Study on the Criteria for Determining Destructive Programs in Computer System Crimes

Chong Jiang

Shanxi Agricultural University, Law, Department of Law, School of Public Administration, Jinzhong, Shanxi, 030801, China

3200312876@qq.com

Abstract. This thesis discusses the identification of destructive programs in computer system crimes and studies the role of relevant identification standards in judicial practice. Firstly, the study's background, purpose, and significance are introduced, and then the concept and characteristics of a destructive program are elaborated in detail, including definition, classification, and characteristics. Then it focuses on identifying destructive programs in computer system crimes, analyzing the role of destructive programs in crimes, and establishing identification standards. The role of relevant identification standards in judicial practice is explored, including the importance of legal provisions, jurisprudence interpretation, and expert identification. The thesis further examines the refinement and improvement of the identification standards of destructive procedures, analyzes the current status of relevant research at home and abroad, existing problems and challenges, and puts forward suggestions for refinement and improvement. Finally, the application and impact of destructive procedures in specific cases are discussed through case studies. The main research findings are derived from the research and discussion in this thesis; the limitations of the research and suggestions for further research are discussed. The study is of practical significance for strengthening the fight against computer system crimes and identifying such crimes in judicial practice.

Keywords: computer system crimes, disruptive programs, identification criteria, judicial practice, case studies.

1 Introduction

1.1 Background of the Study

As a kind of malware, destructive programs are increasingly rampant in computer systems, bringing great threats to network security. With the rapid development of the Internet, the types and quantities of destructive programs are increasing, bringing great losses and impacts to computer systems. Therefore, the recognition and identification of destructive programs have become one of the hot spots in the current research on computer system crimes.

Z. Zhan et al. (eds.), *Proceedings of the 2024 10th International Conference on Humanities and Social Science Research (ICHSSR 2024)*, Advances in Social Science, Education and Humanities Research 858,
https://doi.org/10.2991/978-2-38476-277-4_92

1.2 Purpose and Significance of Research

The purpose of this study is to explore the identification criteria of destructive programs in computer system crimes and their judicial role. Through an in-depth analysis of the concept, characteristics, and classification of destructive programs and taking into account cases and the current state of research at home and abroad, it puts forward proposals to improve the identification criteria. The study aims to deepen understanding, promote the development of related fields, provide new ideas for combating computer system crimes, and contribute to building a more secure network and social stability.

Focusing on the identification of destructive programs in computer system crimes is of theoretical and practical significance. The research helps to improve laws and regulations and raise the level of system security protection; it promotes the standardization and specialization of expert appraisal and enhances judicial justice and efficiency; it provides a reference for the improvement of the determination standard and a concrete basis for future research and practice. It is expected that the research can promote the enhancement of computer system security and social security in China.

2 Concepts and Characteristics of Destructive Procedures

2.1 Definition of Destructive Programs

A destructive program is a category of malware whose main purpose is to damage or disrupt a computer system, network, or data. This malware may lead to serious consequences such as system crashes, data loss, and information leakage. A destructive program is usually hidden in a normal program to trick the user into executing it, and once it is executed, it begins to damage the system or data. Therefore, the definition of destructive programs focuses on their destructive effects on computer systems, networks, and data, as well as the way they are hidden and spread. The definition of destructive programs is crucial in computer system crimes, as it helps the judiciary identify and prosecute criminals who use this malware. Therefore, an accurate definition of destructive programs is important for effectively combating computer system crime.

2.2 Classification of Destructive Programs

Destructive programs can be divided into various types according to the method of destruction and the degree of impact. Direct destructive elements, such as viruses and worms, directly change the system structure or destroy key files; indirect destructive elements, such as Trojan horses, backdoors, and the use of loopholes or malicious code, indirectly damage the system. In addition, according to the nature of the harm, the mode of transmission, and the scope of infection, which can be divided into light, medium, and heavy destructive programs, the degree of impact on the system and the degree of harm vary. Therefore, when studying the criteria for the identification of destructive programs, it is necessary to give full consideration to their characteristics

and differences to more accurately identify and respond to destructive behaviors in computer system crimes.

2.3 Characteristics of Destructive Programs

Destructive programs are those that have a malicious purpose and are capable of causing damage to a computer system. In the context of computer system crimes, the characteristics of destructive programs include the following:

①Destructive programs are characterized by a high degree of concealment. Such programs often disguise themselves as normal software or files to avoid system detection and defense. Through virtualization technology and other means, destructive programs can quietly lurk in the system, waiting to be triggered before showing their malicious intent.

