**A.M.Kurganov**
IIV Akademiyasi
Tillarni o‘rganish kafedrasi boshlig‘i
dotsent (PhD) podpolkovnik

**S.A.Isayev,**
IIV Akademiyasi Magistraturasi
Tashkiliy-Strategik Boshqaruv
tinglovchisi, podpolkovnik

# THE NEED FOR LEGAL REGULATION IN COMBAT WITH CYBERCRIME IN THE REPUBLIC OF UZBEKISTAN

***Annotation.*** *The article deals with the significance of the fundamental reforms concerning cybersecurity carried out in Uzbekistan, the essence and content of the concepts as cybersecurity, cybercrime, computer security, their types, the legislation of the Republic of Uzbekistan in the field of informatization and cybersecurity is given, the place of the Republic of Uzbekistan in the Global Cybersecurity Index, as well as the gaps existing in legislative practice related to the regulation of issues of responsibility in the information space and proposals for combating cybercrime.*

***Keywords:*** *cybersecurity, cybercrime, computer security, hacker, phishing, privacy.*

# НЕОБХОДИМОСТЬ ПРАВОВОГО РЕГУЛИРОВАНИЯ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ В РЕСПУБЛИКЕ УЗБЕКИСТАН

***Аннотация.*** *В статье излагается значение осуществляемых в Узбекистане коренных реформ, касающихся кибербезопасности,*

*суть и значение таких понятий как кибербезопасность, киберпреступления, компьютерная безопасность, их виды, даётся законодательство Республики Узбекистан в сфере информатизации и кибербезопасности, место Республики Узбекистан в Глобальном индексе кибербезопасности, а ткже пробелы имеющиеся в законодательной практике, связанные с регулированием вопросов ответственности в информационном пространстве и предложения для борьбы с киберпреступностью.*

***Ключевые слова**: кибербезопасность, киберпреступления, компьютерная безопасность, хакер, фишинг, конфиденциальность.*

## ЎЗБЕКИСТОН РЕСПУБЛИКАСИДА КИБЕРЖИНОЯТЧИЛИККА ҚАРШИ КУРАШИШНИ ҲУҚУҚИЙ ТАРТИБГА СОЛИШ ЗАРУРИЯТИ

***Аннотация.** Мақолада Ўзбекистонда киберхавфсизлик ва кибержиноятчиликка қарши курашиш соҳасида амалга оширилаётган туб ислоҳотларнинг аҳамияти, киберхавфсизлик, кибержиноят, компьютер хавфсизлиги каби тушунчаларнинг моҳияти ва мазмуни, уларнинг турлари, Ўзбекистон Республикасининг ахборотлаштириш ва киберхавфсизлик соҳасидаги қонун ҳужжатлари, Ўзбекистон Республикасининг Глобал киберхавфсизлик индексидаги ўрни, шунингдек, ахборот маконида жавобгарлик масалаларини тартибга солиш билан боғлиқ қонунчилик амалиётида мавжуд камчиликлар ва кибержиноятларга қарши курашиш бўйича таклифлар баён этилган.*

***Калит сўзлар:** киберхавфсизлик, кибержиноят, компьютер хавфсизлиги, хакер, фишинг, махфийлик.*

Systematic work was carried out in the field of promotion of human rights, strengthen the accountability and transparency of state bodies, increasing the role of civil society institutions, the media, political activities and public associations as well. The political, legal, socio-economic, scientific and educational foundations have been created for building the New Uzbekistan in the country.

As a result, nowadays Uzbekistan occupies the most significant place on the level of security among the countries of the world. Even

experienced foreign diplomats who traveled to many countries recognize that Uzbekistan is a safe place to live in peace. First of all, it is the merit of the country's law enforcement bodies of course, in particular the internal affairs bodies as well.

The Global Law and Order rating for 2019 confirmed the position of Uzbekistan as a safe country. In this rating, Uzbekistan took fourth place along with Switzerland as the safest countries in the world.

A consistent and balanced policy implemented in the Republic of Uzbekistan in all spheres of society contributes to the active integration of our country into the international community. The system of providing state, banking and other services online is being consistently improved and modernized, which makes it as easy as possible for the population to receive these services and eliminates the corruption component.

