

**General Prosecutor's Office of the Republic of  
Uzbekistan**

**Academy of the General Prosecutor's Office of the Republic of  
Uzbekistan**

5A240124 – Investigative activity

Khalmuratov Aybek Orazbaevich

Information technology crime investigation

**MASTER OF SCIENCE DESSERTATION**

**Scientific supervisor (adviser)** –  
associate professor at the Department  
of supervision over the execution  
of supervision over the execution  
on crime control and offence prevention  
laws, AGPO of RUz, DSc, I.R. Astanov

## Contents:

|   |    |
|---|----|
| <b>Introduction</b> .....   | 3  |
| <b>Chapter 1. IT-crimes: concept, measures, cooperation</b> .....   | 9  |
| 1.1. The concept and certain types of IT-crimes .....   | 9  |
| 1.2. Improve mechanisms and measures to prevent IT-crimes .....   | 20 |
| 1.3. International cooperation in solving IT-crime issues .....   | 34 |
| <b>Chapter 2. Particular aspects of some operational and investigative actions during IT-crime investigation</b> .....                                | 43 |
| 2.1 Particular aspects of Search and Intelligence operations during IT-crime investigation .....  | 43 |
| 2.2. Particular aspects of the tactics of Incident Scene Inspection, Search (Seizure), Interrogation of defendant during IT-crime investigation ..... | 53 |
| 2.3. Particular aspects of planning and commissioning of computer forensic expert examination during IT-crime investigation .....                     | 69 |
| <b>Conclusion</b> .....   | 81 |
| <b>List of literature references</b> .....  | 87 |
| <b>Annexes (on Russian)</b> .....   | 93 |

## Introduction

**Relevance and necessity of the topic of dissertation research.** XXI century – the century of rapid development of scientific and technological progress. All over the world information technologies and the Internet are firmly entrenched in everyday life. At the same time, IT-crime has been declared a global international challenge in the modern world. This is evidenced by the adopted international agreements providing for joint steps to combat this high-tech evil. In particular, the UN General Assembly, the Council of Europe, the SCO<sup>1</sup>, the CIS<sup>2</sup>, the League of Arab States and other organizations have adopted special acts on information and communication technologies, combating and preventing criminal use of information technologies, and preventing crime in this area at regional and international level. According to statistics, to date mobile telecommunications networks have reached about 7 billion people (95% of the world's population) and the amount of damage from IT-crimes is 1% of the world's GDP per year<sup>3</sup>. World practice shows the damage from IT-crime can be calculated in amounts whether make up the annual budgets of large cities. In most countries in Europe and the Americas, IT-crime generates income comparable to that generated by drug and arms trafficking<sup>4</sup>.

As President of the Republic of Uzbekistan Sh.M. Mirziyoyev noted, “active introduction of advanced technologies and development of global information and communication space dynamically and quickly transform all processes, promote the development of new forms of cooperation at the level of continents, regions, States and business”<sup>5</sup>. Hence, program measures are implemented in our republic to combat crimes in the field of information technologies. The Strategy of actions on five

---

<sup>1</sup> Shanghai Cooperation Organization – official website. – [Electronic resource] – Available at. – URL: <http://eng.sectsc.org/> (Date of review 03.04.2020).

<sup>2</sup> Commonwealth of Independent States – official website. – [Electronic resource] – Available at. – URL: <http://cis.minsk.by/> (Date of review 03.04.2020).

<sup>3</sup> Azad M.M., Mazid K.N., Sharmin S.Sh. Cyber crime problem areas, legal areas and the cyber crime law // International Journal of New Technology and Research (IJNTR) ISSN: 2454-4116, Volume-3, Issue-5. – Dhaka, Bangladesh: Shanto Mariam University of Creative Technology, 2017. – P. 01.

<sup>4</sup> Mikhlina A.S. Criminal law. The special part (Textbook). – Moscow, RF: Jurisprudence, 2000. – P. 289 (unofficial translation from Russian).

<sup>5</sup> President of the Republic of Uzbekistan Sh.M. Mirziyoyev addresses the session of CIS Council of Heads of State dated October 12, 2017.

priority directions of development of the Republic of Uzbekistan in 2017-2021 includes the issues of “improvement of criminal legislation, improvement of the system of ensuring information security and information protection, timely and adequate counteraction to threats in the information sphere”<sup>1</sup>.

In this regard, establishing responsibility for the dissemination of information what poses a threat to the rights and freedoms of the individual, the interests of society and the State is an urgent task<sup>2</sup>.

The specific nature of IT-crime presents a challenge in the IT-crime detection and investigation for most law enforcement officials. These include difficulties in generalizing investigative practice with respect to each type of offence under consideration; lack of methodological recommendations on both the organization of criminal investigations and the tactics involved in conducting investigations; and insufficient qualification of investigators to work with specific sources of evidence-based information digitized in the form of electronic messages, pages and websites.

Due to the sharp aggravation of the criminal situation in the country caused by the growth of IT-crime, as well as the creation of more and more sophisticated ways of their implementation, the challenge of developing forensic tactics for the investigation of these offences becomes more urgent than ever. In turn, it needs to activate and expand the range of scientific research in this area, which is aimed at increasing the effectiveness of all forms and directions of organization of investigative activities to solve crimes in virtual space<sup>3</sup>.

The needs of investigative practice taking notice the state of IT-crime detection testify to the need for additional comprehensive research into the tactics of

---

<sup>1</sup> Decree of the President of the Republic of Uzbekistan “On Strategy of Actions on Further Development of Uzbekistan” № UP-4947 from 07.02.2017 – [Electronic resource] – Available at. – URL: <https://lex.uz/docs/3107042> (Date of review 04.04.2020).

<sup>2</sup> Rahaman M.A. Cyber crime affects society in different ways // the Financial Express. Published: July 04, 2016. Updated: October 24, 2017. – official website. – [Electronic resource] – Available at. – URL: <https://thefinancialexpress.com.bd/views/reviews/cyber-crime-affects-society-in-different-ways> (Date of review 04.04.2020).

<sup>3</sup> Itari D., Anthony E.O., Mercy N. Cyber space technology: Cyber crime, cyber security and models of cyber solution, a case study of Nigeria // International Journal of Computer Science and Mobile Computing, Vol.6 Issue.11, ISSN 2320-088X. – Nigeria: IJCSMC, 2017. – P. 94.

operative and investigative actions, the development of new tools and techniques that take cognisance of modern advances in forensics and related sciences.

The aforesaid confirms the particular urgency of the scientific research.

**Research object** is a system of social relations governing criminal, criminological and forensic measures to investigate IT-crimes.

**Research subject** consists of conceptual approaches in the field of criminal law, forensics, criminology, criminal procedure in the area of IT-crimes investigation and law enforcement practice of national legislation and experience of foreign countries.

**Research purpose** is to develop proposals and recommendations for further improvement of criminal law, criminology and forensic measures to counter IT-crimes.

**Research objectives** are as follows:

- to develop proposals for improving criminal legislation and ensuring its effectiveness;
- to develop proposals for improving the national legal framework in terms of increasing the effectiveness of counteracting IT-crime, the latest threats and challenges in the information sphere;
- to develop proposals for improving the effectiveness of criminal law measures to counter IT-crimes based on the study of the experience of developed foreign countries;
- to highlight the particular aspects of the tactics of Search and Intelligence operations in the IT-crimes investigation;
- to highlight the particular aspects of the tactics set to Incident Scene Inspection, Search (Seizure), Interrogation of defendant<sup>1</sup> in the investigation of cybercrime;
- to highlight the practical guidelines for the conduct of computer forensic expert examination<sup>2</sup> in the investigation of cybercrime;

---

<sup>1</sup> According to Criminal Procedure Code of the Republic of Uzbekistan herein refer to “suspect” (“accused”).

<sup>2</sup> According to international investigation practice defined as “digital forensics”.

**Degree of scientific development of the topic.** Criminal, criminological and forensic researches of crimes in field of information technology are a new direction not only national, but also international criminal science. Abroad, such scientists as M.Gercke, J.Howard, J.Smith, D.Denning, S.Furnell, P.Grabosky, P.Himanen, E.Hickey, D.Parker, etc. considered the questions of studying the features of the crime elements, differentiation of criminal responsibility, qualification and proof during IT-crimes investigation.

Among the scientists of the CIS countries one can enumerate the works of V.S. Karpov, T.L. Tropina, V.B. Vehov, T.M. Lopatina, Yu.M. Baturin, V.V. Popova, D.A. Ilyushin, V.V. Stepanov, A.I. Semikalenova, A.L. Osipenko and other scientists who have made a significant contribution to the study, investigate and counter IT-crime.

In our country the general legal aspects of criminal and criminological (E.S. Abdurakhmanov, R. Kabulov, M.H. Rustambaev, K.R. Aburasulova, M. Sobirov, N.S. Salayev, D.I. Safarov, A. Rasulev) and also forensic (A.S. Zakutsky, T.N. Butunbaev) countermeasures to the considered crimes were investigated. Apart from, 2 dissertations for the scientific degree of the doctor of philosophy (PhD) were completed. One of them is on the topic of responsibility for theft committed using computer equipment (Kh.R.Ochilov). The other is devoted to improving criminal law and criminological measures to combat crimes in the field of information technology and security (A.K.Rasulov).

However, the comprehensive study of the tactics of operational and investigative actions in the IT-crime investigation is still beyond the scope of subject studies. The analysis of theoretical and applied developments in the field of forensic science on this topic allows us to talk about a certain lack of specific practical and scientifically significant grounded recommendations related to the tactics of operational and investigative actions in the IT-crime investigation.

**Research methods.** At the decision of objectives in view were used general scientific and special methods of scientific cognition: system, concrete-sociological, comparative-legal, analytical, method of the quantitative analysis (content analysis),

logical-legal, etc. In aggregate, all these methods allowed to some extent to ensure the reliability and validity of the results of the dissertation research.

The norms of international law, the Constitution, Criminal Code, Criminal Procedure Code and other normative legal acts form the **research legal basis**.

**Scientific novelty** of the research lies is as follows:

- the high degree of public danger of certain crimes committed using telecommunication networks and the Internet were explained;
- it is well-founded to establish responsibility for some crimes committed using telecommunication networks and the Internet;
- the need to improve criminal liability for crimes committed in the field of information technology was grounded;
- identified the need for comprehensive implementation of legal, organizational and technical measures by law enforcement agencies to ensure information security while securing information;
- suggested the necessity to recognize actions having negative influence, committed with the use of tools of information technologies, as socially dangerous act.
- the significant role of Search and Intelligence activities in the IT-crime investigation is proved;
- the specifics of certain investigative actions in the IT-crime investigation are presented;
- proposed the need for further scientific research in the framework of the problem under consideration with a view to preparing practical recommendations on the development of tactics of operational and investigative actions in respect of certain types of IT-crime.

The scientific novelty of the research is confirmed by the provisions and results put forward for public defense.

**Practical significance** of the research is as follows:

- relevant proposals were developed regarding the recognition of criminal, criminological and forensic measures as the main tools of counteract IT-crimes, as

well as the need to incorporate them into national criminal legislation and other legal acts of Uzbekistan.

– on the deep study basis of the current IT-crimes combating state and the relevance on cardinal review of the system and mechanisms of counteraction in this field, the issue of adopting a conceptual special normative-legal act in the sphere of combating cybercrime is raised. In particular, the *Draft Law on combating crimes in the field of information technologies of the Republic of Uzbekistan* has been prepared, where on the basis of analysis the goals have been defined, tasks and key problems on combating IT-crimes have been revealed taking into account modern challenges and threats;

– it has been argued that the establishment of *specialized unit to combat IT-crime* contribute to ensuring public order and enhance the effectiveness of the detection and investigation of IT-crime through Search and Intelligence operations;

– it is proved that the establishment of *Special Computer Forensic Centre* for digital forensics serve to improve the efficiency and quality of the IT-crime incidents detection through testing and research, as well as Expert Testimony. In addition, testing of security equipment in the area of information security. The suggested center carries out functions of original “range” on testing of the newest protection frames against computer viruses, malicious programs, burglaries etc.;

– formulated recommendations and proposals aimed at improving the quality and effectiveness of operational and investigative tactics in the IT-crime investigation.

**Probation of the dissertation research results.** The main provisions and conclusions of the research are reflected in five articles covering various aspects of the topic under development, published in scientific journals and conference proceedings.

**Structure of the dissertation.** The research consists of an introduction, two chapters with six paragraphs, a conclusion, a list of literature and annexes. The main part of dissertation is 92 pages long.



## **Chapter 1. IT-crimes: concept, measures, cooperation**

### **1.1. The concept and certain types of IT-crimes**

The active growth of all kinds of information technology threats poses an extremely urgent task for every State – the need to ensure information security in modern society.

As the first President of the Republic of Uzbekistan I.A. Karimov attached significance, “it is particularly important to note the development of high-tech telecommunications industry is strategically important for us. Presently, it is unthinkable to imagine life without computer equipment, information technologies, Internet, cellular telephone communication”<sup>1</sup>.

In turn, the head of our State Sh.M. Mirziyoyev rightly points out “...it is necessary to take into account and use the significant advantages of modern computer technologies, especially the Internet”<sup>2</sup>.

The world’s annual assessment of the IT-crime raises concerns about the low level of citizens protection in modern information society. Basically, the range of issues is quite wide – from technical insecurity to the vulnerability of work support systems designed for conducting monetary transaction.

As R.S. Belkin believes, the language of science (terminology) should be distinguished by exceptional accuracy, certainty, unambiguousness of the used designations and terms. Initially, the introduction of new concepts and definitions into forensics can be carried out at the expense of scientific knowledge real results<sup>3</sup> on the basis of interconnection and interpenetration.

---

<sup>1</sup> Karimov I.A. Our main task is to further develop the country and improve the welfare of the people. Report of the President of the Republic of Uzbekistan at the meeting of the Cabinet of Ministers dedicated to the results of socio-economic development of the country in 2009 and the most important priorities of the economic program for 2010.

<sup>2</sup> Mirziyoev Sh.M. Critical analysis, strict discipline and personal responsibility should become a daily norm in the activity of each manager. Report of the President of the Republic of Uzbekistan at the extended session of the Cabinet of Ministers dedicated to the results of socio-economic development of the country in 2016 and the most important priority directions of the economic program for 2017.

<sup>3</sup> Belkin R.S. The course of forensics: a training manual for universities. Moscow, RF: UNITY DANA, 2001 – P. 182-187. (unofficial translation from Russian).

The above-mentioned argument is also true for the concepts of “IT-crime”. At present, the term is used widely enough in connection with the information and telecommunication breakthrough in the XXI century. Simultaneously, they have become an integral part of all spheres of human activity. For the most part, in the systems of remote banking via communication channels with the help of electronic means, electronic data carriers, technical devices, computer programs’ transfer funds and utilities are paid, various goods are bought and sold.

In general, with the development of information technologies, the term “computer” is becoming commonplace. Nowadays almost all gadgets have access to the Internet. With the development of 3G and 4G networks, mobile phones are connected to a global network using UMTS<sup>1</sup> or HSPDA<sup>2</sup> technology. Such networks on speed practically do not concede possibilities of connection to a network the Internet by tools of the trivial computer. Doubtless, they will surpass it on technical characteristics and parameters in the future.

In order to prevent compromising the information systems and websites of the “UZ” domain zone, as well as alerting national Internet users about emerging threats, the “Cyber Security Center”<sup>3</sup> the State Unitary Enterprise presented the Review<sup>4</sup>. The threat study showed:

- 106,508 cases refer to hosts who are members of botnet networks;
- 13,882 related to blocking IP-addresses blacklisted by various services due to spamming or password brute-forcing;
- 8,457 is related to the use of the TFTP<sup>5</sup> and related ports. Using of them can lead to the download of foreign content due to the lack of authentication mechanisms;

---

<sup>1</sup> Universal Mobile Telecommunications System – the third-generation network.

<sup>2</sup> High Speed Downlink Packet Access – the fourth-generation network.

<sup>3</sup> Official website of the “Cyber Security Center” SUE of Uzbekistan – [Electronic resource] – URL: <https://tace.uz/> (Date of review 08.04.2020) (unofficial translation from Russian).

<sup>4</sup> Cyber Security of the Republic of Uzbekistan. Outcomes of 2019. – [Electronic resource] – URL: <https://review.uz/ru/post/kiberbezopasnost-respubliki-uzbekistan-itogi-2019-goda> (Date of review 08.04.2020) (unofficial translation from Russian).

<sup>5</sup> Trivial File Transfer Protocol – a formal set of format, timing, sequencing, and error control rules for transferring files to and from a remote computer system running the TFTP service.

- 2,114 refers to the use of the vulnerable RDP<sup>1</sup>;
- 1,042 cases involving the use of software and database management system without authentication mechanism and expired or unreliable SSL certificates<sup>2</sup>.

Thereby, the problem is compounded by the reality that it is not possible to solve these issues by the forces of only one State. There is a need for international coordination to counter this transnational scourge. Indeed, the Manual on the Prevention and Control of Computer-Related Crime for United Nations (UN) Member States<sup>3</sup> recognize criminal offenses in virtual space as a global international challenge. Similar provisions are contained in other international legal instruments. Such as the Budapest Convention of the Council of Europe “On Cybercrime”<sup>4</sup>, ASEAN Declaration to Prevent and Combat Cybercrime<sup>5</sup>, the Okinawa Charter on Global Information Society<sup>6</sup>.

It should also be stressed to date the world community has not developed a common terminology and a common approach to the phenomenon and concept of IT-crime, which is used along with the concept of cyber or computer crime.

Most IT-crime literature usually begins with the interpretation of the word “cybercrime” and “computer crime”. In this sense, in recent time various methods have been adopted to give the most accurate description as possible for both words. Before assessing these strategies, the connection between “cybercrime” and “computer-related crimes” or “computer-oriented crimes” needs to be determined. Without going into depth at this point, the term “cybercrime” is broader than computer-related crimes, as a computer network must be involved. Computer-

---

<sup>1</sup> Remote Desktop Protocol – a proprietary protocol to provide remote display and input capabilities over network connections for Windows®-based applications between two computers.

<sup>2</sup> A certificate used to provide SSL. It encrypts traffic and verifies the identity of the server.

<sup>3</sup> United Nations Manual on the prevention and control of computer-related crime – [Electronic resource] – Available at. – URL: [http://216.55.97.163/wp-content/themes/bcb/bdf/int\\_regulations/un/CompCrims\\_UN\\_Guide.pdf](http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf) (Date of review 10.04.2020).

<sup>4</sup> Convention of the Council of Europe “On cybercrime”. November 23, 2001. – [Electronic resource] – URL: [https://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest\\_/7\\_conv\\_budapest\\_en.pdf](https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf) (Date of review 10.04.2020).

<sup>5</sup> ASEAN Declaration to Prevent and Combat Cybercrime – [Electronic resource] – Available at. – URL: <https://asean.org/asean-declaration-prevent-combat-cybercrime/> (Date of review 12.04.2020).

<sup>6</sup> The Okinawa Charter on Global Information Society. One of the four documents issued at the G8 Summit Meeting at Kyushu-Okinawa on 21-23 July, 2000. – [Electronic resource] – Available at. – URL: <https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html> (Date of review 12.04.2020).

oriented crimes also involve certain behaviors that have no connection to a network but instead affect individual computer systems<sup>1</sup>. Apart from, many foreign scientific resources, crimes committed in computer and telecommunication systems are nominated in different ways: e-crimes, digital crimes, high-tech crimes, Internet crimes, online crimes, information crimes, electronic crimes, technology crimes, crimes in the field of computer information, computer misconduct etc. Therefore, in this research we use the word “IT crime” in order to make a real widespread study of these categories.

So far, there is no definition of “IT-crime” in the Criminal Code of Uzbekistan. In the modern legal literature of Uzbekistan, “IT-crime” is understood as “crimes in the field of information technology”. Despite the different descriptions and approaches both abroad and in Uzbekistan, there is a difference between “crimes committed in the sphere of information technologies” and “crimes committed by means of information technologies”. The first category of crimes falls within the Chapter 20 of the Criminal Code. These are Article **278**<sup>1</sup>. Violation of the rules of informatization, Article **278**<sup>2</sup>. Illegal (unauthorized) access to computer information, Article **278**<sup>3</sup>. Manufacture for marketing purposes or marketing and distribution of special means for obtaining illegal (unauthorized) access to a computer system and telecommunication networks, Article **278**<sup>4</sup>. Modification of computer information, Article **278**<sup>5</sup>. Computer sabotage, Article **278**<sup>6</sup>. Creation, use or distribution of malicious programs, Article **278**<sup>7</sup>. Illegal (unauthorized) access to telecommunication networks.

The second category is crimes committed with by means of information technologies: computers (phones, tablets), program devices, information systems, local and global networks, telecommunication networks, malware, etc.

Criminal legislation of the Republic of Uzbekistan includes Article **103**. Incitement to suicide, Article **103**<sup>1</sup>. Inducement to suicide, Article **167**. Embezzlement, Article **168**. Fraud, Article **169**. Theft,

---

<sup>1</sup> Cisar P., Maravic Cisar S., Bosnjak S. Cybercrime and digital forensics – technologies and approaches // DAAAM International scientific book. ISBN 978-3-901509-98-8, ISSN 1726-9687. Chapter 42. – Vienna, Austria: 2014. – P. 526.

Article **188**<sup>1</sup>. Illegal fundraising activities, Article **244**<sup>1</sup>. Production, keep, distribution or demonstration of products threatening public security and public order, Article **278**. Organization and performance of gambling and other risk-based games.

Many scientists and researchers have attempted to design this concept. According to V.A. Nomokonov, T.L. Tropina, the cybercrime is more extensive than computer crime and accurately reflects such phenomena as crime in the virtual space<sup>1</sup>. It should also be noted, virtual space is a space whichever is simulated and mediated by electronic devices. In our opinion, the most complete identification reflecting aspects of this negative phenomenon is given in D.N. Karpov's article: "cybercrime is an act of social deviation with the aim of causing economic, political, moral, ideological, cultural and other types of damage to an individual, organization and State through any technical tools with access to the Internet". By and large, it reflects not legal aspects, but social and economic problems of modern society<sup>2</sup>.

Technically, P. De Hert, G. González Fuster and B.J. Koops believe that IT-crime in the broad sense is any illegal act committed through or in connection with computer devices, including such crimes as the illegal storage, offering or dissemination of information through the use of computer technologies<sup>3</sup>. In general, IT-crime is linked by these authors to offences committed on various information networks.

K.N. Evdokimov indicates, it is reasonable to consider computer crime in a narrow and broad sense. In the narrow sense, "computer crime" is a set of crimes, where the direct main object of criminal offense are public relations protected by law in the field of safe creating, storing, processing and transferring computer information. Typically, the subject of the crime are computer information, tools on protection of computer information, information and telecommunication networks,

---

<sup>1</sup> Nomokonov V.A., T.L. Tropina. Cybercrime as a new criminal threat // *Criminology. Yesterday. Today. Tomorrow*. – №1 (24). – 2012. – P. 47. (unofficial translation from Russian).

<sup>2</sup> Simonov N., Klenkina O., Shikhanova E. Leading Issues in Cybercrime: A Comparison of Russia and Japan // *Advances in Social Science, Education and Humanities Research*, volume 441. 6th International Conference on Social, economic, and academic leadership (ICSEAL-6-2019). – Paris, France: Atlantis Press SARL, 2020. – P. 506.

<sup>3</sup> De Hert P., González Fuster G., Koops B.J. Fighting cybercrime in the two Europes // *Dans Revue internationale de droit pénal* 2006/3-4 (Vol. 77) – Brussel, Belgium: Vrije Universiteit Brussel, 2006 – P. 262-267.

tools on storage, processing and transmission of computer information. From their perspective, this qualification fully coincides with the notion of “crimes in the sphere of information technology” formed by the legislator. On a gross scale, the definition of “computer crime” is interpreted as follows. Computer crime is a set of crimes where the main direct object of criminal offense is public relations in the sphere of computer information and information technologies, safe functioning of tools on creating, storing, processing, transferring and protecting computer information. Otherwise, at the same time computer information, information and telecommunication networks; tools on creating, storing, processing and transferring computer information (PC<sup>1</sup>, smartphones, iPhones, cash registers, ATMs<sup>2</sup>, payment terminals and other computer devices) are not only the objects of a criminal act but they are also used as a tool and instrument of crime committing”<sup>3</sup>.

Other scientists refer to IT-crimes as illegal acts committed through computer and mobile (cellular) communications on networks. Widely, Julian Jang-Jaccard and Surya Nepal argue, IT-crimes are socially dangerous acts committed by means and methods of computer and mobile (cellular) equipment, their software components in respect of information placed, used, processed and changed in the virtual space of the Internet network<sup>4</sup>.

According to the authors of the book “Social Engineering and Social Hackers” M.V. Kuznetsov, I.V. Simdyanov, social engineering is manipulation of a person or group of people to break into security systems and steal important information<sup>5</sup>. As it is noted, these authors, the greatest threat to information security will be represented by more and more advanced methods of social engineering used for hacking the existing security facilities. Explaining this by the fact that social

---

<sup>1</sup> Personal Computer – [Electronic resource] – Available at. – URL: [https://www.webopedia.com/TERM/P/personal\\_computer.html](https://www.webopedia.com/TERM/P/personal_computer.html) (Date of review 10.04.2020).

<sup>2</sup> Automated Teller Machine (ATM) – [Electronic resource] – Available at. – URL: <https://www.investopedia.com/terms/a/atm.asp> (Date of review 10.04.2020).

<sup>3</sup> Volevodz A.G. Counteraction to computer crimes: legal basis of international cooperation. – Moscow, RF 2002. (unofficial translation from Russian).

<sup>4</sup> Jang-Jaccard J., Nepal S. A survey of emerging threats in cybersecurity // Journal of Computer and System Sciences. Volume 80, Issue 5. – Australia: CSIRO ICT Centre, 2014 – P.973-993.

<sup>5</sup> Kuznetsov M.V., Simdyanov I.V. Social engineering and social hackers. – Saint Petersburg, RF, 2007. (unofficial translation from Russian).

engineering does not require significant financial investments and thorough knowledge of computer technologies by trespassers. This view is shared by R. Mogull, head of information security at Gartner Corporation, and R. Forsythe, managing director of the regional divisions at the Sophos antivirus company, who describes it as “a new cynical type of fraud”.

Oppositely, A. Wadhwa, N. Arora believe that IT-crimes are actions on the Internet, in which the computer is either the tool or the subject of criminal attacks in virtual space<sup>1</sup>. From A.H. Al-Hamami’s point of view, IT-crimes are socially dangerous acts committed with the use of computer equipment in respect of information processed and used on the Internet<sup>2</sup>.

Let’s look at modern and widespread types of IT-crimes around the world.

**Financial crimes** – the socially dangerous acts encroaching on financial and economic relations, namely fraud with credit cards, theft of money resources at the moment of bank operations performance, etc.<sup>3</sup>

**Phishing** – is extracting information from trustworthy citizens for access to bank accounts. It is widely used in countries where Internet banking services are popular. To date, targeted phishing has become widespread. Target phishing is used in narrow user groups. They contain messages with a social context encourage potential victims to open an executable file or go to a site containing malicious code.

In practice, the more dangerous type of fraud than phishing is so-called **pharming**. Although, pharming is the procedure of redirecting a victim secretly to a false IP-address. To our way of thinking, it is a more sophisticated, albeit technically complexed method of fraud than phishing<sup>4</sup>.

Another dangerous type of IT-crime is **computer remote hacking**. Surprisingly, it allows computer trespassers to read and edit documents whether are

---

<sup>1</sup> Wadhwa A., Arora N. A Review on Cyber Crime: Major Threats and Solutions // International Journal of Advanced Research in Computer Science. Volume 8, No. 5. ISSN No. 0976-5697 – Gurgaon, India: Amity University Haryana, 2017 – P.2217-2221.

<sup>2</sup> Al-Hamami A.H. Proposals to Win the Battle Against Cyber Crime. DOI: 10.4018/978-1-4666-6583-5.ch008 – Amman, Jordan: Amman Arab University, January, 2014 – P. 5.

<sup>3</sup> Chambers-Jones C., Hillman H. Financial Crime and Gambling in a Virtual World: A New Frontier in Cybercrime. ISBN 978 1 78254 519 4 – Cheltenham, UK: University of West England, 2014 – P. 4.

<sup>4</sup> Brody R., Mulig E., Phishing, pharming and identity theft // Academy of Accounting and Financial Studies Journal, Volume 11. – USA: University of New Mexico, 2007 – P. 43-56.

saved on file servers and desktops of computers. Apart from, they have the ability to introduce their own malicious programs, as well as collect various types of information through audio, video surveillance. One of the newest viruses what have emerged recently is cyberweapons, the purpose of whichever is to destroy industrial infrastructure. These include such viruses as Duqu, Stuxnet, Gauss, Flame. Behind such viruses are no longer low-skilled specialists in information technology, but very super professionals<sup>1</sup>.

Other dangerous examples of IT-crime are<sup>2</sup>:

**Cyber pornography** refers to obscene sites whether allow visitors to post obscene movies, videos and photos with minors.

Up to a point, it is also fair to include dating chats whether contain obscene information about users and descriptions of virtual sex with minors.

**Cyber drug trafficking** is a drug trade for using the latest technology to encrypt messages sent by email clients. In such messages, drug traffickers coded the place and manner in which the goods are exchanged for money.

**Cyberterrorism** is the commission of terrorist acts in virtual space. Undoubtedly, this category of crime may include the simple dissemination over the Internet of information about terrorist acts that may be committed at a specified time in the future. And also highlight such types of IT-crimes as **online gambling** and **cyber harassment**.

It is worth mentioning the victims of IT-crime are juvenile. According to the Ministry of Internal Affairs of the Republic of Uzbekistan, the most terrible and irreversible process of minors' exposure was their mass involvement in suicidal groups, whichever romanticize death and popularize passing on life<sup>3</sup>.

---

<sup>1</sup> Wangen G. The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism // Open Access. Information. ISSN 2078-2489. DOI:10.3390/Info6020183 - Gjøvik, Norway: Gjøvik University College, 2015 – P. 184.

<sup>2</sup> Oluga S.O., Azizah Bt H.A., Ahmad Jamah A.A., Haroon Sh.O., Maryam Omar A.S., Nur Adlya Bt.M. An Overview of Contemporary Cyberspace Activities and the Challenging Cyberspace Crimes/Threats // (IJCSIS) International Journal of Computer Science and Information Security, Vol. 12, No. 3. ISSN 1947-5500 – Kedah, Malaysia: Universiti Utara Malaysia, 2014 – P. 62-100.

<sup>3</sup> MIA: The Blue Whale game came to Uzbekistan two months ago. – [Electronic resource] – Available at. - URL: <https://www.uzdaily.uz/ru/post/32021> (Date of review 15.04.2020) (unofficial translation from Russian).



Hence, the underage girls and boys can be affected not only by direct contact in correspondence on social networks. Alternatively, through suggestions for watching videos, discussion of TV series, helping to solve one's homework. Most of all, certain online books, recommendations for reading literature and listening to music can be offered.

Unfortunately, one of the brightest samples of modern times is the "Blue Whale" online game for juniors and teenagers. The final stage of the play is suicide of a participant. In particular, the list of tasks for the participants is also given, such as cutting the lip, slipping hands with a needle, sitting with legs down on the edge of the roof, drawing with a blade on the hands and feet, etc.

It makes sense, countries such as Uzbekistan, Russia, Ukraine, Bulgaria, Latvia, Italy, the Middle East and the USA have already "collided" with the Blue Whale. Currently, to counter IT-crime is actively conducted. Nowadays preventive measures are actively taken to avert such IT-crimes, the victims of which are minor child.

It follows because IT-crime undermines not only the computer security of society and the information security of computer users, but also the public order of the State as a whole. As a consequence of the "IT-crime" definitions given in the article, as well as individual types of this category of crimes, a common characterization can be formulated. Legally, the IT-crime is a set of crimes prohibited by the Criminal Code of the Uzbekistan committed in virtual space, where the main direct targets of a criminal attack are constitutional rights and freedoms of persons and citizens, social relations in the field of computer information and information technologies, social relations in the sphere of economy and economic activity, social relations in the sphere of State power, social relations in the area of population health and public morality.

There are crimes against the confidentiality, integrity and availability of computer systems, networks and computer data, and abuse of those systems, networks and data. Clearly, this is a violation of social relations protected by law in the sphere of secure creating, storing, processing and transferring computer

information with the aim of causing economic, political, moral, ideological, cultural and other types of damage to a person, society, State and the world as a whole.

The peculiarities of IT-crimes are transboundary; non-standard ways of crimes committing; automation of criminal acts; anonymity of acts; complexity of disclosure of the IT-crime (low percentage of disclosure); interaction of different criminal communities; high income of criminal activity.

It is important to understand given IT-crime covers a wide range of social relations and has a large number of different ways of crime committing. The IT-crime undermines not only the information security of society, but also the public order of the entire State. Importantly, it includes deprivation of material resources, as well as threats to the life and health of citizens. Thereby, IT-crime must be combated at the international level. No doubt, the effective detection of the IT-crime requires active international cooperation and support, as well as constant updating of inter-state and national laws. But it should also be noted, in order to be more successful, every State needs to adopt domestic laws which are not contradictory to one another. As K.N. Evdokimov notes, legal regulation of combating cybercrime issues is the basis of the combating cybercrime entire system. Respectively, amendments and modifications to existing criminal legislation are necessary and relevant at the current stage of development of society.

At present, national jurisprudence considers crimes in the field of information technology from the perspective of relations of information technology use and, on this basis, substantiates the characteristics of IT-crimes in Uzbekistan. For instance, R.K. Kabulov and E.S. Abdurakhmanov note that crimes in the field of information technology violate relations that ensure the lawful and secure use of information technology, thereby threatening the security of individuals, society and the State<sup>1</sup>. The difference in terminology indicates that there is no uniform approach to the problem under study. This is objectively determined by the difficulty of combining

---

<sup>1</sup> Kabulov R.K., Abdurakhmanov E.S. Crimes in the field of information technologies: Study guide. – Tashkent, Uzbekistan: Academy of MIA of the Republic of Uzbekistan, 2009. – P. 62. (unofficial translation from Russian).

the concept of “computer information” with the traditional institutes of criminal law and criminal procedure science<sup>1</sup>.

Summarizing the abovementioned, we propose to define “information technology crimes” as *socially dangerous acts (actions and inactions), committed both intentionally and carelessly, causing or creating a threat of real infliction of essential damage or material damage to social relations in the sphere of information technologies.*

Actually, the main issue of Uzbek legislation in the sphere of computer information and high technologies is not that it is poorly developed, but whether it is developing slowly. Due to the imperfection of the law, there have been experience where no criminal cases have been initiated for several years. It is clear to everyone there is no crime without a crime scene.

