DOI: https://doi.org/10.36910/6775-2524-0560-2020-41-13
УДК 004.05(075.8)

[1]**Марценюк Василь Петрович**, д.т.н., професор,
https://orcid.org/0000-0001-5622-1038
[2]**Сверстюк Андрій Степанович**, к.т.н., доцент,
https://orcid.org/0000-0001-8644-0776
[3]**Андрущак Ігор Євгенович**, д.т.н., професор,
https://orcid.org/0000-0002-8751-4420
[3]**Кошелюк Віктор Андрійович,** к.т.н., ст.викладач.
https://orcid.org/0000-0002-4136-5087
[3]**Потейчук Михайло Іванович,** аспірант.
https://orcid.org/0000-0001-7263-0958
[1]Університет Бєльсько-Бяли, Польща
[2]Тернопільський національнийний медичний університет імені І.Я. Горбачевського, Україна
[3]Луцький національний технічний університет, Україна

FEATURES OF TECHNOLOGY OF PROTECTION AGAINST UNAUTHORIZEDLY INSTALLED MONITORING SOFTWARE PRODUCTS

Марценюк В.П., Сверстюк А.С., Андрущак І.Є., Кошелюк В.А., Потейчук М.І. Особливості технології захисту від несанкціоновано встановлених моніторінгових програмних продуктів. У статті розглядається проблема програмних продуктів (модулів), призначених для забезпечення спостережуваності обчислювальних систем, фіксування діяльності користувачів і процесів, використання пасивних об'єктів, а також однозначно встановлених ідентифікаторів причетних до певних подій користувачів і процесів - з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

Ключові слова: моніторинговий програмний продукт, Log-файл, сигнатура баз, Spyware.

Марценюк В.П., Сверстюк А.С., Андрущак И.Е., Кошелюк В.А., Потейчук М.И. Особенности технологии защиты от несанкционированно установленных мониторинговой программных продуктов. В статье рассматривается проблема программных продуктов (модулей), предназначенных для обеспечения наблюдаемости вычислительных систем, фиксирование деятельности пользователей и процессов, использование пассивных объектов, а также однозначно установленных идентификаторов причастных к определенным событиям пользователей и процессов - с целью предотвращения нарушения политики безопасности и/или обеспечения ответственности за определенные действия.

Ключевые слова: мониторинговый программный продукт, Log-файл, сигнатура баз, Spyware.

Martsenyuk V.P., Sverstiuk A.S., Andrushchak I.Ye., Kosheliuk V.A., Poteichuk M.I. Features of technology of protection against unauthorizedly installed monitoring software products. The article considers the problem of software products (modules) designed to ensure the observability of computer systems, recording the activities of users and processes, the use of passive objects, as well as clearly identified identifiers of users and processes involved in certain events - to prevent security and / or ensuring responsibility for certain actions.

Keywords: monitoring software, Log-file, database signature, Spyware.

Formulation of the problem. The most vulnerable element of any computer system (and the greatest threat to computer security) is personnel. Some people may simply be unprepared: they may inadvertently destroy important information stored in the system or interfere with the operation of the system. Others may intentionally break the rules and use the computer for personal gain. There are also true criminals who steal data (or computers themselves) or intentionally damage a computer object [1].

Analysis of research. Personnel protection is a big problem that is currently receiving great attention around the world. In Ukraine, it is especially acute, since the lack of specialized hardware and software, as well as the incompetence of responsible persons, create fertile ground for the development of various forms of industrial and commercial espionage. The object of industrial espionage is usually confidential information constituting a commercial secret. The subjects of industrial espionage, both in the form of illegal collection of confidential information and in the form of its illegal use, are persons who (or with the help of whom) implement external threats (competitors, competitors' agents, partners) or internal threats (employees) to the information security of business entities. activities. At the same time, a mandatory sign of the objective side of the illegal use of information containing commercial secrets is large material losses of a business entity, losses that are 50 or more times higher than the non-taxable minimum income of citizens per month established by law.

Presentation of the main material and the justification of the results. Personnel Security Programs use two main approaches. The first is related to the development of rules for the safe use of computers when working in a network, the delimitation of access to information, as well as the development of physical protection measures (guarding premises, using surveillance systems).

The second approach is associated with determining the composition of the software (software and hardware) that is used by the security administrator of the computing system to ensure its observability - the properties of the computing system, which makes it possible to record the activities of users and processes, the use of passive objects, and also unambiguously establish the identifiers of users involved in certain events and processes to prevent security policy violations and / or ensure accountability for certain actions. It is this property, depending on the quality of its implementation, that allows, to one degree or another, to control the observance of the established rules of safe work on computers by the employees of the enterprise [2].