At the same time, special attention is paid to the provision of Internet and mobile communications services. Unfortunately, in parallel with this, terms such as "hacker", "Internet scammer", "phishing", "cybersecurity", and "cybercrime" are broadly being mentioned in our everyday life.

The main conclusion of the Global Risk Report released by the World Economic Forum in 2020, «cybercrime» is listed as one of the main problems of the 21st century. The main reasons for this are two contradictory trends:

1) Loss of public trust in the Internet, which is the fifth in terms of strategic risk;

2) Providing a public good through unmatched technological change.

In this regard, it is advisable to understand what such concepts as «**computer security**», «**cyber security**» mean.

Computer security is a section of information security that characterizes the impossibility of causing damage to a computer that exceeds the amount of acceptable damage to it from all identified and studied sources of its failures under certain operating conditions and at a given time interval.

**Computer security** is a security measures applied to protect computing devices (computers, smartphones and others), as well as computer networks (private and public networks, including the Internet). The field of activity of system administrators covers all processes

and mechanisms by which digital equipment, the information field and services are protected from accidental or unauthorized access, modification or destruction of data, and is of increasing importance due to the growing reliance on computer systems in the developed community.

**Cybersecurity** is a section of information security, within which the processes of formation, functioning and evolution of cyber objects are studied, in order to identify the sources of cyber danger that are formed in this case, determine their characteristics, as well as their classification and the formation of regulatory documents, the implementation of which should guarantee the protection of cyber objects from all identified and studied sources of cyber hazard.

**Cybersecurity** is the process of using security measures to ensure the confidentiality, integrity, and availability of data. The system administrator ensures the protection of assets, including data on the local network of computers and servers. In addition, buildings and, most importantly, personnel are taken under protection.

**The goal of cybersecurity** is to protect data (both in transit and/or exchange and in storage). Countermeasures may also be applied to ensure data security. Some of these measures include (but are not limited to) access control, staff training, auditing and reporting, risk assessment, penetration testing, and authorization requirements.

World practice in recent years shows that the chances of a successful investigation of cybercrime is only 0.05%! Meanwhile, the estimated damage from cybercrime will cost, according to experts, the global economy $6 trillion as early as 2021. For comparison, this is twice as much as the criminal world earns from “traditional” crimes: drug trafficking, prostitution, robberies, arms sales, etc.

While debate continues about the reasons for such a large gap between the scope of cybercrime and the capacity of law enforcement and law enforcement structures are mainly disputes about public openness and national security.

In general, the following **types of cybercrime can be distinguished** as financially oriented (phishing, cyber extortion, carding, skimming, etc.). For example: citizens filed applications with the police department, in which they report that an unknown person, using the Telegram messenger, reports on the results of a competition allegedly held among

persons who have contributed money to buy cars, then fraudulently finds out the details of bank plastic cards as a result, illegally appropriates the funds available on them (these acts are qualified by part 3 of the article 169 of the Criminal Code of the Republic of Uzbekistan);

*cybercrimes related to the invasion of privacy or the mercenary use of personal data of other persons*, by registering his mobile phone in the national UZIMEI system, a person discovers that an unknown mobile device has already been registered to his personal passport data (part 2 of the article 1412 and part 2) 2 article 182 of the Criminal Code of the Republic of Uzbekistan);

*cybercrime against public safety and public order*; for example, it was found that a number of persons are engaged in the dissemination of materials on the Internet that promote extremism (part 3 of the article 2441 of the Criminal Code of the Republic of Uzbekistan).

In this regard, the President of the country set a task for legal services, in particular the Ministry of Internal Affairs, to prepare drafts of relevant legislative and other regulatory legal acts. Thus, the Laws of the Republic of Uzbekistan «About Informatization», «About Electronic Government», « About the Protection of Information in the Automated Banking System», Resolution of the Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan as of January 26, 2022 No. 1781-IV "About the Bill of the Republic of Uzbekistan No. PL-869 « About cybersecurity», Decrees of the President of the Republic of Uzbekistan No. DP-4947 as of February 7, 2017 « About the strategy of actions for the further development of the Republic of Uzbekistan», « About the development strategy of New Uzbekistan for 2022-2026» as of 01/28/2022 No. UP-60, Decrees of the President of the Republic of Uzbekistan No. PR-4024 as of November 21, 2018 « About measures to improve the system for monitoring the implementation of information technologies and communications, organizing their protection» No. PP-4452 as of September 14, 2019 « About additional measures to improvement of the system of control over the introduction of information technologies and communications, organization of their protection».

