ANALYSIS OF THE FOUNDATIONS AND LEGAL FRAMEWORK OF LEGAL RESEARCH IN THE FIELD OF CYBERSECURITY

S.N.Kurbonov
Doctor of Philosophy (PhD) in Legal Sciences
https://doi.org/10.5281/zenodo.17231495

Abstract. The article discusses the importance of cybersecurity in the modern world, the increase in cyber threats with the advancement of digitalization and the Internet, the damage caused by cybercrimes, and their global scale. It highlights national cybersecurity strategies in Uzbekistan, the development of the legislative framework, and the role of the "Digital Uzbekistan - 2030" program in ensuring security. Additionally, the article examines issues of international cooperation, scientific research, and the challenges in regulating cyberspace.

Keywords: cybersecurity, cybercrime, digitalization, threats, statistics, national strategy, legislation, digital economy, international cooperation, scientific research.

Cybersecurity is a crucial field that ensures the safety of individuals, society, and the state in the modern world. The development of digitalization, the internet, artificial intelligence, and cloud technologies is currently increasing threats such as hacking, data breaches, and cyberterrorism. This necessitates legal solutions to these problems.

According to analyses and statistics, the annual global damage from cybercrime in the world is expected to reach 11.4 trillion dollars by 2024, and it is projected to grow by 120 percent to 25.8 trillion dollars by 2026. Some sources suggest that by 2026, cybercrimes are expected to occur 5 times more frequently than the total number of global transnational crimes[1].

According to the State Unitary Enterprise "Cybersecurity Center," over 27,000,000 malicious and suspicious network incidents threatening information and cybersecurity were observed in the national internet segment during 2020. Additionally, 680 incidents occurred within the framework of ensuring the security of information systems and websites, including website failures lasting 1,000,000 minutes due to malfunctions[2]. In 2021, more than 17,097,478 malicious and suspicious network incidents threatening information and cybersecurity were observed in the national Internet segment. Furthermore, 636 incidents occurred within the framework of ensuring the security of information systems and websites, with malfunctions causing website failures lasting 1,048,216 minutes[3].

In the fight against cybercrime, it is necessary to consider the latency of this type of crime. According to experts, the latency of cybercrimes is 80% in the USA, 85% in Great Britain, 75% in Germany, and over 90% in Russia. This indicates that the statistics of actual cybercrime occurrences may be even higher[4].

The Action Strategy on five priority areas of development of the Republic of Uzbekistan for 2017-2021, approved by the Decree of the President of the Republic of Uzbekistan dated February 7, 2017 No. UP-4947, outlines the fifth direction titled "Ensuring security, interethnic harmony and religious tolerance, pursuing a deeply considered, mutually beneficial and practical foreign policy." Within this framework, the strategy defines the implementation of measures to protect the country's constitutional order, sovereignty, and territorial integrity, as

well as improving the regulatory framework in the field of cybersecurity. Specifically, it envisions the development of the National Cybersecurity Strategy for 2020-2023, the draft Law "On Cybersecurity," and the Concept of a Unified Information Policy of the Republic of Uzbekistan.

It should be noted that 17 legislative acts, 9 Presidential Decrees and Resolutions, 14 Resolutions of the Cabinet of Ministers, as well as relevant norms and many interdepartmental regulatory legal acts related to the field of cybersecurity have been adopted.

The development and implementation of the "Digital Uzbekistan 2030" program in Uzbekistan will serve, first of all, to form sound and perfect organizational and legal mechanisms, as well as to ensure close cooperation between government bodies and business entities in the implementation of innovative ideas, technologies, and developments, to cover production and services in all spheres and sectors with digital technologies, to train personnel with deep modern knowledge and intellectual potential in this area, thereby creating a "safe information society" environment in the country[5].

In recent years, within the framework of the development of the digital economy, large-scale work has been carried out to ensure security in the use of e-commerce and digital services.

At the same time, the timely detection and effective investigation of crimes committed using information and communication technologies require the use of special digital methods and tools, the development of techniques for working with digital evidence, the training of highly qualified specialists, and the creation of a systematic research base in this area.

In order to create effective mechanisms for the timely and complete detection of crimes in our country, the unconditional implementation of the principle of the inevitability of responsibility, including the further improvement of the process of proving a person's guilt with scientifically and technically substantiated reliable evidence, the Law Enforcement Academy of the Republic of Uzbekistan has been tasked with conducting innovative research in the field of digital forensics, analyzing and implementing big data ("Big Data"), artificial intelligence, and other advanced technologies, within which the Research Institute of Digital Forensics has been established on the basis of the Scientific and Methodological Center of Digital Forensics[6].