②Destructive programs have the characteristic of being highly destructive. Once triggered for execution, such programs can cause serious impacts on the normal operation of the system, such as destroying files, tampering with data, altering configuration information, etc., thus leading to system crashes or data loss.

③Destructive programs are characterized by strong propagation. Once infected with a virus or malware, such programs will spread in various ways, infecting more computer systems and forming a chain of destruction.

④Destructive programs also have the characteristic of being highly targeted. This type of program usually selects appropriate means and methods of attack according to the characteristics and vulnerabilities of the target system to achieve the purpose of destroying or stealing information.

In conclusion, the characteristics of destructive programs are complex and varied and need to be analyzed and studied in depth in research and prevention to guarantee the security and stable operation of computer systems.

3 Problems of Identifying Destructive Programs in Computer System Crimes

3.1 Overview of Computer System Crime

Computer system crime is the use of computers and networks to carry out illegal activities, violate rights and interests, or disrupt order. It takes various forms, including hacking, e-commerce fraud, and virus transmission. Crime is covert, global, and rapid, posing a threat to individuals, businesses, and the state. Therefore, research, technical prevention, law enforcement efforts, and the construction of laws and regulations need to be strengthened to combat crime and maintain cybersecurity and social stability.

3.2 The Role of Destructive Programs in Computer System Crime

Disruptive programs play a key role in computer system crime and are becoming increasingly harmful as technology develops. It can be used to carry out denial-of-service (DDoS) attacks, causing systems to crash, affecting users, and leading to financial losses. Meanwhile, destructive programs can steal sensitive information, such as privacy and trade secrets, leading to crimes such as financial fraud. In addition, it is used for extortion and intimidation, and it may even paralyze critical infrastructure, causing serious disasters in society. Therefore, strengthening the research and regulation of destructive programs and improving laws and regulations are crucial to combating computer system crimes.

3.3 Criteria for Determining Destructive Procedures

The identification of destructive programs is one of the core issues in computer system crime cases. In judicial practice, the identification of destructive programs needs to be carried out according to certain standards and methods to ensure the accurate definition of criminal behavior and the effective admission of evidence. The criteria for the identification of destructive programs are shown in Table 1, which mainly includes the analysis and judgment of the program's functional characteristics, viral behavior, propagation methods, and other aspects.

First, in determining destructive programs, the functional characteristics of the program need to be considered. Destructive programs usually have the function of damaging, tampering with, or disrupting the normal operation of a computer system. By analyzing the code and execution logic of the program, it can be determined whether the program has destructive characteristics. In addition, it is necessary to consider such features as the program's hidden nature and self-starting ability, which help determine the degree of destructiveness of the program.

Second, the identification of destructive programs also requires attention to virus behavior. Viruses are a common form of destructive program with the ability to self-replicate and infect other programs. In the process of destructive program determination, it is necessary to analyze the propagation path of the program, the mode of infection, and the characteristics of the virus code to determine whether it is a viral destructive program.

In addition, the determination of destructive programs also needs to consider the mode of dissemination of the programs. Destructive programs are usually disseminated through networks or other media, so the path and mode of dissemination of the programs need to be analyzed and traced. By analyzing the propagation characteristics of the program, the source and propagation path of the destructive program can be determined, providing important clues for the investigation and determination of responsibility in the case.[1]

In summary, the criteria for the determination of destructive programs involve the analysis and judgment of many aspects, such as the functional characteristics of the program, the behavior of the virus, and the mode of dissemination. Judicial organs should take these factors into account when determining destructive programs to en-

sure that criminal acts are determined objectively and accurately and that network security and social order are maintained.

Table 1. Criteria for recognizing destructive procedures

The core of the problem	Determination of need	criteria for determining whether something is right	Functional characteristic	Virus Behavior Analysis	Analysis of modes of dissemination	Judicial considerations
The determination of destructive programs is one of the core issues in computer system crime cases.	The determination of disruptive procedures needs to be based on certain criteria and methods to ensure the precise definition of the criminal act and the effective admissibility of evidence.	The determination criteria mainly include the analysis and judgment of the program's functional characteristics, virus behavior, and propagation mode.	Functional characteristics of a program include its ability to damage, tamper with, or disrupt the normal operation of a computer system, as well as concealment and self-starting capabilities.	The identification of destructive programs also requires attention to the ability of the virus to self-replicate and infect other programs.	The paths and modes of propagation of programs need to be analyzed to determine the source and spread of destructive programs.	When the judiciary determines destructive programs, it should take into account the functional characteristics, viral behaviors, and modes of transmission.
				Analyze transmission paths, infection methods, and virus code characteristics.	Provide clues for the case investigation and determination of responsibility.	To ensure the objective and accurate determination of criminal behavior and the maintenance of network security and social order.

