Design of Personal Information Security Protection System in Computer Network

Qiyuan Jie

{jieqiyuan2008@126.com}

College of Computer and Information, Department of Information, Hohai University, Nanjing, 211100, Jiangsu Province, China

Abstract. With the rapid development of computer network technology, people pay more and more attention to the security of personal information. This issue involves multiple aspects, including the protection of different information resources such as physical and chemical layers, but also concerns about large data storage spaces (such as optical disk storage) and other information security issues. At the same time, due to the many unique functions and characteristics of computer network technology, users have a certain degree of dependence on personal information systems. This article aims to introduce a data encryption processing method based on the TCP/IP (Transfer Control Protocol/Internet Protocol) protocol to meet this challenge. This article will deeply discuss theories such as cryptography and access control, and design corresponding systems to protect user privacy from illegal means such as Trojan horses and virus intrusions. Finally, by using the identity authentication method, the key codes corresponding to the personal information content stored in the database will be verified and analyzed. The verification results show that the data integrity of the personal information in the system can be as high as 95%.

Keywords: Computer Network, Personal Information, Information Security, Protection System

1 Introduction

With the rapid development of the Internet, the network has become an indispensable part of people's life, and gradually integrated into the daily life and work in the information age. Personal information security plays a very important role. Computers and communication technologies, storage systems, and other information systems together constitute data resources. Therefore, effective protection of these data resources becomes particularly necessary. At the same time, in recent years, digital software has emerged continuously, making users' use more convenient and efficient.

Research on personal information security abroad started earlier, and developed countries such as the United States and Germany have established relatively mature and complete protection mechanisms in computer networks. However, domestic research on the concept and application of personal information data started relatively late. With the acceleration of social informatization, domestic scholars have also begun to pay attention to the importance and necessity of personal information security, and

ICSETPSD 2023, November 17-18, Coimbatore, India

DOI 10.4108/eai.17-11-2023.2342817

have carried out related work to achieve certain results. However, there are still some problems to be solved. Some scholars have proposed a "blacklist system", that is, when a company or organization is required to disclose personal information, it needs to go through a strict review process. Once it contains important customer data or other illegal information, it will be recorded in the company's database [1-2]. Some scholars believe that there are many security risks when individual users use the Internet for social activities, and apply some advanced foreign defense methods and concepts to the Internet [3-4]. Therefore, this paper will conduct research on the personal information security protection system based on the computer network.

With the continuous progress of society, computer network technology is becoming more and more popular, and people can obtain many resources through the Internet when using computers. However, personal information security is affected by many factors. This article aims to introduce a firewall-based method to solve the problem of personal information protection and intrusion prevention system design, and analyze and study the key parts of data encryption, identity authentication and authorization in the computer and propose solutions to achieve user privacy control measures. Finally, through the use of a protective gateway, the attack target is converted to the internal network, so as to effectively prevent illegal activities and protect the rights and interests of citizens.

2 Discussion on Personal Information Security Protection System in Computer Network

2.1 Computer Network

Computer networks are composed of various types of data, which are connected together through communication technologies to form a huge and open Internet. In this world, people can easily access the information they need. With the development of science and technology, people rely more and more on computer networks. In the past, personal computers were only used to handle work, but now computers can be used to process files, store and transmit emails, etc. [5-6]. At the same time, due to the strong capacity and scalability of computer network, it has become an indispensable part of modern life. By encrypting and protecting information, hackers or other illegal visitors can be prevented from stealing personal privacy and gaining the benefits of others, thereby ensuring the safety of users' property and personal living environment. At the same time, it is also very important to ensure the reliability and availability of the server, and provide timely fault notification and recovery functions to ensure the normal operation of the network. Its personal information protection network algorithm belongs to a certain category C_{ij} in the text category $C=\{C_1,C_2,...,C_m\}$. According to the naive Bayesian classification method, there are:

