European Journal of Research volume 5 issue 5 2020 pages 20-

# CYBERCRIME IN LEGISLATION REPUBLICS OF UZBEKISTAN

**A.U.Anorboev**

Chief legal adviser of the legal department of the Ministry of Information Technologies and Communications Development of the Republic of Uzbekistan; independent candidate of the Military Technical Institute of the National Guard of the Republic of Uzbekistan;
E-mail: amirxan786@ mail.ru

**Abstract**

The article analyzes the continuation of the author's research on "Cybercrime: criminal and criminological aspects". This article is devoted to explaining the essence and significance of effective ways and mechanisms of cyber security in Uzbekistan.

This article analyzes the effective ways and mechanisms of cyber security in Uzbekistan, taking into account examples of existing problems.

**Keywords:** cybersecurity, cyberspace, cybercrime, cyberterrorism, crime, administrative offense, clutch, unified governance, strategy.

**Introduction.** As it is known, information rules the world [1], and this information can be used differently by everyone, and it can be a group of people who are planning to realize their evil intentions.

In general, each country is fighting cybercrime to prevent this information from being used for malicious purposes in a country trying to create a secure cyberspace.

The main reason for the rapid growth of cyberterrorism is primarily that it is a very economic and effective method for terrorists, for rapid terrorist acts.

For example, by the end of 2018, Uzbekistan had 22.8 million Internet users[2] and mobile communications.

22 million 800 thousand [3], also the total connection speed of international networks with Uzbekistan is 104.1 Gbit/s[4].

Currently, the national domain zone "UZ" has more than 66,000 active domains. In 2017 in Uzbekistan there were about 166,000 active domains.

53,000 active domains[5].

The availability of Internet services for each user means that they can become victims of cyber terrorism.

According to UZCERT Information Security Incident Prevention Services, their number increased in 2018.

Up to 65,000, also during the monitoring of information security events.

54,953,759 information security events were detected in the information systems of government agencies for 2018 and the first quarter of 2019. Of these, 2,502,353 are high-risk events [6].

Many positive developments are currently being made in Uzbekistan to create cyberspace.

In particular, defined by the main tasks and priority directions of the Ministry of Information Technologies and Communications of the Republic of Uzbekistan the implementation of complex measures to ensure cybersecurity and the introduction of modern technologies for the protection of networks, software products, information systems and resources, participation in the regulation of the application of technologies for the collection, processing and storage of personal and biometric data [7], the State Inspectorate for Control in the field of information and telecommunications of the Republics of Uzbekistan.

In state and economic administration bodies, local government bodies, other organizations and departments

ISSN 2521-3261 (Online)/ ISSN 2521-3253 (Print)
DOI 10.37057/2521-3261 https://journalofresearch.info/

In the manner prescribed by law[8], the University of Shard has been established

In Uzbekistan, which provides training at the level of international standards of highly qualified specialists in the field of cybersecurity in relevant areas of education [9].

The Council of Heads of State of the Shanghai Cooperation Organization (SCO) was held on June 14 this year and adopted the Bishkek Declaration. Twenty-two documents have been signed aimed at developing partnership between the SCO member nations in various spheres, interaction between the SCO and other international organizations, the Concept of Cooperation in Digitalization has been approved at the proposal of the President of Uzbekistan.

And information and communication technologies, and the Programme on Development of Interregional Cooperation among SCO Member States. These documents will make it possible to launch new areas of multilateral cooperation within the SCO[10].

However, cybercrime remains one of the biggest problems for us.

China, the USA, Estonia, Ukraine, the Netherlands, Spain, Austria, Great Britain and other countries have adopted a special law.

On cybersecurity or amendments and additions to legislation.

For example, China adopted the Law "On State Security" on 01.07.2015, the Law "On Cyber Security" on 01.06.2017, the Law "On Combating Terrorism" in 2016.

In accordance with these laws, Uzbekistan takes measures to combat cybercrime [11].

Russian [12], Ukrainian [13], Georgian [14], Kazakh [15] and Estonian [16] laws already clearly define the role of information technologies and communications in cybersecurity.

