

A. ANORBOYEV

ENSURING THE DEVELOPMENT OF
THE STATE AND SOCIETY IN NEW
UZBEKISTAN: INSTITUTIONAL
REFORMS, LEGAL MECHANISMS
AND DIGITAL TRANSFORMATION



MONOGRAPH

Tashkent - 2026

**Institute of Legislation and Legal Policy
under the President of the Republic of Uzbekistan**

A. ANORBOYEV

**ENSURING THE DEVELOPMENT OF THE STATE AND SOCIETY IN
NEW UZBEKISTAN: INSTITUTIONAL REFORMS, LEGAL
MECHANISMS AND DIGITAL TRANSFORMATION**

MONOGRAPH

Tashkent – 2026

A. Anorboyev. Ensuring the Development of the State and Society in New Uzbekistan: Institutional Reforms, Legal Mechanisms and Digital Transformation. Monograph. – Tashkent: “Dimal” Publishing House, 2026. – 259 p.

Editor-in-Chief:

Doctor of Law (DSc), Professor A. Rasulov

Reviewers:

Doctor of Law (DSc), Professor B. Ismailov, Doctor of Law (DSc) B. Muminov, Doctor of Law (DSc), Associate Professor S. Nurumbetova.

ЎУК	344414
ORCID	https://orcid.org/0009-0003-5355-8753
Publons	QPB-1888-2026
SSRN:	12260788
Index Copernicus	48623
РИИЦ	3827-4098
DOI	10.5281/zenodo.21374052
GOOGLE академия	https://scholar.google.com/citations?user=KIJpct8AAAAJ&hl=ru
ZiyoNet	https://profile.ziynet.uz/uzc
DergiPark	https://dergipark.org.tr/tr/pub/@amiriddin-anorboyev
Academia	https://independent.academia.edu/AnorboyevAmiriddin/Network?tab=suggested
Scopus	https://www.scopus.com/pages/home
Clarivate Analytics	https://apps.clarivate.com/account?app=endnote&tab=personal
КиберЛенинка	https://cyberleninka.ru/me
OpenAIRE	https://www.openaire.eu/f/269/create-new-article
GitHub	https://github.com/explore
Webofscience	QPB-1888-2026

This monograph examines the legal, institutional, and strategic mechanisms for modernizing public administration in New Uzbekistan in the context of digital transformation. The work puts forward long-term comprehensive solutions aimed at administrative and legal reforms, the development of human capital, the productive and efficient use of available resources, support for civil society institutions, ensuring information security, preventing hybrid threats in the media environment, and defining the legal and ethical boundaries of the use of artificial intelligence.

The central focus of the research is the legal and technical qualification of offenses committed through information and communication technologies, particularly cybercrime and cyber-corruption. Specific organizational and technical mechanisms have been developed to strengthen the role of digital forensics in ensuring justice and detecting crimes.

Furthermore, an entirely new methodology, “Cyberalogy,” has been introduced into the academic field, through which modern algorithms are presented for developing advanced research that fully meets the requirements of international scientific databases, including Scopus and Google Scholar. This fundamental work serves as a strategic guide for public administration officials, lawmakers, doctoral researchers specializing in cybersecurity and IT law, and the broader academic community.

This monograph has been published upon the recommendation of the Academic Council of the Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan and is dedicated to the enduring memory of the late distinguished statesman and public figure, Member of the Senate of the Oliy Majlis, Doctor of Law, Professor M. Mirakbar Hajiakbarovich Rakhmonqulov.