Supervisory monitoring can occur as different frequencies depending on the certification agency, but usually consider the hardware and software of the product, as well as the manufacturer's constant adherence to functional safety management systems.

Only the method of application of monitoring software products allows to see the line between security management and security breach.

Unauthorized use - installation of monitoring software products takes place without the knowledge of the owner (security administrator) of the automated system or without the knowledge of the owner of a specific personal computer. Unauthorized monitoring software products are called spyware. Unauthorized use is usually associated with illegal activity. As a rule, unauthorized spyware products have the ability to configure and obtain a "complete" executable file, which during installation does not display any messages and does not create windows on the screen; such products also have built-in means of delivery and remote installation of the configured module on the user's computer, ie the installation process does not require direct physical access to the user's computer and often does not require the rights of a system administrator;

Authorized use - the installation of monitoring software products is with the knowledge of the owner (security administrator) of the automated system or with the knowledge of the owner of a specific personal computer. Authorized employee monitoring software (parental control software, access control software, personnel security programs) usually requires either physical access to the user's computer or the mandatory presence of system administrator rights to configure and install these programs.

Known monitoring software products. This category includes monitoring software products, the signature of which (on any basis) is included in the signature databases of the main known manufacturers of anti-spyware or anti-virus software products [3].

Unknown monitoring software products. This category includes monitoring software products whose signature is not included in the signature databases of major well-known manufacturers of anti-spyware software products and / or anti-virus software products and will probably never be included in them for various reasons, namely:

- monitoring software products (modules) developed under the auspices of various governmental organizations;
- spyware, which is developed in limited quantities (often only one or more copies) to solve a specific problem related to the theft of critical information from a user's computer (for example, software products used by malicious professionals). These software products can be slightly modified by the open source codes of monitoring software products, taken from the Internet and compiled by the attacker, which allows you to change the signature of the monitoring software product;
- commercial monitoring software products, which are very rarely included in the signature databases of well-known manufacturers of anti-spyware software products and / or anti-virus software products. This leads to the fact that attackers on the Internet a full-featured version of this commercial monitoring software can turn the latter into a spyware that is not detected by anti-spyware and / or anti-virus software;
- spyware that is part of viruses. Until spyware is entered into the virus database, these spyware products are unknown. An example is the world-famous viruses, which have caused a lot of trouble in recent years, include a module for intercepting keyboard keystrokes and sending the received information to the Internet.

Protection against "known" unauthorized monitoring software products: use of anti-spyware software products and / or anti-virus software products from well-known manufacturers, with automatic updating of signature databases.

Protection against "unknown" unauthorized monitoring software products: the use of anti-spyware software products and / or anti-virus software products from well-known manufacturers that use so-called heuristic (behavioral) analyzers to counter spyware, ie do not require a signature database.

Protection against "known" and "unknown" unauthorized monitoring software products includes the use of anti-spyware software products and / or anti-virus software products from well-known vendors that use: constantly updated spyware signature databases to counter spyware; heuristic (behavioral) analyzers that do not require a signature base.

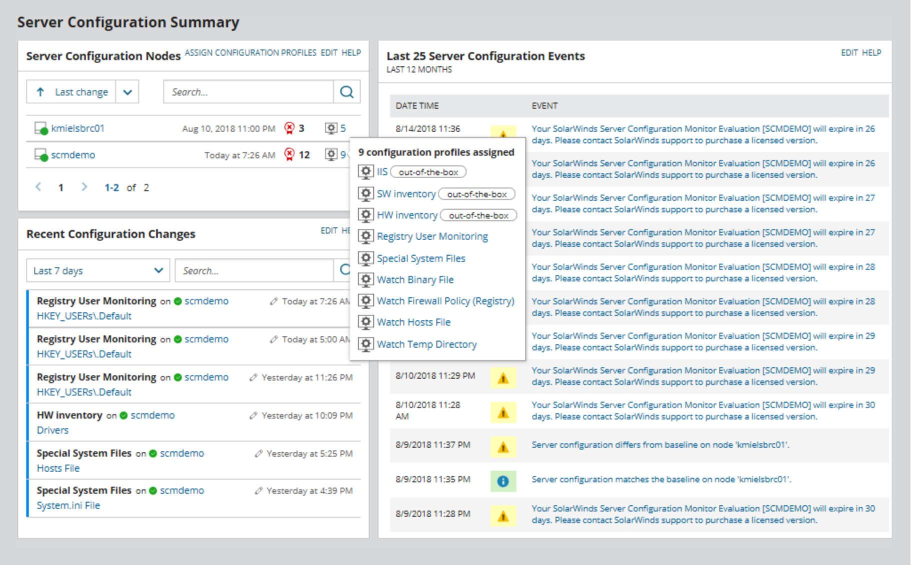
However, many Ukrainian enterprises often limit themselves to any one security measure, for example, buying an expensive firewall operating on the border of the internal corporate network and the external global Internet network. This assumes that all computers connected to the network have access to the Internet through this firewall. Meanwhile, the largest corporations in the world annually lay off hundreds of employees for bringing their modems and connecting to the external network via telephone lines from their workplaces. If there is a leak of critical information, the security administrator, not having additional software, is practically unable to identify the attacker and determine to which computer, at what time the modem was unauthorizedly connected, and what information was compromised. From this point of view, firewalls cannot provide reliable protection from personnel [4].

