Advances in Computer, Signals and Systems (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2024.080306
ISSN 2371-8838 Vol. 8 Num. 3

Analysis of computer network information security and protection strategy

Xuwei Zhang[1,a,*], Yanfang Wang[2]

[1]*Philippine Christian University Center for International Education, Manila, 1004, Philippines*
[2]*Jinhua Guangxin Network Engineering Co., Ltd, Jinhua, 321000, China*
[a]*32271853@qq.com*
[*]*Corresponding author*

Keywords: Computer; network; information security; protection

Abstract: In the contemporary development of computer network, the attention of computer network information security and the analysis of protection strategies can protect personal privacy, prevent data leakage and guarantee the reliability of network services. Computer network information security is not only related to the protection of personal privacy and corporate secrets, but also has an important impact on social stability. Therefore, it is of great practical significance to study the computer network information security and the corresponding protection strategies. Based on the reality, this paper makes a comprehensive and in-depth analysis of the main problems of computer network information security, including phishing, computer virus, DDoS attack and network security vulnerabilities. On the basis of in-depth analysis of these problems and their causes, this paper further discusses the scientific and effective protection strategies, such as firewall technology, anti-virus software and intrusion detection system. These strategies aim to meet the increasingly complex network security challenges, prevent network information security problems, and provide useful reference for relevant personnel in the field of network information security. By implementing these strategies, we are expected to improve the overall level of computer network information security, and build a more secure and reliable network environment.

1. Introduction

With the rapid development of computer network, while bringing convenience to people, the problem of network security has become increasingly prominent. Computer network security has become a topic of much attention, especially in the background of the information age, network security has become an important basis for social stability and development. Therefore, it is necessary to strengthen the research of computer network information security, analyze the security protection strategy, avoid criminals using the network to violate the privacy and interests of others, so that the network can play an ideal role in modern society and improve the security of network information.

2. The importance of strengthening the computer network security protection

2.1 Protect personal privacy and security

Personal privacy security is becoming more and more important in today's digital society, and people increasingly rely on the Internet in their daily life and work. Personal privacy information includes personal identity information, financial information, communication content, etc. Once leaked or stolen, it may lead to serious property loss, credit crisis, and even threaten personal security. With the popularity of services such as electronic payments and online banking, personal financial information is often stored on Internet platforms. If relevant information is stolen by hackers, personal accounts may be stolen and funds transferred, causing serious economic losses[1]. In addition, once personal credit card information, credit card information, ID number and other sensitive information are stolen, hackers can use relevant information to carry out fraudulent activities, resulting in personal credit damage, and even unable to carry out normal financial transactions. Strengthening computer network security protection can effectively prevent hacker attacks through encryption technology, firewall and other means, and protect personal privacy from infringement. At the same time, strengthening the computer network security protection can avoid the malicious use of personal information. In the network environment, people's personal information and privacy data may be stolen by criminals, and then used for a variety of illegal activities, such as stealing personal property, fraud, etc. If personal information is not protected, it is easy to become a victim of criminals. Strengthening computer network security protection can effectively prevent personal information from being maliciously used and protect personal privacy and security. And through encrypted transmission, secure connection and other technical means to protect the transmission of personal privacy on the Internet security, to ensure that personal information is not leaked.

2.2 Prevent data leakage

Data leakage refers to the process in which unauthorized individuals or organizations obtain sensitive information. Relevant information may include personal identity information, financial data, trade secrets, etc., which will cause serious losses to individuals and organizations. Therefore, strengthening the computer network security protection is the key to prevent data leakage. By strengthening the network security technology, the network vulnerabilities can be blocked as much as possible to improve the security of the system. Such as the installation of firewall, intrusion detection system, data encryption and other technologies, can effectively prevent hackers, to avoid data leakage. To ensure the integrity and security of company data, it is imperative to reinforce access control, audit functions, and other technical measures. This will allow for the effective monitoring of enterprise employees' operations, thereby preventing any unauthorized acquisition or dissemination of sensitive information. Many enterprises need to share data with third-party partners, such as suppliers and customers, in their business[2]. However, data contribution increases the risk of data leakage. The risk of data leakage can be effectively reduced by establishing a secure data sharing mechanism, signing confidentiality agreements, and strengthening the security review of third-party partners through the process of data sharing. In addition, strengthening computer network security can prevent malware attacks. By strengthening network security technology, timely update system patches, install anti-virus software, regular security detection and other measures, can effectively prevent malicious software attacks, protect data security.

