Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Crimes in the field of information technology and security: determinants and warnings

Abdulaziz RASULEV [1] **Surayyo Rakhmonova**[2]

Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
High School Judges With the supreme judicial council of the Republic of Uzbekistan

ARTICLE INFO

Article history:
Received 10 august 2020
Received in revised form 20 august 2020
Accepted 25 august 2020
Available online
August 2020

Keywords:
Information security
Information technology
Criminal law
Hackers
Cybercrime
Causes and conditions.

ABSTRACT

This article analyzes the determinants of crimes in the field of information technology and security. Based on the study of foreign experience and scientific and theoretical views, the causes and conditions of cybercrime, the identity of the criminal were investigated. Based on the results of the analysis, relevant conclusions were drawn and proposals were developed.

Ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятлар: детерминантлар ва олдини олиш

Ключевые слова:
Ахборот хавфсизлиги
Ахборот технологиялари
Жиноят қонунчилиги
Хакерлар
Кибержиноят
Сабаб ва шарт-шароитлар.

АННОТАЦИЯ

Мазкур мақола ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятлар детерминантларининг таҳлилига бағишланган. Хорижий тажриба ва илмий-назарий қарашларни ўрганиш асосида киберэжиноятларнинг сабаб ва шарт-шароитлари, жиноятчи шахси таҳлил қилинган. Таҳлил асосида тегишли хулосалар қилинган ва таклифлар ишлаб чиқилган.

[1] DSc, Professor, Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, Tashkent, Uzbekistan
Email: rasuleff@mail.ru

[2] DSc, Professor High School Judges With the supreme judicial council of the Republic of Uzbekistan, Tashkent, Uzbekistan
Email: raxmonovasurayyo@gmail.com

Преступления в сфере информационных технологий и безопасности: детерминанты и предупреждение

Ключевые слова:
Информационная безопасность
Информационные технологии
Уголовное законодательство
Хакеры
Киберпреступность, причины и условия.

АННОТАЦИЯ

Настоящая статья посвящена анализу детерминантов преступлений в сфере информационных технологий и безопасности. На основе изучения зарубежного опыта и научно-теоретических взглядов были исследованы причины и условия киберпреступлений, личность преступника. По итогам анализа были сделаны соответствующие выводы и разработаны предложения.

INTRODUCTION

Information technologies and virtualization of various spheres of society's life have become a paradigm of modern public relations. The new model of relations began to dictate its own rules in all sectors, including the criminal sphere.

Despite the increasing and changing, modernizing crime in the real world, the virtual world is also not far behind. Modern criminals are trying to conquer virtual spaces, which is why a new era of crime has emerged – the era of cybercrime. The fight against cybercrime, i.e. crimes in the field of information technology and security, is becoming more and more global. In particular, all states and the international community are taking measures to ensure information security and prevent criminal attacks using information and communication technologies. Statistics indicate that as of the first half of 2020, about seven billion people (94% of the world's population) were covered by mobile and / or telecommunications networks [1]. The amount of damage caused by cybercrime is 1.3% of the world's GDP per year [2].

In the Republic of Uzbekistan, the development of information technologies is proceeding at a rapid pace. The results of the measures taken to develop the information and communication sphere should be particularly noted. According to statistical data from the Ministry for the development of information technologies and communications, the number of Internet users in Uzbekistan has exceeded 22 million (19 million of them are mobile Internet users), and 2,017 base stations were installed for the development of mobile communication networks in 2019, which makes the number of them more than 26,000 in the Republic. At the same time, 96 percent of Uzbekistan's residents are covered by mobile communications, and 70 percent have access to a broadband mobile Internet network [3].

The Strategy of actions for five priority areas of development of the Republic of Uzbekistan in 2017-2021 provides for the issues of «improving criminal legislation, improving the system of information security and information protection, timely and adequate counteraction to threats in the information sphere» [4]. In this regard, the fight against crime that threatens the rights and freedoms of the individual, the interests of society and the state, the protection of information security as an object of criminal law protection, and the development of a set of measures to counter cybercrime are urgent tasks. The concept of improving the criminal and criminal procedure legislation of the Republic of Uzbekistan, approved by the decree of the President of the Republic of Uzbekistan from 14 May 2018 the year number PP–3723, also provides for the revision of the norms providing for liability in the field of information technologies, taking into account technological progress, including the expansion of the categories of crimes related to cybercrime [5].

