The American Journal of Political Science Law and Criminology
ISSN 2693-0803 Volume 08 - 2026

Legal Policy of Uzbekistan On Countering Cybercrime: Current Challenges and Strategic Priorities

Abdulaziz K. Rasulev
Academic Secretary, Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan, Doctor of Legal Sciences, Professor, Uzbekistan

Sayfillo N. Ramazanov
Judge of the Criminal Court of Jizzakh, Uzbekistan

Received: 28 Feb 2026 | Received Revised Version: 16 Mar 2026 | Accepted: 04 Apr 2026 | Published: 30 Apr 2026

Volume 08 Issue 04 2026 | Crossref DOI: 10.37547/tajpslc/Volume08Issue04-19

Abstract

This article examines the legal policy of the Republic of Uzbekistan on countering cybercrime as of 9 September 2026. The aim of the study is to assess whether criminal law, criminal procedure, institutional coordination and financial regulation form a coherent cycle of crime prevention, interruption of suspicious transactions, preservation of electronic evidence, investigation and compensation for harm. Applying doctrinal and systemic-structural methods, the study analyses legislation on cybersecurity, personal data, payment systems and digital evidence, presidential acts adopted in 2023–2026 and relevant international standards. It is established that the national model has moved beyond a predominantly technical model of information-system protection towards an interagency framework for preventing cybercrime. At the same time, risks persist in the form of overlapping mandates, fragmented rulemaking, insufficiently regulated expedited preservation of electronic data, uncertainty as to the conditions of liability of digital intermediaries, and incomplete safeguards for individual rights where technologically intrusive measures are applied. The article substantiates proposals for a coordinated legislative package, procedural mechanisms for the rapid preservation of data and the temporary suspension of transactions, differentiated liability for intermediaries and money mules, victim-centred remedies, measurable performance indicators and the alignment of national law with the United Nations Convention against Cybercrime.

Keywords: Cybercrime; cybersecurity; legal policy; digital evidence; digital forensics; financial fraud; money mules; digital intermediaries; victim protection; international cooperation.

Cite This Article: Abdulaziz K. Rasulev, & Sayfillo N. Ramazanov. (2026). Legal Policy of Uzbekistan On Countering Cybercrime: Current Challenges and Strategic Priorities. The American Journal of Political Science Law and Criminology, 8(04), 108–115. https://doi.org/10.37547/tajpslc/Volume08Issue04-19

1. Introduction

Digitalisation is transforming not only the ways in which services are delivered but also the structure of criminal opportunity. An information system may be the direct object of an attack, or it may serve as the means of committing fraud, extortion, the unlawful trafficking of personal data or the laundering of stolen funds. Legal policy on countering cybercrime therefore cannot be reduced to the protection of computer networks. It encompasses criminal-law classification, the procedural handling of electronic data, operational-investigative measures, financial monitoring, the obligations of digital

intermediaries, victim protection and international cooperation [19; 20].

For Uzbekistan, the problem has acquired a systemic character. An official statement of 12 March 2026 reported that the number of internet users in the country had exceeded 31 million and that 14 million people were active users of social networks. According to the same source, over six years the number of reports concerning cybercrime increased forty-eight-fold; in 2025, 82 per cent of frauds and 76 per cent of thefts were committed in cyberspace, while material damage to natural and legal persons exceeded 2 trillion soums [13]. These indicators describe the scale of the registered problem, but they do not in themselves explain the causes of its growth: the trend is shaped by the spread of digital services, changes in recording and registration practice, the accessibility of reporting channels and a genuine increase in the number of offences.

The aim of the article is to determine whether the norms and institutions currently in force constitute a coherent system for countering cybercrime. The research question is formulated as follows: which legal mechanisms are required in order to connect the technical detection of an incident with the rapid prevention of harm, the procedurally admissible fixing of evidence, investigation and the restoration of the victim's rights? The working hypothesis is that the acts adopted in 2023–2026 have created the foundation of such a system, but that its effectiveness depends on eliminating overlapping powers and on the procedural regulation of the actions performed in the first hours after an attack or fraudulent transaction is detected.

