Ministry of Education of the Republic of Belarus
Educational institution
Belarusian State University of
Informatics and Radioelectronics

UDC 004.42:629.33

Al–Rubaye Issa Mohammed Mishaal

Abstract

THESIS
For master's degree in technical sciences

Specialty 1–45 80 02 «Telecommunication systems and computer networks»

<div style="text-align:right">

Supervisor
Astrovsky I.I
PhD, associated professor

</div>

Minsk 2019

Normative control

_____
_____

INTRODUCTION

Information networks are very important in the lives of individuals and organizations alike, where they play an effective role in accomplishing the tasks and objectives desired. Due to the proliferation of computer networks and the dependence of public and private institutions on their efficiency and quality of work, any disruption or destruction there of may result in great losses and disruption to the services of citizens. The spread of pirates, dangers and misuse was the idea of study to reduce damage in advance by taking precautionary measures from a comprehensive security perspective. The study concluded that the problems of protecting and securing the resources of computer networks are not only in the supply and installation of hardware and software, but in the provision and preparation of the person capable of managing and operating these devices and software within the framework of policies and procedures within an environment where team spirit prevails. In the absence of a congruence between the organizational structures and the human resources protection working procedures and functions in the sample studied, access to better protection of computer networks requires the redesign of organizational structures. In order to overcome the difficulties of protection, it is necessary to provide information security specialists. Providing a sufficient number of information security personnel, possessing scientific qualifications commensurate with the requirements of the work of protection and providing functional names with a statement of tasks and duties, especially for jobs related to protection and safety. The decision makers must provide the necessary budgets for the development of the staff and increase their numbers according to the required specialties, and the work necessary to match the procedures with the international standards related to information security, and documented the procedures of protection work and network plans and update periodically.

SUMMARY

Because of the spared of computer networks in all life fields, quality of business services for public and private organizations might be affected by any downtime or sabotage of computer networks, which may lead to great losses and disruption to citizen's services, the spread of the pirates and the dangers and misuse of the idea of the study to limit the damage already taking precautionary measures from the perspective of comprehensive security, and through the analysis of survey results.

The study found that the problems of protecting and securing resources for computer networks, does not only lie in the supply and installation of hardware and software, but also lies in the provision and preparation of human resources, they are capable of managing and operating hardware and software in the framework of the policies and procedures in an environment dominated by cooperation stuff. And the lack of compatibility between the organizational structures,procedures and functions of human resources working in the field of protection of the studied sample networks, access to better protect computer networks require the redesign of organizational structures.

Computer users should have attend required to enable them to consider protection parameters while they perform their work properly. And People who perform protection tasks should be appreciated by providing bonuses, and/or certificates of appreciation. Also the incomes of protection staff especially the experts should be increased to let them stay and not leave their jobs.

We must take care of the ethics of the staff, giving qualities of integrity, honesty and devotion to high priority and be included in employment policies. It should be ensured yearly that the ethical levels of staff is available, also it's better to increase the moral sense of responsibility whenever possible.

In order to reduce the risk from penetration and infection of computers, sufficient efforts should be made to aware and train users, to be able to install updates, to know right ways to open their e–mail, and avoid visiting unsafe Web sites.

The purpose of my thesis is to develop a Handbook for training students and staff on the protection of information in corporate networks.

For this it is necessary to solve the following tasks:
– Review of historical and theoretical information on corporate networks.
– Show security.
– Choice of software.
– Development of training and testing program for trainees.
–Description of the developed program product and ways of its modernization.

CORPORATE NETWORK

A corporate network is a structure whose main purpose is to make the work and internal processes of a particular enterprise or organization as efficient, ergonomic and safe as possible

The customer of the corporate network services is exclusively the personnel of this enterprise. The complexity, structure, hierarchical division within the organization is determined by the scale of the enterprise itself and the complexity of its tasks.

The question of introducing a corporate network at a particular enterprise should be raised on the basis of serious research and
 analysis of all work processes and internal technical and human communications. There are often situations when the funds and efforts spent on the organization of the internal network do not pay off due to a non–professional, superficial approach to understanding the mechanisms and goals of the enterprise. Reasonable use of the potential of the corporate network in the enterprise provides the following benefits:

The obvious increase in labor productivity due to the competent organization of parallel computing processes, which is impossible to achieve in the presence of powerful but autonomous computing devices. Resilience to failures and failures of individual elements of the system is transferred much less painful in the case of combining these elements into a single network. duplication of data on various types of network media, the ability to switch requests and processes to healthy internal network segments, dynamic and static reconfiguration capabilities – this is what the use of the corporate network gives in case of failures.

GENERAL DESCRIPTION OF WORK

Technological progress one of the means of communication is important and growing, as it provides an opportunity to enter the world to each other, and rely on sending all kinds of data through the network, all of this led to the risk of a leak of such data and access to competitors so was the need to maintain information security is important, the internet is considered a double–edged sword, as it is considered an important entrance for many useful things, but it nevertheless opens the field in front of a lot of hurtful things to penetrate the devices, There are a number of security issues that must have attention in order to stay on the safe operation of network and computers, by us today, I will talk in my thesis about some security information.

Network security specialists monitor computer networks for security threats or unauthorized users. They may identify compromised machines and report on security measures taken to address threats. Network security specialists also analyze security risks and develop response procedures. Additional duties may include developing and testing software deployment tools, firewalls and intrusion detection systems.

Some network security workers research, evaluate, recommend and implement other security devices as well. This may include installing computer security software, conducting regular security audits, preparing security status reports, educating users on computer security, creating security documentation for users, assisting in disaster recovery and gathering evidence regarding cybercrimes.

Network security specialists strive to stop cybercrimes, and to do so they run risk assessment checks on systems, maintain firewalls, update security procedures and monitor all systems. The rate of job growth for this industry was expected to be much faster than average during the 2014-2024 decade. Successful job candidates have training in computer networks and computer security systems, which is generally available through undergraduate degree programs; network security specialists also typically earn certifications through vendors or computer security training organizations.