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

On the specific features of disclosure and investigation of cybercrimes

Alimjhan MATCHANOV [1]

Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

ARTICLE INFO

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

Keywords:
Cybercrime
Internet
Computer
Information and communication technologies
Crime detection
Investigation
Investigator.

ABSTRACT

The methods of dealing with cybercrime and factors for achieving a positive result are considered in the article, in order to analyse the current state of cybercrime. The author, pointing out the problems, faced by investigators in the investigation of cybercrimes, comes to the conclusion that it is necessary to improve this law enforcement activity. Particular attention is paid to a comprehensive study of problems relating to criminal-legal qualification, criminal-procedure procedures for conducting investigations, forensic techniques and tactics, intelligence-gathering and international cooperation. All this is aimed at optimizing the mechanism for conducting investigative, procedural and investigative actions to detect, record and verify digital evidence electronically. This work highlights and describes the salient features of the study of scientific, theoretical and practical problems relating to the law enforcement activities of officials of State investigative bodies, criminal investigation agencies, experts and specialists, those responsible for detecting and investigating cybercrime. The article clarifies the characteristics of the target of the attack, as expressed in the information stored on the technical media of information systems and transmitted through the communication channels of the global Internet. The author generalizes the material on the subject under study and introduces the term «investigation technology», which most fully reflects the complex mechanism, the intersectoral approach (criminal law, criminal procedure, forensics, investigative activities, forensic expertise, international criminal law, legal psychology, etc.) in the procedure of pre-trial criminal proceedings in criminal cases involving offences committed in cyberspace. The views of domestic and foreign scientists on the criminal, criminological, forensic, intelligence and international legal characteristics of cybercrime are presented. Considerable attention is paid to the

[1] DSc, Professor, Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, Tashkent, Uzbekistan
E-mail: alimjan-60@inbox.uz

subjective and objective factors contributing to the commission of the criminal acts in question, and examples are given of the most common types. The conclusion contains a list of the causes that contribute to the commission of these crimes and author's proposals to improve the algorithm of law enforcement in the detection and investigation of cybercrime.

Кибержиноятларни очиш ва тергов қилиш хусусиятлари тўғрисида

Калит сўзлар:
Кибержиноятлар
Интернет, компьютер
Информацион-коммуникацион технологиялар
Жиноятларни очиш
Тергов қилиш
Терговчи.

АННОТАЦИЯ

Мақолада кибержиноятчиликни хозирги замон ҳолатини таҳлил қилиш мақсадида, оптимал тергов қилиш ва криминалистик таъминлашга боғлиқ бўлган унга қарши курашиш ва ижобий натижани етишиш учун омиллар кўриб чиқилган. Кибержиноятларни тергов қилишда вужудга келадиган терговчиларга дуч этилиши мумкин муаммоларга муаллиф эътибор қаратган холда ушбу ҳуқуқни мухофаза қилиш фаолиятини такомиллаштириш зарурлиги тўғрисида хулосага келган. Жиноят-ҳуқуқий квалификацияси, тергов қилишнинг жиноят-процессуал тартиби, криминалистик услуби ва тактикасига, жиноятлари фош этишнинг тезкор-қидирув таъминлаш, халқаро хамкорликга алоҳида эътибор қаратилган. Бунинг барчаси тергов, процессуал харакатлар ва тезкор-қидирув таъдбирлар орқали электрон шаклида рақамли далилларни аниқлаш, қайд этиш ва текширишга қаратилган. Ушбу ишда кибержиноятларни тергов ва очишга маъсул бўлган давлат тергов, жиноят-қидирув органлари, экспертлар ва мутахассислар ҳуқуқни қўллаш фаолиятида илмий-назарий ва амалий қўлланиш муаммолар алоҳида этиборга олинади ва тасвирланади. Мақолада глобал коммуникацион алоқа Интернет тармоғи орқали узатилаётган ва информацион тизимининг техник ташувчиларда сақланилаётган ахборотда ўз ифодасини топган хусусиятлар аниқланган. Муаллиф томонидан тадқиқот олиб бораётган мавзуси бўйича материал умумлаштирилган ва илмий айланмага «тергов қилиш технологияси» атамасини киритган, ушбу комплекс механизмини кибермақонда содир этишга оид жиноят ишларни судга қадар иш юритиш жараёнида юритиш тармоқлараро ёндашиш (жиноят ҳуқуқи, жиноят процесси, криминалистика, тезкор-қидирув фаолияти, суд экспертизаси, халқаро жиноят ҳуқуқи, юридик психологияси ва бошқ.) энг тўла ифодалайди. Кибержиноятларни тавсифлашга каратилган миллий ва хорижий олимларни жиноят-ҳуқуқий, криминалогик,

