DOI: 10.36910/6775-2524-0560-2020-38-07
УДК 004.05(075.8)
**Марценюк Василь Петрович**, д.т.н., професор,
https://orcid.org/0000-0001-5622-1038
Університет Бєльсько-Бяли, Польща[1)]
**Дідманідзе Ібраім Шотаевич**, д.фіз.-мат.н., професор,
https://orcid.org/0000-0001-6695-4980
Батумський державний університет імені Шота Руставелі, Грузія[2)]
**Андрущак Ігор Євгенович**, д.т.н., професор,
https://orcid.org/0000-0002-8751-4420
**Крадінова Тетяна Адамівна**, к.т.н., доцент,
https://orcid.org/0000-0002-5611-1290
**Рудь Катерина Іванівна,** аспірант.
Луцький національний технічний університет, Україна[3)]

# ІНФОРМАЦІЙНА БЕЗПЕКА: ТЕХНОЛОГІЇ АНТИВІРУСНОГО ЗАХИСТУ

**Марценюк В.П., Дідманідзе І.Ш., Андрущак І.Є., Крадінова Т.А., Рудь К.І. Інформаційна безпека: технології антивірусного захисту.** У статті розглядається нормативно-методичні основи класифікації загроз інформаційної безпеки, пов'язаних із застосуванням шкідливих програм щодо інформаційних систем. Виділено загрози впливу на інформаційні системи окремих типів шкідливих програм**.**
**Ключові слова:** інформаційна безпека, зловмисне програмне забезпечення, комп'ютерний вірус, комп'ютерний антивірус, загрози, еволюція комп'ютерних вірусів, троян, приховування вірусів, антивірусні методи.

**Марценюк В.П., Дидманидзе И.Ш., Андрущак И.Е., Крадинова Т.А., Рудь К.И. Информационная безопасность: технологии антивирусной защиты**. В статье рассматривается нормативно-методические основы классификации угроз информационной безопасности, звязаных с применением вредоносных программ в отношении информацинных систем. Выделены угрозы воздействия на информационные системы отдельных типов вредоносных программ.
**Ключевые слова:** информационная безопасность, вредоносное программное обеспечение, компьютерный вирус, компьютерный антивирус, угрозы, эволюция компьютерных вирусов, троян, сокрытие вирусов, антивирусные методы.

**Martsenyuk V.P., Didmanidze I.Sh., Andrushchak I.Ye., Kradinova T.A., Rud K.I. Information security: anti-virus protection technologies.** The article deals with the normative and methodological bases of classification of information security threats related to the use of malware against information systems. The threats to the impact on the information systems of certain types of malware are highlighted. In the process, antivirus experts desing and develop new methodologies to make them stronger, more and more every day. The purpose of this paper is to reviev these methodologies and outline their strengths and weaknesses to encourage those and interested in more investigation on these areas.
**Keywords:** information security, malware, computer virus, computer antivirus, threats, evolution of computer viruses, trojans, virus hiding, antivirus methods.

**Formulation of the problem.** In the modern world, information technology plays a significant role in all spheres of human life. Presentation of modern areas of production, science, sports, economics and culture becomes impossible without the use of computer technology. Computer technology in connection with total computerization is a priority course for the development of 21st century science. The need for computers arises in everyday life, both during work, research and education, as well as in leisure planning and the implementation of free time.

On this year's day, there are tens of thousands of outdoor computer computers. It's independent of such an abundance, the number of types of customers, which is one type of one mechanism by the principle of principle, it is divided. If there is a combination of virusi, yaki can be brought immediately to the decimal type. The main and most widespread classifications of computer components are those for middle class living, but for the types of computer systems in which there are viruses. The flip side of all the advantages of computer technology is their vulnerability. Vulnerability of information includes the exposure of information to various destabilizing factors, which can lead to a violation of its confidentiality, integrity, accessibility or misuse, which undoubtedly adversely affects the owner of the information.

**Analysis of research.** The issue of paramount importance for the user is the problem of data and system security, the possibility of fearless use of information brought from outside and ensuring the stable operation of the computer. The problem of external threats is particularly acute in connection with the development of the Internet, as it is through it that viruses and malware are often introduced that appear, modernize and infect thousands of computers daily. Trojan programs (backdoors, rootkits, ransomware Trojans, Windows blockers), worms, viruses, dialers, spyware, phishig attacks - this is not a complete list of unpleasant surprises that an insecure user will sooner or later encounter.