For example, according to Article 1 of Law No. 2469-VIII of 21 June 2018 of Ukraine "On Basic Principles of Ensuring Cyber Security", cyberterrorism is a terrorist activity carried out as follows

In cyberspace or with its use [17].

But Uzbekistan has no Cyber Security Law. Therefore, it is advisable to adopt a separate law on this issue.

Also, the Uzbek Criminal Code does not provide for liability for cybercrimes [18].

Under article 4 of the Criminal Code, only the Criminal Code defines the crime, the punishable nature of the act and other legal consequences of its commission. No one may be found guilty of a crime and punished except by a court sentence and in accordance with the law[19].

Also, according to Article 10 of the Criminal Code, every person in whose act it is established that a crime has been committed shall be liable[20].

Under article 11 of the Code of Criminal Procedure, judges, procurators, pretrial investigators, persons conducting initial inquiries and defence counsel, as well as all persons taking part in criminal proceedings, must accurately observe and comply with the requirements of the Constitution, this Code and other legislative acts of Uzbekistan. Any derogation from the precise application and observance of the law, whatever the motives, is a violation of the law in criminal proceedings and entails established liability.

In addition, in accordance with paragraph 2 of the first part of the article.

83 The Code of Criminal Procedure does not contain any elements of a crime in its act: a suspect, an accused person or a defendant is found innocent and is subject to rehabilitation.

Accordingly, in accordance with article 333 of the Code of Criminal Procedure, when circumstances stipulated in article 83, paragraph 2, of the Code are identified, an official of the body conducting the pre-investigatory inspection, the person conducting the initial inquiry or pretrial investigation or the procurator issues a ruling refusing to institute criminal proceedings when there is no element of an offence in his or her act[21].

In this regard, we consider it appropriate to include the concept and mechanism of cyberterrorism in the Law of the Republic of Uzbekistan "On cybersecurity", and we also consider it necessary to include the following article in the Criminal Code:

First of all, we need to provide modern technologies and mature personnel.

It would be advisable to review the following legislation in Uzbekistan.

ISSN 2521-3261 (Online)/ ISSN 2521-3253 (Print)
DOI 10.37057/2521-3261 https://journalofresearch.info/

In particular, Uzbekistan has not yet developed a strategy to protect against cyberterrorism; at the same time, cybercrime is becoming increasingly dangerous in the world, with more than 200,000 operations per day[22], resulting in the loss of about 500 billion individuals and legal entities. According to a survey conducted by Juniper Research in 2016[23], one example is that by 2019 computer fraud losses could rise to more than $2.1 trillion[24], with each month's crime rates increasing by 10-15%[25], it is clear that tactical plans such as strategy should be developed and practical measures taken.

At present, the entire document flow in the state power and administration is carried out using the following information technologies.

With a view to strengthening control over processing, execution and storage of documents, optimization of information flows on paper and electronic carriers, creation of uniform information space for input, processing, the analysis and storage of documents, maintenance of security of information exchange, economy and rational use of a paper, and also increase of efficiency of interaction between The Executive Office of the Cabinet of Ministers of the Republic of Uzbekistan and state and economic management bodies, local government authorities ensured the introduction of a single secure e-mail, i.e. a single secure corporate e-mail, in the Executive Office of the Cabinet of Ministers, state and economic management bodies, local government authorities

«E-Xat» and electronic document management systems, i.e. "E-Hujat" electronic document management systems and, starting from January 1, 2012, electronic information exchange between them[26].

In the ministries and departments themselves, document management is carried out using information technologies such as "germes", "portal" and others.

In execution of the Decree of the President of the Republic of Uzbekistan dated August 8, 2018 No. UP-5505 "On approval of the Concept of improvement of normative activity", the Ministry of Justice together with the Ministry for development of information technologies and communications of the Republic of Uzbekistan and the "Single integrator on creation and support of state information systems - UZINFOCOM" LLC created and since January 1, 2019 launched in a test mode on the World Wide Web as a pilot operation of the "Single electronic system of development". (project.gov.uz) [27].

At the moment, all drafts of regulatory legal acts are subject to placement by organizations developing projects on the Unified portal of interactive public services of the Republic of Uzbekistan, that is, on the site "regulation.gov.uz" for public discussion. [28].

