1 answer		2 answer		3 answer	
D2	V3	M1	A4	D1	V2
1	0	1	0	0	1

Table 2: Answer options and their meanings

We got a contradiction, since Denis and Viktor took 2st place. Hence, D2 is true, V3 is falsely impossible.

Let us again make a truth table, but now suppose that D2 is false, then according to the condition of the problem V3 it is true. Reasoning, we get the following table 3:

1 answer		2 answer		3 answer	
D2	V3	M1	A4	D1	V2
0	1	0	1	1	0

Table 3: Answer options and their meanings

In this table, the conditions of the problem are met, the solution has been obtained. From Table 3 we get that Denis took 1st place, Mikle – 2nd place, Viktor – 3rd place, Aleks – 4th place. This will be the answer to this non-standard task.

As you can see, non-standard tasks in mathematics:

- develop logical and combinatorial thinking of students,
- support the perception of spatial relationships of students and indicate the connection between mathematics and everyday life,
- arouse interest in mathematics,
- the solution of these problems does not always depend on the knowledge and skills of school mathematics,
- these tasks are aimed at activating students in mathematics.

The systematic use of non-standard tasks contributes to the development of students' ingenuity, the development of logical thinking. Students' reasoning becomes consistent and logical. Students become more interested in mathematics, they begin to think out of the ordinary, analyze and apply knowledge in non-standard situations in real life.

References

[1] Дрозина В.В., Дильман В.Л. Механизм творчества решения нестандартных задач. М.: БИНОМ. Лаборатория знаний, 2012, 255с.

SECURITY ISSUES AND MAIN IMPLEMENTATION OF CORPORATE INFORMATION SYSTEMS

Yeleussiz M.Y.[1], **Khasanova A.B.**[2], **Dakarim G.K.**[3], **Datkabaeva M.A.**[4]

[1,2,3,4]Ye.A. Buketov Karaganda University, Karaganda, Kazakhstan
[1]E-mail: erzhanovna18@bk.ru

[2]E-mail: ainara28@mail.ru
[3]E-mail: gulderai0905@mail.ru
[4]E-mail: datkabaeva.moldir@bk.ru

New information technologies are actively introduced in all sectors of the economy. The emergence of local and global information networks has offered computer users the possibility of rapid exchange of information. If until now such networks are used only for special and narrow purposes (academic lines, networks of local military departments, etc.).b.) in the case of a network, the development of the Internet and similar systems has led to the use of each person global data networks (WAN) in everyday life.

With the development and complexity of tools, methods and forms of automation of information processing, society's dependence on the degree of security of information technologies used by them increases. The relevance and importance of information security depends on the following factors:

- high growth rates of personal computers used in various fields of activity;
- instant expansion of the range of users available directly to computing resources and data sets;
- increasing the amount of information collected, stored and processed by computers and other automation tools;
- concentration of information relating to different and heterogeneous substances in a single database;
- hot development of software that does not meet even the minimum security requirements;
- ubiquitous distribution of network technologies and integration of local networks into the global network;
- the development of the global Internet Network, which does not prevent the violation of the security of information processing systems around the world.

Modern methods of collection, processing and transmission of information contribute to the emergence of threats associated with the possibility of loss, distortion and disclosure of data directed to end users or related. Therefore, information security of computer systems and networks is one of the leading areas of information technology development. Consider the basic concepts of information security of computer systems and networks [1].

Information security means the state of security of processed, stored and transmitted data from unauthorized submission, transformation and destruction, as well as the state of protection of information resources from the impact aimed at violation of their performance.

The nature of these effects can be varied. There are both attempts to infiltrate intruders and errors of employees, as the failure of hardware and software, natural disasters (earthquakes, hurricanes, fires, etc.).b.) the dictionary has two-way translation. The security of computer networks and systems can be achieved by ensuring the confidentiality, integrity, reliability, legal significance of information, efficiency of access to it, as well as the adoption of a set of measures to ensure the integrity and availability of information resources and components of the system or network. The basic properties of the above information need to be discussed more fully.

