COMPARATIVE LEGAL ANALYSIS OF FOREIGN COUNTRIES WITH UZBEKISTAN IN THE SPHERE OF CYBER SECURITY AND SOME CONCLUSIONS

Ramazonov Ismoilbek Abdirashidovich
Master student of the direction of "Sports Law"
No. 70420105
Tashkent State University of law
Tel.: +998909887227
email: ismailrashidovich@gmail.com

Abstract: Annotation: this thesis deals with issues in the field of the information society and information security. In addition, a comparative analysis of the legal practice of foreign countries is carried out and methods for resolving the problems that have arisen in ensuring cybersecurity are considered. And also based on the study, some conclusions were drawn and recommendations were given.

Key words: cyber law, cyber security, cyber attack, cyber threat, foreign experience.

СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ ЗАРУБЕЖНЫХ СТРАН С УЗБЕКИСТАНОМ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ И НЕКОТОРЫЕ ВЫВОДЫ

Рамазонов Исмоилбек Абдирашидович
Магистрант направления «Спортивного права»
№ 70420105
Ташкентского государственного юридического университета
Тел.: +998909887227
email: ismailrashidovich@gmail.com

Аннотация: в данном тезисе рассмотрены вопросы в сфере информационного общества и информационной безопасности. Кроме того, проводится сравнительный анализ правовой практики зарубежных стран и рассмотрены методы разрешения возникших проблем по обеспечению кибербезопасноти. А так же исходя из проведенного исследования сделаны некоторые выводы и даны рекомендации.

Ключевые слова: икиберправо, кибербезопасность, кибератака, киберугроза, зарубежный опыт.

The current stage of development of the world community is characterized by the globalization of the information sphere, the formation of signs of the information society, which significantly affects the area of legal relations and relevant regulators. The Internet is the entity that stimulates globalization in other areas of social life and influences the role of the legal system. the active development of information technologies, the global Internet is developing at a colossal pace, both in quantitative and qualitative terms (the number of operators and users of the Network is increasing, the range of services being provided is expanding). With the emergence of new public relations associated with the use of the Internet, legal regulation in this area is of particular importance, which will ensure the sustainable and effective development of legislation in the field

of relations on the Internet. These changes exacerbate the problem of the rule of law and raise the question of the formation of a rule of law society.

In conclusion, it is worth noting that restrictive measures introduced in the world contributed to the accelerated development of distance learning, telemedicine, online commerce and other areas. But along with this, the challenges of information security have become much more acute, the level of cybercrime, various risks and threats in this area has increased dramatically, ranging from the dissemination of distorted information and counterfeit medicines to various forms of online fraud and hacker attacks. The Internet has become increasingly used to disrupt the performance of information and communication networks, critical infrastructure of the state, as well as interference in the private life of citizens. And the cross-border nature of these threats dictates the need to complement national efforts with collective action at the regional and international levels.

Based on the foregoing, we can understand that there are some problems in ensuring cybersecurity. We have already understood that state intervention is necessary to ensure and implement cybersecurity, since it is the state that acts as a guarantor to ensure our rights. In addition, it should be noted that the legislation of the Republic of Uzbekistan comes from the idea of a personality, a society, a state, the state policy of the Republic of Uzbekistan in the field of cybersecurity is aimed primarily at ensuring the constitutional rights of citizens of the Republic of Uzbekistan, protecting the rights of each segment of the population and ensuring security in the whole state. I pursue these goals, then some situations that require an urgent solution will be described. Therefore, based on the above analysis in the dissertation work, we will give our decisions based on foreign experience, logical thinking and the legal framework.

The President signed the Law No. Z R U-764 dated April 15, 2022 “On Cybersecurity”. The law consists of 8 chapters and 40 articles, the Document is published in the National Database of Legislation and will come into force on 17.07.2022 .[1]

Drawing conclusions, it is worth noting that one of the main laws in the field of cybersecurity will soon come into force. But in our opinion, we should think about how to create more detailed and narrow-profile norms that not only regulate certain legal relations, but define and regulate them. We can see this kind (nature) of norms in the practice of foreign countries of the Council of Europe.

In addition, attention should be paid to the creation of high-quality and impenetrable security programs. As far as we know, we have state programs to ensure security of various categories, which must correspond to a certain level of protection. And for the highest protection, employees should be trained who can develop and further refine the system in case of detection of vulnerabilities. Here, it is necessary to place emphasis on the training of highly qualified and efficient personnel.

And speaking of the vulnerabilities of the software system, one should pay attention to the experience of the United States. For example, the first program called Hack the Pentagon (“Hack the Pentagon ”) ran from April 18 to May 12, 2016. During this period, 138 unique and legitimate reports of security holes were submitted. There is such a notion that the creator himself in rare cases can truncate the vulnerable sides, and therefore another person should check for strength. There are a number of benefits to this experience:

- firstly, this is a chance for hackers to demonstrate and test their skills;
- secondly, hackers are rewarded and, in addition, legally hack the system;
- thirdly, the state recognizes the vulnerabilities of the system, but at the same time finds new personnel.

In this connection, in Uzbekistan, too, introduce a system of rewards for legal hacking of the system and the discovery of vulnerabilities.

And also, I would like to note that the state often takes on great responsibilities, in connection with which the achievement of the goals set may be delayed. And in order to develop the economy and the private sector, some aspects of cybersecurity should be transferred to the private sector. That is, if you pay attention to the experience of the Republic of Kazakhstan, they transferred the provision of cyber security to the private sector,

[1]See:https://www.norma.uz/novoe_v_zakonodatelstve/prinyat_zakon_o_kiberbezopasnosti

delegated their responsibilities. The private sector, by obtaining a special license, carries out its activities, in turn, the state conducts supervision (control) on the conscientious fulfillment of its obligations.

In addition, in our opinion, when exposing intruders, it is very difficult to find out I P-addresses, and therefore one should pay attention to the digital trace. In this connection, with specialists in this field, it is necessary to develop methods and methods for exposing the guilty person wherever he (she) is. Today, access to the network is carried out through VPN and this is one of the problem points.