Security and protection of information in networks
Shamuhamedov G. [1], Hydyrov N. [2] (Republic of Turkmenistan)

Безопасности и защиты информации в сетях
Шамухамедов Г. Х.[1], Хыдыров Н. К.[2] (Республика Туркменистан)

[1]Шамухамедов Гуванч Ходжамухамедович / Shamuhamedov Guvanch –преподаватель, кафедра информационных технологий;
[2]Хыдыров Недир Какамырадович / Hydyrov Nedir – студент, факультет финансов,
Туркменский государственный институт финансов, г. Ашхабад, Республика Туркменистан

Abstract: *in modern times all the more clearly a tendency to increase the volume of information, including critical for individuals, businesses, organizations or states, which are stored, processed and transmitted by means of automated data processing systems for telecommunications channels.*
Аннотация: *в наше время все более отчетливо наблюдается тенденция к увеличению объема информации, в том числе важное значение для отдельных лиц, предприятий, организаций или государствами, которые хранятся, обрабатываются и передаются с помощью автоматизированных систем обработки данных для телекоммуникационных каналов.*

Keywords: *unauthorized access, eavesdropping, substitution of attribution information, modification of information, physical protection*
Ключевые слова: *несанкционированного доступа, подслушивания, замена информации атрибуции, модификация информации, физическая защита*

The widespread use of computer technology in automated data processing systems and management exacerbated the problems of protection of information circulating in computer systems from unauthorized access. Protecting information in computer systems has a number of specific features associated with the fact that information is not strictly related to the carrier can be easily and quickly copied and transmitted over communication channels. We know a very large number of threats to information that may be implemented as from outside intruders, and by the insiders. [6]

Problems arising from the security information transmission when the computer networks can be divided into three main types:

- interception - the integrity of the information stored, but her privacy violated;
- substitution authorship information - this problem can have serious consequences. For example, if someone could send a letter on your behalf (this type of fraud is called spoofing) or Web - server can pretend to electronically store, take orders, credit card numbers, but do not send any goods.
- modification of information - in this case the original message is edited or changed completely, and the other is sent to the recipient.

In computer networks (BC) focused information belongs to certain people who are in the personal initiative or in accordance with the official duties, and only they have the right to use this information. Such information must be protected from all forms of outside interference, especially from reading and copying of this information, people who do not have the right to access this information.

Physical protection of systems and data can be carried out only with respect to communication nodes and workstations, and is impossible to transfer funds, which have a greater length. For this reason, in networks to be used means precluding unauthorized access to data and ensuring their privacy. [2]

The main areas of information security in computer networks (AC) are:

- improving the institutional and organizational and technical measures of information processing technology in the computer;
- blocking unauthorized access to the information processed in a computer;
- blocking unauthorized information by technical means.

It should identify the main factors hindering a solution of information security in the sun:

- mass application;
- an ever-growing complexity of the operation;
- a variety of PC software, architecture and easy adaptability to solve various user tasks.

Difficulties encountered in organizing the protection of computer networks:

- extended range of control - therefore a separate subnet administrator has to monitor the activities of users who are beyond his reach;
- unknown perimeter - the network is easy to expand, and this leads to the fact that determine the precise boundaries of the network is often difficult, the same unit may be available for the users of different networks;

- use of a variety of software and hardware - connection of several systems in a network increases the vulnerability of the entire system because each system is configured to perform its security requirements, which may be incompatible with the requirements of other systems;

- difficulty in the management and control of access to the system - many attacks on the network can be made from remote locations without the physical access to a particular site. In such cases, the identification of the offender, as a rule, it is very difficult;

- multipoint attacks - one and the same set of data may be transferred in networks via several intermediate nodes, each of these nodes it is a potential source of danger.

In addition, the majority of networks can be accessed via Wi-Fi or Internet, which greatly increases the number of possible points of attack. Such a method is very easy to implement and equally difficult to control, so it is considered one of the most dangerous.