The nature of these effects can be varied. There are both attempts to infiltrate intruders and errors of employees, as the failure of hardware and software, natural disasters (earthquakes, hurricanes, fires, etc.).b.) the dictionary has two-way translation. The security of computer

networks and systems can be achieved by ensuring the confidentiality, integrity, reliability, legal significance of information, efficiency of access to it, as well as the adoption of a set of measures to ensure the integrity and availability of information resources and components of the system or network. The basic properties of the above information need to be discussed more fully.

The integrity of information is understood as its ability to maintain its structure and / or content in the process of transmission and storage. The integrity of the information is ensured if the data in the system does not differ from the current data semantically, that is, if they were not accidentally or intentionally distorted or violated.

Reliability of information-quality of information imposed on the source or the subject, he was released.

TCP/IP is a set of computers that is compatible between different types, providing communication it is used for linear inhomogeneous media. Compatibility is one of the main advantages of TCP/IP, so most local computer networks support these protocols. In addition, TCP/IP protocols are available to the resources of the global Internet Network. In this case, it is typically used as an internetwork Protocol that supports TCP/IP packet routing, typically as an internetwork Protocol. Due to its fame, TCP/IP has become the de facto standard for interworking.

However, the ubiquity of the TCP/IP Protocol stack has shown its weaknesses. Tomasin your planning TCP/IP networks, the defense had not seen the disturbing stegani architecturely created on the basis of reasons. They did not even expect that they will be the main factor terminating the effective means of protection, TCP/IP protocols.

Protocols TCP / IP, IP-networks and information security services relevant to heart failure of the Internet will consider in more detail. These drawbacks occur when all TCP/IP stack protocols and Internet services are opened. Most of these problems are due to historical dependency on the UNIX Internet operating system. ARPAnet (Foreword to the Internet) was created as a connecting network of research centers, scientific, military and government institutions, large universities in the United States. These structures used the UNIX operating system as the platform needed to communicate and solve their own problems. Therefore, the features of the programming methodology and its architecture in the UNIX environment have left their traces of the implementation of TCP/IP exchange protocols and security policies in the network. Due to the openness and wide distribution of UNIX system has become a favorite cereal hackers.

Application layer (SMTP, Telnet, FTP...)				Data
Transport layer (SMTP, Telnet, FTP...)			TCP topic	Data
Internet layer (IP)		IP topic	TCP topic	Data
The level of network access (Ethernet, FDDI, ATM, ...)	Ethernet-topic	IP topic	TCP topic	Data

Table 1: TCP/IP Protocol data encapsulation diagram

Therefore, the presence of flaws in the protection from the moment of occurrence in the aggregate TCP/IP Protocol is not surprising.

In practice, IP networks are vulnerable to a number of methods of unauthorized access to the data exchange process. With the development of computer and network technologies (for example, with the advent of mobile Java-applications and ActiveX controls, the list of possible types of network attacks on the IP network is constantly increasing [2]. Network attacks are as diverse as their contrast-oriented systems. Some attacks are very difficult. Others are able to implement a normal operator, not even knowing what consequences can lead to its activities. The most common today are the following attack options [3].

Listen. Many data is transmitted over computer networks in an unprotected (plaintext) format, allowing an attacker who gains access to the data network to listen to or read the traffic. It is said that listening in computer networks (sniffing or snooping). If services provide regular encryption, data transmitted over the network will be available for reading. To listen in computer networks, you can use packaging sniffers, called as follows. Packages of packages of hunting grounds transferred through the sniffer network domain of all known applications. Currently sniffers are used in networks on full legitimate grounds. They are used for validation and error analysis of the traffic. However, some network applications use text-based data (Telnet, FTP, SMTP, POP3, and so on).b.) in connection with the sending, you can use the sniffer to find useful and sometimes confidential information (such as usernames and passwords).