$$P(C_j|d)=\frac{P(C_j)P(d|C_j)}{P(d)} \tag{1}$$

$$P(d)=\sum_{i=1}^{m}P(C_i)P(d|C_i) \tag{2}$$

Formulas (1) and (2) represent the probability (ie, the posterior probability) that d belongs to category C_i under the condition of a given document d. Therefore, the classification problem becomes seeking C_j, as follows:

$$P(C_j|d)=\max\left\{P\left(C_j|d\right)\right\}_{i=1}^{n} \tag{3}$$

Support vector machines are effective data mining tools for classification, clustering, and time series analysis. The role of the computer network is to digitize, spatialize and intelligently process information in the physical world, connect various departments in different regions and countries through the Internet, and share resources to achieve interconnection. In the local area network, two ways of remote control and local management can be used for information sharing and interaction; using wireless technology in a wide area to control the network in the entire area, and at the same time, it can also access the global address network service or some users through the Internet to meet the requirements of different needs [7-8]. In this system, it is responsible for collecting user information and assigning it to the corresponding application software, and processing the information. At the same time, it can also transmit relevant files to other service providers through communication protocols and store them in the database to achieve the required functions. When transmitting information on the Internet, it is necessary to convert the original data into formatted files or other forms of services that can be utilized, shared, and have certain regular characteristics, such as email and communication protocols. Information on the web is often stored on servers in different ways. Electromagnetic wave signals are transmitted on the Internet. These signals are combined in various formats to produce a variety of communication methods and exchange methods. At the same time, services such as multimedia files and image materials can also be provided. All these services need to be realized through the network, so they also have the ability to transmit and share information, which is the so-called "paperless" transmission and storage.

2.2 Importance of Personal Information

Computer networks are composed of various types of data, which are connected together through communication technologies to form an open and huge Internet. It provides people all over the world with easy access to the information they need. With the continuous advancement of science and technology, people are increasingly dependent on computer networks [9-10]. Personal information plays an important role in computer networks, and its security is directly related to the normal operation and use of the Internet by users. If there is no perfect, safe and reliable protection mechanism, it will face problems such as hacker intrusion or virus intrusion, which will cause huge losses. Collecting and storing data on the Internet is pervasive and

complex. The Internet is characterized by openness and sharing, allowing users to interact and communicate directly. However, this also brings a drawback, personal privacy information is easy to leak, resulting in unnecessary losses. On the one hand, the confidential files of the enterprise may be illegally intercepted or deleted, affecting the normal use of network communication functions, or destroying system resource allocation, etc. On the other hand, important data and business secrets may be leaked [11-12]. Figure 1 is a data map of information protection strategies.