CONTENTS

INTRODUCTION.....	6
 CHAPTER I. INSTITUTIONAL FOUNDATIONS OF PUBLIC ADMINISTRATION AND ADMINISTRATIVE REFORMS.....	9
1.1-§. Accounting for Benefits and Preferences and Improving Their Effectiveness.....	9
1.2-§. Improving the Institutions of Rotation and Attestation of Civil Servants.....	16
1.3-§. Improving Procedures for Handling Appeals Based on the Experience of Estonia and Denmark.....	23
 CHAPTER II. IMPROVING CIVIL SOCIETY INSTITUTIONS AND LOCAL GOVERNANCE.....	36
2.1-§. Improving Legislation in the Field of Implementing Socially Significant Projects through the Involvement of Civil Society Institutions and Business Entities.....	36
2.2-§. Establishing a Clear Mechanism for Interaction between Non-Governmental Non-Profit Organizations and Local Executive Authorities and Councils of People's Deputies.....	42
2.3-§. Legal, Organizational and Digital Foundations for Improving the Mahalla Governance System.....	53
 CHAPTER III. DIGITAL TRANSFORMATION OF SOCIETY AND THE STATE AND INFORMATION SECURITY.....	61
3.1-§. The Necessity and Significance of Further Developing a Digital New Uzbekistan.....	61
3.2-§. The Necessity and Procedure for Introducing a Strategic System for Prompt Response to Information in the Media Space that Undermines the National and Public Security of the Republic of Uzbekistan.....	72
3.3-§. The Social Necessity and Organizational and Legal Mechanisms for Restricting Artificial Intelligence Systems in the Republic of Uzbekistan.....	80
3.4-§. Strategic Protection of Children from Information Harmful to Their Health and Ensuring Their Social Protection.....	87
 CHAPTER IV. ENSURING JUSTICE AND COMBATING CYBERCRIME.....	99
4.1-§. Improving the Criminal-Law and Organizational Foundations for Combating Cybercorruption.....	99
4.2-§. Legal Aspects of International Instruments on Combating Cybercrimes, Including Cybercorruption.....	123
4.3-§. Improving the Mediation Institution.....	153
4.4-§. Further Strengthening the Role of Forensic Examination in Detecting Crimes and Cybercrimes Committed through the Use of Information and Communication Technologies.....	164

CHAPTER V. IMPROVING SCIENTIFIC RESEARCH AND THE CYBERALOGY METHODOLOGY.....	196
5.1-§. The Concept of Cyberalogy, Its Content, Essence and Significance.....	196
5.2-§. Methodology for Preparing Information and Analytical Materials, Articles and Theses Based on the Cyberalogy Method and Its Significance for the Development of Science.....	201
CONCLUSION.....	211
LIST OF REFERENCES.....	237

INTRODUCTION

In the current era, characterized by the rapid intensification of globalization processes and a fundamental turning point in political, economic and technological transformations on a global scale, strategically restructuring the system of state and public administration is becoming the highest priority task determining the future of every sovereign country. In this regard, the scientific-practical and fundamental collective monograph entitled “Strategic-Digital Transformation of the State and Society: Problems and Solutions,” presented under the heading “Global Challenges: Problems and Strategic Solutions,” serves as an important guide for the country’s next stage of development, with the aim of comprehensively studying the scientific-theoretical and practical foundations of the large-scale reforms being implemented in the Republic of Uzbekistan, objectively identifying existing systemic problems, and developing their long-term strategic solutions. The preparation and publication of this major scientific study carries profound spiritual and symbolic significance, and this book is dedicated to the enduring memory of the late distinguished statesman and public figure of our country, Member of the Senate of the Oliy Majlis, Doctor of Law, Professor Rakhmonqulov Mirakbar Hajiakbarovich, as a symbol of boundless reverence, profound respect and deep gratitude on behalf of his disciples who have developed in this field. This scientific work has been developed directly on the basis of the scientific research, legal and organizational ideas that Mirakbar Hajiakbarovich himself led, systematically advanced during his lifetime, and whose conceptual foundations he created over many years, representing a consistent continuation of the great school established by the Mentor in the development of national legislation, modernization of public administration and legal regulation of information security in our country. The high human qualities of Mirakbar Hajiakbarovich, his unparalleled services in strengthening the foundations of statehood, his invaluable contribution to the development of science, his bright image and cherished name will live forever in the hearts of his disciples and in the history of national jurisprudence. This monograph was created with the aim of consistently continuing the great scientific work initiated by the Mentor, elevating the traditions of the scientific school he founded to a higher level, and providing scientific support for the strategic directions of the fundamental reforms being implemented by the Head of our state.

