ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 7, Issue 9 , September 2020

Legal Bases of Information Security in Electronic Commerce

Nazarova Gulchexra Nurmuxanbetovna, Akhmadbekov Khokimbek Khasan ugli

Tashkent University of Information Technologies named after Muhammad al-Khwarizmi,
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

ABSTRACT: The article scientifically analyzes the general characteristics of electronic commerce, computer criminals, the concept of computer crime, classifies the factors that cause computer crime in electronic commerce, and also develops recommendations for improving e-commerce transactions in all forms of online fraud. The author scientifically substantiated his views in order to resolve various contradictions on these issues.

KEY WORDS: E-commerce, electronic document, information and communication technologies, electronic payment, internet, virtual bank, internet banking.

I.INTRODUCTION

Electronic commerce is an integral part of the economy of our century, ensuring the exchange of economic information between business entities on the basis of modern information technologies. Its development is transforming the modern economy into a virtual economy, as a result of which the efficiency of business communications is increasing. Experts around the world predict that the role of e-commerce in the economy will continue to grow and become an important sector in the future.

The introduction of information and communication technologies in business has created a particular revolution in the direct relations of enterprises with consumers. Practical measures are being taken in Uzbekistan to ensure the widespread use of information and communication technologies and the rapid pursuit of an “informational society”.

The state policy of the Republic of Uzbekistan in the field of informatization is aimed at creating a national information system, taking into account the modern world principles of development and improvement of information resources, information technologies and information systems [1].

In recent years, Uzbekistan has taken certain measures to develop computerization and information and communication technologies. In the field of informatization and telecommunications, a normative legal framework has been created, which defines the important economic, legal and organizational bases of information and communication technologies.

In particular, the Oliy Majlis of the Republic of Uzbekistan has adopted a number of laws on the development and introduction of modern information technologies. In particular, a comprehensively improved regulatory framework has been created for the effective regulation of economic and financial relations between its participants in the field of e-commerce. These include the Law on Informatization (11.12.2003), the Law on Electronic Document circulation (29.04.2004), the Law on Electronic Payments (16.12.2005) and the Law on Electronic Commerce (22.05.2015), The Law “On electronic digital signature” (20.08.2015), the Law “On e-government” (9.12.2015) and other normative documents.

The first edition of the Law of the Republic of Uzbekistan “On electronic commerce” was adopted on April 29, 2004. On May 22, 2015, amendments and additions were made to the previous Law on Electronic Commerce, and a new version consisting of twenty articles was adopted [2].

In order to implement this Law and further develop e-commerce with the widespread use of modern information and communication technologies, on September 8, 2015, the Cabinet of Ministers signed Decree No. 258.

II. OBJECTS AND METHODS OF RESEARCH

In this Decree, in particular, the Ministry of Economy of the Republic of Uzbekistan is assigned as a specially authorized state body in the field of e-commerce. It also instructed that the Ministry of Foreign Economic Relations,

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 9 , September 2020

Investments and Trade, the Central Bank, the Ministry of Information Technologies and Communications and other relevant ministries and departments to develop a concept for further development of e-commerce in the Republic of Uzbekistan and submit it to the Cabinet of Ministers. .

The measures taken to introduce modern information and communication technologies have allowed to achieve certain results in the digitization of sectors of the economy, including the development of e-commerce.

