HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

UDC 342.924

DIGITAL LAW IN ENSURING CYBERSECURITY: REFORMS AND PROSPECTS IN LAW ENFORCEMENT ACTIVITIES OF UZBEKISTAN

Alimzhan Atabaevich Matchanov

professor of the Department of Cyber Law of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, Doctor of Law, Professor,

tel. +9987747073, E.mail: alimjan.matchanov@gmail.com

Abstract: The article examines digital law as an emerging intersectoral direction of legal regulation of public relations in the context of digitalization and its importance for ensuring cybersecurity of the Republic of Uzbekistan. Modern changes in national legislation are analyzed, including the Law of the Republic of Uzbekistan «On Cybersecurity», legislation on personal data and e-government, as well as the Cybersecurity Strategy of the Republic of Uzbekistan for 2026–2030. Particular attention is paid to the transformation of law enforcement activities under the influence of digital technologies, the problems of detecting, recording, preserving and using digital evidence, cross-border access to electronic data, the use of artificial intelligence and training. Based on the analysis of national and foreign experience, the author's model of a digital law enforcement circuit is proposed, combining regulatory, organizational, technological, procedural and international components.

Keywords: digital Law, Cybersecurity, Cybercrime, Law Enforcement, Digital Evidence, Electronic Evidence, Digital Forensics, Artificial Intelligence.

KIBERXAVFSIZLIKNI TA'MINLASHDA RAQAMLI HUQUQ: O'ZBEKISTON HUQUQNI MUHOFAZA QILUVCHI ORGANLARI FAOLIYATIDAGI ISLOHOTLAR VA ISTIQBOLLAR

Annotatsiya. Mazolada raqamlashtirish sharoitida shakllanayotgan raqamli huquqning O'zbekiston Respublikasida kiberxavfsizlikni ta'minlashdagi o'rni hamda huquqni muhofaza qiluvchi organlar faoliyatiga ta'siri tadqiq etiladi. O'zbekiston Respublikasining “Kiberxavfsizlik to'g'risida”gi Qonuni, shaxsga doir ma'lumotlar va elektron hukumat sohasidagi qonunchilik, shuningdek, O'zbekiston Respublikasining 2026–2030-yillarga mo'ljallangan Kiberxavfsizlik strategiyasi tahlil qilinadi. Huquqni muhofaza qiluvchi organlar faoliyatining raqamli texnologiyalar ta'sirida transformatsiyasi, raqamli dalillarni aniqlash, qayd etish, saqlash va ulardan foydalanish, elektron ma'lumotlarni transchegaraviy olish, sun'iy intellektdan foydalanish hamda kadrlar tayyorlash masalalariga alohida e'tibor qaratiladi. Milliy va xorijiy tajriba asosida normativ-huquqiy, tashkiliy, texnologik, protssessual va xalqaro komponentlarni birlashtiruvchi raqamli huquqni muhofaza qilish konturi modeli taklif etiladi.

Kalit so'zlar: raqamli huquq, kiberxavfsizlik, kiberjinoyatchilik, huquqni muhofaza qiluvchi organlar, raqamli dalillar, elektron dalillar, raqamli kriminalistika, sun'iy intellekt.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

PROSPECTS FOR THE USE OF ARTIFICIAL INTELLIGENCE IN THE METHODOLOGY OF TEACHING LEGAL DISCIPLINES IN UZBEKISTAN

Abstract. The article examples digital law as an emerging cross-sectoral area of legal regulation in the context of digital transformation and its role in ensuring cybersecurity in the Republic of Uzbekistan. It analyzes recent developments in national legalization, including the Law of the Republic of Uzbekistan "On Cybersecurity", legalization on personal data and e-government, as well as the Cybersecurity Strategy of the Republic of Uzbekistan for 2026–2030. Particular attention is given to the transformation of law enforcement activities under the influence of digital technologies, the identification, collection, reservation and use of digital evidence, cross-border access to electronic data, the use of artificial intelligence and professional training. Based on national and international expertise, the author proposals a model of a digital law-enforcement cybersecurity framework combining normative, organizational, technological, procedural and international components.

Keywords: digital law, cybersecurity, cybercrime, law enforcement, digital evidence, electronic evidence, digital foresight.