In the context of New Uzbekistan, the processes of modernizing public administration entered a new qualitative stage beginning in 2016, and this period is characterized by the fundamental administrative philosophy that “the state bodies should serve the people, not the people serve the state bodies.” The Addresses of the Head of State to the Oliy Majlis and the people of Uzbekistan, as well as the adopted Development Strategies and the “Uzbekistan – 2030” Strategy, are serving as a solid legal and political foundation for fundamentally reforming the country institutionally. In particular, the introduction, by Presidential Decree DP–21 dated February 16, 2026, “On Updating the ‘Uzbekistan – 2030’ Strategy,” of an entirely new, digitized system of strategic planning based on the “goal – action – result” chain requires the activities of public administration bodies to be restructured on the principles of effectiveness and transparency. The first chapter of this monograph is

devoted precisely to a systematic analysis of the conceptual foundations of the institutional and administrative reforms being implemented to modernize public administration in New Uzbekistan, the processes of improving the activities of central government bodies, including the positive and negative aspects of the 2022 administrative reforms that reduced the number of ministries and agencies from 61 to 28, and their reflection in labor legislation and judicial practice. In addition, this chapter comprehensively examines, on the basis of the advanced experience of developed foreign countries such as Germany, the United States, the United Kingdom, Canada, the Republic of Korea and the Czech Republic, issues related to the KPI system for evaluating the activities of public authorities, the digital monitoring platform consisting of “Green,” “Yellow” and “Red” categories, and the improvement of the institution of the civil service based on the Law “On Civil Service.” In the context of the Head of State declaring a “state of emergency” in the field of combating corruption and strengthening compliance controls across all agencies, this chapter objectively reveals the effectiveness of internal control systems and structural problems in the supervisory functions of the Accounts Chamber. One of the most important areas enhancing the scientific value and practical significance of the monograph is the problem of maintaining an inventory of benefits and preferences provided by the state and assessing their economic effectiveness, which has been studied in the content of the book as a separate object of systematic analysis. Although currently in our country direct benefits have been established by 519 legislative acts, preferences by 44 documents, and various relief measures by 4,467 documents, a system for monitoring their actual economic return on investment (ROI) and effectiveness through digital solutions and artificial intelligence technologies has not yet been sufficiently developed. Looking at international experience, the monograph provides an in-depth study of how the United States “Tax Expenditures List,” Canada’s “Tax Expenditures and Evaluations” registry, the European Union’s “State Aid Register,” and Singapore’s “Fiscal AI” systems use artificial intelligence algorithms to assess the economic impact of tax benefits and subsidies in real time. Based on this advanced foreign experience, the authors of the monograph have developed a specific, step-by-step system of organizational and legal proposals for creating a unified automated information system “Benefits Effectiveness” based on artificial intelligence technologies and maintaining its open registry. In addition, the book identifies legislative gaps concerning the institutions of mandatory rotation and attestation of civil servants. Although the rotation system is established in Article 39 of the Law “On Civil Service,” the absence of a Presidential act specifying the list of positions subject to mandatory rotation and the relevant terms, as well as the lack of a unified procedure for conducting employee attestation, hinder the elimination of corruption risks within the system. The monograph presents this problem in comparison with the experience of civil service examinations in the Czech Republic and the assessment systems for teachers and information and communication technology employees in our country, and proposes preventive mechanisms for instilling an “integrity vaccine” among civil servants.