криминалистик, тезкор-қидирув ва халқаро-ҳуқуқий қарашлар ифодаланган. ўрганилаётган жиноятларни содир этишга сабаб бўлган субъектив ва объектив омиллар бўлиб, бундан ташқари уларнинг энг кўп тарқалган турларига кўп эътибор қаратилган. Хулосада ушбу жиноятларни содир этишга олиб келувчи сабаблар руйхати келтирилиб, ҳуқуқни мухофаза қилувчи органлар фаолиятини алгоритмини кибержиноятларни очиш ва тергов қилишни такомиллаштиришга оид муаллифнинг фикрлари ишлаб чиқилган.

Об особенностях раскрытия и расследования киберпреступлений

Ключевые слова:
Киберпреступления
Интернет
Компьютер
Информационно-коммуникационные технологии
Раскрытие преступлений
Расследование
Следователь.

АННОТАЦИЯ

В статье, с целью анализа современного состояния киберпреступности, рассматриваются методы борьбы с ней и факторы достижения положительного результата, зависящего от оптимизации следствия и криминалистического обеспечения. Автор, указывая на проблемы, с которыми сталкиваются следователи в расследовании киберпреступлений, приходит к выводу о необходимости совершенствования данной правоохранительной деятельности. Особое внимание уделено комплексному исследованию проблем, связанных с уголовно-правовой квалификацией, уголовно-процессуальным порядком проведения расследования, криминалистической методикой и тактикой, оперативно-розыскным обеспечением раскрытия, международным сотрудничеством. Все это направлено на оптимизацию механизма проведения следственных, процессуальных действий и оперативно-розыскных мероприятий по выявлению, фиксированию и проверке цифровых доказательств в электронной форме. В данной работе выделяются и описываются характерные особенности исследования научно-теоретических и практико-прикладных проблем правоприменительной деятельности должностных лиц государственных органов следствия, уголовного розыска, экспертов и специалистов, ответственных за раскрытие и расследование киберпреступлений. В статье выяснены особенности объекта посягательства, выраженного в информации, хранящейся на технических носителях информационных систем и передаваемой по коммуникационным каналам связи глобальной сети Интернет. Автором обобщен материал по исследуемой теме и вводится в научный оборот термин «технология расследования», который наиболее полно отражает комплексный механизм, межотраслевой подход (уголовное право, уголовный процесс,

криминалистика, оперативно-розыскная деятельность, судебная экспертиза, международное уголовное право, юридическая психология и др.) к процедуре досудебного производства уголовных дел связанных с преступлениями, совершенными в киберпространстве. Излагаются взгляды отечественных и зарубежных ученых в сфере уголовно-правовых, криминологических, криминалистических, оперативно-розыскных и международно-правовых характеристик киберпреступлений. Значительное внимание уделяется субъективным и объективным факторам, способствующим совершению рассматриваемых преступных деяний, а так же приведены примеры наиболее распространённых их видов. В заключении приводится перечень причин, способствующих совершению этих преступлений, и выработаны авторские предложения по совершенствованию алгоритма деятельности правоохранительных органов в раскрытии и расследовании киберпреступлений.

INTRODUCTION

Nowadays computer and other technical information telecommunication systems, that we could use on the Internet and in local systems are very widespread, in our modern world, where everything changes fast. The brand-new virtual projection of the real world was created as a result. Almost the all spheres of our society involved in this projection, where they become transboundary. Thus, all these processes created unprecedented conditions for the exchange of information, improving the use of the telecommunication technologies in an innovative virtual space, that does not have any national borders.

In addition to the all positive sides of information communication technology (ICT), there are also some negative consequences of this reality.

Namely: the opportunities for illegal penetration into the created information and telecommunications network for the purpose of criminal enrichment or other criminal intentions. These socially-dangerous actions are called “cybercrimes” (“cyber” is a Greek word, where “cybernetics” is science of managing and exchanging information between people and machines). These crimes took a special place among such socially-dangerous transnational crimes as terrorism, extremism, drug trafficking, human trafficking, illegal arms trade, corruption.

According to the World Economic Forum in 2018, the damage to the global economy from cybercrime amounted to $1.5 trillion. In 2022, losses are projected at $8 trillion, and in 2030 they could reach $90 trillion and it is more than world GDP nowadays[1].

