TECHNICAL SCIENCES AND TECHNOLOGIES
UDC 004.735

Mariya Verovko, Iryna Posadska

ANALYSIS AND COMPARISON OF THE FUNCTIONALITY OF NETWORK MONITORING TOOLS

Марія Верьовко, Ірина Посадська

АНАЛІЗ ТА ПОРІВНЯННЯ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ ЗАСОБІВ МОНІТОРИНГУ МЕРЕЖІ

Мария Веревко, Ирина Посадская

АНАЛИЗ И СРАВНЕНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЙ СРЕДСТВ МОНИТРИНГА СЕТИ

The analysis and comparison of the functionality of the most popular network monitoring and traffic monitoring tools is described in the paper. The results of the investigation of the network monitoring and traffic monitoring tools performance, tested in the real LAN, are also presented.

Key words: *network, traffic, monitoring, LAN.*
Fig.: 2. Tabl.: 3. Bibl.: 7.

Представлено аналіз і результати порівняння найбільш популярних засобів моніторингу мережі та мережевого трафіку. Показано результати дослідження продуктивності засобів моніторингу мережі й мережевого трафіку, виконаного у реальній локальній мережі.

Ключові слова: *мережа, трафік, моніторинг, ЛОМ.*
Рис.: 2. Табл.: 3. Бібл.: 7.

Представлен анализ и результаты сравнения наиболее популярных средств мониторинга сети и сетевого трафика. Показаны результаты исследования производительности средств мониторинга сети и сетевого трафика, выполненного в реальной локальной сети.

Ключевые слова: *сеть, трафик, мониторинг, ЛВС.*
Рис.: 2. Табл.: 3. Библ.: 7.

Introduction. Due to the growth of popularity of the Internet and wide usage of computer networks in all areas of human life the task of network administration has become a valuable and complex issue, which requires large amount of human, hardware and software recourses. To perform presented task a wide range of network monitoring tools, which provide different set of functionality, is available for modern network administrators. However, the problem of selection of an appropriate tool, which will provide all necessary information about a network and all required functionality, is quite difficult, despite the wide availability of such tools on market. The main issues, associated with this problem, are:

- disparity of the declared and real functionality;
- limitation of the available functions in different versions;
- requirement of additional payment for necessary functionality;
- low performance in the real LANs;
- redundancy of the resulted information.

The task of network monitoring can be divided on two main tasks – monitoring of network elements and monitoring of information, transmitted over the network. These tasks are more frequently called as the task of network monitoring and the task of traffic monitoring.

Network monitoring system is a system, provided inventory and advanced diagnostics of computer networks; constant monitoring of the functioning of used networking equipment, application systems and network services; collection of statistics (real time and archived) and visualization of key performance indicators and operating parameters of the network infrastructure; optimization of load on the network equipment and servers; fixation of incidents; analysis of the impact of the encountered problem on the business processes and critical applications; determination of the cause of the incident and its automatic correction or notification of responsible for its elimination persons. Usage of such systems allows active monitoring of the availability, status and performance of the components of the corporate network, analysis and optimization of their load, and also the prediction of the occurrence of emergency situations.

Monitoring of the network traffic is a complex task, which includes the collection and analysis of data, transmitted over the network. The devices, which collect traffic destined for other devices, are called sniffers and can be used for both destructive and good purposes. The analysis of abilities of available sniffers allows obtaining information about the resources, which system administrators have to prevent attacks and unauthorized access.

The determination of the abilities of the most popular tools for network monitoring and traffic monitoring, their analysis and comparison and the development of the recommendations, based on the conducted research, is the main task of the current investigation.

Related work. Network monitoring is the process connected with both network performance and network security issues. That is the reason why the investigation and development of network monitoring tools and algorithms is the task of great importance and described in the works of many researchers.

The task of the network management and network performance investigation using network monitoring tools is described in the papers of Y. Breitbart, J. Friedmann, A. Greenberg, Y. Yemini, G. Goldschmidt etc. [1–3]

Usage of network monitoring for issues related to network security has been investigated in the researches of F.T. Grampp, R.H. Morris and S.M. Bellovin. [4–5] At the same time many investigators propose their own systems for network monitoring. [6–7]

Methodology. Free monitoring tools have been tested in the network of CNUT (range 192.168.0.0-192.168.17.255). This is a corporate network, which includes a large number of subnets and network equipment with different levels of protection (servers, switches, routers etc). The scheme of the network, used during the investigation, is presented in Fig.1.