2.3 Ensure the reliability of network services

In today's society, the network has become an important carrier of people's work, study and life. The reliability of network service is directly related to information security and smooth communication. Strengthening the computer network security protection can effectively improve the reliability of network services, prevent the network from malicious attacks, and ensure the normal operation of the network system. In order to ensure the stability and reliability of the network system operation, we are committed to optimize the network architecture, improve the system stability, and effectively reduce the probability of network failure. During the operation of the network system, it often causes the system crash or service interruption due to hardware failures, software problems or human operation errors, causing inconvenience to the network users[3]. By strengthening network security protection, doing a good job of system backup, timely fault recovery work, finding and dealing with system problems, we can improve the stability of the network system, reduce the occurrence of service interruption, and ensure the reliability of network service. By improving the quality and reputation of network services, we will further enhance user satisfaction and inject strong impetus into the steady development of the network. The reliability of the network service is an important standard to measure the network service providers, and the users are more inclined to choose the network platform that can provide the stable service. By strengthening the network security protection and improving the reliability of network services, users can make the use of network services smoothly, so as to build a safe, stable and reliable network environment.

3. Common computer network security problems

3.1 Phishing

Table 1: Phishing data sheet

Phishing means	description	risk grade
Email fishing	Send emails disguised as legitimate institutions or individuals to induce victims to click on malicious links or download malicious attachments	tall
Website fishing	Make fake websites with similar appearance to legal websites, and cheat users to enter their personal information, account number and password, etc	centre
Social phishing	Fake them as other users or organizations on social networking platforms to induce users to click on malicious links or share personal information	centre
Software fishing	Disqueraged as normal software or game, induce users to download or install	tall

Phishing (Phishing) is a form of online fraud that steals user information disguised as a legitimate institution. Phishing attacks usually send users information disguised as legitimate institutions, such as banks and e-commerce platforms, through email, text messages, social media and other channels, etc., to induce users to click on links or provide personal information, so as to obtain sensitive data such as user account number, password and credit card information. Phishing attacks are a common cyber security threat that poses a serious threat to the information security of individuals and organizations. Phishing attacks are a form of "social engineering attacks" that allow users to mistakenly assume that information is from trusted sources, thus reducing user vigilance. Attackers often fake legitimate websites, email templates or text messages, making it difficult for users to tell the truth[4]. In addition, phishing attacks often use a user's curiosity, fear, or urgency to

induce users to take immediate action to obtain their personal information. In the face of phishing, individuals may suffer property losses because of personal information leakage, and even face the risk of personal privacy leakage. For enterprises, phishing attacks may lead to serious consequences such as confidential information leakage, financial loss, reputation damage and so on. In addition, phishing attacks may lead to the interruption of network services, affecting the normal operation of the business. Phishing attacks originated earlier, not a new intrusion method, but the harm caused by it is gradually expanding. As early as 2009, more than 90% of the Internet users in China have encountered phishing, about 45 million Internet users suffered economic losses, the total amount of fraud as high as 7.6 billion yuan[5]. In today's era, phishing is still popular, which is the main problem facing the computer network information security. As shown in Table 1.

3.2 Computer viruses

Table 2: Computer virus data sheet

Virus type	description	extent of injury
Worm virus	Can self-replicate and spread to other systems, endangering network security	tall
cockhorse	Masaged as useful software, actually implanted malicious code, can steal user information or control systems	tall
script	Malicious code written in the scripting language can be executed by malicious scripts	centre
Macro virus	Implant document, perform malicious behavior through macro commands	low

Computer virus is a kind of malware that self-copies and spreads, which can damage the computer systems or steal user information. Computer viruses can exist in the form of files, programs, scripts, etc., and spread through the Internet, mobile storage media, mail, and other channels. Computer viruses can spread in a variety of ways, including infected files, online downloads, malicious links and so on. A computer virus can cause a computer system to crash, causing data loss[6]. Secondly, computer viruses may steal users' personal information, account passwords and other sensitive data, leading to the disclosure of personal privacy. There are many kinds of computer viruses, including worm viruses, Trojan horses, scripts, macro viruses and so on. Viruses can be transmitted through infection files, system guidance area, network transmission, and other on, causing damage to system files and data. Worm (Worm) is a self-replicated malicious software that can spread remotely through the network and infect other hosts; Trojan horse (Trojan) is hidden behind normal programs, such as stealing information and control system; script (Script) is written by script language and uses the network for virus transmission; macro viruses (Macro) mainly infects Office documents and uses Office templates. As shown in Table 2.

