Advances in Economics, Business and Management Research, volume 138
2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020)

Specifics of Crime in Digital Space

Kirilenko V.S.* Zhmurko R.D.

Institute of Service Sector and Entrepreneurship of the Don State Technical University in Shakhty
Corresponding author: e-mail:Shpigunova96@mail.ru

ABSTRACT
This paper discusses all measures to combat digital crime, which may be divided into technical, organizational, and legal ones. Technical measures include the protection against unauthorized access to a computer system, backing up important computer systems, taking structural measures to protect against theft and sabotage, providing backup power, developing and implementing special software and hardware security systems, and much more. Organizational measures include the protection of computer systems, the selection of personnel, the elimination of cases of especially important work being done by only one person, the availability of a plan for restoring the center's performance after failure, the organization of service of the computer center by a third-party organization or persons uninterested in hiding the facts of the center's disruptions, the flexibility of means of protection against all users (including top management), imposing responsibility on persons who should ensure the safety of the center, the choice of the location of the center, etc. Legal measures should include the development of standards establishing responsibility for computer crimes, the protection of copyrights of programmers, the improvement of criminal and civil law, as well as legal proceedings. Legal measures should also include issues of public control over the developers of computer systems and the adoption of relevant international measures.
Keywords: *criminal responsibility, digital crimes, law, technology, information, legislation, systems*

1. INTRODUCTION

The development of a modern society based on the use of a huge amount of the most diverse information is unthinkable without the widespread introduction of electronic computers in all spheres of life of society. Computers serve not only for the storage and processing of relevant information at the level of individual managerial or business units or for the use as a means of communication between citizens but also for broad implementation to ensure internal and external security of the state. However, the unfolding of the scientific and technological revolution determines not only radical progressive changes in the composition of factors of economic development of Russia but also negative trends in the development of the criminal world, which lead to the emergence of new forms and types of criminal attacks. This is clearly manifested in the fact that criminal groups and communities are actively using the latest achievements of science and technology in their activities.

2. METHODOLOGICAL RESEARCH

In this regard, the fact of the emergence and development in Russia of a new type of criminal attacks, which have been previously unknown to domestic legal science and practice and which are associated with the use of computer technology and information processing technologies, i.e. computer crimes, is of particular concern. These crimes made the Russian legislator take urgent adequate legal measures to counter this new type of crime. The first steps in this direction were the adoption of the Law of the Russian Federation "On the Legal Protection of Computer Software and Databases" dated 09/23/1992 [3]; Federal Law "On Information, Informatization, and Information Protection" dated 02/20/1995 [4]. The next step is the inclusion of special Chapter 28 "Crimes in the Field of Computer Information" in the new Criminal Code of 1996. The crimes contained in this chapter are actions, the essence of which is by no means the use of the very electronic computing technology as a means to commit crimes. This chapter includes socially dangerous actions encroaching on the security of information and computer processing information systems. The object of computer crime is quite complicated. There are certain value relationships in society regarding the use of automated data processing systems. The content of these relations is the rights and interests of individuals, society, and the state in relation to computer systems, which are understood as values subject to legal protection. Computer crimes encroach on these rights and interests, which are a specific (group) object of crimes in the field of computer information. Thus, the specific object of crime in the field

of computer information is public relations that violate the formation and use of automated information resources and means of their support. The specific object is complicated. It includes, in turn, other objects aimed at the rights and legitimate interests of a) holders (owners) and users of information, computers, their systems and networks, means of support; b) individuals and legal entities, information about which is available in automated information resources; and c) society and the state, including the interests of national security [1]. The generic object is public safety. The subject of computer crimes is an automated data processing system that includes both a bodily element (computers and network equipment) and a non-bodily element (software and other information).