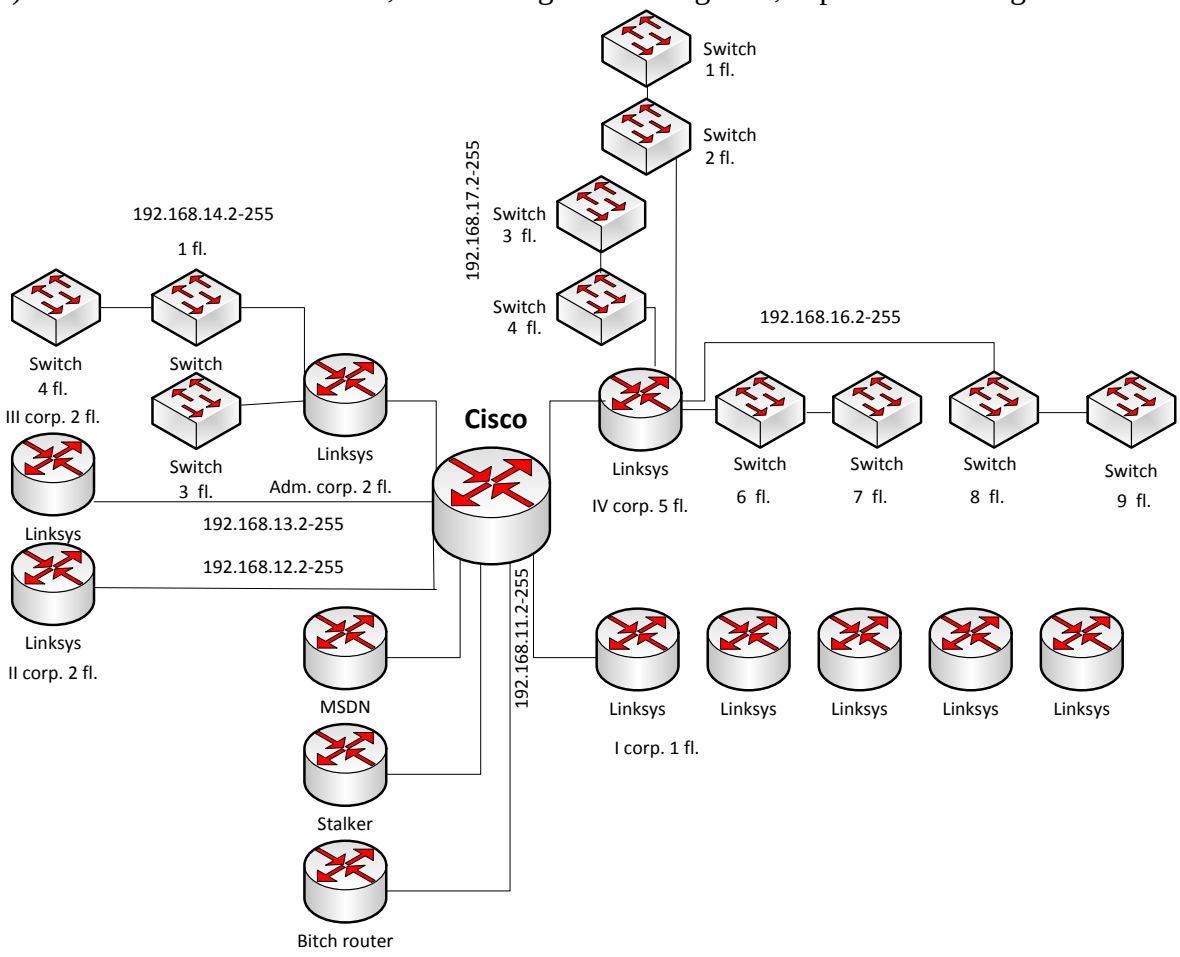

Fig. 1. The scheme of the investigated network

Tools for network monitoring. *Advanced IP Scanner* isreliable and free network scanner for analyzing local networks. The program is designed for scanning all the devices on the network, providing access to shared folders and FTP-servers makes possibility to remotely control computers (via RDP and Radmin), and can even remotely disable them.