2. Methodology and Limitations of the Study

The study is based on the doctrinal analysis of legal norms, a systemic-structural comparison of the powers of state bodies and a functional analysis of the complete response cycle. International instruments are used as a benchmark for assessing the tools of electronic data preservation, cross-border cooperation and legal safeguards, rather than as grounds for the mechanical transplantation of foreign solutions. Normative acts and information concerning their status were verified against official or state resources as of 9 September 2026.

The empirical basis is confined to published official statements. Primary anonymised datasets of criminal statistics, data on the movement of cases, asset recovery and the outcomes of appeals against blocking decisions were not available in the public domain for the purposes of this study. The article therefore does not establish a causal link between any individual reform and changes in the level of crime, nor does it evaluate the performance of any particular authority. Official indicators are used to describe the scale and structure of the problem, with mandatory reference to the source and the reporting period.

3. The Formation of the National Model for Countering Cybercrime

3.1. The Basic Legal Framework

The contemporary legal framework comprises several interconnected components. Constitutional guarantees of private life, the confidentiality of correspondence and judicial protection define the limits of state interference [1]. The Law "On Cybersecurity" establishes the principles and organisational foundations for the protection of information systems and critical information infrastructure [2]. The Laws "On Personal Data" and "On Informatisation" regulate the handling of information and the obligations of its owners and operators [3; 4]. Legislation on payments, payment systems and electronic commerce extends security requirements to financial and commercial digital services [5; 6].

The Criminal Code contains a dedicated chapter on offences in the sphere of information technologies and at the same time permits the application of general corpora delicti where digital technology serves as the means of committing the act [7]. This combination of special and general norms corresponds in principle to the distinction between cyber-dependent crimes, which can be committed only against computer systems or data, and crimes whose scale or modus operandi has been transformed by the digital environment [19; 20]. It follows that the improvement of criminal law should not entail the creation of a separate offence for every new technology. The legislator must identify the specific gap, preserve the technological neutrality of the wording and exclude competition between norms.

3.2. Institutional and Procedural Development

Presidential Resolution No. PP-381 of 30 November 2023 linked the protection of consumers of digital products with the prevention of offences, the use of anti-fraud mechanisms and the improvement of work with electronic evidence [9]. Resolution No. PP-229 of 21 June 2024 assigned research and practical tasks in the

field of digital forensics to the Law Enforcement Academy, including the search for, seizure, storage and examination of digital traces, as well as the application of big-data analysis, artificial intelligence and blockchain analytics [10].

Law No. ZRU-1003 of 21 November 2024 marked an important procedural milestone. It introduced the concepts of electronic data and digital evidence into criminal, civil, economic and administrative proceedings, regulated their submission, inspection, examination, storage and evaluation, and enshrined the requirement to preserve the integrity and identity of copies [8]. The characterisation of national law as failing to recognise digital evidence therefore no longer corresponds to the regulation in force. The present task is the practical elaboration of procedures and the uniformity of their application.

Resolution No. PP-153 of 30 April 2025 designated the Ministry of Internal Affairs as the authorised body for introducing uniform practice in combating cybercrime and for coordinating the responsible agencies. The same act mandated the preparation of a draft law on combating offences committed through the use of information technologies and endorsed proposals concerning the liability of money mules and compensation for damage at the expense of financial institutions where a causal link exists between the damage and their failure to comply with security requirements [11]. These provisions are significant in that they shift part of the emphasis from subsequent investigation towards the prevention of harm and the allocation of duties among the participants of the digital ecosystem.