4 The Judicially Recognized Role of Relevant Accreditation Standards

4.1 Legal Provisions and Interpretation of Jurisprudence

In computer system crimes, the identification of destructive programs cannot be separated from legal provisions and jurisprudential interpretations. The Criminal Law of the People's Republic of China stipulates the definition, categorization, and criminal liability of destructive programs, providing specific guidance for the application of the law. At the same time, jurisprudence in judicial practice also provides an important reference for the determination of disruptive procedures. Judges study jurisprudence to better understand the characteristics of disruptive processes and ensure the accurate determination of criminal acts. Legal provisions and case law interpretations are crucial in the determination process, which needs to be strictly followed and combined with practice to effectively combat computer crime. At the same time, laws and regulations need to be continuously improved to meet new challenges and safeguard network security and social stability.

4.2 Importance of Expert Appraisal

Expert appraisal plays a crucial role in the field of justice, especially in the process of determining disruptive procedures. The expert appraisal is an in-depth analysis and assessment of the techniques and procedures involved in a case through specialized knowledge and technical means, providing the court with objective and professional opinions and conclusions.[2]

First, expert appraisal plays a pivotal role in computer system crime cases, helping judges and juries gain an in-depth understanding of the complex technical issues in the case. The functions and features of destructive programs often involve esoteric technical knowledge that requires an expert to identify them through specialized knowledge accurately. Not only are experts able to explain technical terms, program code, and data structures, but they can also assist judges and juries in better grasping the facts of a case so that they can make informed decisions.

Secondly, expert appraisal provides objective evidence to support the case. The experts use scientific methods and technical means to carry out in-depth analysis and verification of the technical issues in the case, providing the court with reliable and authoritative evidence. These conclusions have a significant impact on the outcome of the case and help to ensure the fairness and accuracy of the decision.

In addition, expert appraisal also helps to enhance the fairness and credibility of cases. The expert's professional appraisal helps to reduce subjective assumptions and misjudgments and ensures the fairness and objectivity of the case process. Expert appraisal not only provides strong technical support for the court but also provides fair treatment for the parties, further maintaining judicial authority and credibility.

In summary, expert appraisal plays an irreplaceable role in identifying destructive procedures. Through professional technical support and objective analysis, we can accurately appraise the characteristics and functions of destructive programs and pro-

vide a scientific and reasonable basis for judicial decisions. Therefore, in computer system crime cases, we should attach great importance to the role of expert appraisal to ensure judicial justice and an effective trial of cases.

4.3 Applicability and Reasonableness of Identification Criteria

The application of identification standards in the administration of justice is very important, and it has a direct impact on the outcome of cases and judicial justice. In computer system crimes, the identification of destructive programs needs to be based on certain identification standards, which must be applicable and reasonable.[3]

First, the applicability of the identification criteria refers to the ability to accurately and comprehensively assess the nature and threat level of destructive programs in practical application. This requires that the standards be able to cover various types of destructive programs, including viruses, Trojan horses, malware, etc., while also taking into account the different forms and means that destructive programs may take. Only based on broad applicability can the identification standards truly help the judiciary accurately identify destructive programs and guarantee a fair trial.

Secondly, the reasonableness of the appraisal criteria means that the criteria themselves should be in line with legal provisions and scientific principles to ensure the objectivity and accuracy of the assessment. Appraisal standards should be established based on science and technology, with the help of advanced technical means and methods of destructive program appraisal. At the same time, the appraisal standard should also follow the provisions of laws and regulations to ensure the legitimacy and validity of its assessment results. Only on a reasonable basis can appraisal standards become a powerful basis for judicial bodies to identify destructive procedures and ensure that criminals are duly punished.

In conclusion, the applicability and reasonableness of identification standards are important guarantees of judicial justice and the maintenance of social security. Future research should continue to deepen the study of destructive programs, constantly refine and improve identification standards, provide more scientific and reliable identification methods for judicial institutions, and effectively combat computer system crimes.