Another example is that some bank employees can commit illegal activities for a certain fee, providing interested parties with information about the financial transactions of any bank customers. This information can be transmitted to the interested party both over the network and in the form of a printout made on a local printer. In the second case, no network monitoring tools are able to detect the violation.

To solve these and many other problems related to protection from personnel, it is necessary to use software or software and hardware that implements the observability property of computing systems, which allows:

- identify (localize) all cases of unauthorized access attempts to confidential information with an exact indication of the time and network workplace from which such an attempt was made. Localize all cases of distortion (destruction) of information;
- to determine the facts of unauthorized installation of software;
- monitor the possibility of using personal computers outside of working hours and identify the purpose of such use;
- to determine all cases of unauthorized use of modems in the local network by analyzing the facts of launching unauthorizedly installed specialized applications;
- determine all cases of typing critical words and phrases on the keyboard, preparation of any critical documents, the transfer of which to third parties will lead to material damage;
- to determine the facts of misuse of personal computers.

Consider a number of technical requirements that must be met by software or software and hardware that ensure the observability of automated systems (AS), i.e. organizational and technical systems that implement information technology and integrate computing systems, physical environment, personnel and processed information. A computing system (CS) means a set of software and hardware designed for information processing (Pic1).



Server Configuration Summary

Server Configuration Nodes

kmielsbrc01	Aug 10, 2018 11:00 PM	3	5
scmdemo	Today at 7:26 AM	12	9

Recent Configuration Changes

Registry User Monitoring on scmdemo — Today at 7:26 AM
HKEY_USERs\.Default

Registry User Monitoring on scmdemo — Today at 5:00 AM
HKEY_USERs\.Default

Registry User Monitoring on scmdemo — Yesterday at 11:26 PM
HKEY_USERs\.Default

HW inventory on scmdemo — Yesterday at 10:09 PM
Drivers

Special System Files on scmdemo — Yesterday at 5:25 PM
Hosts File

Special System Files on scmdemo — Yesterday at 4:39 PM
System.ini File

9 configuration profiles assigned

- IIS (out-of-the-box)
- SW inventory (out-of-the-box)
- HW inventory (out-of-the-box)
- Registry User Monitoring
- Special System Files
- Watch Binary File
- Watch Firewall Policy (Registry)
- Watch Hosts File
- Watch Temp Directory