Decree No. UP-38 of 10 March 2026 approved the Cybersecurity Strategy for 2026–2030, provided for a National Coordination Council, the development of central and sectoral monitoring and response centres, regulations governing interaction with entities operating critical information infrastructure, and an information system for the prompt interaction of state bodies, law enforcement agencies, banks and telecommunications operators [12]. In January 2026, the creation of a dedicated cybercrime department within the Ministry of Internal Affairs and of a cybercrime and digital law unit within the Ministry of Justice was also announced [14]. In the financial sector, the CERT-CBU Cybersecurity Centre is operational, and since 2025 minimum information security and cybersecurity requirements have been established for commercial banks [15; 16].

The national model thus encompasses technical, law enforcement, financial, research and coordination levels. Its strength lies in the recognition that the outcome depends not on a single agency but on the speed of interaction along the entire chain. At the same time, an increase in the number of institutions does not in itself guarantee coherence: clear grounds for the transfer of data, time standards for response and rules for resolving conflicts of competence are required.

4. Systemic Problems of Legal Regulation

4.1. Distinguishing Cybersecurity from Countering Cybercrime

Cybersecurity and countering cybercrime overlap, yet they pursue different immediate objectives. The former is directed at the resilience and protection of systems and at the prevention and elimination of incidents. The latter presupposes establishing the elements of an offence, protecting the victim, gathering evidence and applying measures of liability. The same set of facts may begin as a technical incident and subsequently acquire a criminal-law classification. The law must define the moment and the procedure of such a transition, without turning every vulnerability into the subject of criminal proceedings and without permitting the loss of evidence before an investigation commences.

The delimitation of functions is particularly important given the simultaneous involvement of the State Security Service as the authorised body in the field of cybersecurity, the Ministry of Internal Affairs as the coordinator of practice in combating cybercrime, the National Coordination Council and sectoral regulators [2; 11; 12]. For each type of event, a normative matrix of responsibility is required: who confirms the incident, who issues the mandatory notification, who initiates a temporary restriction on a transaction, who ensures the preservation of event logs, who takes the procedural decision and who informs the victim.

4.2. Fragmentation of Norms and the Risk of Over-Criminalisation

Norms relating to digital crime are distributed across criminal and procedural legislation, the laws on cybersecurity, personal data, communications, payments and electronic commerce, and the subordinate requirements of regulators. Such dispersal is inevitable, since the subject matter of regulation differs in each case. It becomes a problem when identical concepts are defined differently, when the time limits for the storage

and transfer of data are not aligned, and when the obligation of one entity is not matched by a corresponding power of another.

The proposed liability of holders of bank accounts, SIM cards, electronic wallets and online accounts must rest upon proven fault. Criminal liability requires the establishment of intent or of another clearly defined form of culpable attitude towards facilitating the offence. The negligent handling of credentials and the deliberate provision of infrastructure to a criminal group differ in their degree of public danger. The norm must also protect persons who have themselves become victims of deception, coercion, SIM-swap fraud or account takeover. Otherwise, efforts against money muling will create the risk of prosecuting the victim instead of the organiser of the scheme.

Deepfakes, malicious applications, crypto-assets and novel forms of social engineering should be addressed primarily as methods of committing and of proving an offence. A new standalone corpus delicti is warranted only where there exists a distinct protected interest and a gap that cannot be closed through interpretation or through an aggravating element. Such an approach enhances the resilience of the law to technological change and observes the principle of legal certainty.

4.3. Timeliness and Admissibility of Digital Evidence

Law No. ZRU-1003 established a general procedural foundation; the digital environment, however, demands procedures designed for the volatility of data. Event logs may be overwritten, cloud data may be held by a foreign provider, and funds may pass through a chain of accounts and crypto addresses. Between the reporting of an incident and the obtaining of evidence there must therefore exist a legally defined regime of expedited data preservation, which is not conflated with final seizure or with access to the content of communications.