If we look at these figures on a global scale, according to the website «Internet world stats», there are 4,833,521,806 Internet users in the world as of the first half of 2020, which is 62% of the World's population (the World's population is 7,796,949,710 people), more than half of them live in developing countries. The world's largest Internet audience has been held by China for five years. As of July 2020, the number of Internet users in China was 854 million. The top 10 countries by the number of Internet users, except China, included India – 560 million, the United States – 313 million, Indonesia – 171 million, Brazil – 149 million, Nigeria – 126 million, Japan – 118 million, Russia – 116 million, Bangladesh – 94 million, Mexico – 88 million [6].

This massive use of the information space and the virtualization of human relations not only in the Republic of Uzbekistan, but also around the world leads to a parallel increase in cybercrime.

This article will generalize the determinants (causes and conditions, the identity of the offender) and measures to prevent crimes in the field of information technology and security.

METHODOLOGY

In solving the tasks set in this article, general scientific and special methods of scientific knowledge were used: system, specific-sociological, comparative-legal, analytical, quantitative analysis (content analysis), logical-legal, etc.

The analysis of the norms of the legislation of the Republic of Uzbekistan and a number of foreign countries, some international acts, doctrinal works, scientific articles in the field of criminal law and criminology was used as an empirical basis.

In particular, the study used statistical data from the Ministry for the development of information technologies and communications of the Republic of Uzbekistan, authoritative Internet portals «Internet world stats», Statista, etc.

Together, all these methods made it possible to ensure the reliability and validity of the research results in a scientific article to a certain extent.

RESULTS OF THE STUDY OF DETERMINANTS

The problem of the causes of crime is one of the central problems in the science of criminology and crime prevention. The causal complex of crime includes its causes and conditions, which together constitute the factors of crime. Causes are socio-psychological determinants that directly generate and reproduce criminality and crimes as their natural consequence; conditions are social phenomena that do not themselves generate criminality and crimes, but contribute to, facilitate, and intensify the formation and action of the cause [7, p.167-168].

The analysis of criminological science in Uzbekistan, in particular, the scientific works of such domestic scientists as K.Abdurasulova [8, p. 179-181], M.Rustambayev [9, p. 98-100], R.Kabulov [10, p. 23-27] indicates the following reasons that contribute to the Commission of these types of crimes, namely:

* insufficient email protection;

* negligence in the work of ICT users;

* ill-conceived personnel policy in matters of hiring and dismissal;

* violation of the technological cycle of design, development, testing and commissioning of computer systems;

* combining the functions of software development and operation within a single structural unit;

* violation of deadlines for changing user passwords;

* violation of the established terms of storage of copies of programs and computer information, and sometimes their complete absence;

* unjustified use of ICT in specific technological processes and operations;

* lack of proper control by the administration over the activities of its employees involved in sensitive stages of processing computer information;

* psychologically incorrect interpersonal relationships between officials and subordinates and other employees.

In our opinion, the most typical reasons and conditions for committing crimes in the field of information technology and security at the present stage are:

* an increase in the number of ICTs and, as a result, an increase in the amount of information processed and stored in ICTs;

* insufficient measures to protect ICTs, ICT systems and their networks;

* insufficient software protection;

* growth of information exchange through global information networks, primarily through social networks;

* absence, imperfection or deviation from the rules of operation of ICT programs, databases and network technology hardware;

* lack or non-compliance of information security tools with modern information challenges and threats;

* violation of the rules for working with legally protected computer information;

* low level of specialized training of law enforcement officers who must prevent, solve and investigate crimes in the field of information technology and security;

* lack of a coordinated and comprehensive state policy in the field of information security.