The objective side of computer crime is characterized by both action and inaction. Action (inaction) is associated with a violation of rights and interests regarding the use of computer systems and networks and, in addition, is committed to the detriment of other, more specific private, public, or state values (personal rights and privacy, property rights and interests, public and state security, and constitutional order). Computer crimes have material components. Action (inaction) should cause significant harm to the rights and interests of the person, society, or state (an exception is a crime with a formal component provided for in Part 1 of Article 273 of the Criminal Code of the Russian Federation [2]: creation, use, and distribution of malware for computers). Criminal consequences are specified in the law in relation to specific types of computer crimes. A causal relationship should be established between the action and the consequence. The subjective side of computer crimes is characterized by intentional guilt, in accordance with the letter of the law. Part 2 of Article 24 of the Criminal Code of the Russian Federation indicates that an action committed by negligence is recognized as a crime only if it is expressly provided for in the relevant article of the Special Part of the Criminal Code. The careless form of guilt is specified in the Special Part only in relation to the qualified types of computer crimes provided for in Part 2 of Article 273 of the Criminal Code and Part 2 of Article 274 of the Criminal Code. These crimes have two forms of guilt and they are also intentional in general, according to Article 27 of the Criminal Code of the Russian Federation. The subject of computer crime is general, a person who has reached the age of 16. Article 274 of the Criminal Code and Part 2 of Article 272 of the Criminal Code of the Russian Federation formulates the characteristics of a special subject: a person who has access to a computer, a computer system, or their network. Computer information is understood to mean details about persons, objects, facts, events, phenomena, and processes recorded in electronic form and stored on a machine medium or electronic computer, regardless of the form, in which they are presented. Crime in the field of computer information (computer crime) is a guilty violation of the rights and interests of others with respect to automated data processing systems provided for in criminal law. Which are committed to the detriment of the rights and interests of individuals and legal entities, society and the state subject to legal protection (personal rights and privacy, property rights and interests, public and state security, and the constitutional order).

3. RESEARCH RESULTS

Today, the rules governing the legal aspects of the operation of electronic computers are provided for in various branches of law. According to experts from law enforcement agencies, the banking sector is the trickiest sector of the Russian economy for criminals. An analysis of recent criminal acts using computer technology, as well as repeated surveys of representatives of banking institutions, distinguish the following most common ways of committing computer crimes against banks and other financial institutions. First, computer crimes committed by unauthorized access to banking databases through telecommunication networks are becoming more common. Second, in recent years, almost no computer crime has been recorded that would have been committed by a single person. Moreover, there are cases when organized criminal gangs hired teams of dozens of hackers who were provided with a separate secure room equipped with the latest computer technology so that they embezzled large sums of money by illegally penetrating computer networks of large commercial banks. Third, the majority of computer crimes in the banking sector are committed with the direct participation of the employees of commercial banks being attacked. Fourth, an increasing number of computer crimes are being committed in Russia using the opportunities offered to its users by the global computer network, the Internet. Thus, the problems of responsibility for crimes in the field of computer information are generated by scientific and technological progress, which created the base for the emergence of relations in the field of use of electronic computer technology. It should be noted that "In the modern world, information has long become of a commercial nature and serves as a special facility of contractual relations related to its collection, storage, retrieval, processing, distribution, and use in various fields of human activity" [5]. There are quite a few criteria for classifying information. In 1991, the following classification of commercial information was proposed, which can be “conditionally divided into two enlarged blocks: scientific and technical, technological information, business information. Each of the blocks has its own varieties.

Scientific and technical, technological information includes information on the design of machinery and equipment (including diagrams and drawings of individual units or products), materials used, their compositions (chemical, etc.), production methods and techniques, design and other information about newly developed or manufactured products, technologies, ways and directions of modernization of known technologies, processes and equipment; software for computers, etc. Business information includes information about the financial side