In summary, the IT-crimes investigation committed in virtual space requires both technical and theoretical knowledge. Given the acute shortage of the latter, there is a need to justify a single concept of virtual space from a forensic point of view. In a nutshell, it will contribute to deepening and expanding the theoretical base terminology of computer forensics. Additionally, with regard to IT-crime, researchers note the successful detection, rapid and complete investigation of IT-crimes requires new approaches. Hence, they should base on a more complete use of science and technology, with the assistance of knowledgeable individuals <sup>2</sup>.

---

<sup>1</sup> Baturin Y.M. Zhodzinsky A.M. Computer crime and computer security. Moscow, RF: Yurid. lit. 2008. – P. 91. (unofficial translation from Russian).

<sup>2</sup> Protasevich A.A., Zveryanskaya L.P. Peculiarities of the scene inspection in cybercrime cases // Izvestia of Irkutsk State Economic Academy (Baikal State University of Economics and Law), № 2, 2013. (unofficial translation from Russian).

## 1.2. Improve mechanisms and measures to prevent IT-crimes

Due to its specific nature and increased social danger, IT-crimes have been analyzed by criminologists, criminalists and IT-specialists from different points of view almost since their appearance. So far, no unified view of IT-crime has been developed.

As far as we are concerned, the views of specialists in this field can be divided into two groups:

1. IT-crimes are an independent type of criminal activity<sup>1</sup>.
2. IT-crimes do not exist as a separate IT-crime<sup>2</sup>. For this reason, they should be regarded only as a qualifying feature of common “traditional” crimes.

In theory, it is also proposed this group includes an unreasonably broad concept of IT-crimes, whichever includes any offense of people’s communications and relations, hindering the application and use of computer equipment.

The first one is absolutely obvious and socially available. Furthermore, exactly and widely used in the world practice. The most striking samples of recent legislation of this kind are the UK Terrorism Act of 2000<sup>3</sup> and the US anti-terrorism law known as the “Act of 2001”<sup>4</sup>. With this law, Congress introduced new concepts expanding the interpretation of the term “terrorism”, creating a new legislative concept of “cyberterrorism”.

Certainly, it seems more appropriate to us given the second direction, rather two interrelated and complementary approaches. Moreover, they allow for a certain adjustment of the Criminal Code of Uzbekistan without its fundamental revision.

---

<sup>1</sup> Aratuly K., Bostanbekov K. Cybercrimes: Concept and Problems of Terminology // Middle-East Journal of Scientific Research 15 (8): ISSN 1990-9233 – Almaty, Kazakhstan: IDOSI Publications, 2013. – P. 1121.

<sup>2</sup> Gercke M. Understanding Cybercrime: Phenomena, Challenges and Legal Response – Geneva, Switzerland: International Telecommunication Union, 2012 – P. 11.

<sup>3</sup> Terrorism Act of 2000 – [Electronic resource] – Available at. – URL: <http://www.legislation.gov.uk/ukpga/2000/11/contents> (Date of review 18.04.2020).

<sup>4</sup> Anti-Terrorism Act of 2001 – [Electronic resource] – Available at. – URL: [https://www.epic.org/privacy/terrorism/ata2001\\_text.pdf](https://www.epic.org/privacy/terrorism/ata2001_text.pdf) (Date of review 18.04.2020).

First and foremost, the terms and concepts contained in the criminal law should be interpreted in accordance with the definitions set forth in a number of laws of the Uzbekistan.

Afterwards, to expand in some cases the qualifying features of crimes to include the qualification feature – *“by using Computer Equipment either Mass Media or Telecommunication Networks and Internet”* (in cases where their use clearly increases the danger of a particular IT-crime).

In our view, it is essential to make amendments and modifications to the Criminal Code in accordance with the state of international IT-crimes at present time.

Let us begin with Chapter 5: Crime against family, youth and morality – Article **125**. Divulgence of adoption secret. It is advisable to add the Article **125** part 2 with a paragraph “d”: *“by using Mass Media or Telecommunication Networks and Internet”*. Accordingly, it should be punished more severely.

Chapter 6: Crime against freedom, honour and dignity – Article **139**. Defamation. Is it not obvious since defamation, “published on the Internet is incomparably more dangerous than the published in printed or otherwise copied text or in the media” and should be punished accordingly more severely? The same can be attributed to Article **140**. Insult. Therefore, it may be also suggested to add with the following wording: *“by using Mass Media or Telecommunication Networks and Internet”*.

Chapter 7: Crimes against constitutional rights and freedoms of citizens – Article **141**<sup>1</sup>. Violation of privacy – certainly requires additional qualification feature: *“by using Computer Equipment either Mass Media or Telecommunication Networks and Internet”*.

Chapter 8: Crimes against peace and security of mankind – Article **155**. Terrorism. It’s quite enough to add paragraph “c” to part 3 of the Article **155**: *“by using Computer Equipment or Telecommunication Networks and Internet”*.

We are especially interested in Chapter 12: Crimes against economic foundation, in particular Article **176**. Manufacturing, sale of forgery money, excise stamps or securities, Article **179**. False entrepreneurship, Article **180**. False bankruptcy, Article **181**. Suppression of bankruptcy, Article **181**<sup>1</sup>. Premeditated bankruptcy. It is known nowadays such crimes are usually committed by tools on falsification of computer information.

Two conclusions follow from here.

Firstly, the crimes committed according to the mentioned articles, in case of application of information technologies, they should be qualified according to the totality of relevant articles and Article **278**<sup>4</sup>. Modification of computer information.

Secondly, *“by using Computer Equipment either Mass Media or Telecommunication Networks and Internet”* in this case can be a qualifying feature, as the danger of a criminal act increases.

We realize – “the application of information technologies” may be an aggravating factor in the committing before mentioned crimes.

To our way of thinking, Article **191**. Illegal collection, divulgence or use of information do not require any special qualification. Because the collection method is not a qualifying feature for them. It would be observed, however, the court practice notes the increasing role of information technologies in these acts.

Chapter 27. Crime against public security and public order.

We also suppose according to the dangerous impact to economic relations, Article **243**. Legitimization Laundering of Proceeds from Criminal Activity and Article **251**<sup>1</sup>. Illicit traffic in superpotent and psychotropic substances – it is quite sufficient to add new part with the following: *“the same acts committed by using Computer Equipment either Mass Media or Telecommunication Networks and Internet”*. Similarly, they will constitute an aggravating circumstance in the committing crime.

Alternatively, it is difficult to attribute directly to Article **255**<sup>1</sup>. Development, manufacture, stockpile, acquisition, transfer, keep, illegal possession and other activities involving bacteriological, chemical and other weapons of mass destruction

the advice, drawings, recommendations on their manufacture posted on some Internet sites, but such actions clearly require some legal assessment.

In similar, the same applies to Article **270**. Growth of prohibited crops, Article **273**. Illicit manufacture, acquisition, keep and other activities with narcotic drugs, their analogues or psychotropic substances for marketing purposes or marketing and Article **276**. Illicit manufacture, acquisition, keep and other activities with narcotic drugs, their analogues or psychotropic substances without marketing purposes in the Chapter 19. Crimes consisting of illicit traffic in narcotic drugs or psychotropic substances. Essentially, it should be pointed out the Uzbek criminal legislation in the sphere of crimes against health does not provide for liability in any way for such acts related to the use of information technologies may cause human casualties. Meanwhile, foreign lawmakers currently provide for such situations. Definitely, the qualifying feature: *“by using Computer Equipment or Telecommunication Networks and Internet”*, the one should be included in Article **130**. Production, importation, distribution, promotion, demonstration of obscene products.

Chapter 29. Crime against constitutional order and internal security of the State.

Let us consider the “informational” approach to the articles of this chapter using the example of Article **163**. Loss of documents containing State secrets. Indeed, it would be advisable to include the qualifying feature, too: *“committed by using Computer Equipment either Mass Media or Telecommunication Networks and Internet”* Just like approach is also offered to apply in Chapter 15. Crime against administrative order – Article **209**. Forgery in public office, Article **210**. Passive bribery, Article **211**. Active bribery, Article **212**. Complicity in bribery, etc. The last ones are new characteristics of actual crimes in Uzbekistan.

By and large, special consideration should be paid to Article **230**<sup>1</sup>. Falsification (forgery) of Evidence. As digital and information technologies allow falsifying not only written documents, but also sound, image, etc.

The arguments we have presented once again there are very specific IT-crimes, which are not reflected in the Criminal Code of Uzbekistan at all. In particular, protection of an individual and society from “harmful” information should be considered as objects.

To sum up, the following conclusions can be drawn.

Criminal law regulation of the Republic of Uzbekistan in the area of crimes involving information technology is not fully in line with the actual situation;

The number of really existing (or supposedly in the near future) criminal acts cannot be qualified under the existing Criminal Code;

The best way to address the noted gaps is to introduce additions to a number of the existing Criminal Code articles that qualify individual acts and to interpret (in relation to information technologies) a number of terms and concepts used in the “traditional” sense;

In some cases, whereas the absence of the existing Criminal Code fundamentally new structures inherent only in information technologies it is necessary to develop and introduce new norms providing for such act’s criminal liability.

According to the 2019 FBI’s Internet Crime Complaint Center (ICCC), the total damage from IT-crime estimated \$ 3,5 billion, while the average damage per crime was \$35,000<sup>1</sup>. Another reputable international company on cybersecurity for the prevention and investigation of IT-crime, Herjavec Group, damage from IT-crime in 2019 worldwide is predicted at \$ 124 billion<sup>2</sup> (USD).

As for Uzbekistan, State authorities should pay special attention to the activities of law enforcement agencies. Only the quality of law enforcement efforts to combat IT-crime depends on the existence of information security for individuals

---

<sup>1</sup> 2019 Internet Crime Report. Federal Bureau of Investigation’s Internet Crime Complaint Center – [Electronic resource] – Available at. – URL: [https://pdf.ic3.gov/2019\\_IC3Report.pdf](https://pdf.ic3.gov/2019_IC3Report.pdf) (Date of review 19.04.2020). P. 3.

<sup>2</sup> 2019 Official Annual Report. Herjavic Group. Cybersecurity Ventures / Editor-in-Chief: Steve Morgan. – [Electronic resource] – Available at. – URL: <https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf> (Date of review 19.04.2020). P. 6.



and the State as a whole<sup>1</sup>. Nevertheless, the main actions to counter IT-crime are taken at the level of individual States. Let us consider at a few typical examples.

The **United Kingdom** established a National High-Tech Crime Unit in 2001, which includes investigators, forensic scientists and computer consultants. Moreover, the National Criminal Intelligence Service (NCIS) is investigating the feasibility and prospects of establishing a national computer crime centre within that service<sup>2</sup>.

In the **United States**, the National Infrastructure Protection Center (NIPC) provides threat assessment, alert and investigation for cyberattacks under two programs. The first program aims to strengthen relationships with partners and includes public and private institutions. The second program, called “InfraGard”, includes the sharing of incident data on a voluntary basis<sup>3</sup>. The U.S. Department of Justice Criminal Division, through its Computer Crimes and Intellectual Property Offenses Section (CCIPS), established the “LawNet” network of federal, state, and local computer experts in January 2000. Additionally, the Department of Defense has created a common database to assist the defense and intelligence community in combating IT-crime. The joint database enables security and defense agencies to respond quickly to computer requests and share important information.

**Australia** has established an E-Security Co-ordination Group (ESCG). The main objective of the ESCG is to provide a secure and reliable electronic operational space for both the public and private sectors. Basically, the ESCG team is responsible for incident reporting, response and coordination under bilateral and multilateral agreements related to IT-crime<sup>4</sup>.

---

<sup>1</sup> International Journal of Information Security and Cybercrime. Volume 8, Issue 2, DOI: 10.19107/IJISC.2019.02 – Bucharest: Romanian Association for Information Security Assurance (RAISA), 2019. – P. 86.

<sup>2</sup> UK Launches First National High-Tech Crime Unit // Enterprise System Journal. High-End Datacenter and Server Solutions – [Electronic resource] – Available at. – URL: <https://esj.com/articles/2001/04/23/uk-launches-first-national-hightech-crime-unit.aspx> (Date of review 20.04.2020).

<sup>3</sup> Computer Crime. A Joint Report. June, 2000. – [Electronic resource] – Available at. – URL: <https://www.state.nj.us/sci/pdf/computer.pdf> (Date of review 20.04.2020). P. 64.

<sup>4</sup> Dunn M., Wigert I. Critical Information Infrastructure (CIIP) Protection Handbook. – Zurich, Swiss: Swiss Federal Institute of Technology Zurich, 2004. – P. 44.

In 2012, the Central Criminal Police Department in **Georgia** established a Cyber Crime Division (special unit) to combat IT-crime. Currently, there are 15 detective-investigators within the Division who are responsible for investigation of IT-crime. The Division is competent to investigate IT-crime offences. However, the Division also provides advice, guidance and technical assistance to other police units across Georgia in investigation of IT-crime and handling of electronic evidence. In addition, the forensics team of the Ministry of the Interior handles the forensic examination duties. In 2014, the Ministry of State Security of Georgia has been established separate IT-crime investigation team, too.

The **Czech Republic** has developed the Concept for the Development of the Capacities of Law Enforcement Agencies to Investigate Cybercrime (approved by the National Security Council). In this connection, the National Centre for Combating Organised Crime was established in 2016, which included the IT-crime unit. The functions of the unit are to coordinate and provide 24/7 technical support, detect and investigate crimes, cooperate internationally and carry out scientific and educational activities in this area.

Meantime, the activity of the law enforcement agencies of Uzbekistan in detecting (uncovering), investigating and preventing criminal acts related to information security offences is the utmost importance in combating IT-crime. As in individual CIS countries, Uzbekistan does not have independent investigative and operational units specializing in combating IT-crime.

At present, this task is mainly entrusted to the Ministry of Internal Affairs, the State Security Service and the General Prosecutor's Office in Uzbekistan. Primarily, IT-crime detection and investigation is carried out by officers with higher law degree (in accordance with qualification requirements) specializing in the investigation of common crimes, including corruption and economic crimes. The investigative officers of the law enforcement agencies in Uzbekistan have no special knowledge of IT-crime cases. Including the lack of skills of the operational units' officers makes it unenforceable to solve crimes in a timely manner, hunt out evidence and prosecute the liable persons. Most of all, the so-called IT technicians among the officers are

exceptional. As a rule, they are persons who have mastered IT technologies on their own and master computer. We do not set a goal to analyze the qualitative composition of these law enforcement agencies. Generally, it is worthy of note at the moment, officers of all law enforcement agencies are successfully coping with the challenges they face. Nevertheless, it is compulsory to put in mind to slightly other circumstance which can essentially raise efficiency of counteraction to crime in field of information technology. For the present moment detection (reveal), investigation, prevention of such crimes is mainly engaged in piece experts serving in divisions of the specified law enforcement agencies. Given the global trends in the number of recorded crimes in the field of information technology and the use of digital technologies in the committing crime, this is clearly insufficient.

Furthermore, Uzbekistan cannot be classified as one of the most cyber-criminal countries, as the proportion of crimes committed in the sphere of information technologies is only 5% of the number of common criminal offences. The capital city of Uzbekistan, Tashkent, is mainly vulnerable to IT-crimes. Not to mention the fact that a large number of financial and banking institutions, educational institutions, industrial enterprises and institutions with various forms of ownership and others are concentrated here.

Taking into consideration as crimes of a terrorist, extremist, corrupt, economic nature, etc., are committed, inter alia, through information and communication technologies. Furthermore, their investigation requires special knowledge, there is a need to establish specialized units in the law enforcement agencies of Uzbekistan. To paraphrase, they will carry out detection, suppression, disclosure, investigation of IT-crimes, as well as operational-technical and information support.

We believe the skills and abilities in detecting (revealing), investigating and preventing such crimes should be possessed by the officers of the Department on combating economic crimes at the General Prosecutor's Office of the Republic of Uzbekistan, whose powers include carrying out Search and Intelligence activities and interrogation of economic crimes. Accordingly, it is offered to create, as an experiment, Anti IT-crime Division – specialized unit to combat IT-crime in the

Office of the Tashkent City Department, with the right to investigate, in cooperation with Tashkent City Prosecutor's Office.

Obviously, law enforcement practice shows that counter crime successful can be carried out only by comprehensively trained officers, provided with perfectly organized and interact in their duties performance. For successful detection (reveal), investigation and prevention of crime, forensic science and the corresponding technical means, tactics and methods of crime investigation play great importance. Inevitably, the gaps of professional, including forensic training of law enforcement officers, and the training of future and existing officers in special practical skills related to the forensic support of detection (reveal), investigation and prevention of crimes in the field of information technology is extremely important.

It must be borne in mind, this simple seemingly understandable task is complicated by a number of negative circumstances. Over the last few decades there have been significant changes in approaches to training not only in forensics. Also, in many other special disciplines, whichever previously determined the quality training level of a graduate with the qualification of "lawyer". Admittedly, forensics as an academic discipline has become a second-rate course of study. Throughout this time, there have been repeated attempts to "cut back" the training course, which were quite successful. The situation has significantly worsened in the last 10 years. During this time forensic science, as a result of "improvement" of educational standards for the "Jurisprudence" specialty, has not found its place in the list of special disciplines for this direction. Predictably, in the curricula of higher education institutions in the cycle section of the special disciplines depending on the specialization, it was retained only thanks to the goodwill of the scientific council members of the particular institution.

Overall, the analysis of the educational and methodical documentation, textbooks, manuals on the discipline "Forensics" for various specialties shows the content "frozen" at the turn of 80s of the last century. For the most part, consequently all programme documentation and educational literature is based on traditional knowledge and ideas about forensic science. For example, with regard to the subject

of our study in the curricula for the “Jurisprudence” specialty only mention is made the topic “Methods of IT-crimes investigation”. There are considered only general recommendations on the investigation of a sufficiently large group of crimes. However, educational and programme documentation does not contain some information. Such as the modern system of forensic traces; the concept and significance of virtual traces on the possibilities of discovery, fixation, seizure and safety of virtual traces in the individual investigative activities providing; the possibilities of expert examination of such traces or their carriers and using the research results to prove individual circumstances of the crime committed. It would appear without a thorough study of these issues. Nowadays, it is very problematic to study the basics of information security investigation methods. The reasons are following such state of affairs. Especially, mediocre knowledge of the teaching staff in the field of information technologies; ignoring one of the principles of education “from the general to private, from the main to the secondary, from traditional to new”; absence of the customer in accurate representations of what the graduate of high school should know, have and possess; absence of real interaction between educational institution and the customer whichever at least assumes; granting by the customer to educational institution of statistical, analytical and other information. All things considered, elimination of these and other reasons can significantly increase the efficiency of the educational process, the level of mastery of theoretical knowledge by graduates and other categories of students and form the appropriate level of skills and abilities, which will effectively counteract IT-crime and crime in general.

In particular, it is important to review and introduce a special system for the recruitment of personnel in law enforcement and special agencies, as well as in expert units (operational officers with technical education). We believe it is applicable to use the positive experience of foreign countries in recruiting operational officers and specialists with technical education to take legal training courses. At the initial stage, it is possible to establish such a requirement for operational officers.

Meanwhile, returning to the legal regulation of the organizational order of the above-cited specialized Division should be marked as follows. To start, define the main tasks of the Anti IT-crime Division:

1. IT-crimes detection when the object of criminal offense is information technologies, their systems and networks, rights of the owner of information in the fields of telecommunications of computer means, their systems and networks are the instrument of committing a crime, as well as offenses of citizens constitutional rights – inviolability of private life, secrecy of correspondence, telephone conversations, postal, telegraphic or other messages, committed by tools of illegal listening to messages and removal of information from equipment.

2. Initiation of criminal cases and urgent investigation actions, if necessary, suppression of the IT-crimes.

3. Identification of individuals, groups and communities engaged in illegal activities in this area, documentation of their criminal activities and implementation prevent measures of IT-crimes.

4. Execution of instructions to investigate IT-crimes, the conduct of Search and Intelligence operations and participation during investigation as part of investigative and operational teams.

Particularly, carrying out the following activities:

1. Analytical intelligence: improvement of information and analytical support for the activities of the Department's authorities, study of promising means and methods of search and comparative analysis of a wide variety of information relevant to combating IT-crimes, from media materials in Internet digital libraries to specific operational data. The purpose of such analysis is to develop new knowledge of how IT-crime involves computer information, how to conceal it, how to identify unauthorized access to information that has not been reported to law enforcement agencies, etc.

2. Computer intelligence is the use of means and methods to organize the public and tacit receipt of information stored and processed by computer systems to obtain information about forthcoming crimes. The activities of covert receipt of

computer information may include both direct access to information resources of interest and the interception of electronic messages transmitted via computer wires and radio networks.

3. Ensure the information security of the Prosecutor's authorities, which extends from the protection of the subjects and interests of the Prosecutor's authorities from substandard information to the protection of restricted departmental information, information technologies and the tools to ensure them.

Essentially, the condition of information and telecommunication systems and the level of their protection is one of the most important factors affecting the information security of the state. One of the main tools of counteracting IT-crime is information security<sup>1</sup>.

International cooperation during IT-crime investigation should be implemented in forms:

(a) Exchange of information, including:

- on IT-crime in preparation for or committed by computer information, information technology and the individuals and legal entities involved;
- on forms and methods of preventing, detecting, suppressing, disclosing and investigating IT-crime;
- on how it was committed;
- on national legislation and international treaties governing the prevention of the detection and IT-crimes investigation;

(b) Execution of requests for the conduct of Search and Intelligence operations and procedural actions in accordance with international treaties on legal assistance;

(c) Planning and conducting coordinated activities and operations to prevent, suppress, detect and investigate IT-crime;

---

<sup>1</sup> Brown I., Edwards L., Marsden Ch. Information Security and Cybercrime – [Electronic resource] – URL: [https://www.researchgate.net/publication/228226770\\_Information\\_Security\\_and\\_Cybercrime](https://www.researchgate.net/publication/228226770_Information_Security_and_Cybercrime) (Date of review 23.04.2020).

(d) Assistance in training and professional development, including through internships of specialists, organization of conferences, seminars and training courses;

(e) Creation of information systems ensuring the performance of tasks related to the IT-crime prevention, suppression, detection and investigation;

(f) Conducting joint research with the Academy of the General Prosecutor's Office and other departments on problems of mutual interest in combating IT-crimes. On the other hand, increasing the amount of information passing through the State media aimed at raising the level of legal, information and computer culture in society.

Basically, organizational measures to prevent IT-crime are considered by many specialists concerned with the security of computer systems to be the most important and effective. It is connected whether they must be the foundation on whichever the entire system for protecting computer information from IT-crimes.

Monitoring of requirements observance to information protection. Likewise, special software and hardware for information systems protection because process information with the limited access in non-state structures are carried out by public authorities. Initially, the Cabinet of Ministers of the Republic of Uzbekistan defines the procedure for such monitoring. Simultaneously, creation of special services ensuring protection of State information with limited access in State bodies.

In today's world, the owner of the information resources or their authorized persons will have the right to monitor compliance with data protection requirements and to prohibit or suspend the processing of information if these requirements are not met. In common, it also has the right to address to public authorities for an correctness estimation of norms and requirements performance on protection of the information on information systems. The relevant authorities are also to be determined by the Cabinet of Ministers of the Republic of Uzbekistan. At the same time, these State bodies must observe the conditions of confidentiality of the information itself and the inspection results. Law enforcement agencies must be involved in the prevention of IT-crime. Since prevention is a mandatory part of law



enforcement activities. Otherwise, interdepartmental control bodies, industry-specific administrative bodies, international bodies and public organizations, as well as the direct management of enterprises and organizations where confidential computer information is accessed by responsible information security officers. The practice of combating IT-crimes shows that positive results can be obtained only with the use of a complex of legal, organizational and technical measures to prevent IT-crime. All of which are equally important. Only complement each other form a targeted system of prophylaxis and prevention of IT-crime under investigation.

It is critical to organize a Specialized Anti IT-crime Division under the Tashkent City Department on combating economic crimes at the General Prosecutor's Office of the Republic of Uzbekistan in cooperation with Tashkent City Prosecutor's Office. Whichever includes investigative and operational groups, functioning 24/7, ensuring specialization of the struggle, direct and continuous process of detection and investigation of crimes.

On the grounds, the functions of the group should include coordination and round-the-clock technical support (24/7 contact point), detection and investigation of crimes, international cooperation, scientific and educational activities in this area.

To sum up, we have concluded to counter IT-crime should be raised to the level of law enforcement priorities, the effectiveness of which will be facilitated by the following factors.

Thus, introduction of unit, specializing in IT-crime counteraction, into investigation units of Prosecutor's authorities will provide qualified investigation of crimes of this category. Today, there is no such specialization both on central and regional levels. In the future, there will be a consolidation of operational and investigative services, with a clear vertical subordination and specialisation, including in countering IT-crime.

### **1.3. International cooperation in solving IT-crime issues**

The development of scientific progress in the XXI<sup>th</sup> century gave rise to technological achievements of global significance. This is due to new challenges affecting not only the interests of individuals and States, but also the international community as a whole. By way of introduction, we would like to underscore the appearance of new scientific and technical objects as a result of eternal and constant aspiration of mankind to cognize the world around is a progressive phenomenon. However, the use of these objects can entail both positive and negative consequences. As they are inseparably connected with a number of ethical, political and legal issues of States and individual's responsibility.

According to both foreign and national scientists and research data, IT-crimes have a high degree of social danger and losses from them in some cases may exceed many times losses from other types of well-known criminal acts. It is reasonably argued that IT-crimes are not limited to the framework of a single state. At the same time, the experience of foreign countries in their struggle against this phenomenon testifies that as a result of IT-crimes committing, harm can be caused in almost all activity spheres of the State and society, as well as in individual rights and interests of a particular individual<sup>1</sup>.

With the spread of computer production in the 1950s and the advent of electronic communication technologies in the 1970s<sup>2</sup>, overcoming the negative consequences of the use of new technological advances has gradually transformed from an issue solvable within individual States into a problem of interstate cooperation.

In order to analyze the interstate cooperation problems to counter IT-crime, the definition of IT-crime as an international legal category is of paramount importance.

---

<sup>1</sup> Iglezakis I. The legal regulation of cyber attacks. (Second edition). ISBN 978-94-035-0933-4 – the Netherlands: Kluwar Law International BV, 2016. – P. 28.

<sup>2</sup> Gercke M. Understanding Cybercrime: Phenomena, Challenges and Legal Response – Geneva, Switzerland: International Telecommunication Union, 2012 – P. 13.

At present, the term “IT-crime” is used in a number of international legal instruments.

There is no need to say that international crime is defined as an act arising from a breach by a State of an international obligation. They are so fundamental to the vital interests of the international community that their breach by the international community is considered a crime. When using global computer systems, the provisions of **Article 4** of the International Convention on the Elimination of All Forms of Racial Discrimination<sup>1</sup> will apply.

Here, States’ Parties condemn all propaganda based on ideas of superiority of one race or group of persons of one colour or ethnic origin. Otherwise, texts whichever attempt to propose or promote racial discrimination in any form. Furthermore, **Article 3, Paragraph (c)**, of the Convention on the Prevention and Punishment of the Crime of Genocide<sup>2</sup> prohibits direct and public incitement to commit genocide. Concerning genocide, which can be carried out using information communication technologies. Moreover, computer networks can be used to prepare and coordinate the commission of other international crimes. Also, computers operating military facilities can be directly served as a means of aggression. It seems reasonable to classify international crimes involving the use of information technology as a specific group of IT-crimes.

For the first time, the definition, classification and evaluation of IT-crime was established by the decision of the Council of Europe “Budapest Convention on Cybercrime”<sup>3</sup>.

An attempt to explain the essence of the concept of IT-crime was made by the Eight UN Congress on the Prevention of Crime and Treatment of Offenders<sup>4</sup>.

---

<sup>1</sup> Convention on the Elimination of All Forms of Racial Discrimination of 07 March 1966. – [Electronic resource] – Available at. – URL: <https://www.ohchr.org/en/professionalinterest/pages/cerd.aspx> (Date of review 26.04.2020).

<sup>2</sup> Convention on the Prevention and Punishment of the Crime of Genocide of 09 December 1948. – [Electronic resource] – Available at. – URL: <https://www.ohchr.org/EN/ProfessionalInterest/Pages/CrimeOfGenocide.aspx> (Date of review 26.04.2020).

<sup>3</sup> Convention on Cybercrime of 23 November 2001. – [Electronic resource] – Available at. – URL: [https://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest\\_/7\\_conv\\_budapest\\_en.pdf](https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf) (Date of review 26.04.2020).

<sup>4</sup> Report of Eight United Nations Congress on the Prevention of Crime and Treatment of Offenders. Havana, 27 August – 7 September, 1990. ISBN 92-1-130143-2 – NY, USA, United Nations, 1991 – P. 140.

According to its resolution, “IT-crime is any crime that may be committed using a computer system or network, within a computer system or network, or against a computer system or network”<sup>1</sup>. In other words, any offense committed in the information technology environment may qualify as the IT-crime.

In 2013, the UN Office on Drugs and Crime (UNODC) published a report entitled “Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector”<sup>2</sup>. Here, the concept of “IT-crime” was defined in relation to the context and purpose of the use of the term of IT-crime. Moreover, as highlighted in the report, IT-crimes include not only crimes against the confidentiality, integrity and availability of data. Also, any act aimed at illicit profit-making, content-crimes and other unlawful acts in virtual space. The report notes, however, there is no need for a universal definition of IT-crime. As, for instance, harmonization of rules relating to the collection and provision of digital evidence is more important for international cooperation in investigating crimes. Similarly, this need is not limited to some artificial term “IT-crime”, as electronic carriers and communications may contain information relating to any IT-crime, whether committed in virtual space or outside it<sup>3</sup>.

The authors of the “model law” (2009) on IT-crime of the International Telecommunication Union (ITU) consider IT-crimes much more widely. They relate them with illegal acts committed in virtual space. Where the subject matter is “computers, computer systems, networks, their computer programs, computer data, content data, data movement and users”<sup>4</sup>.

In a way, number of international crimes may could also be committed using computers. Such as acts are provided for in international treaties and interfere with

---

<sup>1</sup> Crimes involving the use of a computer network / Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders //A/ CONF. 187/10.

<sup>2</sup> Malby S., Mace R., Holterhof A., Brown C., Kascherus S., Ignatuschtschenko E. Comprehensive Study on Cybercrime. V.13-80699 – Vienne, Austria, UNODC, February 2013 – P. 11.

<sup>3</sup> Nomokonov V.A., Tropina T.L. Cybercrime: predictions and problems of struggle...; Comprehensive Study on Cybercrime and responses by Member States, international community and private sector // United Nations Document (UNODC/ CCPCJ/EG.4/2013/2: UNODC.Comprehensive Study on Cybercrime, February 2013, P. XVII). (unofficial translation from Russian).

<sup>4</sup> Gercke M. Understanding Cybercrime: A Guide for Developing Countries. – Geneva, Switzerland: International Telecommunication Union, 2009 – P. 17.

normal relations between States. They are detrimental to peaceful cooperation in various fields of relations and penalize organizations and citizens. Such acts are punishable either by the rules set out in international treaties or by national legislation in accordance with those treaties. In particular, they are announced or made public in any way in order to encourage the circulation or trade of pornographic objects. And activities to distribute or trade in pornographic objects through computer networks.

As well as the means of obtaining them, which follows from the provisions of **Article 1** of the International Convention for the Suppression of the Circulation of and Traffic in Obscene Publications<sup>1</sup>.

It is well to bear in mind, various forms of IT related fraud have now become global in scope. Particularly, in banking networks, distribution of software and databases without obtaining the necessary licenses from an owner of the intellectual property rights and other IT offences<sup>2</sup>. Certainly, they raise concerns about the state of international peace and security Reports of “hacking” by hackers of databases and software of the Pentagon appear in the press from time to time.

In order to effectively combat the misuse of information technology, IT-crimes should not be understood in the restricted sense. In this sense, they are understood in the acts of OECD<sup>3</sup> and the Council of Europe. Where a rather limited list of IT-crimes directly related to the disruption of the normal functioning is envisaged. For this reason, define the concept of IT-crimes, the manner in which they are committed should be taken into consideration in the first place internationally.

Thus, all crimes committed with the use of separate computers or information communication technologies should be classified as IT-crimes.

---

<sup>1</sup> Convention for the Suppression of the Circulation of and Traffic in Obscene Publications of 12 September 1923. – [Electronic resource] – Available at. – URL [https://treaties.un.org/doc/Treaties/1950/02/19500202%2006-19%20AM/Ch\\_VIII\\_02p.pdf](https://treaties.un.org/doc/Treaties/1950/02/19500202%2006-19%20AM/Ch_VIII_02p.pdf) (Date of review 01.05.2020).

<sup>2</sup> Mihai I.-C., Ciuchi C., Petrică G. Considerations on Challenges and Future Directions in Cybersecurity. ISBN 978-606-11-7004-3 – Craiova, Romania: Sitech Publishing, 2019 – P. 165.

<sup>3</sup> Organisation for Economic Co-operation and Development. – official website. – [Electronic resource] – Available at. – URL: <https://www.oecd.org/> (Date of review 01.05.2020).

It is not excluded, as computer networks develop, States will agree on new norms containing measures to combat IT-crimes and the range of crimes of an international nature will expand.

IT-crime in the context of global computer networks is transnational in nature. Consequently, it should not only be addressed only in national legislation.

Any country's information security is "a State of security of the country (vital interests of the individual, society and the State in a balanced manner) in the information field against internal and external threats"<sup>1</sup>.

What's more, problems arising in the process of inter-states cooperation in combating IT-crimes as well as problems related to cooperation in suppressing and punishing other categories of crimes, can be divided into the following groups:

- 1) location of the crime scene;
- 2) identification of the crime and extradition of criminals;
- 3) investigation of a crime;
- 4) prosecution, including transfer of proceedings;
- 5) determination of the place of serving a sentence for the committed crime.

With regard to IT-crimes, the issues of locating, identifying and investigating the crime are the most difficult. Not surprisingly, IT-crimes have a high degree of latency<sup>2</sup>. Methods of committing IT-crimes cause significant difficulties in detection. Clearly, as criminals, using computer and access codes, remain essentially anonymous. Moreover, the investigation of such crimes is applicable only through the involvement of highly qualified specialists in the field of information technology. They must have as much knowledge as hackers. On the other side, investigation is also complicated by the actuality the IT-criminal may be in one State and the results of criminal activity may be seen in the territories of other States.

As a study result of a large number of scientific works by various authors, IT-crime has been classified according to the degree of preparedness of users of

---

<sup>1</sup> Bachilo I.L., Lopatin V.N., Fedotov M.A. Information law: Textbook / Under edition of B.N. Topomin. Saint-Petersburg, RF, 2001. – P. 420. (unofficial translation from Russian).