The potential losses from cybercrimes are estimated at $10.2 billion. About 70-80% of cybercrimes were prevented, because of the timely notification of the IC3 Center and the expeditiously investigation of incidents. The actual losses are about $3.5 billion[2].

There was an explanation in “Comprehensive Study on Cybercrime”, which is considered as the most official explanation for legislative regulation[3]. Cybercrime is any criminal activity, where the target and/or tool is a computer or network device. The result depends on the effectiveness of legal regulation and the algorithm of the procedural order of investigation.

The different criminal law, criminological and criminal procedural aspects of cybercrimes have been the object of scientific research among the scientists from different countries. Namely: A.K. Rasulev[4], R. Gayfutdinov[5], KH.R. Ochilov[6], O.M. Safonov[7], T.L. Tropinina[8] (considered criminal law, criminological aspects); V. O. Davydov[9], S. I. Zakharin[10], S. A. Kovalev[11], K. V. Kostomarov[12], S. V. Krygin[13], V. A. Meshcheryakov[14], A.D. Tlish[15], A.A. Shalevich[16], Yang Wei[17] Feng (examined issues of cybercrime investigation); Debra L. Shinder[18], Donn B.Parker[19], Brian Craig[20], Hashimoto Naoki[21] (revealed some aspects related to the fight against cybercrime). But the above scientists did not consider countering cybercrime from the point of view of an integrated approach to optimizing disclosure and investigation.

The feature of the disclosure and investigation of cybercrimes is the obligatory use of information and communication technologies. Accordingly, investigators and operational staff must know the methodology and tactics, the procedure for appointing expertise in the IT sphere. The officials, that are responsible for the detection and investigation of cybercrimes must have the necessary knowledge in ICT sphere. They must promptly react to this kind of crime.

To conclude all the above, one should note here, that nowadays there is a need to rethink and systematize the methods of disclosing and investigating cybercrimes.

THE PURPOSE OF THE STUDY

In the original article there is an analysis of the current state of the law enforcement practice of disclosing and investigating cybercrimes, identifying problems and developing proposals for improving criminal legal qualifications, procedural investigation procedures, forensic and operational-search support. The significance of the study is due to the need for a new conceptual, comprehensive approach to the methodology for disclosing and investigating cybercrimes. This is due to the growing threat of this type of crime, causing global, transnational damage to economic relations, national security around the world and in Uzbekistan as well.

Our objective is to identify relevant problems and ways to resolve them, that are associated with offenses in the virtual space. For this purpose, we analyze qualifications, criminal procedural methods, forensic and operational-investigative support of technology for disclosing and investigating cybercrimes. During the research of the literature of this sphere, it was noticed, that there was no enough attention to this problem. Nowadays, ways to improve the disclosure and investigation of cybercrimes are developing in two directions: criminal law, which includes qualification and criminological aspects, and criminal procedural, that is expressed in forensic and operational-search support.

The main purpose of the study was to consider theoretical and practical issues of the activities of authorities, that disclose and investigate cybercrimes. The development of evidence-based recommendations and rational ways of organizing the fight against this type of crime was the purpose as well.

MATERIAL AND RESEARCH METHODS

The instruments for committing cybercrimes are computer, information and telecommunication systems and technical means, that are used in their commission. The

main target of criminals is an information, that we keep on technical media of information systems and share by the Internet global channels.

The technology of disclosing and investigating cybercrimes includes a criminal-legal block, consisting of a complex of branches of criminal procedure, operational-search, international criminal law, criminalistics, juridical psychology, and forensic expertise. Fast detection and successful investigation of cybercrimes is based on correct criminal law qualifications, optimal criminal procedural methods of investigation, effective investigative support, rational forensic tactics, successful international cooperation, the use of the rules of juridical psychology and the achievements of forensic expertise.

The optimization of technology of disclosing and investigating cybercrimes provides theoretical, methodological and practical directions of improvement, where the one of the main questions is definition of cybercrime, and the methods of proving crimes.

In the aspect of disclosure and investigation of cybercrimes, a lot of attention should be paid to the peculiarities of using digital evidence in criminal and investigative process. The procedure of their detection, receipt, fixation and use has its own characteristics, that associated with their virtual, digital nature. The investigating authorities involve experts with special knowledge in conducting expertise and special researches, for the successful investigation of these crimes. The practical aspect of disclosing and investigating cybercrimes includes the acquisition by investigators, interrogators, employees, that carrying out pre-investigation checks and investigative activities. But there are some obstacles, that interrupt solving the crime. Among them, one can highlight such as: the lack of an optimal investigation algorithm, a deficit of qualified personnel among law enforcement officals and special programs for their training, as well as specialized training courses for practitioners, who reveal and investigate cybercrimes.

