International Journal of Academic and Applied Research (IJAAR)
ISSN: 2643-9603
Vol. 5 Issue 1, January - 2021, Pages: 27-30

Means of Information Protection

Usmonov Makhsud

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
maqsudusmonov22@gmail.com

Abstract: *Hardware and software of information protection - various electronic devices (independently or in combination with other means) that perform information protection functions (user identification and authentication, restriction of access to resources, event logging, cryptographic protection of information, etc.) are special programs. Data protection software is special software designed to ensure information security and is included in computer software. Protection against computer viruses and other programs and changes is an independent area of protection of information processing in computer systems.*

Keywords: Computer data protection techniques. Computer data protection software. Mixed means of computer data protection.

INTRODUCTION

1. Technical means of computer data protection.

2. Computer data protection software.

3. Mixed means of computer data protection.

Hardware and software means of information protection - various electronic devices and special programs that perform information protection functions (user identification and authentication, restriction of access to resources, event logging, cryptographic protection of information, etc.) (independently or in combination with other means) . Data protection software is special software designed to ensure information security and is included in computer software. Protection against computer viruses and other programs is one of the independent ways to protect the processing of information in computer systems. Inadequate assessment of this risk can have serious negative consequences for users 'information. The security of a network is determined by the security of all the computers and network devices on it. An intruder can discredit an entire network by disrupting the work of any of the network's founders. Software and hardware tools called "firewalls" are used to block threats from the network that everyone uses. Information security software means special programs that are designed to provide information security only and are included in the software of computer tools. The main software tools for information protection include: - programs that identify and authenticate users in computer systems; - programs that restrict the rights of users of computer system resources; - information encryption programs; - programs that protect information resources (system and application software, databases, computer systems of education, etc.) from illegal alterations, use and reproduction. The term identification, in the sense of information security in computer systems, refers to the unique recognition of the unique name of a computer systems entity. Authentication means confirming that the name provided matches the subject (authenticating the subject). Examples of data protection utilities include:

METHODS

- programs that delete residual information (cache, temporary files, etc.); - Audit programs used to recover various events and incidents related to the security of computer systems and to prove that such events and incidents have occurred (record keeping); - programs that simulate the work with the offender (misleading the offender as if he received confidential information); - control programs for testing the security of computer systems, etc. Advantages of data protection software include: - ease of reproduction; - flexibility (the ability to configure certain computer systems used in different conditions, taking into account the specifics of the threat to information security); - Ease of use - some programs, such as encryption programs, operate in a "transparent" (invisible to the user) mode, while others do not require any additional new (compared to other programs) skills; - by modifying them to account for new threats to information security the existence of the existing limitless possibilities of factoring. Disadvantages of information security software include: - Decreased efficiency of security systems due to the use of computer system resources; - very low efficiency (compared to hardware that performs the same function, for example, an encryption device); - the fact that many information protection software is not directly installed in the computer software (pictures below), which in principle creates a fundamental opportunity for the violator to bypass these programs; - the ability to intentionally modify information security

software when using computer systems. Protection against computer viruses and other programs is one of the independent ways to protect the processing of information in computer systems. Inadequate assessment of this risk can have serious negative consequences for users 'information. Knowledge of the mechanisms of action of viruses, methods and means of combating them allows you to effectively organize anti-viral actions, minimize the likelihood of damage and losses from their effects. Computer viruses are small-scale executable programs that spread and self-develop in computer systems. Viruses can destroy or delete software or data stored on computer systems. Viruses can modify themselves as they spread. The seriousness of the consequences of the mass spread of viruses and their impact on the resources of computer systems has led to the need to create and use special antivirus tools and methods of their use. Antivirus tools are used to solve the following problems: - detection of viruses in computer systems; - virus - blocking programs;

- Eliminate the effects of viruses. It is advisable to detect viruses at the stage of their deployment, or at least before the onset of the virus's destructive functions. It should be noted that there are no antivirus tools that can detect all types of viruses. If a virus is detected, the virus should be stopped immediately to minimize the potential for harmful effects on the system. Elimination of the effects of the virus is carried out in two ways: - removal of the virus; - Recover files, memory areas. System recovery depends on the type of virus, the time it was detected, and the time it started to infect. If viruses delete data from a storage location during the login process and the data is intended to be modified as a result of malware, the lost data cannot be recovered without backing up the data. . Anti-virus software uses software and hardware that are used in a specific sequence and combination to create anti-virus methods. One of the main conditions for the safe operation of a computer system is to follow a number of rules that have been tested in practice and proved to be highly effective. The first rule is to use legally licensed software. Pirated copies of the software are more likely to contain viruses than official ones. The second rule is to create a data backup. You must first save the media on which the software distributions are written. If possible, carriers should be able to block data if possible. Care should be taken to keep work-related information secure. It is necessary to make backup copies of files related to regular work and store them in removable media protected from writing. If such copies are being made on non-removable media, it is a good idea to create them in the permanent memory of a completely different computer. This saves either the full copy of the file or copies of the changes being made. The third rule is the regular use of antivirus tools. Antivirus tools should be updated regularly. The fourth rule is to be careful when using new removable media and new files. When new removable media are obtained, of course, the presence of bootable and file viruses must be checked, and the resulting files must be checked for the presence of file viruses. Verification should be done using scanning software and programs that perform heuristic analysis . When working with received documents and tables, it is necessary to disable the execution of macros built into text and table editors until these files are fully scanned. The fifth rule is to scan the system, especially distributed systems or shared systems, for files and removable media on special computers. It is best to do this from an automated workstation of the system administrator or the person responsible for data security. Disks and files can be made available to users of the system after a thorough antivirus scan. The sixth rule is to block such actions unless they are intended to be written to the media.