3.3 DDoS attack

Distributed denial of Denial-of-Service (DDoS) attack is a network attack using a large number of legitimate or illegal requests to provide services normally. DDoS attacks usually use a large number of botnets (botnet) or a large number of hosts controlled by malware, causing network congestion and preventing legitimate users to access the site[7]. DDoS attacks may cause unavailable target systems or network services, causing economic losses and affecting corporate reputation. Because a large number of malicious requests occupy too many system resources, legitimate users cannot access the target site, resulting in service interruption. Second, DDoS attacks may be used

for cyber extortion, and the attacker threatening the target network by launching an attack, demanding a ransom to stop the attack. In addition, DDoS attacks may be used to divert attention to attackers on other security vulnerabilities, causing greater damage. There are various types of DDoS attacks, including UDP Flood, TCP Flood, HTTP Flood, etc[8]. UDP Flood Attack send a large number of UDP packets to the target server and occupy the bandwidth of the target server, leading to network congestion; TCP Flood attacks exhaust the resources of TCP connection requests and failing the target server to handle normal connection requests, while HTTP Flood attacks simulate a large number of legitimate HTTP requests and occupy the server resources, making it unable to process the requests normally. As shown in Table 3.

Table 3: DDoS attack data sheet

Attack type	description	extent of injury
SYN Flood Attack	Send a lot of forged TCP connection requests and consume the server resources	tall
ICMP Flood Attack	Send large numbers of ICMP packets and occupy the target network bandwidth	centre
UDP Flood Attack	Send large numbers of UDP packets to congestion the target service port	tall

3.4 Computer have network security vulnerabilities

Computer network security vulnerability refers to the security vulnerability existing in a computer network that may be exploited by an attacker. Network security vulnerabilities may be caused by software defects, configuration errors, design vulnerabilities or unverified code, etc. An attacker can exploit the relevant vulnerabilities to attack, invade or destroy the system. The existence of network security vulnerabilities poses a serious threat to computer network security, which may lead the system to be invaded by remote attackers, obtain sensitive information, tamper with data or destroy the normal operation of the system[9]. Attackers can use vulnerabilities to conduct malicious code injection, denial of service attack (DoS), withdrawal attack and other behaviors, causing serious security problems. Secondly, network security vulnerabilities may be used for lateral diffusion. Once the attacker successfully uses the vulnerability to invade the system, he may continue to attack other network systems, forming chain attacks and causing greater damage. There are various types of network security vulnerabilities, including buffer overflow, code injection, cross-site script (XSS), cross-site request forgery (CSRF), etc. Buffer overflow is a common type of vulnerability. Covering the adjacent memory area, attackers may cause the program to crash or execute malicious code; code injection is the system to obtain permission; XSS and CSRF are common Web application vulnerabilities; by injecting malicious scripts or fake requests into the web page.

4. Security protection strategy of computer network information

4.1 Security protection strategy based on phishing issues

Computer phishing is a common means of network attack, phishing risk = Σ (attack success rate attack impact), the attack success rate can be obtained by historical data and statistical analysis, and the attack impact can be calculated by evaluating the potential impact of phishing attack on the system and the user. Through the quantitative assessment of phishing risk, the prevention strategy can be better formulated, and the following measures can be taken to prevent: (1) establish a strong anti-phishing filter. By using advanced anti-phishing technology, we can accurately identify and

effectively intercept all kinds of phishing websites, malicious links and false information, so as to ensure the security of network security and user data. Anti-phishing filters can identify potential phishing attacks by checking the website URL and analyzing the content of their messages. (2) Implement a secure email gateway. Anti-phishing techniques usually used in secure email gateways include URL link analysis, blacklist filtering, etc. Secure mail gateways can filter email messages containing malicious links or attachments, mark potential phishing messages, and effectively intercept malicious messages. (3) Use multi-factor authentication. Multi-factor authentication can improve the security of user login and reduce the risk of phishing attacks. Multi-factor authentication usually includes "knowledge factors" (such as password), "ownership factors" (such as mobile phone verification code) and "biological factors" (such as fingerprint identification) to reduce the scope of phishing attacks and protect user privacy. (4) Build and improve the safety awareness education and training system. For employees and users who use computer networks, it is necessary to strengthen network security awareness training, guide them on how to identify phishing attacks' characteristics, and be alert to unknown links. In order to improve employees' cognition and response ability to network security, we have decided to organize regular training on network security knowledge. The move aims to make employees more familiar with the means of common attacks such as phishing through professional guidance and practical drills, so as to reduce the success rate of such attacks and ensure enterprise information security. (5) In order to strengthen the network security guarantee, we must establish a sound network security monitoring system. This system needs to be efficient enough to quickly detect and respond to threats such as phishing attacks. By closely monitoring network traffic and user behavior, we are able to identify abnormal activities, deeply analyze potential risks, and immediately take the necessary protective measures. In addition, regular assessment of network security status and timely repair of potential vulnerabilities are of great significance to improve system security. We will be committed to continuously improve this system to ensure that the network security is fully and effectively guaranteed.[10]As shown in Figure 1.