Attacks on the password. Hackers can make attacks on passwords using a number of methods such as IP-spoofing and sniffing packages, full exceeding (brute force attack), “Trojan name”. Due to the fact that due to the fact that due to the fact that due to the fact that due to the fact that due to the fact that due to the fact that due to the fact that due to the fact that due to the fact that due to the fact that due to the fact that since There is only one password, so many users had access to all the resources and applications. If the application is running in client-server mode and the credentials are sent in a text format that can be read over the network, this information can be used to make other corporate or external resources available. Although the Login and password are often obtained through IP spoofing and sniffing packages, hackers try to record and identify the login and password, creating many commonly used features for it. For often a full attack on the invasion, a special program is used that allows the use of public resources(for example, a server). As a result, a hacker can provide a password and use resources under the name of a simple user. If the user has significant advantages in use, the hacker can make it possible for him to open it in the future, even if the user has changed his password and login.

Viruses and applications such as "Trojan name". Recent users ’workstations become weak for viruses and”Trojan names". Viruses are injected into other programs to perform certain unwanted functions on the end user’s workstation. As an example command.com (the main interpretation of Windows systems), which are written to a file and delete other files, including all earned command.com it can be said that the virus that infects the options. An example of a typical "Trojan name"is a program that looks like a simple game for the user’s workstation. However, until the user has played the game, the malware sends its copy by e-mail to each subscriber listed in the user’s address book. All subscribers will receive the game by mail and contribute to its further distribution. The fight against viruses and” Trojan names "is carried out with the help of effective anti-virus software running at the user or network level. Anti-virus tools are able to detect most viruses and “Trojan names” and prevent their spread. Daily receipt and use of the latest information about viruses can help you to effectively deal with them. As more viruses and “Trojan names” appear, new versions of antivirus tools and applications must be installed.

Linear intelligence. Network intelligence is the collection of information about the network

through public data and applications. When preparing attacks against a network, a hacker usually tries to get more information about it. Network intelligence is created in the form of DNS queries, ping sweep and port scanning. DNS queries help you understand who owns a domain and what addresses have been transferred to that domain. Echo testing of addresses opened with DNS allows you to see which hosts are running in this environment. After receiving the list of hosts, the hacker uses port scanning tools to create a complete list of services supported by these hosts. And thus, "scout"analyzes the characteristics of applications running on hosts. As a result, you can get information that can make an attack. Currently, there are other types of attacks.

It's not hard to see that the above attacks can be possible for a number of reasons:

- first, identify the sender only by its IP address;
- secondly, the identification procedure is carried out only at the stage of establishing the connection-after which the authenticity of the accepted packages is not checked;
- third, important data related to the system is transmitted unencrypted over the network.

References

[1] Березин А.С., Перчиков В.И. Защита информации в открытых сетях // Корпоративные системы. – 2001. - № 1. – С. 65 – 69.

[2] Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452с.

[3] Иванов П. IPSec: защита сетевого уровня // Сети. – 2000. – 320с.

BRAINSTORMING AS AN INTERACTIVE TECHNOLOGY IN THE FORMATION OF COGNITIVE-COMMUNICATIVE COMPETENCIES IN TEACHING DISCIPLINES IN ENGLISH

Yesbayeva D.N.[1], **Yessenbayeva G.A.**[2]

[1]School of Robotics "Byte Karaganda, Kazakhstan
[1]E-mail: assyl.di@gmail.com
[2]Karaganda Buketov University, Karaganda, Kazakhstan
[2]E-mail: esenbaevagulsima@mail.ru

Due to the growing professional significance of English in the labour market, the socio-cultural context of its study in non-linguistic faculties of universities has changed significantly. Today, the most productive and promising are modern pedagogical interactive technologies that allow the most complete formation of foreign language communicative competence of students both in the personal-professional aspect and in the cognitive-operational aspect simultaneously [1].

Teaching subjects in English at the faculties of exact sciences (mathematics, physics, chemistry, economics, etc.) is often accompanied by forced memorization by students of a large number of new words related to the new topic, but not related to each other in meaning, as well as lexical and grammatical rules and features of a foreign language. This usually causes rejection, unacceptance and a painful experience of learning English. With this type of study of a professional foreign language, cognitive and communicative competencies are poorly developed in students.