Consider the technology of Wi-Fi. Wi-Fi was created in 1991 in the Netherlands. Products Wi-Fi, which were originally designed for systems and cash services, present on the market under the name WaveLAN. It provides data rates from 1 to 2 Mbit / s.

Wi-Fi (Eng. Wireless Fidelity - «Wireless Fidelity") - standard equipment Wireless LAN. Wi-Fi is a wireless data transfer protocol, which makes a number of computers to connect to the network, or to connect them to the Internet, a short-range, which uses radio waves.

Wi-Fi technology is developed based on the IEEE 802.11 standards consortium Wi-Fi Alliance.

Currently, many organizations use Wi-Fi. This is due to the fact that under certain conditions, the performance of the network already exceeds 100 Mbit / sec. Users are able to move between access points in the network coverage Wi-Fi.

Also, now many mobile devices (smartphones, tablets, and PDAs) equipped with Wi-Fi devices that allows you to connect over a local network to the Internet through an access point.

As a rule, the usual circuit Wi-Fi network includes at least one client and at least one access point (access point). In this case, all the computers must be equipped with wireless cards (customers). They are connected directly with each other via radio, which operates under the standard 802.11b. The scheme of such a compound is shown in Figure 1.1.

Figure 1.1 - Connection of the "point-point"

In this case, the clients are connected via network adapters "directly", and the access point is not used. Being transmitted network identifier SSID (Eng. Service Set IDentifier, Network name - the network identifier, network name) from the access point by using special signaling packets at speeds of 0.1 Mbit / s every 100 ms. Thus, the 0.1 Mbit / s - the lowest rate of data transmission technology using Wi-Fi. If the client knows the network identifier (SSID), it can determine whether you can connect to a given access point. If the area of the access point contains two identical SSID, in this case, the receiver selects one or the other on the basis of the signal level. When using Wi-Fi transmitted data on the air. Therefore, Wi-Fi has properties that are similar to the nonswitched network, and it can occur the same problems as when dealing with non-switched networks.

Another way - a model of infrastructure connections. With this model all computers equipped with wireless cards and connect to an access point that has the ability to connect to a wired network. This model is used to connect more than two computers.

The scheme of such a compound is shown in Figure 1.2. It is worth mentioning the expansion of this model through the repeater. When using this device, the access point simply extends the range of another access point operating in infrastructure mode.

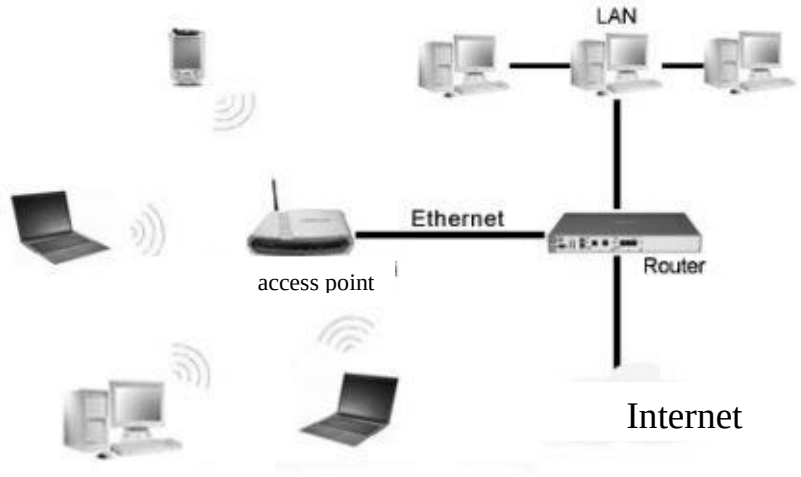

Fig. 1.2 - Infrastructure Connect

Another way to connect is to connect with a modem and a router. The AP is included in a router, the router is switched to the modem (these devices can be combined). Now on every computer in the range of Wi-Fi, which has adapter Wi-Fi, the Internet will work. The scheme of such a compound is shown in Figure 1.3.