Cybersecurity is one of the most important areas ensuring the security of individuals, society, and states in the modern world. The globalization of cyberspace, the increasing complexity of borders between jurisdictions, and the transnational nature of cybercrimes require the harmonization of legislation at the international level.

Increase in cyber threats According to international organizations, including Interpol and the UN, the annual damage from cybercrime exceeds 6 trillion US dollars, and the number of attacks on critical infrastructure is increasing year by year.

In addition, the need to protect human rights, strengthening cybersecurity measures, creates a risk of violation of the confidentiality of personal data, freedom of speech, and the right to access information, which requires a coordinated legal approach.

The development of new technologies, such as blockchain, artificial intelligence, and quantum computing, currently used in practice, requires the adaptation of legislation to new realities.

Also, the insufficient formation of theories and scientific approaches in this area necessitates the clarification of the concepts used in it, the classification of cyber threats (for

example, phishing, DDoS attacks, malware) and a deep study of their impact on legal systems. The conditions for applying and implementing the basic principles of confidentiality, integrity, and accessibility of data (CIA triad) are not reflected in the legislation.

Moreover, the fact that states have not ratified international standards and agreements, such as important documents such as the Budapest Convention (2001), and UN approaches to regulating cyberspace, also causes scientific debate. It should be noted that problems in the field of law enforcement, in particular, the boundaries of jurisdiction in cyberspace, the identification of cybercriminals, the collection and recognition of digital evidence, as well as difficulties related to international cooperation, are also causing various problems.

In general, the main goal of research in this area is the systematization of knowledge on the legal aspects of cybersecurity and the development of recommendations for improving the regulatory framework. Special attention will be paid to the need to develop universal international standards for effectively combating cyber threats while preserving the principles of state sovereignty. The lack of a unified approach to regulating cyberspace allows for the creation of legal loopholes used by cybercriminals to evade responsibility.

Ensuring the security of cyberspace and the early eradication of cybercrime is a multifaceted process that requires everyone to feel responsible and act in unity. In order to ensure cybersecurity, it is important to identify the factors and conditions leading to the emergence of cybercrimes, prepare substantiated recommendations by analyzing pre-trial investigation materials, cases of administrative offenses, and criminal cases using scientific methods, and use modern technological approaches in their implementation in law enforcement practice.

References:

Тошпулатов А. Кибержиноятларни жиловлаш орқали хавфсиз кибермакон яратиш. Рақамли трансформация шароитида кибержиноятларнинг барвақт олдини олишда Ўзбекистон тажрибаси // Электрон манба: https://gov.uz/uz/iiv/news/view/52319 (мурожаат вақти: 09.08.2025).

“Киберхавфсизлик маркази” давлат унитар корхонаси томонидан тайёрланган 2020-2021 йиллар якуний ҳисоботлари //
https://tace.uz/upload/iblock/9d5/1.%20%D0%98%D1%82%D0%BE%D0%B3%D0%B8%202021_%
D1%83%D0%B7.pdf.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2004 йил 24 ноябрдаги “Оммавий коммуникациялар соҳасида бошқарув тузилмасини такомиллаштириш чора-тадбирлари тўғрисида”ги 555-сонли қарори // https://lex.uz/ru/docs/373340 (мурожаат вақти: 09.08.2025).

Тошпулатов А. Кибержиноятларни жиловлаш орқали хавфсиз кибермакон яратиш. Рақамли трансформация шароитида кибержиноятларнинг барвақт олдини олишда Ўзбекистон тажрибаси // Электрон манба: https://gov.uz/uz/iiv/news/view/52319 (мурожаат вақти: 09.08.2025).

Собиров Ш. Ўзбекистонда киберхавфсизликни таъминлаш – давр талаби таҳлил ва тавсиялар // Электрон манба: https://zamin.uz/jamiyat/81496-zbekistonda-

kiberhavfsizlikni-taminlash-davr-talabi-talil-va-tavsijalar.html (мурожаат вақти: 09.08.2025).
Ўзбекистон Республикаси Президентининг 2024 йил 21 июндаги “Рақамли криминалистика соҳасида илмий-тадқиқот фаолиятини ташкил этиш чора-тадбирлари тўғрисида”ги ПҚ-229-сон қарори // Электрон манба: https://lex.uz/uz/docs/6977736 (мурожаат вақти: 09.08.2025)..