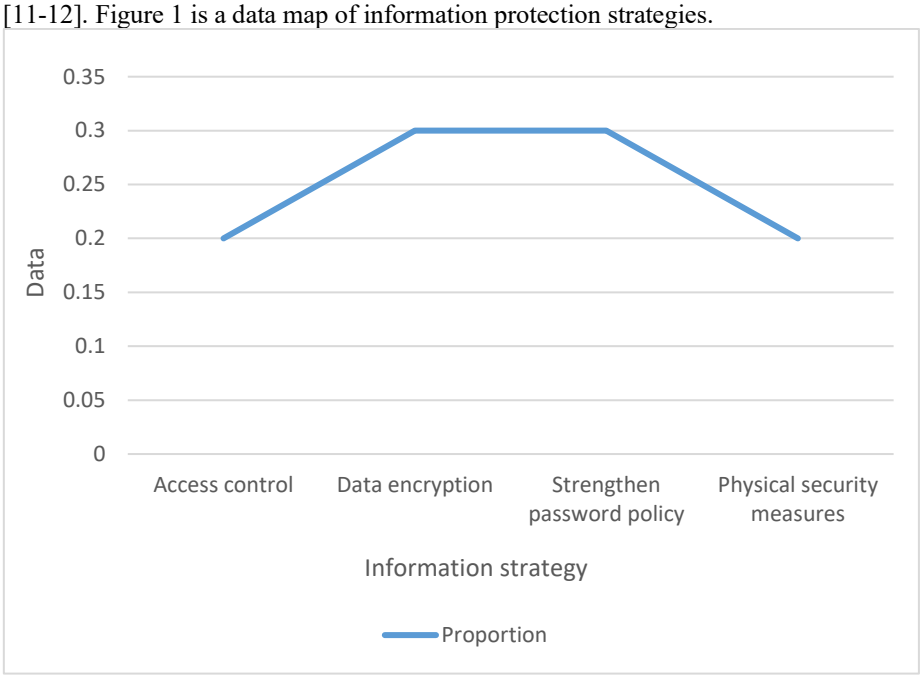

Fig.1 Information protection strategy

When transmitting information on the Internet, it is necessary to convert the original data into formatted files or other forms of services that can be used and shared with certain regular characteristics, such as email and communication protocols. Information on the web is often stored on servers in different ways. Electromagnetic wave signals are transmitted on the Internet. These signals are combined in various formats to produce a variety of communication methods and exchange methods. At the same time, services such as multimedia files and image materials can also be provided. All these service contents rely on the network to achieve, so they also have the ability to transmit and share information, which is the so-called "paperless" transmission and storage [13-14].

2.3 Information Security Protection

Information security protection refers to protecting the computer network and encrypting the data and files in it to ensure that it will not be leaked during storage and use. Its essential goal is to prevent the leakage of users' personal privacy, and adopt various technical means to prevent the risk of leakage and theft of personal information. Therefore, in the network environment, personal information systems must strengthen

measures such as user identity authentication and access authority settings to ensure that information will not be illegally invaded or stolen. Information security protection is an important part of the personal information system in the computer network, which aims to protect the data transmission process between users, systems and social entities from being leaked [15-16]. On the Internet, all behaviors exist in some form and are interrelated. These activities include encrypting information content (such as files), format and carrier (such as images or videos), and storage methods; protecting the network resources owned by unauthorized legal or illegal users through computer technology to ensure that users can normally access and apply their core data and realize various business functions. Information security protection aims to protect data, files, etc. through various means for encryption to ensure high reliability and integrity during transmission. Its goal is to ensure that users and other organizations in network services have a comprehensive and clear understanding of them. Figure 2 is a graph of the proportion of information leakage risk behaviors.