Such a regime should comprise the grounds for and the duration of mandatory preservation, the range of authorised officials, the identification of the dataset, protection against alteration, documentation of the chain of custody, subsequent judicial or prosecutorial authorisation in the cases prescribed by law, and the procedure for lifting the measure. Methodological standards should provide for the creation of verifiable copies, the use of control hash values, the use of write-blocking devices and the full logging of the specialist's actions. International materials treat authenticity, integrity and a reproducible chain of data handling as the central conditions of the reliability of electronic evidence [18; 19].

Procedural efficiency must not diminish the guarantees of the defence. The defence must have a genuine opportunity to verify the origin, completeness and extraction methods of the data, to challenge the opinion of a specialist or expert, and to obtain access to the materials on which the conclusion of the prosecution is based, subject to lawful restrictions. In the case of automated analytics and artificial intelligence tools, it is necessary to record the version of the software, the input data, the processing parameters and the extent of human involvement in taking the procedural decision.

4.4. Liability of Digital Intermediaries and Compensation for Harm

Banks, payment organisations, telecommunications operators, marketplaces, cloud providers and digital platforms possess different capacities to prevent crime. They cannot be subsumed under a single formula without regard to their control over the specific risk. The legal obligation must correspond to the function of the intermediary: a bank is able to halt a transfer and conduct enhanced verification; a telecommunications operator is able to detect an anomalous SIM-card replacement; a platform is able to restrict a phishing account; a cloud provider is able to preserve specified data upon a lawful request.

Compensation for harm at the expense of a financial institution, envisaged by the direction of reform adopted in 2025, requires a clear legal construction [11]. The law must define the standard of due security, causation, the allocation of the burden of proof, the time limits for the consideration of claims, the limits of liability and an independent appeal procedure. Automatic exemption of the intermediary upon formal compliance with internal rules would be insufficient, yet unconditional liability for any instance of fraud would fail to take account of the conduct of other participants. A risk-based approach is better founded, under which the technical and organisational measures, the timeliness of the response, the nature of the breach and the contribution of each participant to the occurrence of the harm are all assessed.

4.5. Protection of Individual Rights

Countering cybercrime entails the processing of large volumes of transactional data, communications metadata, device identifiers, biometric features and the

content of communications. Constitutional guarantees and the principle of legality require that powers of access to such data have a clear basis, a defined purpose and defined limits [1]. Since personal data legislation provides special exemptions for a number of law enforcement processing operations, the requisite safeguards must be expressly enshrined in criminal procedure and operational-investigative regulation rather than merely implied [3].

The minimum set of safeguards includes the necessity and proportionality of the interference, a distinction between access to metadata and access to the content of communications, independent authorisation of the most intrusive measures, the logging of requests, the limitation of retention periods, the destruction of data once the purpose has ceased to exist, departmental and external oversight, and an effective remedy. The automatic blocking of an account must be accompanied by notification, an intelligible statement of grounds and a rapid review procedure, provided that notification does not create an immediate risk to the investigation.

4.6. International Cooperation

The cross-border character of infrastructure renders international cooperation an element of domestic effectiveness. Uzbekistan signed the United Nations Convention against Cybercrime on 25 October 2025 [17]. This creates a practical basis for taking stock of national corpora delicti, procedural powers, mechanisms of legal assistance, personal data protection and victim support. Signature should not be conflated with ratification; as at the date of this study, the depositary information for Uzbekistan records signature alone.

In preparing national procedures, it is also expedient to take into account the accumulated standards of the Budapest Convention as comparative material: the expedited preservation of stored computer data, production orders, search and seizure, the real-time collection of traffic data, round-the-clock points of contact and safeguards for rights [18]. The use of these standards in the present study does not imply any assertion that Uzbekistan is a party to that convention. Rather, it allows the completeness of the national procedural toolkit and its compatibility with prevailing practice in international cooperation to be tested.