<sup>2</sup> Sun J.-R., Shih M.-L., Hwang M.-Sh. A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure // International Journal of Network Security, Volume 17, No. 5. – Taichung, Taiwan: Asia University, 2015. – P. 500.

criminal “information technology” and their level of qualification. In publications of national and foreign literature<sup>1</sup> five types of users can be found. Thus, A.E. Serejkina notes in her paper, the five selected types of users differ diametrically in terms of computer literacy. At first, **system programmers** are developers of operating (software) systems, translators and other system programs. Next, **applied programmers** make programs for solving special tasks in high-level languages and deal with their debugging and documentation. Third, **programming users**, who are not professional programmers, make up the programs they need to solve their professional tasks. Then, **non-programming users** apply ready-made software products whether do not require programming skills to work with them. Last, **naive (or random) users** are those who first come across a computer<sup>2</sup>.

The FBI’s experience in investigating IT-crime cases demonstrates the active use of officer deployment methods and simulated criminal activity as “subscribers” to social pages containing extremist and terrorist materials to establish direct contact with criminals.

Proceeding from the above and as a practice of IT-crimes investigation, one of the challenges is also the lack of proper interaction with official representatives of social networks (YouTube, Facebook, Instagram, WhatsApp, Twitter, Telegram, VK, OK, etc.)<sup>3</sup> for Uzbekistan.

With regard to the determination of the crime scene, States could establish the relevant rules by concluding a multilateral treaty. It would seem advisable to include in the treaty a provision according to whichever the scene of committing IT-crime should be the territory of the State where the consequences of the committed act occurred. However, where it is known from which computer data entry and other

---

<sup>1</sup> the United Nations Survey of Cybercrime in the United States): Dening, V.; Essing, G.; Maas, S. Man – Computer Dialogue Systems. Adaptation to user requirements (first in English). Moscow: World, 1984. C. 112; Puchkova, I.M. Psychological aspects of professional training of computer users: Author’s abstract. ... Cand. psychol. of sciences. M., 1995. C. 19; Smolyan, G.Ya. Engineering and Psychological Studies of Human Machine Systems // Voprosy psichologii. 1971. № 5. C. 150 – 155; Tikhomirov, O.K.; Babanin, L.N. Computer and New Problems of Psychology. Moscow: Moscow State University Publishing House, 1986. C. Moscow: MSU Publishing House, 1986. P. 204.; etc. (unofficial translation from Russian).

<sup>2</sup> Serjekina A.E. Mental states of computer users in the process of computerized activity: Thesis Abstract. – Kazan, RF, 1998. – P. 16-17. (unofficial translation from Russian).

<sup>3</sup> Proceedings of the Regional Symposium for Central Asia “Combating Cybercrime and Ensuring Information Integrity and Security”, Tbilisi, Georgia, 15–17 October 2018. (unofficial translation from Russian).

acts constituting criminal interference with the functioning of other computers, including those located in the territory of foreign States, the location of such computer should be recognized as the scene of crime committing. Especially, the scene of committing crime may be determined separately for each act, even if it was committed by the same person.

Overall, a more complex issue is the problem of specifying the national authorities that are competent to investigate IT-crimes. In a multilateral treaty, a general rule on IT-crime investigation at the scene of committing crime can be harmonized with a number of exceptions. Firstly, IT-crimes may be committed in the territory of a State whether does not have the necessary technical equipment or expertise to investigate them. In that case, it is applicable to transfer the initiated criminal case for investigation to the authorities of another State after consultation among the competent representatives of the States concerned. Secondly, if computer crimes are committed by the same person, it is available to refer the case for investigation to the authorities of the State where the person has his or her residence place or nationality. Thirdly, if the same person has committed IT-crimes, the effects of which have occurred in more than one State, criminal proceedings against that person may be initiated in each State. Initially, states may then agree, through mutual consultation, to have a case investigated by the authorities of one State or to establish a joint body to investigate the case. Fourthly, it is feasible to transfer the materials of criminal proceedings initiated in connection with an IT-crime to the competent authorities at the residence place or location of the victim. If the investigation of the case by these authorities is in the victim's interest and for the aim of quickly and fully establishing all the circumstances of the case.

Talimonchik V.P. believes, the interests of States to counter IT- crimes can be best served by establishing a system of international control over the transmission of information in computer networks. As well as establishing control over the investigation of offences related to the use of global computer networks and personal



computers with transboundary consequences<sup>1</sup>. Special principles of international information exchange, especially the free, wide and balanced circulation of information, should be respected. On the whole, a system of international control and investigation can only be established if facilities are used whether do not impede the free flow of legitimate information.

We agree, control over the content of information, the most complex crimes investigation or crimes that affect the interests of two or more States, coordination of the national authorities' activities (the proposed division) to investigate IT-crimes should be carried out within the international organization framework.

It is feasible the control of electronic data content and investigation would be part of the functions of INTERPOL<sup>2</sup>. In such a case, however, it should be considered INTERPOL coordinates the cooperation of national criminal police authorities. Combating international crimes is not directly within the competence of INTERPOL. It is likely that a single international organization will be established to coordinate the inter-states cooperation to counter international crimes and IT-crimes. It seems to us that, Uzbekistan could take such an initiative.

More or less, the establishment of an international organization to combat IT-crimes would contribute to the effectiveness of inter-state cooperation in this area. In particular, States lacking highly qualified personnel and developed communication systems would be able to turn to it for assistance. Even States whether have everything necessary for IT-crime investigation need information support for their activities and data on the experience of other States. In other words, crimes that affect the interests of many States and require joint efforts to solve them may be referred to such an organization for investigation.

In order to analyse the status and exchange information on IT-crime among the CIS, SCO and other international organizations, to assess preventive and operational measures taken at the national level and to conduct special training for

---

<sup>1</sup> Talimonchik V.P. Computer crimes and new problems of cooperation of the states // Legislation and economy, № 5, 2005. – P. 17. (unofficial translation from Russian).

<sup>2</sup> International Criminal Police Organization – official website. – [Electronic resource] – Available at. – URL: <https://www.interpol.int/> (Date of review 02.05.2020).

law enforcement officers, it is proved to create an international organization to counter international IT-crime. Namely, the establishment of this organization will make it possible to systematically collect, process and provide information, technical and forensic support to the relevant units of law enforcement agencies. Such an international organization would make it possible to coordinate joint investigations at the inter-State level, as well as specialized education and training for specialists and experts. Apart from, the proposed organization could facilitate the necessary research and software development, assess and analyse existing and potential threats, generate forecasts and issue early warnings.

After all, one can be concluded to counter IT-crime involves both the use of traditional means applied by States (within existing international organizations, as well as bilateral treaties on legal assistance and multilateral treaties on individual offences and on legal assistance in criminal matters) and the creation of new, more effective means.

## **Chapter 2. Particular aspects of some operational and investigative actions during IT-crime investigation**

### **2.1. Particular aspects of Search and Intelligence operations during IT-crime investigation**

Undoubtedly, modern life is based on economic relations connected with active development of information technologies, without which no activity in the world society is possible.

According to the ITU, Internet users increased to 4.1 billion people in 2019. Regarding to the report, 96% of the world's population is now in the zone of access to mobile digital signal. For 93% it is 3G network or more advanced. In Europe, the Western Hemisphere and Asia Pacific region the coverage is 95%, in Arab countries – 91%, in the CIS space – 88%, in Africa – 79%<sup>1</sup>.

In fact, the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan in its report for 2018 states the number of Internet users has increased by more than 20 million people<sup>2</sup>.

However, if we compare the increase in users in Uzbekistan and other countries, Uzbekistan is still fifteen to twenty years behind. Typically, there are also negative points in informatization, namely the emergence of IT-crimes. Considering the certain statistics of the data and experience in revealing and investigation of crimes in the specified direction in Uzbekistan and the United States of America, Great Britain and France, it is available to come to a conclusion the normative maintenance of counteraction to the specified crimes in the United States of America makes more than two thousand, and in Uzbekistan no more than seventy regulating acts.

---

<sup>1</sup> International Telecommunication Union – official website. – [Electronic resource] – Available at. – URL: <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx> (Date of review 07.05.2020).

<sup>2</sup> Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan. – official website. – [Electronic resource] – Available at. – URL: <http://mitc.uz/en/stat/4> (Date of review 07.05.2020) (unofficial translation from Russian).

Unfortunately, the more information technology is involved in commercial trafficking, the greater the need to protect it from illegal activities<sup>1</sup>. From our perspective, the law-enforcement agencies in Uzbekistan are faced with an urgent task. To solve IT-crimes at a high professional level.

According to some statistics of the General Prosecutor's Office of the Republic of Uzbekistan for 2018-2019, in Uzbekistan there was a decrease in crimes in the field of information technologies in terms of number, but an increase by type of IT-crimes (in **2018**, **35** such crimes were registered, of whichever: **13** – under Article **278**<sup>1</sup>. Violation of the rules of informatization, **8** – under Article **278**<sup>3</sup>. Manufacture for marketing purposes or marketing and distribution of special means for obtaining illegal (unauthorized) access to a computer system and telecommunication networks, **5** – under Article **278**<sup>4</sup>. Modification of computer information; the number of crimes related to information technologies decreased in **2019** – a total of **22** of which **2** – under Article **278**<sup>1</sup>, **11** – under Article **278**<sup>2</sup>. Illegal (unauthorized) access to computer information, **2** – under Article **278**<sup>3</sup>, **2** – under Article **278**<sup>4</sup>, **2** – under Article **278**<sup>6</sup>. Creation, use or distribution of malicious programs). We would like to concentrate attention to a reduction in the number of cases in whichever the perpetrators of these crimes are identified. This decrease is particularly characteristic of crimes under Article **278**<sup>1</sup>.

The above data record is the reality whether IT-crimes are latent. Hence, they have a low level of detection. Accordingly, this is a huge field of activity for criminals. It is carried out with the aim of generating profit through criminal means with little chance of being prosecuted.

It is mandatory to zero in the IT-crimes detection, disclosure and investigation is impossible without tactical methods of Search and Intelligence operations. In the first place, carrying out of Search and Intelligence operations is stipulated in **Article 3** of the Law “On Search and Intelligence activities”<sup>2</sup>. We would like to

---

<sup>1</sup> Lee K.R. Impacts of Information Technology on Society in the new Century. – [Electronic resource] – Available at. – URL: <https://www.zurich.ibm.com/pdf/news/Konsbruck.pdf> (Date of review 18.05.2020).

<sup>2</sup> Law of Republic of Uzbekistan “On Search and Intelligence activities” № ZRU-344 from 25.12.2012. – [Electronic resource] – Available at. – URL: <https://lex.uz/docs/2106527> (Date of review 18.05.2020) (unofficial translation from Russian).

provide special focus on such Search and Intelligence operations as make enquiries; sample collection; quick-look; research of items and documents; interception of communications.

As it is known, officers (specialists) of the so-called IT-industry (cellular operators, programmers, etc.) are involved in activities in the field of information technology, whose capabilities are quite wide<sup>1</sup>. Therefore, they can provide information support to the activities of law enforcement agencies to combat IT-crime in accordance with the procedure established by law. In the process of interaction, the latter obtain the necessary access to information resources and may use them for operational and official purposes.

Almost, in order to identify the causes and conditions of committing IT-crimes, certain situations are highlighted:

1. When a crime is committed by professionals through the development and implementation of malicious software products that can stop any business from operating<sup>2</sup>.

2. When ordinary users, for profit and by deception<sup>3</sup>. They post information on the Internet about the sale of expensive items at an undervalue, referring to a share or other fictional basis. Including of consumers, rejoicing at an interesting price, pay them through various electronic payment systems without thinking about who and for what.

Seeing that this information indicates whether previously, to commit the IT-crime, it was necessary to have global knowledge in this area. Now that, with the maintain of software products and instructions on the Internet that will help to illegally access computer information, such illegal actions can be carried out by any person using a personal computer.

---

<sup>1</sup> Zinin A.M., Semikalenova A.I., Ivanova E. Participation of the Specialist in Proceedings: Textbook. Moscow, RF, 2016. – P. 229. (unofficial translation from Russian).

<sup>2</sup> Southern African Fraud Prevention Services (SAFPS). Fraud Prevention. Common fraud scams & how to prevent them – [Electronic resource] – Available at. – URL: [https://www.safps.org.za/Home/FraudPrevention\\_CommonFraudScams](https://www.safps.org.za/Home/FraudPrevention_CommonFraudScams) (Date of review 21.05.2020).

<sup>3</sup> Financial Cryptography. Comments: The Myth of the Superuser, and other frauds by the security community – [Electronic resource] – Available at. – URL: [https://financialcryptography.com/cgi-bin/mt/mt-comments.cgi?entry\\_id=921](https://financialcryptography.com/cgi-bin/mt/mt-comments.cgi?entry_id=921) (Date of review 21.05.2020).

Eventually, the statistics of IT-crimes analyzed above indicates low detection and efficiency of investigation as well as judicial proceedings. In turn, law enforcement agencies face some problems in IT-crimes detection, exposition and investigation. The main ones are normative regulation imperfection of relations and IT-crimes latency.

Currently, significant amounts of information are concentrated in information resources and different technical devices in digital form on various electronic devices and systems. In this connection, operative units are tasked with effectively searching, recording and storing computer information to combat IT-crime.

From a technical point of view, computer information can be obtained:

- when copying data from external information storage devices;
- remotely or directly by accessing memory devices installed in a computer through a computer network;
- through technical channels of communication and intermediate service devices included in them.

The information received may be in the form of texts, photographs, diagrams, video films, documents, etc.<sup>1</sup>.

There are computers in various structures of interest to law enforcement agencies. A number of them are not included in the computer network and are not connected to the technical channel and telecommunication networks. Additionally, they hold so-called “confidential information” from their point of view. A limited number of persons have access to such information. They are the ones who are of great operational interest to law enforcement agencies.

It should be noted, the Law on Search and Intelligence Activities does not fully regulate access to computer data for the purpose of collecting operational and relevant information carried out by the operative units. Inevitably, it is useful to remember, Article 14. “Interception of communications” of the Law on Search and Intelligence Activities gives a comprehensive concept of the specified Search and

---

<sup>1</sup> Efremova M.A. To the question of computer information concept // Russian justice. – № 7. – 2012. – P. 51. (unofficial translation from Russian).

Intelligence operation – an operation consisting in tacit interception and fixation with the use of special technical tools on text, graphic and other information transferred via technical communication channels, which is important for solution of Search and Intelligence activity tasks. As can be seen from the before content of the article, there are no regulations on the removal of information stored in computers not connected to the technical communication channel and telecommunication networks.

As noted by A.L. Osipenko<sup>1</sup>, legislatively such variant of fixation of corresponding measures was offered in the model law “On Search and Intelligence activities” (new edition) (accepted at XXVII plenary session of Inter-parliamentary Assembly of the CIS Member States (the decision № 27-6 from November 16, 2006). Here the mentioned operation was called “monitoring of information and telecommunication networks and systems”. It is described as obtaining information needed to solve specific tasks of Search and Intelligence activities. And also, their fixation by observation with application of special technical tools on electromagnetic characteristics and other physical fields arising during processing of information in information systems and databases and its transmission through electric communication networks, computer networks and other telecommunication systems.

Accordingly, such a definition, overloaded with technical details. To paraphrase, it contains technical inaccuracies and does not give a sufficiently clear idea to the content of the proposed operation. We agree with the opinion of A.L. Osipenko. In the sense the term “monitoring” refers to the collection, analysis and evaluation of information in a particular area. It is an activity of observation of relevant phenomena. Thereby, its use can hardly be considered successful for all those actions aimed at obtaining computer information<sup>2</sup>.

---

<sup>1</sup> Osipenko A.L. New technologies of obtaining and analysis of the Search and Intelligence information: legal problems and prospects of implementation // Herald of Voronezh Institute of Ministry of Internal Affairs of Russia. – № 2 – 2015. P. 13–19. (unofficial translation from Russian).

<sup>2</sup> Osipenko A.L. New Search and Intelligence activity “obtaining of computer information”: content and basis of implementation // Scientific bulletin of Omsk academy of Ministry of Internal Affairs of Russia. – № 2. – 2017. – P. 38–48. (unofficial translation from Russian).

As it is well known, the main way to collect the operative information is to carry out the Search and Intelligence operations. Their list is defined in **Article 14** of the Law on Search and Intelligence Activities. It would seem, the said Law reflects an exhaustive list of Search and Intelligence operations. However, for some reason the legislator has not defined the receipt of computer information as an independent Search and Intelligence operation. Most likely, they considered whether the Search and Intelligence operation – “Interception of communications” – gives an exhaustive notion of access to computer information for the purpose of gathering operative information to combat IT-crimes.

It is worth mentioning the definition given in the Agreement on cooperation among of the CIS members states in the fight against crimes in the field of information technology. Here, computer information is defined as “*information stored in the memory of a computer, on machine or other carriers in a form accessible to the computer or transmitted through communication channels*”<sup>1</sup>.

As it follows from this thesis, the legislators of the CIS foresaw whether interest computer information may be stored on a computer that does not have access to external technical communication channels and telecommunication networks. Such carriers often contain information enables law enforcement agencies to prevent and suppress IT-crime by individuals who pose a danger to society and the State in a timely manner. Definitely, law enforcement practices have shown the IT-criminals, including traditional criminals, often store operational information on computer devices which are not connected to the technical channel and telecommunications networks. These are prohibited terrorist organizations whose leaders and members focused on computers whether contain information on how to produce explosives, the tactics of terrorist activities and so on. It is practically unfeasible to obtain such information without carrying out Search and Intelligence operations. Often IT-criminals and persons involved in criminal activity install programs on computers since are not connected to the external environment, whichever provide for the

---

<sup>1</sup> Agreement on cooperation among of the CIS member states in the fight against crimes in the field of information technology (Dushanbe, 28 September 2018) – [Electronic resource] – Available at. – URL: <https://lex.uz/docs/4748982> (Date of review 18.04.2020). (unofficial translation from Russian).



destruction of the contents of information carriers during unauthorized access to the computer database. Up to a point, they use various programs that make it difficult to obtain information, etc. In brief, receiving such information legally within the framework of the current legislation is one of the primary tasks of law enforcement agencies.

It should be pointed out, the receipt (removal) of information in the memory of such computer by carrying out Search and Intelligence operations is not regulated. To our way of thinking, it is obligatory to *remove information stored in the memory of a computer whether does not have access to a technical communication channel and telecommunication networks, or to obtain information stored in the memory of a computer that is not connected to computer communication networks, should be defined as an independent Search and Intelligence operation – “Receipt of computer information”*.

It has to be noted, expansion the implementation practice of this Search and Intelligence operation will require addressing a whole range of organizational and legal issues. Similarly, normative regulation improvement of ensuring citizens' rights issues. In corresponding normative legal acts powers of the law enforcement agencies which are carrying out Search and Intelligence activities should be specified.

In our opinion, the new Search and Intelligence operation should be referred to the operations which demand the prosecutor's sanction. The said Search and Intelligence operation should be carried out only within the framework of a well-founded operative registration case. Alternatively, the tactics of the mentioned Search and Intelligence operation will be regulated by departmental regulatory documents of the relevant ministries and departments vested with the powers to carry out the Search and Intelligence operations.

Within the framework of the topic theses the one cannot but touch upon the issue of the application of so-called measures to encrypt the information contained in their computers by the inspected officers. It is essential to agree with A.L. Osipenko, the solution of this problem should not be sought so much in the

legal field. Well and how much in the adequate building and technological improvement of the special tools' arsenal used by operative officers.

As it has been mentioned before, the reasons of latency include the absence of material traces during the crime preparing and committing, the variety of ways of crime committing, the difficulty of determining the scene and time of crime committing as well as its event.

Likewise, a malicious programme on the network can be launched in one place. And it is triggered in another place. It is not always applicable to establish territorial boundaries<sup>1</sup>. Nonetheless, computer information can be in one case as a trace carrier of a crime, and in another case, it can be traces of illegal acts.

When scientists describe the traces of IT-crimes, they do not agree on their concept and essence. As the theory of forensics and practice shows, the traces of crime include various changes in the environment, which were formed under the criminal act influence<sup>2</sup>.

In general, the traces of crime are divided into material and ideal. Material traces can be classified as: prints on material objects, items, documents, bodies of victims and others. Ideal traces may include: the prints (events) in the memory, consciousness, citizens (victims, witnesses, criminals, etc.). Based on the special characteristics of the trace formation analysis in IT-crime committing, it can be seen that they do not fit into the above classifications. Therefore, some scientists<sup>3</sup> have concluded whether it is necessary to introduce the concept of “virtual traces” – the average between material and ideal. This position is supported by A.K. Shemetov<sup>4</sup>, Yu.V. Gavrilin<sup>5</sup>, V.A. Milashev<sup>6</sup>. Hence, there may be a need to reconsider the forensic theory of traces formation.

---

<sup>1</sup> Kleijssen J., Perri P. Cybercrime, evidence and territoriality: issues and options // Netherlands Yearbook of International Law 47. 2016. – Netherlands: T.M.C. ASSER PRESS and the authors, 2017 – P. 157.

<sup>2</sup> Belkin R.S. Forensics course. – Moscow, 1999. P. 837. (unofficial translation from Russian).

<sup>3</sup> Meshcheryakov V.A. et al. (unofficial translation from Russian).

<sup>4</sup> Shemetov A.K. On the concept of virtual traces in forensic science // Russian investigator. - № 20 – 2014. – P. 52–54. (unofficial translation from Russian).

<sup>5</sup> Gavrilin Yu.V. Investigation of illegal access to computer information. – Moscow, 2001. P. 88. (unofficial translation from Russian).

<sup>6</sup> Milashev V.A. Problems in tactics of search, fixation and removal of traces in case of illegal access to computer information in computer networks: Thesis Abstract. – Moscow, RF, 2004. – P. 21. (unofficial translation from Russian).

We can confidently say in the IT-crimes exposition, detection and investigation, traces are the main element in the research, examination and restoration of the mechanism of crime committing. Based on practice during IT-crimes exposition, detection and investigation, it needs to identify and investigate traces not only in the technical tools (computers) itself. For example, the receipt and sending of messages, date, time, but also their technical channel of communication. Although, the technical channel may include information on the messages sent, information contained in the operator's equipment in the LOG files, various connection protocols. As noted before, the files may contain text information, images, music, software, etc. Actually, the information which can be obtained to prove a crime is being prepared or committed must be verified as accurately as available. When information collecting, the investigator should stimulate an interest to obtaining information about the name, date of birth, address, telephone number, addresses of other persons, e-mail addresses, personal account number for payment, reference data, IP-address, etc. Moreover, it is also necessary to receive the forgoing information within the framework of Search and Intelligence operations.

Generally, criminal cases on IT-crimes are initiated on the basis of information received during Search and Intelligence activities, or on the fact of the crime committing. When criminal proceedings are instituted on the already fact of the crime committing, after a certain time the necessary information (traces) is not retained by the provider. Accordingly, the investigator does not have the opportunity to restore the mechanism for crime committing in the field of information technology or to obtain evidence. Thus, there is a high probability that the crime will never be solved.

On the whole, the same situation may arise when a criminal case is initiated as the Search and Intelligence activities result. In case of long-term development, the information (traces of a crime) will not be received in time due to its not being preserved or a short period of storage. Therefore, we suggest to take certain measures to remedy this situation.

Namely, to make amendments and modifications to **Article 22** of the Law of the Republic of Uzbekistan “On Telecommunications” № 822-I from 20.08.1999 for inclusion of norms *about duties of operators and providers to store information on facts of reception, transfer, delivery and processing the voice information, text messages from services users via telecommunications networks within three years, concerning the content part (the voice information, photo, video) to establish term of storage till six months*. These additions to the legislation are necessary when carrying out Search and Intelligence operations, as well as investigative actions by law enforcement agencies whichever activity is directed to IT-crimes counteraction.

Finally, economic and financial well-being of Uzbekistan depends on correctness and timeliness of law enforcement agencies actions to IT-crimes counteraction.

## **2.2. Particular aspects of the tactics of Incident Scene Inspection, Search (Seizure), Interrogation of defendant during IT-crime investigation**

It is worthy of note, the knowledge in the area of Search and Intelligence activities alone is not sufficient to counter IT-crimes effectively. In order to fully and comprehensively understand the nature of IT-crimes, a comprehensive investigation of the crime makes it feasible to build the right strategy and tactics to combat IT-crimes<sup>1</sup>.

Consequently, the following investigative actions are carried out at the initial stage of IT-crime investigation: Incident Scene Inspection, Search (Seizure), Interrogation, digital forensics. Furthermore, the complexity of investigative actions lies in the factuality that the Criminal Procedure Code of Uzbekistan does not set forth the rules for collecting and recording digital evidence, since due to the rapid variability of computer systems it is unrealizable to do so. In addition, the development of methods is complicated by the lack of competent experts in departments.

Accordingly, with all the actions taken, an investigator has to organize his own interaction with systems of different levels. In practice, they include the following elements: the computer, computer systems, networks (both global and local), computer user programs, data circulating in these elements<sup>2</sup>.

Inevitably, faced with this challenge, experts suggest using the recommendations of scientific professional organizations<sup>3</sup>.

One of the most important investigative actions during IT-crime investigation is incident scene inspection. This procedural action can be carried out before and after the initiation of criminal proceedings (**Article 137** of the Criminal Procedure Code of Uzbekistan).

---

<sup>1</sup> Ischenko E.P. Forensic science: lecture course. M., 2008., P. 6-8. (unofficial translation from Russian).

<sup>2</sup> Shevchenko E.S. Tactics of separate investigative actions during cybercrimes investigation // Law and right. – № 8. – 2015. – P. 128-138. (unofficial translation from Russian).

<sup>3</sup> Yablokov N.P. Forensics: Workshop – Moscow, RF: Yurist, 2004. – P. 518. (unofficial translation from Russian).

As a rule, Search in IT-crime cases is primarily the computer information inspection. At the initial stage of the investigation of crimes, as stated by I.A. Makarenko<sup>1</sup>, has guiding information. Typically, it is obtained during the investigative search. However, the computer information inspection of is not a complete inspection, but rather a tool check. Therefore, it requires some knowledge of the technical tools used, the operation of which is not always evident. Next, the point is whether human senses are unable to perceive computer information without the interaction of “technical mediators”. Then, computer information, which appears before us in its original form on a display monitor, undergoes quantitative transformations, whichever sometimes turn into qualitative. And in no technical device or software can be sure. Correspondingly, instead of the real file (its contents), the Incident Scene Inspection participants can see a very distorted view. It is not without reason, there is a view whether computer information inspection is generally not acceptable, but that an examination should be conducted. Even the practice does not allow accepting this statement in any way.

To start, preparation for Incident Scene Inspection in cases of this category includes the need to address a number of organizational issues both general to any investigative inspection, and specific, acceptable only for IT-crimes. General includes the invitation of the understood, knowledgeable in information technology, instruction of the inspection participants, specific – mandatory participation during inspection of specialists in different fields of knowledge (forensic experts, as well as IT-experts). Sometimes it is needed to invite not one expert, but even several. The choice of expert will depend on the type of IT-crime and the amount of initial information about the crime committed<sup>2</sup>.

Before Incident Scene Inspection starting, measures should be taken to prepare the appropriate computer equipment, with the assistance of an expert, to be

---

<sup>1</sup> Makarenko, I. A. Tactical features of obtaining information about the identity of the offender in the course of the incident scene inspection // Criminal procedural and criminalistic readings in the Altai: annual inter-regional scientific-practical conference dedicated to the memory of attorney of the Russian Federation, Doctor of Law, Professor E. N. Tikhonov. 7–8. Barnaul, RF, 2008. – P. 266 – 268. (unofficial translation from Russian).

<sup>2</sup> Cengage Learning Course Technology and EC-Council. Computer Forensics. Evidence Collection and Preservation. Volume 1. Investigation Procedures and Response. – NY, USA: EC-Council Press, 2010 – P. 1-17.

used to read and store the seized information. Eventually, software to enable the information copying and analysis on site would also be required.

If the investigator has decided to involve the expert during inspection, the Main Expert and Forensic Center of the Ministry of Internal Affairs of Uzbekistan<sup>1</sup>, the Republican Forensic Examination Center named after Kh.Sulaymonova at the Ministry of Justice of Uzbekistan<sup>2</sup>, “Cyber Security Center” the State Unitary Enterprise as well as non-governmental forensic and expert organizations can provide all possible assistance in this regard. Particularly, they have staff members specializing in the information technology objects research. Basically, in the absence of appropriate experts on staff in any region, the investigator may engage the staff of scientific-research institutes, firms and organizations engaged in the software and hardware development, their operation and repair.

Immediately upon arrival at the incident scene, measures must be taken to ensure the information, stored on the inspected computers and on removable carriers<sup>3</sup>:

- Prevent people working at the time or in the room for other reasons from touching the computer equipment or using the telephone;
- Not to allow anyone to turn off the power to the facility;
- Not to allow anyone to manipulate the computer equipment, if the result is not known in advance, including the investigator;
- Determine whether the computers in the inspected premises are connected to the local network. If there is a local network, the server should be of greatest interest. Since that’s where most of the information is stored. And also, all computers connected to a network to whichever the server has access. It is recommended to

---

<sup>1</sup> Resolution of the President of the Republic of Uzbekistan “On measures to radically improve the activity of the internal affairs agencies in investigating crimes” № PP-2898 from 18.04.2017. – [Electronic resource] – Available at. – URL: <https://lex.uz/docs/3180663> (Date of review 31.05.2020).

<sup>2</sup> Resolution of the President of the Republic of Uzbekistan “On measures to further improve forensic examination activities” № PP-4129 from 17.01.2019. – [Electronic resource] – Available at. – URL: <https://lex.uz/docs/4172026> (Date of review 31.05.2020).

<sup>3</sup> Ndarake Effiong E. Computer Forensics Investigation (Step by step guide). – Nigeria: Efficacy Technologies Limited, July, 2013 – P. 10.

inspect this computer in particular. At the same time, it should be kept in mind that the server may be not one but several computers located in different premises;

- Establish whether the computer is connected to equipment or computing equipment outside the inspected premises;

- Find out whether the computer is connected to a telephone line. If connected, it may receive calls to continue receiving or transmitting information. If information received by the computer via e-mail or other communication may be of investigation interest, it should not be disconnected;

- Determine which operating system is loaded, whichever applications are running and whatever data are entered into the computer. At the same time, the officer should provide the focus to the date and current time on the computer display. Everything displayed on the display monitor should be described in a Protocol and if possible recorded with a photo or video recording<sup>1</sup>.

We agree with D.A. Ilyushin about the use of the tactical method “from the center to the periphery” during Incident Scene Inspection. Depending on the type of the scene, such “centre” (the starting point of the investigation action) may be, for instance, an electronic terminal with the help of which the operation was carried out whichever resulted in causing damage (if the place where the signs of a crime and/or criminal acts were discovered is inspected). Also, the workplace where the means of crime committing was manufactured<sup>2</sup>.

During inspection it is mandatory to consider probability of acceptance by the persons interested in crime concealment, measures on information and other valuable data destruction; probability of installation in inspected computers of special protection frames against unauthorized access whichever, not having received in the established time a special signal or a code, automatically destroy all information stored on the computer or the most important part of investigation

---

<sup>1</sup> It should also be noted that modern computer software using standard tools (e.g. Print Screen keyboard button (sometimes called PrntScrn, PrtScn, PrtScr or PrtSc) or special software allows you to copy a picture of the entire computer screen to the clipboard, after which it can be saved on a medium or printed on a printer.

<sup>2</sup> Ilyushin D.A. Peculiarities during investigation of crimes committed in the sphere of Internet services provision: Thesis Abstract. Volgograd, RK, 2008. – P. 126. (unofficial translation from Russian).



interesting; probability of installation in inspected computers of other information protection frames.

Thereby, the expert participation is extremely important already at the first stage of the Incident Scene Inspection. Apart from, they will help to understand the special computer equipment details, indicate the Seizure subject and prevent intentional or accidental information destruction<sup>1</sup>. Importantly, the inspected objects can be roughly divided into four main groups: office premises; computer equipment; computer data carriers; and documents.

The office premises inspection is necessary for general overview. In doing so, the boundaries of the Incident Scene Inspection are determined<sup>2</sup>. At first, the total number and location of workplaces in the office premises. At second, the specific order of computer equipment and computer data carriers' storage locations is also specified. This will make it affordable in the future to study the possibility of unauthorized entry by persons into the room where the computer is located.

Additionally, in the office premises inspection, it is obligatory to centre on a number of criteria of the inspected premises. First, where it is located (in the administrative building, in a residential building or in a public place or office). Secondly, the security system, alarm system and video surveillance cameras presence. Third, the windows, doors and locking mechanisms conditions<sup>3</sup>.

During the inspection, it is advisable to draw a diagram of the inspected areas, buildings and premises, with the equipment locations on it. In addition, the inspected objects have to be photographed according to the forensic photography rules. Begin with, the general view of the building and the room are shoot. Then, according to the nodal photography rules, individual computers and devices connected to them have to be taken photos. In case of system unit opening, its separate units must be photographed according to the detailed shooting rules. Especially those parts,

---

<sup>1</sup> Hewling M.-O. Digital forensics: an integrated approach for the investigation of cyber/computer related crimes. Thesis Abstract. – Eng, UK: University of Bedfordshire. – P.54.

<sup>2</sup> Bailey W., McAdam T. Law, Science and Experts. Civil and Criminal Forensics. ISBN 978-1-61163-188-3 – North Carolina: USA, Carolina Academic Press, 2014 – P.85.

<sup>3</sup> Topical issues of crime detection and investigation // Investigation bulletin. Issue. 3. Part 2. Kazan, RF: Master Line, 2001. – P. 110. (unofficial translation from Russian).

according to the operating instructions, should not be installed on the motherboard or in the unit's case. This should all be determined by the expert.

In the process of the room inspection, the officer should direct attention to small pieces of paper and scraps with useful information for the investigation. Clearly, they are often attached to the computer or in its close proximity. Therefore, investigator should also make allowance for any traces left on the table where the computer was installed. Moreover, contamination, indentation marks and other signs indicating whether the computer and peripheral devices have been moved and reconnected on site.

In the computer equipment tools' inspection, separate computers can be direct objects. Whichever are not components of local or global networks. There may also be workstations entering into a network. Besides, servers, network communication lines, connection cables and peripheral devices may be also direct objects of separate computers.

In this case, the computer configuration must be installed. In common, all devices, their model numbers and serial numbers are described here. As well as the inventory numbers of each of the devices. All these data are assigned by the accounting department when the enterprise is put on balance sheet. Furthermore, other information on factory labels should be installed too.

According to V.E. Lapshin, one of the main tasks the investigator must be solved during the Incident Scene Inspection is correct description and construction of the initial forensic model<sup>1</sup>.

When inspecting a running computer with the participation of the expert, the officer should determine whichever program is currently running. Also, the type of software loaded into the computer at the time of the inspection. This may indicate the tasks for which this computer was used. If necessary and practicable, the investigator should stop the program execution. At the same time, set what information is received after the program is finished. Then, define and restore the

---

<sup>1</sup> Lapshin V.E. Theoretical basics of the scene inspection // Expert criminalist. – RF, № 3, 2009. – P. 2-5. (unofficial translation from Russian).

name and purpose of the program called before the inspection. After that, the officer should determine the presence of information storage devices in the computer, their type and number. When technically possible, it is customary to copy information such may be relevant to the case.