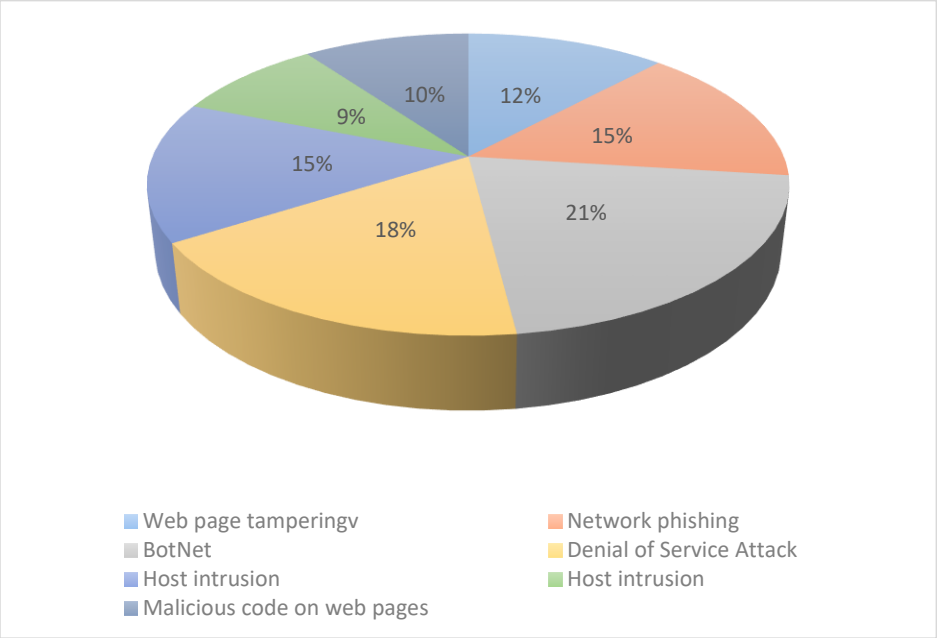

Fig.2 Dangerous behavior of information leakage

Protecting data from destruction, illegal use or disclosure by various means. In personal information management, the most important thing is to ensure that all users on the Internet can obtain a reliable, authentic, complete and accurate identity authentication system to ensure the security and confidentiality of the network environment [17-18]. In addition, it is necessary to strengthen the professional skills training of the design and operation and maintenance personnel of the security protection system, and understand its operation methods and procedures, in order to effectively protect the security of user information. Information security protection is to take certain technical measures to protect data and storage during system operation,

so as to prevent or reduce uncertainties caused by external environmental factors. This protection is achieved through technical means, for example, using passwords, electronic keys, etc. to prevent illegal operations and ensure the security of transmission between users and servers. Using identity authentication or physical isolation to prevent hackers or Trojans from intruding, and use firewalls, security protocols, and intrusion detection systems to protect computer networks to ensure that data is not leaked and destroyed during transmission, thereby ensuring information security [19-20]. When transmitting important content such as user names and passwords in a computer network, a special method can be used to achieve plaintext or unauthorized access control. For example, combined with digital signature and other public key algorithms to process sensitive documents, it can also be regarded as ciphertext encryption, and the ciphertext can be decrypted by technical means such as information digest length limitation.

3 Experimental Process of Personal Information Security Protection System in Computer Network

3.1 Architecture of Personal Information Security Protection System

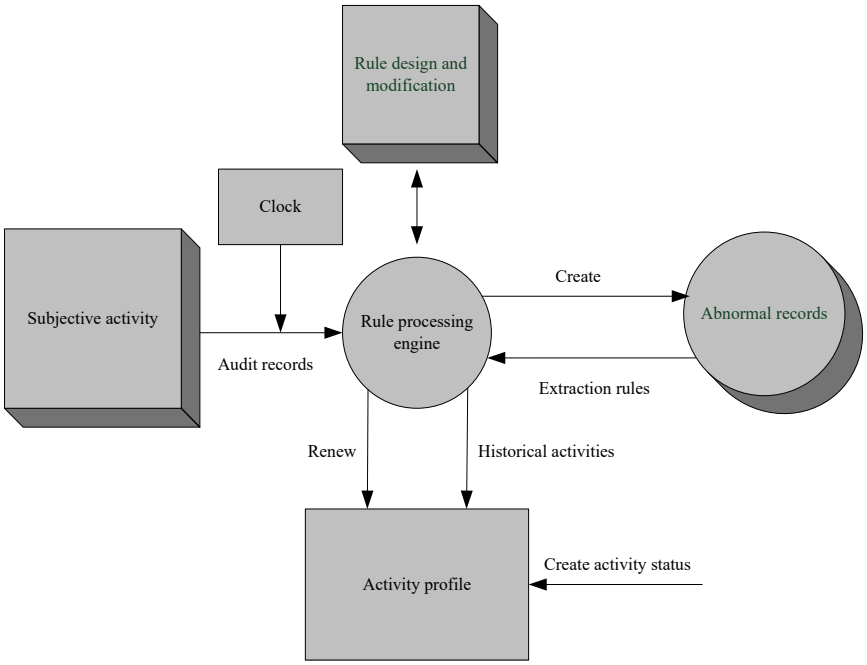

Fig.3 Personal information security protection system

In the computer network personal information security protection system, as shown in Figure 3, the modules include data protection and access control. The first is data