Thus, Uzbekistan, according to the data of October 12, 2021, «Global Cybersecurity Index» took 70th place in the rating of countries in terms of cybersecurity. This Global Cybersecurity Index combines 82 questions in

five main areas, each of which is awarded 20 points. When compiling the rating, the following indicators are taken into account: legal, technical and organizational measures, and criteria for capacity development and cooperation. In the segment of legal measures, Uzbekistan received 19.27 points, in terms of capacity development - 15.68 points, in terms of cooperation - 13.56 points, in technical measures - 12.56 points and in organizational - 10.05 points. The overall final result was 71.11 points. Among the countries of Central Asia, the Republic took second place, losing only to Kazakhstan.

In addition, the National Cybersecurity Strategy for 2020-2023 was developed, which includes regulating the fight against crime in the national cyberspace, the formation of a unified cybersecurity system and a legal framework in the field of protecting critical infrastructure from cyber attacks strengthening cyber security measures in the country.

Adoption of the bill «About Cyber Security» is expected, which will include mechanisms for protecting information and communication technologies from modern cyber threats, the rights of state bodies, enterprises and organizations in the field of cyber security and define their responsibilities in this area.

President of Uzbekistan Shavkat Mirziyoyev noted «returning the trust of the people» as the main task of the entire reform of the internal affairs bodies of the country. With this slogan, the head of state acknowledged that over the past years, the population has accumulated a lot of negativity towards the law enforcement agencies of the country.

Among these ongoing reforms, a special place deserves the improvement of the rule-making process, increasing the level of professional training of officers of legal services, strengthening their role and responsibility for the high quality of legal support for the activities of internal affairs bodies.

Within the framework of the Decree of the President «About the Development Strategy of New Uzbekistan for 2022-2026» adopted on January 28, 2022 No. DP-60, which approved the Development Strategy developed as a result of a wide public discussion based on the principle “From the Action Strategy to the Development Strategy” New Uzbekistan for 2022-2026 and the State Program for its implementation in the «Year of Promotion of Human Interests and Development of

Mahalla», provides for the implementation of measures, in particular, improving the practice of consulting with civil society institutions in the legislative process, developing and expanding the assessment of the regulatory impact of acts legislation as part of the application of elements of the "smart regulation" model in order to ensure the stability, quality and effectiveness of the legal regulation of public relations, reviewing the requirements for modern technologies and digital activities in the framework of increasing the competitiveness of the legal system and mobilizing new drivers of the economy, reduction of legislative acts in the framework of reducing the "regulatory burden" in industries, systematization of legal acts regulating the activities of state bodies, development of a concept for the development of legislation of the Republic of Uzbekistan, reduction of the circle of state bodies with the authority to adopt departmental normative legal acts, as well as continuation of work on optimizing the number of these acts in order to create and ensure a safe space in the country.

At the same time, in our opinion, there are still certain gaps in legislative practice related to the regulation of liability issues in the information space.

In this regard, it is proposed that it is advisable to take the following measures to build global immunity to combat cybercrime:

*firstly*, it is the development, review and coordination of information security policy; consulting assistance to state and economic bodies on organizational and technical issues of ensuring information and cyber security; providing state and economic bodies with regulations in the field of ensuring information and cyber security (regulatory support); holding seminars and trainings on ensuring information and cyber security; coordination of annual action plans to ensure information and cyber security of state and economic bodies and coordination of their implementation;

*secondly*, cooperation is needed at the transnational, national and corporate levels. Here we are talking about such a problem as the inability to conduct investigations on a cyber-transnational scale, as is done, for example, by Interpol or foreign intelligence agencies in relation to «traditional» criminals and crimes;

*thirdly*, it is necessary to attract and exchange experience with foreign

experts, that is, to exchange and share their achievements and practices in order to raise the general level of law enforcement structures, especially in those countries that become the main victims and at the same time important nodes of organized cybercrime;