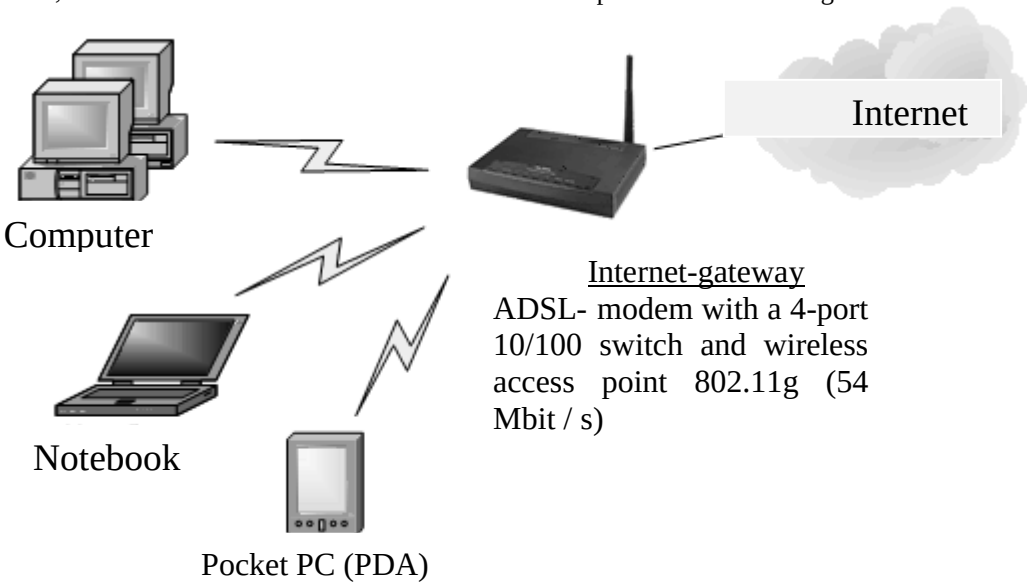

Fig. 1.3 - Connection via an access point built-in modem

At the moment there are four main standard Wi-Fi - is IEEE 802.11a, IEEE 802.11b, IEEE 802.11g and IEEE 802.11n. Table 1.1 shows a comparison of the standards.

Table 1.1. Compare Wi-Fi standards

Standard	**Throughput**	**Radius of action**	**frequencies**
802.11a	up to 54 Mbit / s	Up to 100 meters	5.0 GHz
802.11b	up to 11 Mbit / s	Up to 100 meters	2,4 GHz
802.11g	Up to 54 Mbit / s	Up to 100 meters	2,4 GHz
802.11n	Up to 300 Mbit / s (in the future to 450 and then 600 Mbit / s)	Up to 100 meters	2,4-2,5 or 5,0 GHz

Providing reliable protection of information includes:

1. Ensuring the security of information on the LAN it is a continuous process, is the systematic control of security, identifying bottlenecks and weaknesses in the system of protection, justification and implementation of the most efficient ways to improve and develop the system of protection.

2. Information security in computer networks can be achieved only by using a complex system of information protection.

3. Proper training of users and their compliance with the rules of protection.

4. No security system is not considered completely reliable. We must proceed from the fact that you can find a skilled attacker, who will find a loophole for access to information. [4]

References

1. *Alferov A. P., Zubov A. Y.* Basics of cryptography. M .: Helios, 2005, p.53.
2. *Baimakova I. A.* Ensuring the protection of personal data. M .: in 1C Publishing, 2010. p.216.
3. *Baldin V. K., Utkin V. B.* Information: Proc. for high schools. M.: Project, 2003. – p.304.
4. *Belov E. B., Moose V. P.* Fundamentals of Information Security: A Training Manual. M .: Hotline - Telecom, 2006. p. 544.
5. *Biyachuev T. A.* Secure corporate networks. SPB .: ITMO, 2004, p. 64.
6. *Moldovyan N. A., Moldovyan A. A.* Introduction to public-key cryptosystems: Textbook. SPb.: 2005. 288 p.