protection, whose main task is to verify user identities. If the user logs in to the database or illegally obtains other people's information through authorization, the system will refuse to provide services to them, and return to the home page to confirm whether the use of the server or client functions is allowed. Once the user enters the correct answer, the system will directly read the information content on the memory, and transmit the personal information data required by the user on the network to the cache table for searching and recording. The architecture of the personal information security protection system is composed of multiple subsystems, and each subsystem is composed of several independent functional modules. These independent modules can implement operations such as accessing, modifying, and deleting data. However, when data is transmitted in the network, there are defects in the storage medium and physical structure that may lead to abnormal use or improper storage, resulting in information leakage or damage. Therefore, the computer system needs to connect all servers and clients to ensure that users can safely log in to the application software they manage and perform corresponding functions. In order to protect personal information systems from attacks and illegal access, users need to obtain corresponding keys when using different types of software, and prevent personal information from being leaked or lost during transmission.

For sensitive files and important materials, certain security protection measures need to be taken to effectively prevent illegal access or steal valuable data stored in other people's computer user accounts. At the same time, setting corresponding passwords in the network can ensure the integrity of information and prevent damage or theft. In the personal information security protection system, the administrator is the core role of the system, including passwords, login names, and permissions. After registering as a member, ordinary users can use their accounts to log in to the network platform to obtain relevant information resources such as personal gateways and website servers that they want to browse and serve. The super administrator is responsible for managing all data and maintaining the security of the database. When users use computers, they need to be authorized by the database management. Without permission, it cannot directly enter the database management system and obtain relevant permissions, and users who have obtained login rights through system authentication cannot access the storage space in the system. If there is no legal identity verification or the password is entered incorrectly, only this piece of data information can be accessed, and it will be encrypted to prevent illegal elements from stealing user accounts and passwords. The access control part is mainly responsible for restricting the input of account numbers and passwords during registration, and at the same time providing necessary query interfaces to help administrators find legal and compliant users.

In addition, it is also necessary to add an index to the database to identify and store the information that the data was intercepted during a certain period of time, so as to prevent illegal users from transferring it after logging in. In order to improve the safety and reliability of personal security defense measures, the database should be backed up, and the application of server log control function, firewall technology and intrusion prevention technology should be strengthened. In addition, a data access analysis module can also be added to improve the fault tolerance rate of the system, thereby reducing the probability of network attacks.

3.2 Functional Test of Personal Information Security Protection System

In order to ensure the security of personal information in the network, it is necessary to detect whether there is an abnormal situation by finding faults when the system is running. Data layers of different types, levels or locations should have different permission access. If the user can log in normally and operate in the application, it means that the software has the appropriate authority to access and protect personal information and prevent illegal modification and other acts. On the contrary, if the user illegally enters the website to maintain personal information, the system needs to be tested, and the abnormal situation and its cause can be detected through the security protection module. During the functional testing process of the computer network personal information security protection system, the input data is mainly checked through user login, and compared with the corresponding data in the database. At the same time, it is also necessary to check whether it complies with relevant regulations. After successful authentication, we can continue to access other resources such as server logs and log files. If the result does not meet the requirements, then returning the address or change the password. Otherwise, it will jump to the blacklist interface to remind users of the functional requirements of the personal information security protection system. The system realizes the functions of user login, registration, deletion and alarm, and can control the operation of database files and application programs on the server after inputting the security algorithm. For illegal visitors, key settings can prevent illegal behavior or isolate intrusion in a secure domain. Use of personal information storage, modification and deletion permissions without internal authorization is prohibited. When personal information data is stored in the database, it can directly find relevant personnel on the website to perform operations. On the contrary, if a field in the database is missing or there is abnormal data, the data can also be detected and deleted from the webpage (for ordinary netizens), and the prompt to enter the password and login date will not pop up, and the system will judge whether there is permission restriction.