Alchemy Network Monitor is designed to monitor the functioning of LAN and servers. In case detection of any problems or faults it should be generated message to the system administrator, that can be transmitted by e-mail, phone (SMS), pager or ICQ. It is a detailed log file.

Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports as well as has many other features. It is widely used by network administrators and just curious users around the world, including large and small enterprises, banks, and government agencies. It runs on Linux, Windows, and Mac OS X, possibly supporting other platforms as well.

*LanScope*is a multithreaded network scanner. LanScope performs network monitoring for the presence of the available resources NetBios (Samba), FTP, and HTTP, scanning ranges given IP-address. It designed to show the access rights to resources: reading, writing. Resource Scanner searches for a given resource name, for example, music, video, etc.

LanSpector is designed for network administrators. It should provide the view of the shared resources on the local network, scanning ip address ranges for the presence of commonly used services, building a detailed report on the NetBios.

*MegaPing*is a utility for monitoring, including finger, name lookup, network time synchronizer, ping, port scanner, traceroute, and whois. MegaPing has separate tool to find specific information. IP-scanner checks the range of IP-addresses, determines which of them are active, converts computer names, if the appropriate mode is selected. Accordingly, by using NetBIOS scanner, it can be checked a range of IP-addresses and individual components - or the entire domain - and get the NetBIOS names of network nodes, registered users and MAC-address.

NetScan is a free multi-threaded ICMP, Port, IP, NetBIOS, ActiveDirectory and SNMP scanner with many advanced features. It is intended for both system administrators and general users who are interested in computer security. The program performs ping sweep, scans for opened TCP and UDP ports, resource shares and services. For devices with SNMP capability available interfaces are detected and basic properties displayed.

NetView is developed as a substitute for the Windows Network Neighborhood. It is enough powerful tool for monitoring and administration of local networks with powerful tools for performing auxiliary functions. It should allow to keep a log with a list of machines, addresses and descriptions and regularly check it for switching off the machine, keep a log of the active network connections (a black and white lists feature).

SoftPerfect Network Scanner is a free multi-threaded IPv4/IPv6 scanner with a modern interface and many advanced features. It is intended for both system administrators and general users interested in computer security. The program pings computers, scans for listening TCP/UDP ports and discovers shared folders, including system and hidden ones.

Total Network Monitor is a program for continuous monitoring of network operation, separate computers, network and system utilities. TNM should notify in advance of the occurrence of faults and generate a detailed report about what happened and when.

Advanced LAN Scanner uses a multi-threaded scanning method, allowing to scan more than 1000 elements per second.

Tools for traffic monitoring. A network analyzer (sniffer) - is software or complex device that is designed to capture and analyze, or only to analyze the network traffic destined for other nodes. The abilities of sniffer are limited to the analysis of the traffic, which goes

only through its network card. To perform the function of packets interception, the network adapter driver of the device must support the promiscuous operating mode.Such operation mode of network adapter is automatically activated at the sniffer start or can be selected manually using the appropriate settings of sniffer. The intercepted traffic is sent to the package decoder that identifies and splits packets to the appropriate levels of the hierarchy.Depending on the capabilities of particular sniffer package information, obtained during interception, can then be additionally analyzed and filtered.

The abilities of following sniffers were analyzed during the investigation: Analyzer v.2.2, CommView, Iris Network Traffic Analyzer and Wireshark.

Utility Analyzer, developed by NetGroup company is a small free available packet analyzer, which doesn't require the installation on the computer. Because of the simplicity Analyzer v.2.2 has only basic tools set.

*CommView*is commercial software with basic trial version. The valuable difference of current utility is the fact that it's not implemented based on WinPcap library, which is currently the basis for almost all available sniffers.

Iris Network Traffic Analyzer is alsocommercial software with basic demo version. Current utility has similar disadvantage: the ability to filter previously captured packets is absent. The main advantage is the ability to display statistical information about packet capture in a graphical form.

Initially developed for a Linux platform, *Wireshark* is the most powerful traffic monitoring tool, correctly available for Windows and Linux users. Wireshark can be started using both graphical interface and command line. The ability to monitor Wireless networks is also realized in this software. The set of the available protocols is the biggest and consists of 752 network protocols. Current utility is the most popular to solve the task of traffic sniffing due it high usability and wide functionality.