Most of all, if the computer is connected to the local network, the investigator needs to set the number of workstations connected to the server, type of network connection and number of servers in the network. If applicable, the officer organizes simultaneous inspection of the workstations and computers included in the local network. Alternatively, if this option is not available, he/she should ensure that they are stopped. Next, the investigator continues the inspection in the idle computer mode.

When inspecting the inoperative computer with the participation of the expert, the location of the computer and its peripheral devices should be determined with the obligatory indication in the Protocol of the name, number, model, shape, color and individual criterions of each of them. Then, it is compulsory to establish the connection order between the forgoing devices, the number of connectors and their specifications. If there are wires and cables in them, their type, color and number should be specified. After that, the investigator should find out whether the computer is connected to the network? What is the method and means of its connection? It is also necessary to check visually and to the touch signs of recent work of the computer (heating of the power supply, printer)<sup>1</sup>.

To some extent, computer data carriers' inspection (laser disks, removable USB devices, etc.) is performed in order to establish the content of the computer information itself and detect external traces. In particular, fingerprints may be detected on the packaging and storage places of machine information.

During the Incident Scene Inspection, documents may be discovered and seized, whichever may later be considered evidence in the case:

---

<sup>1</sup> Gerhan D., Larson S., Schroeder J., Woodlan L. Effectively Using Cutting-Edge Computer Forensics in Non-Compete and TradeSecret Cases // Minnesota Continuing Legal Education. Session 509. – Minnesota, USA: Employment Law Institute, 2017. – P. 6.

- Traces of the crime committed (encrypted, handwritten entries, network passwords and access codes, communication diaries);
- Traces of computer hardware and technology. In this connection, the investigator should search for paper media whether may have remained inside the output devices as a consequence of a device malfunction;
- Descriptions of hardware and software;
- Established the rules of work with the computer, regulations governing the rules of work with the given computer, system, network;
- Computer work logs, listings, technical, technological, credit and financial, accounting documentation, etc.

In a way, standard tools and techniques for detecting traces on a computer can be referred to:

- Special programs. Such as, an image is drawn from a data file recorded in \*.jpg<sup>1</sup> format using a special algorithm;
- Hardware and software tools for forensic examination of computer data carriers “EnCase Forensic Edition”. This is a software for collection and analysis of computer data working in the Windows environment. It is intended for forensic research of computer data carriers, based on international specifications and requirements for law enforcement agencies;
- Technical tools like (UFED) – mobile package for digital data collection and analysis<sup>2</sup> and Mosaic+ – mobile suppressor<sup>3</sup>.

During document inspection, special focus should be paid to erasures and corrections in the text, as well as additional records. Especially the absence or the violation of the page numbering of the documents is to be considered. Besides, the glued pages, sheets, forms in the documents. Further, it is important to consider orders on performance of certain works on change of programs for the computer,

---

<sup>1</sup> image storage format. – [Electronic resource] – Available at. – URL: [https://www.tf.uni-kiel.de/matwis/amat/html\\_en/kap\\_4/backbone/r4\\_1\\_2.html](https://www.tf.uni-kiel.de/matwis/amat/html_en/kap_4/backbone/r4_1_2.html). (Date of review 03.06.2020).

<sup>2</sup> Universal Forensic Extraction Device is used to extract, decode and analyse data from various mobile devices: mobile phones, smartphones, tablets and phones with chips manufactured in China.

<sup>3</sup> designed to block the operation of eavesdropping devices and block the operation of mobile phones within the surveyed area, as well as to block the transmission of data by means of devices with chips manufactured in China.

and also orders concerning input of the additional information not provided by technological process. To search for discrepancies of registration forms conducted in the system to the rules established by technical and technological documentation.

During the inspection it is essential to keep in mind the observance of the elementary rules of computer equipment handling. When withdrawing certain computer equipment and computer data carriers, the rules for their packaging and transportation must be observed.

As A.I. Semikalenova notes, if it is an external data carrier, it must be packaged and sealed at the places of opening the package. In contrast, if it is an internal data carrier, which is part of special equipment, it should be separated from the equipment, if available. And to prepare for transfer or transfer together with the equipment, whichever should be packed and sealed to the expert for examination<sup>1</sup>. Particular attention should be paid to the log files Inspection. Primarily, logs are not a direct source of evidence. Meanwhile, the mediator is an expert opinion in a legitimate procedural form or an expert opinion.

Initially, proof force of logs is based on correctness and immutability. These properties have to be observed for the following events. Firstly, the correctness of fixing events and generating records in the generating program. Secondly, the invariability in transferring records from the generating program to the logging one. Thirdly, correctness of record processing in the logging program. Then follows the invariability in storing logs till the moment of seize and correctness in the examination procedure, and also invariability at storage after seize till examination or transfer for examination. Next follows the correctness in interpreting logs. If at least one of these actions is not followed, the log ceases to be evidence.

Doubtless, the procedure for attaching the logs into evidence is presented in the following order. At first, the investigator with the expert in the presence of a representative serving the provider and two witnesses examines the server content.

---

<sup>1</sup> Semikalenova A.I. Forensic software and computer expertise in criminal cases: Thesis Abstract – Moscow, RF: Lawyer, 2005. – P. 97. (unofficial translation from Russian).

OEM<sup>1</sup> software and hardware are used in this process. At second, the investigator compiles the protocol, whichever reflects the characteristics of the server, OS<sup>2</sup> version, the state of the generating and logging program. As well as the presence of logs files, their timestamps, access rights to log files, user accounts, which have the right to write to log files. Certainly, the investigator together with an expert selects the necessary log records, they are printed on the printer and copy all the logs examined to disk. In turn, they are sealed and sent to for examination. At the end, all these are attached to the inspection protocol. All the log sheets are signed by the inspection participants<sup>3</sup>.

It is worth noting, the service providers are careless with log storage, although this is their responsibility. When an accident occurs, many of them refer to ignorance for the saving logs rules. In this regard, it is necessary to introduce administrative responsibility of the telecom's operators for improper performance of their duties, up to including license revocation.

Now that, Search and Seizure, as opposed to Incident Scene Inspection, is carried out only on the initiated criminal case basis<sup>4</sup>. In addition, if the inspection records the state of the incident scene the removal of the found traces and items. During the Search and Seizure, specific items and documents of evidentiary value in the case, as well as criminally obtained valuables are searched and seized (Chapter 20 of the Criminal Procedural Code of the Republic of Uzbekistan).

In IT-crime investigations, Search and Seizure are carried out when there is information about the persons involved in the crime committing. As well as information about the manner, means or scene of the IT-crime and the probable location of the evidence. Search and Seizure tactics also have their own characteristics. This is due not only to the deliberate destruction of information of

---

<sup>1</sup> Object Exchange Model. – [Electronic resource] – Available at. – URL: <http://infolab.stanford.edu/~mchughj/oemsyntax/oemsyntax.html> (Date of review 06.06.2020).

<sup>2</sup> Operating System (Windows, Linux, Unix, BSD, Amiga OS, Mac OS, etc.).

<sup>3</sup> Barbara J. Handbook of Digital and Multimedia Forensic Evidence. – New Jersey, USA: Humana Press – 2008. – P. 36.

<sup>4</sup> Jones N., George E. Fredesvinda Insa Mérida, Uwe Rasmussen, Victor Völzow. Electronic Evidence Guide (A Basic Guide for Police Officers, Prosecutors and Judges) Version 2.0 – Strausbourg, France: Cybercrime Division of the Directorate General of Human Rights and Rule of Law, 2014. – P. 38.

evidentiary value. Besides, it is conditioned by the undetected accomplices or other interested persons among the personnel at the workplace of the defendant or his / her close relatives in the residence place. It is also necessary to give consideration the probability of careless conduct of the investigator and other members of the investigation and operational team, whichever as a result of unqualified handling of the software and hardware can damage information or destroy traces.

The following principles should guide during the Search:

- The information should not be altered during the seizure of computer equipment, removable carriers and their subsequent storage;
- Access to the information and its research on site are permissible when it is unenforceable to remove the medium and send it for examination;
- All operations with computer equipment shall be recorded.

In the preparatory phase of the Search, when selecting experts, it is obligatory to take under advisement the specifics of the computer equipment and the method of access used in the crime committing. With the participation of experts, the officer has to evaluate the data obtained during the information technology criminal case investigation. In doing so, the investigator should take measures the security of the Search site in terms of preservation of evidence. Moreover, it is essential to determine the time and measures to ensure the surprise of the upcoming search (seizure) for both defendants and others who may be in the investigation scene. Apart from, he investigator also addresses the issue of transportation and packaging materials for the removal of seized equipment and carriers.

If it is planned to the apartment search of an individual and if the investigator has reason to believe that the apartment owner will take measures to prevent this investigative action. In this case, the officer is advised to involve neighbors to enter the apartment of the searched person. In any case, the investigator must ensure whether the search is carried out suddenly in order to prevent the information destruction. Also, to prevent the physical destruction of machine data carriers by the defendants. Thereby, the Search in the organization is best conducted in the middle of the working day, if there are grounds for its deposition.

As for the tactics and general rules for the Seizure of computer equipment during the search, they can be summarized as follows:

Seeing that the investigator or other officers take control of the searched premises, including the electric panel. If local personnel cannot be removed from the equipment, all their actions must be recorded in the Protocol. In rare instances where the Search has been reported to accomplices outside the control of the investigator. To illustrate, in the same organization, but one floor above. It is mandatory, as soon as possible, to disconnect network connections and modems. Thus, to paraphrase, with the help of LiteManager Pro remote-control program, a criminal, being in any place, can control power of the searched computer;

Obviously, all connected devices, including peripherals, are not switched off when the search is carried out;

- The computer equipment is then photographed or videotaped. Particular attention shall be paid to the connected cables. For easy fixing and recording, it is compulsory to provide labels for each cable;

- On working computers, the image is recorded on the monitor display and the programs loaded at that moment are marked;

- The search also requires a workplaces inspection for password notes and other data;

- If the printer is printing something, the investigator has to wait until the print is finished. Anything on the output tray of the printer is described and removed;

- After the foresaid steps, the expert turns off computers. If there is no expert due to the search urgency, the desktop is turned off by pulling the cord out of the system power supply by the officer. In addition to disconnecting the notebook from the power supply, the battery is removed without closing the lid. The investigator also removes all computer equipment and carriers that were present at the search time, regardless of their legal affiliation;

- Next, the investigator has to pack all the seized equipment. Each technical device is packed in a separate bag and subsequently numbered;



– The investigator should interrogate all users separately for passwords and network names without waiting to be questioned, as computer information has the property of being easily and quickly deleted. Passwords are not included in the interrogation report or explanation. Also, at this stage, the investigator should make a list of all freelance and temporary experts of the firm. In this way, programmers and other persons who have a labour relations with the victim organization can be found for their subsequent interrogation.

Next, when conducting the Search, the investigator must have an idea of the perpetrator identity. And the officer must also know the level of his or her information technology knowledge. Furthermore, knowledge about the perpetrator's identity allows the expert, for instance, to make the right decision to shut down the computer. As we know, there are two methods to shut down the PC: “cold” and by regular command. When the first one is used (it is done by removing the cord from the power supply or the socket), the information in RAM<sup>1</sup> and other places will be lost., Thereby, the contents of temporary files loaded by current processes on the computer, “live” until the computer is turned off. If the defendant in front of the investigator is a medium or high-level expert, there may be a program on the user's computer. It will trigger when the personal computer is shut down using the standard method, which will destroy the information on the computer (usually hackers equip their computers with a “logical bomb”). In any case, the expert should apply this or that option based on the circumstances of the case: what information is more necessary for the officer.

In continuation of the topic of computer shutdown during the search, I would like to note the following. When during the search it comes to the seizure of the computer, sometimes the defendant tries to impose on the investigator in every way potential method of shutting down the computer. In this case, the defendant hopes whether the method he or she recommends will occur automatically destroy information (as in the situation with a logical bomb). All these actions must be

---

<sup>1</sup> Random Access Memory. – [Electronic resource] – Available at. – URL: [https://www.tutorialspoint.com/computer\\_fundamentals/computer\\_ram.htm](https://www.tutorialspoint.com/computer_fundamentals/computer_ram.htm) (Date of review 09.06.2020).

recorded in the Report. If later, during the computer forensic expert examination of the defendant's computer, it turns out since the method recommended by him would lead to the information destruction on the computer, it indirectly confirms the guilt of the person in crime committing.

Sometimes during the Search, while copying and removing information by the expert, data that exists before the computer is shut down or the session of the program is over, but has not yet been saved, such as the contents of RAM, can be useful. Such data is photographed by the expert at the incident scene. For IT-crimes allegedly committed from the computer under investigation, a list of processes, information on current network connections, and a sample of traffic should be collected.

Afterwards, when preparing, planning and conducting Interrogations of defendants (Chapter 10 of the Criminal Procedure Code of the Republic of Uzbekistan (General rules of interrogation)), the investigator should provide the focus to the committed crime circumstances, the subject and the subjective side. Before conducting interrogation, the officer should consult with the expert. If necessary, the investigator should even invite the expert to take part in the Interrogation and draw up the detailed Interrogation plan together with him or her.

At the initial stage of Interrogation, the following general circumstances are clarified:

- Whether the defendant has computer skills. If so, where, when and under what circumstances he or she has learned to work with computer hardware and specific software?
- The workplace and position of the defendant. Whether he or she works on a computer at his workplace? Whether he or she has lawful access to computer equipment? If so, what types of software he or she has access to? What operations with computer information he or she performs at the workplace of the computer?

▪ Does the defendant have lawful access to the WAN<sup>1</sup> Internet? Does he or she work on the Internet? Whether he or she is assigned identification codes and passwords to work on a computer network at his or her workplace? If he or she is not working, what operations are performed on his or her PC or on the computers of others in his or her immediate environment? Where and from whom he or she purchased software for his or her computer?

▪ What are the circumstances preceding the crime committing by the defendant? When he or she had the intention to commit the crime? What influenced the decision? Why this particular object of attack was chosen? Motives for committing the crime, its purpose, etc.

When interrogating defendants, it is very important for the investigator to clarify in detail the technology of the committed crime or crimes. Besides, the officer should obtain information about what electronic and material evidence of the committed crime is or could be preserved. And also, where it is available to find the information interesting for the investigation.

In the subsequent stage of the Interrogation from the defendant investigator must find out the specific circumstances of IT-crime:

- Place of unauthorized entry into the computer system, i.e. inside the victim organization or from outside?
- How did the intrusion happen? Where is the computer equipment installed?
- How did the defendant access the computer network? What are the ways to overcome the information protection?
- From whom did the defendant obtain data on the information protection measures used in the victim organization and ways to overcome it?
- What means did the defendant use when the crime committing?
- Ways to conceal access to the computer network?
- The number of facts of illegal intrusion?
- Using his or her official position to access the network.

---

<sup>1</sup> Wide Area Network. – [Electronic resource] – Available at. – URL: <https://www.comptia.org/content/guides/what-is-a-wide-area-network> (Date of review 10.06.2020).

During the Interrogation, the investigator receives and records the information in detail in the interrogation Report. Apart from, information on computer operations performed in the last 3-4 days. As well as actions such as: what amount was stolen, what sites were visited, what programs (applications) were installed, etc. In this case, the investigator should exclude the possibility of staging the IT-crime, which happens quite often in practice. This can be avoided by raising additional questions, studying the victim identity, establishing the availability of professional knowledge in the field of information technology for the interviewees and assigning the expert examinations<sup>1</sup>.

In summary, the most important task during the Interrogation of defendants about the circumstances of committing computer crimes is to determine the form and degree of their guilt in the act. Also, the investigator must establish the attitude of defendants to the harmful consequences that have occurred. During the Interrogation of defendants, the circumstances in whichever they committed IT-crime and other crimes for which such access was sought are determined.

---

<sup>1</sup> Inman K., Crim M., Rudin N. Principles and Practice of Criminalistics. The Profession of Forensic Science. – NY, USA: CRC Press, 2001. – P. 77.

### **2.3. Particular aspects of planning and commissioning of computer forensic expert examination during IT-crime investigation**

Virtually all countries in the world regardless of their level of development are subject to IT-crime. However, the openness, transparency and globality of the Internet creates not only criminal problems, but also offers enormous opportunities to effective counter crime. In the first place, new information technologies, including those implemented via the Internet, can and should play an important role in combating asocial behaviour and crime. Therefore, the capabilities of the Internet should be actively introduced into the practice of law enforcement agencies<sup>1</sup>.

Overall, during IT-crime investigation, both traditional types of forensic expert examination and forensic special expert examination – computer forensic expert examination<sup>2</sup> or digital forensics (world practice), correspond verbatim to computer-technical forensics or computer-technological forensics (CIS practice) should be conducted.

Computer forensic expert examinations are necessary both to investigate the information and technological processes proper for the capturing (accumulation, storage, search, actualization and dissemination) of information and its presentation to the consumer in the operation conditions of automated information systems and networks, as well as individual technical and other tools for ensuring these processes.

In comparison, computer forensics is difficult to attribute to investigative actions because, as noted by Sh. Saleem<sup>3</sup>, computer information cannot be perceived by a person directly with his eyes, ears, fingers. It can only be perceived with the help of special technical means. Sh. Saleem's statement cannot be disagreed with. Since computer information resulting from the IT-crime leaves virtual traces.

---

<sup>1</sup> Men J. China's Belt & Road Initiative and EU-China Relations // Proceedings of International Symposium on Policing Diplomacy and the Belt & Road Initiative. June 28 – 30, 2016, Hangzhou, China. ISBN: 978-0-9721479-0-3 / Editors: Yuewei Ge, Lisa Hale, and Jin Zhang. – Georgia, USA: American Scholars Press, 2016. – P. 85.

<sup>2</sup> Nelson B., Phillips A., Steuart Ch. Guide to Computer Forensics and Investigations. (Third edition) – USA: Course Technology, Cengage Learning Inc., 2009 – P. 27.

<sup>3</sup> Saleem Sh. Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics. Thesis Abstract. – Stockholm, Sweden: Stockholm University, 2015 – P. 43.

Essentially, project documentation on development and operation of computer systems and networks can be the direct objects of computer forensic expert examination. The processes of information collection, processing, accumulation, storage, search and dissemination are reflected there. Another object of research is documented information and materials for certification of information systems, technologies and facilities of their maintenance and licensing of activities on formation and use of information resources. And also, there can be administration orders and arrangements, instructions, protocols, contracts, regulations, charters and methods of computer systems and networks operation.

Beginning computer forensic expert examination is assigned in cases when special knowledge of information process technology is required to resolve issues arising during investigation. By tools of computer forensic expert examination, it is possible to determine, for instance, conformity of existing technological process of computer information processing with the design and operational documentation on concrete information system or network. It is also optional to find out specific deviations from the established information technology and the immediate perpetrators' violation of the established information technology. Particularly, the expert examination will also help verify the reliability of organizational and technological measures to protect computer information and the harmful consequences that have arisen as a consequence of an illegal violation of the established technology of computer information processing. Moreover, it is also probable to identify the circumstances since contributed to the criminal violation of electronic information processing technology, etc.<sup>1</sup>

When investigating IT-crime, one must lay account with the actuality considering virtually any treatment of computer information requires special knowledge. The source of such knowledge is an expert and a specialist. It follows whether a special role during IT-crime investigation belongs to digital forensics,

---

<sup>1</sup> Grispos G., Storer T., Glisson W.B. Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics // International Journal of Digital Crime and Forensics, Volume 4, Issue 2 – 2012. – P. 29.

since the facts concerning computer information can be established only on the basis of forensics.

Simultaneously, information interaction between the investigator and the expert takes place in two directions. First, “investigator – expert”, here the investigator must provide the expert with the task and the information necessary for its performance. Second, “expert – investigator”, in this case the expert transmits information to the investigator about the circumstances under whichever questions were asked. However, if the information interaction “investigator – expert” is inaccurate in the outgoing information, then the opposite information interaction will be also with errors<sup>1</sup>.

Importantly, objects of computer forensic expert examination are all tools with whichever access to information resources is provided. When the investigation object is an information carrier, it is better to conduct research with a copy of it to avoid damage to the original. There is no norm in the Criminal Procedure Code of the Republic of Uzbekistan and the Law of the Republic of Uzbekistan “on Forensic Examination” № ZRU-249 from 01.06.2010<sup>2</sup> prohibits conducting research with a copy of the carrier. As a matter of fact, the expert can make a copy on such carrier, which will be more convenient and quicker to work with. The original may be required in the future. Appropriately, directly in court as physical evidence and in the course of repeated or supplementary expert examination. However, there are digital forensics methods, although they are rarely used, whichever require the use of the original in the examination. Accordingly, if the expert, during the Search, for instance, seized a copy of a server disk due to the impossibility of removal the server or its disk in kind, and then it turns out, in order to answer the question posed in the Decree on commissioning of computer forensic expert examination, research of the original is required, the investigator finds himself “in an awkward position”. Thereby, many researchers offer such a solution whether the expert must assume

---

<sup>1</sup> Pisarev E.V. Information interaction between the investigator and the expert. – RF.: Vector of science TSU, № 3 (29). 2014. – P. 211 – 214. (unofficial translation from Russian).

<sup>2</sup> Paragraph “C” of the Articles 167, 168, 169 of the Criminal Code of the Republic of Uzbekistan. – committed by using computer hardware. – [Electronic resource] – Available at. – URL: <http://lex.uz/docs/1633100> (Date of review 13.06.2020).

what questions the investigator will raise to the expert, and what methods will subsequently be used in the study.

Undoubtedly, the main tasks of computer forensic expert examination include determining the technical condition of computer equipment and its suitability. It is used to solve the problems provided by the design and operational documentation for this automated system and technical execution of specific technological information processes and individual operations, whichever became the subject of preliminary investigation. It is also possible, through this examination, to restore the contents of damaged information files and individual files on the carriers, as well as to identify technical causes of computer malfunctions. Besides, it is useful in establishing the authenticity of information recorded on computer carriers and the changes made to them, in detecting illegal modifications, additions and insertions of a criminal nature in the computer programme and in establishing the conformity of information protection devices against unauthorized access, etc.

Generally, when choosing an organization (among the civil ones) that will conduct computer forensic expert examination, preference is given to the experience of the State organization representatives because at present there are no private enterprise and legal entities dealing with them in Uzbekistan.

Indeed, five general branches of computer forensic expert examination can be distinguished depending on the object of the research according to world practice.

**Computer forensics**<sup>1</sup> involves conducting a diagnostic study of the technical (hardware) tools of a computer system, determining the functionality, actual and initial status, manufacturing technology, operating conditions, etc. This branch of expert examination is conducted to research exactly the computer system hardware, i.e. material information carriers. Inevitably, the objects of computer forensics include personal computers, peripheral devices (printers, modems, etc.), network hardware (servers, workstations, active equipment, network cables, etc.),

---

<sup>1</sup> Corby M. Computer Forensics. Data Security Management. – [Electronic resource] – Available at. – URL: <http://www.ittoday.info/AIMS/DSM/82-03-71.pdf> (Date of review 14.06.2020).



components (hardware blocks, expansion cards, memory chips, magnetic tapes, hard disk drives, solid state drives, flash cards, memory cards, etc.) and other means.

**Database forensics**<sup>1</sup> consists in studying the operational goal, characteristics and system requirements, algorithm and structural attributes, user (consumer) state of the system, application and author's software of the computer system as specific objects of expert examination submitted for research. One word, this branch is intended for research of computer system software.

**Forensic data analysis** is conducted for the purpose of expert examination aimed at search, detection, analysis and evaluation of information prepared by a user or generated (created) by programs to organize information processes in the computer system. This branch of expert examination implies resolution of diagnostic and identification issues related to computer information.

**Network forensics** involves the study of the functional purpose of computer tools whether implement any network information technology. It is aimed at solving hardware, software and information aspects of establishing facts and circumstances in cases. Accordingly, the facilities operate in the network<sup>2</sup>.

**Mobile device forensics**<sup>3</sup>. The objects of this branch of expert examination include mobile phones, smartphones, tablets, sim-cards, as well as components, etc.

Clearly, computer forensic expert examination during IT-crime investigations are often assigned at the initial stage of the investigation. Once the Incident Scene Inspection, Search and Seizure are done. However, when there is insufficient information for further investigation, the officer makes the Decree on the need to appoint the computer forensic expert examination of the objects found and/or seized in the investigative actions.

After deciding on computer forensic expert examination, the investigator is faced with the challenge of specifying the branch of computer forensic expert

---

<sup>1</sup> Bhawan N. Cyber Crime Investigation Manual. – New Delhi, India: Swati Communications, 2011. – P. 20.

<sup>2</sup> Gladun A., Rogushina J. Застосування онтологічного аналізу для обробки великих даних у домені кібербезпеки. – Kiev, Ukraine: ИНСТИТУТ ПРОБЛЕМ РЕГИСТРАЦИИ ИНФОРМАЦИИ НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК УКРАИНЫ МАТЕРИАЛЫ XIX МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ (ВЫПУСК 19) – P. 49-58. (unofficial translation from Ukrainian).

<sup>3</sup> Pollard C., Anzaldua R. Computer Forensics for Dummies. – Indianapolis, Indiana, USA: Wiley Publishing Inc, 2008 – P. 219.

examination. As noted by M.M. Menzhega, indication by the investigator of this or that branch of digital forensics may lead to unnecessary complication of the aim of the expert examination. Otherwise, it will lead to difficulties during the expert examination or when answering the questions posed<sup>1</sup>. V.V. Polyakov and A.V. Shebalin hold a similar viewpoint. They point out that it is enough for the investigator to note the branch of computer forensic expert examination. Typically the expert, having analyzed the questions and assessed the objects, will determine the branch of digital forensics himself<sup>2</sup>. However, one cannot agree with their opinion, as the expert does not determine the branch of computer forensic expert examination on his own.

Not surprisingly, the complexity of digital forensics lies in its understanding by other participants in the litigation. Since it is difficult for the expert to explain in simple words the mechanism of the committed crime and the conclusions made on the basis of the research. Sometimes it is difficult to translate a technical term into a language accessible to the general public, let alone a legal term. As a consequence, some concepts cannot be explained at all without using a technical dictionary. Seeing that, only two participants understand what we are talking about at the trial stage. These are the expert and the defendant.

At the same time, the constant creation of the newest information systems, communication technologies, computer equipment and their improvement are a favorable basis for the emergence of new global threats to information networks and society as a whole<sup>3</sup>.

Strengthening the logistical capacities of units specializing to counter IT-crime is also an important task. Practice shows that the current state of technical equipment of the units lags far behind IT-criminals in Uzbekistan. At this stage, they

---

<sup>1</sup> Menzhega M.M. Technique of investigating the creation and use of computer malware. Moscow, RF.: Jurlitinform, 2010. – P. 122. (unofficial translation from Russian).

<sup>2</sup> Polyakov V.V. Shebalin A.V. To the question about assignment of the computer forensic expert examination, the object of which is a smartphone on crimes in the sphere of computer information: Collection of criminalistic readings – Barnaul, RF, 2013. – P. 85. (unofficial translation from Russian).

<sup>3</sup> Rasulev A.K. The criminological characteristic of crimes in the sphere of information (computer) crimes // Вопросы современной юриспруденции: сб. ст. по матер. LVIII междунар. науч.-практ. конф. № 2(53). – Новосибирск: СибАК, 2016. – [Electronic resource] – URL: <https://sibac.info/conf/law/lviii/47211> (Date of review 16.06.2020) (unofficial translation from Russian).

are using modern information and communications technology and special means. Such “advance” of the criminal world in virtual space has a negative impact on the detection of IT-crime and bringing perpetrators to justice. Therefore, in our view, Special Computer Forensic Centre should be established at the offered Anti IT-crime Division under the Department on combating economic crimes at the General Prosecutor’s Office of the Republic of Uzbekistan. In brief, it will assist in testing and research work in the area of conducting digital forensics. The centre will serve as a kind of “testing ground” for the latest means of protection against computer viruses, malware, hacking, etc.

Another challenge is the drafting of questions. As N.N. Fedotov notes, investigators have problems when posing questions for computer forensic expert examination. Up to a point, it is related to the lack of knowledge in the field of information technology, as well as lack of understanding in special terminology<sup>1</sup>.

The complexity of computer forensic expert examination also lies in the ambiguity of answers received by the investigator, judge, prosecutor, or advocate to questions posed to the expert at the stage of the court hearing. In other words, two different answers can be obtained to the question whether the IP-address of the computer on the Internet unambiguously identifies it. A negative answer can be given, meaning an abstract computer and any IP-address. But an affirmative answer can be given for a particular computer and a particular address. If the officer looks at the case file. Thus, the experts now not only explain the questions. In fact, they draw conclusions about the guilt or innocence of a person.

Provided that the investigator should clearly present the possibilities of digital forensics in order to correctly formulate questions and get the expected answers to them. Paradoxically, in order to ask a question correctly, one should know most of the answer, and somewhere the full answer. In short, the investigator should have basic knowledge of information technology. It is clear, in order to formulate

---

<sup>1</sup> Fedotov N.N. Forensics – computer forensics. Moscow, RF.: Legal World, 2007. – P. 254 – 255. (unofficial translation from Russian).

questions for computer forensic expert examination it is better to always involve the expert who will conduct the study.

However, the development of universal list of questions is an extremely difficult task. Because each IT-crime has its own characteristics and requires a non-trivial approach.

Despite, in order for the digital forensics question list to be correctly compiled, the investigator need to consider some specific criterions.

At first, the questions should not be legal (e.g., is the subject of the research forgery?), should not affect the cost of the subject of the research (e.g., what is the cost of the subject of the research?) and should not cover translation of text, correspondence, etc.

At second, questions should have technical nature (e.g., what is the general characteristics of the software presented, what components (software tools) does it consist of?). In spite of the question may concern the clarification of jargon and computer terms.

At third, the questions should be based on the objectives of the study (identification or diagnostic).

Still, when formulating questions, the investigator should not specify the type and content of information to be found, studied and attached to the case. Because the expert will decide for himself what information is relevant to the case. For this purpose, the expert should be acquainted with the criminal case in the part whether relates to the matter of expert examination or the factual allegations of the case can be set out in the Decree on commissioning of computer forensic expert examination. If there is a lack of information, the expert may request additional material.

Unlike, when searching for digital traces of various kinds of computer actions, it is better to formulate questions not about traces but about actions. It should be remembered, although, the expert can determine when, how, and who performed the illegal access. Also, it is possible to determine this only in rare cases when the computer under expert examination contains some information about the user.

When expert examining individual files, disks and other carriers, it makes sense for the investigator to question not only the presence of particular content on the carriers, but also about the detection and decryption of hidden, proprietary and other information. Usually, such information is provided by the appropriate file format (as the case may be). In addition, the investigator may include the issue of recovering erased files, even if the carriers have been formatted several times. In this case, it is obligatory to find out the way of the information appeared on the carriers. When a file cannot be recovered, it is probably to prove its presence in the past by information about the file, whichever can be stored in different places. On the contrary, when researching malware and hardware, it is sometimes necessary to study more than just its properties and functionality. It also requires learning about the origin, creation process and comparison of versions. In this case, it is recommended that two separate expert examinations be conducted as part of the software and hardware examination. The first one examines the contents of computer carriers. The second will consider the attributes of detected programs<sup>1</sup>.

At study of ICQ<sup>2</sup> archives it is essential to mean whether in any case at reception or sending of the message the information on it is written down on a disk at least once. Additionally, it means that if not in the explicit, it can “pop up” in the latent form at expert examination. In archive on the computer the user can store a large number of messages, including their copies. As a consequence, it is better to ask the expert to detect all correspondence, both in the explicit and remote form. Accordingly, the investigator should not give the task, find and print all the correspondence, or reduce the work to the detection of a single letter. Those messages such are relevant to the case will be printed out and attached to the Expert Testimony. The rest of the messages will be burned to a CD<sup>3</sup> because supplementary expert examination may be required.

---

<sup>1</sup> Malin C., Casey E., Aquilina J. Malware Forensics Field Guide for Windows Systems. – MA, USA: Elsevier, 2012. – [Electronic resource] – Available at. – URL: <http://index-of.es/Varios-2/Malware%20Forensics%20Field%20Guide%20for%20Windows%20Systems.pdf> (Date of review 18.06.2020).

<sup>2</sup> “I Seek You”. – [Electronic resource] – Available at. – URL: <https://techterms.com/definition/icq> (Date of review 18.06.2020).

<sup>3</sup> Compact Disk. – [Electronic resource] – Available at. – URL: <https://www.britannica.com/technology/compact-disc> (Date of review 18.06.2020).

Likewise, it is better for the investigator to entrust the expert with the question of attributing this or that correspondence to the materials of the criminal case. For this reason, the investigator should acquaint the expert with the materials of the criminal case. Besides the discovery of the archive, the investigator should also raise the question of whether the discovered messages were received or sent. In practice, the investigator should know where the message was sent, i.e. the second correspondent. If it is not known to the investigator, it needs to raise the question to the expert about where else it is practicable to find out a copy of the given message or traces of its stay.

At studying printed documents, the investigator should be borne in mind that all printouts are considered on an equal footing with electronic carriers by the expert. Since the information on electronic carriers is presented in digital form. Importantly, the printouts contain not only human-oriented information, but also machine oriented information, too. To illustrate, the U.S. printer manufacturers put a printout on each page of hidden information about the date, time and serial number of the printer. In addition to this information, the printer has its own individual criterions inherent to each model. Therefore, the expert examination can not only “tie” the printed document to the particular printer, but also determine on the printer what model it was printed.

The appointment of computer forensic expert examination is very important for the collection of evidence. Hence, the investigator should provide the expert with materials for the study. Such materials include the seized objects during the Incident Scene Inspection, which were mentioned above. If it is not possible to provide the expert with devices for the examination, it is reasonable for the investigator to make a copy of the hard disk at the crime scene, for example, in the organization or premises<sup>1</sup>.

What’s more, the study of the user identity under study is carried out considering the intensity of human use of the computer. Documents, photos, music,

---

<sup>1</sup> Wolf J.-P. An Ontology for Digital Forensics in IT Security Incidents: Diplomarbeit. – Germany: Universität Augsburg, 2014. – P. 65.

correspondence, settings, availability of programs, etc. – all this individualizes the information content of the computer. Furthermore, they reflect the intellect, abilities, inclinations and preferences of the user. Thereby, to assess the user identity of the computer under study should conduct a comprehensive examination by conducting digital forensics and forensic psychological analysis. At the same time, they both need to remember that in order to assess the identity qualification, it is critical to find on the user's computer the results of his intellectual activity, i.e. programs written by him.