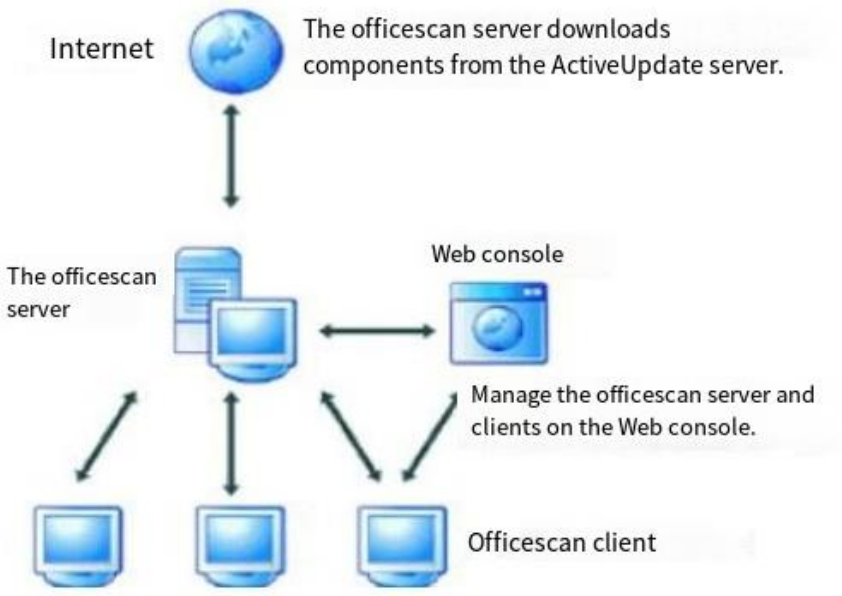

Figure 1: Security protection of phishing

4.2 Security protection strategy for computer viruses

For the possible virus attack of the computer, a scientific and effective security protection

strategy should be formulated, which can be achieved through the following methods: (1) install anti-virus software. When choosing anti-virus software, you should choose reputable brands, such as 360 anti-virus, Tencent computer butler, Avast anti-virus software, etc., and ensure the timely update of the virus library. Antivirus software works by identifying the virus through the signature code in the virus library. In general, the signature code is encoded according to the feature of the virus. When antivirus software finds a virus matching features in a computer, it sends an alarm and processes it.(2) Regular virus scanning. Virus scanning enables a comprehensive inspection of the documents and procedures in the system to detect potential viral threats. The virus scanner scans the files and directories in the system and detects them for a virus. If a virus is found, the scanner will isolate it and remind the user to clear it promptly, so as to protect the system security.(3) Download of software and files from unknown sources is prohibited. Software and documents from unknown sources may carry viruses and cause harm to computer systems. When using the calculation, you should try to avoid downloading the software and files with unknown sources, especially the files obtained through E-mail, network download and other ways. When downloading the software and files, you should ensure a reliable source and conduct antivirus testing.(4) Strengthen the email security management. Mail is one of the common ways of virus transmission, and extra caution needs to be taken. When using a computer, you should try to avoid downloading files with unknown sources, especially through E-mail, network download and other ways. For enterprise users, mail security management can be strengthened by setting mail filtering rules, mail scanning and encryption. (5) Update system patch. Vulnerabilities in operating systems and applications are important gateway to virus attacks. Timely updating of system patches can fix vulnerabilities and improve system security. The vulnerability utilization formula is: Risk = (Threat x Vulnerability) / Countermeasure. That is, the ratio of the risk is equal to the threat and the vulnerability. By timely updating the system patch, the vulnerability of the system can be reduced and the risk of being attacked by the virus can be reduced[11]. As shown in Figure 2.