4 Experimental Analysis of Personal Information Security Protection System in Computer Network

Table 1. Personal Information Security Protection System Function Test

Test times	Requirement analysis	Risk assessment	Compatibility (%)	Serviceability(%)
1	Data encryption and decryption	Low	93	92
2	Data classification and access control	Low	95	94
3	Security audit and monitoring	Low	95	96
4	Data backup and recovery	Low	97	94
5	Security vulnerability scanning and repair	Low	95	96

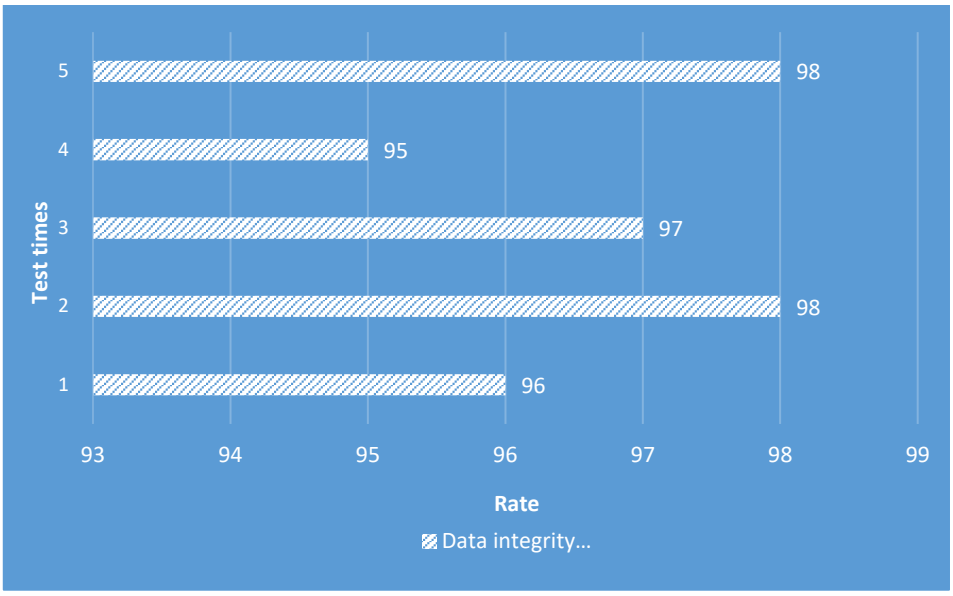

Fig.1 Data integrity of personal information

In order to protect the security of users' personal information, the network system will encrypt sensitive data after users input it, and transmit the encrypted data to the database or server. At the same time, the system will also set an alarm function, once the password is cracked, an alarm will be issued. To ensure security, the system first needs to verify that the stored key matches the one set by the user. Secondly, it is necessary to detect the identity information of all visitors and relevant information of authorized personnel to confirm whether there is any illegal operation and record it. Additionally, data can be encrypted in the background for added security. Table 1 is the data performance of this test.

If a system has been hacked or attacked by a malicious program, administrators are alerted and can take appropriate action. In the computer network system, the user's personal information will change with the time of use, so the data needs to be encrypted. It can be seen from Figure 4 that the data integrity of personal information in this system can be as high as 95%. Through the cryptographic algorithm, the encrypted ciphertext can be converted into plaintext. When the data changes, the corresponding level or authority will also increase accordingly. If it is a super administrator, it can also modify the contents of confidential files and other important information stored by ordinary registrants in the database.

5 Conclusion

With the continuous progress of society, computer network has become an indispensable part of people's life, and its development is becoming more and more rapid. However, in the Internet age, the issue of personal information security has become increasingly prominent. This paper aims to address some current hidden

dangers of personal information security, and proposes a comprehensive measure to protect user data and related documents. These measures include firewalls, anti-virus software and other technologies as the core, and through setting access control policies and encryption algorithms to realize the detection and protection management of a large number of individual sensitive content stored in the server. In addition, the password verification function of the key can also be used to prevent illegal logins from stealing other people's private resources, thereby solving the above problems and improving the operating efficiency of the computer network system. The implementation of these measures will help ensure the security of personal information to protect users from cyber attacks and violations.