Most of all, the forensic literature notes such possibility of digital forensics as confirmation or denial of the “digital alibi”<sup>1</sup> of the defendant who claims to have worked at his computer at the certain time. Although it is not IT-crime in this case, the digital forensics examination is mandatory for checking the alibi.

According to the results of the expert examination, the investigator will have to do a lot of work together with the operational officers by conducting investigations and Search and Intelligence operations to determine whether IP-addresses belong to specific individuals. For instance, such requests may be inquiries to hosting providers to obtain data about the IP-address (server) owner, which are served by mentioned provider. When recording register servers, the user provides the data, mainly it is a telephone number, postal address, residence address, but some hosting providers in their security policy require to provide passport data as well, which will simplify the procedure of criminal identifying<sup>2</sup>.

In general, the expert is faced with questions relating the availability of relevant information on the objects under examination. Exactly what's relevant to an investigative case. In particular the suitability the objects under examination for certain purposes and actions performed using objects, their time and sequence.

---

<sup>1</sup> Ewing A. Digital Footprints in the Snow, Understanding Timestamps and Metadata for Legal Cases // the barrister – The largest independent magazine for Barristers practicing in the UK. – April 15, 2019. – [Electronic resource] – Available at. – URL: <http://www.barristermagazine.com/digital-footprints-in-the-snow-understanding-timestamps-and-metadata-for-legal/> (Date of review 20.06.2020).

<sup>2</sup> Carr J. Inside Cyber Warfare. Second Edition. Mapping the Cyber Underworld. – Sebastopol, Ukraine: O'Reilly Media, 2012. – P. 132.

Especially important is the identification of electronic documents, computer programs and properties of the programs.

From these facts, one may conclude that any investigative action carried out during IT-crime investigation will require special knowledge. This knowledge is needed first and foremost in order to know where to look for crime traces, and then to correctly consolidate and process of evidence. In a nutshell, the role of computer forensic expert examination should be particularly emphasized. Owing to its modern capabilities, it allows to detect falsification of log files, which are a reference point for the investigation in the criminal identity.



## Conclusion

The results of research, analysis of theoretical and legal sources indicate the need for further academic study of the problems undertaken. Thereby, researches of a modern condition of counteraction to IT-crimes in the Republic of Uzbekistan show that its level at present does not correspond to reality. Importantly, there is a need for complex coordination of measures on combating crimes on the national scale.

Summing up the study developed the following main theoretical conclusions and scientific recommendations to improve the tactics of operational and investigative actions in the IT-crime investigation. It is also possible to formulate practical solutions and methodological bases for improving existing legislation aimed at enhancing the efficiency of combating IT-crime in the Republic of Uzbekistan.

1. Now that, it is offered to define “information technology crimes” as *socially dangerous acts (actions and inactions), committed both intentionally and carelessly, causing or creating a threat of real infliction of essential damage or material damage to social relations in the sphere of information technologies.*

2. Apart from, a legal analysis of criminal legislation of Uzbekistan on combating IT-crime has revealed a number of gaps, contradictions and omissions in national legislation. In particular, it seems advisable to provide in the Article 125. Divulgence of adoption secret, Article 130. Production, importation, distribution, promotion, demonstration of obscene products, Article 139. Defamation, Article 140. Insult, Article 141<sup>1</sup>. Violation of privacy, Article 155. Terrorism, Article 176. Manufacturing, sale of forgery money, excise stamps or securities, Article 179. False entrepreneurship, Article 180. False bankruptcy, Article 181. Suppression of bankruptcy, Article 181<sup>1</sup>. Premeditated bankruptcy, Article 191. Illegal collection, divulgence or use of information, Article 243. Legitimization Laundering of Proceeds from Criminal Activity and

Article 251<sup>1</sup>. Illicit traffic in superpotent and psychotropic substances – for the next qualifying feature:

*“by using Computer Equipment either Mass Media or Telecommunication Networks and Internet”*

3. In addition, it is offered that the following additions to the Article 255<sup>1</sup>. Development, manufacture, stockpile, acquisition, transfer, keep, illegal possession and other activities involving bacteriological, chemical and other weapons of mass destruction the advice, drawings, recommendations on their manufacture posted, Article 270. Growth of prohibited crops, Article 273. Illicit manufacture, acquisition, keep and other activities with narcotic drugs, their analogues or psychotropic substances for marketing purposes or marketing, Article 276. Illicit manufacture, acquisition, keep and other activities with narcotic drugs, their analogues or psychotropic substances without marketing purposes, Article 209. Forgery in public office, Article 210. Passive bribery, Article 211. Active bribery, Article 212. Complicity in bribery, Article 163. Loss of documents containing State secrets and Article 230<sup>1</sup>. Falsification (forgery) of Evidence be made with the following qualifying feature:

*“by using Computer Equipment or Telecommunication Networks and Internet”*

4. In practice, countering IT-crime should be raised to the level of law enforcement priority. Due to the fact that a large number of financial and banking institutions, educational institutions, industrial enterprises and institutions with various forms of ownership and others are located in the center of the Republic of Uzbekistan – in Tashkent city. Accordingly, it is suggested that a Specialized **Anti IT-crime Division** for combating IT-crime be established as an experiment in the Tashkent City Department on combating economic crimes at the General Prosecutor’s Office of the Republic of Uzbekistan, with the right to investigate. The establishment of specialized unit to combat IT-crime, comprising investigation and operational teams, will contribute to the effectiveness of the IT-crime counteraction. It will be operational 24/7 contact point. In accordance with international

recommendations, the suggested law-enforcement body will ensure the specialization, immediacy and continuity of the IT-crime detection and investigation process.

In the future, the association of operational, investigative and forensic services under the General Prosecutor's Office of the Republic of Uzbekistan will organise a clear vertical reporting line and specialization. This will include combating IT-crime, which should yield positive results and speed up the mechanisms for investigating IT-crime. In general, these actions are aimed at meeting modern requirements for combating IT-crime.

5. With a view to assessing and exchanging information on IT-crime, evaluating national preventive measures and operational activities and conducting specialized training for law enforcement officials between countries, it is recommended that an international organization to counter international IT-crime be established. The formation of that organization will make it possible to systematically collect, process and provide information, technical and forensic support to the relevant law enforcement units. Such an international organization would make it possible to coordinate joint investigations between States, as well as specialized education and training for specialists and experts. The offered organization can facilitate the necessary research and software development, assess and analyse existing and potential threats, generate forecasts and issue early warnings.

Currently, significant amount of information is concentrated in information resources and different technical devices in digital form on various electronic devices and systems. In this regard, operative and investigative units are challenged to effectively capture, fix and accumulate computer information to combat IT-crime.

6. In view of the need to regulate the removal of information stored in computers not connected to the technical communication channel and telecommunications networks, it is proposed to amend and supplement **Article 14** of the Law of the Republic of Uzbekistan "On Search and Intelligence activities" №

ZRU-344 from 25.12.2012. The new Search and Intelligence operation shall be carried out with the approval of the prosecutor. And to look as follows:

*Receipt of computer information – removal of information stored in the memory of a computer whether does not have access to the technical communication channel and telecommunication networks, or obtain of information stored in the memory of a computer that is not connected to the computer communication networks.*

7. Next, in order to improve mechanisms to recover the commission of IT-crime offence for obtaining evidence in the detection and investigation of criminal cases. Amendments and additions are proposed to Article 22 of the Law of the Republic of Uzbekistan “On Telecommunications” № 822-I from 20.08.1999 in order to include norms *about duties of operators and providers to store information on facts of reception, transfer, delivery and processing the voice information, text messages from services users via telecommunication networks within three years, concerning the content part (the voice information, photo, video) to establish term of storage till six months.*

8. Then, it is necessary to review and introduce a special system for the recruitment of officers in law enforcement agencies and expert subdivisions – operational officers with technical education. We believe that it is possible to use the positive experience of foreign countries that attract to the positions of operational officers and specialists the persons with technical education, as a rule, with legal training courses. At the initial stage, such a requirement can be established for operational officers.

The following are the most important provisions of forensic tactics for IT-crime investigation at the current stage. Such as rational tactical techniques of investigators in the preparation and conduct of some investigative activities and forensic tactical recommendations will contribute to the development and establishment of computer forensics.

9. Moreover, when formulating the concept of trace in digital forensics, it is recommended to proceed from the following methodological prerequisites. First, the

trace reflects to IT-criminal's activity. Second, the trace is an integrative system reflecting the specialties of a IT-criminal's identity, a process or an action of a computer system in IT-crime committing. The definition of a trace, formulated in this form, allows us, in our opinion, to cover the whole variety of traces occurring during IT-crime committing.

The main tasks of interrogation in the IT-crimes cases investigation are as follows. Identification of elements of IT-crime composition on the basis of trace information and determination of time, scene, method and motives of IT-crime commission. The effectiveness of solving the above tasks depends to a large extent on preparation for the production of investigative actions.

**10.** Besides, Search and Seizure during IT-crime investigation involve obtaining evidence of how the crime was committed. It involves the use of computer equipment and telecommunications networks. The purpose of the Search in the IT-crime investigation is to detect and seize computer equipment. Where traces of computer information relating both to the IT-crime itself and to the perpetrators (information on their location or movement) remain. As well as objects resulting from the crime (product), e.g. counterfeit computer programs, malicious programs. In addition, documents containing important information for the case, e.g. receipts; notebooks with personal records; documents on transfer, cashing, etc. The productivity of the search and seizure during IT-crime investigation is largely due to the careful preparation of the case.

**11.** Starting with the decision on the need to appoint the computer forensic expert examination, the investigator must communicate with the expert. Information interaction between them takes place in two directions. Initially, investigator to expert, where the investigator must provide the expert with the task and the information necessary for its performance. And back, expert to investigator, where the expert transmits information to the investigator about the circumstances under which the questions were asked. In interaction, the investigator may also ask for advice to determine the specific type of forensics, explaining the case summary and show him the available materials for the appointment of expert examination. The

type of expert examination correctly defined in the course of the appointment will reduce the time of the digital forensics.

**12.** Finally, In order to improve the qualitative evidence during IT-crime detection and investigation, it is suggested to establish the **Special Computer Forensic Centre** within the mentioned Department on combating economic crimes at the General Prosecutor's Office of the Republic of Uzbekistan. The Centre will assist in ensuring quality computer forensic expert examination, conducting testing and research work in this area, as well as testing protective equipment in the area of information technology.

In conclusion, the challenge of countering IT-crime is complex. Its realization is linked to the conduct of ongoing scientific research primarily in the fields of criminology, criminal law, criminal procedure, forensics, Search and Intelligence activities and other sciences. The elaboration of clear initiatives to counter IT-crime will help to ensure the purpose and objectives of national security in the Republic of Uzbekistan.

## **List of literature references**

### **I. Fundamental literature:**

1. Mirziyoev Sh.M. Critical analysis, strict discipline and personal responsibility should become a daily norm in the activity of each manager. Report of the President of the Republic of Uzbekistan at the extended session of the Cabinet of Ministers dedicated to the results of socio-economic development of the country in 2016 and the most important priority directions of the economic program for 2017.

2. Karimov I.A. Our main task is to further develop the country and improve the welfare of the people. Report of the President of the Republic of Uzbekistan at the meeting of the Cabinet of Ministers dedicated to the results of socio-economic development of the country in 2009 and the most important priorities of the economic program for 2010.

### **II. International laws and regulations:**

1. Convention for the Suppression of the Circulation of and Traffic in Obscene Publications of 12 September 1923.

2. Convention on the Prevention and Punishment of the Crime of Genocide of 09 December 1948.

3. Convention on the Elimination of All Forms of Racial Discrimination of 07 March 1966.

4. The Okinawa Charter on Global Information Society. One of the four documents issued at the G8 Summit Meeting at Kyushu-Okinawa on 21-23 July, 2000.

5. Vienna Declaration on Crime and Justice from April 2000.

6. Convention on Cybercrime of 23 November 2001.

7. Doha Declaration on integrating crime prevention and criminal justice into the wider United Nations agenda to address social and economic challenges and to

promote the rule of law at the national and international levels, and public participation from April 2015.

8. Agreement on cooperation among of the CIS member states in the fight against crimes in the field of information technology from 28 September 2018.

### **III. National laws and regulations:**

1. Criminal Code of the Republic of Uzbekistan from 22.09.1994.

2. Criminal Procedure Code of the Republic of Uzbekistan from 22.09.1994.

3. Law of Republic of Uzbekistan “On Search and Intelligence activities” № ZRU-344 from 25.12.2012.

4. Law of Republic of Uzbekistan “On guarantees and freedom of access to information” № 400-I from 24.04.1997.

5. Law of Republic of Uzbekistan “On telecommunications” № 822-I from 20.08.1999.

6. Law of Republic of Uzbekistan “On the principles and guarantees of freedom of information” № 439-II from 12.12.2002.

7. Law of Republic of Uzbekistan “On Informatization” № 560-II from 11.12.2003.

8. Law of Republic of Uzbekistan “On electronic digital signature” № 562-II from 11.12.2003.

9. Law of Republic of Uzbekistan “On electronic document flow” № 611-II from 29.04.2004.

10. Decree of the President of the Republic of Uzbekistan “On Strategy of Actions on Further Development of Uzbekistan” № UP-4947 from 07.02.2017.

11. Resolution of the President of the Republic of Uzbekistan “On measures to radically improve the activity of the internal affairs agencies in investigating crimes” № PP-2898 from 18.04.2017.

12. Resolution of the President of the Republic of Uzbekistan “On measures to further improve forensic examination activities” № PP-4129 from 17.01.2019.



#### **IV. Foreign laws and regulations:**

1. Computer Crimes Act tit. XLVI Chapter 815 of 1978.
2. Protection of children UK Act of 1978.
3. Telecommunications Act of 1984.
4. Computer Fraud and Abuse Act (CFAA) of 1986.
5. Data Protection Act of 1998.
6. Computer Misuse Act of 1990.
7. Terrorism Act of 2000.
8. Anti-Terrorism Act of 2001.

#### **V. Foreign monographs, scientific articles and collections:**

1. Bailey W., McAdam T. Law, Science and Experts. Civil and Criminal Forensics. ISBN 978-1-61163-188-3 – North Carolina: USA, Carolina Academic Press, 2014 – 336 p.
2. Barbara J. Handbook of Digital and Multimedia Forensic Evidence. – New Jersey, USA: Humana Press – 2008. – 139 p.
3. Bhawan N. Cyber Crime Investigation Manual. – New Delhi, India: Swati Communications, 2011. – 135 p.
4. Gercke M. Understanding Cybercrime: Phenomena, Challenges and Legal Response – Geneva, Switzerland: International Telecommunication Union, 2012 – 356 p.
5. Inman K., Crim M., Rudin N. Principles and Practice of Criminalistics. The Profession of Forensic Science. – NY, USA: CRC Press, 2001. – 372 p.
6. International Journal of Information Security and Cybercrime. Volume 8, Issue 2, DOI: 10.19107/IJISC.2019.02 – Bucharest: Romanian Association for Information Security Assurance (RAISA), 2019. – 86 p.
7. Jones N., George E. Fredesvinda Insa Mérida, Uwe Rasmussen, Victor Völzow. Electronic Evidence Guide (A Basic Guide for Police Officers, Prosecutors

and Judges) Version 2.0 – Strausbourg, France: Cybercrime Division of the Directorate General of Human Rights and Rule of Law, 2014. – 199 p.

8. Malby S., Mace R., Holterhof A., Brown C., Kascherus S., Ignatuschtschenko E. Comprehensive Study on Cybercrime. V.13-80699 – Vienne, Austria, UNODC, February 2013 – 287 p.

9. Mihai I.-C., Ciuchi C., Petrică G. Considerations on Challenges and Future Directions in Cybersecurity. ISBN 978-606-11-7004-3 – Craiova, Romania: Sitech Publishing, 2019 – 340 p.

10. Dunn M., Wigert I. Critical Information Infrastructure (CIIP) Protection Handbook. – Zurich, Swiss: Swiss Federal Institute of Technology Zurich, 2004. – 403 p.

11. Ndarake Effiong E. Computer Forensics Investigation (Step by step guide). – Nigeria: Efficacy Technologies Limited, July, 2013 – 21 p.

12. Nelson B., Phillips A., Steuart Ch. Guide to Computer Forensics and Investigations. (Third edition) – USA: Course Technology, Cengage Learning Inc., 2009 – 607 p.

13. Pollard C., Anzaldua R. Computer Forensics for Dummies. – Indianapolis, Indiana, USA: Wiley Publishing Inc, 2008 – 355 p.

## **VI. CIS monographs, scientific articles and collections:**

1. Aratuly K., Bostanbekov K. Cybercrimes: Concept and Problems of Terminology // Middle-East Journal of Scientific Research 15 (8): ISSN 1990-9233 – Almaty, Kazakhstan: IDOSI Publications, 2013. – 1124 p.

2. Carr J. Inside Cyber Warfare. Second Edition. Mapping the Cyber Underworld. – Sebastopol, Ukraine: O'Reilly Media, 2012. – 294 p.

3. Efremova M.A. To the question of computer information concept // Russian justice. – № 7. – 2012.

4. Fedotov N.N. Forensics – computer forensics. Moscow, RF.: Legal World, 2007.

5. Gavrilin Yu.V. Investigation of illegal access to computer information. – Moscow, 2001.
6. Ischenko E.P. Forensic science: lecture course. M., 2008.
7. Kabulov R.K., Abdurakhmanov E.S. Crimes in the field of information technologies: Study guide. – Tashkent, Uzbekistan: Academy of MIA of the Republic of Uzbekistan, 2009.
8. Kuznetsov M.V., Simdyanov I.V. Social engineering and social hackers. – Saint Petersburg, RF, 2007.
9. Lapshin V.E. Theoretical basics of the scene inspection // Expert criminalist. – RF, № 3, 2009.
10. Osipenko A.L. New technologies of obtaining and analysis of the Search and Intelligence information: legal problems and prospects of implementation // Vestnik of Voronezh Institute of Ministry of Internal Affairs of Russia. – № 2 – 2015.
11. Pisarev E.V. Information interaction between the investigator and the expert. – RF.: Vector of science TSU, № 3 (29). 2014.
12. Shemetov A.K. On the concept of virtual traces in forensic science // Russian investigator. - № 20 – 2014.
13. Shevchenko E.S. Tactics of separate investigative actions during cybercrimes investigation // Law and right. – № 8. – 2015.
14. Volevodz A.G. Counteraction to computer crimes: legal basis of international cooperation. – Moscow, RF 2002.
15. Yablokov N.P. Forensics: Workshop – Moscow, RF: Yurist, 2004.

## **VII. Thesis Abstracts for PhD and DSc in Law:**

1. Hewling M.-O. Digital forensics: an integrated approach for the investigation of cyber/computer related crimes. Thesis Abstract. – Eng, UK: University of Bedfordshire. – 254 p.

2. Ilyushin D.A. Peculiarities during investigation of crimes committed in the sphere of Internet services provision: Thesis Abstract. Volgograd, RK, 2008. – 226 p.

3. Ochilov Kh.R. Responsibility for theft committed using computer equipment. Thesis Abstract. – T.: TSUL, 2017. – 297 p.

4. Rasulov A.K. Improving criminal law and criminological measures to combat crimes in the field of information technology and security. Thesis Abstract. - T.: AMIA, 2018. – 332 p.

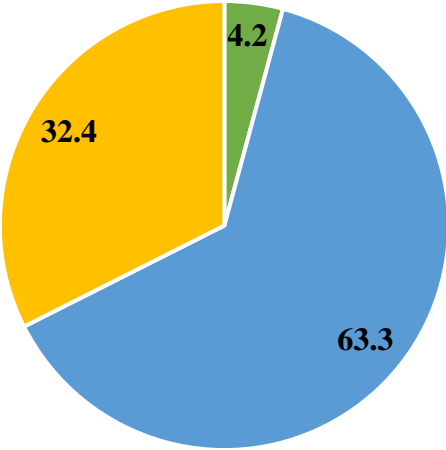
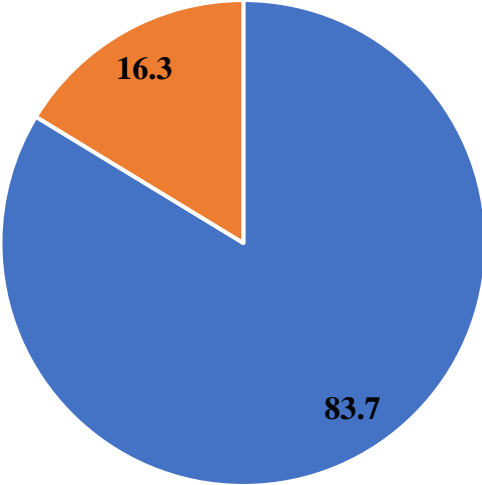
5. Saleem Sh. Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics. Thesis Abstract. – Stockholm, Sweden: Stockholm University, 2015 – 243 p.

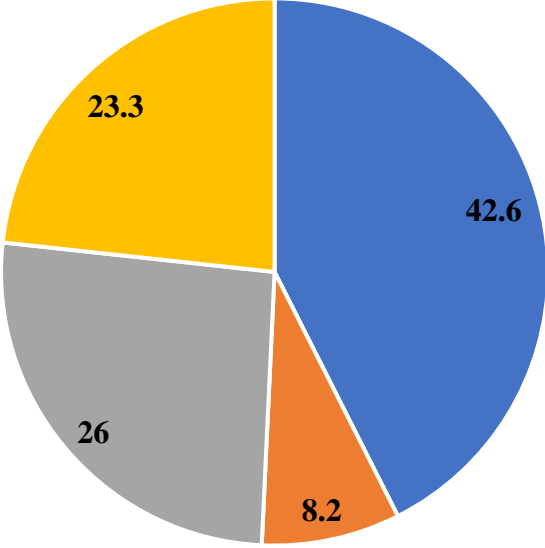
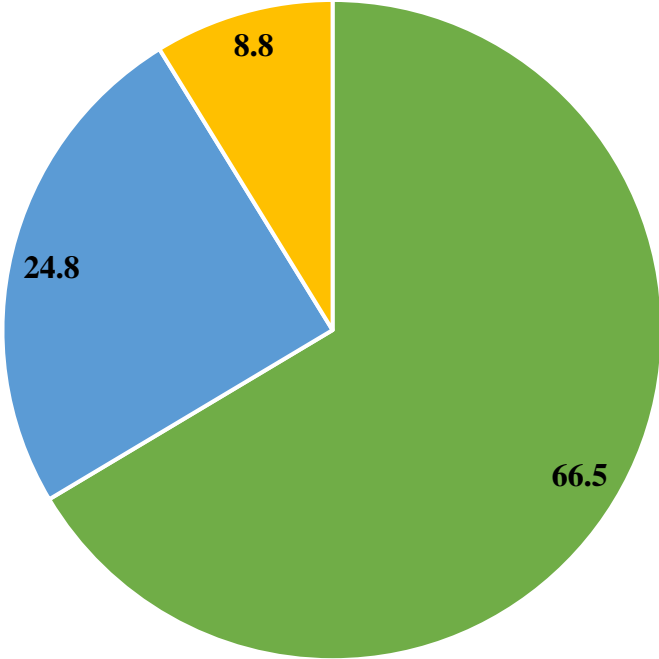
#### **VIII. Internet resources:**

1. [www.europarl.europa.eu](http://www.europarl.europa.eu)
2. [www.interpol.int](http://www.interpol.int)
3. [www.itu.int](http://www.itu.int)
4. [www.investopedia.com](http://www.investopedia.com)
5. [www.legislation.gov.uk](http://www.legislation.gov.uk)
6. [www.oecd.org](http://www.oecd.org)
7. [www.ohchr.org](http://www.ohchr.org)
8. [www.researchgate.net](http://www.researchgate.net)
9. [www.state.nj.us](http://www.state.nj.us)
10. [www.webopedia.com](http://www.webopedia.com)

Annexes (on Russian)

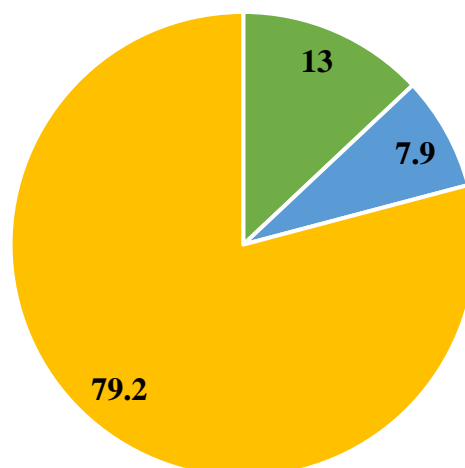
ПРИЛОЖЕНИЕ № 1. Результаты проведенного опроса

| №                 | Ответы на вопросы (%)  |                   |             |               |      |         |      |           |      |
|-------------------|--|-------------------|-------------|---------------|------|---------|------|-----------|------|
| 1.                | <p data-bbox="699 367 1023 405">Возраст респондентов</p>  <p data-bbox="587 994 1139 1032">■ меньше 20 лет ■ 20-30 ■ старше 30</p> <table border="1"><caption>Возраст респондентов</caption><thead><tr><th>Возрастная группа</th><th>Процент (%)</th></tr></thead><tbody><tr><td>меньше 20 лет</td><td>4.2</td></tr><tr><td>20-30</td><td>63.3</td></tr><tr><td>старше 30</td><td>32.4</td></tr></tbody></table> | Возрастная группа | Процент (%) | меньше 20 лет | 4.2  | 20-30   | 63.3 | старше 30 | 32.4 |
| Возрастная группа | Процент (%)  |                   |             |               |      |         |      |           |      |
| меньше 20 лет     | 4.2  |                   |             |               |      |         |      |           |      |
| 20-30             | 63.3   |                   |             |               |      |         |      |           |      |
| старше 30         | 32.4   |                   |             |               |      |         |      |           |      |
| 2.                | <p data-bbox="730 1099 1002 1137">Пол респондентов</p>  <p data-bbox="703 1765 1043 1803">■ Мужчина ■ Женщина</p> <table border="1"><caption>Пол респондентов</caption><thead><tr><th>Пол</th><th>Процент (%)</th></tr></thead><tbody><tr><td>Мужчина</td><td>83.7</td></tr><tr><td>Женщина</td><td>16.3</td></tr></tbody></table>   | Пол               | Процент (%) | Мужчина       | 83.7 | Женщина | 16.3 |           |      |
| Пол               | Процент (%)  |                   |             |               |      |         |      |           |      |
| Мужчина           | 83.7   |                   |             |               |      |         |      |           |      |
| Женщина           | 16.3   |                   |             |               |      |         |      |           |      |

|    |  |
|----|--|
| 3. | <p style="text-align: center;"><b>Сфера деятельности респондентов</b></p>  <p style="text-align: center;"> <span style="color: blue;">■</span> Юриспруденция    <span style="color: orange;">■</span> Экономика    <span style="color: gray;">■</span> IT-сектор    <span style="color: yellow;">■</span> другое </p>  |
| 4. | <p style="text-align: center;"><b>Как часто Вы пользуетесь сетью Интернет (социальные сети, поисковики, почта и т.д.) в сутки?</b></p>  <p style="text-align: center;"> <span style="color: green;">■</span> более трех часов в сутки    <span style="color: blue;">■</span> 1-3 часа в сутки    <span style="color: yellow;">■</span> менее 1 часа в сутки </p> |

Какая информация в социальных сетях и информационных ресурсах (блоги, мессенджеры и т.д.) является для Вас более безопасной?

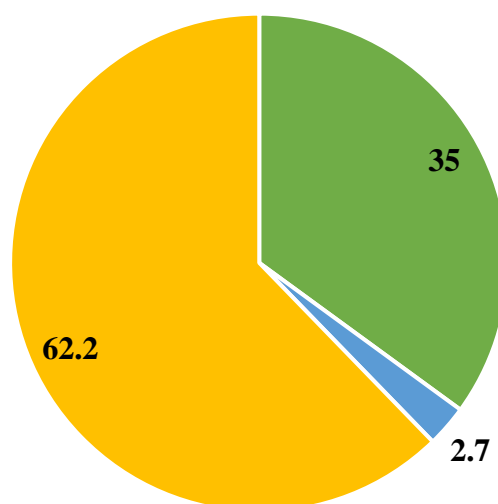
5.



- информация, содержащая в себе наибольшее количество статистических данных и аргументов;
- информация, размещенная в нескольких источниках
- информация официальных и/или государственных источников

Какими информационными ресурсами Вы часто пользуетесь в сети Интернет?

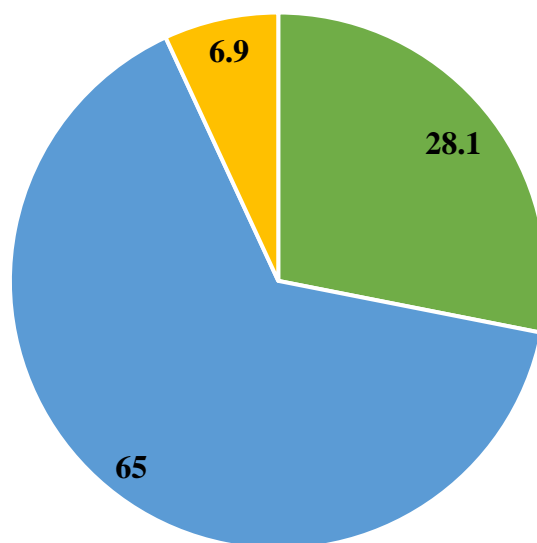
6.



- поисковые системы (Google, Yandex, Opera и другие)
- электронные почты (Mail.ru, Gmail.com, Umail.uz и другие)
- социальные сети и блоги (Facebook, Instagram, Twitter, Telegram, WhatsApp, WeChat и другие)

Сталкивались ли вы с преступлениями в сфере информационных технологий (киберпреступлениями), такими как Интернет-мошенничество, взлом паролей, похищения личных данных, распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и др

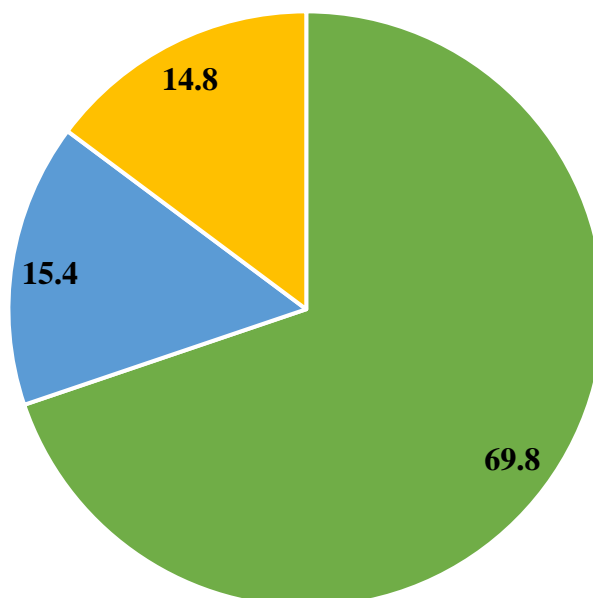
7.



■ Да ■ Нет ■ Затрудняюсь ответить

Понимаете ли вы разнице между «Преступления в сфере информационных технологий» и «Преступлениями совершаемых с помощью информационных технологий»?

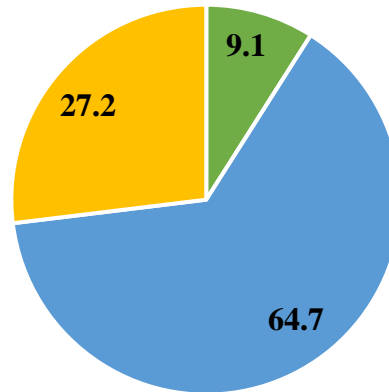
8.



■ Да ■ Нет ■ Затрудняюсь ответить



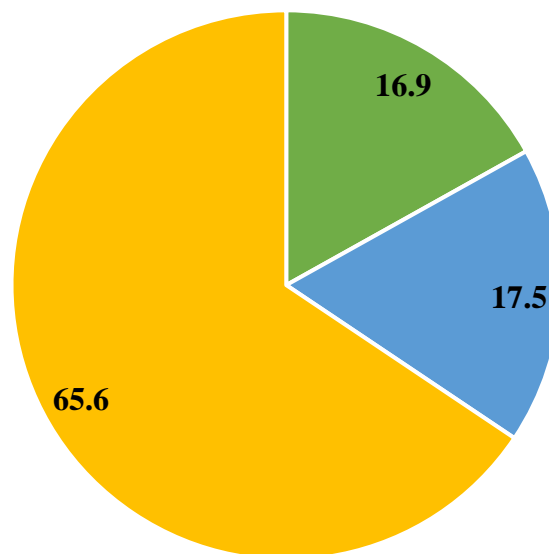
Какое определение «Преступления в сфере информационных технологий» в большей степени отражает содержание данного понятия?



9.

- преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства
- общественно опасные деяния (действия и бездействия), совершаемые как умышленно, так и по неосторожности, причиняющие либо создающие угрозу реального причинения существенного вреда или материального ущерба общественным отношениям в сфере информационных тех
- любая преступная или криминальной активность в виртуальном пространстве (киберпространстве), совершаемой с использованием информационных технологии

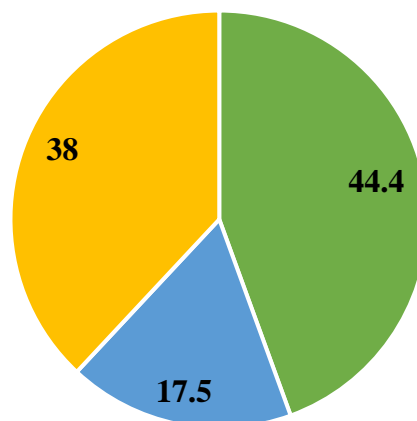
Что на Ваш взгляд должно охраняться от преступлений в сфере информационных технологий (киберпреступлений)?



10.

- компьютерная информация на информационных технологиях
- информационная инфраструктура и система
- информационные ресурсы, сети, средства и технологий

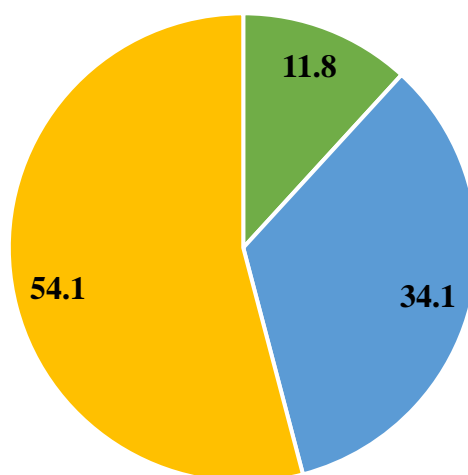
**Назовите самый оптимальный способ законодательного регулирования преступлений в сфере информационных технологий (киберпреступлений)?**



11.