Nevertheless, a number of problems and shortcomings remain in the country, which hinder the creation of a full market for e-commerce and the access of local enterprises producing goods (services) to foreign markets. In particular:

First, the current system of legal regulation of relations in the field of e-commerce is not compatible with the rapid changes in the development of the industry and, in turn, does not provide access to e-commerce for the general population and businesses;

secondly, outdated bureaucratic barriers to the export of goods (services) through e-commerce still remains, which do not allow local businesses to fully compete in foreign markets, as well as cost optimization, remain;

thirdly, the process of introduction of modern information and communication technologies aimed at the development of e-commerce is not properly organized, which leads to the stagnation of the digitalization of the economy and the development of entrepreneurial activity;

fourth, the lack of integration of domestic payment systems with popular foreign analogues affects the full international cooperation of the country's business entities with leading foreign organizations in the field of e-commerce, as well as the export potential and competitiveness of the domestic market;

fifth, the level of popularization of e-commerce opportunities and benefits, including cashless payments for goods (services), especially on the ground, remains low, which leads to an increase in the size of the shadow economy and a decrease in tax revenues to the state budget;

Sixth, the current taxation system does not encourage the expansion of business entities in the field of e-commerce, including media, which leads to an increase in clandestine exchange of products via the Internet, as well as limits investment and modern technology in this area [3].

Today, special attention is paid to the development of e-commerce in our country. In particular, the Presidential Decree - 5953 of March 2, 2020 on the state program for the implementation of the Strategy of Actions in the five priority areas of development of the Republic of Uzbekistan for 2017-2021 in the “Year of development of Science, Enlightenment and Digital Economy” with the participation of foreign experts analysis of incidence factors and approval of the program to combat it; control over the timely and complete implementation of the project “digital marking and online cash register”;

development of mechanisms to reduce the illegal activities of individual entrepreneurs;

Particular attention is paid to improving the procedure for identifying entities in the field of e-commerce, the development of a taxation mechanism, taking into account the calculation and payment of value added tax.

Ensuring the safe conduct of secure e-commerce with the help of new information technologies and global information networks is one of the most important issues in the world today. In industrialized countries, the total turnover of the new information technology market and e-commerce market is gradually reaching 2 trillion dollars. The losses from various offenses (fraud, theft, blocking of sites, etc.) at a time approaching tens of billions of dollars.

Today, the development of e-commerce is influenced by a number of factors. In particular, the problem of combating computer crime requires that the world`s leading countries, or in other words, the “eight” countries, work together.

In a speech to the G8 summit in Denver (1997), the heads of state stressed the need to step up efforts in two directions:

1. Investigation and high-tech crimes with the use of computer and telecommunications technologies on a cross-border basis.
2. Provide the state structure with technical and legal opportunities to combat “high-tech” crimes, regardless of their location.

In the speeches of the G8 ministers, strategic directions in the fight against high-tech crime were identified:

- Improvement of the legal system;
- Development of cross-border principles of access to stored computer data; Improving mechanisms for identification and identifying opportunities in the field of high technology;
- Establishment of a network of call centers;
- Development of partnerships with high-tech entrepreneurs.

In particular, the risk of fraud on the Internet was highlighted. Accordingly, internet fraud poses a significant risk to their credibility in e-commerce transactions in all its forms. The G8 states stressed the importance of exchanging

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 9 , September 2020

information on the scheme of processes used by criminals, the methods and techniques used, the actions taken by victims of crime and law enforcement agencies.

General descriptions of computer criminals. The practice of law enforcement shows that the complexity of the collection of evidence among the facts of a crime committed in the field of e-commerce is characterized by the difficulty of proving and bringing such a case to court.

In recent years, sufficient attention has been paid to the problem of crime in e-commerce. However, the main part of this is devoted to the study of legal and criminological aspects of computer crime, and despite the availability of a sufficient amount of scientific work, the problem of crime prevention in the field of e-commerce has not been sufficiently studied. At the same time, one of the most important issues is the prevention of crime in this group of managers, the development of scientifically based and tested in practice.

There are currently different perspectives on the concept of computer crime. From the point of view of many experts, it is a relatively well-founded and shared concept, which is an illegal act in the field of automated information processing. The legislation of most countries, as well as the legislation of the CIS countries, began to develop within the framework of this approach.

III. RESULTS OF THE INVESTIGATIONS AND DISCUSSION

The following forms of computer crime structure have been proposed during this period.