Adherence to the above recommendations will significantly reduce the risk of virus infection and protect the user from irreparable loss of information. The integrity of the information in the system and the right to use it during the stages of using the computer network is ensured by: - the integrity of the information available in the computer system; - increase the resistance of computer systems to rejection; - elimination of system reboots and "hangs"; - creation of information resources; - use a well-defined set of programs; - adherence to specific procedures for maintenance and replenishment; - Carry out a set of antivirus measures. Integrity and ease of use of information is achieved through the creation of a backup of hardware, blocking user error, the use of reliable elements of computer systems and stable operating systems. Threats of intentional overuse of system elements are eliminated. To do this, the program uses mechanisms to measure the intensity of the arrival of orders and mechanisms to limit or block such orders. In such cases, the possibility of detecting a sudden increase in the flow of orders for data transmission or execution of programs should also be considered in advance. One of the main conditions for ensuring the integrity and usability of information in a computer network is to create a backup of it. The strategy of creating an information backup is chosen taking into account the importance of information, the requirements for the uninterrupted operation of computer systems, the difficulty of data recovery. Only authorized software should be used on secure computer systems. The list of programs that are officially allowed to be used, the methods of checking their integrity, and the frequency of their use must be determined before computer systems can be put into operation. One of the simplest ways to control the integrity of a program is through a set of controls. A control sum is a sequence of bits written to the end of a data block. It is necessary to save the control set in encrypted form or to use a secret algorithm for calculating the control sum in order to exclude the modification of the control file by modifying the control set and closing it.

RESULTS

- Eliminate the effects of viruses. It is advisable to detect viruses at the stage of their deployment, or at least before the onset of the virus's destructive functions. It should be noted that there are no antivirus tools that can detect all types of viruses. If a virus is detected, the virus should be stopped immediately to minimize the potential for harmful effects on the system. Elimination of the

effects of the virus is carried out in two ways: - removal of the virus; - Recover files, memory areas. System recovery depends on the type of virus, the time it was detected, and the time it started to infect. If viruses delete data from a storage location during the login process and the data is intended to be modified as a result of malware, the lost data cannot be recovered without backing up the data. . Anti-virus software uses software and hardware that are used in a specific sequence and combination to create anti-virus methods. One of the main conditions for the safe operation of a computer system is to follow a number of rules that have been tested in practice and proved to be highly effective. The first rule is to use legally licensed software. Pirated copies of the software are more likely to contain viruses than official ones. The second rule is to create a data backup. You must first save the media on which the software distributions are written. If possible, carriers should be able to block data if possible. Care should be taken to keep work-related information secure. It is necessary to make backup copies of files related to regular work and store them in removable media protected from writing. If such copies are being made on non-removable media, it is a good idea to create them in the permanent memory of a completely different computer. This saves either the full copy of the file or copies of the changes being made. The third rule is the regular use of antivirus tools. Antivirus tools should be updated regularly. The fourth rule is to be careful when using new removable media and new files. When new removable media are obtained, of course, the presence of bootable and file viruses must be checked, and the resulting files must be checked for the presence of file viruses. Verification should be done using scanning software and programs that perform heuristic analysis . When working with received documents and tables, it is necessary to disable the execution of macros built into text and table editors until these files are fully scanned. The fifth rule is to scan the system, especially distributed systems or shared systems, for files and removable media on special computers. It is best to do this from an automated workstation of the system administrator or the person responsible for data security. Disks and files can be made available to users of the system after a thorough antivirus scan. The sixth rule is to block such actions unless they are intended to be written to the media.

DISCUSSION

Adherence to the above recommendations will significantly reduce the risk of virus infection and protect the user from irreparable loss of information. The integrity of the information in the system and the right to use it during the stages of using the computer network is ensured by: - the integrity of the information available in the computer system; - increase the resistance of computer systems to rejection; - elimination of system reboots and "hangs"; - creation of information resources; - use a well-defined set of programs; - adherence to specific procedures for maintenance and replenishment; - Carry out a set of antivirus measures. Integrity and ease of use of information is achieved through the creation of a backup of hardware, blocking user error, the use of reliable elements of computer systems and stable operating systems. Threats of intentional overuse of system elements are eliminated. To do this, the program uses mechanisms to measure the intensity of the arrival of orders and mechanisms to limit or block such orders. In such cases, the possibility of detecting a sudden increase in the flow of orders for data transmission or execution of programs should also be considered in advance. One of the main conditions for ensuring the integrity and usability of information in a computer network is to create a backup of it.

CONCLUSION

The security of a network is determined by the security of all the computers and network devices on it. An intruder can discredit an entire network by disrupting the work of any of the network's founders. Software and hardware tools called "firewalls" are used to block threats from the network that everyone uses. Information security software means special programs that are designed to provide information security only and are included in the software of computer tools. The main software tools for information protection include: - programs that identify and authenticate users in computer systems; - programs that restrict the rights of users of computer system resources; - information encryption programs; - programs that protect information resources (system and application software, databases, computer systems of education, etc.) from illegal alterations, use and reproduction. The term identification, in the sense of information security in computer systems, refers to the unique recognition of the unique name of a computer systems entity. Authentication means confirming that the name provided matches the subject (authenticating the subject). Examples of data protection utilities include:

REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

3 Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

4Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

5 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.