In accordance with a presidential decree

No. R-5017 of 9 August 2017 "On measures to introduce a Unified Interdepartmental Electronic System for the Performing Arts Discipline" ensured the connection of ministries, departments, local executive authorities and other organizations to the Unified Interdepartmental Electronic System for the Performance Discipline "Ijro.gov.uz", that is «e-ijro»[29].

The national database of legislation of the Republic of Uzbekistan, that is, the site "lex.uz" are the official sources of publication of regulatory legal acts [30].

None of the above programs are interconnected.

This is considered the biggest system error.

It is because of this error that all software can attack.

As a result of this attack, it can cause significant damage to the interests of the individual, society and the state.

Human destiny can change dramatically.

The reputation of the state in the international arena may fall.

What is needed to prevent this problem?

In our opinion, the strategy and concept of cybersecurity in Uzbekistan should be developed and implemented.

For example, in accordance with the Decree of Ukraine dated March 15, 2016 No. 96/2016, the Cyber Security Strategy of Ukraine was approved [31].

ISSN 2521-3261 (Online)/ ISSN 2521-3253 (Print)
DOI 10.37057/2521-3261 https://journalofresearch.info/

Similar strategies have been adopted in the USA [32], Estonia [33], Lithuania [34], Spain [35], Germany [36], Slovakia [37], Japan [38], Switzerland [39], Norway [40], New Zealand [41], India [42], Australia [43], South Africa [44], Canada [45], Finland [46], Austria [47], Romania [48], Poland [49], France [50], Czech Republic [51], Netherlands [52], Luxembourg [53] and other states.

Looking at international practice in the fight against cybercrime, we see the following examples.

The only country that meets all the criteria for protection against hacker attacks is Singapore. The top 10 also includes the USA (2nd place), Malaysia (3rd place), Oman (4th place), Estonia (5th place), Mauritius (6th place) and Australia (7th place). Georgia and France shared the 8th place. Canada was ranked 9th. The 10th place went to Russia[54].

Uzbekistan has not yet been defined as an authorized state body to develop and implement state policy to combat cybercrime.

This authority is exercised by the Ministry of Defence in Australia, the Ministerial Committee on Security in Belgium, the Information Security Committee in Brazil, the Canadian Computer Emergency Rapid Response Centre in Canada, the Ministry of Economic Affairs and Communications in Estonia, the Ministry of Transport and Communications in Finland, the General Secretariat of National Defence within the Prime Minister's Office and the French National Agency for Information Systems Security, by the Federal Agency for Information Security in Germany, the Ministry of Informatics and Communications in Hungary, the National Information Council in India, the Ministry of the Interior in Italy, the Cabinet Secretariat in Japan, all government organizations and their subsidiaries in the Republic of Korea, the Office of Modernization and Planning Management in Malaysia, the Ministry of the Interior and Kingdom Relations in the Netherlands, the Centre for Critical Infrastructure Protection in New Zealand, the Civil Defence Administration and the Crisis Plan, Управлением безопасности информационных сетей и связи в Сингапуре, Министерством промышленности, туризма и торговли, The Ministry of Public Administration and the Ministry of the Interior in Spain, the Office of Cyber Security in the Cabinet Office in the United Kingdom, and a number of different organizational units in Switzerland, Sweden are also dealing with cyberterrorism[55].

Well, how do foreign countries fight cybercrime?

For example, in the Republic of Hungary, a public-private partnership fund ensures the systematic allocation of funds for cybersecurity [56].

Also in Italy, a postal police service was established and it oversees computer crime rapid response centres at the national and regional levels. A, the Association of Italian Experts on Critical Infrastructure coordinates public and private cybersecurity [57].

It should be noted that the time has come for Uzbekistan to establish an authorized body to combat cybercrime and develop specific measures in this regard.

One of the most effective ways to alleviate the difficulties of the current population of Uzbekistan is to improve the country's legislation through international standards.

In the framework of the international counter-terrorism instruments, the Convention on cybercrime is of particular importance. The Convention was signed by the members of the European Union on 23 November 2001 in Budapest. It consists of article 48 [58].

The rules of this Convention are governed by the following three main points:

Convergence of the criminal law assessment of crimes in the field of computer information;

Convergence of national criminal procedure measures aimed at ensuring the collection of evidence in the investigation of such offences;

International cooperation in criminal proceedings aimed at the collection of evidence of the commission of such offences abroad[59].