Analysis and comparison: tools for network monitoring. During the search of free network monitoring tools there the following features were found:

– Despite the large number of monitoring tools available in the Interenet, about 80% of them are only demo or trial version (WhatsUp Gold, Observer, LAN Looking Any Network, XSpider, SNMP Manager, Net Meter, Actine Network Monitor, etc). The 30-day free period of operating life is declared, however after 1-2 minutes after installation the abnormal program behavior typically detected.

– A significant number of programs have only limited functionality from the set, presented in the manuals (Zabbix, Net Gear Genie, Net Privacy Monitor, PC Agent, Net Cut).

– Some programs, as Net Privacy Monitor, provide information only about the facts of connections to your network resources.Other perform monitoring only to the nearest switch (Net Gear Genie, Net Cut, etc);

– A significant number of programs requires registration and additional installations of web servers, etc. (Net Crunch, Total Network Inventory, LAN Spy, Big Brother.

The comparison of network analyzers is presented in the Tables 1 and 2.

Table 1

The comparison of network analyzers (part 1)

	Node status (active / inactive)	**Device name**	**IP address**	**Conformity of the device name and IP address**	**MAC address**	**Producer of network card**
1	2	3	4	5	6	7
Advanced IP Scanner	+	+	+	+	+	+
Alchemy Network Monitor	+	Partially	Partially	-	-	-
Angry IP Scanner	+	+	+	+	-	-

End table 1

1	2	3	4	5	6	7
Lanscope	+	+	+	+	-	-
Lanspector	+	*	+	Partially	-	-
MegaPing	+	-	+	-	-	-
NetScan	+	+	+	+	-	-
NetView	+	+	+	+	-	-
Soft Perfect Network Scanner	+	+	+	+	+	-
Total Network Monitor	+	+	+	+	-	-
Advanced LAN Scanner	+	+	+	+	+	-

Table 2

The comparison of network analyzers (part 2)

	Active ports	**OS**	**Working group**	**TTL**	**Used protocols**
Advanced IP Scanner	-	-	-	-	Unknown
Alchemy Network Monitor	Only for nodes with a device name	-	-	-	ICMP- for devices with IP addresses; FTP, HTTP, HTTPS, SMTP- only where devices names are indicated
Angry IP Scanner	-	-	-	-	ICMP, DNS
Lanscope	FTP and HTTP only	-	-	-	FTP**
Lanspector	-	Partially	Partially	+	FTP, http, Telnet, SSH, DNS
MegaPing	-	-	-	+	Unknown
NetScan	-	-	-	-	Unknown
NetView	-	-	-	-	Unknown
Soft Perfect Network Scanner	-	*	+	-	Unknown
Total Network Monitor	-	-	+	+	ICMP
Advanced LAN Scanner	+	*	+	-	+

* - Parameter is stated in the software documentation, but was not obtained during the investigation in the real LAN.

** - Also provides characteristics of FTP connection: access error, protected by a password, FTP- server; HTTP- gives a characteristic of “WWW server”.

Analysis and comparison: tools for traffic monitoring. Conducted analysis of the sniffers available for network administrators allowed determining the general characteristics for all of the network analyzers. The allocated characteristics are presented below:

– All software sniffers could be divided into two categories: sniffers, supporting the launch from the command line, and sniffers with a graphical interface. Some of the sniffers support both functions.

– The main differences between sniffers include the set of available protocol, depth of analysis of captured packets, capabilities of filters configuration and presence of compatibility with other programs.

– Almost all sniffers perform the analysis of the encoded packets.

– All sniffers distribute captured packets through the levels and protocols. But not all sniffers include the ability to recognize the protocol and display the intercepted information.

– Typically, the window of any sniffer with a graphical user interface consists of three areas.

– The first area displays summary data about captured packets. Usually, only basic fields set is displayed in this area, such as the time of packet interception; IP-addresses of the source and destination; MAC-address of the source and destination, source and destination port addresses; protocol type (network, transport or application layer); some summary information about the intercepted data.

– The second area is dedicated to the statistical information about previously selected packet.

– The third area contains the hex or ASCII representation of the package content.

However the investigated tools have significant difference in the possibilities of traffic capturing and analysis.The comparison of network traffic sniffers is presented in the Table 3.