of the enterprise (financial statements, status of settlements with customers, debt, loans, or solvency), profit margin, cost of production, etc., strategic and tactical plans for the development of production, including with the use of new technologies, inventions, know-how, etc., plans and volumes of sales of products (marketing plans, data on the nature and volume of trade operations, levels of limit prices, availability of goods in warehouses, etc.), analysis of the competitiveness of the products, the effectiveness of exports and imports, estimated time-to-market, plans for promotional activities, list of shopping and other customer, agents, intermediaries, competitors; information about the relationship with them, their financial standings, operations and volumes, conditions of existing contracts, etc.)" [6]. A large number of diverse threats to the security of information of various origins are known. The types of dangers generated, the degree of malicious intent, sources of threats, etc. may serve as criteria for dividing multiple threats into classes. All the variety of existing classifications can be reduced to a certain system classification. An important role is played by the information security policy. Information Security Policy (ISP) is a set of laws, rules, practical recommendations, and practical experiences that determine management and design decisions in the field of information protection. Based on the ISP, the management, protection, and distribution of critical information are built in the system. It should cover all the features of the information processing procedure, determining the behavior of the IS in various situations. For a specific information system, the security policy should be individual. It depends on information processing technology, software and hardware used, organization structure, etc. When developing and implementing a security policy, it is advisable to observe the following principles: 1) the inability to bypass protective equipment (all information flows to and from the protected network should pass through an information protection system (IPS). There should be no "secret" modem inputs or test lines bypassing the screen);
2) the reinforcement of the weakest link (the reliability of any IPS is determined by the weakest link. Often, such a link is not a computer or program, but a person, and then the problem of ensuring information security goes beyond technical aspect); 3) the inadmissibility of the transition to the open state (under any circumstances (including emergencies), the IPS either fully performs its functions or should completely block access); 4) the minimization of privileges (prescribes to grant users and administrators only that access that they need to perform official duties); 5) the separation of duties implies a distribution of roles and responsibilities, in which one person cannot violate the process that is critical to the entire organization. This is of particular importance to prevent malicious or unskilled actions by the system administrator; 6) the multi-level protection (prescribes not to rely on one protective line, no matter how reliable it may seem. Physical protection should be followed by software and hardware means, identification and authentication should be followed by access control and, as the last line, by logging and auditing. The layered defense is capable of at least delaying the attacker, and the presence of such a boundary as logging and auditing makes it difficult to perform malicious actions imperceptibly); 7) the variety of protective means (recommends organizing defensive lines of various nature so that a potential attacker would be required to master various and, if possible, incompatible skills to overcome the IPS); 8) the principle of simplicity and controllability of the information system in general and the IPS in particular determines the possibility of formal or informal proof of the correct implementation of protection mechanisms. Only a simple and controllable system allows verifying the consistency of the configuration of different components and performing centralized administration; and 9) ensuring ultimate support for security measures (non-technical in nature. It is recommended to provide a set of measures aimed at ensuring staff loyalty, continuous training, including theoretical and, what is most important, practical training, from the very outset).

4. DISCUSSING THE RESULTS

The base of security policy is an access control method that determines the procedure of access for system subjects to system objects. The name of this method, as a rule, defines the name of the security policy. Currently, two types of security policies are best studied, discretionary and mandatory (credential), based on discretionary and mandatory access control methods, respectively. The discretionary access control is a method of controlling the access of system subjects to objects based on the identification and recognition of a user, process, or group, to which it is attributed. The mandatory access control is the concept of access of subjects to information resources by the heading of secrecy of information permitted to use, as defined by the secrecy label. Moreover, there is a set of requirements that enhance the effect of these policies and that are designed to control information flows in the system. It should be noted that security measures designed to implement any of the above access control methods only provide capabilities for reliable control of access or information flows. Determining the access rights of subjects to objects or information flows (powers of subjects and attributes of objects, assigning criticality labels, etc.) is the responsibility of the system administration [7]. Illegal access to computer information is the most common type of crime in the field of computer information. Moreover, it is a rather dangerous crime, which is becoming increasingly threatening. In connection with universal computerization and the Internet, information has become available to almost all users of personal computers. This type of crime affects the interests of the entire international community, causes harm to both states and peoples, and to specific persons [10]. Therefore, it is not by chance that this article opens Chapter 28 of the Criminal Code. The peculiarity of this article is that it envisages responsibility for unauthorized access to information only if it is captured on a computer carrier, in

an electronic computer, in a computer system, or in their network. It follows from this that the encroachment on information that is designed to generate computer information but has not yet been transferred to computer storage is not a crime. A criminal action entailing responsibility can be expressed in penetration into a computer system by using special hardware or software tools to overcome established protection systems; illegal use of valid passwords or disguise as a legitimate user to penetrate a computer, steal information media, provided that measures were taken to protect them if such the action entailed the destruction or blocking of information; and using someone else's name (password). The content of the actions taken is in obtaining and implementing the ability to dispose of information at one's discretion without the relevant rights. The social danger of creating, using, or distributing malware is determined by the fact that malware may paralyze the operation of a computer system at the most unexpected moment, which may lead to adverse consequences [9]. The object of this crime is the safety of using intellectual and physical means of computer technology, as well as the correct operation of electronic computers. The objective side of this crime is expressed in the unlawful creation, use, and distribution of computer malware or the introduction of malicious changes to existing software (creation of computer viruses). Computer systems are now increasingly affecting our lives and the failure of computers, computer systems, or their network may lead to disastrous consequences. Therefore, the establishment of certain rules for operating a computer, a computer system, or their network is aimed at preserving information and computer equipment, ensuring the possibility of their long-term use in the interests of owners and users. Information, in respect of which adverse consequences occur, should be protected by law, as was previously mentioned [8].