5. Priorities for the Improvement of Legal Policy

5.1. A Unified Legislative Architecture

The first priority should be not a new strategic document formally "preceding" the Strategy for 2026–2030 already adopted, but a coordinated package for its legal implementation. Such a package may comprise a framework law on countering offences committed through the use of information technologies, together with concurrent amendments to the Criminal Code, the Criminal Procedure Code, the Code of Administrative Liability and the laws on operational-investigative activity, cybersecurity, personal data, payments and communications. The package approach is needed in order to synchronise concepts, powers, time limits and safeguards, and not in order to place all norms within a single statute.

It is expedient to assign to the framework law the principles of state policy, the categories of participants, coordination, prevention, incident notification, the obligations of intermediaries, victim protection, interagency exchange and international cooperation. Corpora delicti, measures of procedural compulsion and rules of evidence should remain in the respective codes. This will preserve the systemic coherence of sectoral legislation and reduce the risk of duplication.

5.2. A Legal Algorithm for Early Response

The central element of the reform should be a normatively enshrined algorithm: risk detection – notification – temporary interruption of the transaction – preservation of data – procedural decision – recovery of assets or lifting of the restriction – investigation and international cooperation. For each stage, the grounds, the responsible entity, the maximum time limit and a digital log of actions must be established. The technical integration of participants without such a legal model would merely accelerate the transmission of indeterminate requests.

The temporary suspension of a suspicious transaction should be applied on the basis of risk indicators and should be short-term, documented and reviewable. Any extension of the restriction should require a decision of the competent authority. The payee and the payer must have access to a review procedure, and persons acting in good faith must have access to compensation for harm caused by unlawful or excessively prolonged blocking. In parallel, confirmation of payee, enhanced verification of anomalous transactions and an interbank mechanism for tracing chains of transfers should be introduced.

5.3. Digital Forensics and Uniform Standards of

Proof

Digital forensics should be developed as a system of methods and competences linking the technical detection of a trace with the requirements of admissibility and verifiability of evidence. Uniform standards should cover the seizure of devices, imaging, hashing, write-blocking, work with cloud data, mobile applications, blockchains and logs, the documentation of software tools and the independent validation of methodologies. The organisational tasks assigned to the Law Enforcement Academy provide a basis for such harmonisation [10].

A register of validated methodologies and software tools should be maintained, laboratories should be audited on a regular basis, and training should be provided for investigators, prosecutors, judges, defence lawyers and experts. The quality of digital evidence depends not only on laboratory equipment, but also on the extent to which all participants in the proceedings understand the limitations of the method and are able to reproduce the conclusion.

5.4. Coordination and Accountability

It would be expedient to establish, under the auspices of the National Coordination Council, a standing mechanism for the legal and technical expert examination of draft acts. Such a mechanism should verify the compatibility of concepts, eliminate the duplication of powers, assess the impact upon human rights and test interagency procedures prior to their large-scale introduction. Decisions on access to data and on blocking must remain with the bodies expressly authorised by law; the coordinating body must not substitute itself for procedural competence.

Information exchange should be constructed upon the principle of minimum necessary access. The law, or regulations approved on its basis, should define the composition of the data, the purpose of the transfer, the grounds for the request, the recipient, the retention period, the procedure for correcting erroneous information, the logging of operations and liability for unlawful use. This is especially important for consolidated anti-fraud systems, in which an erroneous flag applied by one participant may entail restrictions throughout the entire financial ecosystem.

5.5. Victim Protection and the Allocation of Liability

The legal model should be assessed by its capacity to prevent and to compensate harm, and not solely by the number of cases initiated. The victim requires a single reporting channel, a tracking number, prompt notification of banks and operators, an intelligible explanation of the status of the funds, the ability to challenge a refusal to block funds or to award compensation, and access to psychological and legal assistance in cases of blackmail, sextortion and other forms of digital violence.