Table 3

The comparison of network sniffers

	Deep analysis	**Monitoring in Wireless networks**	**Filtering at the capturing stage**	**Post-filtering**	**Additional features**
Utility Analyzer	-	-	+	-	– Only basic tools set and set of protocols.
CommView	-	+	+	-	– Not implemented using WinPcap library. – Ability to change IP and MAC addresses by the users names. – Statistical information in an additional window.
Iris Network Traffic Analyzer	+	-	+	-	– Ability to display statistics in a graphical form.
Wireshark	+	+	+	+	– Available for Windows and Linux users. – Both graphical interface and command line. – 752 network protocols

Data obtained by traffic analysis. Traffic monitoring and analysis is a powerful tool, because it allows obtaining all the information, distributed over the network. The description of the data, which can be received from the traffic, captured by network sniffer, is presented using the Wireshark utility example. Current utility is the most popular to solve the task of traffic sniffing due it high usability and wide functionality. The main window of Wireshark utility is presented in Fig. 2.

The analysis of the packets, captured using Wireshark, allow to get following information about the network:

– Obtain all the data from not encrypted (and sometimes encrypted) traffic, such as passwords and other information (Logins, session, cookies);

– Obtain data from the protocols headers;

– Determine the characteristics of network devices (IP-addresses, MAC-addresses and ports);

– Identify network services that are configured in the network (DNS, DHCP, WWW);

– Determine the servers and their characteristics.

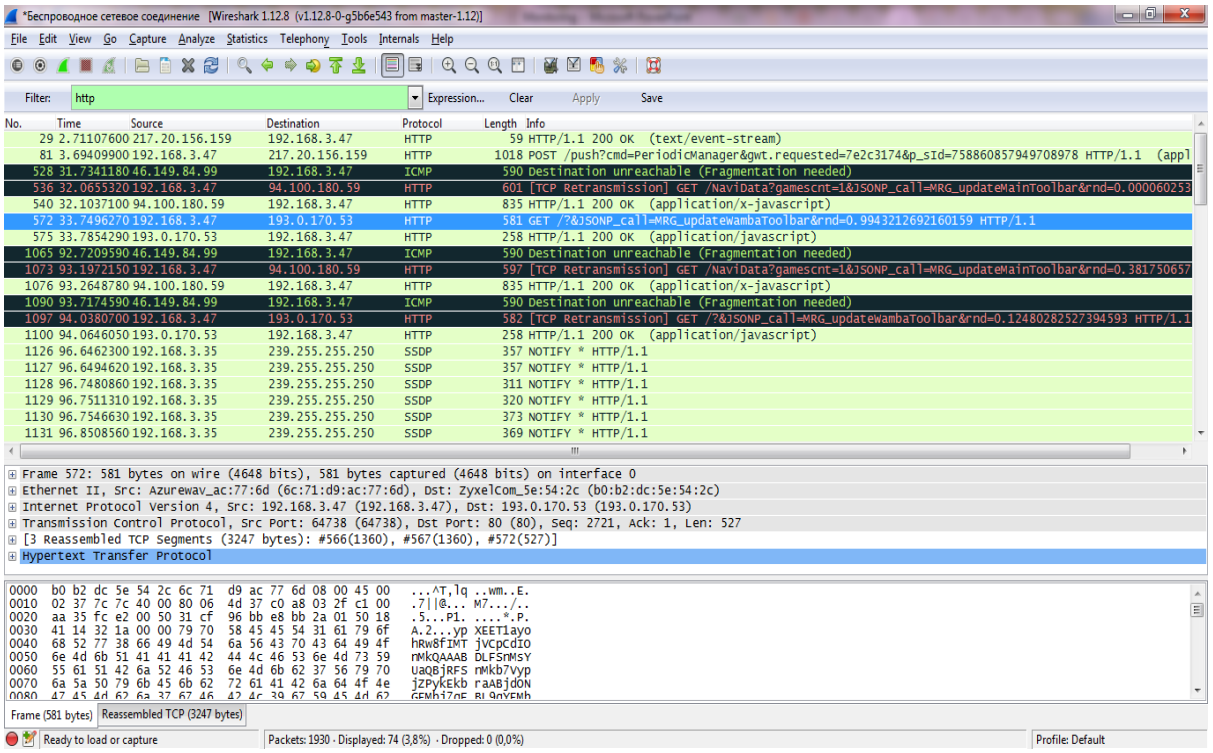

Fig. 2. The main window of Wireshark utility

All presented information can be used to get an unauthorized access to the DMZ-zone devices, which can be used as a start for intrusion to other network. However sniffers abilities can be used also to prevent intrusions into the network. Using the Wireshark data network administrator can:

– Detect a parasitic, viral and loopback traffic, which presence increases the load on the network equipment and communication channels.

