

JOURNAL OF DIGITAL LAW AND INNOVATION (JDLI)

LAW • TECHNOLOGY • INNOVATION • JUSTICE

 OPEN
ACCESS

ISSN
3093-9364



OUR FIELDS

- Digital law
- Cybersecurity law
- Artificial intelligence and robotics law
- Intellectual property law
- LegalTech and legal innovations
- E-government and digital public services
- Legal aspects of AgroTech and GreenTech
- Smart city and digital governance



OUR INDEXING

 Google Scholar

 Zenodo

 DOI

 OpenAIRE

 Open Access



AI

! Unauthorized Access

UNAUTHORIZED
ACCESS

SYSTEM
BREACH



CYBER ATTACK



DIGITAL LAW



<https://unireview.uz/index.php/jdli>



Published by
UniLex Global



VOLUME 2

ISSUE 1



AUGUST 2026



“UNILEX GLOBAL” LLC

**Raqamli huquq va innovatsiya
jurnali
Journal of Digital Law and
Innovation**

**August, 2026
VOLUME 2, ISSUE 1**



EDITORIAL TEAM

Editor-in-Chief, Tukhtashev Hikmatilla Ismatillaevich - Head of the Department of Legal Sciences, Doctor of Philosophy in Legal Sciences (PhD), TIAME National Research University, Tashkent, Republic of Uzbekistan.

1. **Editorial Board Member Borotov Mirodiljon Xomudjonovich** — Doctor of Legal Sciences, Professor, Head of the Department of Civil Law, International Law and International Organizations, Institute of State and Law of the Academy of Sciences of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
2. **Editorial Board Member Maripova Sevarxon Aribjanovna** — Doctor of Philosophy in Legal Sciences (PhD), Associate Professor, Department of Social Sciences, Cyber University State University, Tashkent, Republic of Uzbekistan.
3. **Editorial Board Member Kaharova Munira Maxamajanovna** — Doctor of Political Sciences (DSc), Researcher, Institute of Criminology of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
4. **Editorial Board Member Yuldashev Mutalib Ibrohimovich** — Doctor of Economic Sciences, Professor, Department of Economics, Tashkent University of Science and Technology, Tashkent, Republic of Uzbekistan.
5. **Editorial Board Member Bafaev Shukhrat Gafurovich** — Doctor of Legal Sciences, Head of the Tashkent City Branch, Center for the Analysis of Democratic Processes, Tashkent, Republic of Uzbekistan.
6. **Editorial Board Member Khodjaeva Aziza Bakhtiyarovna** — Doctor of Philosophy in Legal Sciences (PhD), “Academy of Labor and Social Relations” under the Federation of Trade Unions of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
7. **Editorial Board Member Khudoyberdieva Viloyat Jabbrovanovna** — Candidate of Legal Sciences (PhD), Olmazor District Department of Public Education, Tashkent City, Republic of Uzbekistan.
8. **Editorial Board Member Boboumarova Munira Kurbonovna** — Doctor of Philosophy in Legal Sciences (PhD), Department for Organization of Investigative Activities, Investigation Division, Tashkent City Internal Affairs Department, Tashkent, Republic of Uzbekistan.
9. **Editorial Board Member Usmonov Vosid Muhammadievich** — Doctor of Philosophy in Legal Sciences (PhD), Diplomatic University, Tashkent, Republic of Uzbekistan.
10. **Editorial Board Member Mirzayeva Malika Baxadirovna** — Doctoral Researcher, PhD, Associate Professor, Department of Digital Technologies and Artificial Intelligence, Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
11. **Editorial Board Member Allayorov Tulqin Ruziqulovich** — Doctor of Philosophy in Philology (PhD), Associate Professor, Nizami Named Tashkent State Pedagogical University, Tashkent, Republic of Uzbekistan.
12. **Editorial Board Member Tosheva Maftuna Anvar kizi** — Doctor of Philosophy in Legal Sciences (PhD), Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
13. **Editorial Board Member Askarov Jaloliddin Toychievich** — Doctor of Philosophy in Legal Sciences (PhD), Deputy Head, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
14. **Editorial Board Member Abdixakimov Islombek Bahodir o'g'li** — Master of Law (LL.M), Head of the Artificial Intelligence and Legal Tech Laboratory, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
15. **Editorial Board Member Kalandarov Aminjon Amondullayevich** — Doctor of Philosophy in Legal Sciences (PhD), Acting Associate Professor, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
16. **Editorial Board Member Hakimov Komil Bakhtiyarovich** — Doctor of Legal Sciences (DSc), Professor, Head of the Department of Criminal Law, Criminology and Anti-Corruption, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.