*fourthly*, it is necessary to introduce the practice of public-private partnership. Since, cybercrime is not only in the area of responsibility of law enforcement agencies. Every victim of cybercrime is a data owner, whether in the public or private sector, which is part of an interconnected and interdependent global ecosystem, and today the potential to fight with organized cybercrime is in the hands of corporate structures. Promoting data sharing and collaboration, as well as defining clear roles and guidelines for leveraging each other's strengths, can help build a united front in the fight against crime in this area;

*fifthly*, it is advisable to study and implement the best practices of some foreign countries where cybersecurity is taught from the school bench. For example, in the UK, schoolchildren are proposed cybersecurity lessons, in which they learn the skills to ensure the safety of British companies and organizations from network attacks by hackers. The curriculum is developed by the UK Ministry of Culture, Media and Sport. Lessons are implemented both online and in the form of extracurricular activities, which take place four times a week and are conducted by expert teachers. With students, real cybersecurity problems and the practice of solving them are considered. The program is aimed at students aged 14 to 18. Classes have been held since September 2017.

**Bibliography:**

1. Criminal Code of the Republic of Uzbekistan dated September 22, 1994 // National Legislation Database, as of February 16, 2022, No. 03/22/754/0134.

2. Law of the Republic of Uzbekistan, as of December 11, 2003, No. 560-II «About Informatization»// National Legislation Database, as of March 30, 2021, No. 03/21/679/0256.

3. Law of the Republic of Uzbekistan, as of 04.04.2006 No. LRU-30 «About the protection of information in the automated banking system»// Collected Legislation of the Republic of Uzbekistan, 2006, No. 14, Art. 112.

4. Law of the Republic of Uzbekistan, as of 09.12.2015 No. LRU-395 «About Electron Government»// Collected Legislation of the Republic of Uzbekistan, 2015, No. 49, art. 611.

5. Decree of the President of the Republic of Uzbekistan, as of January 28, 2022 No. UP-60// National Legislation Database, January 29, 2022 No. 06/22/60/0082.

6. Decree of the Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan, as of January 26, 2022, No. 1781-IV «About the Bill of the Republic of Uzbekistan No. PZ-869 «About Cybersecurity»// https://lex.uz/docs/5860338.

7. Decree of the President of the Republic of Uzbekistan, as of February 7, 2017 No. DP-947 «About the strategy of actions for the further development of the Republic of Uzbekistan»//National database of legislation, 05/01/2021, No. 06/21/6217/0409.

8. Decree of the President of the Republic of Uzbekistan, as of January 28, 2022 No. DP-60 «About the Development Strategy of New Uzbekistan for 2022-2026»//National database of legislation, 01/29/2022, No. 06/22/60/0082.

9. Decree of the President of the Republic of Uzbekistan, as of November 21, 2018 No. PP-4024 «About measures to improve the system of control over the introduction of information technologies and communications, the organization of their protection»// National database of legislation, 22.11.2018, No. 07/18/4024/2200; 06/29/2021, No. 06/21/6252/0617.

10. Decree of the President of the Republic of Uzbekistan, as of September 14, 2019 No. PP-4452 “About additional measures to improve the system of control over the introduction of information technologies and communications, the organization of their protection”// National database of legislation, 16.09.2019, No. 07/19/4452/4207.

11. Cybersecurity rating: Uzbekistan entered the top 70 countries// https://uz.sputniknews.ru.

12. Uzbekistan thinks about cybersecurity.//https://www.gazeta.uz.

13. Decree of the President of the Republic of Uzbekistan as of January 28, 2022 No. DP-60 «About the Development Strategy of New Uzbekistan for 2022-2026»//National Legislation Database, January 29, 2022, No. 06/22/60/0082.

14. Reform of the Ministry of Internal Affairs in Uzbekistan: will expectations come true?// cabar.asia/ru.

15. Fighting cybercrime - what happens to the law when the law can't be enforced?// https://tace.uz.

16. «Reliance spells end of road for ICT amateurs», as of May 07, 2013, The Australian.//https://ru.wikipedia.org.

17. https://ru.wikipedia.org.

18. Cybersecurity: Understanding the Online Threat// https://ru.wikipedia.org.

19. Fighting cybercrime - what happens to the law when the law can't be enforced?// https://tace.uz.

20. Cyber Security vs Cyber Crime//https://iiv.uz.