Computer security

Habovets Y., Denisenko L., Krasnova E.

Computer technology is increasingly becoming part of our lives. Today, few of us are able to spend a day without using gadgets and the Internet. Communication cannot be represented without correspondence in messengers and social networks. All human life or it`s important aspects are stored in one`s phones, computers or any other device. All of these trends require a well-developed system of protection, which will not allow the attackers to access personal information of the person. Today, computer security is developing at the same tremendous pace as technology. But let's see in details what computer security is?

The majority of people involved in business and using the Internet is definitely aware of how important the security of the network is. Any transactions occurring in the company, whether the development plans, and the turnover of important documents or actions with finance, without proper protection sooner or later will become known to attackers. Unfortunately, this is the truth with the world, everything that was not protected on the network, will be stolen. The computer system is totally safe when switched off, disassembled, or locked under a key that was destroyed. In all other cases there is a chance of losing sole control over it. First of all, to increase security you need to use passwords of a certain complexity. The safest of them should include lowercase and Superscript Latin letters, numbers and characters, e.g. "_".

Another integral part of the system security and computer is antivirus software. Thus whatever the software has not been installed, the system can only protect the user. Reliable computer protection is ensured by the proper use of antivirus programs. The user should scan for viruses all of the media that is connected to the computer, to adhere to certain rules when working with email. It is very important to use only certified antivirus software packages. Today in Russia, these are the Kaspersky and Dr.WEB.

What is an antivirus program? Antivirus program (antivirus) - program to detect computer viruses and unwanted programs in General, and restore contaminated with such programs, files, and also for prevention of infecting files or operating system with malicious code.

Good antivirus software should provide effective protection in real time, to check the contents of the hard disk automatically or using the manual start, to be able to protect your computer even against unknown viruses, repair infected files, receive daily updates of your software and to ensure top-notch security.

It is also important to follow the method of connection to the network. The connection must be secure; otherwise, just connecting to the computer it immediately becomes almost completely open to intruders. Connection security is ensured by special encryption technology. When exchanging information in this connection it uses a special Protocol to transfer data, which your computer and a server know a secret key that allows both encryption and decryption of information.

Here we come to one of the most important processes of computer security - the encryption. It is engaged in a special branch of mathematics - cryptography. Cryptography primarily consists of two major areas: cryptography (encryption directly) and methods of disclosure (cryptanalysis). Consider the principle of operation of cryptographic systems. The aim of the work is that the text that was written by someone else, or any other information (all of this is called clear text), was turned into a completely incomprehensible jumble of characters (ciphertext, cryptogram). In its turn, the recipient who is to receive the transmitted information must be able to decode (decrypt) it. Thus a cryptanalyst who is considered the opponent should not be able to decrypt the cryptogram. If he was able to decrypt the data and he is able to do the same with any other information encrypted by the cryptosystem, then we say that the cryptosystem has been disclosed.

To ensure maximum safety of information cryptography should follow the next rule, which has been made by the Dutchman Kerkhoff: cipher strength should be determined only by the secrecy of the key. In other words, the rule is that the whole encryption mechanism, in addition to the secret key, is initially known to the adversary.

There are two kinds of cryptosystems: symmetric (secret-key) and asymmetric (public key). The first is characterized by the presence of a universal key capable to encrypt and decrypt the information. The key must be kept confidential by both parties. This is kryptonite that has its pros and cons. It is believed that the complexity of the key, the more unlikely will be the opening of just such a system. Also it has simplicity and great speed.

Asymmetric system assumes the existence of two keys - private and public. One of the keys is used to encode information and the other - for decryption. The public key is freely available to everyone, a secret is available only to one person - the recipient of the information. The system enhances security as only one person has an access to information. Cryptographic protection is a relatively cheap method of protection and the tools to overcome it, or has an incredibly high price or doesn`t not exist a priori. To find out how secure the cryptosystem is one must fully know the algorithm of its work. Only by fulfilling this condition, it is possible to check the stability protection. Only a specialist is able to do this, and it is very often when the system is so complex that inspection is economically feasible. Cryptography is a very important part of computer and information security, so any country in the world pays special attention on it and strictly controls everything about it. To be eligible for the creation of cryptographic products, the company must be certified. To obtain such a certificate is a very difficult task, sometimes it is even impossible.

In the twenty-first century technologies stepped forward so much that there were devices even without access to the system able to read someone else's information. Therefore, another integral part of keeping data safe is active (physical) protection. It is used when certain source of danger can appear. Usually the following measures are taken:

• Search and disabling of devices capable of intercepting the transmitted information

• Search and detention of persons who install such devices

• Identifying potential vulnerabilities in the security system that will help cyber criminals to gain unauthorized access, and so on.

Nowadays various electronic masking devices are actively applied to create broadband noise signal that interferes with the operation of devices that can be used by attackers to gain access to information.

Thus, it becomes clear that computer security and information protection are now actively developing. And it is not only a natural feature, but a necessity. If these directions are a little slow, in our information age, it can lead to absolutely unpredictable consequences. A huge responsibility today rests on the shoulders of future professionals in computer and information security. It is quite clear that perfect methods of protection do not exist. There

is no such antivirus which will always protect your computer from danger. All this is proved mathematically based on the theory of finite automata. Data security is first of all only in our hands. If we use a special software, it will increase our data security level which is so precious.

List of used literature and internet resources

- Torokin A. A. Engineering and technical protection of information - Ed. Gelios ARV, 2005
- Galkin A. P. Assess the need for information protection of the enterprise - Bulletin of the Association of Russian evaluation. 1999. No. 1. P. 55-58.
- Sobolev A. N., Kirillov V. M. Physical foundations of technical means of information security. - M.: Gelios ARV, 2004
- D. McNamara Secrets of computer espionage: Tactics and countermeasures. Per. from English. - M.: Publishing House. BINOM, 2006.
- Petrakov A.V. foundations of practical information security. - M.: SOLON-Press, 2006
- ru.wikipedia.org