CURRENT ISSUES OF LEGAL SUPPORT FOR CYBERSECURITY IN THE REPUBLIC OF UZBEKISTAN AND PROSPECTS FOR ITS IMPROVEMENT

Azizbek Baxodirov

1st year student of "Cyber University" State University

Sherzod Khamraevich Samarov

Cyber University State University

Methodologist of the Faculty of Law and Business

ARTICLE INFO

Keywords:

cybersecurity,
digital law,
critical information
infrastructure,
cyber incident,
personal data,
artificial intelligence,
legal regulation,
NIS2,
cybercrime,
information security audit.

ABSTRACT

This article examines the current state of the legal framework for cybersecurity in the Republic of Uzbekistan from constitutional, information-law, criminal-law, and comparative-law perspectives. The rapid digitalization of public administration, finance, education, healthcare, and entrepreneurship has increased dependence on information systems while also intensifying the risks posed by phishing, malware, distributed denial-of-service (DDoS) attacks, personal data breaches, and artificial intelligence-assisted manipulation. The study analyzes the Constitution of the Republic of Uzbekistan, Law No. ZRU-764 "On Cybersecurity," Law No. ZRU-547 "On Personal Data," relevant information legislation, the Budapest Convention model, the NIS2 Directive, international standards, and academic literature. The findings demonstrate that Uzbekistan has established the principal institutional and legal foundations of cybersecurity. However, risk-based incident reporting, public-private cooperation, liability for cross-border incidents, AI-assisted cyberattacks, independent auditing, the rights of persons affected by data breaches, and compensation mechanisms remain insufficiently defined. Accordingly, the article proposes a five-stage legal mechanism integrating identification, prevention, monitoring, response, and accountability.

O'ZBEKISTON RESPUBLIKASIDA KIBERXAVFSIZLIKNI HUQUQIY TA'MINLASHNING DOLZARB MASALALARI VA UNI TAKOMILLASHTIRISH ISTIQBOLLARI

MAQOLA MA'LUMOTI

Kalit so'zlar:

kiberxavfsizlik,
raqamli huquq,
muhim axborot infratuzilmasi,
kiberhodisa,
shaxsga doir ma'lumotlar,
sun'iy intellekt,
huquqiy tartibga solish,
kiberjinoyat,
axborot xavfsizligi auditi.

ANNOTATSIYA

Mazkur maqolada O'zbekiston Respublikasida kiberxavfsizlikni huquqiy ta'minlashning zamonaviy holati konstitutsiyaviy, axborot-huquqiy, jinoyat-huquqiy va qiyosiy-huquqiy jihatdan tadqiq etiladi. Davlat boshqaruvi, moliya, ta'lim, sog'liqni saqlash va tadbirkorlikning jadal raqamlashtirilishi axborot tizimlariga bog'liqlikni kuchaytirish bilan birga fishing, zararli dasturlar, DDoS hujumlari, shaxsga doir ma'lumotlarning buzilishi va sun'iy intellekt yordamidagi manipulyatsiyalar xavfini oshirmoqda. Tadqiqotda O'zbekiston Respublikasi Konstitutsiyasi, "Kiberxavfsizlik to'g'risida"gi O'RQ-764-sonli Qonun, "Shaxsga doir ma'lumotlar to'g'risida"gi O'RQ-547-sonli Qonun, tegishli axborot qonunchiligi, Budapesht konvensiyasi modeli, NIS2 direktivasi, xalqaro standartlar va ilmiy adabiyotlar tahlil qilindi. Natijalar O'zbekistonda kiberxavfsizlikning asosiy institutsional-huquqiy poydevori yaratilganini, biroq hodisalar haqida tavakkalchilikka asoslangan xabar berish, davlat va xususiy sektor hamkorligi, transchegaraviy hodisalarda javobgarlik, sun'iy intellekt yordamidagi hujumlar, mustaqil audit, ma'lumotlar buzilishidan zarar ko'rgan shaxslarning huquqlari hamda kompensatsiya mexanizmlari yetarlicha aniqlashtirilmaganini ko'rsatadi. Shu asosda aniqlash, oldini olish, kuzatish, javob qaytarish va javobgarlik bosqichlarini birlashtiruvchi besh bosqichli huquqiy mexanizm taklif etiladi.