Last 25 Server Configuration Events
LAST 12 MONTHS

DATE TIME		EVENT
8/14/2018 11:36	⚠	Your SolarWinds Server Configuration Monitor Evaluation [SCMDEMO] will expire in 26 days. Please contact SolarWinds support to purchase a licensed version.
		Your SolarWinds Server Configuration Monitor Evaluation [SCMDEMO] will expire in 26 days. Please contact SolarWinds support to purchase a licensed version.
		Your SolarWinds Server Configuration Monitor Evaluation [SCMDEMO] will expire in 27 days. Please contact SolarWinds support to purchase a licensed version.
		Your SolarWinds Server Configuration Monitor Evaluation [SCMDEMO] will expire in 27 days. Please contact SolarWinds support to purchase a licensed version.
		Your SolarWinds Server Configuration Monitor Evaluation [SCMDEMO] will expire in 28 days. Please contact SolarWinds support to purchase a licensed version.
		Your SolarWinds Server Configuration Monitor Evaluation [SCMDEMO] will expire in 28 days. Please contact SolarWinds support to purchase a licensed version.
		Your SolarWinds Server Configuration Monitor Evaluation [SCMDEMO] will expire in 29 days. Please contact SolarWinds support to purchase a licensed version.
8/10/2018 11:29 PM	⚠	Your SolarWinds Server Configuration Monitor Evaluation [SCMDEMO] will expire in 29 days. Please contact SolarWinds support to purchase a licensed version.
8/10/2018 11:28 AM	⚠	Your SolarWinds Server Configuration Monitor Evaluation [SCMDEMO] will expire in 30 days. Please contact SolarWinds support to purchase a licensed version.
8/9/2018 11:37 PM	⚠	Server configuration differs from baseline on node 'kmielsbrc01'.
8/9/2018 11:35 PM	ℹ	Server configuration matches the baseline on node 'kmielsbrc01'.
8/9/2018 11:28 PM	⚠	Your SolarWinds Server Configuration Monitor Evaluation [SCMDEMO] will expire in 30 days. Please contact SolarWinds support to purchase a licensed version.

Pic.1 Network monitoring tools

The architecture of any network software that claims to be portable and versatile should be based on the TCP / IP protocols. The TCP / IP family of protocols is intended for an interconnected network consisting of separate heterogeneous packet subnets connected to each other by gateways, to which dissimilar machines are connected. Each of the subnets operates in accordance with its specific requirements and has its own nature of the communication means. However, it is assumed that each subnet can receive a packet of information (data with a corresponding network header) and deliver it to a specified address on that particular subnet. The subnet is not required to guarantee mandatory packet delivery and to have a reliable end-to-end protocol. Thus, two machines connected to the same subnet can exchange packets. Usually, for security reasons, programs that implement aircraft observability are limited to working on a subnet with a given mask with line of sight of the entire IP address space [5].

When it is necessary to transfer a packet between machines connected to different subnets, the sending machine sends the packet to the appropriate gateway (the gateway is connected to the subnet just like a normal node). From there, the packet is routed along a specific route through the gateway and subnet system until it reaches a gateway connected to the same subnet as the receiving machine; there the package is forwarded to the recipient. The interconnected network provides a datagram service. The problem of packet delivery in such a system is solved by implementing IP in all nodes and gateways. The gateway layer is essentially the basic element in the entire protocol architecture, providing the ability to standardize upper layer protocols.

Aircraft observability programs are executed using "client-server" technology.

There is one server side and a limited number of client sides.

Client parts are installed on end-user workstations that can run on various operating systems.

The main functions of the client side:

- registration of certain events;
- keeping a log of registration;
- transfer of the registration log to the server part according to the criterion established by the security administrator.

The client side should:

- boot automatically when the operating system boots;
- be invisible to the user;
- register texts typed in graphical and console windows;
- register the time and date of system boot and the name of the current user;
- register the time and date of launched applications;
- register the time and date of switching between tasks;
- register the addresses of the visited Internet sites;
- be able to apply filters to control strictly defined applications;
- be able to control on a schedule;
- be resistant to the user's influence;
- transfer reporting information to the server side invisibly to the user;
- use as little system resources as possible without significantly affecting system performance;
- be able to automatically install in a local network;
- do not interfere with antivirus and other software.

Thus, the client part collects detailed information about what actions were performed by the user on the computer. To log events in operating systems (OC) of the Microsoft Windows family, you can use kernel-level drivers or a hook mechanism. A trap is part of the Windows message processing engine that allows an application to install a routine to intercept system message traffic and process certain types of messages before they reach the recipient application's windowing routine.

Windows contains many different types of hooks. Each of them is responsible for one or another aspect of the message processing mechanism. For each of these types, the system maintains separate hook chains, which are a list of pointers to callback routines. When an event occurs associated with a particular type of trap, the system sends a corresponding message sequentially to each procedure in the trap chain. The actions that a trap procedure can perform depends on the type of trap. For some types of traps, the procedure can only register messages, for other types it can change the parameters of messages and even interrupt their passage through the chain of traps.

The hook procedure can be global, logging messages from all threads in the system, or targeting a single thread. The hook global procedure is called in the context of any application from a dynamic link library module. A thread-specific procedure is called in the context of an associated thread and can be located both in the main executable module and in a dynamic link library module.

