# E-COMMERCE SECURITY: LEGAL AND POLICY ASPECTS OF TECHNOLOGY SOLUTIONS IN UZBEKISTAN

**Akhmadbekov Khokimbek Khasan ugli,**
**Rayimov Sherzod Toshtemirovich**
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

## ABSTRACT:

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.

## KEY WORDS:

Electronic document, information and communication technologies, electronic payment, internet, virtual bank.

## I.INTRODUCTION

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. 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[2].

## 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, 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.

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. [3].

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.

## III. RESULTS OF THE INVESTIGATIONS AND DISCUSSION

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 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.

## IV. CONCLUSION

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. 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.

## 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.