- Using or attempting to use a computer system or computer network for the purpose of obtaining money, private property, or services under the guise of false offers and promises or by posing as another person;
- Intentional actions committed to modify, damage, destroy, or steal a computer, computer system, computer networks, or mathematical software systems, programs, or information within them.
- Intentional disruption of communication between computers, calculation or computer systems.

In order to unify the national legislation, the EU participation was approved in 1989 by the Cabinet of Ministers of the European Union - a list of infringers of the rights proposed to the countries - to bring together the desired strategy for the production of legislation related to computer crime in e-commerce. This list of computer crimes includes the least and unconditional offenses.

The e-commerce information security system should take into account the minimum list (first of all) and the unconditional list (if possible) in the conduct and implementation of international e-business in accordance with international requirements.

Based on the analysis of specific computer criminals, the simplest actions that can cause great damage to e-commerce can be distinguished:

- forgery of accounts and payment slips;
- forgery of payment documents;
- looting of cash and non-cash funds;
- Receipt of payments;
- transfer of funds to fake accounts;
- Shopping with a fraudulent payment (for example, with a counterfeit or stolen credit card);
- illegal currency transactions;
- obtaining illegal loans;
- Illegal management of real estate;
- Illegal receipt of benefits, services and goods;
- sale of confidential information.

According to available estimates, 52% of computer crimes committed are money laundering, 16% are hacking and destruction of computer equipment, 12% are exchange of original data, and 10% are theft of software and information.

- The informational features of the business entity have a significant impact on the circumstances of the crime. The following indicators play a clear role in this.

The number of computers in the business entity and their types;
Topology of computer systems;

- Whether it is possible to document access to information;
- Availability of access to the global network;
- Type of telecommunication equipment used;

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 9 , September 2020

- The type of software used in email;
- Use or non-use of software or hardware security of information and methods of its implementation;
- The type of external, optical and other media used.

In general, the perpetrators of computer crimes can be divided into “external” and “internal” computer intruders.

E-commerce practice shows that in most cases the biggest risk is computer hackers in the “external type”. Based on the current experience of the media, they are called hackers. However, now it is important to form a specific subculture of hackers in order to fight hackers more successfully.

In order to combat crime and ensure the information security of e-commerce, it is necessary for business leaders to classify hackers according to their interests and areas of specialization.The concept of a class hacker includes the following levels: private hackers, freebies, information brokers, and metahackers.

We`ll consider the particularities of the highlighted levels. Private hackers mainly specialize in computer and computer hacking, and they can be divided into classic hackers, crackers, system crackers, and hacker-carders.

Classic hackers are professionals who have an unconventional, original approach to the problem, who are fully aware of the software and hardware, who have a high level of thinking and achieve results. For them, the main reason for the activity is not money, but the feeling of overcoming technical obstacles and realizing that he is capable of everything. They are wary of public administration, because they believe that every action of law enforcement agencies will lead to the destruction of the self-governing world of the Internet. Classic hackers access computers and software in order to demonstrate their professional capabilities without damaging anyone, and feel spiritually satisfied with this.

The main idea of the classic hacker movement is: “Information should be free and accessible to all”. Of course, not everyone agrees with this slogan, and especially members of the e-commerce world and their information WEB resources have been surrounded by the most classic hackers. Classic hackers study the process of computers and programs with great interest, so they often enter prohibited areas and electronic storage areas of information.

Crackers, as a rule, carry out hacking of programs for information retrieval, damage and other purposes, the implementation of code generation, hacking of software-level software security tools.

System cyber crackers specialize in breaking into local and global computer systems. The main manifestations of cyber cracker crime are unauthorized access to computer systems and networks, modification and destruction of data. While the signature and source of cyber crackers change from one attack to another, their mode of action is largely based on exploiting the weaknesses of systems and networks (choice of protections and passwords, illegal registration, etc.).