Threats to information security are divided into active and passive. Passive ones are mainly aimed at unauthorized use of information resources of information systems, without affecting its functioning, listening to communication channels, etc. Active threats are aimed at disrupting the normal functioning of information systems with a targeted effect on its components. Active threats, for example, include the failure of a computer or its operating system, the distortion of information in a data bank, and the destruction of software.

A computer program has its own author and a specific purpose, therefore, the behavior of a virus in a system is set by its creator (virus writer). Definition A computer virus implies a program with the functions of propagating its own copies in files of other programs. A mandatory attribute that a computer virus possesses is the ability to infect other files on the computer. Computer viruses have the ability to inject themselves into the "body" of other programs and files on a computer for their own reproduction.

**Presentation of the main material and the justification of the results.** The first computer viruses were created by their authors solely for the purpose of self-assertion - the authors tried to confirm their own abilities by writing these programs. Often, no other functional application other than self-copying, the output of any messages of a comic nature, such programs did not carry. It only interfered with working on an infected system, but there was no talk of destroying user information as a result of infection with such a computer virus. Later, viruses began to possess destructive functions: they deleted certain user files, sometimes a number of system files, on the infected system, which rendered the operating system unusable. A characteristic of that period was the WIN.CIH virus, which at some point in time caused damage to the motherboard of the computer, writing incorrect information to the BIOS [1].

Over time, the number of computer viruses created began to decline, giving the palm of the eye to Trojan horses. Today, cybercriminals have become the destiny of professionals with the goal of their activities to make a profit. Of the most common computer viruses in recent times, it is worth noting Sality and Virut (according to the classification of Kaspersky Lab). Both of these computer viruses carry a distinct economic component, involving the infected computer in an entire zombie network that can secretly submit to its owner (virus writer) via the Internet, send spam, or even make DOS attacks on Internet services. In fact, looking at the Virut or Sality computer virus, we come across a trojan supplemented by a method of propagating a computer virus for greater efficiency.

The most common malware family today is trojans. The term "trojan" was borrowed from the legendary story about the Trojan horse, thanks to which in ancient times an invisible penetration into the territory of the enemy was made. In the same way, modern computer trojans imperceptibly enter the victim's computer and begin their secretive existence there. In fact, these are all the same malicious computer programs, but lacking the ability to reproduce their copies through files of other programs. The trojan is created already completely ready for work. Computer Trojans usually have as their goal spyware or thieves, during which they can send spam from an infected computer, record and send information entered on the keyboard, collect and steal all kinds of passwords, carry out secret remote control of the infected computer via the Internet, and much more. The classification of trojans is quite extensive. Today you can find ransomware trojans, trojans for sending spam from an infected computer (spam bots from the English Spam bot), trojans for remote control of an infected computer (backdoors from the English backdoor), trojans for the secret or deceitful installation of other trojans (droppers), trojans for covert download from the Internet of other trojans (downloaders). It is also worth mentioning trojans for stealing passwords from an infected computer (for example, passwords from messenger programs, social networks, online games) and trojans for automatically infecting a computer via the Internet. Recently, Trojans pretending to be anti-virus programs have been quite popular.

The following Trojan programs are most common:

1. Keyloggers (Trojan-SPY) - Trojans that are constantly in memory and store all the data coming from the keyboard for the subsequent transfer of this data to the attacker. Usually in this way an attacker tries to find out passwords or other confidential information.

2. Password hijackers (Trojan-PSW) - trojans, also designed to receive passwords, but do not use keyboard tracking. Typically, such Trojans implement methods for extracting passwords from files in which these passwords are stored by various applications.

3. Remote management utilities (Backdoor) - trojans that provide complete remote control over a user's computer. There are legal utilities of the same property, but they differ in that they inform about their purpose during installation or are supplied with documentation that describes their functions. Trojan remote control utilities, on the contrary, do not give out their real purpose, so the user does not suspect that his computer is controlled by an attacker. The most popular remote control utility is Back Orifice.

4. Anonymous smtp-servers and proxies (Trojan-Proxy) - trojans that perform the functions of mail servers or proxies and are used in the first case for spam mailings, and in the second for hackers to trace tracks.

5. Browser settings modifiers (Trojan-Cliker) - Trojans that change the start page in the browser, the search page, or any other settings for organizing unauthorized access to Internet resources.