- внести законодательные обязательства учреждения должности специалиста по информационной безопасности в государственных органах, организациях, предприятиях и учреждениях
- ужесточение санкций, существующих за эти преступления
- принятие специального нормативно-правового акта – Закон «О противодействии преступлениям в сфере информационных технологий»

**Какие меры должно принимать государство в отношении киберпреступников, нанесших серьезный ущерб физическим и юридическим лицам, а также государственным интересам?**

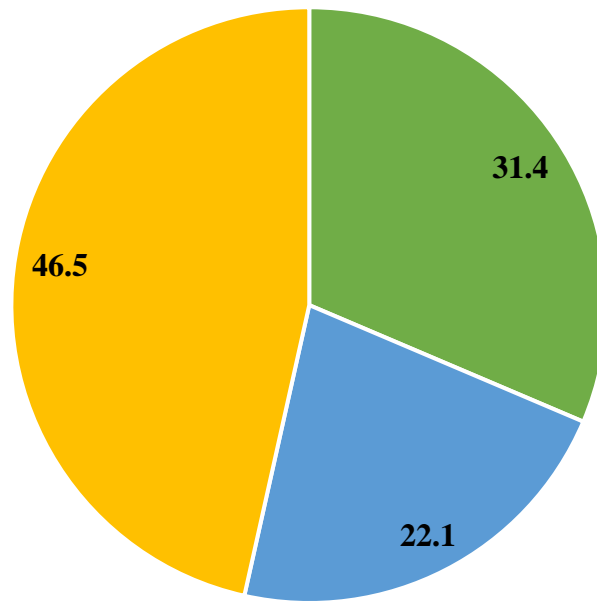


12.

- привлечение к ответственности в рамках существующих составов правонарушений в Кодексе Республики Узбекистан об административной ответственности
- привлечение к ответственности в рамках существующих составов преступлений в Уголовный кодекс Республики Узбекистан
- внести уголовную ответственность за подобные преступления в виде отдельного состава преступления

**Какой вид наказания является наиболее эффективным в Вашем понимании для предупреждения преступлений в сфере информационных технологий (киберпреступлений)?**

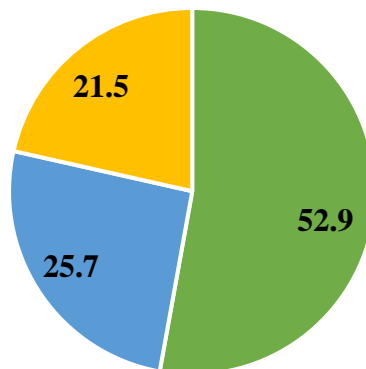
13.



■ штраф ■ обязательные общественные работы ■ лишение свободы

**Какие меры на Ваш взгляд наиболее эффективны для повышения уровня противодействия преступлениям в сфере информационных технологий (киберпреступлениям)?**

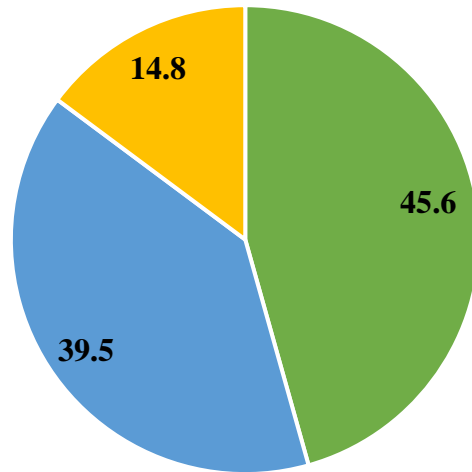
14.



- установление новых составов преступлений с учетом современных вызовов и угроз, создание специализированного органа по изучению проблем киберпреступности, борьбы с ними, усиление профилактики правонарушений в сети Интернет, подготовка трансдисциплинарных с широкое внедрение современных информационно-коммуникационных технологий в работу правоохранительных органов, повышение квалификации сотрудников
- ужесточение уголовно-правовой политики по противодействию преступлениям в сфере информационных технологий, увеличение штата сотрудников уполномоченных государственных органов

**Какой государственный орган или организация, по Вашему мнению должны обеспечивать информационную безопасность в Республике Узбекистан?**

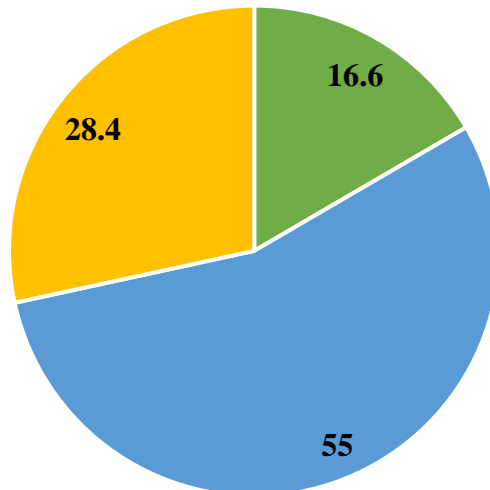
15.



- правоохранительные органы (органы прокуратуры, СГБ, МВД)
- Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан и его подведомственные организации
- пользователь, организация и учреждения

**Какой правоохранительный орган, по Вашему мнению эффективно обеспечить борьбу с преступлениями в сфере информационных технологий (киберпреступления) в Республике Узбекистан?**

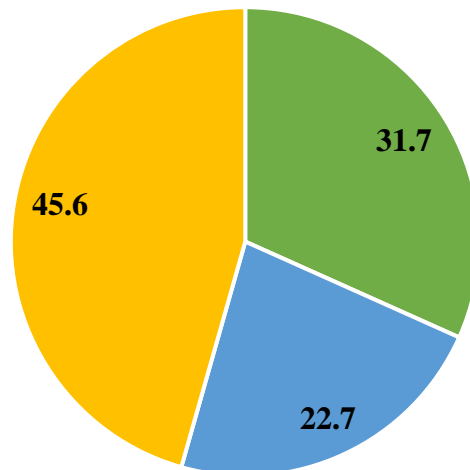
16.



- Органы внутренних дел
- Органы СГБ
- Органы прокуратуры, и их оперативные подразделения

**Какие меры воздействия необходимо применять в отношении лиц, склонных к совершению преступлений в сфере информационных технологий (киберпреступлений)?**

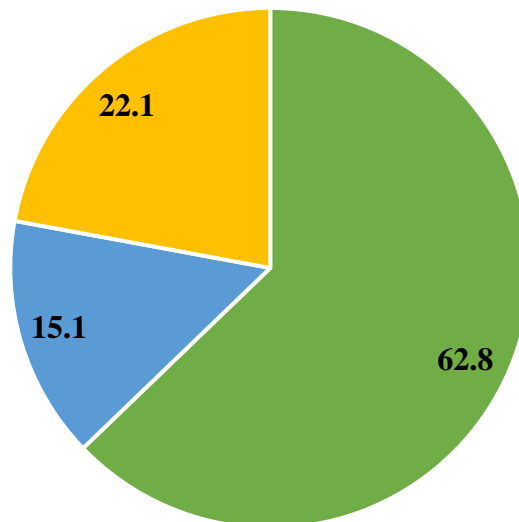
17.



- усилить ответственность вплоть до лишения свободы
- применять высокие размеры штрафа
- наложить обязательство сотрудничать по вопросам информационной безопасности и технологий

**Как вы думаете каким способом больше всего можно обнаружить преступления в сфере информационных технологий (киберпреступлений)?**

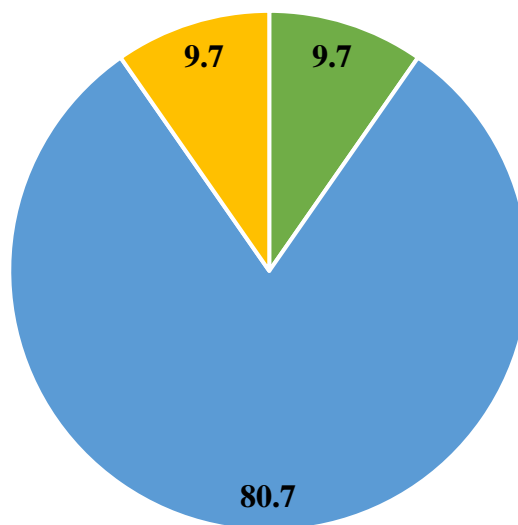
18.



- путем осуществления оперативно-розыскной деятельности
- путем обращения физических и юридических лиц
- затрудняюсь ответить

Как вы думаете, при расследовании преступлений в сфере информационных технологий (киберпреступлений), какое из следственных действия играет наибольшее значения?

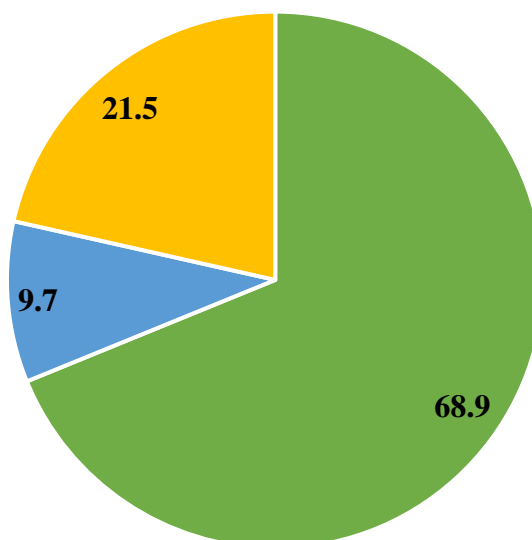
19.



- Осмотр место происшествия, обыск (выемка) и допрос
- Назначения компьютерной-технической (цифровой) экспертизы
- Затрудняюсь ответить

Ваше отношение к составление международного договора (такого как, Будапештской конвенции) по борьбе с киберпреступлениями и сотрудничеству стран в рамках ШОС, СНГ или другой организации, инициатором которого был бы Республика Узбекистан?

20.



- Да, согласен
- Нет, не согласен
- Затрудняюсь ответить

**ПРИЛОЖЕНИЕ № 2. СОПОСТАВИТЕЛЬНАЯ ТАБЛИЦА**

**к проекту закона «О внесении изменений и дополнений в Уголовный кодекс Республики Узбекистан»**

| Действующая редакция  | Предлагаемая редакция  | Обоснование  |
|---|--|--|
| <p><b>Статья 125. Разглашение тайны усыновления</b></p> <p>Разглашение охраняемой законом тайны усыновления или удочерения детей-сирот либо детей, лишенных родительской опеки, совершенное вопреки воле усыновителей или удочерителей либо органа опеки и попечительства, —</p> <p>наказывается штрафом от пятидесяти до ста базовых расчетных величин или обязательными общественными работами до трехсот часов либо исправительными работами до двух лет.</p> <p>То же деяние:</p> <p>а) совершенное лицом, обязанным хранить эту тайну в связи с профессиональной деятельностью или занимаемым служебным положением;</p> <p>б) совершенное из корыстных или иных низменных побуждений;</p> <p>в) повлекшее тяжкие последствия, —</p> <p align="center"><b>дополняется</b></p> <p>наказывается штрафом от ста до двухсот базовых расчетных величин или обязательными общественными работами от трехсот до трехсот шестидесяти часов либо</p> | <p><b>Статья 125. Разглашение тайны усыновления</b></p> <p>Разглашение охраняемой законом тайны усыновления или удочерения детей-сирот либо детей, лишенных родительской опеки, совершенное вопреки воле усыновителей или удочерителей либо органа опеки и попечительства, —</p> <p>наказывается штрафом от пятидесяти до ста базовых расчетных величин или обязательными общественными работами до трехсот часов либо исправительными работами до двух лет.</p> <p>То же деяние:</p> <p>а) совершенное лицом, обязанным хранить эту тайну в связи с профессиональной деятельностью или занимаемым служебным положением;</p> <p>б) совершенное из корыстных или иных низменных побуждений;</p> <p>в) повлекшее тяжкие последствия,</p> <p><b>г) с использованием средств массовой информации, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет, —</b></p> <p>наказывается штрафом от ста до двухсот базовых расчетных величин или обязательными общественными работами от трехсот до трехсот шестидесяти часов либо</p> | <p>Институт тайны усыновления является важным институтом, который определяет соотношение интересов личности, общества и государства, частного и публичного начала права, основания и предел вмешательства государства в негосударственную сферу, уровень информационной защиты в Республике Узбекистан.</p> <p>Огромное значение при рассмотрении вопроса о разглашении информации, охраняемой законом, имеет проблема обеспечения информационной безопасности общества и государства, а именно – применительно к защите тайны усыновления. В системе правоотношений, возникающих в сфере использования информации, особое место занимает институт тайны усыновления. Важность и значимость этого института в эпоху информационных технологий, когда информация становится самым основным и ценным ресурсом в обществе, многократно возрастает.</p> <p>Сеть Интернет является очень удобной средой для распространения различной информации, в том числе тайны усыновления. С учетом высокой общественной опасности разглашение тайны усыновления с использованием современных информационно-коммуникационных технологий и сети Интернет, а также в целях реализации норм международных актов в области противодействия совершению указанных</p> |

|   |   |   |
|---|---|---|
| <p>исправительными работами от двух до трех лет.</p>  | <p>исправительными работами от двух до трех лет.</p>  | <p>действий, считается целесообразным дополнить статью 125 УК Республики Узбекистан.</p>  |
| <p><b>Статья 130. Изготовление, ввоз, распространение, рекламирование, демонстрация порнографической продукции</b></p> <p>Изготовление или ввоз на территорию Республики Узбекистан с целью распространения, рекламирования, демонстрации, а равно распространение, рекламирование, демонстрация порнографической продукции, совершенные после применения административного взыскания за такие же действия, —</p> <p>наказывается штрафом от четырехсот до шестисот минимальных размеров заработной платы или обязательными общественными работами до трехсот шестидесяти часов либо исправительными работами до трех лет.</p> <p>Те же действия, совершенные:</p> <p>а) повторно или опасным рецидивистом;<br/>б) по предварительному сговору группой лиц, —</p> <p>наказываются обязательными общественными работами от трехсот шестидесяти до четырехсот восьмидесяти часов или ограничением свободы от одного года до трех лет либо лишением свободы до трех лет.</p> <p>Изготовление или ввоз на территорию Республики Узбекистан с целью распространения, рекламирования, демонстрации, а равно распространение, рекламирование, демонстрация</p> | <p><b>Статья 130. Изготовление, ввоз, распространение, рекламирование, демонстрация порнографической продукции</b></p> <p>Изготовление или ввоз на территорию Республики Узбекистан с целью распространения, рекламирования, демонстрации, а равно распространение, рекламирование, демонстрация порнографической продукции, совершенные после применения административного взыскания за такие же действия, —</p> <p>наказывается штрафом от четырехсот до шестисот минимальных размеров заработной платы или обязательными общественными работами до трехсот шестидесяти часов либо исправительными работами до трех лет.</p> <p>Те же действия, совершенные:</p> <p>а) повторно или опасным рецидивистом;<br/>б) по предварительному сговору группой лиц, —</p> <p>наказываются обязательными общественными работами от трехсот шестидесяти до четырехсот восьмидесяти часов или ограничением свободы от одного года до трех лет либо лишением свободы до трех лет.</p> <p>Изготовление или ввоз на территорию Республики Узбекистан с целью распространения, рекламирования, демонстрации, а равно распространение, рекламирование, демонстрация</p> | <p>Производство и оборот детской порнографии рассматривается в международно-правовых актах (например, Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии от 25 мая 2000 года) как киберпреступление, что позволяет в полной мере использовать международные механизмы борьбы с преступностью для противодействия ей.</p> <p>УК Республики Узбекистан предусматривает уголовную ответственность за изготовление или ввоз на территорию Республики Узбекистан с целью распространения, рекламирования, демонстрации, а равно распространение, рекламирование, демонстрация порнографической продукции (статья 130). При этом за изготовление или ввоз на территорию Республики Узбекистан с целью распространения, рекламирования, демонстрации, а равно распространение, рекламирование, демонстрация порнографической продукции с описанием или изображением несовершеннолетнего либо вовлечение несовершеннолетнего в качестве исполнителя в действиях порнографического характера предусматривается более строгая ответственность. С учетом высокой общественной опасности распространения или демонстрации порнографической продукции с использованием современных информационно-коммуникационных технологий и сети Интернет, а также в целях реализации норм</p> |



|  |   |  |
|--|---|--|
| <p>порнографической продукции с описанием или изображением несовершеннолетнего либо вовлечение несовершеннолетнего в качестве исполнителя в действиях порнографического характера —</p> <p>наказывается ограничением свободы от трех до пяти лет либо лишением свободы от трех до пяти лет.</p> <p style="text-align: center;"><b>дополняется</b></p>  | <p>порнографической продукции с описанием или изображением несовершеннолетнего либо вовлечение несовершеннолетнего в качестве исполнителя в действиях порнографического характера —</p> <p>наказывается ограничением свободы от трех до пяти лет либо лишением свободы от трех до пяти лет.</p> <p><b>Действия, предусмотренные частью третьей настоящей статьи, совершенные с использованием средств массовой информации, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет, —</b></p> <p><b>наказывается лишением свободы от пяти до семи лет.</b></p>    | <p>международных актов в области противодействия совершению указанных действий, считается целесообразным дополнить статью 130 УК Республики Узбекистан.</p>  |
| <p><b>Статья 139. Клевета</b></p> <p>Клевета, то есть распространение заведомо ложных, позорящих другое лицо измышлений, совершенная после применения административного взыскания за такие же действия, —</p> <p>наказывается штрафом до двухсот минимальных размеров заработной платы или обязательными общественными работами до трехсот часов либо исправительными работами до двух лет.</p> <p>Клевета в печатном или иным способом размноженном тексте либо в средствах массовой информации —</p> <p style="text-align: center;"><b>дополняется</b></p> | <p><b>Статья 139. Клевета</b></p> <p>Клевета, то есть распространение заведомо ложных, позорящих другое лицо измышлений, совершенная после применения административного взыскания за такие же действия, —</p> <p>наказывается штрафом до двухсот минимальных размеров заработной платы или обязательными общественными работами до трехсот часов либо исправительными работами до двух лет.</p> <p>Клевета в печатном или иным способом размноженном тексте либо в средствах массовой информации, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно в сети Интернет —</p> | <p>На сегодняшний день Интернет стал использоваться не только для совершения преступлений в сфере информационных технологий, но и для совершения традиционных преступлений против личности. В частности, участились случаи использования сети Интернет для распространения клеветнических и оскорбляющих сведений. В целях предупреждения указанных преступлений следует внести соответствующие изменения в статье 139 УК Республики Узбекистан.</p> |

|   |   |  |
|---|---|--|
| <p>наказывается штрафом от двухсот до четырехсот минимальных размеров заработной платы или обязательными общественными работами от трехсот до трехсот шестидесяти часов либо исправительными работами от двух до трех лет или ограничением свободы до одного года или лишением свободы до одного года.</p> <p>Клевета:</p> <p>а) соединенная с обвинением в совершении тяжкого или особо тяжкого преступления;</p> <p>б) повлекшая за собой тяжкие последствия;</p> <p>в) совершенная опасным рецидивистом;</p> <p>г) из корыстных или иных низменных побуждений —</p> <p>наказывается ограничением свободы от одного года до трех лет либо лишением свободы до трех лет.</p> | <p>наказывается штрафом от двухсот до четырехсот минимальных размеров заработной платы или обязательными общественными работами от трехсот до трехсот шестидесяти часов либо исправительными работами от двух до трех лет или ограничением свободы до одного года или лишением свободы до одного года.</p> <p>Клевета:</p> <p>а) соединенная с обвинением в совершении тяжкого или особо тяжкого преступления;</p> <p>б) повлекшая за собой тяжкие последствия;</p> <p>в) совершенная опасным рецидивистом;</p> <p>г) из корыстных или иных низменных побуждений —</p> <p>наказывается ограничением свободы от одного года до трех лет либо лишением свободы до трех лет.</p> |  |
| <p><b>Статья 140. Оскорбление</b></p> <p>Оскорбление, то есть умышленное унижение чести и достоинства личности в неприличной форме, совершенное после применения административного взыскания за такие же действия, —</p> <p>наказывается штрафом до двухсот минимальных размеров заработной платы или обязательными общественными работами до двухсот сорока часов либо исправительными работами до одного года.</p> <p>Оскорбление в печатном или иным способом размноженном тексте либо в средствах массовой информации —</p>   | <p><b>Статья 140. Оскорбление</b></p> <p>Оскорбление, то есть умышленное унижение чести и достоинства личности в неприличной форме, совершенное после применения административного взыскания за такие же действия, —</p> <p>наказывается штрафом до двухсот минимальных размеров заработной платы или обязательными общественными работами до двухсот сорока часов либо исправительными работами до одного года.</p> <p>Оскорбление в печатном или иным способом размноженном тексте либо в средствах массовой информации, телекоммуникационных сетей и</p>   | <p>На сегодняшний день Интернет стал использоваться не только для совершения преступлений в сфере информационных технологий, но и для совершения традиционных преступлений против личности. В частности, участились случаи использования сети Интернет для распространения клеветнических и оскорбляющих сведений. В целях предупреждения указанных преступлений следует внести соответствующие изменения в статьи 140 УК Республики Узбекистан.</p> |

|  |   |  |
|--|---|--|
| <p style="text-align: center;"><b>дополняется</b></p> <p>наказывается штрафом от двухсот до четырехсот минимальных размеров заработной платы или обязательными общественными работами от двухсот сорока до трехсот часов либо исправительными работами от одного года до двух лет.</p> <p>Оскорбление:</p> <p>а) в связи с выполнением потерпевшим своего служебного или гражданского долга;</p> <p>б) нанесенное опасным рецидивистом или лицом, ранее судимым за клевету, —</p> <p>наказывается штрафом от четырехсот до шестисот минимальных размеров заработной платы или исправительными работами от двух до трех лет либо ограничением свободы до одного года или лишением свободы до одного года.</p> | <p><b>информационно-коммуникационных технологий, а равно в сети Интернет</b> —</p> <p>наказывается штрафом от двухсот до четырехсот минимальных размеров заработной платы или обязательными общественными работами от двухсот сорока до трехсот часов либо исправительными работами от одного года до двух лет.</p> <p>Оскорбление:</p> <p>а) в связи с выполнением потерпевшим своего служебного или гражданского долга;</p> <p>б) нанесенное опасным рецидивистом или лицом, ранее судимым за клевету, —</p> <p>наказывается штрафом от четырехсот до шестисот минимальных размеров заработной платы или исправительными работами от двух до трех лет либо ограничением свободы до одного года или лишением свободы до одного года.</p> |  |
| <p><b>Статья 141<sup>1</sup>. Нарушение неприкосновенности частной жизни</b></p> <p>Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия, совершенное после применения административного взыскания за такие же действия, —</p> <p>наказывается штрафом от пятидесяти до ста минимальных размеров заработной платы или обязательными общественными работами до трехсот часов либо исправительными работами до двух лет.</p> <p>Те же действия:</p>  | <p><b>Статья 141<sup>1</sup>. Нарушение неприкосновенности частной жизни</b></p> <p>Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия, совершенное после применения административного взыскания за такие же действия, —</p> <p>наказывается штрафом от пятидесяти до ста минимальных размеров заработной платы или обязательными общественными работами до трехсот часов либо исправительными работами до двух лет.</p> <p>Те же действия:</p>   | <p>Сегодня в сети Интернет практически не является трудным найти личные сведения об определенных лицах, в частности, в социальных сетях с легкостью можно найти персональные данные. Защита сведений о частной жизни лица, составляющих его личную или семейную тайну, также требует правовой охраны и в виртуальном пространстве. Современные хакеры использует специальные технические средства слежения, перехвата информации и иные технологии. При этом использование данных средств не указано в качестве квалифицирующего признака. С учетом этого, следует внести изменения в статью 141<sup>1</sup> УК Республики Узбекистан.</p> |

|   |   |  |
|---|---|--|
| <p>а) повлекшие тяжкие последствия;<br/> б) совершенные из корыстных побуждений;<br/> в) совершенные опасным рецидивистом,<br/> —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказываются штрафом от ста до двухсот минимальных размеров заработной платы или обязательными общественными работами от трехсот до трехсот шестидесяти часов или ограничением свободы от одного года до трех лет либо лишением свободы до трех лет.</p>   | <p>а) повлекшие тяжкие последствия;<br/> б) совершенные из корыстных побуждений;<br/> в) совершенные опасным рецидивистом;<br/> г) с использованием средств компьютерной техники, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно в сети Интернет —</p> <p>наказываются штрафом от ста до двухсот минимальных размеров заработной платы или обязательными общественными работами от трехсот до трехсот шестидесяти часов или ограничением свободы от одного года до трех лет либо лишением свободы до трех лет.</p>   |  |
| <p><b>Статья 155. Терроризм</b><br/> Терроризм — насилие, использование силы, иные деяния, создающие опасность личности или собственности, либо угроза их осуществления для понуждения государственного органа, международной организации, их должностных лиц, физического или юридического лица совершить или воздержаться от совершения какой-либо деятельности в целях осложнения международных отношений, нарушения суверенитета и территориальной целостности, подрыва безопасности государства, провокации войны, вооруженного конфликта, дестабилизации общественно-политической обстановки, устрашения населения, —</p> <p>наказывается лишением свободы от восьми до десяти лет.</p> | <p><b>Статья 155. Терроризм</b><br/> Терроризм — насилие, использование силы, иные деяния, создающие опасность личности или собственности, либо угроза их осуществления для понуждения государственного органа, международной организации, их должностных лиц, физического или юридического лица совершить или воздержаться от совершения какой-либо деятельности в целях осложнения международных отношений, нарушения суверенитета и территориальной целостности, подрыва безопасности государства, провокации войны, вооруженного конфликта, дестабилизации общественно-политической обстановки, устрашения населения, —</p> <p>наказывается лишением свободы от восьми до десяти лет.</p> | <p>Информационный терроризм наиболее перспективным среди всех других видов терроризма. Он действует в интеллектуальной сфере и порождает новый вид насилия, связанный с киберпространством.</p> <p>Одной из информационного терроризма разновидностей является кибертерроризм, представляющий собой использование современных достижений в области информационно-коммуникационных технологий в качестве средства для нарушения функционирования важнейших национальных инфраструктур (правительственных, платежных, финансовых, транспортных, энергетических), принуждения или запугивания правительства, гражданского населения.</p> <p>Другая разновидность информационного терроризма подразумевает использование средств массовой информации, сервисов</p> |

|   |   |  |
|---|---|--|
| <p>Покушение на жизнь, причинение телесного повреждения государственному или общественному деятелю или представителю власти, совершенное в связи с их государственной или общественной деятельностью с целью дестабилизации обстановки или воздействия на принятие решений государственными органами либо воспрепятствования политической или иной общественной деятельности, — наказываются лишением свободы от десяти до пятнадцати лет.</p> <p>Действия, предусмотренные частью первой или второй настоящей статьи, повлекшие:</p> <p>а) смерть человека;<br/>б) иные тяжкие последствия, —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказываются лишением свободы от пятнадцати до двадцати пяти лет или пожизненным лишением свободы.</p> <p>Лицо, участвовавшее в подготовке терроризма, освобождается от уголовной ответственности, если оно своевременным предупреждением органов власти или иным способом активно способствовало предотвращению наступления тяжких последствий и реализации целей террористов, если в действиях этого лица не содержится иного состава преступления.</p> | <p>Покушение на жизнь, причинение телесного повреждения государственному или общественному деятелю или представителю власти, совершенное в связи с их государственной или общественной деятельностью с целью дестабилизации обстановки или воздействия на принятие решений государственными органами либо воспрепятствования политической или иной общественной деятельности, — наказываются лишением свободы от десяти до пятнадцати лет.</p> <p>Действия, предусмотренные частью первой или второй настоящей статьи, повлекшие:</p> <p>а) смерть человека;<br/>б) иные тяжкие последствия;<br/>в) с использованием средств массовой информации, средств компьютерной техники, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет, —</p> <p>наказываются лишением свободы от пятнадцати до двадцати пяти лет или пожизненным лишением свободы.</p> <p>Лицо, участвовавшее в подготовке терроризма, освобождается от уголовной ответственности, если оно своевременным предупреждением органов власти или иным способом активно способствовало предотвращению наступления тяжких последствий и реализации целей террористов, если в действиях этого лица не содержится иного состава преступления.</p> | <p>Интернет террористическими группами для имущественного, финансового, информационного и прочего обеспечения своей деятельности, но не для непосредственного совершения терактов.</p> <p>Следовательно, на сегодняшний день информационные технологий, в целом Интернет стал часто использоваться для совершения информационного терроризма. В целях предупреждения указанных преступлений считаем целесообразным внести соответствующие изменения в статьи 155 УК Республики Узбекистан.</p> |
|---|---|--|

|  |  |  |
|--|--|--|
| <p><b>Статья 163. Утрата документов, содержащих государственную тайну</b></p> <p>Утрата документов, а равно предметов или веществ, сведения о которых составляют государственную или военную тайну, лицом, которому они были доверены в связи со служебной или профессиональной деятельностью, если утрата явилась следствием нарушения правил обращения с указанными документами, предметами или веществами —</p> <p>наказывается ограничением свободы от одного года до трех лет либо лишением свободы до трех лет.</p> <p>То же деяние, повлекшее тяжкие последствия, —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказывается ограничением свободы от трех до пяти лет либо лишением свободы от трех до пяти лет.</p> | <p><b>Статья 163. Утрата документов, содержащих государственную тайну</b></p> <p>Утрата документов, а равно предметов или веществ, сведения о которых составляют государственную или военную тайну, лицом, которому они были доверены в связи со служебной или профессиональной деятельностью, если утрата явилась следствием нарушения правил обращения с указанными документами, предметами или веществами —</p> <p>наказывается ограничением свободы от одного года до трех лет либо лишением свободы до трех лет.</p> <p>То же деяние, <b>совершенные с использованием телекоммуникационных сетей и информационно-коммуникационных технологий, а равно повлекшее тяжкие последствия, —</b></p> <p>наказывается ограничением свободы от трех до пяти лет либо лишением свободы от трех до пяти лет.</p> | <p>Необходимость учета развитие современных информационных технологий, поскольку постоянно модернизируются и появляются новые виды носителей информации, а также новые способы ее передачи по различным каналам связи. Совершенствование уголовного законодательства в сфере защиты государственной тайны должно осуществляться с учетом научно-технического прогресса.</p> <p>В связи с высокой общественной опасности совершения преступления с использованием информационно-коммуникационных сетей считаем целесообразным дополнить статью 163 соответствующим пунктом.</p> |
| <p><b>Статья 176 Изготовление, сбыт поддельных денег, акцизных марок или ценных бумаг</b></p> <p>Изготовление с целью сбыта или сбыт поддельных банковских билетов (банкнот), металлической монеты, акцизных марок а также ценных бумаг либо иностранной валюты или ценных бумаг в иностранной валюте, —</p> <p>наказывается ограничением свободы от двух до пяти лет либо лишением свободы до пяти лет.</p> <p>Те же действия, совершенные:</p>   | <p><b>Статья 176 Изготовление, сбыт поддельных денег, акцизных марок или ценных бумаг</b></p> <p>Изготовление с целью сбыта или сбыт поддельных банковских билетов (банкнот), металлической монеты, акцизных марок а также ценных бумаг либо иностранной валюты или ценных бумаг в иностранной валюте, —</p> <p>наказывается ограничением свободы от двух до пяти лет либо лишением свободы до пяти лет.</p> <p>Те же действия, совершенные:</p>   | <p>Для совершения преступлений по изготовлению, сбыты поддельных денег, акцизных марок или ценных бумаг все чаще используются устройства, в основе которых лежат информационно-коммуникационные технологии и компьютерные средства их изготовления и функционирования.</p> <p>Именно, с использованием цветного печатного оборудования и компьютерной обработки изображения преступниками совершается преступления, указанное в статье 176 УК.</p>   |

|   |  |   |
|---|--|---|
| <p>а) повторно или опасным рецидивистом;<br/>б) в крупном размере;<br/>в) по предварительному сговору группой лиц, —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказываются лишением свободы от пяти до десяти лет.<br/>Те же действия, совершенные:<br/>а) в особо крупном размере;<br/>б) организованной группой или в ее интересах, —<br/>наказываются лишением свободы от десяти до пятнадцати лет.</p>  | <p>а) повторно или опасным рецидивистом;<br/>б) в крупном размере;<br/>в) по предварительному сговору группой лиц;<br/>г) с использованием средств компьютерной техники, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет, —</p> <p>наказываются лишением свободы от пяти до десяти лет.<br/>Те же действия, совершенные:<br/>а) в особо крупном размере;<br/>б) организованной группой или в ее интересах, —<br/>наказываются лишением свободы от десяти до пятнадцати лет.</p>  | <p>В сети Интернет на некоторых сайтах можно найти советы, чертежи, рекомендации по изготовлению и сбыта поддельных денег, акцизных марок или ценных бумаг, что можно расценивать как интеллектуальное пособничество. В связи с этим, следует внести изменения в статью 176 УК Республики Узбекистан.</p>   |
| <p><b>Статья 179. Лжепредпринимательство</b><br/>Лжепредпринимательство, то есть создание предприятий и других предпринимательских организаций без намерения осуществлять уставную деятельность в целях получения ссуд, кредитов, освобождения (снижения) прибыли (дохода) от налогов или извлечения иной имущественной выгоды, —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказывается штрафом от ста до двухсот базовых расчетных величин или лишением определенного права до пяти лет, или исправительными работами до трех лет или ограничением свободы от одного года до трех лет либо лишением свободы до трех лет.</p> | <p><b>Статья 179. Лжепредпринимательство</b><br/>Лжепредпринимательство, то есть создание предприятий и других предпринимательских организаций без намерения осуществлять уставную деятельность в целях получения ссуд, кредитов, освобождения (снижения) прибыли (дохода) от налогов или извлечения иной имущественной выгоды, <b>путем телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет</b> —</p> <p>наказывается штрафом от ста до двухсот базовых расчетных величин или лишением определенного права до пяти лет, или исправительными работами до трех лет или ограничением свободы от одного года до трех лет либо лишением свободы до трех лет.</p> | <p>Общеизвестно, как за рубежом и в Республике Узбекистан, что в настоящее время подобные преступления, как правило, совершаются путем фальсификации компьютерной информации.</p> <p>Включение квалифицирующего признака увеличить опасность преступного деяния. Так как они направлены против устоев экономики Республики Узбекистан.</p> <p>С учетом высокой общественной опасности совершения преступления с использованием телекоммуникационных сетей и информационно-коммуникационных технологий следует дополнить статью 179 соответствующим пунктом.</p> |