The second chapter of the study focuses on the legal and digital foundations for improving civil society institutions and the local governance system. The authors have scientifically substantiated the need to develop legislation governing the implementation of socially significant projects through the involvement of non-governmental non-profit organizations and business entities, as well as to establish clear mechanisms for cooperation between NGOs, local executive authorities and Councils of People's Deputies. In particular, in connection with the President's declaration of 2026 as the "Year of Mahalla Development and Social Advancement," the legal substance of historic reforms such as decentralizing the mahalla governance system, increasing the independence of district budgets, retaining a certain portion of value-added tax revenues at the local level, and allocating 20 trillion soums for mahalla infrastructure constitutes the core of this chapter. The third chapter is devoted to the problems of ensuring information security in the context of the digital transformation of society and the state. It provides an in-depth analysis of the fundamental modernization of the E-Government platform based on artificial intelligence technologies within the framework of the "Digital Uzbekistan – 2030" Strategy, the introduction of a strategic system for promptly responding to threats in the media environment that undermine national and public security, the social necessity of legally restricting artificial intelligence, and mechanisms for the strategic protection of children from information harmful to their health. The fourth chapter covers the criminal-law and organizational foundations for ensuring justice and combating cybercrime, the legal aspects of international instruments concerning the fight against cybercorruption, the improvement of the institution of mediation, and issues related to strengthening the role of forensic examination in detecting digital crimes. The fifth chapter is devoted to the concept of "Cyberalogy," an entirely new direction in science, its content, essence and significance, and systematically presents the methodology for preparing information and analytical materials, scientific articles and theses based on the Cyberalogy method.

Based on the systematic analyses presented in the monograph, conceptual proposals and recommendations aimed at further improving the process of modernizing public administration in our country have been developed, including such strategic initiatives as the adoption of separate laws "On the Bodies of Executive Power of the Republic" and "On Administrative Decentralization," the development of a concept for the gradual abolition of the "manual control" method in public administration, and the development of the "Zero Bureaucracy" digital platform based on the experience of the United Arab Emirates.

This monograph is of high value not only due to its scientific and theoretical comprehensiveness, but also because it is based on real statistics, process-oriented analyses and an assessment of practical reforms, and may serve as a systematic guide for heads of government bodies, policymakers, researchers conducting scientific studies, and the broad expert community interested in the prospects for the country's digital and strategic development. This work is an important source serving to strengthen the foundations of statehood and shape the strategic-digital image of New Uzbekistan.

CHAPTER I. INSTITUTIONAL FOUNDATIONS OF PUBLIC ADMINISTRATION AND ADMINISTRATIVE REFORMS

1.1-§. Accounting for Benefits and Preferences and Improving Their Effectiveness

At present, **519** legislative acts directly establish benefits, **44** legislative acts directly establish preferences, and **4,467** legislative acts establish various types of relief measures and provisions granting benefits¹. However, sufficient opportunities have not been created to monitor the effectiveness of the benefits and preferences being provided through digital solutions. At the same time, the procedure for granting benefits and preferences established by Resolution RP–3756 of the President of the Republic of Uzbekistan dated May 31, 2018, “On Measures to Fundamentally Improve the Procedure for Granting Benefits and Preferences”², as well as by other regulatory legal acts, is not being systematically monitored, and no monitoring is being conducted in this regard. It should be emphasized that Presidential Decree DP–21 of the President of the Republic of Uzbekistan dated February 16, 2026, “On Additional Measures for Consistently Continuing Reforms and Bringing Them to a New Stage within the Framework of the Priority Areas of the Country’s Development until 2030,” establishes the need to transform the country into a regional IT hub through the development of digital technologies, bring Uzbekistan among the Top 50 countries in the World Bank’s “Statistical Performance Index,” achieve a position among the Top 30 in the United Nations E-Government Development Ranking, and increase the coverage of civil service bodies by the strategic planning system to 100 percent³.

Therefore, **in ensuring that limited resources meet unlimited needs and ensuring the rational management of budgetary funds**, as well as in discontinuing the provision of benefits and preferences to areas that have proven ineffective in the further development of the reforms being implemented by the Head of State, and **further developing areas that are producing positive results**, it is of **significant importance** to have a unified list of the benefits and preferences granted, and, based on this list, to determine whether the benefits being provided are justified and to assess their level of effectiveness.