6. Installers of other malicious programs (Trojan-Dropper) - trojans that provide an opportunity for an attacker to perform a hidden installation of other programs.

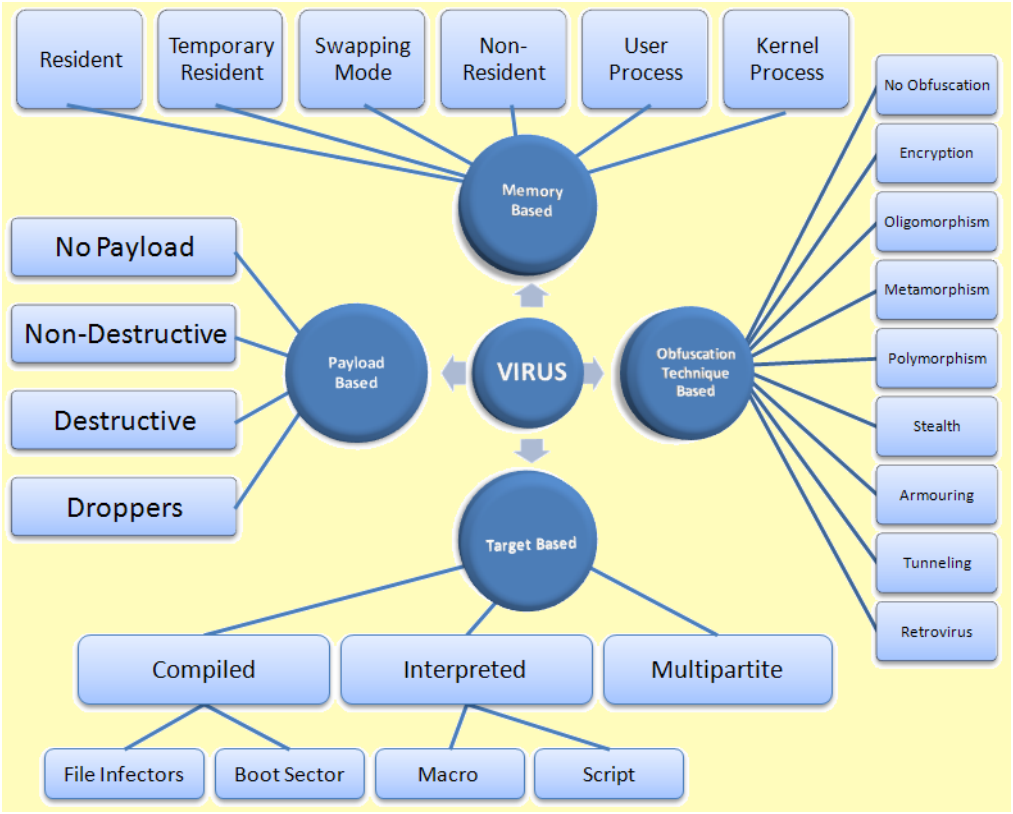
7. Trojan Downloader - Trojans designed to download new versions of malware, or adware, to a victim computer.

8. Trojan-Notifier - Trojans of this type are designed to inform their "host" about an infected computer.

9. "Bombs" in archives (ARCBomb) - trojans, which are archives specially designed in such a way as to cause abnormal behavior of archivers when trying to unzip data - freezing or significant slowdown of a computer, filling a disk with a lot of "empty" data.

10. Logical bombs - more often not so much trojans as trojan components of worms and viruses, the essence of which is to, under certain conditions (date, time of day, user actions, external command), perform a certain action: for example, data destruction.

11. Dialing utilities - a relatively new type of trojan, which is a dial-up utility for accessing the Internet through paid mail services. Such trojans are registered in the system as the default dialer utilities and entail large bills for using the Internet (Pic 1). [2].




Pic 1. Types of "Virus"

Vulnerabilities in operating system modules contribute to Trojan infection. They also pose a threat to the computer's security interms of Trojans infected vulnerabilities in the web browser and its plug-ins (extensions). Despite the fact that Internet Explorer, the most popular browser among users, is gradually losing ground, the main vector of attackers is aimed specificall at this browser. For invisible penetration of a trojan through a vulnerable browser, attackers use the so-called exploits - special data codes that cause memory corruption and allow access to its neighboring areas, which ultimately allows the Trojan to infect a computer. Vulnerability in browser plug-ins is associated with extensions such as Adobe Flash Player for displaying FLASH animations in a browser or Adobe Acrobat Reader for displaying PDF documents in a browser. To prevent computer infection through the Internet, you need to use high-quality anti-virus

programs equipped with web filters. Only reliable products of two Russian companies can be attributed to reliable anti-viruses: Kaspersky Labs and DRWeb [3].