The Convention proposes to incorporate into the legislation of States parties uniform rules on criminal liability for cybercrime.

The object of cybercrime, in accordance with the Convention, is a wide range of public relations protected by the rules of law arising from information processes related to the production,

ISSN 2521-3261 (Online)/ ISSN 2521-3253 (Print)
DOI 10.37057/2521-3261 https://journalofresearch.info/

collection, processing, accumulation, storage, search, transmission, distribution and consumption of computer information, as well as in other areas where computers, computer systems and networks are used.

The objective side of cybercrime is characterized by the distinction against the confidentiality, integrity and availability of computer data and systems related to the use of computers, data content related to copyright and related rights violations.

The subject of cybercrime can be any person who has committed the above actions.

All offences referred to in the Convention are punishable only if committed intentionally.[60].

Indeed, these crimes are transnational international crimes.[61].

These crimes do not choose a border for which States are not internationally recognized.[62].

Cybercrime may directly or indirectly affect the victim [63].

Accordingly, the Convention provides for a list of individual measures for each State party to combat these crimes.[64].

This crime is characterized by its extensive and remote management and significant damage, and States must cooperate closely in international relations to combat this crime.

According to the head of state, today it is important to pursue a coordinated policy to ensure security, to create favorable conditions for sustainable development of Uzbekistan. [65].

Everyone has the right to a social and international order in which rights and freedoms can be fully realized.

In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society. [66].

Failure to comply with this requirement undermines human rights and interests. Bearing in mind that addressing the consequences of cyberterrorism is necessary not only for the future of the State, but also for individuals and society.

One of the most effective ways to combat cyberterrorism is to cooperate with foreign countries and implement practical measures.

The scale of this crime can be very broad, but cyberterrorist tries to do everything he hates, even if it is from any territory.

Accordingly, it is very important that the criminal law seems to be international cooperation of the country.

The similarities are of course based on international instruments.

In terms of implementation, the mandatory fulfilment of obligations imposed on the State demonstrates the importance of implementation. [67].

**Conclusion**

It was therefore time to introduce the implementation of the Convention in Uzbek criminal law.

In this regard, the implementation of the aforementioned proposals can help protect our people from cybercrime, and this is a duty for each of us.

**References:**

1. From the website of the National Information Agency of Uzbekistan: A. Sattarov. The old adage "the world is ruled by information" has come true today.. http://uza.uz/oz/programs/25-years/achonlardir-bashorat-tarzida-aytilgan-dunyeni-akhborot-bosh--20-02-2018/.

2. From the website of the Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan: http://mitc.uz/ru/stat/7.

ISSN 2521-3261 (Online)/ ISSN 2521-3253 (Print)
DOI 10.37057/2521-3261 https://journalofresearch.info/