It is well known that in the United States, the European Union, Singapore, Canada, Australia, Brazil, Singapore, Norway, Estonia and other countries, opportunities have been created to assess the effectiveness of benefits and preferences through artificial intelligence technologies. In particular, **in the United States**, the U.S. Government Accountability Office (GAO) and the Office of Management and Budget (OMB) use AI algorithms to calculate the economic return

¹ lex.uz – National Database of Legislation of the Republic of Uzbekistan.

² Decree № RP–3756 of the President of the Republic of Uzbekistan dated May 31, 2018, “On Measures to Fundamentally Improve the Procedure for Granting Benefits and Preferences” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³ Decree № DP–21 of the President of the Republic of Uzbekistan dated February 16, 2026, “On Additional Measures for Consistently Continuing Reforms and Bringing Them to a New Stage within the Framework of the Priority Areas of the Country’s Development until 2030” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

on investment (ROI) of tax benefits and subsidies. *For example*, the “**Data Analytics for Tax Expenditures**” project analyzes the effectiveness of more than 150 federal benefits in real time. **In Canada**, the GC InfoBase system presents the financial implications of benefits and preferences in the form of interactive reports. Artificial intelligence modules calculate “what-if” scenarios and indicate the most effective course of action to decision-makers. **In Singapore**, the “Fiscal AI” system was launched by the Ministry of Finance within the framework of the “Smart Nation” program, and it uses AI to **automatically assess and update in real time** the economic impact of budget expenditures and tax benefits. **In the European Union**, the European Court of Auditors and the European Commission’s DG BUDG use AI systems to calculate the return on subsidies and benefits and assess their impact across sectors. **In Australia**, the “Budget AI Modeller” forecasts the economic effectiveness of benefits and preferences and determines the return on investment (ROI) by sector and region¹.

Furthermore, in order to obtain an accurate inventory of benefits and preferences, it is advisable to maintain an open registry thereof, which has already been introduced in a number of foreign countries. In particular:

In the United States, the U.S. Department of the Treasury publishes an annual comprehensive list of federal tax benefits (Tax Expenditures List), including the estimated budgetary losses associated with each benefit². **In Canada**, the Department of Finance maintains an interactive registry of benefits and preferences (Tax Expenditures and Evaluations), and their financial impact is presented in the annual report³. **In the European Union**, the European Commission maintains a database of all state aid and preferences (State Aid Register), and the registry specifies the date on which the benefit was granted, the sector, its value, and its purpose⁴. **In Brazil**, the federal government provides an **open registry of tax benefits** through the public portal (Benefícios Tributários da União)⁵. **In Australia**, the Department of the Treasury maintains a comprehensive report on tax and customs concessions (Tax Expenditures and Insights)⁶. **In South Africa**, the Tax Service publishes an annual report on benefits and their value (Tax Expenditure Report)⁷. **In Japan**, the Ministry of Finance maintains a comprehensive registry of benefits and provides a financial assessment for each one⁸.

Furthermore, in accordance with the Annex, it was determined that 20 countries maintain specialized registries of benefits and preferences⁹.

¹ Цифровая гуманитаристика и технологии в образовании (DHTE 2025): сб. статей VI Международной научно-практической конференции. 13-14 ноября 2025 г. | Digital Humanities and Technology in Education (DHTE 2025): Collection of Articles of the VI International Scientific and Practical Conference. November 13–14, 2025. / Под ред. В.В. Рубцова, М.Г. Сороковой, Н.П. Радчиковой. – М.: ФГБОУ ВО МГППУ, 2025. – 607 с.

² <https://home.treasury.gov/policy-issues/tax-policy/tax-expenditures>.

³ <https://www.canada.ca/en/departement-finance/services/publications/federal-tax-expenditures.html>.

⁴ <https://competition-cases.ec.europa.eu/search>.

⁵ <https://portal.datransparencia.gov.br/>.

⁶ <https://treasury.gov.au/publication/p2024-489823>.

⁷ <https://www.treasury.gov.za/documents/national%20budget/2020/>.

⁸ https://www.mof.go.jp/english/policy/tax_policy/index.html.

⁹ <https://reestr.uz/>.