In addition to the secret trojan infection, there is the possibility of open infection with the Trojan - the user actually gives the attacker a "green light" when the Trojan is "offered" to the user under the guise of something useful. The method of misleading the user by communicating to him important data that is actually false, is currently experiencing another round of its development. New techniques have not yet been discovered, old and long-tried are used on an appalling scale. One of the most striking examples of this technique is phishing attacks. Phishing is a type of online fraud whose purpose is to obtain user credentials. Organizers of phishing attacks send emails on behalf of popular brands and insert links to fake sites into them. Once on this site, the user runs the risk of informing criminals of valuable information, such as their credit card number. You can often stumble upon banners and pop-ups that mimic the interface of the Windows operating system. When hackers try to install a virus on someone's computer, in most cases they need the user to personally run the program. To convince the owner of the computer to do this, the virus is usually passed off as some useful software. Faking under system messages, banners "find" non-existent viruses and trojans on the computer, and then offer to install a certain antivirus, which is actually a Trojan. Thus, the user is fraudulently forced to voluntarily install the trojan into his computer, somewhere playing on curiosity, and somewhere on inattention and fear [4].

It is also worth mentioning such methods of infection with Trojans as instant messaging systems (ICQ, MSN Messenger, etc.), as well as e-mail, which began the era of computer virus infection via the Internet. Now this method of reproduction can no longer be called popular, since anti-virus products and security systems on mail servers have learned with enviable success to find and neutralize computer viruses and trojans in e-mail. The infection vector of Trojans and viruses via the Internet has shifted towards infected websites. According to statistics from anti-virus companies, the content of viruses and trojans in e-mail today is at the level of 2-3 percent of the total number of letters, which in itself is small. But, nevertheless, e-mail cannot be completely deducted. You should never open and run attachments in emails from unknown senders. Recently, attackers began to send links to an infected site instead of attachments in their letters, therefore, clicking on links in letters from unknown senders is also not recommended. As for instant messaging systems, here again it is possible to run into links to infected sites, which can be sent in your message to one of the contacts whose computer is currently infected with the Trojan, or if the client's number and password could be known to attackers.Consider some of the features of information security threats recorded in 2010, which can be called the heyday of Internet fraud [5].

1. Banking Trojans. The first place in the list of cyber pests is awarded to banking Trojans. This category of malware includes those that are aimed at obtaining unauthorized access by attackers to the accounts of individuals and legal entities through remote banking systems. The latter are now rapidly gaining popularity, and criminals seek to take advantage of this popularity. It is likely that in 2011 we will witness a shift in the sphere of interests of Internet fraudsters from private users to legal entities, on whose accounts much more significant amounts of money are concentrated.

2. Windows blockers. The second place is rightfully occupied by the classic Windows blockers, which have kept users and experts of antivirus companies in suspense since the fall of 2009. Windows blockers include malware that displays a window (blocking other windows) with the requirements of attackers. Thus, the user is deprived of the opportunity to work on the computer until he pays for the unlock. A variety of such blockers, as well as fraudulent pretexts, is shocking - from the requirements to pay a fine for using pirated software to the requirements for paying for the ordered content.

3. Data encryptors. In 2010, many new modifications of encryption Trojans appeared, the purpose of which is user documents. After the Trojan encrypts the documents, information is displayed that it is necessary to send money to the attackers for the decryption. In the vast majority of cases, virologists quickly develop utilities with which you can decrypt user data, but since it is not always possible and attackers require significant amounts of money to decrypt, Trojan.Encoder is on the third line of our top ten.

4. Redirectors to malicious and fraudulent sites. These malicious programs are created by cybercriminals to modify the hosts system file in such a way that when they try to access a popular site, a fake site with a design similar to the original is displayed in an Internet browser. Usually, access to most search engines is blocked in order to deprive the user of the opportunity to "deal with" the virus on their own. Moreover, money will be required from the user under various pretexts. The most popular scam requirements are: the user must send an SMS to unlock access to the social network; the user must send an SMS to confirm that he is not a bot. At the same time, some viruses change the path to the hosts file in the registry, thus reducing the likelihood that the average user will cope with the malware on his own.