АКТУАЛЬНЫЕ ВОПРОСЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ УЗБЕКИСТАН И ПЕРСПЕКТИВЫ ЕЕ СОВЕРШЕНСТВОВАНИЯ

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:

кибербезопасность,
цифровое право,
критическая
информационная
инфраструктура,
киберинцидент,

АННОТАЦИЯ

В статье исследуется современное состояние правового обеспечения кибербезопасности в Республике Узбекистан с конституционно-правовой, информационно-правовой, уголовно-правовой и сравнительно-правовой точек зрения. Стремительная цифровизация государственного управления, финансов, образования, здравоохранения и предпринимательства усилила зависимость от информационных

*персональные данные,
искусственный интеллект,
правовое регулирование,
киберпреступность,
аудит информационной
безопасности.*

систем и одновременно повысила риски фишинга, вредоносного программного обеспечения, DDoS-атак, утечек персональных данных и манипуляций с применением искусственного интеллекта. Анализ охватывает Конституцию Республики Узбекистан, Закон № ЗРУ-764 «О кибербезопасности», Закон № ЗРУ-547 «О персональных данных», смежное информационное законодательство, модель Будапештской конвенции, Директиву NIS2, международные стандарты и научную литературу. Установлено, что в Узбекистане сформированы базовые институциональные и правовые основы кибербезопасности, однако требуют дальнейшего развития правила уведомления об инцидентах, государственно-частного взаимодействия, трансграничной ответственности, противодействия атакам с применением искусственного интеллекта, независимого аудита и защиты прав пострадавших лиц. Предлагается пятиэтапный правовой механизм, охватывающий выявление, предупреждение, обнаружение, реагирование и ответственность.

INTRODUCTION

The digital transformation of state institutions and private economic activity has made cybersecurity a prerequisite for the continuity of contemporary society. Electronic public services, remote banking, cloud platforms, digital education, health-information systems and online commerce create substantial efficiency gains, but they also expand the attack surface and increase the potential consequences of information-system failure. Cybersecurity can therefore no longer be understood solely as a technical function performed by information-technology departments. It is a legal condition for national security, economic stability, public-service continuity and the effective exercise of constitutional rights.

Cyber incidents may affect the confidentiality, integrity and availability of data, interrupt essential services and expose individuals to financial, reputational and psychological harm. Phishing, malicious software, ransomware, distributed denial-of-service attacks and social engineering remain persistent threats. Artificial intelligence intensifies the problem by facilitating scalable spear-phishing, synthetic identities, deepfakes, automated vulnerability discovery and rapid adaptation of malicious code. These developments challenge legal regimes designed around identifiable actors, territorially bounded conduct and comparatively stable technological risks.

Uzbekistan has responded by adopting Law No. ZRU-764 of 15 April 2022 “On Cybersecurity,” which regulates relations in the field and defines cyber threats, cyber

incidents, cyberattacks, cyber protection, cybersecurity entities and critical information infrastructure [1]. The Law identifies critical infrastructure across public administration, defence, energy, water, healthcare, banking, transport, information and communication technologies, environmental protection and other strategically important sectors. It thereby provides a common statutory vocabulary and institutional basis for prevention, detection and response.

The cybersecurity framework is complemented by Law No. ZRU-547 “On Personal Data,” general information legislation, criminal and administrative liability rules, electronic-government legislation and sector-specific requirements [2–5]. The Constitution provides the broader rights-based foundation through guarantees relating to privacy, personal data, access to information and judicial protection [3]. Taken together, these instruments demonstrate that cybersecurity regulation operates at the intersection of public security and individual rights.

International developments show a transition from general information-security duties toward risk-based governance and mandatory incident accountability. Directive (EU) 2022/2555 (NIS2) extends cybersecurity risk-management and notification obligations across essential and important entities [6]. The Budapest Convention provides a widely used model for substantive cybercrime offences, procedural powers and international cooperation [7]. ISO/IEC 27001:2022 and OECD guidance emphasize systematic risk management, governance responsibility and continual improvement [8, 9].

Uzbekistan’s position in the second tier of the International Telecommunication Union’s Global Cybersecurity Index 2024 indicates meaningful institutional development while also underscoring the need for continued improvement across legal, technical, organizational, capacity-development and cooperation pillars [10]. Formal adoption of legislation is therefore only one part of effective cybersecurity governance; implementation capacity, institutional coordination, professional skills and enforceable remedies remain equally important.