3. From the Internet site: http://uz.infocom.uz/2018/01/27/ozbekistonning-mobil-aloqa-abonentlari-soni-22-mln-800-mingga-yetdi/.
4. From the Internet site: http://uz.infocom.uz/2018/01/27/ozbekistonda-internetdan-foydalanuvchilar-soni-20-milliondan-oshdi/.
5. From the Internet site: https://uzcert.uz/blog/saidakbar/kiberbezopasnost-uzbekistana-v-tsifrakh-itogi-2018-goda/.
6. Sadikov S. Cyber security of Uzbekistan in numbers: 2018 results.// https://uzcert.uz/blog/saidakbar/kiberbezopasnost-uzbekistana-v-tsifrakh-itogi-2018-goda/.
7. Decree of the President of the Republic of Uzbekistan dated February 19, 2018 № UP-5349 "On measures for further improvement of information technologies and communications" // National database of legislation, 20.02.2018 г., № 06/18/5349/0792.
8. «On measures for further improvement of information technologies and communications" Regulation on the State Inspection for control in the field of information and telecommunications, approved by the decision of the President of the Republic of Uzbekistan dated 21 November 2018 № PP-4024 Republic of Uzbekistan // National database of legislation, 22.11.2018 г., № 07/18/4024/2200.
9. Presidential Decree No. PP-4278 of 10 April 2019 on the establishment of the University of Sharjah in Uzbekistan // National legislative database, 11.04.2019 г., №07/19/4278/2920.
10. From the official website of the President of the Republic of Uzbekistan: https://president.uz/ru/2663.
11. Review of the criminal law on counter-terrorism and China's "Counter-Terrorism Law" / Eurasian Scientific Journal, No. 5, 2016 (May). Zhang Zemei https://chinalaw.center/administrative_law/china_state_security_law_2015_russian/ / E.Yu. Makarova, A.A. Vasilenko prevention and fight against cyberterrorism in China. Chinese experience in Russia. https://core.ac.uk/download/pdf/155234277.pdf.
12. Federal Law of the Russian Federation of 06.03.2006 № 35-FZ "On Combating Terrorism" // Collection of Legislation of the Russian Federation , 2006, № 11, ст.1146; № 31, ст.3452; 2011, № 19, ст.2713.
13. The Law of Ukraine of Rejection 5, 2017 No. 2163-VIII "On Establishment of Ambushes of the Ukrainian Security Service". / (Verkhovna Rada Publications (VVR), 2017, No. 45, Articles 403, 2018, No. 31, Article 241. / https://zakon.rada.gov.ua/laws/show/2163-19.
14. Law of Georgia of June 27, 2007, No. 5071-Âc "On Combating Terrorism". // https://matsne.gov.ge/ru/document/download/21796/9/ru/pdf.
15. Law No. 416 of the Republic of Kazakhstan "On Combating Terrorism" of 13 July 1999. // "Kazakhstanskaya Pravda" 30.07.99 № 182-183; (Vedomosti of the Parliament of RK), 1999, N 19, art. 649.
16. https://www.rup.ee/rus/novosti/novoe-v-zakonodatelstve/v-estonii-vstupil-v-silu-zakon-o-kiberbezopasnosti.
17. Law of Ukraine No. 2163-VIII of Release 5, 2017 "On Founding Ambushes of the Ukrainian Security Service". / (Verkhovna Rada Publications (VVR), 2017, No. 45, Articles 403, 2018, No. 31, Article 241.
18. Criminal Code of Ukraine dated April 5, 2001 No. 2341-III (as amended and supplemented as of April 25, 2019). // Published: "Vedomosti Verkhovna Rada of Ukraine" dd. 29.06.2001 No. 2341-III (as amended and supplemented as of 25.04.2019). No. 2341-III (as amended and supplemented as of 25.04.2019 // Published: "Vedomosti Verkhovna Rada of Ukraine" dd. 29.06.2001 No. 2341-III (as amended and supplemented as of 25.04.2019). № 25-26. C.256.
19. Rasulev A.K. Counteraction to cyberterrorism: international legal and criminal-legal aspects. -T.: TDUU Nashrioti, Yurik Fanlar Akhborotnomasi and Amaliy Kukukiy journalist, 2018. C.95.

ISSN 2521-3261 (Online)/ ISSN 2521-3253 (Print)
DOI 10.37057/2521-3261 https://journalofresearch.info/

20. The Criminal Code of the Republic of Uzbekistan, approved by the Law of the Republic of Uzbekistan dated 22 September 1994 № 2012-XII (Vedomosti of the Supreme Soviet of the Republic of Uzbekistan, 1995, № 1, art. 3; 2018, № 1, art. 4, № 4, art. 4). 218, 224, No. 7, Art. 430, No. 10, Art. 679

21. Criminal Procedure Code of the Republic of Uzbekistan approved by the Law of the Republic of Uzbekistan dated 22 September 1994 No. 2013-XII // Vedomosti of the Supreme Soviet of the Republic of Uzbekistan, 1995, No. 2, Art. 5; No. 12, Art. 269; 1997, No. 2, Art. 56, No. 9, Art. 241; 1998, No. 5-6, Art. 102, No. 9, Art. 181; 1999, No. 1, Art. 20, No. 5, Art. 124, No. 9, Art. 229; 2000, No. 5-6, Art. 153,

22. No. 7-8, Art.217; 2001, No. 1-2, Art.2. 11, 23, No. 9-10, Art.217; 2001, No. 1-2, Art.11, 23, No. 9-10. 165, 182; 2002, No. 9, Art. 165; 2003, No. 5, Art. 67; 2004, No. 1-2, Art. 18, No. 9, Art. 171; Bulletins of the Chambers of the Oliy Majlis of the Republic of Uzbekistan, 2005, No. 12, Art. 418; 2006, No. 6, Art. 261; 2019, No. 1, Art. 3, 5, No. 3, Art. 161, No. 5, Art. 418; 2006, No. 6, Art. 261; 2019, No. 1, Art. 418. 259, 267, No. 7, Art. 386.

23. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p.392.

24. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. P.392.

25. Steve Morgan (January 17, 2016). "Cyber Crime Costs Projected To Reach $2 Trillion by 2019." Forbes. Retrieved September 22.2016.

26. Ochilov Ҳ.R. Ўзгалар mulkini computer vositalaridan foydalanib talon-born kilganlik uchun zhovobgarlik. Monograph // - T.: TDU sashrioti, 2017. Б.22.

27. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan dated May 4, 2011 № 126 "On measures for the introduction and use of a single secure e-mail and electronic document management system in the executive office of the Cabinet of Ministers, state and economic administration bodies, local government authorities" // Collection of Legislation of the Republic of Uzbekistan, 2011, № 18, Art. 181.

28. The Decree of the Cabinet of Ministers of the Republic of Uzbekistan dated 8 April 2019, No. 284 "On organizational measures to introduce a unified electronic system of development and coordination of draft regulatory legal acts" // National Legislation Database, 09.04.2019, No. 09/19/284/2911.

29. The Decree of the President of the Republic of Uzbekistan dated April 13, 2018 № PP-3666 "On organizational measures for further improvement of the Ministry of Justice of the Republic of Uzbekistan" // National database of legislation, 14.04.2018, № 07/18/366/1073, 11.07.2018, № 06/18/5475/1489.

30. Resolution of the President of the Republic of Uzbekistan dated October 5, 2018, no. PP-3962 "On measures to further strengthen the performing discipline in government agencies and organizations" // National Legislation Database, 06.10.2018, No. 07/18/3962/2004.

31. The Law of the Republic of Uzbekistan dated December 24, 2012 No. ZRU-342 "On regulatory legal acts" // Collection of Legislation of the Republic of Uzbekistan, 2012, No. 52, Art. 583; 2014, No. 50, Art. 588; 2015, No. 32, article 425; 2016, No. 39, article 457; 2017, No. 37, article 978, National Database of Legislation, 05.01.2018, No. 03/18/456/0512, 10.01.2018, No. 03/18/459/0536, 19.04.2018, No. 03/18/476/1087, 09.01.2019, No. 03/19/512/2435.

32. Benjamin S., Schreyer F., Theodore H. Democratic governance and challenges to cybersecurity // Geneva: Geneva Centre for the Democratic Control of Armed Forces, 2013. C. 35-45.

33. From Internet site: International Network for Cyberspace. May 2011. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/international_strategy_for_cyberspace_US.pdf.

34. Site: 2014-2017 Strategies for Cyber Security https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf. // https://constitutions.ru/?p=11234.

ISSN 2521-3261 (Online)/ ISSN 2521-3253 (Print)
DOI 10.37057/2521-3261 https://journalofresearch.info/

35. From the Internet site: Resolution of the Government of the Republic of Lithuania No. 796 of 29 June 2011 on the approval of the Programme for the Development of Electronic Information Security (Cyber Security) for 2011-2019 // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf/.

36. Internet site: Estrategia de Ciberseguridad Nacional // https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional.

37. Internet site: German cybersecurity strategy // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Germancybersecuritystrategy20111.pdf.

38. From Internet: National Strategy for Information Security in the Slovak Republic // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Slovakia_National_Strategy_for_ISEC.pdf.

39. From the Internet site: Information Security Strategy for the Protection of the Nation 11 May 2010 Information Security Policy Council. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/New_Strategy_English_Japan.pdf.

40. From Internet site: Switzerland National Strategy for Protection against Cyber Threats 19 June 2012. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Switzerlands_Cyber_Security_strategy.pdf.