In this paper, we will focus on two main causes of cybercrime. One of them, as mentioned above, is the growth in the number of Internet users. In sociology, there is a «15% Rule», according to which if the World's population grows by 15%, the number of crimes committed will grow by 15%. This rule also applies to cybercrime. Thus, according to Kaspersky Lab, the number of hacker DDoS attacks in the world in 2019 increased by 25% compared to 2017 and by 18% compared to 2018 [11].

According to the world's expert and analytical centers, 24 users over the age of 18 become victims of cybercrime every second, so more than 2.4 million people suffer from the actions of cybercriminals every day. The number of victims for 2019 is more than 700 million people, each of whom on average loses more than 376 dollars [12].

The issues of countering crimes in the field of information technology and security are particularly relevant in the context of the coronavirus pandemic. As a result of the spread of the coronavirus pandemic, the Internet has become the resource through which people began to receive information quickly. During the coronavirus pandemic, the flow of information increased in virtual space, resulting in an increased flow of raw and false information on the Internet. Users believe a source with a large number of subscribers, so the bulk, or rather every fifth fake news falls under existing websites that can easily be found in Google, which already indicates that potential criminals are not even masked, but have openly moved to the» virtual front «of influencing people's minds [13].

Of particular concern are the facts of activation of virtual fraudsters during the coronavirus pandemic, when fraudsters use the topic of coronavirus as a «bait» and ask to click on the link in emails allegedly sent from the Bank. These emails may contain a «trap site». So, in the Russian Federation during the pandemic, the number of domains with the word «coronavirus» increased by 4 thousand at once. In addition, the number of phishing mailings increased by 30%. The purpose of such mailings is to extract passwords, usernames, and card data by faking messages from a trusted source. Phishing pages are very similar to the original pages of the banks' website, as a result of which people become victims of criminals [14]. The pandemic has also become an occasion for the implementation of political actions by malefactors. So, in the Russian Federation – in Vladikavkaz on April 20 of this year, there was a popular gathering of several thousand citizens against the self-isolation regime, demanding the resignation of the head of the region and the dissolution of the Republican Parliament [15].

As noted in the report of the United Nations Office on drugs and crime (UNODC) on cybercrime and the COVID-19 coronavirus, «the COVID-19 pandemic is an unprecedented challenge for the entire world community. Many have switched from traditional methods of performing operations to online mode, and criminals have also arrived. While the scale and sophistication of cybercrime is growing and the number of victims is increasing, in some countries law enforcement officials are forced to perform other duties. Compounding the situation for the public and governments is the economic impact of COVID-19. Thus, there are ideal conditions for potential cybercrime» [16, p. 4]. As we can see, a significant problem is the freedom and irresponsibility of Internet users, primarily the malicious blogger. The free use of information and communication technologies and the Internet can have certain negative consequences. For example, this has a particularly negative impact on everyday users. Like any state, the Republic of Uzbekistan also intends to resolve the issue of preventing the spread of negative content. The problem of this issue is the lack of specific measures of responsibility for the misuse of the Internet. At the same time, the legislation provides for prohibitions on «using» the Internet in a negative sense in accordance with the Law of the Republic of Uzbekistan «On Informatization». In particular, the owner of the website and (or) the website page, including the blogger, is obliged to prevent the use of his website and (or) the website page on the world information network, which contains publicly available information, for the purpose of spreading negative content and committing other actions that entail criminal and other liability in accordance with the law [17]. In this regard, an important task is to establish responsibility for the misuse of the Internet by hackers.

When analyzing the determinants of cybercrime, it is essential to analyze the identity of the criminal in the field of information technology and security. The characteristics of criminals in the field of information technology and security allow us to distinguish the following types:

1. **«Novice»**. This category of person commits offenses for the first time and is characterized by the use of various information technologies (personal computer, laptop) for personal consumer purposes – to download music, games or applications. Most of them

are teenagers or young people aged 15-25 years. Gender-in the vast majority of cases male. Education – secondary, specialized or higher education.