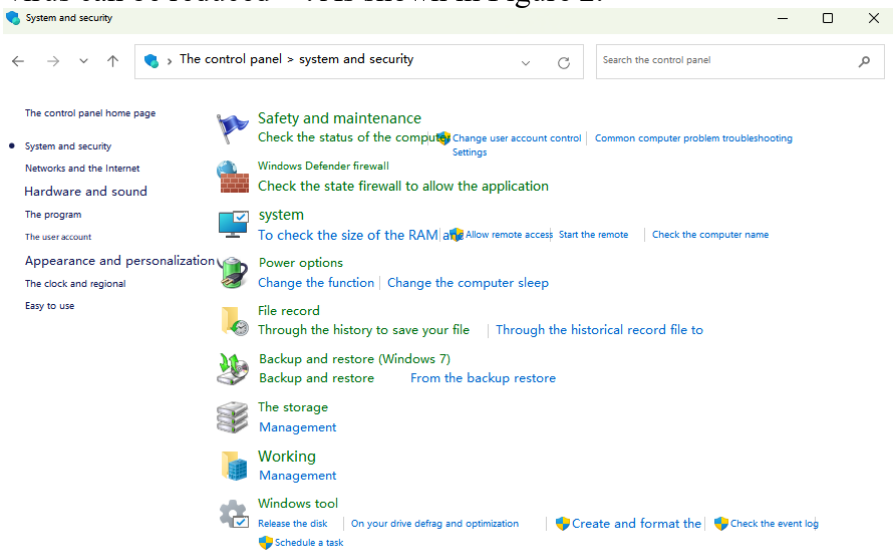

Figure 2: Prevention of computer viruses

4.3 Security strategies for DDoS attacks

In the face of DDoS attacks, the computer system needs to adopt a series of security protection strategies to protect the network security. The following are the common security protection strategies: (1) traffic filtering. Firewall, intrusion detection system (IDS) and intrusion prevention

system (IPS) are used to monitor and filter network traffic in real time. By setting rules, you can intercept abnormal traffic and malicious requests, reduce server load and prevent DDoS attacks. When setting the firewall rules, you can filter according to the traffic source, destination port, protocol and other information to intercept abnormal traffic and malicious requests. IDS and IPS devices can monitor network traffic in real time, detect abnormal behavior in time and take corresponding measures. In addition, the black and white list mechanism can be used to blacklist the malicious IP addresses to avoid continuing attacks on the server.(2) CDN acceleration. Use the Content Distribution Network (CDN) services to distribute the static resources of the website to nodes around the world, reducing server pressure. At the same time, CDN service provides DDoS attack protection function, which can intercept malicious traffic at the edge nodes, and only transfer the normal traffic to the source server, so as to protect the server from attacks.(3) Implement the flow limiting strategy. By setting a limited access rate, each IP address, user or source can prevent malicious attackers from taking too many resources. The token bucket algorithm or leakage bucket algorithm can be used to achieve flow limiting control, smooth limit the flow, and avoid the server by flood attack.(4) Strengthen cloud protection services. Cloud protection service is a flexible and efficient DDoS protection solution. By introducing the traffic to the cloud for cleaning and filtering, the malicious traffic can be effectively identified and blocked. Due to the flexibility and powerful processing power of cloud protection services, they can handle large-scale DDoS attacks and ensure the stable operation of network servers.(5) Establish a safety monitoring system. By establishing a security event monitoring system, one can monitor the network traffic, system log, and user behavior in real time, and find out any abnormal situations in a timely manner. When DDoS attacks are found, emergency response measures should be taken in time, such as blocking the IP address of the attacker, increasing protective equipment rules and regulations, etc., to reduce losses and restore the normal operation of the network[12]. As shown in Figure 3.