The purpose of this study is to evaluate whether the current legal framework adequately addresses emerging cybersecurity risks and to develop proposals for its systematic improvement. The research focuses on five questions: the coherence of national legislation; duties applicable to critical infrastructure; incident notification and information sharing; protection of individuals and personal data; and the regulation of transboundary and AI-enabled threats.

METHODOLOGY

The study employs formal legal, systematic legal, comparative legal and analytical methods. The formal legal method was used to interpret the Constitution, Law “On Cybersecurity,” Law “On Personal Data,” information legislation and relevant liability provisions. Particular attention was paid to the statutory concepts of cyber threat, cyber incident, cyberattack, cyber protection, cybersecurity entity and critical information infrastructure because these definitions determine the scope of duties and institutional competence.

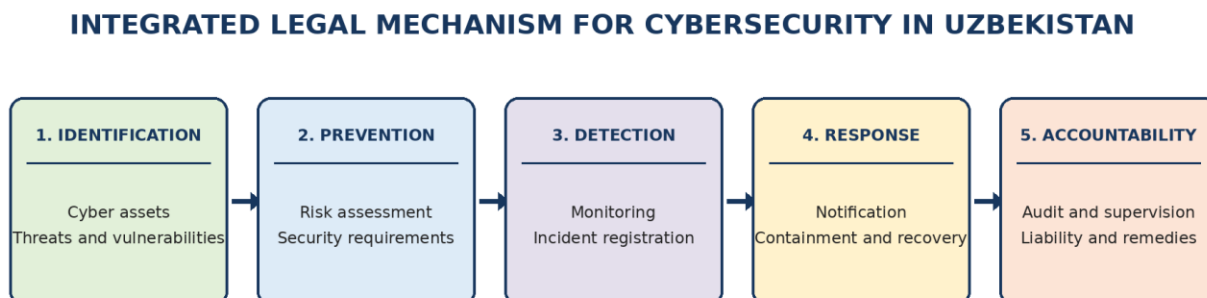
The systematic method was applied to examine cybersecurity regulation as an interconnected framework rather than as a single legislative act. This framework includes prevention, security standards, monitoring, incident registration, public–private coordination, personal-data protection, criminal investigation, administrative supervision, recovery, judicial protection and compensation. The method revealed points at which legal duties are dispersed across separate instruments or are not supported by detailed procedural rules.

Comparative legal analysis examined Directive (EU) 2022/2555, the Budapest Convention framework, ISO/IEC 27001:2022, OECD digital-security risk-management principles and the ITU Global Cybersecurity Index. These sources were selected because they represent complementary regulatory dimensions: organizational risk governance, cybercrime cooperation, management standards, public policy and national capacity assessment.

The analytical stage organized the identified issues according to the lifecycle of a cyber incident: identification of assets and risks; preventive controls; monitoring and detection; notification and coordinated response; and accountability, recovery and remedies. The study does not provide a quantitative count of cyber incidents or calculate the causal effectiveness of individual legal rules. Its conclusions are normative and comparative and should be understood as proposals for legislative and institutional development.

Source selection prioritized official legislation, intergovernmental instruments, standards and peer-reviewed scholarship. Current statutory titles and adoption details were verified against the National Database of Legislation. The analysis distinguishes between rules presently contained in Uzbek legislation and international mechanisms proposed as comparative models; the latter are not presented as automatically binding domestic law.

Figure 1. Integrated legal mechanism for cybersecurity in Uzbekistan



Legality, proportionality, data protection, continuity and human oversight must be ensured at every stage.

Source: Developed by the author on the basis of Law No. ZRU-764 “On Cybersecurity,” Law No. ZRU-547 “On Personal Data,” the NIS2 Directive, the Budapest Convention framework and ISO/IEC 27001:2022 [1, 2, 6–8].

RESULTS

The analysis confirms that Uzbekistan has moved from fragmented information-protection rules toward a dedicated cybersecurity framework. Law No. ZRU-764 establishes core terminology, policy principles, public authority competences, cybersecurity rights and duties, and a legal regime for critical information infrastructure. This is a significant institutional achievement because it creates a common legal basis across sectors whose operational disruption may affect national security and public welfare.

At the same time, several issues require more detailed procedural regulation. A general duty to ensure cybersecurity does not by itself answer when an incident must be reported, which facts must be included, how severity should be assessed, how confidential commercial information should be protected during information exchange, or when affected individuals must be notified. Legal certainty requires these obligations to be differentiated according to risk, sector, scale and potential harm.