This is necessary to differ cybercrime from offences in a computer technology sphere. These crimes are very similar to each other, but still the first concept is broader than the second and more accurately reflects the nature of such a phenomenon as crime in the information space. Fundamentally, the prefix “cyber” can be correlated with the concept of information technology in the global Internet. On the other hand, crimes in the sphere of computer technology can be classified as crimes, that are committed by using computer tools or programs.

The research methods were determined on the basis of the dialectical provisions of the theory of knowledge in the information space in its correlation and interdependence. In addition, an interdisciplinary approach was used as well. The research required the use of knowledge in the sphere of criminal law, and investigative process, forensic science, cybernetics, computer science, international law and other sciences, which predetermined the complex nature of this study.

The general and specific methods of scientific research, that include formal-logical, system-structural, comparative-analytical, statistical and other research methods, was used in this research.

RESULTS AND ITS DISCUSSION

The definition of “cybercrime” can be perceived as socially dangerous acts, that are associated with the commission of crimes in the sphere of information and communication technologies.

In other words, cybercrime is a combination of crimes, that are committed in the information and telecommunications, virtual space with the help of media materials in the information networks of the Internet, as well as other means of access to cyberspace (cyberspace - it is a space that is simulated and mediated by information devices).

It should be recognized, that information and communication technologies are being introduced and developed much faster and this is due to scientific and technological progress in this sphere. Legal regulation and prompt response from law enforcement agencies lag significantly behind this process[22, p.155].

In criminal law, cybercrime is a generic definition, that encompasses information technology crime in the narrow sense of the word, where computer hardware is the subject, and information security is the object of crime.

We could find the criminal actions in sphere of computer information in XX1 chapter of CC of the Republic Of Uzbekistan "Information Technology Crimes". Actus reus of these crimes affect an insignificant part of socially dangerous acts, that are related to the illegal use of information and communication technologies. One should note here, that in CC of the Republic of Uzbekistan (in the commentaries, as well), the issues of using information and communication methods and means of collecting, accumulating and disseminating information are not widespread. Thus, the use of DDos attacks, phishing (a type of Internet fraud) and other means and methods of committing cybercrimes, especially in the sphere of Internet banking, has not been specifically reflected in the Criminal Code of the Republic of Uzbekistan.

The cybercrimes pose a serious threat to public relations in the area of information technology, and therefore the fight against them in modern conditions has become a serious problem for the state and citizens[23, c.7]. The created law enforcement structures develop countermeasures to neutralize these crimes, determine the strategy and tactics of countering cybercrime.

Essentially, cybercrime is a socially-dangerous act in the virtual space, which can be designated as a kind of crime, that is modeled by using computer technology and other information, telecommunication means in cyberspace. Therefore, according to T.L. Tropina's words, cybercrime is a combination of crimes, that is committed in cyberspace with the help of computer systems or networks, as well as other means of access to cyberspace[24, c.25]. Consequently, a crime, that is committed in cyberspace is illegal interference in the operation of computers, computer programs and networks, unauthorized modification of computer data, as well as other illegal socially-dangerous actions, that are committed with the help of ICT.

It should be mentioned, that in the investigation of cybercrime investigators are faced with serious difficulties that are associated with a lack of knowledge and experience of the investigation of these crimes[25, c.47].

According to V.A. Nomokonova, T.L. Tropina words, cybercime is broader than computer crime and more accurately reflects the nature of such a phenomenon as crime in the information space[26, c.47].

The cybercrimes are committed under certain conditions that must be identified, and on the basis of scientific analysis, a methodology for disclosing and investigating cybercrimes should be developed. The factors contributing to the commission of cybercrimes can be conditionally divided into two types: objective and subjective. The first include the presence of the necessary computer equipment, modern and high-tech

software and the access to the information network by a potential offender. The subjective factor includes the offender, as a specialist in the area of information technology, possessing the necessary abilities and technical skills in the computer sphere. Nevertheless, it should be taken into account, that the intensive development of ICT allows various criminals to commit cybercrimes, and knowledge of the technical capabilities of computer technology and the features of their software helps them in this. This type of criminal activity is becoming widespread and an increasing number of citizens, enterprises and organizations, become victims of cybercrimes. A.K. Rasulev points out the need to ensure the principle of inevitability of responsibility for cybercrimes[27, c.37].