|   |   |   |
|---|---|---|
| <p><b>Статья 180. Лжебанкротство</b><br/> Лжебанкротство, то есть заведомо не соответствующее действительности объявление хозяйствующим субъектом об экономической несостоятельности исполнения обязательств перед кредиторами, причинившее им крупный ущерб, —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказывается штрафом от ста пятидесяти до двухсот пятидесяти базовых расчетных величин или обязательными общественными работами от трехсот до трехсот шестидесяти часов либо исправительными работами от двух до трех лет или ограничением свободы от двух до трех лет или лишением свободы от двух до трех лет.</p> <p>В случае возмещения причиненного материального ущерба не применяется наказание в виде ограничения свободы и лишения свободы.</p> <p>Лицо, впервые совершившее преступление, освобождается от ответственности, если оно в тридцатидневный срок со дня обнаружения преступления возместило причиненный материальный ущерб.</p> | <p><b>Статья 180. Лжебанкротство</b><br/> Лжебанкротство, то есть заведомо не соответствующее действительности объявление хозяйствующим субъектом об экономической несостоятельности исполнения обязательств перед кредиторами, причинившее им крупный ущерб, <b>путем телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет,</b> —</p> <p>наказывается штрафом от ста пятидесяти до двухсот пятидесяти базовых расчетных величин или обязательными общественными работами от трехсот до трехсот шестидесяти часов либо исправительными работами от двух до трех лет или ограничением свободы от двух до трех лет или лишением свободы от двух до трех лет.</p> <p>В случае возмещения причиненного материального ущерба не применяется наказание в виде ограничения свободы и лишения свободы.</p> <p>Лицо, впервые совершившее преступление, освобождается от ответственности, если оно в тридцатидневный срок со дня обнаружения преступления возместило причиненный материальный ущерб.</p> | <p>Общеизвестно, как за рубежом и в Республике Узбекистан, что в настоящее время подобные преступления, как правило, совершаются путем фальсификации компьютерной информации.</p> <p>Включение квалифицирующего признака увеличить опасность преступного деяния. Так как они направлены против устоев экономики Республики Узбекистан.</p> <p>С учетом высокой общественной опасности совершения преступления с использованием телекоммуникационных сетей и информационно-коммуникационных технологий следует дополнить статью 180 соответствующим пунктом.</p> |
| <p><b>Статья 181. Соккрытие банкротства</b><br/> Умышленное сокрытие хозяйствующим субъектом своей неплатежеспособности путем представления сведений и документов, не соответствующих действительности, искажения бухгалтерской</p>   | <p><b>Статья 181. Соккрытие банкротства</b><br/> Умышленное сокрытие хозяйствующим субъектом своей неплатежеспособности путем представления сведений и документов, не соответствующих действительности, искажения бухгалтерской</p>   | <p>Общеизвестно, как за рубежом и в Республике Узбекистан, что в настоящее время подобные преступления, как правило, совершаются путем фальсификации компьютерной информации.</p> <p>Включение квалифицирующего признака увеличить опасность преступного деяния. Так</p>  |



|   |   |   |
|---|---|---|
| <p>отчетности или иного утаивания своей экономической несостоятельности, причинившее крупный ущерб кредиторам,<br/>—<br/><b>дополняется</b></p> <p>наказывается штрафом от ста пятидесяти до двухсот пятидесяти базовых расчетных величин или обязательными общественными работами от трехсот до трехсот шестидесяти часов либо исправительными работами от двух до трех лет или ограничением свободы от двух до трех лет или лишением свободы от двух до трех лет.</p> <p>В случае возмещения причиненного материального ущерба не применяется наказание в виде ограничения свободы и лишения свободы.</p> <p>Лицо, впервые совершившее преступление, освобождается от ответственности, если оно в тридцатидневный срок со дня обнаружения преступления возместило причиненный материальный ущерб.</p> | <p>отчетности или иного утаивания своей экономической несостоятельности, причинившее крупный ущерб кредиторам, <b>путем телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет</b> —</p> <p>наказывается штрафом от ста пятидесяти до двухсот пятидесяти базовых расчетных величин или обязательными общественными работами от трехсот до трехсот шестидесяти часов либо исправительными работами от двух до трех лет или ограничением свободы от двух до трех лет или лишением свободы от двух до трех лет.</p> <p>В случае возмещения причиненного материального ущерба не применяется наказание в виде ограничения свободы и лишения свободы.</p> <p>Лицо, впервые совершившее преступление, освобождается от ответственности, если оно в тридцатидневный срок со дня обнаружения преступления возместило причиненный материальный ущерб.</p> | <p>как они направлены против устоев экономики Республики Узбекистан.</p> <p>С учетом высокой общественной опасности совершения преступления с использованием телекоммуникационных сетей и информационно-коммуникационных технологий следует дополнить статью 181 соответствующим пунктом.</p>   |
| <p><b>Статья 181<sup>1</sup>. Преднамеренное банкротство</b></p> <p>Преднамеренное банкротство, то есть умышленное создание или увеличение неплатежеспособности, совершенное индивидуальным предпринимателем или должностным лицом, учредителем (участником) либо собственником имущества юридического лица в личных интересах или интересах иных лиц, повлекшее устойчивую экономическую</p>   | <p><b>Статья 181<sup>1</sup>. Преднамеренное банкротство</b></p> <p>Преднамеренное банкротство, то есть умышленное создание или увеличение неплатежеспособности, совершенное индивидуальным предпринимателем или должностным лицом, учредителем (участником) либо собственником имущества юридического лица в личных интересах или интересах иных лиц, повлекшее устойчивую экономическую</p>   | <p>Общеизвестно, как за рубежом и в Республике Узбекистан, что в настоящее время подобные преступления, как правило, совершаются путем фальсификации компьютерной информации.</p> <p>Включение квалифицирующего признака увеличить опасность преступного деяния. Так как они направлены против устоев экономики Республики Узбекистан.</p> <p>С учетом высокой общественной опасности совершения преступления с использованием телекоммуникационных сетей и</p> |

|   |  |   |
|---|--|---|
| <p>несостоятельность (банкротство) этого индивидуального предпринимателя или юридического лица, причинившее крупный ущерб кредиторам, —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказывается штрафом от ста пятидесяти до двухсот пятидесяти базовых расчетных величин или обязательными общественными работами от трехсот до трехсот шестидесяти часов либо исправительными работами от двух до трех лет или ограничением свободы от двух до трех лет или лишением свободы от двух до трех лет.</p> <p>В случае возмещения причиненного материального ущерба не применяется наказание в виде ограничения свободы и лишения свободы.</p> <p>Лицо, впервые совершившее преступление, освобождается от ответственности, если оно в тридцатидневный срок со дня обнаружения преступления возместило причиненный материальный ущерб.</p> | <p>несостоятельность (банкротство) этого индивидуального предпринимателя или юридического лица, причинившее крупный ущерб кредиторам, <b>путем телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет</b> —</p> <p>наказывается штрафом от ста пятидесяти до двухсот пятидесяти базовых расчетных величин или обязательными общественными работами от трехсот до трехсот шестидесяти часов либо исправительными работами от двух до трех лет или ограничением свободы от двух до трех лет или лишением свободы от двух до трех лет.</p> <p>В случае возмещения причиненного материального ущерба не применяется наказание в виде ограничения свободы и лишения свободы.</p> <p>Лицо, впервые совершившее преступление, освобождается от ответственности, если оно в тридцатидневный срок со дня обнаружения преступления возместило причиненный материальный ущерб.</p> | <p>информационно-коммуникационных технологий следует дополнить статью 181<sup>1</sup> соответствующим пунктом.</p>  |
| <p><b>Статья 209. Должностной подлог</b></p> <p>Должностной подлог, то есть внесение должностным лицом государственного органа, организации с государственным участием или органа самоуправления граждан из корыстной или иной заинтересованности заведомо ложных сведений и записей в официальные документы, подделка или составление и выдача заведомо ложных документов,</p>   | <p><b>Статья 209. Должностной подлог</b></p> <p>Должностной подлог, то есть внесение должностным лицом государственного органа, организации с государственным участием или органа самоуправления граждан из корыстной или иной заинтересованности заведомо ложных сведений и записей в официальные документы, подделка или составление и выдача заведомо ложных документов,</p>  | <p><b>Должностной подлог</b> так называемыми «электронными деньгами», денежными переводами посредством платежных систем или даже денежными суррогатами, такими как криптовалюта. При таком способе совершения преступления исключается непосредственный контакт между участниками.</p> <p>В связи с этим, необходимо дополнить статью 210 соответствующим пунктом, при совершении</p> |

|   |   |  |
|---|---|--|
| <p>повлекшие существенный вред правам или охраняемым законом интересам граждан либо государственным или общественным интересам, —</p> <p>наказывается штрафом от ста до трехсот базовых расчетных величин или лишением определенного права до пяти лет или обязательными общественными работами до трехсот шестидесяти часов либо исправительными работами до двух лет или ограничением свободы от одного года до двух лет или лишением свободы до трех лет.</p> <p>То же действие, совершенное:</p> <p>а) повторно или опасным рецидивистом;<br/>б) в интересах организованной группы, —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказывается штрафом от трехсот до шестисот базовых расчетных величин или ограничением свободы от двух до пяти лет либо лишением свободы до пяти лет с лишением определенного права до трех лет.</p> | <p>повлекшие существенный вред правам или охраняемым законом интересам граждан либо государственным или общественным интересам, —</p> <p>наказывается штрафом от ста до трехсот базовых расчетных величин или лишением определенного права до пяти лет или обязательными общественными работами до трехсот шестидесяти часов либо исправительными работами до двух лет или ограничением свободы от одного года до двух лет или лишением свободы до трех лет.</p> <p>То же действие, совершенное:</p> <p>а) повторно или опасным рецидивистом;<br/>б) в интересах организованной группы;<br/><b>в) с использованием средств компьютерной техники, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет, —</b></p> <p>наказывается штрафом от трехсот до шестисот базовых расчетных величин или ограничением свободы от двух до пяти лет либо лишением свободы до пяти лет с лишением определенного права до трех лет.</p> | <p>которых могут использоваться информационные технологии.</p>   |
| <p><b>Статья 210. Получение взятки</b></p> <p>Получение взятки, то есть заведомо незаконное принятие должностным лицом государственного органа, организации с государственным участием или органа самоуправления граждан лично или через посредника материальных ценностей либо извлечение имущественной выгоды за выполнение или невыполнение в интересах дающего взятку определенного действия,</p>   | <p><b>Статья 210. Получение взятки</b></p> <p>Получение взятки, то есть заведомо незаконное принятие должностным лицом государственного органа, организации с государственным участием или органа самоуправления граждан лично или через посредника материальных ценностей либо извлечение имущественной выгоды за выполнение или невыполнение в интересах дающего взятку определенного действия,</p>   | <p>Получение взятки так называемыми «электронными деньгами», денежными переводами посредством платежных систем или даже денежными суррогатами, такими как криптовалюта. При таком способе совершения преступления исключается непосредственный контакт между взяткодателем и взяткополучателем.</p> <p>В связи с этим, необходимо дополнить статью 210 соответствующим пунктом, при совершении</p> |

|   |  |  |
|---|--|--|
| <p>которое должностное лицо должно было или могло совершить с использованием своего служебного положения, —<br/>наказывается штрафом от пятидесяти до ста базовых расчетных величин или ограничением свободы от двух до пяти лет либо лишением свободы до пяти лет с лишением определенного права.</p> <p>Получение взятки:</p> <p>а) повторно, опасным рецидивистом или лицом, ранее совершившим преступления, предусмотренные статьями 211 или 212 настоящего Кодекса;</p> <p>б) в крупном размере;</p> <p>в) путем вымогательства;</p> <p>г) по предварительному сговору группой должностных лиц —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказывается лишением свободы от пяти до десяти лет.</p> <p>Получение взятки:</p> <p>а) в особо крупном размере;</p> <p>б) в интересах организованной группы, —<br/>наказывается лишением свободы от десяти до пятнадцати лет.</p> | <p>которое должностное лицо должно было или могло совершить с использованием своего служебного положения, —<br/>наказывается штрафом от пятидесяти до ста базовых расчетных величин или ограничением свободы от двух до пяти лет либо лишением свободы до пяти лет с лишением определенного права.</p> <p>Получение взятки:</p> <p>а) повторно, опасным рецидивистом или лицом, ранее совершившим преступления, предусмотренные статьями 211 или 212 настоящего Кодекса;</p> <p>б) в крупном размере;</p> <p>в) путем вымогательства;</p> <p>г) по предварительному сговору группой должностных лиц;</p> <p><b>д) с использованием средств компьютерной техники, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет, —</b><br/>наказывается лишением свободы от пяти до десяти лет.</p> <p>Получение взятки:</p> <p>а) в особо крупном размере;</p> <p>б) в интересах организованной группы, —<br/>наказывается лишением свободы от десяти до пятнадцати лет.</p> | <p>которых могут использоваться информационные технологии.</p>   |
| <p><b>Статья 211. Дача взятки</b><br/>Дача взятки, то есть заведомо незаконное предоставление должностному лицу государственного органа, организации с государственным участием или органа самоуправления граждан лично или через</p>   | <p><b>Статья 211. Дача взятки</b><br/>Дача взятки, то есть заведомо незаконное предоставление должностному лицу государственного органа, организации с государственным участием или органа самоуправления граждан лично или через</p>  | <p>Дача взятки так называемыми «электронными деньгами», денежными переводами посредством платежных систем или даже денежными суррогатами, такими как криптовалюта. При таком способе совершения преступления</p> |

|  |   |   |
|--|---|---|
| <p>посредника материальных ценностей или имущественной выгоды за выполнение или невыполнение в интересах давшего взятку определенного действия, которое должностное лицо должно было или могло совершить с использованием своего служебного положения, —</p> <p>наказывается штрафом от пятидесяти до ста базовых расчетных величин или ограничением свободы от двух до пяти лет либо лишением свободы до пяти лет.</p> <p>Дача взятки:</p> <p>а) повторно, опасным рецидивистом или лицом, ранее совершившим преступления, предусмотренные статьями 210 или 212 настоящего Кодекса;</p> <p>б) в крупном размере —</p> <p>наказывается лишением свободы от пяти до десяти лет.</p> <p>Дача взятки:</p> <p>а) в особо крупном размере;</p> <p>б) в интересах организованной группы, —</p> <p>наказывается лишением свободы от десяти до пятнадцати лет.</p> <p style="text-align: center;"><b>дополняется</b></p> <p>Лицо, давшее взятку, освобождается от ответственности, если в отношении него имело место вымогательство взятки и это лицо в течение тридцати суток после совершения преступных действий добровольно заявило о случившемся, чистосердечно раскаялось и активно способствовало раскрытию преступления.</p> | <p>посредника материальных ценностей или имущественной выгоды за выполнение или невыполнение в интересах давшего взятку определенного действия, которое должностное лицо должно было или могло совершить с использованием своего служебного положения, —</p> <p>наказывается штрафом от пятидесяти до ста базовых расчетных величин или ограничением свободы от двух до пяти лет либо лишением свободы до пяти лет.</p> <p>Дача взятки:</p> <p>а) повторно, опасным рецидивистом или лицом, ранее совершившим преступления, предусмотренные статьями 210 или 212 настоящего Кодекса;</p> <p>б) в крупном размере —</p> <p>наказывается лишением свободы от пяти до десяти лет.</p> <p>Дача взятки:</p> <p>а) в особо крупном размере;</p> <p>б) в интересах организованной группы;</p> <p><b>в) с использованием средств компьютерной техники, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет, —</b></p> <p>наказывается лишением свободы от десяти до пятнадцати лет.</p> <p>Лицо, давшее взятку, освобождается от ответственности, если в отношении него имело место вымогательство взятки и это лицо в течение тридцати суток после совершения преступных действий добровольно заявило о случившемся,</p> | <p>исключается непосредственный контакт между взяткодателем и взяткополучателем.</p> <p>В связи с этим, необходимо дополнить статью 211 соответствующим пунктом, при совершении которых могут использоваться информационные технологии.</p> |
|--|---|---|

|   |   |   |
|---|---|---|
|   | чистосердечно раскаялась и активно способствовало раскрытию преступления.   |   |
| <p><b>Статья 212. Посредничество во взяточничестве</b></p> <p>Посредничество во взяточничестве, то есть деятельность, направленная на достижение соглашения о получении или даче взятки, а равно непосредственная передача взятки по поручению заинтересованных лиц, —</p> <p>наказывается штрафом от пятидесяти до ста базовых расчетных величин или ограничением свободы от двух до пяти лет либо лишением свободы до пяти лет.</p> <p>То же действие, совершенное:</p> <p>а) повторно, опасным рецидивистом или лицом, ранее совершившим преступления, предусмотренные статьями 210 или 211 настоящего Кодекса;</p> <p>б) при получении или даче взятки в крупном размере;</p> <p>в) при получении взятки заведомо для посредника группой должностных лиц, действующих по предварительному сговору, —</p> <p>наказывается лишением свободы от пяти до десяти лет.</p> <p>Посредничество во взяточничестве, совершенное:</p> <p>а) за вознаграждение;</p> <p>б) при получении или даче взятки в особо крупном размере;</p> <p>в) в интересах организованной группы, —</p> | <p><b>Статья 212. Посредничество во взяточничестве</b></p> <p>Посредничество во взяточничестве, то есть деятельность, направленная на достижение соглашения о получении или даче взятки, а равно непосредственная передача взятки по поручению заинтересованных лиц, —</p> <p>наказывается штрафом от пятидесяти до ста базовых расчетных величин или ограничением свободы от двух до пяти лет либо лишением свободы до пяти лет.</p> <p>То же действие, совершенное:</p> <p>а) повторно, опасным рецидивистом или лицом, ранее совершившим преступления, предусмотренные статьями 210 или 211 настоящего Кодекса;</p> <p>б) при получении или даче взятки в крупном размере;</p> <p>в) при получении взятки заведомо для посредника группой должностных лиц, действующих по предварительному сговору, —</p> <p>наказывается лишением свободы от пяти до десяти лет.</p> <p>Посредничество во взяточничестве, совершенное:</p> <p>а) за вознаграждение;</p> <p>б) при получении или даче взятки в особо крупном размере;</p> <p>в) в интересах организованной группы</p> <p>г) с использованием средств компьютерной техники,</p> | <p>Посредничество во взяточничестве так называемыми «электронными деньгами», денежными переводами посредством платежных систем или даже денежными суррогатами, такими как криптовалюта. При таком способе совершения преступления исключается непосредственный контакт между взяткодателем и взяткополучателем, осуществляемая через посредника.</p> <p>В связи с этим, необходимо дополнить статью 212 соответствующим пунктом, при совершении которых могут использоваться информационные технологии.</p> |

|  |  |  |
|--|--|--|
| <p style="text-align: center;"><b>дополняется</b></p> <p>наказывается лишением свободы от десяти до пятнадцати лет.</p> <p>Лицо, выполнявшее посреднические функции во взяточничестве, освобождается от ответственности, если оно в течение тридцати суток после совершения преступных действий добровольно заявило о случившемся, чистосердечно раскаялось и активно способствовало раскрытию преступления.</p>   | <p><b>телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет, —</b></p> <p>наказывается лишением свободы от десяти до пятнадцати лет.</p> <p>Лицо, выполнявшее посреднические функции во взяточничестве, освобождается от ответственности, если оно в течение тридцати суток после совершения преступных действий добровольно заявило о случившемся, чистосердечно раскаялось и активно способствовало раскрытию преступления.</p>  |  |
| <p><b>Статья 230<sup>1</sup>. Фальсификация (подделка) доказательств</b></p> <p>Фальсификация (подделка) доказательств лицами, осуществляющими доказывание, или лицами, привлекаемыми к участию в доказывании, выразившаяся во внесении из корыстных или иных низменных побуждений заведомо ложных сведений и других искажений в документы либо предметы, при собирании, проверке и оценке доказательств по материалам последственных проверок и уголовных дел —</p> <p>наказывается штрафом от трехсот до четырехсот базовых расчетных величин или ограничением свободы от трех до пяти лет либо лишением свободы от трех до пяти лет с лишением определенного права.</p> <p>Те же действия:</p> <p>а) совершенные по предварительному сговору группой лиц;</p> | <p><b>Статья 230<sup>1</sup>. Фальсификация (подделка) доказательств</b></p> <p>Фальсификация (подделка) доказательств лицами, осуществляющими доказывание, или лицами, привлекаемыми к участию в доказывании, выразившаяся во внесении из корыстных или иных низменных побуждений заведомо ложных сведений и других искажений в документы либо предметы, при собирании, проверке и оценке доказательств по материалам последственных проверок и уголовных дел —</p> <p>наказывается штрафом от трехсот до четырехсот базовых расчетных величин или ограничением свободы от трех до пяти лет либо лишением свободы от трех до пяти лет с лишением определенного права.</p> <p>Те же действия:</p> <p>а) совершенные по предварительному сговору группой лиц;</p> | <p>Так как информационные технологии в принципе позволяют фальсифицировать не только письменные документы, но и звук, изображение, видео и т.д. на электронных носителях посредством средств компьютерной техники, телекоммуникационных сетей и информационно-коммуникационных технологий необходимо дополнить статью 230<sup>1</sup> соответствующим пунктом.</p> |

|  |   |  |
|--|---|--|
| <p>б) повлекшие задержание, заключение под стражу, привлечение к уголовной ответственности или освобождение от уголовной ответственности, осуждение либо оправдание лица, —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказываются лишением свободы от пяти до семи лет с лишением определенного права.</p> <p>Фальсификация (подделка) доказательств по уголовному делу о тяжком или особо тяжком преступлении, а равно фальсификация (подделка) доказательств, повлекшая тяжкие последствия, —</p> <p>наказывается лишением свободы от семи до десяти лет с лишением определенного права.</p> | <p>б) повлекшие задержание, заключение под стражу, привлечение к уголовной ответственности или освобождение от уголовной ответственности, осуждение либо оправдание лица;</p> <p><b>в) с использованием средств компьютерной техники, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет, —</b></p> <p>наказываются лишением свободы от пяти до семи лет с лишением определенного права.</p> <p>Фальсификация (подделка) доказательств по уголовному делу о тяжком или особо тяжком преступлении, а равно фальсификация (подделка) доказательств, повлекшая тяжкие последствия, —</p> <p>наказывается лишением свободы от семи до десяти лет с лишением определенного права.</p> |  |
| <p><b>Статья 243 Легализация доходов, полученных от преступной деятельности</b></p> <p>Легализация доходов, полученных от преступной деятельности, то есть придание правомерного вида происхождению собственности (денежных средств или иного имущества) путем ее перевода, превращения или обмена, а равно сокрытие либо утаивание подлинного характера, источника, местонахождения, способа распоряжения, перемещения, подлинных прав в отношении денежных средств или иного имущества либо его принадлежности, если денежные</p>  | <p><b>Статья 243 Легализация доходов, полученных от преступной деятельности</b></p> <p>Легализация доходов, полученных от преступной деятельности, то есть придание правомерного вида происхождению собственности (денежных средств или иного имущества) путем ее перевода, превращения или обмена, а равно сокрытие либо утаивание подлинного характера, источника, местонахождения, способа распоряжения, перемещения, подлинных прав в отношении денежных средств или иного имущества либо его принадлежности, если денежные средства или иное имущество получено в</p>  | <p>Развитие информационной инфраструктуры создало предпосылки для широкого распространения преступлений в сфере телекоммуникаций и компьютерной информации как внутри страны, так и за рубежом. Электронные банки и системы электронной оплаты предоставляют практически неограниченные возможности для легализации денежных средств. Кроме того, новые информационно-финансовые инструменты обладают такими качествами как удобство, оперативность и анонимность, что, несомненно, порождает увеличение спроса и предложений, на рынке незаконных финансовых услуг.</p> |



|   |   |   |
|---|---|---|
| <p>средства или иное имущество получено в результате преступной деятельности, —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказывается лишением свободы от пяти до десяти лет.</p>   | <p>результате преступной деятельности, <b>путем использования средств компьютерной техники, телекоммуникационных сетей и информационно-коммуникационных технологий, равно сети Интернет</b> —</p> <p>наказывается лишением свободы от пяти до десяти лет.</p>   | <p>В Интернете уже существуют аукционы, виртуальные казино и «финансовые ворота», с помощью которых все операции финансового рынка становятся доступными. Более того, новое поколение информационных технологий повысило возможности для спекулятивных и иных махинаций и просто не оставило большинству компаний времени на традиционные способы накопления капитала, на повышение выживаемости на основе легитимных способов получения доходов.</p> <p>С учетом вышеуказанного предлагается дополнить статью 243 УК Республики Узбекистан.</p>  |
| <p><b>Статья 251<sup>1</sup>. Незаконный оборот сильнодействующих или ядовитых веществ</b></p> <p>Незаконное изготовление, переработка, приобретение, хранение, перевозка или пересылка с целью сбыта, а равно незаконный сбыт сильнодействующих или ядовитых веществ, не являющихся наркотическими средствами, их аналогами или психотропными веществами, либо оборудования для их изготовления или переработки —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказываются ограничением свободы от одного года до трех лет либо лишением свободы на срок до трех лет.</p> | <p><b>Статья 251<sup>1</sup>. Незаконный оборот сильнодействующих или ядовитых веществ</b></p> <p>Незаконное изготовление, переработка, приобретение, хранение, перевозка или пересылка с целью сбыта, а равно незаконный сбыт сильнодействующих или ядовитых веществ, не являющихся наркотическими средствами, их аналогами или психотропными веществами, либо оборудования для их изготовления или переработки <b>с использованием средств компьютерной техники, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет</b> —</p> <p>наказываются ограничением свободы от одного года до трех лет либо лишением свободы на срок до трех лет.</p> | <p>Для совершения преступлений по изготовлению, переработке, приобретению, хранения, перевозке или пересылке с целью сбыта, а равно незаконный сбыт сильнодействующих или ядовитых веществ все чаще используются устройства, в основе которых лежат информационно-коммуникационные технологии и компьютерные средства их изготовления и функционирования.</p> <p>В сети Интернет на некоторых сайтах можно найти советы, чертежи, рекомендации по изготовлению, переработке, приобретению, хранения, перевозке или пересылке с целью сбыта, а равно незаконный сбыт сильнодействующих или ядовитых веществ, что можно расценивать как интеллектуальное пособничество. В связи с этим, следует внести изменения в статью 251<sup>1</sup> УК Республики Узбекистан.</p> |

|   |   |   |
|---|---|---|
| <p>Те же действия, совершенные повторно или группой лиц по предварительномуговору, —<br/>наказываются ограничением свободы от трех до пяти лет либо лишением свободы от трех до пяти лет.<br/>Действия, предусмотренные частью первой настоящей статьи, совершенные организованной группой либо в крупном размере, —<br/>наказываются лишением свободы от пяти до десяти лет.<br/>Нарушение правил производства, приобретения, хранения, учета, отпуска, перевозки или пересылки сильнодействующих или ядовитых веществ, если это повлекло по неосторожности их хищение либо причинение иного существенного вреда, —<br/>наказывается штрафом от пятидесяти до ста базовых расчетных величин или исправительными работами до трех лет или ограничением свободы от двух до пяти лет либо лишением свободы до пяти лет.</p> | <p>Те же действия, совершенные повторно или группой лиц по предварительномуговору, —<br/>наказываются ограничением свободы от трех до пяти лет либо лишением свободы от трех до пяти лет.<br/>Действия, предусмотренные частью первой настоящей статьи, совершенные организованной группой либо в крупном размере, —<br/>наказываются лишением свободы от пяти до десяти лет.<br/>Нарушение правил производства, приобретения, хранения, учета, отпуска, перевозки или пересылки сильнодействующих или ядовитых веществ, если это повлекло по неосторожности их хищение либо причинение иного существенного вреда, —<br/>наказывается штрафом от пятидесяти до ста базовых расчетных величин или исправительными работами до трех лет или ограничением свободы от двух до пяти лет либо лишением свободы до пяти лет.</p> |   |
| <p><b>Статья 255<sup>1</sup>. Разработка, производство, накопление, приобретение, передача, хранение, незаконное завладение и иные действия с бактериологическим, химическим и другими видами оружия массового уничтожения</b><br/>Разработка, производство, накопление, приобретение, передача, хранение, незаконное завладение и иные действия с бактериологическим (биологическим), химическим и другими видами оружия</p>   | <p><b>Статья 255<sup>1</sup>. Разработка, производство, накопление, приобретение, передача, хранение, незаконное завладение и иные действия с бактериологическим, химическим и другими видами оружия массового уничтожения</b><br/>Разработка, производство, накопление, приобретение, передача, хранение, незаконное завладение и иные действия с бактериологическим (биологическим), химическим и другими видами оружия</p>   | <p>Для совершения преступлений по разработке, производства, накоплении, приобретении, передаче, хранении, незаконное завладение и иные действия с бактериологическим, химическим и другими видами оружия массового уничтожения все чаще используются устройства, в основе которых лежат информационно-коммуникационные технологии и компьютерные средства их изготовления и функционирования.</p> |

|   |   |   |
|---|---|---|
| <p>массового уничтожения, запрещенного международными договорами Республики Узбекистан, —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказывается лишением свободы от пяти до восьми лет.</p> <p>Те же деяния, повлекшие:</p> <p>а) смерть человека;</p> <p>б) иные тяжкие последствия, — наказываются лишением свободы от восьми до пятнадцати лет.</p>  | <p>массового уничтожения, запрещенного международными договорами Республики Узбекистан, <b>с использованием средств компьютерной техники, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет</b> —</p> <p>наказывается лишением свободы от пяти до восьми лет.</p> <p>Те же деяния, повлекшие:</p> <p>а) смерть человека;</p> <p>б) иные тяжкие последствия, — наказываются лишением свободы от восьми до пятнадцати лет.</p>  | <p>В сети Интернет на некоторых сайтах можно найти советы, чертежи, рекомендации по разработке, производства, накоплению, приобретению, передаче, хранении, незаконное завладение и иные действия с бактериологическим, химическим и другими видами оружия, что можно расценивать как интеллектуальное пособничество. В связи с этим, следует внести изменения в статью 255<sup>1</sup> УК Республики Узбекистан.</p>   |
| <p><b>Статья 270. Культивирование запрещенных к возделыванию культур</b></p> <p>Культивирование, то есть незаконный посев или выращивание опийного или масличного мака, растения каннабис либо других растений, содержащих наркотические средства или психотропные вещества, —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказывается штрафом от двадцати пяти до пятидесяти базовых расчетных величин или обязательными общественными работами до трехсот шестидесяти часов или исправительными работами до трех лет либо ограничением свободы от одного года до трех лет или лишением свободы до трех лет.</p> <p>То же действие, совершенное:</p> | <p><b>Статья 270. Культивирование запрещенных к возделыванию культур</b></p> <p>Культивирование, то есть незаконный посев или выращивание опийного или масличного мака, растения каннабис либо других растений, содержащих наркотические средства или психотропные вещества, <b>с использованием средств компьютерной техники, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет</b> —</p> <p>наказывается штрафом от двадцати пяти до пятидесяти базовых расчетных величин или обязательными общественными работами до трехсот шестидесяти часов или исправительными работами до трех лет либо ограничением свободы от одного года до трех лет или лишением свободы до трех лет.</p> <p>То же действие, совершенное:</p> | <p>Для совершения преступлений по посеве или выращиванию опийного или масличного мака, растения каннабис либо других растений, содержащих наркотические средства или психотропные вещества все чаще используются устройства, в основе которых лежат информационно-коммуникационные технологии и компьютерные средства их изготовления и функционирования.</p> <p>В сети Интернет на некоторых сайтах можно найти советы, чертежи, рекомендации по посеве или выращиванию опийного или масличного мака, растения каннабис либо других растений, содержащих наркотические средства или психотропные вещества, что можно расценивать как интеллектуальное пособничество. В связи с этим, следует внести изменения в статью 270 УК Республики Узбекистан.</p> |

|  |  |  |
|--|--|--|
| <p>а) лицом, ранее совершившим преступление, составляющее незаконный оборот наркотических средств или психотропных веществ;</p> <p>б) по предварительному сговору группой лиц;</p> <p>в) на площади средней величины, — наказывается штрафом от пятидесяти до ста базовых расчетных величин или ограничением свободы от трех до пяти лет либо лишением свободы от трех до пяти лет.</p> <p>То же действие, совершенное:</p> <p>а) особо опасным рецидивистом;</p> <p>б) организованной группой или в ее интересах;</p> <p>в) на площади большой величины, — наказывается лишением свободы от пяти до десяти лет.</p> | <p>а) лицом, ранее совершившим преступление, составляющее незаконный оборот наркотических средств или психотропных веществ;</p> <p>б) по предварительному сговору группой лиц;</p> <p>в) на площади средней величины, — наказывается штрафом от пятидесяти до ста базовых расчетных величин или ограничением свободы от трех до пяти лет либо лишением свободы от трех до пяти лет.</p> <p>То же действие, совершенное:</p> <p>а) особо опасным рецидивистом;</p> <p>б) организованной группой или в ее интересах;</p> <p>в) на площади большой величины, — наказывается лишением свободы от пяти до десяти лет.</p> |  |
| <p><b>Статья 273. Незаконное изготовление, приобретение, хранение и другие действия с наркотическими средствами, их аналогами или психотропными веществами с целью сбыта, а равно их сбыт</b></p> <p>Незаконное изготовление, приобретение, хранение, провоз или пересылка с целью сбыта, а равно сбыт наркотических средств, их аналогов или психотропных веществ в небольших размерах —</p> <p style="text-align: center;"><b>дополняется</b></p>  | <p><b>Статья 273. Незаконное изготовление, приобретение, хранение и другие действия с наркотическими средствами, их аналогами или психотропными веществами с целью сбыта, а равно их сбыт</b></p> <p>Незаконное изготовление, приобретение, хранение, провоз или пересылка с целью сбыта, а равно сбыт наркотических средств, их аналогов или психотропных веществ в небольших размерах <b>с использованием средств компьютерной техники, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет</b> —</p>  | <p>Для совершения преступлений по изготовлению, приобретению, хранению, провозе или пересылке с целью сбыта, а равно сбыт наркотических средств, их аналогов или психотропных веществ в небольших размерах все чаще используются устройства, в основе которых лежат информационно-коммуникационные технологии и компьютерные средства их изготовления и функционирования.</p> <p>В сети Интернет на некоторых сайтах можно найти советы, чертежи, рекомендации по изготовлению, приобретению, хранению, провозе или пересылке с целью сбыта, а равно сбыт наркотических средств, их аналогов или психотропных веществ в небольших размерах, что можно расценивать как интеллектуальное пособничество. В связи с этим, следует внести</p> |