The digital transformation of society has changed not only the way in which communication, economic activity and the provision of public services are conducted, but also the mechanism by which crimes are committed. Modern crime is increasingly using digital infrastructure as a means, object or environment for committing illegal acts. However, the digital component is not limited to cybercrime itself: email correspondence, banking transactions, mobile device data, geolocation information, cloud storage, CCTV records, and social media data can be essential in traditional crime investigations.

For the law enforcement system, this means a qualitative change in the object of professional activity. If previously the main source of evidentiary information was material objects, documents and testimony of persons, today a significant part of the information exists exclusively in digital form.

The urgency of the problem for Uzbekistan is confirmed by the dynamics of cybercrime. According to published data, in 2021–2025 the number of cybercrimes in the republic increased from 4,865 to 62,440, that is, more than 11 times. During this period, citizens suffered damage in excess of 3.7 trillion soums as a result of cybercrimes [1].

Consequently, countering cybercrime can no longer be considered solely as a technical challenge. It requires the simultaneous development of criminal law, criminal procedure, criminology, data law, international cooperation and professional training for law enforcement officials.

In these conditions, the category of digital law acquires special importance, which it is advisable to consider as a set of interrelated legal norms regulating social relations regarding creation, processing, storage, transmission, use, protection and legal assessment of digital information.

In modern legal literature, digital law is increasingly viewed not as a fully formed independent branch of law, but as a complex intersectoral array of legal norms. Its specificity is that digitalization simultaneously affects constitutional rights, civil circulation, criminal law, criminal procedure, administrative regulation, information security and international cooperation.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

Five interrelated elements are of particular importance for law enforcement: (1) legal regulation of cybersecurity; (2) protection of personal data; (3) regulation of electronic public administration; (4) criminal law counteraction to cybercrime; (5) procedural regulation of the acquisition and use of digital information.

The national legal framework of Uzbekistan in this area has received significant development. The basic special act is the Law of the Republic of Uzbekistan dated April 15, 2022 № ZRU-764 «On Cybersecurity» [2]. The official list of legislation of the Ministry of Internal Affairs of the Republic of Uzbekistan confirms the details of this law and the date of its adoption.

The Law of the Republic of Uzbekistan dated July 2, 2019 № ZRU-547 «On Personal Data», which forms the legal basis for the processing and protection of information relating to a specific or identifiable individual, is also important.

The next element is legislation on e-government. The Law of the Republic of Uzbekistan dated December 9, 2015 № ZRU-395 «On Electronic Government» established the legal basis for the functioning of electronic interaction between the state, citizens and organizations [3].

The legal significance of electronic documents and digital procedures is supplemented by the Law of the Republic of Uzbekistan «On Electronic Digital Signature», adopted in 2022. The law regulates relations in the field of use of electronic digital signatures [4].

Thus, the national system already contains the main elements of digital legal regulation. However, the problem lies not so much in the absence of separate regulations, but in the need to ensure their systematic interaction in relation to law enforcement activities.

A qualitatively new stage in the development of the national cybersecurity system is associated with the Decree of the President of the Republic of Uzbekistan dated March 10, 2026 № UP-38 «On defining the Cybersecurity Strategy of the Republic of Uzbekistan and improving the cybercrime prevention system» [5]. The decree approved the Cybersecurity Strategy Republic of Uzbekistan for 2026–2030 [6]. The fundamental significance of this document lies in the transition from a predominantly infrastructural understanding of cybersecurity to a comprehensive model that includes legal, organizational, technical, personnel and international mechanisms.

The goals are to strengthen national protection of critical information and government digital infrastructure. This applies to systematically reducing the risks existing in cyberspace, actively combating cybercrime, developing digital innovations and artificial intelligence technologies, as well as developing international cooperation.

Particularly noteworthy is the consolidation in the Strategy of the task of increasing the capabilities of digital forensics and the potential of specialized law enforcement units. It also provides for the creation of national centers for monitoring and responding to cybersecurity incidents and the formation of operational interaction between critical information infrastructure entities, the authorized body and law enforcement agencies. Hence, modern reform involves a shift from responding to committed cybercrime to continuous monitoring, early detection, prevention and technology-enabled investigation.

