



CRIMINOGENIC CHARACTERISTICS OF YOUTH CYBERCRIME

Rafikova Muattar Ravshanovna

Head of the Department of Social and Humanitarian Sciences,
Customs Institute,

Doctor of Philosophy (PhD) in Pedagogical Sciences,
Associate Professor, Lieutenant Colonel

Abstract. *The article examines the criminological characteristics of cybercrime among young people and the main criminogenic factors contributing to youth involvement in cybercrime. Special attention is paid to the prevention of cybercrime and the development of digital culture and legal awareness among youth.*

Key words: *cybercrime, youth crime, criminogenic factors, information security, cybercrime, criminology.*

Annotatsiya. *Mazkur maqolada yoshlar o'rtasida kiberjinoyatchilikning kriminologik xususiyatlari, uning paydo bo'lishi va rivojlanishiga ta'sir etuvchi kriminogen omillar tahlil qilinadi. Zamonaviy axborot texnologiyalari rivojlanishi sharoitida yoshlarning internet muhitidagi faoliyati bilan bog'liq xavf-xatarlar, kiberjinoyatlar turlari hamda ularning oldini olish choralari ilmiy jihatdan o'rganiladi. Shuningdek, yoshlar o'rtasida kiberjinoyatchilikni kamaytirish uchun huquqiy, ijtimoiy va tashkiliy choralar taklif etiladi.*

Kalit so'zlar: *kiberjinoyatchilik, yoshlar jinoyatchiligi, kriminogen omillar, axborot xavfsizligi, kiberjinoyat, kriminologiya.*

Аннотация. *В статье анализируются криминологические особенности киберпреступности среди молодёжи, а также основные криминогенные факторы, способствующие вовлечению молодых людей в киберпреступную деятельность. Особое внимание уделяется вопросам профилактики киберпреступности и повышению правовой культуры молодёжи.*

Ключевые слова: *киберпреступность, преступность среди молодёжи, криминогенные факторы, информационная безопасность, криминология.*

Today, information and communication technologies have become one of the key factors in the development of society. The widespread use of the Internet, electronic services, and the growth of the digital economy have significantly simplified human life. At the same time, this process has also led to the emergence and development of new types of crimes, particularly cybercrime. In the conditions of an information society, cyberspace has become an important arena of social relations. The global nature of the Internet, along with the increasing popularity of digital services and e-commerce, has given rise to new forms of criminal activity.

Cybercrimes are crimes committed using information technologies and are considered one of the fastest-growing types of modern crime. Since young people are the main users of the Internet, the likelihood of their involvement in cybercrime-related activities is increasing¹.

Youth cybercrime, unlike traditional crime, has an intellectual nature, and its criminogenic sources are associated with a specific socio-psychological environment.

Cybercrime is a set of crimes committed through computer systems, information networks, or digital technologies². Such crimes differ from traditional crimes in the following characteristics:

- a high technological level of committing the crime;
- the anonymity of the offender;
- the absence of geographical boundaries;
- the rapid spread of criminal consequences.

In criminological studies, cybercrimes are usually divided into the following main types:

1. illegal access to computer systems (hacking);
2. fraud committed via the Internet;
3. creation and distribution of malicious software (viruses);

4. illegal acquisition of personal data;
5. crimes related to electronic payment systems.

The main characteristic of cybercrimes is that they are committed in a digital environment, and in many cases it is difficult to identify the offender.

A number of factors contribute to the emergence of cybercrime among young people. In particular, the development of cybercrime among youth is associated with several social, economic, and psychological factors. These include the following:

• **Widespread use of the Internet.**

Today, young people are the most active users of the Internet. The Internet provides broad opportunities for exchanging information, communicating, and using various services, but this environment also creates opportunities for illegal activities³.

• **High level of technical knowledge.**

Many young people possess certain knowledge in programming, computer technologies, and information systems. In some cases, this knowledge may be used for illegal purposes.

• **Insufficient social control.**

In some cases, parents or educational institutions do not sufficiently monitor the online activities of young people. This may create conditions that facilitate the commission of cybercrimes.

• **Material interest.**

The desire to earn quick and easy money through the Internet may encourage some young people to engage in fraud or other illegal activities.

• **Anonymity of the virtual environment.**

Because it is difficult to identify the person who commits a cybercrime, some young people feel less responsible for their actions.

In practice, there are various types of cybercrimes committed by young people. Most commonly, young people are involved in the following types of cybercrimes:

- fraud through social networks;

- obtaining bank card information;
- phishing attacks;
- distribution of malicious software;
- fraud through online games.

In many cases, such crimes are committed out of curiosity, experimentation, or financial gain.

A young cybercriminal often has a high level of digital literacy, is active on social networks, and is interested in technology. Unlike a traditional criminal, such an individual seeks to achieve superiority not through physical aggression but through intellectual ability.

Motivation is manifested in the following directions:

- financial gain;
- demonstrating one's abilities;
- group influence;
- ideological reasons;
- personal conflict.

The latent nature of cyberspace leads offenders to feel safe, which increases the risk of recidivism.

To prevent cybercrime among young people, the following measures are of great importance:

1. increasing legal awareness among youth;
2. expanding knowledge of cybersecurity within the education system;
3. promoting the rules of safe Internet use;
4. conducting preventive activities by law enforcement agencies;
5. strengthening parental control over children's Internet activities;
6. early identification of young people prone to deviant behavior and working with them individually from a psychological perspective.

In addition, improving state policy in the field of information security also plays an important role in combating cybercrime. From a legal perspective, the implementation of international standards into national legislation is of significant importance.

In conclusion, cybercrime is one of the pressing problems of modern society. Along with the development of information technologies, the number of such crimes is also increasing. Since young people are the primary users of the Internet, they are more frequently exposed to risks related to cybercrime.

Youth cybercrime is a complex social phenomenon of the information society, and its criminogenic characteristics are determined by a combination of social, psychological, and technical factors. Effective prevention requires not only punitive measures but also a systematic policy that includes education, moral upbringing, digital culture, and international cooperation.

In general, the criminogenic characteristics of youth cybercrime show that it is formed through the interaction of social, psychological, and technical factors. Addressing this problem requires not only punitive measures but also a comprehensive preventive policy, the development of legal awareness, the formation of digital culture among youth, and directing the intellectual potential of young people toward positive activities. Only in this way can stable information security be ensured in the conditions of a digital society.

References:

1. Zaripov Z.S. *Criminology*. – Tashkent: Tashkent State University of Law, 2021. – p. 214.
2. David Wall *Cybercrime: The Transformation of Crime in the Information Age*. – Cambridge: Polity Press, 2017. – p. 35.
3. Majid Yar, Kevin F. Steinmetz *Cybercrime and Society*. – London: SAGE Publications, 2019. – p. 52.
4. Rustamboyev M.X. *Criminal Law*. – Tashkent, 2020. – p. 412.

5. Zaripov Z.S. *Criminology*. – Tashkent: TSUL, 2021.
6. Rustamboyev M.X. *Criminal Law*. – Tashkent: Legal Literature Publishing House, 2020.
7. David Wall *Cybercrime: The Transformation of Crime in the Information Age*. – Cambridge: Polity Press, 2017.
8. Majid Yar, Kevin F. Steinmetz *Cybercrime and Society*. – London: SAGE Publications, 2019.
9. Susan W. Brenner *Cybercrime and the Law*. – Boston: Northeastern University Press, 2018.
10. United Nations Office on Drugs and Crime *Comprehensive Study on Cybercrime*. – Vienna, 2013.