd Elektrotechniczny 90, 130-132 (2014).
[15] Cieszczyk, S., Komada, P., Akhmetova, A., "Open path FT-IR spectra analysis method for monitoring of environment and processes with varying conditions, " Annual Set The Enviromnent Protection, 18, 218-234 (2016).