Hackers perform illegal transactions involving credit cards, generation of non-existent credit numbers, approximation and theft of real credit numbers. Their motto is: “Let others pay for me”.

Analogs of credit card numbers are placed in the exact schemes of banks, which are based on pirated software-credit generators. The entire collection of such programs can now be found on the internet or on pirate CDs that are readily available.

The analysis of the differences between hackers and crackers is of interest in the context of the set of issues we are considering related to information security in e-commerce. The difference between them is that while hackers are computer security researchers and analysts, crackers are ordinary thieves. As proof, a hacker can be described from Guy L. Steele`s dictionary: Unlike most computer users who just want to know the minimum amount of information they need, computer systems are an individual who enjoys learning about the performance of parts and expanding their capabilities. It is the individual who enjoys the programming process itself, not the theory in this regard. Unlike a hacker, the main purpose of a cracker is to carry out direct hacking in order to gain unauthorized access to steal, exchange and declare the fact of tampering with third-party information. It breaks into systems and networks and steals foreign information, i.e. intellectual property. In addition to “external intruders”, information security can be compromised by “internal intruders”. They are the number of staff who support the operation of the e-commerce system. The list of personnel in this system is compiled in descending order of risk by personnel category and is given below:

Risk group	User level
The biggest risk	System administrator. Security Administrator
Big risk	System operator. Data entry and preparation operator. Data Processing Manager.
Medium risk	System programmer. System Engineer. Software Manager
Limited risk	Practical programmer. Communication Engineer or Operator. Database administrator. Instrumentation Engineer

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 7, Issue 9 , September 2020

Low risk	The multifaceted nature of this problem should be taken into account when considering the information security features of an economic entity, for example, an enterprise engaged in e-commerce.

The complexity of the timely formation of information security for e-commerce is based on the interdisciplinary and international nature of the problems of information security of computer systems and networks. The level of information security required for the construction of such a system, the technological information protection of computer systems and networks, the validity of technical means and methods used in information protection, a set of interrelated issues in the field of legislation and regulations of e-commerce security.

Today, to participate in tenders for the development of practical and customized software tools, databases, websites and other software products for the real economy, management, business, health, science and education, as well as for the implementation of e-commerce [4] are given special attention. In order to implement the relevant instructions of the "information security Doctrine" in ensuring information security in general and in e-commerce in particular, it is expedient for the executive authorities and enterprises to concentrate their efforts on:

— protection of material and technical facilities that form the physical basis of the entire electronic commerce, as well as information resources of the information technology system;
— ensuring the proper and uninterrupted operation of the database (bank) and telecommunications systems;
— protection of information from illegal access, falsification or destruction through technical channels;
— development of a system of certification of informatization, software products and information security tools;
— development of a system of information security and licensing of activities in the field of international information exchange;
— formation of local licensing centers;
— Improvements and developments on the basis of the international system of training, retraining in the field of information security.

IV. CONCLUSION

In conclusion, in recent years, Uzbekistan has taken certain measures to develop e-commerce. In particular, the regulatory framework defining the legal and organizational framework of the industry has been created, hardware and software, platforms have been formed, payments in the banking system are made in electronic form. Taking into account the above, it goes without saying that the development of e-commerce will contribute to the sustainable economic development of our country and the widespread use of its potential will lead to an increase in the welfare of the population.

REFERENCES

1. Law of the Republic of Uzbekistan "On Informatization". Tashkent, December 11, 2003, No. LRU № 563-11.
2. Law of the Republic of Uzbekistan "On electronic commerce". Tashkent, May 22, 2015, No. LRU-385.
3. Program of the President of the Republic of Uzbekistan on the implementation of the Strategy of Actions for the five priority areas of development of the Republic of Uzbekistan for 2017-2021 "The Year of development of science, enlightenment and digital economy", Tashkent, March 2, 2020, PD-5953.
4. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan on measures for further development of computerization and introduction of information and communication technologies, Tashkent, June 6, 2002.