The liability of intermediaries should be differentiated according to the risk under their control, and the liability of money mules according to the form of fault and the role played within the scheme. The voluntary and timely reporting of a compromise by the holder of an account or profile may be taken into account as a ground for exemption from administrative liability or for mitigating the consequences, provided that the person did not share in the criminal intent. Such a construction encourages the early disclosure of networks while at the same time preserving the possibility of prosecuting professional intermediaries of criminal infrastructure.

5.6. Performance Indicators

The indicators of the Strategy's implementation should measure outcomes rather than the volume of departmental activity. They include: the proportion of suspicious transactions prevented; the amount and share of assets recovered; the median time from report to suspension of a transaction; the proportion of data preservation requests executed within the prescribed time; clearance rates for homogeneous categories of offence; the duration of investigations; the number of unfounded blocking decisions overturned; the rate of repeat victimisation; compliance with incident notification deadlines; and the results of independent security audits.

The publication of indicators should be accompanied by the calculation methodology, the denominators employed and a clear distinction between registered offences, reports, incidents and prevented transactions. Otherwise, a decline in the number of registered cases may be mistaken for success, and an increase in detection for deterioration. Scholarly and public assessment requires anonymised data enabling analysis by region, modus operandi, payment channel, amount of damage, recovery of funds and procedural outcome, without the disclosure of personal data.

5.7. International Compatibility

In connection with the signing of the United Nations

Convention against Cybercrime, an article-by-article assessment of the conformity of national law should be conducted and an implementation plan prepared [17]. Of particular importance are the point of contact, the expedited preservation of data, legal assistance concerning electronic evidence, confiscation and the return of assets, the protection of personal data, victim support and the conditions governing the transfer of information. Implementation must be accompanied by an assessment of the necessity and proportionality of the new powers and by verification of their compatibility with the Constitution.

6. Conclusion

Between 2023 and 2026, Uzbekistan established the legal and institutional foundation for a transition from fragmented response to an interagency model of countering cybercrime. Its key elements have been the regulation of digital evidence, the development of digital forensics, the definition of the coordinating role of the Ministry of Internal Affairs, the creation of the National Coordination Council, sectoral cybersecurity mechanisms and the Strategy for 2026–2030.

The next stage of the reform requires that these elements be aligned within a single legal cycle. Priority belongs to a clear delimitation of competences, the expedited preservation of electronic data, the procedurally supervised suspension of transactions, differentiated liability for intermediaries and money mules, effective compensation for harm and verifiable safeguards for individual rights. A framework law is capable of ensuring coordination, but criminal liability and procedural powers must be enshrined in the specialised codes.

The effectiveness of legal policy should be measured by the harm prevented, the speed of evidence preservation, the recovery of assets, the quality of investigations and the number of erroneous restrictions corrected. Such an approach connects the security of digital infrastructure with the tasks of criminal justice and the protection of citizens, without substituting one sphere for the other.

