Research on Computer Security Guarantee Measures in Network Environment

SHI Zi-xin
Wuwei Occupational College, Wuwei, Gansu, 733000

Abstract: In recent years, computer network technology has been rapidly developed and popularized, and it also plays an important role in people's life and work. However, because the computer network itself has the characteristics of openness, it is easy to cause some security problems in the process of use. Computer networks not only affect people's experience of using computer networks, but also cause certain economic losses in severe cases. Therefore, how to do a good job of computer security protection in the network environment has become an important issue that relevant technical personnel need to pay attention to.

1. Introduction
Computer systems have the characteristics of complexity and openness in the process of operation. During the computer application process, they will encounter a variety of factors, which will cause a series of problems such as hardware damage. It will also cause bad effect to users' application experience. Therefore, in the network environment, we also need to do a good job in computer security, and in time to curb some computer security risks caused by external factors, so as to ensure the normal operation of the entire computer system.

2. Application of Computer Network Technology
With the rapid development of network technology, the proportion of people's lives and work has become more and more, and the links with various industries have become closer. However, in the process of computer application, various security problems emerge endlessly. Only by comprehensively considering and analyzing the various influencing factors of computer network information security, and finding a relative solution, can we ensure the security of users in the use of computer technology. This also is the prerequisite important for the further development of the computer industry in China[1].

Because of the extensive and open nature of computer network technology, computer security issues cannot be completely avoided. Users need to adopt effective protective measures in time to use computer technology in order to maintain information security. Computer network technology involves a number of comprehensive disciplines. Therefore, in computer network protection technology, relevant knowledge of many different disciplines must be integrated in order to avoid the occurrence of various application security risks.

3. Computer Network Security Technology Overview

3.1 Network Technology Protection
In view of various security problems in the application process of computer network technology, users must also actively adopt network technology to protect their work, and to ensure that users' network
information systems do not have malicious changes or information leakage during normal access security issues, and can promote the security of computer network applications. When the network system is in operation, it will record and store the flowing data at any time, and also provide the necessary network management services for the operation of the network system. In the application of various dynamic data, system hardware, and system software in network systems, it is necessary to give necessary technical protection measures to ensure the computer's operating effect [2].

3.2 Network Security Management
Computer network technology needs to involve multiple disciplines and multiple contents in the application process. Therefore, it is necessary to adopt a comprehensive management model to achieve network security management, and it also involves a variety of information security technologies such as communication technology, cryptography technology. In the computer network security protection work, it is necessary to implement comprehensive management of multiple levels of hardware, software, and computer data to avoid problems such as file content changes or information leakage during data transmission. Only in this way can problems such as hacking be avoided and the overall operating effect of the computer system be guaranteed.

4. Principles of Computer Security Management in Network Environment

4.1 From Outside to Inside
The open nature of the computer network itself, if the computing security protection measures are not done well, will also lead to the long-term exposure of the entire system in an environment full of computer viruses, which will cause greater difficulties in the use of hardware security. Therefore, in the use of computer systems, users must carefully maintain various computer hardware without the problem of random disassembly. Once the computer system fails, it needs to be handled in a specific repair shop. In the process of safety management, we must first determine whether the fault is an internal fault or an external fault. The external fault is generally obvious, and it is specifically manifested in line problems, etc. [3]. If there is no problem with the computer hardware circuit, it can basically be determined to be an internal fault. At this time, computer maintenance personnel need to perform more detailed and in-depth inspections to ensure the inspection results and lay a good foundation for subsequent computer maintenance work.

4.2 From Static to Dynamic
Static maintenance refers to the computer maintenance work when the power is not connected. Generally, the process of static maintenance is relatively simple, and it can effectively deal with some external computer faults [4]. Dynamic maintenance can perform more in-depth inspection and maintenance of the computer, but it takes a long time and the process is more complicated. In the dynamic maintenance process, the fault location needs to be determined after the power is connected, which also causes a relatively large obstacle to the later maintenance work. Through the maintenance mode from static to dynamic, the maintenance efficiency can be greatly improved.

4.3 From Shallow to Deep
The normal operation of the computer system can be guaranteed only if there is no problem with the basic equipment and the main equipment. Because of the complexity of computer systems, if any hardware problem occurs, it is easy to cause security risks. Therefore, during the operation and maintenance of the computer, it is necessary to follow the principle of shallow to deep maintenance. The first step is to start with simple computer hardware testing, to test the basic equipment, to ensure that there are no problems with the basic equipment, and then to perform some complex equipment testing to ensure the overall operation and maintenance effect.
5. Problems in the Operation of Computer Network Technology

5.1 Virus Trojan Software
Viruses and Trojans are the most common types of computer security failures. Most of these viruses are artificially set malicious software. Once a computer is invaded by a virus, it will cause very large economic losses to users and cause problems such as information disclosure. The Trojan software will directly bypass the computer's own protective equipment. In severe cases, it will directly control the main computer. It also has the characteristics of concealment and unauthorizedness. Therefore, in the computer security maintenance work, measures must be taken to avoid the invasion of the computer caused by viruses and Trojan horse software.

5.2 System Vulnerability
The characteristics of the computer's own openness, there will also be a lot of system vulnerabilities in the operation process, these vulnerabilities can not be completely avoided, at this time users need to resort to some security protection software and protective measures to avoid system vulnerabilities for computer software Impact. The causes of computer software system vulnerabilities mainly include the inherent problems of computers, the use of illegal software by network users, the users' free download of software, and the lack of regular maintenance of their computer systems [6].

5.3 Lack of Security Configuration
Improper security configuration is also an important factor leading to computer security problems, but many computer users do not pay enough attention to this problem, and do not install security protection software during the use of the computer. In addition, some users have problems with inadequate operations during the use of network software. In the process of computer system application, some bad software is also bound. These softwares will cause some security risks after they are opened. Only after regular maintenance of the computer system can its application security be improved, which is of great significance to the improvement of computer operation security.