5. False antiviruses. False antiviruses look like antivirus software, and often their design resembles several antivirus products at once. But these malware have nothing to do with antiviruses. Once installed in the system, such "antiviruses" immediately report that the system is allegedly infected, and for the treatment of the system it is supposedly necessary to purchase a paid version of the antivirus program. In some cases, they threaten to delete all information from the hard drive or make the computer unusable.

6. Blockers launch IM-clients. For several months in 2010, attackers spread a malicious program that blocked the launch of popular instant messaging clients. Users of ICQ, QIP and Skype were under attack. The IM client was replaced by a similar interface malware, in which, upon startup, the user was informed that his account was blocked for spamming, and to restore access to the corresponding service, it was necessary to send an SMS message, naturally, to a paid number.

7. False archives. Attackers invented and implemented dozens of schemes for obtaining illegal income, and the malware itself fell on hundreds of millions of computers [6].

Almost all Internet users have come across such a window at least once in their life. Attackers create fake torrent trackers or file storages from which you can supposedly download popular or rare content. These resources appear in the first lines of popular queries in search engines. Using such a resource, the victim receives an allegedly self-extracting archive with the desired information for downloading. In reality, the "archive" turns out to be an executable file (* .exe), the interface and icon are very similar to a self-extracting archive. The difference between such an archive and the present is that in the process of "unpacking" at a certain moment the user is informed that a certain amount of money must be paid to complete the process.

8. Bootlockers. In November 2010, a blocker was distributed, which, during infection, is recorded in the boot area of the hard drive, thereby blocking the loading of the operating system used. When you turn on the computer, information with the requirements of the attackers is displayed on the user's screen.

Like any application, computer viruses can be divided into two main stages of the life cycle - storage and execution. The storage stage corresponds to the period when the virus is simply stored on the disk together with the object to which it is embedded. At this stage, the virus is most vulnerable to antivirus software, as it is not active and cannot control the OS for self-defense. Some viruses at this stage use mechanisms to protect their code against detection. The most common method of protection is to encrypt most of the body of the virus. Its use in conjunction with code-mutation mechanisms (discussed below) makes it impossible to isolate signatures - persistent virus code snippets [7].

The stage of execution of computer viruses, as a rule, includes five stages: 1) loading the virus into memory; 2) search for the victim; 3) infection of the found victim; 4) performance of destructive functions; 5) transfer of control of the program-carrier of the virus. Let's look at these steps in more detail.

Downloading the virus. The virus is loaded into memory by the OS at the same time as the executable object into which the virus is embedded. For example, if a user executes a program file containing a virus, then obviously the virus code will be loaded into memory as part of that file. In the simplest case, the process of downloading the virus is nothing more than copying from disk to RAM, sometimes accompanied by setting addresses, after which the transfer of control of the code body of the virus. These actions are performed by the OS, and the virus itself is in a passive state. In more complex situations, the virus can, after obtaining control, perform additional actions that are necessary for its functioning. In this regard, two aspects are considered. The first aspect is related to the maximum complication of the virus detection procedure. Some viruses use sophisticated algorithms to provide protection during storage. Such complications include encryption of the main body of the virus. However, the use of encryption only is half-way, since the part of the virus that provides the decryption of the virus at the boot stage should be kept open. To avoid such a situation, virus developers use mechanisms of "mutations" of the decryptor code. The essence of this method is that when embedded in the object of a copy of the virus, part of its code related to the decoder is modified so that there are textual differences with the original, but the results of the work remain unchanged. The following code modification techniques are commonly used:

- changing the order of independent instructions;
- replacement of some instructions with equivalent results;
- replacement of registers used in the instructions for others;
- introducing randomly noisy instructions.

Viruses that use similar mechanisms of code mutation are called polymorphic viruses. When sharing encryption and mutation mechanisms, the embedded copy of the virus will be different from the original, as one part of it will be modified and the other will be encrypted on a key created specifically for that copy of the virus. And this significantly complicates the detection of the virus in the computer system. Polymorphic

viruses (polymorphic) are hard-to-detect viruses that have no signatures, that is. E. Containing no permanent section of code. In most cases, two samples of the same polymorphic virus will have no coincidence. Polymorphism is found in viruses of all types - file, boot, and macro [8].