2. **«Amateur»**. This category of personality represents individuals who periodically commit offenses in the computer network, mainly technical personnel (system administrators, technical consultants). This group includes men (less often women) aged 20-30 years. The formation of «Amateurs» comes from the skills of the past as a «novice» or in connection with life circumstances (running errands and «orders»).

3. **«Professional»**. This category of professional persons who are professionally engaged in illegal activities and are referred to as hackers. This is a class of educated people who know all the basics of computer programming and technical work. Age-25-40 years. Gender – in most cases male. D.Bukin rightly notes that high technical readiness is their main feature, high latency of crimes is the basis of their motivation, internal predisposition is the main condition for entering the criminal path, and the socio – economic situation in the country is the main reason for the final choice [18, p.28].

Based on the above groups, it can be argued that a cybercriminal is characterized by technical training, has a set of methods that allow him to carry out various frauds (obtaining unauthorized access, hacking security keys, etc.). In most cases, this is a graduate (or senior student) of a technical university, who has his own personal computer or laptop. In the vast majority of cases, these are men aged 15-40 years. As a rule, the studied persons have a closed character, are often depressed, prone to personal experiences, and are touchy. Their progress in school was not brilliant, but they learn the basics of computer science and mathematics well. For the most part, they may have an incomplete family, where there is a complex psychological atmosphere. According to statistics, 72.2% of hackers lived with one of their parents at the time of the crime, in 51.3% of cases, the main success of hackers in training was in the exact sciences, and in 33.1% they started their activities with a desire to try computer hacking techniques [19]. Cybercriminals are characterized by legal nihilism and high self-esteem. In most cases, they feel their impunity and invulnerability, ignore the requirements of the law and consider it quite normal to independently determine the morality and correctness of certain legal norms based on their own criteria. They often show infantilism, irresponsibility, uncompromising, lack of understanding of the possible consequences of their actions, and often ignore public opinion and interests. In such cases, «the assessment of the situation is carried out not from the standpoint of social requirements, but based on personal experiences, resentments, problems and desires» [20, p. 104]. The motives of the crime – various motivating factors that contribute to the commission of cybercrime can be attributed (most cybercrimes are committed for selfish reasons) political and religious views, hooliganism.

Today, the Internet has become an important and significant resource in the lives of young people, an almost irreplaceable medium of communication, and in connection with this, attacks by young hackers – schoolchildren and teenagers-have recently begun to spread. On the Internet, each user can find relevant information to form the skills and abilities of a hacker. In the beginning, this becomes fun for the user, which in the future can cause offenses, as well as crimes on the Internet. This is why the number of young cybercriminals is growing. A prime example is Jonathan Joseph James, who started hacking information systems from an early age. He hacked into major organizations, including the military threat reduction Agency, which is a division of the US Department of Defense. After that, they got access to user names and passwords, as well as the ability to view confidential information. On June 29 and 30, 1999, James attacked NASA when he was 15 years old. He managed to gain access by hacking the password of a server belonging to a government Agency located in the state of Alabama. James was able to roam the web freely and steal several files, including the source code of the international space station. According to NASA, the value of the software stolen by James is estimated at $ 1.7 million. After the hack was discovered, NASA had to shut down the system to check and restore it to working order, which cost $ 41,000. NASA caught James quickly, as agency did everything to stop him. Jonathan became widely known for being the first minor sent to prison for «hacking» in the United States at the age of 16. [21]

Young hackers often commit cybercrimes to demonstrate their skills and capabilities in front of their peers. So in Germany, a boy named Linus Henze discovered a breach in the macOS system, which allows you to steal all the passwords stored on the device. He announced this on Twitter and posted a video of the hack on YouTube [22]. Using this maneuver, it was possible to gain access to more than two million usernames and passwords of users.