Windows OS contains the following main types of traps:

- to intercept messages sent to the procedure for processing the window of the receiving application, before or after their processing by this procedure;

- to intercept messages queued, record input messages;

- to replay a previously recorded sequence of messages;

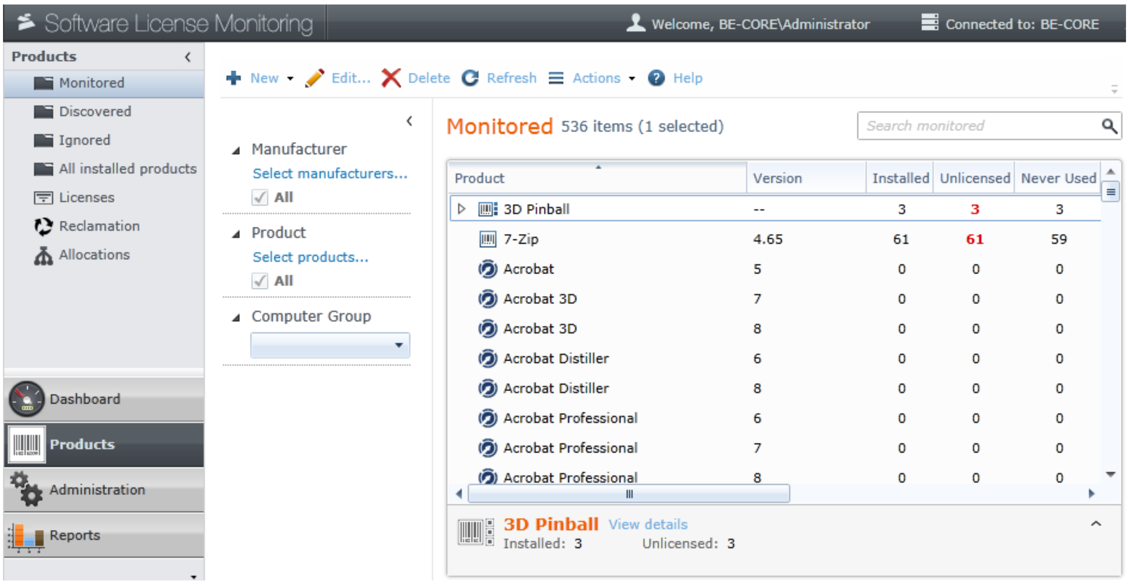
- to intercept messages generated by any event of entering information in a dialog box;

- to intercept messages generated by a keyboard event, intercept messages generated by the mouse event; for debugging other traps.

Thus, this mechanism provides a very flexible set of tools that are used by the client parts to register system events.

The server part is managed only by the security administrator of the computing system. the information accumulated in the logbook becomes critical upon reaching a certain volume, SLM. Its loss or misuse (modification, familiarization) may harm the owner of the information or the AU, or any other natural (legal) person or group of persons. The main function of the server side is the centralized collection and storage of logs transmitted from the client side. A logbook is an ordered set of registration records, each of which is entered by the client part upon the fact of a controlled event.

The biggest problem in the development of the server side is to ensure the stable operation of the system when the server side will serve tens of thousands of clients. At the same time, it is necessary to ensure that there are no memory "leaks" due to incomplete freeing of heap sizes SLW (Pic 2).



Monitored 536 items (1 selected)

Product	Version	Installed	Unlicensed	Never Used
3D Pinball	--	3	3	3
7-Zip	4.65	61	61	59
Acrobat	5	0	0	0
Acrobat 3D	7	0	0	0
Acrobat 3D	8	0	0	0
Acrobat Distiller	6	0	0	0
Acrobat Distiller	8	0	0	0
Acrobat Professional	6	0	0	0
Acrobat Professional	7	0	0	0
Acrobat Professional	8	0	0	0

3D Pinball View details
Installed: 3 Unlicensed: 3

Pic 2. SLM overview

Programs that implement the property of aircraft observability are very complex and expensive complexes. Therefore, they must have adequate security measures against unauthorized use. First, software protection technologies are used - checking the integrity of code and data, encrypting data, encrypting traffic between the client and server parts, etc. Secondly, hardware protection keys are used, into which personal information about the customer, the maximum allowable number of clients, a range of IP addresses, etc. are stitched. It is characteristic that observability programs can be used not only in the local network of an enterprise, but also in the global Internet. therefore, you must hard-code the range of client IP addresses and their maximum number, the server IP address and the subnet mask [6].

For convenient analysis of logs by means of database management systems, it is necessary to provide for the possibility of automatic conversion of logs to DBF format. This allows you to apply SQL queries and make selections based on criteria of interest Spyware.