As an example, such a variety as “spamming” can be distinguished, which implies sending spam on the Internet, other types of ICT and, in particular, cellular communications. Users receive various messages they do not need. These messages overload information system, which ultimately causes them moral and material harm. In most countries of the world, legal regulations define “spamming” as a cybercrime and the perpetrators as criminals.

Another type of cybercrime is “carding”. This type of cybercrime is the commission of a special type of fraud with payment cards, when transactions are carried out without the knowledge of the cardholder. Thus, criminals commit theft of information from personal computers, ATMs, online stores.

Another widespread type of cybercrimes in the modern world is Internet banking, the essence of which is expressed in illegal enrichment through unauthorized withdrawals of funds and extortion in various forms. There are many other types of cybercrime, likewise.

It is necessary to take into consideration the fact that scientific and technological progress does not stand still. Innovative telecommunication technologies are developing exponentially, and at the same time, the dynamics of the use of high technologies is being actively implemented, and, therefore, new types of cybercrimes are emerging.

According to the analysis of national and international experience, it can be stated that the peculiarity of the disclosure and investigation of cybercrimes is the misuse of information communication technologies and that illegal acts are committed in virtual cyberspace, that has a transboundary nature[28, c. 136].

Nowadays, national and international law is faced with tasks, that are related to the timeliness and necessity to improve the legal regulation of the fight against cybercrimes[29, c.52]. The norms of regulation public relations in the information technology area in legislation of Uzbekistan and other countries, are no longer sufficient. Consequently, there is an urgent necessity to develop appropriate proposals to resolve the problems, that are related to the effectiveness of the detection and investigation of cybercrimes.

CONCLUSION

In conclusion it can be argues, that disclosure and investigation of cybercrimes is an actual problem of our time. This is due to a number of reasons.

Namely:

1. There are gaps in the current legislation, that is governing the criminalization of cybercrime;

2. The criminal procedure and forensic methods of investigating cybercrimes are insufficiently developed

3. The lack of qualified specialists in the sphere of information and communication technologies, with the knowledge to disclose and investigate cybercrimes;

4. The techniques for conducting appropriate expertise have not been developed, due to high material costs;

5. The forensic and investigative tactics of disclosing and investigating cybercrimes are not sufficiently developed;

6. There are no any international standards in the conduct of an investigation;

7. The foreign experience in disclosing and investigating cybercrimes is insufficiently studied.

In order to resolve the above problems, from our point of view, it is necessary to: systematically generalize, analyze investigative practice and prepare information and analytical materials on the status of detection and investigation; to identify, summarize and analyze the causes and conditions that contribute to the commission of these crimes, develop comprehensive measures to eliminate them and monitor the algorithm, identify conceptual directions for improving the investigation methodology and tactics of conducting investigative actions; to create an innovative, automated search system for records, databases, information systems for disclosure, investigation and the production of complex expertise in the sphere of ICT; to ensure the study and implementation into practice of advanced foreign and national work experience, modern systems, forms, methods and tactics of disclosure and investigation; to organize comprehensive preventive measures to prevent cybercrimes, including interaction with the media and civil society institutions.

References:

1. https://plusworld.ru/daily/cat-security-and-id/v-2022-godu-ushherb-ot-kiber prestupnosti-dostignet-8-trillionov-dollarov/ (Date of Referral: 8.08.2020 года)

2. https://www.angaratech.ru/press-center/novosti/summarnye-poteri-ot-kiber intsidentov-v-mire-sostavlyayut-poryadka-3-5-mlrd_1006/(Date of Referral: 8.08. 2020 года)

3. Dolgachev A.O. Concept and features of cybercrime // Scientific search FGBOW VO «Ivanovsk State University» [Electronic resource]. 2017. 9 Access Mode: https:///elibrary.ru/item.asp?id=29674026/ (Date of Referral: 8.08.2020)

4. Rasulev A. K. Improvement of criminal-legal and criminological measures of fight against crimes in the sphere of information technologies and safety: Doctoral (DSc) dissertation abstract on legal sciences. - T., 2018. - 74 pp.

5. Hijfutdinov R. R. Concept and classification of crimes against the security of computer information: Autoref. dis. Jurid. sciences. - Kazan, 2017. - 26 pp.

6. Ochilov Kh R. Liability for embezzlement of one's belongings by the use of computer tools: Doctoral (PhD) Dissertation abstract on legal sciences. – T., 2017. – 63 p.