But in addition to users, the reasons can be attributed to the lack of regulation of international and national criminal law. To date, some international legal bases for cooperation in the fight against computer crime have been established. These include the Council of Europe Convention on cybercrime of 2001, Measures to combat computer-related crime adopted at the Eleventh United Nations Congress on the prevention of crime and the treatment of offenders in Bangkok on 25 April 2005, the global cybersecurity programme approved by the International telecommunication Union in 2007, the Okinawa Charter for the global information society adopted on 23 July 2000 in Okinawa, Japan, and others. In the CIS countries, on February 17, 1996, at the VII plenary session of the Interparliamentary Assembly, a Model criminal code was adopted, which regulates responsibility for computer crimes; on June 1, 2001, an Agreement on cooperation between the CIS member States in combating computer information crimes was signed in Minsk. The 2000 United Nations Convention against transnational organized crime, adopted by General Assembly Resolution 55/25 of 15 November 2000, indirectly addresses the problems of cybercrime if committed by organized criminal groups. From all this, we can conclude that today there is no single international act that could unify the norms for combating cybercrime.

In addition, many countries around the world have laws authorizing illegal activities in the virtual space. These include the laws of the States of Florida and Arizona of the United States «Computer crime act of 1978», which establishes criminal liability for crimes in the field of computer information, «**The Law on fraud and misuse of computers**», the main legal act that establishes criminal liability for crimes in the field of computer information. Subsequently, it became the main normative legal act establishing criminal liability for crimes in the field of computer information, included in the form of § 1030 in Title 18 of the us Code of laws, the «**National information infrastructure protection Act**», as well as «**The Patriot Act**» of 2001, which, among other things, contains a special Chapter «**Computer crime and intellectual property**». In the UK, «**The Computer abuse Act**» has been in force since August 1990. The first paragraph of this Act concerns «**unauthorized access to computer data**».

Responsibility for these crimes is provided for in Chapter XX[1] of the Criminal Code of the Republic of Uzbekistan, referred to as «**Crimes in the field of information technology**». Criminal sanctions at the national level do not provide reliable protection from cybercrime because the existing law there are not enough articles on crimes in the field of information technology and security, a clear classification of cybercrime, and the complexity of interpreting and applying existing articles limit the actions of law enforcement. The legislative body should carry out systematic work not only to develop new legal norms, but also appropriate sanctions, while creating the necessary mechanism for ensuring the activities of law enforcement agencies, Prosecutor's offices, judicial and punitive bodies that can effectively prosecute and punish those responsible for crimes in the field of information technology and security.

Criminal laws should be supplemented by appropriate civil sanctions. The absence of special rules in the current civil code of the Republic of Uzbekistan regulating all existing aspects of virtual civil relations, including the electronic form of transactions, creates additional difficulties in recognizing their evidentiary value. The adoption of the Laws «**On e-Commerce**», «**On electronic digital signature**», «**On electronic document management**», «**On appeals of individuals and legal entities**», «**On e-government**» has not yet completely corrected the situation, because the Civil code of the Republic of Uzbekistan still requires written registration of transactions. Moreover, the position of some of the articles, a legitimate part of the fault could technically be charged and the victim as a legal entity that has not adopted the reasonable precautions and due to the fact that ICT and other equipment recognized as a source of danger to users, focusing on the imperfection of the law, aspire for its part, not only to help the officials, how to hold a neutral stance. In addition, all the above-mentioned laws state that persons guilty of violating the law are liable in accordance with the established procedure. Unfortunately, there are currently no such provisions in the Criminal Code or the Code of administrative responsibility of the Republic of Uzbekistan.

DISCUSSION OF CONCLUSIONS AND PROPOSALS

Given the above, and taking into account the special urgency of the issues in the field of information technology, security rapidly growing information society and developing in this context, new forms and methods of cybercrime make scientific and academic community to think seriously, to join forces in international cooperation, and collaboration with the relevant specialized agencies fighting in this area.

One of the conditions for creating an effective system of international information security is the development and adoption of a modern, universal international legal act that provides adequate protection against new threats, while taking into account the national sovereignty of states in contrast to the outdated European Convention on cybercrime. The conclusion of a universal international treaty on combating information crimes, which would take into account the accumulated experience of international agreements in this area and the peculiarities of the national legislation of the participating countries, is quite a complex and time-consuming task. **Such a universal regulator could be a separate UN Convention on combating cybercrime and ensuring global information security**, which at the international level would help to comprehensively and systematically counter cybercrime and cyberterrorism, as well as to combat them.