The time we live in is characterized by the extreme intensity of the development of all forms of social activity, including political life and entrepreneurship. Some politicians quickly succeed others, some businessmen instantly earn a fortune, others go broke. The pages of the periodical press are full of reports of fraud, major unlawful schemes, abuse of power, extortion, theft, contract killings of entrepreneurs, etc. All these unpleasant pieces of modern life have one thing in common, each crime is based on confidential information obtained in one way or another, without possession of which it is sometimes impossible to commit a crime or to escape punishment. The criminal law made the first attempt to implement the criminal law policy in a new area for it, in the field of computer legal relations. How successful it is, to what extent effectively it may protect the rights of counterparts, all this depends on many factors of a political, economic, scientific, technical, and organizational nature.

I would like to emphasize that no hardware, software, or any other solutions may guarantee absolute reliability and security in computer networks. Although people today are concerned about the issue of computer security, there are many holes in the protective armor of any system. System administrators may infinitely strengthen protection but there is still a way to bypass it. There is a so-called hacking rule: something that one person has thought of will come up with another; what one has hidden, the other will reveal. But at the same time, it is possible to reduce the risk of losses with an integrated approach to security issues

5. CONCLUSIONS

In conclusion, I would like to say that today, the criminal law in the field of computer information is far from ideal. The foreseeable components of computer crimes do not fully cover all types of computer attacks that are being committed to date. All the foregoing allow concluding that the complexity of computer technology, the ambiguity of qualifications, as well as the difficulty of collecting evidence, lead to the fact that most computer crimes go unpunished. Currently, the Criminal Code of the Russian Federation provides for only three components of crime in the field of computer information, i.e. unlawful access to computer information; creation, use, and distribution of computer malware; and violation of the rules for operating a computer, a computer system, or their network, which naturally does not cover all types of crimes in this field. In this regard, it is thought that taking into account the latest technologies and the opinions of specialists in the field of computer technology, it would be advisable to expand the components of crimes at the legislative level, which provide for responsibility for other types of socially dangerous actions in the field of computer security.

REFERENCES

[1] Konstituciya RF ot 12.12.1993 (s uchetom popravok ot 30.12.2008 №6-FKZ, 7–FKZ) // SZ RF. – 2009. – №4. – St.445

[2] Ugolovnyj kodeks Rossijskoj Federacii : [prinyat Gos. Dumoj 24 maya 1996 g. :odobr. Sovetom Federacii 5 iyunya 1996 g., s izmeneniyami i dopolneniyami po sostoyaniyu na 30 marta 2016 g.] // Sobranie zakonodatel'stva RF. – 1996. – № 25. – St. 2954

[3] Federal'nyj Zakon RF «O pravovoj ohrane programm dlya EVM i baz dannyh» ot 23.09.1992g. (v red. ot 02.11.2004 g.)

[4] Federal'nyj zakon «Ob informacii, informatizacii i zashchite informacii» ot 20.02.1995g.

[5] Suhova S.V. Sistema bezopasnosti NetWare / S.V.Suhova –M.: Seti, 1995.- 60-70s.

[6] Belyaev V. Bezopasnost' v raspredelitel'nyh sistemah / V. Belyaev – M.: Mysl', 2015. – 36-40s.

[7] Vedeev D. Zashchita dannyh v komp'yuternyh setyah / D.Vedeev – M.:Prosvyashchenie, 2016 – 12–18s.

[8] Komp'yuternye seti i sredstva zashchity informacii: Uchebnoe posobie/ Kamalyan A.K., Kulev S.A., Nazarenko K.N., Lomakin S.V., Kusmagambetov S.M.; Pod red. d.e.n., professora A.K. Kamalyana. – Voronezh: VGAU, 2014.

[9] Leont'ev V. P. Novejshaya enciklopediya personal'nogo komp'yutera 2017. – M.: OLMA–PRESS Obrazovanie, 2017.

[10] CHernyakov M.V., Petrushin A.S. Osnovy informacionnyh tekhnologij. Uchebnik dlya vuzov: – M.: IKC «Akademkniga», 2016.