5 Refinement and Improvement of Criteria for Determining Destructive Processes

5.1 Current Status of Relevant Domestic and Overseas Research

The issue of criteria for the determination of destructive programs has always attracted the attention of scholars at home and abroad. In foreign countries, research focuses mainly on the in-depth analysis of the technical and behavioral characteristics of destructive procedures, such as their concealment, self-replicating ability, and potential harm, which are used as important bases for identification. At the same time, Europe, Japan, and other countries are constantly improving their systems of recognizing de-

structive procedures through the comprehensive application of laws, technologies, and practical experience.

In contrast, domestic research in this area is still insufficient, mostly limited to the interpretation of legal provisions and case analysis. Therefore, scholars have suggested that research on the technical characteristics of disruptive procedures be strengthened to better guide judicial practice and ensure the accurate identification of criminal acts. In addition, the country is actively exploring the establishment of a specialized agency for the identification of destructive procedures, which, through the provision of a professional technical team, will be responsible for the identification of destructive procedures and the collection of evidence to further improve the accuracy and scientificity of the determination.

Research at home and abroad on the issue of criteria for the identification of destructive procedures is being deepened and improved, but there are still some challenges and problems that need to be solved. Future research should pay more attention to the combination of technology and law and establish a more scientific and effective system for the identification of destructive procedures to better meet the challenges of destructive procedures in computer system crimes.[4]

5.2 Problems and Challenges

There are multiple problems and challenges in the identification of destructive procedures. First, the technological development of destructive procedures is rapidly changing, and new types of destructive procedures are constantly emerging, bringing new challenges to crime investigation and judicial determination. Owing to the technical and hidden nature of destructive procedures, it is difficult to accurately identify and characterize them, resulting in difficulties in their identification.

Secondly, the role of destructive programs in computer system crimes has become increasingly prominent, with various types of destructive programs posing a great threat to network security and information security. However, the existing standards for the identification of destructive programs are inadequate in responding to new types of destructive programs and are unable to respond in a timely and effective manner to the ever-changing forms and means of crime.

In addition, the subjective and technical nature of expert appraisal is also a difficult issue in the determination of destructive procedures. Expert appraisal plays a crucial role in the process of determining destructive procedures, but the results of the expert appraisal are affected by personal experience, technical level and level of understanding, and lack of objectivity and standardization, which can easily lead to uncertainty and controversy in the results of the determination.[5]

Therefore, establishing scientific, reasonable, objective, and fair criteria for the determination of destructive procedures, strengthening the combination of technical and legal means, and improving the objectivity and accuracy of expert appraisal are important issues and challenges facing the current determination of destructive procedures. Further in-depth studies and research are needed to improve the determination system and safeguard the accuracy and authority of criminal evidence.[6]

5.3 Suggestions for Refinement and Improvement

In the course of our research, we found that there are still some problems and challenges in the criteria for the identification of destructive programs, and to better deal with the problem of destructive programs in computer system crimes, we put forward the following suggestions for improvement and refinement:[7]

Research on the definition and classification of destructive procedures should be strengthened, and the characteristics of various types of destructive procedures should be clarified, to more accurately identify and distinguish between different types of destructive procedures. At the same time, legislative bodies should be pushed to strengthen the control and supervision of disruptive procedures, build a more complete system of laws and regulations, intensify the fight against disruptive procedure crimes, and increase the penalties for offenders to create an effective deterrent effect.

In addition, it is vital to strengthen the construction and training of forensic identification organizations and expert teams to enhance their professionalism and technical capabilities, ensure that identification results are objective, fair, and accurate, and provide strong support for judicial practice. Finally, it is advocated that international cooperation and information exchange should be strengthened to jointly address cross-border destructive procedural criminal activities and that international law enforcement cooperation and information-sharing should be intensified to form a collaborative mechanism for combating destructive procedural crimes.

Through the refinement and improvement of the above suggestions, we can more effectively deal with the problem of determining destructive programs in computer system crimes and enhance the accuracy and fairness of judicial determinations to further protect the security and stability of computer systems.

6 Case Studies and Discussions

6.1 Case 1: A Company Accused of Using Destructive Programs to Steal Trade Secrets

In this case, a company was involved in a judicial dispute over the use of a suspected destructive program to steal trade secrets. A destructive program is malicious software that destroys, tampers with, or steals data from a target, causing serious damage. The determination of a destructive program requires consideration of the malicious and destructive nature of the program's design, the legality of its dissemination and use, and whether it has caused damage to the victim. The court will determine whether the alleged program is destructive according to the identification criteria and expert opinion and will rule accordingly.