International experience allows us to assess the place of the national system of Uzbekistan in the overall process of cybersecurity development. The International Telecommunication Union's Global

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

Cybersecurity Index 2024 evaluates states in five areas: legal measures, technical measures, institutional measures, capacity development and international cooperation [7].

According to materials from ITU (International Telecommunications Union, or ITU) International Telecommunication Union), Uzbekistan has improved its position considerably, with the country's score rising from 71 points in the previous assessment to 89.2 points, placing the State in the second group – Advancing [8].

It is especially important that the new assessment names not only legal measures, but also capacity development and international cooperation as Uzbekistan's strengths. This allows us to conclude that the further development of the national system should be focused not only on creating a regulatory framework, but also on increasing the ability of law enforcement agencies to practically use digital technologies.

In other words, the next stage of reform should be associated with the transition from «legal support for cybersecurity» to «enforcement in the digital environment».

One of the most significant challenges of digital transformation is changing the evidence base of the criminal process. In practice, digital information can be found: on a smartphone; personal computer; organization server; in cloud storage; at a telecom operator; in a banking information system; on a social network; in a messenger; on a server located outside the state.

NIST (US National Institute of Standards and Technology (National Institute of Standards and Technology) emphasizes that the preservation of digital evidence has specific features that distinguish it from traditional types of evidence. Digital data can be easily modified, copied and moved, and the actual location of information in the cloud infrastructure can sometimes be unknown [9].

INTERPOL (International Criminal Police Organization) defines digital forensics as the branch of forensic forensics concerned with the identification, receipt, processing, analysis and presentation of data stored in electronic form. Electronic evidence, as assessed by the organization, is a component of virtually all categories of criminal activity [10].

It follows that the traditional model «to remove the physical medium and examine it» is gradually giving way to a more complex model: «detection of a digital trace, legal sanction, fixation of the digital environment, data acquisition, ensuring integrity, forensic analysis, procedural assessment». One of the most difficult challenges remains the cross-border nature of digital information. The criminal may be in Uzbekistan, the victim – in another state, and the information necessary for the investigation – stored on an international digital platform.

In parallel, a universal international legal mechanism is being formed – UN Convention against Cybercrime, adopted on December 24, 2024 [11]. Uzbekistan signed this Convention on 25 October 2025 [12] (Hanoi Convention). As of 18 July 2026, the Convention has not yet entered into force: 40 ratifications, acceptances, approvals or accessions are required; as of that date, there were 79 signatures of states and 3 parties that have ratified it. This fact is of direct importance for national legislation, since it requires the preparation of procedures that will allow the effective implementation of future international mechanisms for obtaining electronic evidence.

For Uzbekistan, it seems advisable to create a unified secure system of electronic requests from law enforcement agencies to providers.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

Increasing law enforcement access to digital information should not mean unlimited data collection. In the digital environment, a fundamental conflict arises between two social entities significant interests: the effectiveness of crime investigation and the individual's right to privacy.

Consequently, the national model of digital law should be based on the principles of: legality – access to data is carried out only on the basis provided by law; necessity – digital information is requested only if there is an objective need; proportionality – the volume of data obtained corresponds to the purpose of the investigation; intended use – the information obtained is not used for purposes unrelated to the basis for its receipt; minimization – redundant information should not be collected unnecessarily; controls – the most intensive forms of intervention must be accompanied by judicial or other independent controls.

It is the combination of these principles that avoids a situation in which the fight against cybercrime itself becomes the basis for excessive interference in digital privacy.

The digitalization of crime and law enforcement is causing traditional legal mechanisms to gradually no longer fully conform to the modern structure of digital social relations. There is a need to create a comprehensive digital law system that should combine rules on cybersecurity, personal data, e-government, digital evidence, artificial intelligence and international cooperation.

Thus, digital law should become not only a tool for regulating technological relations, but also the foundation of a new law enforcement model in which the effectiveness of the investigation is combined with evidence, technological validity, international compatibility and the guarantee of human rights.