The additional steps that polymorphic viruses perform at the download stage are to decipher the main body of the virus. When using stealth algorithms, viruses can completely or partially hide themselves in the system. The most common stealth algorithm intercepts system requests to control OS actions. Viruses that use stealth algorithms are called stealth viruses. Stealth viruses (Stealth) are able to hide their presence on the system and avoid detection by antivirus programs. These viruses can intercept OS requests to read / write infected files, while they either temporarily treat these files, or "substitute" for themselves uninfected pieces of information, emulating the "purity" of infected files.

In the case of macros, the most popular way is to bar calls from the macro view menu. One of the first file stealth viruses was the "Frodo" virus, the first bootstrapping stealth virus was the "Brain" virus. Often, viruses use a variety of non-standard techniques to delve deeper into the core of the OS, either to protect against the detection of their resident copy, or to complicate treatment against the virus.

The second aspect is related to the so-called resident viruses. Since the virus and the object in which it is embedded, are for the OS as a whole, they are naturally located in a single address space after download. Upon completion of the object, it is unloaded from memory, while also unloading the virus, going into the passive storage. However, some types of viruses are capable of being stored in memory and remain active after the end of the virus carrier. These viruses are called resident.

Resident viruses, when infected with a computer, leave in memory their resident part, which then intercepts the OS access to the objects of infection and introduced into them. Resident viruses are in memory and are active until the computer is shut down or OS restarted. Macro-viruses can be considered as resident, since for most of them the basic requirements are fulfilled - constant presence in the computer memory for the whole time of work of the infected editor and interception of functions used in working with documents. In this case, the role of the OS takes on the editor, and the concept of "reboot operating system" is treated as an exit from the editor [9].

Non-resident viruses do not infect your computer memory and retain activity for a limited time. Some viruses leave small resident programs that do not spread the virus in memory. Such viruses are considered non-resident. It should be noted that the distribution of viruses into resident and non-resident is true mainly for file viruses. Boot viruses, like macroviruses, are resident viruses.

**Conclusion and prospects for further research**

Analyzing all of the above, we can conclude that in the face of a significant increase in countering virus attacks and a significant increase in user literacy in the field of countering Internet threats, virus writers and hackers are forced to actively develop methods of the social formation that a certain amount of money must be paid to complete the process. In fact, the user is deceived twice - sends money to attackers and does not receive any information that is useful to himself.

The process of developing malicious programs and means of countering them is a constant war of technologies. Original ideas are regularly implemented in viruses, which requires adequate actions from antivirus software developers. The authors strongly recommend that you follow the news on the websites of anti-virus companies and follow the advice of information security experts about the need to update software (not only anti-virus) or perform specific actions to improve computer security.

**References**

1. Bragg, R. Network Security. Complete Guide / R. Bragg, M. Rhodes-Ousley, K. Strasberg. - M.: Ecom, 2006. - 912 p. - ISBN 5-7163-0132-0.
2. Gordon, J. Computer viruses without secrets / J. Gordon. - M.: New publishing house, 2006. - 320 p. - ISBN 5-9643- 0044-8.
3. Devyanin P.N. Analysis of security of access control and information flow in computer systems / P.N. Devian. - M.: Radio and communication, 2006. - 176 p. - ISBN 5-256-01768-3.
4. Kaspersky K. Computer viruses: inside and out / K. Kasperski. - St. Petersburg. : Peter, 2005. - 528 p. - ISBN 5-469-01282-4
5. Kozlov D.A. Encyclopedia of computer viruses / D.A. Kozlov, A.A. Parandovsky, A.K. Parandovsky. - M.: SOLON-R, 2001. - 464 p. - ISBN 5-93455-091-8.
6. Sobeykis V.G. Alphabet of the hacker 3. Computer virology / V.G. Sobekis. - M.: Major, 2006. - 512 p. - ISBN 5-98551-013-1.
7. Stolings V. Fundamentals of Network Protection. Applications and Standards / W. Stallings. - M.: Williams, 2002. - 432 p. - ISBN 5-8459-0298-3.
8. Hamidullin R.R. Methods and means of protection of computer information: Textbook. / R.R. Hamidullin, I.A. Brigadnov, A.V. Frost. - St. Petersburg: OSTU, 2005. - 178 p.
9. Khoroshko V.A. Methods and means of protection of information. / V.A. Khoroshko, A.A. Chekatkov. - K .: Junior Publishing House, 2003. - 504 p.