41. From: Norwegian Cyber Security Strategy // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Norway_Cyber_Security_StrategyNO.pdf.

42. Internet site: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/India_Cyber_Security_Strategy.pdf.

43. Internet site: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/India_Cyber_Security_Strategy.pdf.

44. From the Internet site: Cyber Security Strategy. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AGCyberSecurityStrategyforwebsite.pdf.

45. From the Internet site: Government Gazette of the Republic of South Africa. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/southafricancss.pdf.

46. From Internet site: Canadian cybersecurity strategy for a stronger and more prosperous Canada. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/canadaNCSS.pdf.

47. From Internet site: Finland's cybersecurity strategy. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf.

48. From Internet site: National ICT Security Strategy Austria. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Austria_Cyber_Security_strategy.pdf.

49. From Internet site: Information Security Strategy in Romania. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/roncss.pdf.

50. From the Internet site: Rządowy program ochrony cyberprzestrzeni rzeczypospolitej polskiej na lata 2011-2016. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf.

51. From the Internet site: French national digital security strategy. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf.

52. Web site: National cyber security strategy of the Czech Republic for the period from 2015 to 2020. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf.

ISSN 2521-3261 (Online)/ ISSN 2521-3253 (Print)
DOI 10.37057/2521-3261 https://journalofresearch.info/

53. Web site: The National Cyber Security Strategy. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Netherlands_Cyber_Security_strategy.pdf.

54. From the Internet site: National cybersecurity strategy II. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf.

55. UN report Global Cybersecurity Index 2017 https://www.rbc.ru/rbcfreenews/595d094d9a79477c6f363649?from=materials_on_subject https://rus.delfi.ee/daily/estonia/estoniya-priznana-pyatoj-samoj-kiberbezopasnoj-stranoj-v-mire?id=78814562. // https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

56. Benjamin S., Schreyer F., Theodore H. Democratic Governance and Cyber Security Challenges // Geneva: Geneva Centre for the Democratic Control of Armed Forces, 2013. C. 35-45.

57. Benjamin S., Schreyer F., Theodore H. Democratic governance and challenges to cybersecurity // Geneva: Geneva Centre for the Democratic Control of Armed Forces, 2013. C. 35-45.

58. Benjamin S., Schreyer F., Theodore H. Democratic governance and challenges to cybersecurity // Geneva: Geneva Centre for the Democratic Control of Armed Forces, 2013. C. 35-45.

59. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

60. Wolevodz, A.G. Convention on cybercrime: innovations in legal regulation / A.G. Wolevodz // Legal issues of communication. - – 2007. - – № 2. - – C. 17-25.

61. Volevodz, A.G. Convention on cybercrime: innovations of the legal regulation (in Russian) / A.G. Volevodz // Legal questions of communication. 2007. № 2. - – c.17-25.

62. Dissertation researches international convention

63. About cybercrime / Huseyn Magomed oglu najafi, doctoral student at the Institute of Philosophy, Sociology and Law of the National Academy of Sciences of Azerbaijan Scientific specialty: 12.00.08 - Criminal law and criminology; Penal enforcement law. From Internet site: http://naukarus.com/mezhdunarodnaya-konventsiya-o-kiberprestupnosti.

64. Doronin A.M. Criminal liability for illegal access to computer information: Dissertation ... cand. lawyer. –M., 2003. –c. 8.

65. Gavrilin Yu.V. Crimes in the sphere of information technologies: Part of author's abstract dissertation. Cand. of Sciences. –M.: 2000. From Internet site: http://www.dissercat.com/content/rassledovanie-nepravomernogo-dostupa-k-kompyuternoi-informatsii.

66. Convention on Cybercrime: protecting you and your rights: From Internet site: http://hub.coe.int/ru/octopus-conference-20121/.

67. From official website of the President of the Republic of Uzbekistan: https://president.uz/ru/2662.

68. Universal Declaration of Human Rights. Source: https://www.standup4humanrights.org/ru/article.html.

69. M.Rakhimova. Khalkaro Mahukuq. -T.: Akademiya nashirioti. 2005. - – p.20.

ISSN 2521-3261 (Online)/ ISSN 2521-3253 (Print)
DOI 10.37057/2521-3261 https://journalofresearch.info/