In order to analyze cybercrime, exchange information about it between the CIS member States, analyze preventive measures and operational measures taken at the national level, as well as conduct special training for law enforcement, judicial and prosecutorial personnel, it is necessary to establish a **Regional coordination center for countering cybercrime within the SCO**.

The creation of this center will allow systematic data collection and processing, providing information, technical and forensic support to the relevant law enforcement agencies of the CIS countries, coordinating joint investigations, as well as specialized training and training of specialists. The center can facilitate the necessary research and software development, assess and analyze existing and potential threats, make forecasts, and issue advance warnings. Within the scope of the Centre's activities will also include assistance to judges, prosecutors and law enforcement officers.

In turn, the analysis of legislation in the field of information technologies and threats of cybercrime to national security indicates the need to systematize and specify the basics of state policy in the field of information security. To this end, **the Concept of information security of the Republic of Uzbekistan** should be adopted. In the concept of information security, based on the analysis of the current state of information security, the goals, objectives and key problems of ensuring information security should be defined.

As part of the implementation of this Concept, as well as the Concept of improving criminal and criminal procedure legislation, it is necessary to improve the norms of the Criminal code of the Republic of Uzbekistan in terms of establishing responsibility for cybercrime by introducing a special section on crimes in the field of information technology and security.

References:

1. http://www.itu.int/

2. http://www.itweapons.com/

3. https://podrobno.uz/cat/tehnp/kolichestvo-internet-polzovateley-v-uzbekistane-sostavlyaet-22-milliona-chelovek/

4. Decree of the President of the Republic of Uzbekistan «On the Strategy of actions for further development of the Republic of Uzbekistan» from 7 February 2017 the year number DP–4947 (*in Russian*).

5. Resolution of the President of the Republic of Uzbekistan «On measures to radically improve the system of criminal and criminal procedure legislation» from 14 May 2018 the year number PP–3723 (*in Russian*).

6. https://www.internetworldstats.com/top20.htm

7. Gladkikh V.I. Criminology: textbook (bachelor's and master's degrees). Moscow: Justitia, 2019, 422 p (*in Russian*).

8. Abdurasulova K. R. Criminology. Textbook. Executive editor: M.Kh.Rustambayev. - T.: «Adolat», 2007. - 216 b (*in Uzbek*).

9. Criminology. Textbook. Collective of authors. Executive editor: M.Kh.Rustambayev. - T.: TSIL 2008 – 586 p (*in Russian*).

10. Kabulov R., Abdurakhmanov E.S. Crimes in the sphere of information technologies: Textbook. - T.: Academy of the Ministry of internal affairs of the Republic of Uzbekistan, 2009. - 80 p (*in Russian*).

11. https://ria.ru/20190805/1557194818.html

12. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

13. https://runet.rbc.ru/materials/pravda-o-feyk-nyus/

14. https://regnum.ru/news/economy/2915482.html

15. https://www.vedomosti.ru/politics/articles/2020/04/20/828521-pervii-v-rossii

16. Report of the United Nations Office on drugs and crime «Cybercrime and COVID19 coronavirus: risks, threats and responses» (source available at: https://www.unodc.org/documents/Advocacy-Section/Russian_-_UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf).

17. Law of the Republic of Uzbekistan «On Informatization» from 11 December 2003 the year number 560-II (*in Russian*).

18. Kardava N.V. Cyberspace as a new political reality: challenges and answers // History and modernity. 2018. no. 1-2-P. 27-28 (*in Russian*).

19. http://www.psyfactor.org/

20. Antonyan Yu.M., Yenikeev M.I., Eminov V.E. Psychology of the criminal and investigation of crimes, Moscow: Yurist, 2006, 190 p (*in Russian*).

21. https://ru.wikipedia.org/wiki/Джонатан_Джозеф_Джеймс

22. https://lenta.ru/news/2019/02/07/vzlomshik/