In future judicial practice, the criteria for the identification of destructive procedures should be constantly refined and improved to meet the development of new types of criminal acts and technical means. Only by ensuring the scientific, objective, and operational nature of the identification criteria can the public interests of society and the legitimate rights and interests of individuals be better protected.[8]

6.2 Case 2: Hacking Attacks Paralyzing Power Systems

Hacking is a common form of computer system crime, and its destructive programs often have serious consequences. In this case, hackers invaded the power system of a large city and manipulated key equipment to paralyze it. Complex destructive programs were used to change the control logic, leading to widespread power outages. The incident caused great inconvenience and losses to residents and business operations, as well as serious disruptions to traffic order. In response to this incident, the relevant departments launched an investigation and tracking work, trying to find out the identity of the hacker and the motive of the crime. Through technical identification and data analysis, it was finally confirmed that the hackers used a series of destructive programs to attack the power system. The incident also drew the attention of all sectors of the community to network security and strengthened monitoring and preventive measures for system security.

Therefore, the incident of power system paralysis caused by a hacker attack is a typical case of computer system crime, and the destructive program used behind it has caused serious consequences for society. To prevent similar incidents from recurring, it is necessary to strengthen the monitoring and management of network security, increase the combat against destructive programs, and safeguard the information security and stable operation of society.

6.3 Case 3: Use of Disruptive Programs in Cyber Frauds

As an important part of the continuous renovation and upgrading of criminal means, network fraud and destructive programs play a particularly critical role. Criminals, through tampering, deletion, dissemination of malicious code and other tactics, and the use of destructive programs to implement network fraud in the community, have brought about a profound economic impact and security risks.

In cases of network fraud, destructive programs are often used for purposes such as stealing sensitive personal information, stealing property, and destroying information systems. For example, by sending e-mails containing Trojan viruses, phishing scams disguised as legitimate websites, and other means, criminals use destructive programs to easily obtain users' account codes, bank card information, and other private data, and then carry out illegal transfers, theft of assets, and other unlawful acts.

In a judicial trial, accurately identifying the destructive program in network fraud cases is particularly critical. Only by clearly defining the types and characteristics of destructive procedures and accordingly conducting professional identification can we more effectively combat cybercrime activities and effectively protect the legitimate rights and interests of citizens. To this end, the judicial authorities should rely on professional and technical teams, with the help of advanced forensic technology and identification methods, to examine the destructive program in network fraud cases for a comprehensive and in-depth review. At the same time, we also need to continuously improve the identification standards of destructive procedures, keep pace with technological development, and update identification methods promptly to improve the efficiency and accuracy of case investigation.

In conclusion, the use of destructive programs in cyber fraud poses a serious threat to social security. Judicial organs should attach great importance to this problem and intensify their efforts to combat it through scientific and reasonable means to fundamentally maintain the security and order of cyberspace.

7 Conclusion

7.1 Key Findings

In this study, we explore the identification of destructive programs in computer system crimes and examine the role of relevant identification standards in the administration of justice. Through the literature review and case analysis, we arrived at the following key findings:

Destructive programs play a crucial role in computer system crimes. Criminals use a variety of destructive programs to carry out malicious acts such as data theft and network attacks, which bring great losses to society and individuals.

Secondly, there are certain deficiencies and loopholes in the existing criteria for the determination of disruptive procedures. Some of the determination criteria are vague and ambiguous, leading to disputes over the determination of disruptive procedures and affecting the fairness and accuracy of judicial decisions.

Finally, because of the shortcomings of the criteria for recognizing destructive procedures, we have put forward some suggestions for improvement and refinement. By strengthening the formulation and revision of relevant laws and regulations, enhancing the professionalism of judicial personnel and expert appraisers, and strengthening international cooperation and exchanges, the criteria for the determination of destructive procedures can be further improved to safeguard information security and the rule of law in society.

In summary, this study has conducted an in-depth discussion on the identification of destructive programs in computer system crimes, studied the role of relevant identification standards in justice, and provided useful references and suggestions for improving the identification standards of destructive programs.

7.2 The Limitations of Research

In this study, although we have explored in depth the issue of criteria for determining disruptive procedures and examined the role of relevant identification criteria in the administration of justice, there are still some limitations that need to be noted and improved.[9]

First, due to the covert and mutable nature of the use of destructive programs in computer system crimes, the exact definition and categorization of destructive programs remain controversial. In actual judicial application, there may be differences in the criteria for recognizing destructive programs between competent authorities and expert opinions, leading to uncertainty in the outcome of judgments.[10]

Secondly, although we have mentioned in the text the importance of expert appraisal in the determination of destructive procedures, there may also be limitations in

the methods and standards of expert appraisal in practice. Experts' opinions may be influenced by subjective factors, and the professionalism and accuracy of expert appraisals need to be further improved.