|   |   |   |
|---|---|---|
| <p>наказывается ограничением свободы от трех до пяти лет или лишением свободы от трех до пяти лет.</p> <p>Деяния, предусмотренные частью первой настоящей статьи, совершенные в размерах, превышающих небольшой, — наказываются лишением свободы от пяти до семи лет.</p> <p>Деяния, предусмотренные частью первой или второй настоящей статьи, совершенные:</p> <p>а) лицом, ранее совершившим преступление, составляющее незаконный оборот наркотических средств или психотропных веществ;</p> <p>б) по предварительному сговору группой лиц;</p> <p>в) в местах отбывания наказания в виде лишения свободы;</p> <p>г) в учебных заведениях или в других местах, которые используются школьниками, студентами для проведения учебных, спортивных или общественных мероприятий, — наказываются лишением свободы от семи до десяти лет.</p> <p>Незаконное изготовление или переработка наркотических средств, их аналогов или психотропных веществ в лабораториях или с использованием средств и оборудования, являющихся чужой собственностью либо с использованием прекурсоров, а равно организация или содержание притонов для потребления или распространения этих средств, а также</p> | <p>наказывается ограничением свободы от трех до пяти лет или лишением свободы от трех до пяти лет.</p> <p>Деяния, предусмотренные частью первой настоящей статьи, совершенные в размерах, превышающих небольшой, — наказываются лишением свободы от пяти до семи лет.</p> <p>Деяния, предусмотренные частью первой или второй настоящей статьи, совершенные:</p> <p>а) лицом, ранее совершившим преступление, составляющее незаконный оборот наркотических средств или психотропных веществ;</p> <p>б) по предварительному сговору группой лиц;</p> <p>в) в местах отбывания наказания в виде лишения свободы;</p> <p>г) в учебных заведениях или в других местах, которые используются школьниками, студентами для проведения учебных, спортивных или общественных мероприятий, — наказываются лишением свободы от семи до десяти лет.</p> <p>Незаконное изготовление или переработка наркотических средств, их аналогов или психотропных веществ в лабораториях или с использованием средств и оборудования, являющихся чужой собственностью либо с использованием прекурсоров, а равно организация или содержание притонов для потребления или распространения этих средств, а также</p> | <p>изменения в статью 273 УК Республики Узбекистан.</p> |
|---|---|---|

|   |   |  |
|---|---|--|
| <p>деяния, предусмотренные частью второй или третьей настоящей статьи, совершенные:</p> <p>а) особо опасным рецидивистом;</p> <p>б) организованной группой или в ее интересах, —</p> <p>наказывается лишением свободы от десяти до пятнадцати лет.</p> <p>Незаконная продажа наркотических средств, их аналогов или психотропных веществ в крупных размерах, —</p> <p>наказывается лишением свободы от десяти до двадцати лет.</p> <p>Лицо, совершившее деяния, предусмотренные частью первой настоящей статьи, освобождается от наказания, если оно добровольно явилось с повинной в органы власти и сдало наркотические средства, их аналоги или психотропные вещества.</p> | <p>деяния, предусмотренные частью второй или третьей настоящей статьи, совершенные:</p> <p>а) особо опасным рецидивистом;</p> <p>б) организованной группой или в ее интересах, —</p> <p>наказывается лишением свободы от десяти до пятнадцати лет.</p> <p>Незаконная продажа наркотических средств, их аналогов или психотропных веществ в крупных размерах, —</p> <p>наказывается лишением свободы от десяти до двадцати лет.</p> <p>Лицо, совершившее деяния, предусмотренные частью первой настоящей статьи, освобождается от наказания, если оно добровольно явилось с повинной в органы власти и сдало наркотические средства, их аналоги или психотропные вещества.</p> |  |
| <p><b>Статья 276. Незаконное изготовление, приобретение, хранение и другие действия с наркотическими средствами, их аналогами или психотропными веществами без цели сбыта</b></p> <p>Незаконные изготовление, хранение, приобретение, провоз или пересылка наркотических средств, их аналогов или психотропных веществ без цели сбыта —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказываются штрафом до пятидесяти базовых расчетных величин или обязательными общественными работами до</p>   | <p><b>Статья 276. Незаконное изготовление, приобретение, хранение и другие действия с наркотическими средствами, их аналогами или психотропными веществами без цели сбыта</b></p> <p>Незаконные изготовление, хранение, приобретение, провоз или пересылка наркотических средств, их аналогов или психотропных веществ без цели сбыта <b>с использованием средств компьютерной техники, телекоммуникационных сетей и информационно-коммуникационных технологий, а равно сети Интернет</b> —</p> <p>наказываются штрафом до пятидесяти базовых расчетных величин или обязательными общественными работами до</p>   | <p>Для совершения преступлений по изготовлению, приобретению, хранении и другие действия с наркотическими средствами, их аналогами или психотропными веществами без цели сбыта все чаще используются устройства, в основе которых лежат информационно-коммуникационные технологии и компьютерные средства их изготовления и функционирования.</p> <p>В сети Интернет на некоторых сайтах можно найти советы, чертежи, рекомендации по изготовлению, приобретению, хранении и другие действия с наркотическими средствами, их аналогами или психотропными веществами без цели сбыта, что можно расценивать как интеллектуальное</p> |

|  |  |  |
|--|--|--|
| <p>трехсот шестидесяти часов или исправительными работами до трех лет либо ограничением свободы от одного года до трех лет или лишением свободы до трех лет.</p> <p>Те же деяния, совершенные:</p> <p>а) в крупном размере;</p> <p>б) лицом, ранее совершившим преступление, составляющее незаконный оборот наркотических средств или психотропных веществ, —</p> <p>наказываются ограничением свободы от трех до пяти лет либо лишением свободы от трех до пяти лет.</p> <p>Лицо, совершившее деяния, предусмотренные частью первой настоящей статьи, освобождается от наказания, если оно добровольно явилось с повинной в органы власти и сдало наркотические средства, их аналоги или психотропные вещества.</p> | <p>трехсот шестидесяти часов или исправительными работами до трех лет либо ограничением свободы от одного года до трех лет или лишением свободы до трех лет.</p> <p>Те же деяния, совершенные:</p> <p>а) в крупном размере;</p> <p>б) лицом, ранее совершившим преступление, составляющее незаконный оборот наркотических средств или психотропных веществ, —</p> <p>наказываются ограничением свободы от трех до пяти лет либо лишением свободы от трех до пяти лет.</p> <p>Лицо, совершившее деяния, предусмотренные частью первой настоящей статьи, освобождается от наказания, если оно добровольно явилось с повинной в органы власти и сдало наркотические средства, их аналоги или психотропные вещества.</p> | <p>пособничество. В связи с этим, следует внести изменения в статью 276 УК Республики Узбекистан.</p>  |
| <p><b>Статья 278<sup>1</sup>. Нарушение правил информатизации</b></p> <p>Нарушение правил <b>информатизации</b>, то есть создание, внедрение и эксплуатация информационных систем, баз и банков данных, систем обработки и передачи информации, санкционированный доступ в информационные системы без принятия установленных мер защиты, причинившее крупный ущерб либо существенный вред правам или охраняемым законом интересам граждан либо государственным или общественным интересам, —</p>   | <p><b>Статья 278<sup>1</sup>. Нарушение правил эксплуатации информационных ресурсов</b></p> <p>Нарушение правил <b>эксплуатации информационных ресурсов</b>, то есть создание, внедрение и эксплуатация информационных систем, баз и банков данных, систем обработки и передачи информации в процессе эксплуатации информационных ресурсов, санкционированный доступ в информационные системы без принятия установленных мер защиты, а равно незаконный (несанкционированный) доступ к ним, причинившее крупный ущерб либо существенный вред правам или охраняемым</p>   | <p>Для обозначения актуальности и важности точного определения, а также указания конкретного объекта преступного посягательства вносятся редакционные изменения.</p> |

|   |   |   |
|---|---|---|
| <p>наказывается штрафом до пятидесяти минимальных размеров заработной платы или исправительными работами до одного года.</p> <p>Те же действия, совершенные с причинением особо крупного ущерба, — наказываются штрафом от пятидесяти до ста минимальных размеров заработной платы или исправительными работами от одного года до двух лет.</p>   | <p>законом интересам граждан либо государственным или общественным интересам, —</p> <p>наказывается штрафом до пятидесяти минимальных размеров заработной платы или исправительными работами до одного года.</p> <p>Те же действия, совершенные с причинением особо крупного ущерба, — наказываются штрафом от пятидесяти до ста минимальных размеров заработной платы или исправительными работами от <b>одного года до двух лет либо ограничением свободы до шести месяцев.</b></p>   |   |
| <p><b>Статья 278<sup>2</sup>. Незаконный (несанкционированный) доступ к компьютерной информации</b></p> <p>Незаконный (несанкционированный) доступ к компьютерной информации, то есть информации в информационно-вычислительных системах, сетях и их составных частях, если это действие повлекло уничтожение, блокирование, модификацию, копирование либо перехват информации, <b>нарушение работы электронно-вычислительных машин, системы электронно-вычислительных машин или их сети</b>, —</p> <p>наказывается штрафом до ста минимальных размеров заработной платы или лишением определенного права до трех лет либо исправительными работами до одного года.</p> <p>То же действие, совершенное:</p> | <p><b>Статья 278<sup>2</sup>. Незаконный (несанкционированный) доступ к компьютерной информации</b></p> <p>Незаконный (несанкционированный) доступ к компьютерной информации, то есть информации, <b>находящейся в компьютере или иных устройствах обработки данных, информационной системе, базах и банках данных, системах обработки и передачи информации</b>, если это действие повлекло уничтожение, блокирование, копирование либо перехват информации, —</p> <p>наказывается штрафом до ста минимальных размеров заработной платы или лишением определенного права до трех лет либо исправительными работами до одного года.</p> <p>То же действие, совершенное:</p> <p>а) по предварительному сговору группой лиц;</p> <p>б) повторно или опасным рецидивистом;</p> | <p>Закон Республики Узбекистан «О гарантиях и свободе доступа к информации» определяет, что каждому гражданину гарантируется право доступа к информации и государство защищает права каждого на поиск, получение, исследование, передачу и распространение информации. Особо указано, что государственные органы, органы самоуправления граждан, общественные объединения, предприятия, учреждения, организации и должностные лица не могут предоставлять информацию, содержащую государственную или иную охраняемую законом тайну.</p> <p>Поэтому злоумышленники могут предпринимать меры по взлому сайтов или других информационных ресурсов государственных органов и организаций. К примеру, 19 ноября 2013 года хакерская группировка Bangladesh Grey Hat Hackers взломала веб-сайты газеты «Народное слово» и</p> |



|  |   |   |
|--|---|---|
| <p>а) по предварительному сговору группой лиц;</p> <p>б) повторно или опасным рецидивистом;</p> <p>в) с использованием служебного положения;</p> <p>г) организованной группой или в ее интересах, —</p> <p>наказывается штрафом от ста до трехсот минимальных размеров заработной платы или исправительными работами от одного года до двух лет или ограничением свободы от одного года до трех лет либо лишением свободы до трех лет.</p> <p style="text-align: center;"><b>дополняется</b></p> | <p>в) с использованием служебного положения;</p> <p>г) организованной группой или в ее интересах, —</p> <p>наказывается штрафом от ста до трехсот минимальных размеров заработной платы или исправительными работами от одного года до двух лет или ограничением свободы от одного года до трех лет либо лишением свободы до трех лет.</p> <p><b>Действия, предусмотренные частью первой или второй настоящей статьи, повлекшие нарушение функционирования Национальной информационной сферы, —</b></p> <p><b>наказываются штрафом от трехсот до шестисот минимальных размеров заработной платы или ограничением свободы до трех лет либо лишением свободы до трех лет.</b></p> | <p>ее узбекской версии «Халқ сўзи». Аналогичный случай с республиканской газетой имел место и 27 марта 2016 года. Тогда на главных страницах сайтов была размещена заставка группы, называющей себя Anonplus. В результате взлома главные страницы газет были изменены. 20 ноября 2017 года были недоступны сайты Министерства юстиции, хокимията Ташкента, Государственного центра тестирования и другие сайты государственных учреждений и организаций. При поиске адресов этих сайтов в Google в результатах можно было увидеть фразу «Hacked By Skidie KhaN : : : TeaM Cyber CommandOs», что говорит об их дефейсе (замена главных страниц). Однако, к сожалению, в Уголовном кодексе не предусматривается специальная норма, устанавливающая ответственность за несанкционированный доступ к государственным информационным ресурсам и системам.</p> |
| <p><b>Статья 278<sup>3</sup>. Изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе</b></p> <p>Изготовление с целью сбыта либо сбыт и распространение специальных программных или аппаратных средств для получения незаконного (несанкционированного) доступа к <b>защищенной компьютерной системе</b> —</p> <p style="text-align: center;"><b>дополняется</b></p>                          | <p><b>Статья 278<sup>3</sup>. Изготовление с целью сбыта либо сбыт, использование или распространение специальных программных или аппаратных средств для получения незаконного (несанкционированного) доступа к защищенным информационным ресурсам, а равно для негласного получения информации</b></p> <p>Изготовление с целью сбыта либо сбыт, <b>использование или</b> распространение специальных программных или аппаратных средств для получения незаконного (несанкционированного) доступа к <b>защищенным информационным</b></p>  | <p>Для обозначения актуальности и важности точного определения, а также указания конкретного объекта преступного посягательства вносятся редакционные изменения.</p>  |

|  |   |   |
|--|---|---|
| <p>наказывается штрафом до двухсот минимальных размеров заработной платы или исправительными работами до одного года.</p> <p>Те же действия, совершенные:</p> <p>а) по предварительному сговору группой лиц;</p> <p>б) повторно или опасным рецидивистом;</p> <p>в) с использованием служебного положения;</p> <p>г) организованной группой или в ее интересах, —</p> <p>наказываются штрафом от двухсот до трехсот минимальных размеров заработной платы или исправительными работами от одного года до трех лет.</p> | <p><b>ресурсам, а равно для негласного получения информации, -</b></p> <p>наказывается штрафом до двухсот минимальных размеров заработной платы или исправительными работами до одного года.</p> <p>Те же действия, совершенные:</p> <p>а) по предварительному сговору группой лиц;</p> <p>б) повторно или опасным рецидивистом;</p> <p>в) с использованием служебного положения;</p> <p>г) организованной группой или в ее интересах, —</p> <p>наказываются штрафом от двухсот до трехсот минимальных размеров заработной платы или исправительными работами от одного года до трех лет.</p> |   |
| <p><b>Статья 278<sup>4</sup>. Модификация компьютерной информации</b></p> <p>Модификация компьютерной информации, то есть незаконное изменение, повреждение, стирание информации, хранящейся в компьютерной системе, а равно внесение в нее заведомо ложной информации, причинившее крупный ущерб либо существенный вред правам или охраняемым законом интересам граждан либо государственным или общественным интересам, —</p> <p style="text-align: center;"><b>дополняется</b></p>                                  | <p><b>Статья 278<sup>5</sup>. Модификация компьютерной информации</b></p> <p>Модификация компьютерной информации, то есть незаконное изменение, повреждение, стирание информации, хранящейся в компьютерной системе, а равно внесение в нее заведомо ложной информации, <b>повлекшее нарушение работы электронно-вычислительных машин, системы электронно-вычислительных машин или их сети,</b> причинившее крупный ущерб либо существенный вред правам или охраняемым законом интересам граждан либо государственным или общественным интересам, —</p>                                       | <p>С учетом того, что модификация компьютерной информации может повлечь за собой нарушение работы электронно-вычислительных машин, системы электронно-вычислительных машин или их сети, предлагается расширить диспозицию части первой статьи 278<sup>4</sup> УК Республики Узбекистан.</p> |

|   |   |  |
|---|---|--|
| <p>наказывается штрафом до ста минимальных размеров заработной платы или исправительными работами до одного года или ограничением свободы до двух лет либо лишением свободы до двух лет.</p> <p>Те же действия, совершенные:</p> <p>а) с причинением особо крупного ущерба;</p> <p>б) по предварительному сговору группой лиц;</p> <p>в) повторно или опасным рецидивистом,</p> <p>—</p> <p>наказываются исправительными работами от одного года до двух лет или ограничением свободы от двух до трех лет либо лишением свободы от двух до трех лет.</p>  | <p>наказывается штрафом до ста минимальных размеров заработной платы или исправительными работами до одного года или ограничением свободы до двух лет либо лишением свободы до двух лет.</p> <p>Те же действия, совершенные:</p> <p>а) с причинением особо крупного ущерба;</p> <p>б) по предварительному сговору группой лиц;</p> <p>в) повторно или опасным рецидивистом,</p> <p>—</p> <p>наказываются исправительными работами от одного года до двух лет или ограничением свободы от двух до трех лет либо лишением свободы от двух до трех лет.</p>  |  |
| <p><b>Статья 278<sup>5</sup>. Компьютерный саботаж</b></p> <p>Умышленный вывод из строя чужого или служебного компьютерного оборудования, а равно разрушение компьютерной системы (компьютерный саботаж) —</p> <p style="text-align: center;"><b>дополняется</b></p> <p>наказывается штрафом от трехсот до четырехсот минимальных размеров заработной платы с лишением определенного права до трех лет или ограничением свободы до двух лет либо лишением свободы до двух лет.</p> <p>Те же действия, совершенные:</p> <p>а) по предварительному сговору группой лиц;</p> <p>б) повторно или опасным рецидивистом,</p> <p>—</p> | <p><b>Статья 278<sup>6</sup>. Компьютерный саботаж</b></p> <p>Умышленный вывод из строя компьютерного оборудования <b>или иных устройств обработки данных, информационной системы, баз и банков данных, систем обработки и передачи информации,</b> а равно разрушение компьютерной системы (компьютерный саботаж) —</p> <p>наказывается штрафом от трехсот до четырехсот минимальных размеров заработной платы с лишением определенного права до трех лет или ограничением свободы до двух лет либо лишением свободы до двух лет.</p> <p>Те же действия, совершенные:</p> <p>а) по предварительному сговору группой лиц;</p> <p>б) повторно или опасным рецидивистом,</p> <p>—</p> | <p>Для обозначения актуальности и важности точного определения, а также указания конкретного объекта преступного посягательства вносятся редакционные изменения.</p> |

|  |  |  |
|--|--|--|
| <p>наказываются исправительными работами от двух до трех лет или ограничением свободы от двух до трех лет либо лишением свободы от двух до трех лет.</p>   | <p>наказываются исправительными работами от двух до трех лет или ограничением свободы от двух до трех лет либо лишением свободы от двух до трех лет.</p>   |  |
| <p><b>Статья 278<sup>6</sup>. Создание, использование или распространение вредоносных программ</b><br/> Создание компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации, копирования или перехвата информации, хранящейся или передаваемой в <b>компьютерной системе</b>, а равно разработка специальных вирусных программ, их умышленное использование или распространение —</p> <p>наказывается штрафом от ста до трехсот минимальных размеров заработной платы или ограничением свободы до двух лет либо лишением свободы до двух лет.</p> <p>Те же действия, совершенные:</p> <p>а) с причинением особо крупного ущерба;</p> <p>б) по предварительному сговору группой лиц;</p> <p>в) повторно или опасным рецидивистом;</p> <p>г) организованной группой или в ее интересах, —</p> <p>наказываются ограничением свободы от двух до трех лет либо лишением свободы от двух до трех лет.</p> | <p><b>Статья 278<sup>7</sup>. Создание, использование или распространение вредоносных программ</b><br/> Создание компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации, копирования или перехвата информации, хранящейся или передаваемой в <b>информационной системе, базах и банках данных, системах обработки и передачи информации, вывода из строя оборудования</b>, а равно разработка в этих целях специальных вирусных программ, их умышленное использование или распространение —</p> <p>наказывается штрафом от ста до трехсот минимальных размеров заработной платы или ограничением свободы до двух лет либо лишением свободы до двух лет.</p> <p>Те же действия, совершенные:</p> <p>а) с причинением особо крупного ущерба;</p> <p>б) по предварительному сговору группой лиц;</p> <p>в) повторно или опасным рецидивистом;</p> <p>г) организованной группой или в ее интересах, —</p> <p>наказываются ограничением свободы от двух до трех лет либо лишением свободы от двух до трех лет.</p> | <p>Для обозначения актуальности и важности точного определения, а также указания конкретного объекта преступного посягательства вносятся редакционные изменения.</p> |

**ЗАКОН РЕСПУБЛИКИ УЗБЕКИСТАН**  
**О борьбе с преступлениями**  
**в сфере информационных технологии**

**Глава 1. Общие положения**

**Статья 1. Цель настоящего Закона**

Целью настоящего Закона является регулирование отношений в области борьбы с преступлениями в сфере информационных технологии.

**Статья 2. Законодательство о борьбе с преступлениями в сфере информационных технологии**

Законодательство о борьбе с преступлениями в сфере информационных технологии состоит из настоящего Закона и иных актов законодательства.

Если международным договором Республики Узбекистан установлены иные правила, чем те, которые предусмотрены в законодательстве Республики Узбекистан о борьбе с преступлениями в сфере информационных технологии, то применяются правила международного договора.

**Статья 3. Основные понятия**

В настоящем Законе применяются следующие основные понятия:

*компьютерная система* – любое устройство или совокупность взаимосвязанных, или смежных устройств, одно или несколько из которых, действуя в соответствии с программой, осуществляют автоматическую обработку данных;

*компьютерные данные* – любое представление фактов, сведений или понятий в форме, пригодной для обработки с помощью компьютерной системы, в том числе программы, предназначенные для выполнения компьютерной системой тех или иных действий;

*поставщик услуг* – любая физические или юридические лица, государственные органы или иные организации, предоставляющая пользователям оказываемых ею услуг возможность обмениваться данными посредством компьютерной системы, а также любая другая организация, осуществляющая обработку или хранение компьютерных данных по поручению службы связи или пользователей ее услуг;

*данные об информационных потоках* – любые данные, связанные с операциями по передаче информации посредством компьютерной системы, которые генерируются компьютерной системой, являющейся звеном соответствующей коммуникационной цепочки, и указывают на источник,

назначение, маршрут, время, дату, размер, продолжительность или тип соответствующего сетевого сервиса;

*меры безопасности* – применение процедур, устройств или специализированных компьютерных программ, с помощью которых доступ к какой-либо компьютерной системе ограничен либо запрещен для некоторых категорий пользователей.

### **Статья 3. Основные принципы борьбы с преступлениями в сфере информационных технологии**

Основными принципами борьбы с преступлениями в сфере информационных технологии являются:

- 1) законность;
- 2) приоритет прав, свобод и законных интересов человека;
- 3) сочетание гласных и негласных методов;
- 4) неизбежность наказания;
- 5) компьютерная безопасность и защита персональных данных;

## **Глава 2. Органы, осуществляющие борьбу с преступлениями в сфере информационных технологии, их правовой статус**

### **Статья 4. Полномочия государственных органов в области борьбы с преступлениями в сфере информационных технологии**

Генеральная прокуратура Республики Узбекистан и Департамент по борьбе с экономическими преступлениями при Генеральной прокуратуре Республики Узбекистан составляют и постоянно актуализируют базы данных о преступлениях в сфере информационных технологии.

Департамент по борьбе с экономическими преступлениями при Генеральной прокуратуре Республики Узбекистан осуществляет оперативно-розыскную деятельность, уголовное преследование, международное сотрудничество, идентификацию лиц, совершивших преступления в сфере информационных технологии.

Департамент по борьбе с экономическими преступлениями при Генеральной прокуратуре Республики Узбекистан совместно с другими органами и организациями осуществляет мероприятия по предупреждению и борьбе с преступлениями в сфере информационных технологии, представляющей угрозу национальной безопасности, проводит оперативно-розыскные мероприятия, принимает меры по выявлению связей международных преступных организаций, осуществляет другие мероприятия в пределах своей компетенции.

Генеральная прокуратура:

координирует, руководит и осуществляет уголовное преследование в порядке, предусмотренном законом;

распоряжается, в рамках осуществления уголовного преследования в связи с обращением органа уголовного преследования или по собственной инициативе, о незамедлительном сохранении компьютерных данных или данных об информационных потоках, в отношении которых существует опасность их уничтожения или повреждения, в соответствии с уголовно-процессуальным законодательством;

предъявляет от имени государства обвинение в судебных инстанциях в порядке, предусмотренном законом.

Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан совместно со Департамент по борьбе с экономическими преступлениями при Генеральной прокуратуре Республики Узбекистан представляют предложения по обеспечению защиты и безопасности компьютерных данных.

Академия Генеральной прокуратуры Республики Узбекистан обеспечивает профессиональное совершенствование персонала, задействованного в осуществлении правосудия в области борьбы с преступлениями в сфере информационных технологии и иные возложенные задачи.

## **Статья 5. Взаимодействие компетентных органов в области борьбы с преступлениями в сфере информационных технологии**

В рамках деятельности по борьбе с преступлениями в сфере информационных технологии государственные органы и иные организации, поставщики услуг, негосударственные организации, другие представители гражданского общества сотрудничают посредством обмена информацией, экспертами, путем проведения совместной деятельности по раскрытию преступлений и выявлению преступников, обучения персонала, реализации инициатив в целях осуществления программ, практик, мер, процедур, реализации минимальных стандартов безопасности компьютерных систем, организуют кампании по информированию о компьютерной преступности и рисках, которым подвергаются пользователи компьютерных систем, а также осуществляют иную деятельность в данной области.

## **Статья 6. Обязанности собственников компьютерных систем**

Собственники компьютерных систем, доступ к которым запрещен или ограничен для некоторых категорий пользователей, обязаны предупредить пользователей о правовых условиях доступа и пользования, а также о правовых последствиях несанкционированного доступа к этим компьютерным системам. Предупреждение должно быть доступно для каждого пользователя.

## **Статья 7. Обязанности поставщика услуг**

Поставщики услуг обязаны:

вести учет пользователей услуг;

сообщать компетентным органам данные об информационных потоках, в том числе данные о незаконном доступе к информации из компьютерных систем, попытках внедрения незаконных программ, нарушении ответственными лицами правил сбора, обработки, хранения, распространения и распределения информации или правил защиты компьютерной системы, предусмотренных в соответствии со статусом информации или степенью ее защиты, если эти действия способствовали присвоению, преобразованию или уничтожению информации либо повлекли иные серьезные последствия, нарушение функционирования компьютерных систем, другие компьютерные нарушения;

исполнять в условиях конфиденциальности, в соответствии с национальным законодательством, запросы компетентного органа о незамедлительном сохранении компьютерных данных или данных об информационных потоках, в отношении которых существует опасность их уничтожения или повреждения, на срок не более 120 календарных дней;

предоставлять компетентным органам по запросу, сделанному в соответствии с законом, данные о пользователях, в том числе о виде сообщения и об услуге, используемой пользователем, о способе оплаты соответствующей услуги, а также любые другие данные, которые могут привести к идентификации пользователя;

принимать меры безопасности путем применения некоторых процедур, устройств или специализированных компьютерных программ, с помощью которых доступ к компьютерной системе ограничивается или запрещается для пользователей, не имеющих разрешений;

обеспечивать мониторинг, надзор и сохранение данных об информационных потоках для идентификации поставщиков услуг, пользователей услуг и канала, по которому было передано сообщение, на срок не менее 180 календарных дней;

обеспечивать расшифровку компьютерных данных, содержащихся в пакетах протоколов сети, с сохранением этих данных в течение не менее 90 календарных дней.

В случае, когда данными об информационных потоках владеют несколько поставщиков услуг, запрашиваемый поставщик услуг обязан незамедлительно предоставить в распоряжение компетентного органа информацию, необходимую для идентификации остальных поставщиков услуг.

### **Глава 3. Международное сотрудничество**

#### **Статья 8. Международное сотрудничество государственных органов**

Государственные органы Республики Узбекистан сотрудничают, в соответствии с законом и с соблюдением обязательств, предусмотренных международными соглашениями, одной из сторон которых является



Республика Узбекистан, с органами других стран, осуществляющими аналогичные функции, а также со специализированными международными организациями в данной области.

Сотрудничество предполагает: международную помощь в области уголовного права; экстрадицию; идентификацию; блокирование, секвестр и конфискацию продукции и средств преступления; осуществление совместных расследований; обмен информацией; подготовку персонала в данной области; иные подобные действия.

### **Статья 9. Совместная оперативно-розыскная деятельность и осуществление уголовного преследования**

По запросу государственных органов Республики Узбекистан или государственных органов и иных организации других государств на территории Республики Узбекистан могут осуществляться, в соответствии с законом, совместные оперативно-розыскные действия в рамках уголовного преследования в целях предупреждения и борьбы с преступностью в сфере информационных технологии.

Совместные расследования осуществляются также на основе двусторонних или многосторонних соглашений, заключенных компетентными органами.

Представители государственных органов Республики Узбекистан могут участвовать в совместных расследованиях, осуществляемых на территории других государств, с соблюдением законодательства этих государств.

### **Статья 10. Запросы государственных органов или иных организации других государств**

В рамках международного сотрудничества компетентные органы других государств могут запрашивать у государственных органов Республики Узбекистан незамедлительное сохранение компьютерных данных или данных об информационных потоках, имеющих в какой-либо компьютерной системе на территории Республики Узбекистан, в отношении которых государственный орган или иная организация другого государства должен сформулировать аргументированный запрос об оказании международной правовой помощи в области уголовного права.

Запрос о незамедлительном сохранении компьютерных данных, предусмотренный частью первой, должен содержать:

- наименование органа, делающего запрос;
- краткое представление фактов, являющихся предметом уголовного преследования, и их правовую аргументацию;
- компьютерные данные, сохранение которых запрашивается;
- любую доступную информацию, необходимую для идентификации обладателя компьютерных данных, обнаружения компьютерной системы;

полезность компьютерных данных и необходимость их сохранения;  
намерение компетентных органов других государств сформулировать запрос о предоставлении международной правовой помощи в области уголовного права.

Срок сохранения данных, предусмотренных частью первой, не может быть менее 60 календарных дней и является действительным до принятия компетентным органом Республики Узбекистан решения об оказании международной правовой помощи в области уголовного права.

Передача компьютерных данных осуществляется только после принятия запроса об оказании международной правовой помощи в области уголовного права.

#### **Глава 4. Ответственность**

##### **Статья 11. Ответственность за нарушение настоящего закона**

Нарушение настоящего закона влечет дисциплинарную, гражданскую, административную или уголовную ответственность в соответствии с законом.

#### **Глава 5. Заключительные положения**

##### **Статья 12.**

Кабинету Министров Республики Узбекистан в трехмесячный срок представить Олий Мажлису Республики Узбекистан предложения по приведению действующего законодательства в соответствие с настоящим законом.

**Президент Республики Узбекистан Ш. МИРЗИЁЕВ**

г. Ташкент

| ПРИЛОЖЕНИЕ<br>№ 4 | Несанкционированный доступ или доступ с превышением санкций | умышленное распространение вирусов | компьютерные хищения | компьютерное мошенничество | компьютерный саботаж | блокировка, копирование, изменение, уничтожение данных | нарушение работы, повреждение, уничтожение компьютерной системы | производство, исполнение оборот специальных средств не санкционированного доступа | компьютерное пиратство | нарушение конфиденциальности электронных сообщений (несанкционированный перехват) | изготовление порнографической продукции с использованием компьютерных технологий | компьютерный шпионаж (коммерческой и иной информации) | подделка записей с использованием компьютерных средств | компьютерный терроризм |
|-------------------|---|------------------------------------|----------------------|----------------------------|----------------------|--|---|---|------------------------|---|--|---|--|------------------------|
| СТРАНЫ            |   |                                    |                      |                            |                      |  |   |   |                        |   |  |   |  |                        |
| 1. США            | ✓   | ✓                                  | ✓                    | ✓                          | ✓                    | ✓  | ✓   | ✓   | ✓                      | ✓   | ✓  | ✓   |  |                        |
| 2. Великобритания | ✓   |                                    |                      |                            |                      | ✓  | ✓   |   |                        | ✓   | ✓  |   |  | ✓                      |
| 3. Австралия      | ✓   | ✓                                  | ✓                    | ✓                          | ✓                    | ✓  | ✓   | ✓   |                        | ✓   | ✓  |   |  |                        |
| 4. Швеция         | ✓   |                                    |                      | ✓                          |                      | ✓  |   |   |                        | ✓   | ✓  |   | ✓  |                        |
| 5. Германия       | ✓   | ✓                                  |                      |                            |                      | ✓  | ✓   |   | ✓                      | ✓   |  |   | ✓  |                        |
| 6. Франция        | ✓   | ✓                                  |                      |                            |                      | ✓  | ✓   |   | ✓                      | ✓   | ✓  | ✓   |  | ✓                      |
| 7. Испания        |   | ✓                                  |                      |                            |                      |  | ✓   | ✓   | ✓                      | ✓   |  |   | ✓  | ✓                      |
| 8. Голландия      | ✓   | ✓                                  | ✓                    | ✓                          |                      | ✓  | ✓   | ✓   | ✓                      | ✓   |  |   | ✓  |                        |
| 9. Дания          | ✓   |                                    |                      | ✓                          |                      |  |   |   |                        | ✓   | ✓  |   |  |                        |
| 10. Швейцария     | ✓   |                                    | ✓                    | ✓                          |                      | ✓  | ✓   | ✓   | ✓                      | ✓   |  |   | ✓  |                        |
| 11. Польша        | ✓   |                                    | ✓                    | ✓                          |                      | ✓  |   |   | ✓                      |   |  |   |  |                        |
| 12. Филиппины     | ✓   | ✓                                  |                      | ✓                          | ✓                    | ✓  | ✓   | ✓   |                        | ✓   |  |   |  | ✓                      |
| 13. Япония        |   |                                    |                      | ✓                          | ✓                    | ✓  | ✓   |   |                        | ✓   |  |   | ✓  |                        |
| 14. Эстония       | ✓   | ✓                                  |                      | ✓                          | ✓                    | ✓  | ✓   | ✓   |                        | ✓   |  |   |  | ✓                      |
| 15. Латвия        | ✓   | ✓                                  |                      |                            | ✓                    | ✓  | ✓   | ✓   |                        |   |  |   |  |                        |
| 16. Россия        | ✓   | ✓                                  |                      |                            |                      | ✓  | ✓   | ✓   |                        |   |  |   |  |                        |
| 17. Азербайджан   | ✓   | ✓                                  |                      |                            |                      | ✓  | ✓   | ✓   |                        |   |  |   |  |                        |
| 18. Грузия        | ✓   | ✓                                  |                      |                            |                      | ✓  | ✓   | ✓   |                        |   |  |   |  |                        |
| 19. Беларусь      | ✓   | ✓                                  | ✓                    |                            | ✓                    | ✓  | ✓   | ✓   |                        |   |  |   |  |                        |
| 20. Таджикистан   | ✓   | ✓                                  | ✓                    |                            | ✓                    | ✓  | ✓   | ✓   |                        |   |  |   |  |                        |
| 21. Украина       | ✓   | ✓                                  | ✓                    | ✓                          |                      | ✓  | ✓   |   |                        | ✓   |  |   |  |                        |
| 22. Казахстан     | ✓   | ✓                                  | ✓                    | ✓                          |                      | ✓  | ✓   | ✓   | ✓                      |   | ✓  | ✓   |  |                        |
| 23. Киргизия      | ✓   | ✓                                  | ✓                    | ✓                          | ✓                    | ✓  | ✓   | ✓   | ✓                      | ✓   | ✓  | ✓   |  |                        |
| 24. Узбекистан    | ✓   | ✓                                  | ✓                    | ✓                          | ✓                    | ✓  | ✓   | ✓   |                        |   | ✓  | ✓   |  |                        |