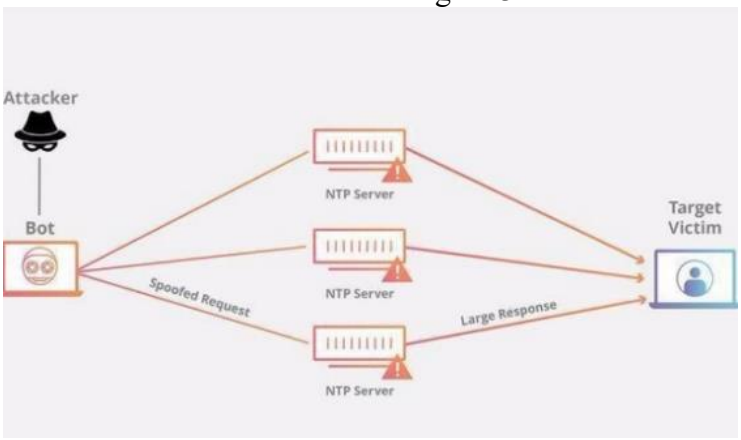

Figure 3: Prevention of DDoS attack

4.4 Strategies to guard against security vulnerabilities in the computer network

When dealing with the risks arising from computer network security vulnerabilities, the following measures can be taken to deal with: (1) formulate network security strategies. The network security strategy should include security policy, risk assessment, security control and emergency response. In the security policy, the basic principles and requirements of network security should be stipulated, including the requirements of access control, data protection, security audit and other aspects. Risk assessment is to evaluate the possible risks brought by network security vulnerabilities, and then formulate corresponding control measures. Security control includes technical control and management control, such as access control, data encryption, security

audit, etc. Emergency response is in the network security event, timely emergency response, to reduce losses.(2) Strengthen security vulnerability scanning. Vulnerability scanning is to scan the network system through scanning tools to find potential security vulnerabilities. Vulnerability scanning tools can be commercial tools or open-source tools, such as Nessus, OpenVAS, etc. After the vulnerability is found, it needs to be repaired in time to ensure the security of the network system. Fivulnerabilities can be updating patches, modifying configuration, closing unnecessary services, etc.(3) Continuously updating the patches. Computer systems, network devices, and software vendors irregularly release security patches to fix known security vulnerabilities. Therefore, the computer should update the patches of the operating system, browser, application and other software in time to ensure the security of the system.(4) Strengthen access control. The administrator should limit the access of users or external systems to the computer network by properly configuring firewalls, access control lists (ACL), and authentication mechanisms. Only authorized users can access the system resources, thus reducing the potential security risks.(5) Strengthen network monitoring and behavior analysis. Network monitoring tools can be used to monitor the network traffic in real time to find abnormal traffic and attack behavior in time. Behavior analysis is to analyze the behavior of users and devices and find abnormal behavior. Through the network monitoring and behavior analysis, the network security vulnerabilities can be found in time, and the corresponding measures can be taken to prevent them. As shown in Figure 4.

Figure 4: Preventing computer network security vulnerabilities

5. Conclusion

To sum up, through the specific analysis of computer network security and protection strategies, we can find out the main network security problems faced by computers at present, understand the causes of network security problems, and the possible harm caused by network security problems. Based on the specific security issues, effective protection strategies are put forward to ensure the healthy use of the network and avoid the economic losses for users and enterprises due to the network security problems. To establish a secure network environment, it is imperative to guarantee that the network effectively supports individuals' learning, daily life, and professional endeavors.

References

[1] Zhao Guanglei, Niu Junpeng. Analysis of computer Network Information Security and its Protection Strategy based on Computer Network Technology [J]. Science and Informatization, 2022 (3): 2.

[2] Li Haojie. Analysis of computer network information security protection strategy and evaluation algorithm [J]. Computer Programming Skills and Maintenance, 2023 (12): 168-170.

[3] Li Long. Computer network information security and Protection strategy in the era of big data [J]. Information

System Engineering, 2022 (7): 4.
[4] Guo Xiufeng. Research on computer Network Information Security and Protection Strategy in the era of Big Data [J]. Computer Application Abstract, 2022, 38 (23): 77-79.
[5] Chen Chong. Analysis of computer network and information security strategies based on big data [J]. Integrated circuit applications, 2023, 40 (7): 230-231.
[6] Pan Tianhao. Analysis of computer network information security protection strategy under the background of information technology [J]. Information and Computer, 2022, 34 (20): 220-222.
[7] Wen Ke-chun, Zhang Yi, Xu Tao. Analysis of computer network information security management strategy [J]. Computer Application Abstract, 2022 (9): 38.
[8] Yun Tao. Discussion on information security risks and defense strategies in the development process of computer network [J]. China Science and Technology Journal Database Industry A, 2022 (6): 3.
[9] Yu Guangxu. Information security protection strategy of computer communication network under the background of information technology [J]. Information and Computers, 2023, 35 (4): 239-241.
[10] Zhang Bofan. Contemporary computer network information security and protection strategy [J]. Chinese Science and Technology Journal Database (abstract edition) Engineering Technology, 2022 (9): 3.
[11] Wang Song, Zhao Ying. Brief analysis of computer network information security influencing factors and prevention strategies [J]. Electronic components and Information Technology, 2022 (10): 213-216.
[12] Hu Yuanyuan, Xiong Jiawei. Analysis of the influencing factors and preventive measures of computer network information security [J]. Network security Technology and Application, 2022 (4): 2.