In addition, the case analysis and discussion in the current state of relevant research at home and abroad may not be able to fully cover all types of disruptive program use, resulting in an in-depth understanding of the issue of the identification of disruptive programs still having certain limitations. In future research, it is necessary to further expand the scope of research to fully understand the application of disruptive procedures in different fields and contexts.[11]

In summary, this study has some limitations in exploring the issue of the identification criteria of destructive procedures, which needs to draw the attention of researchers and judicial departments to improve further and refine the content and methods of the relevant research to enhance the accuracy and effectiveness of the identification of destructive procedures.[12]

7.3 Recommendations for Further Research

In further studying the issue of criteria for determining disruptive procedures, it is suggested that in-depth discussions be carried out in the following areas:[13]

First, the existing classification of disruptive procedures can be divided into greater detail and accuracy to better understand the characteristics and modes of conduct of different types of disruptive procedures. This will help to identify more accurately the types and characteristics of disruptive procedures in actual cases and improve the efficiency and accuracy of judicial handling.[14]

Secondly, the development and dissemination mechanisms of destructive programs can be further explored, and the motives of the creators of destructive programs and the logic behind their actions can be analyzed. Through an in-depth study of the process of the creation and dissemination of destructive programs, such criminal acts can be better prevented and combated to protect the security of computer systems.[15]

In addition, in-depth analyses can be conducted in conjunction with actual cases to explore the application and impact of destructive procedures in different types of crimes. Through case studies, the harmful and destructive nature of destructive procedures can be demonstrated more intuitively, providing judicial practice with research results that provide more practical guidance.

Finally, relevant studies at home and abroad can be comprehensively compared and summarized, drawing on the experience and practice of other countries on the issue of destructive procedural recognition standards, to provide a broader vision and ideas for China's research in related fields. This can promote the improvement and development of China's destructive program recognition standards and promote academic research and judicial practice in related fields to achieve more significant results.

References

1. YU Jie. On the Investigation Model of Duty Crime [D]. Southwest University of Political Science and Law, 2014.
2. ZHOU Min, SHAO Hai. Judicial Identification and Judicial Adjudication of Medical Injury: Departure from Dilemma and Fit Concept [J]. Journal of the Gansu University of Political Science and Law, 2015.
3. SUN Daocui. New Discussion on the Standard and Model of Crime Stratification [J]. Rule of Law Research, 2013.
4. HUANG Haihua. A Practical Study on the Operation Mode of Compulsory Isolation Drug Treatment in the Z Province of East China [D]. Nanchang University, 2016.
5. AN Duo. Identification Disputes in Civil Justice and its Resolution Mechanism [D]. Southwest University of Political Science and Law, 2017.
6. QU Hong. Investigation on the Causes and Countermeasures of Misjudged Criminal Cases Caused by False Identification Conclusions [J]. Journal of Qinghai Normal University (Philosophy and Social Sciences Edition), 2012.
7. HUANG Weihong. Research on the Construction Plan of the Traffic Emergency Support System in Chongqing [D]. Chongqing Jiaotong University,2016.
8. LOU Miaomiao. Prevention of Juvenile Crimes to Ensure Public Security [D]. East China University of Political Science and Law, 2015.
9. LI Zongjing. Research on the Mechanism of Judicial Expertise of Public Security Organs in China [D]. Yunnan University, 2017.
10. WANG Zhenke. Research on the Criminal Responsibility of Passion Crime [D]. Southwest University of Political Science and Law, 2015.
11. ZHANG Jin. Research on Cloud Storage Forensics Strategy and Evidence Ability under Electronic Monitoring [D]. East China University of Political Science and Law, 2015.
12. WANG Mei, CAO Xuefei. Definition of Research Objects and Analysis of Influencing Factors of Juvenile Delinquency in Western Countries [J]. Journal of Jiangsu Police College, 2014.
13. WANG Zhihua. Research on Second Victimization of Crime Victims [D]. China University of Political Science and Law, 2014.
14. YUAN Guanglin. Research on Professional Quality Training of Chinese Police [D]. East China Normal University, 2014.
15. ZHANG Chenyi. Research on Combating Food and Drug Crimes by Dalian Public Security Organs [D]. Dalian Maritime University, 2016.