The comparison with NIS2 demonstrates the value of management accountability, supply-chain risk controls, proportional security measures and staged incident notification. The Budapest Convention framework additionally illustrates the need for procedural capacity and rapid international cooperation when electronic evidence, offenders and victims are located in different jurisdictions. ISO/IEC 27001:2022 supports an auditable cycle of risk assessment, control implementation, monitoring and continual improvement.

Table 1. Principal cybersecurity legal challenges and directions for improvement

Legal issue	Current regulatory basis in Uzbekistan	Identified gap	Recommended improvement
Critical information infrastructure	Law No. ZRU-764 defines relevant entities and sectors	Audit frequency and risk differentiation require greater procedural detail	Risk-based mandatory audits and sector-specific minimum controls
Cyber-incident notification	Cybersecurity entities have prevention and response duties	Uniform thresholds, content and deadlines are insufficiently differentiated	Staged notification based on severity and potential harm
Personal-data breaches	Law No. ZRU-547 governs processing and protection of personal data	Notification, compensation and effective remedies require strengthening	Mandatory notice to authority and affected persons; compensatory remedies
Public-private information sharing	General cooperation and authority competences	Uncertainty regarding confidentiality, use limitation and liability	Protected information-sharing channels and statutory safe-use rules
AI-enabled cyber threats	Covered indirectly by general cybersecurity and liability rules	No tailored duties concerning deepfakes, automated attacks and model misuse	Technology-neutral AI threat rules, provenance controls and human oversight
Cross-border cybercrime	Criminal and procedural legislation; international cooperation mechanisms	Speed of evidence preservation and jurisdictional coordination	Specialized contact mechanisms and expedited preservation procedures

Source: Compiled by the author from the Constitution and Laws of the Republic of Uzbekistan, Directive (EU) 2022/2555, the Budapest Convention framework and international cybersecurity standards [1–10].

The findings demonstrate that regulatory fragmentation is not simply a drafting problem. It can produce uncertainty over institutional responsibility, inconsistent compliance costs, delayed notification and unequal protection for individuals affected by comparable

incidents. The legal framework should therefore connect substantive security duties with procedural requirements, supervisory powers, evidence standards, liability rules and accessible remedies.

The protection of personal data is particularly important because many cyber incidents simultaneously constitute confidentiality breaches and violations of individual rights. A rights-based cybersecurity model should specify when an operator must notify the competent authority and affected persons, preserve evidence, mitigate harm and provide information about available remedies. Security secrecy should not be used to exclude individuals from information necessary to protect their interests.

The proposed five-stage mechanism in Figure 1 treats cybersecurity as a continuous legal process. Identification determines protected assets and risks; prevention translates risk into proportionate controls; detection requires monitoring and reliable incident registration; response covers notification, containment, coordination and recovery; accountability includes audit, supervision, liability, judicial protection and compensation. A failure at any stage weakens the entire chain.

DISCUSSION

Cybersecurity as a legal institution. The findings support the view that cybersecurity is not reducible to technical protection. It organizes legal relations among the state, critical-infrastructure operators, service providers, employees, users and individuals whose information is processed. It also mediates potentially competing interests: national security, business continuity, privacy, freedom of information, confidentiality and due process.

Risk-based regulation. Uniform obligations may overburden smaller entities while failing to impose adequate safeguards on high-impact operators. A risk-based approach should consider sector, systemic importance, volume and sensitivity of data, dependency relationships, likelihood of disruption and potential harm. Minimum duties should remain universal, while enhanced obligations should apply to critical and important entities.

Critical infrastructure and audit. The statutory identification of critical information infrastructure is a major strength of Uzbek law [1]. However, legal effectiveness depends on objective classification, periodic reassessment and independent verification. Mandatory audits should be proportionate, based on accredited methodologies and connected to enforceable remediation plans rather than treated as formal compliance exercises.

Incident notification. Rapid notification improves situational awareness and allows

coordinated containment, but premature reporting may be incomplete. A staged model can balance these concerns: an early warning after awareness of a significant incident, a more detailed incident notification after preliminary assessment and a final report describing causes, impact and corrective measures. Clear thresholds are necessary to avoid both under-reporting and excessive low-value reporting.

Personal data and individual remedies. Cybersecurity regulation is often institution-centred, whereas data-protection law is rights-centred. Effective reform should integrate these perspectives. Persons affected by a significant breach should receive intelligible information about the nature of the event, likely consequences, mitigation measures and complaint or compensation mechanisms, subject to narrowly tailored security exceptions.