References

1. Constitution of the Republic of Uzbekistan, as amended by Constitutional Law No. ZRU-837 of 1 May 2023. Available at: https://lex.uz/ru/docs/6449035 (accessed 9 September 2026).
2. On Cybersecurity: Law of the Republic of Uzbekistan No. ZRU-764 of 15 April 2022. Available at: https://lex.uz/ru/docs/5960604 (accessed 9 September 2026).
3. On Personal Data: Law of the Republic of Uzbekistan No. ZRU-547 of 2 July 2019. Available at: https://lex.uz/ru/docs/4396419 (accessed 9 September 2026).
4. On Informatisation: Law of the Republic of Uzbekistan No. 560-II of 11 December 2003. Available at: https://lex.uz/ru/docs/82956 (accessed 9 September 2026).
5. On Payments and Payment Systems: Law of the Republic of Uzbekistan No. ZRU-578 of 1 November 2019. Available at: https://lex.uz/ru/docs/4575788 (accessed 9 September 2026).
6. On Electronic Commerce: Law of the Republic of Uzbekistan No. ZRU-792 of 29 September 2022. Available at: https://lex.uz/ru/docs/6213428 (accessed 9 September 2026).
7. Criminal Code of the Republic of Uzbekistan, approved by Law No. 2012-XII of 22 September 1994. Available at: https://lex.uz/ru/docs/111457 (accessed 9 September 2026).
8. On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan Aimed at Improving the System of Work with Digital Evidence: Law of the Republic of Uzbekistan No. ZRU-1003 of 21 November 2024. Available at: https://lex.uz/Pages/GetPdf.aspx?file=LexUz_7297768.pdf (accessed 9 September 2026).
9. On Measures to Strengthen the Protection of the Rights of Consumers of Digital Products and Services and to Combat Offences Committed by Means of Digital Technologies: Resolution of the President of the Republic of Uzbekistan No. PP-381 of 30 November 2023. Available at: https://lex.uz/Pages/GetPdf.aspx?file=LexUz_6794972.pdf (accessed 9 September 2026).
10. On Measures to Organise Research Activity in the Field of Digital Forensics: Resolution of the President of the Republic of Uzbekistan No. PP-229 of 21 June 2024. Available at: https://lex.uz/Pages/GetPdf.aspx?file=LexUz_7003037.pdf (accessed 9 September 2026).
11. On Measures Aimed at Further Strengthening Activity to Combat Offences Committed with the Use of Information Technologies: Resolution of the President of the Republic of Uzbekistan No. PP-153 of 30 April 2025. Available at:

https://lex.uz/Pages/GetPdf.aspx?file=LexUz_7641305.pdf (accessed 9 September 2026).

12. On the Determination of the Cybersecurity Strategy of the Republic of Uzbekistan and the Improvement of the Cybercrime Prevention System: Decree of the President of the Republic of Uzbekistan No. UP-38 of 10 March 2026. Text of the document in the NRM.uz information system. Available at: 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_sovershenstvovanii_sistemy_preduprejdeniya_kiberprestupnosti&products=1_vse_zakonodatelstvo_uzbekistana (accessed 9 September 2026).
13. The Fight against Organised Crime and Cybercrime Will Be Intensified. Official website of the President of the Republic of Uzbekistan, 12 March 2026. Available at: https://president.uz/ru/lists/view/9009 (accessed 9 September 2026).
14. The Activity of Law Enforcement Bodies Has Been Critically Reviewed and New Tasks for Ensuring Public Safety Have Been Defined. Official website of the President of the Republic of Uzbekistan, 27 January 2026. Available at: https://president.uz/ru/lists/view/8882 (accessed 9 September 2026).
15. On the CERT-CBU Cybersecurity Centre of the Central Bank of the Republic of Uzbekistan. Available at: https://cbu.uz/ru/cert/about/ (accessed 9 September 2026).
16. Regulation on Minimum Requirements for Information Security and Cybersecurity of Commercial Banks of the Republic of Uzbekistan, registered with the Ministry of Justice on 18 August 2025, No. 3669. Available at: https://nrm.uz/contentf?doc=802068_polojenie_o_minimalnyh_trebovaniyah_k_informacionnoy_bezopasnosti_i_kiberbezopasnosti_kommercheskih_bankov_respubliki_uzbekistan&products=1_vse_zakonodatelstvo_uzbekistana (accessed 9 September 2026).
17. United Nations Convention against Cybercrime: status and depositary information. Available at: https://treaties.un.org/Pages/showDetails.aspx?clang=_en&objid=0800000280670c50 (accessed 9 September 2026).
18. Council of Europe. Convention on Cybercrime and Related Standards. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 9 September 2026).
19. United Nations Office on Drugs and Crime. Comprehensive Study on Cybercrime. Vienna, 2013. Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed 9 September 2026).
20. Clough J. Principles of Cybercrime. 2nd ed. Cambridge: Cambridge University Press, 2015. DOI: 10.1017/CBO9781139540803.