7. Safonov O. M. Criminal Law Evaluation of the Use of Computer Technologies in Crime Commission: Status of Legislation and Law Enforcement Practice, Prospects for Improvement: Autoref. Dis. Jurid. Sciences. - M., 2015. - 22 pp.

8. Tropina T.L. Cybercrime: Concept, State, Criminal Law Measures: Autoref. dis. ... Jurid Sciences. - Vladivostok, 2005. - 27 s.

9. Davydov V. O. Informational support for the detection and investigation of extremist crimes committed through computer networks: Avref. dis. ... Jurid. sciences. - Rostov-on-Don, 2013. - 26 pp.

10. Zacharine S. I. Information support for the investigation and activities to identify wanted persons, objects and instrumentalities through computer technology: Avtoref. dis. ... Jurid. sciences. - Volgograd, 2003. - 28 pp.

11. Kovalev S. A. Basics of computer simulation in investigation of crimes in the sphere of computer information: Autoref. dis. ... Jurid. sciences. - Voronezh, 2011. - 22 s.

12. Kostomarov K. V. Initial stage of investigation of crimes related to illegal access to computer information of banks: Avotref. Dis. ... Court. Jurid. Sciences. - Chelyabinsk, 2012. - 30 pp.

13. Krygin S. V. Investigation of crimes committed in the sphere of computer information: Autoref. dis. ... Jurid. sciences. - Nizhny Novgorod, 2002. - 30 s.

14. Meshcheryakov V. A. Fundamentals of the methodology of investigation of crimes in the sphere of computer information: Autoref. dis. ... doc. Jurid. sciences. - Voronezh, 2001. - 39 s.

15. Tlich A. D. Problems in the methodology of investigation of crimes in the sphere of economic activity committed with the use of computer technologies and plastic cards: Autoref. dis. ... Jurid. sciences. - Krasnodar, 2002. - 29 pp.

16. Cheyevich A. A. Features of the use of special knowledge in computer technology in crime investigation: Autoref. dis. ... Jurid. Sciences. - Irkutsk, 2007. - 24 pp.

17. Yang Wei Feng Computer Crime Investigation in the People's Republic of China: Autoref. dis. ... Jurid. sciences. - M.,2006. - 23 pp.Shinder Debra L. Scene of the Cybercrime. Computer Forensics Handbook / Debra L. Shinder. -Rockland: Syngress, 2003. – 752 p.

18. Shinder Debra L. Scene of the Cybercrime. Computer Forensics Handbook / Debra L. Shinder. -Rockland: Syngress, 2003. – 752 p.

19. Parker Donn B. Fighting Computer Crime: A New Framework for Protecting Information / Donn B. Parker. Wiley, 1998. – 528 p.

20. Craig B. (Brian), prof. Cyberlaw: the law of the internet and information technology / B. Craig. – Boston: Pearson, 2012. – XVII, 262 p

21. Hashimoto, Naoki. "Current issues and measures for prevention of cybercrime." Sōsa kenkyū [Investigation research] 56, no. 2 (February 2007): 20–29.

22. Tropina, T., Self- and Co-regulation in Fighting Cybercrime and Safeguarding Cybersecurity. In: Jähnke at al. (eds.), «Current Issues in ITU Security», Duncker & Humblot, Berlin, 2012. – P. 155.

23. Matchanov A.A. Detection and investigation of cybercrime. - Training manual. - T. Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, 2020. - S.7.

24. Tropina T.L. Cybercrime: concept, state, criminal law measures of struggle: Autoref. dis. ... Jurid. sciences. - Vladivostok, 2005. - 27 s.

25. Nesterovich S.A. Problems in investigating cybercrime faced by investigators/Journal of Science and Education. 8 (44) 2018. Volume 2. c.47.

26. Nomokonov V.A. Cybercrime as a new criminal threat / V.A. Nomokonov, T.L. Tropina // Criminology. Yesterday. Today. Tomorrow. - 2012. - 1 (24). - C. 47.

27. Rasulev A. K. Improvement of criminal law and forensic measures to combat information technology and security crimes: Avref. dis. ... dr. Jurid. Sciences (Dsc). - T., 2018. - C. 37.

28. Borodkina T.N., Pavluk A.V. Cybercrime: concept, content and countermeasures. Socio-political sciences. 1 - 2018. - C. 136.

29. Rasulev A.K. Modern trends in the development of international cooperation in countering cybercrime // Bulletin of the Supreme Court of the Republic of Uzbekistan // 2015, No. 6. - P. 52-54.