List of sources used:

1. National News Agency of Uzbekistan. As a result of cybercrimes, citizens suffered damage exceeding 3.7 trillion soums. 24/12/2025. [UZA – material about the dynamics of cybercrime in Uzbekistan] (https://uza.uz/ru/posts/v-rezultate-kiberprestupleniy-grazhdanam-byl-nanesen-uscherb-prevyshayuschiy -37-trilliona-sumov_799702?utm_source=chatgpt.com)
2. Law of the Republic of Uzbekistan dated April 15, 2022 № ZRU-764 «On cybersecurity». National framework of legislation of the Republic of Uzbekistan. [Law of the Republic of Uzbekistan «On Cybersecurity»] (https://lex.uz/ru/docs/5960609?utm_ source=chatgpt.com)
3. Law of the Republic of Uzbekistan dated December 9, 2015 № ZRU-395 «On electronic government». National framework of legislation of the Republic of Uzbekistan. [Law of the Republic of Uzbekistan «On Electronic Government»](https://lex.uz/en/docs/2833860?utm_source=chatgpt.com)
4. Law of the Republic of Uzbekistan «On Electronic Digital Signature». 2022. [Text of the Electronic Digital Signature Act](https://lex.uz/Pages/GetPdf.aspx?file=LexUz_6378533.pdf&utm_source=chatgpt.com)
5. Decree of the President of the Republic of Uzbekistan dated March 10, 2026 № UP-38 «On defining the Cybersecurity Strategy of the Republic of Uzbekistan and improving the cybercrime prevention system». [Presidential Decree № UP-38](https://nrm.uz/contentf?doc=803280_ukaz_prezidenta_respubliki_uzbekistan_ot_10_03_2026_g_n_up-38_ob_opredelenii_strategii_kiberbezopasnosti_respubliki_uzbekistan_i_

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

sovershenstvovanii_sistemy_preduprejdeniya_kiberprestupnosti&products=1_vse_zakonodatelstvo_uzbekistana&utm_source=chatgpt.com)

6. Cybersecurity strategy of the Republic of Uzbekistan for 2026–2030. Appendix № 1 to the Decree of the President of the Republic of Uzbekistan dated March 10, 2026 № UP-38. [Cybersecurity Strategy of the Republic of Uzbekistan for 2026–2030](https://nrm.uz/contentf?doc=803273_strategy_kiberbezopasnosti_respubliki_uzbekistan_na_2026-2030_gody_%28 prilojenie_n_1_k_ukazu_prezidenta_ruz_ot_10_03_2026_g_n_up-38%29& products=1_vse_zakonodatelstvo_uzbekistana&utm_source=chatgpt.com)
7. International Telecommunications Union. Global Cybersecurity Index 2024. Geneva, 2024. [ITU – Global Cybersecurity Index](https://www.itu.int/en/ITU-D/Cybersecurity/ pages/global-cybersecurity-index.aspx?utm_source=chatgpt.com)
8. International Telecommunications Union. Uzbekistan has risen to the category of advanced countries in terms of information security development. 2025. [ITU – Uzbekistan results in Global Cybersecurity Index 2024](https://www.itu.int/ru/ITU-D/Regional-Presence/CIS/Pages/News/01/14/2025.aspx?utm_source=chatgpt.com)
9. Guttman B., White D.R., Williams S., Walraven T. Digital Evidence Preservation: Consultations for Evidence Handlers. NISTIR 8387. National Institute of Standards and Technology, 2022. [NIST – Digital Evidence Preservation](https://www.nist.gov/ publications/digital-evidence-preservation-considerations-evidence-handlers?utm_source= chatgpt.com)
10. INTERPOL. Digital Forensics. International Criminal Police Organization. [INTERPOL – Digital Forensics](https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics?utm_source=chatgpt.com)
11. United Nations. United Nations Convention against Cybercrime; Strength International Cooperation for Combatting Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes. New York, 24 December 2024. [United Nations – Convention against Cybercrime](https://treaties.un.org/Pages/showDetails.aspx?clang=_en&objid=0800000280670c50&utm_source=chatgpt.com)
12. United Nations Treaty Collection. United Nations Convention against Cybercrime <TAG1> Status of Treaties. Information about the signing of the Convention by Uzbekistan 25/10/2025. [U.N. Treaty Collection <TAG1>status of the Convention against Cybercrime](https://treaties.un.org/Pages/ ViewDetails.aspx?chapter=18&clang=_en&mtdsg_no=XVIII-16&src=TREATY&utm_source= chatgpt.com)