6. Computer Network Security Protection Strategy

6.1 Physical Protection Measures
Physical protection measures are important measures for computer network security protection. In physical protection measures, users need to create a good physical operating environment for the computer, have the security of the computer room containing the computer, and the security of the hardware equipment, and ensure that Will be harmed by electromagnetic interference and some natural disasters. In addition, during the operation and management of the computer room, fire prevention, waterproofing, and moisture-proof work should be done well. In addition, physical measures for computer network security protection are of great significance to the improvement of computer operating performance. In the computer network security protection system, it is necessary to regularly do a good job of inspecting the surrounding environment of computer equipment, and to deal with problems that affect the quality and security of computer operation in a timely manner. Clarify the operation safety of the power supply system of the computer equipment room and observe whether there are abnormal conditions or noise during the operation of the equipment. It is necessary to strictly control the people entering and leaving the computer room, so as to avoid the influence and harm caused by human factors to the computer software system. The physical system is an important prerequisite to ensure the normal operation of computer software. In the process of computer hardware protection, targeted physical protection measures must be adopted to avoid the impact of external physical factors on the computer operation.

6.2 Building A Sound Government Management System
Computer network security is of great significance to enterprises and even national security, and it is
also an important part of China's national security system. In recent years, although China has issued a series of network security management policies, there are still many problems in concrete implementation. However, maintaining computer network security requires relevant legal means to restrict and sanction cyber illegal intrusions and cyber crimes. This can regulate the operation of computer networks and deal with some illegal acts in a timely manner. In addition, we must pay attention to improving the management skills and legal thinking of computer managers, and require all managers to have a noble character and a good idea of the rule of law. In order to give full play to the political management system, first of all, government departments need to be able to formulate security management specifications for computer network security. For example, the implementation of computer network security information management mechanism and computer network management system can standardize and improve the use of computers, and ensure that all computer network operations can be implemented in accordance with the law [7]. The legal basis is also an important measure to deepen the security management of computer networks. Chinese government units need to pay more attention to this aspect.

6.3 Improve the Technical Level of Computer Network Security Management

Prevent computer viruses. In recent years, with the continuous development of computer network technology in China, there are more and more types of computer viruses, which have also caused serious threats to the safe use of computers. At present, they are also developing towards the trend of intelligent viruses. Therefore, in the process of computer network security maintenance, computer virus prevention technology must be continuously improved. With the help of anti-virus software and security protection software, users can effectively avoid the impact of viruses on the normal operation of computer systems and ensure the security of computer network operations promotion. Through the application of computer anti-virus measures, it is possible to detect and deal with the virus in the first time in time to avoid a series of computer network security problems caused by viruses.

Using firewall technology. Firewall technology, as the first barrier for computer security protection, mainly controls the access mode to prevent vicious attacks, and avoids the impact of viruses and hackers on computer systems. It can be said that firewall technology is a security tool that is independent of other computer systems. Only by fully understanding the importance of firewall technology for network security can the computer server operation security be further improved. As the most common computer security protection system, firewall technology has been widely used in various computer systems. Only with the help of the firewall technology, a security isolation technology, can the overall operation effect of the computer be guaranteed through the way of setting permissions.

At present, many users have adopted encryption technology to protect the operating security of computer systems in the computer network security protection work. At present, there are many computer data encryption technologies, but commonly used are key management technology. In this security management technology, users' computer storage information and network transmission technology need to be re-encoded to prevent unauthorized customers from occupying the computer. Network resources, and the difficulty of cracking information resources has been further improved. Computer network encryption technology includes multiple modes such as connection port network nodes and network connection encryption, among which different encryption methods have different functions.

7. Conclusion

In summary, in recent years, China's Internet technology has developed very rapidly and has also been well applied in many fields. However, the structure of the computer system is relatively complicated, and it also has the characteristics of openness. In the process of using it, it will be affected by various factors such as external factors and malicious attacks. Under the existing network environment, people are required to be able to pay more attention to computer network security technology. On the basis of clarifying the factors that affect the security of computer network use, take targeted measures to avoid
problems such as illegal intrusion and ensure the security of the computer network environment. It is 
also important to improve the user experience significance.

Acknowledgement
Foundation item: the stage research results of the 2019 Gansu vocational education teaching reform 
research project based on"the construction and Practice Research of one platform, two main lines and 
six linkage practical teaching system of electronic information specialty in Higher Vocational 
Education" (subject No.: 2019gszyjjy-53)

References
[1] Luan Lijuan. Application Analysis of Cloud Computing Technology in Computer Security Storage 
[J]. Computer Programming Skills and Maintenance, 2019, (12): 166-168.
[2] Su Peng. Analysis and countermeasures of computer security under network environment [J]. 
Digital World, 2019, (9): 258.
[3] Shi Jinguo. Exploration of Computer Security Protection Path in Network Environment [J]. Digital 
Design (Part Two), 2019, (5): 22-23.
[4] Liu Fang. Analysis and countermeasures of computer security problems in network environment 
[J]. Architectural Engineering Technology and Design, 2019, (13): 4547.
[5] Zhou Mo. Analysis of Computer Security Problems and Solutions in Network Environment [J]. 
Knowledge Guidance, 2018, (29): 17-17.
[6] Yang Shengbiao. Analysis and countermeasures of computer security under network environment 
[J]. Technology and Market, 2019, 26 (7): 82-83, 85.
[7] Lu Fei. Computer Security Problem Analysis and Strategy Research in Network Environment [J]. 
Modern Information Technology, 2018, 002 (006): 165-166.