Our next step is to find out whether use of the keystroke recorder is legal or illegal action in each particular case. Unauthorized installation of a keylogger or other software that includes keystroke logger as a module is any installation without the knowledge or consent of the PC owner (administrator). As a rule, such software products have ability to configure and obtain a “packed” installation executable file that is delivered to the victim`s computer with the help of various illegal schemes (phishing, personalized spam, social engineering). During installation it doesn`t display any messages or create any windows on the screen. That is, the keylogger installation process doesn`t require direct physical access to the user`s computer as well as administrative privilege. Such keyloggers are often constituents of malicious spyware and used to steal confidential information such as logins and passwords, bank card data, etc. Authorized use of a keylogger is use of such software with the knowledge and consent of the PC owner or security administrator. As a rule, authorized monitoring software products require physical access to computer and administrative privilege for configuration and installation that excludes (or at least minimizes) risks of unauthorized use of such programs.

It should be noted that modern keystroke recording software have much more capabilities than their “classic” counterparts. Nowadays a keylogger is actually a software package that in addition to capturing of keystrokes also enables to monitor almost all users’ activity (visited websites, communication via messengers, installation and launch of programs, creation, change and deletion of files, sending email and many other things). Besides, many keyloggers allow taking screenshots of the screen with a certain periodicity or with a binding to any events. Also, a modern keylogger can record information from the microphone and/or web camera. In addition to the function of information collection, keylogger can also have monitoring functions, namely, restrict access to certain sites and/or programs, respond to a specific keyword typed in the URL bar of the browser or in the messenger window. Thus, software for covert surveillance and access control is more appropriate name for such a complex software product.

During a network connection, the two processes exchange data. An abstract network connection point expression is a socket. Each socket in use has a type and a process associated with it. Sockets exist within communication domains. Domains are abstractions that imply a specific addressing structure and multiple protocols that define the different types of sockets within a domain. Observability programs can use two types of sockets - TCP or UDP. Stream sockets that use the TCP transport protocol must be created when guaranteed delivery of data is required, for example, when sending the server side of the client log. Datagram sockets use the UDP transport protocol, which allows small, fixed-length packets to be sent without confirmation of delivery and without establishing a virtual connection. The client side can use datagram sockets, for example, to send activity signals [7].

Conclusion and prospects for further research

The most effective protection of an automated system is provided only by a set of interrelated physical, technical and organizational measures. In modern conditions, especially when thousands of computers belonging to one organization are dispersed geographically (in different buildings, cities, countries), it is impossible to talk about the security of the infrastructure of an automated system without ensuring its observability.

Promising directions for the development of observability programs are: development of modules for audio and video control of computing systems, which sharply increase the information content of reporting information;

- development of multi-platform client and server parts;

- development of modules for prompt notification of the security administrator about the state of the server side and violations of the established security policy using cellular and paging communications.

References

1. Addicott J. Cyberterrorism: Legal Policy Issues / Jeffrey F. Addicott // Legal Issues in the Struggle against D. Ankov, K. Seiger, W. Fonstorh. Computer crimes. Guide to Combating Computer Crimes: Per. from English. - M.: Mir, 2009. - 351 p.

2. ND TZI 1.1-003-99. Terminology in the field of information protection in computer systems from unauthorized access. // Department of Special Telecommunication Systems and Information Protection of the Security Service of Ukraine. - Kiev, 2009.

3. Zolotov S. Protocols of the Internet - SPb .: BHV - Saint Petersburg, 2008. - 304 p.

4. RFC 1180. TCP/IP tutorial. T.J. Socolofsky, C.J. Kale. Jan-01-1991.

5. Prokofeva D.M. Pidpryamnytske spying in the information system. // Information Technologies and Information Technologies: Collection of Science Works. - Zaporizhzhya: Legal Institute of the Ministry of Internal Affairs of Ukraine, 1998. - VIP. 2.

6. Kutsenko V.N., Golubov V.O. Recommendations for securing the software and technical information retrieval in computer fences. // Information Technologies and Information Technologies: Collection of Science Works. - Zaporizhzhya: Legal Institute of the Ministry of Internal Affairs of Ukraine, 2018. - VIP. 2.

7. Krasnostup M.D. Information security of Ukraine: the day and the problem. // Information Technologies and Information Technologies: Collection of Science Works. - Zaporizhzhya: Legal Institute of the Ministry of Internal Affairs of Ukraine, 2019. - VIP.