Artificial intelligence. AI-enabled attacks challenge attribution and scalability but do not require an entirely separate legal system. Technology-neutral duties of reasonable security, traceability, authenticity and accountability can be supplemented by targeted rules for synthetic media, automated social engineering, high-risk model access, provenance indicators and human review. Liability should depend on conduct, control, foreseeability and failure to take proportionate safeguards rather than on the mere use of AI.

Public-private cooperation. The state cannot independently observe all threats affecting privately operated networks. Conversely, compulsory information sharing without confidentiality guarantees may discourage candid reporting or expose commercial secrets. Legislation should specify permitted purposes, access controls, retention periods, onward disclosure restrictions and protection against use of shared information for unrelated objectives.

Cross-border enforcement. Cyber incidents frequently involve foreign infrastructure, providers and evidence. Effective investigation requires rapid preservation of volatile data, specialized contact points, lawful cross-border cooperation and safeguards protecting privacy and procedural rights. The Budapest Convention framework offers a useful comparative architecture for harmonizing offences and procedural cooperation [7].

Institutional capacity. Legal rules cannot be implemented without trained personnel, technical expertise and institutional coordination. Cyber-law education should be expanded in universities and professional training. Judges, prosecutors, investigators, regulators and compliance officers require specialized knowledge of electronic evidence, incident response, cloud systems, artificial intelligence and cross-border cooperation.

CONCLUSION

The research demonstrates that Uzbekistan has established a substantial legal foundation for cybersecurity through the Constitution, Law “On Cybersecurity,” personal-data legislation, information law and related liability mechanisms. The adoption of a dedicated cybersecurity law and the recognition of critical information infrastructure represent essential steps toward protecting state, societal and economic interests in the digital environment.

Nevertheless, contemporary risks require the transition from general statutory duties to a more detailed and risk-based procedural framework. Priority areas include staged incident notification, proportionate minimum security measures, mandatory audits for critical infrastructure, secure public-private information sharing, supply-chain governance, personal-data breach remedies, regulation of AI-enabled threats and expedited cross-border cooperation.

The five-stage model proposed in the article connects identification, prevention, detection, response and accountability. Its purpose is to ensure that cybersecurity obligations operate as a continuous legal chain rather than as isolated technical requirements. Each stage should be governed by legality, proportionality, data minimization, confidentiality, service continuity, evidence preservation, human oversight and access to effective remedies.

Accordingly, the long-term effectiveness of Uzbekistan’s cybersecurity system will depend not only on the adoption of new norms but also on consistent enforcement, qualified personnel, independent compliance assessment, institutional trust and measurable implementation. Cybersecurity legislation should preserve the capacity of the state and operators to respond rapidly while simultaneously protecting constitutional rights and the rule of law.

REFERENCES

1. Republic of Uzbekistan. (2022). Law No. ZRU-764 “On Cybersecurity” (15 April 2022). <https://lex.uz/docs/5960604>
2. Republic of Uzbekistan. (2019). Law No. ZRU-547 “On Personal Data” (2 July 2019). <https://lex.uz/docs/4396419>
3. Constitution of the Republic of Uzbekistan. (2023). <https://lex.uz/docs/6445145>
4. Republic of Uzbekistan. (2003). Law “On Informatization.” National Database of Legislation.
5. Republic of Uzbekistan. Criminal Code and Code of Administrative Liability: provisions concerning unlawful access, interference with information systems and violations of personal-data requirements.
6. European Parliament and Council. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
7. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention), ETS No. 185. <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
8. International Organization for Standardization. (2022). ISO/IEC 27001:2022—Information security management systems—Requirements.
9. OECD. (2015). Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0415>
10. International Telecommunication Union. (2024). Global Cybersecurity Index 2024. <https://www.itu.int/epublications/publication/global-cybersecurity-index-2024>
11. European Union Agency for Cybersecurity. (2024). ENISA Threat Landscape 2024. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
12. Kshetri, N. (2021). Cybersecurity Management: An Organizational and Strategic Approach. University of Toronto Press.
13. Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. Praeger.
14. Lessig, L. (2006). Code: Version 2.0. Basic Books.
15. Solove, D. J., & Schwartz, P. M. (2021). Information Privacy Law (7th ed.). Wolters Kluwer.
16. OECD. (2024). OECD Digital Economy Outlook 2024. OECD Publishing.
17. United Nations Office on Drugs and Crime. (2013). Comprehensive Study on Cybercrime. United Nations.
18. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. <https://doi.org/10.6028/NIST.CSWP.29>