– Identify the network malware and unauthorized software such as network scanners, flooder, Trojans, clients of peer to peer networks etc.

– Locate the network fault or error of network configuration agents.

– Get information about invasions to get correct security policy settings.

It should be mentioned that the majority of the tasks are solved by network administrators empirically. Network sniffers do not have sufficient levels of automation for intelligent data processing and decision making. The additional methods and approaches, which allow automation of the analysis of network traffic and to detect network anomalies, will be significant help for network administrator to prevent cyber-attacks.

Conclusion. The area of the typical LAN, its' complexity and number of nodes makes it impossible to perform network administration without the automation tools. At the same type to perform the task of network administration successfully usage of both types of monitoring – network nodes monitoring and network traffic monitoring – is required.

The results of presented research show that the abilities of software, available for modern network administrator, are completely different. Considering the information, obtained during the investigation, the conclusion also can be made, that not all abilities of network analyzers, which were determined by manufacturer, are really available in the software. However, the Advanced LAN Scanner and Wireshark are highlighted as the software with the widest functionality. At the same time, other tools, which are presented in the research, can also be used for the decision of the specific tasks. The selection of the appropriate tool depends on the set of functions, which network administrator requires from it.

Future work. Only network nodes monitoring and traffic monitoring tools are considered in the article. The complex intrusion detection systems, which combine presented functionality and additional abilities on intrusion detection, haven't been investigated. The research of such type of the system is the necessary step to obtain the complete information about network monitoring tools abilities.

Presented monitoring tools give a complete picture only in complex and in case of simultaneous usage of several of them. The development of software with a wider and combined functionality will significantly optimize the network administrator's job. The additional requirement for such software is the including of elements of the decision-making system, but not only raw data presentation.

References

1. Breitbart, Y. et al. (2001). Efficiently monitoring bandwidth and latency in IP networks. *Proceedings of the Inter International Conference on Computer Communications*, pp. 933–942.

2. Caceres, R. et al. (2000). Measurement and analysis of IP network usage and behavior. *IEEE Communications Magazine (may 2000)*, pp.144–151.

3. Yemini, Y., Goldschmidt, G. Yemini, S. (1991). Network management by delegation. Proceedings of the *IFIP/IEEE International Symposium on Integrated Network Managemen*t, pp. 95–107.

4. Grampp, F. T., Morris, R.H. (1984). Unix operating system security. *AT and T Bell Labs Technical Journal*, october 1984, vol. 63.

5. Bellovin, S. M.(1989). Security problems in the TCP/IP protocol suite. *Computer Communications Review*, april 1989, vol. 19.

6. Shirbhate, R.S., Patil, P.A. (2012). Network Traffic Monitoring Using Intrusion Detection System. *International Journal of Advanced Research in Computer Science and Software Engineering*, january 2012, issue 1, vol. 2.

7. Li, L., Thottan, M., Yao, B., Paul, S. (2003). Distributed Network Monitoring with Bounded Link Utilization in IP Networks. Proceedings of the *IEEE INFOCOM 2003.*

Verovko Mariya – PhD in Technical Sciences, assistant of Information and Computer Systems Department, Chernihiv National University of Technology (95 Shevchenka Str., 14027 Chernihiv, Ukraine).
Верьовко Марія Вадимівна – кандидат технічних наук, асистент кафедри інформаційних та комп'ютерних систем, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14027, Україна).
Веревко Мария Вадимовна – кандидат технических наук, ассистент кафедры информационных и компьютерных систем, Черниговский национальный технологический университет (ул. Шевченко, 95, г. Чернигов, 14027, Украина).
E-mail: miya.tevkun@gmail.com

Posadska Iryna – PhD student, Chernihiv National University of Technology (95 Shevchenka Str., 14027 Chernihiv, Ukraine).
Посадська Ірина Сергіївна – аспірант, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14027, Україна).
Посадская Ирина Сергеевна – аспирант, Черниговский национальный технологический университет (ул. Шевченко, 95, г. Чернигов, 14027, Украина).
E-mail:irrkin@gmail.com