References

[1] Skrynnyk O .Some Aspects of Information Security in Digital Organizational Management System[J].Marketing and Management of Innovations, 2021, 4(4):279-289.

[2] Black M L .Usable and Useful: On the Origins of Transparent Design in Personal Computing:[J].Science, Technology, & Human Values, 2020, 45(3):515-537.

[3] Lozovsky V V .Information Security: Protection against Internal and External Impacts in Cyberspace[J].Military Thought, 2019, 28(4):10-14.

[4] Cheng W , Ou W , Yin X ,et al.A Privacy-Protection Model for Patients[J].Security and Communication Networks, 2020, 2020(1):1-12.

[5] Choi W S , Lee J Y , Shin J .A Study on the Protection and Utilization of Personal Information for the Operation of Artificial Intelligence and Big Data in the Fourth Industrial Revolution[J].Jouranl of Information and Security, 2019, 19(5):63-73.

[6] Fataliyev T , Mehdiyev S .Industry 4.0: The Oil and Gas Sector Security and Personal Data Protection[J].International Journal of Engineering and Manufacturing, 2020, 10(2):1-14.

[7] Viljoen I , Castelyn C , Pope A ,et al.Contact tracing during the COVID-19 pandemic: Protection of personal information in South Africa[J].South African Journal of Bioethics and Law, 2020, 13(1):15-20.

[8] Souza J S D , Abe J M , Lima L A D ,et al.The Brazilian Law on Personal Data Protection[J].International Journal of Network Security & Its Applications, 2020, 12(6):15-25.

[9] Liu J , Zhou S .Application Research of Data Mining Technology in Personal Privacy Protection and Material Data Analysis[J].Integrated Ferroelectrics, 2021, 216(1):29-42.

[10] Chellappan K , Kannan M K J .PII classification and Applicability in Personal Data Protection Bill 2019[J].GIS-Zeitschrift fü Geoinformatik, 2021, 1(8):1417-1424.

[11] Krasniqi S . Legal Protection of Personal Data in the Function of Protection of Human Rights and Freedoms[J]. International Journal of Research -GRANTHAALAYAH, 2020, 8(10):193-197.

[12] Yarovenko H .Influence of the Country Economic Development on the Dependence of the Use of Personal Information Security and the Consequences of Cybercrime[J].Visnik Sums′kogo deržavnogo unìversitetu, 2020(1):188-198.

[13] Maslova M , Ryzhaja K .Internet Fraud as a Threat to Personal Information Security[J].NBI Technologies, 2019(2):25-28.

[14] Kibakin M V .Social diagnostics of information security of digital society: methodological and regulatory aspects[J].Digital Sociology, 2020, 2(3):25-32.

[15] Klychova G , Zakirova A , Zalyalova N ,et al. The Theoretical Bases of Ensuring

Economic Security in the Enterprise Human Resources Management System[J]. Vestnik of Kazan state agrarin university, 2020, 14(4):107-113.
[16] Belhadjali M , Abbasi S , Whaley G .Personal Information Privacy: Some Findings on Gender Difference[J].Archives of Business Research, 2021, 9(7):95-99.
[17] Yarovenko H , Kuzmenko O , Stumpo M .DEA-Analysis Of The Effectiveness Of The Country's Information Security System[J].SocioEconomic Challenges, 2020, 4(3):142-153.
[18] Sizov V A , Malinichev D M , Mochalov V V .Improvement of the Regulatory Framework of Information Security for Terminal Access Devices of the State Information System[J].Open Education, 2020, 24(2):73-79.
[19] Boc K , Dvorak Z , Ekerevac Z .Security of Information and Communication Technologies[J].FBIM Transactions, 2019, 7(1):29-37.
[20] Pechyonkina A , Selifanov V .Security Systems Used with Virtualization Technology[J]. Interexpo GEO-Siberia, 2019, 6(2):150-158.