Currently, it has been established that, within the Unified Register of Information Systems and Resources of the Digital Government, information exchange regarding the granting of benefits and preferences in the relevant sector, industry or area has been established through 6 information systems, namely, the **“Register of Positive Expert Opinions on Preferential Goods”** information system¹, the **“Yashil imtiyoz”** information system², the **“Agroplatforma”** information system³, the **“MedRefer”** information system⁴, the **certificate database**⁵, and the **“E-Imtiyoz”** information system⁶.

For example, in the **“E-Imtiyoz”** information system introduced by Resolution № 595 of the Cabinet of Ministers dated September 22, 2021, “On Measures to Further Improve the Registration of Taxpayers and Simplify the Procedure for Reimbursing Value Added Tax,” opportunities have been created to automatically link existing tax benefits to the MXIK codes of goods and services, organizations and facilities when using tax benefits; automatically verify, compare and monitor the established periods and amounts of tax benefits; automatically generate information on organizations that have used tax benefits; and automatically send information on available benefits to taxpayers’ personal accounts⁷.

Therefore, it should be emphasized that it would be advisable to maintain an **accurate inventory of benefits and preferences** granted under legislative acts, Presidential and Government acts through a registry within a unified automated information system based on artificial intelligence technologies, and establishing such a system **will ensure the generation of the following information in real time**:

- 1) obtaining accurate information on the number, name, value (amount), validity period of benefits and preferences, when and on the basis of which document, to which categories of entities, in which sector, industry and area (sector), and for what purposes they have been granted;
- 2) based on accurate information, analyzing the achievements (results) attained through each benefit and preference granted, as well as the benefits and losses incurred by the budget, and determining budget losses;
- 3) verifying whether the entities granted benefits or preferences comply with the requirements of legislation concerning conflicts of interest;
- 4) determining whether the entities granted benefits or preferences continue to meet the requirements necessary for such benefit or preference;
- 5) ensuring transparency through the formation of an open state budget;
- 6) establishing state and public oversight over the benefits and preferences being granted;
- 7) verifying and forecasting the expediency of granting additional and new benefits and preferences.

¹ <https://singlewindow.uz/>.

² <https://eco.gov.uz/>.

³ <https://agroplatforma.uz/>.

⁴ <https://gov.uz/uz/ssv>.

⁵ <https://akkred.uz/uz>.

⁶ <https://my.soliq.uz/>.

⁷ Resolution № 595 of the Cabinet of Ministers of the Republic of Uzbekistan dated September 22, 2021, “On Measures to Further Improve the Registration of Taxpayers and Simplify the Procedure for Reimbursing Value Added Tax” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

It is precisely on the basis of this information that it will become possible to **determine the accurate accounting** of all **benefits** and preferences granted, assess the extent to which they have justified themselves, and **determine through artificial intelligence whether additional and new benefits and preferences may or may not be granted**, thereby ensuring the systematization of the reforms being implemented in this area by the Head of State.

Based on the foregoing, the following is proposed:

1. To establish a republican working group consisting of the Statistics Agency, National Agency for Social Protection, Ministry of Economy and Finance, Ministry of Digital Technologies, Ministry of Justice, Tax Committee, Customs Committee, Institute of Legislation and Legal Policy, and other interested ministries and agencies;

2. After the working group has been fully constituted, to implement the following:

to conduct an inventory of benefits and preferences granted by legislative acts, as well as Presidential and Government acts;

to prepare a final list of all identified benefits and preferences;

to prepare a final list of information systems that, based on the unified list of benefits and preferences prepared, provide the possibility of maintaining records of benefits and preferences in the relevant areas;

to submit to the Presidential Administration a draft resolution of the President of the Republic of Uzbekistan specialized in the procedure for granting benefits and preferences and maintaining records thereof, providing for the following:

to approve a regulation on the procedure for granting benefits and preferences through regulatory documents and determining their effectiveness;

to introduce the unified automated comprehensive information system “**Benefits Effectiveness**,” based on artificial intelligence technologies and maintained on an open platform accessible to all, specialized in granting benefits and preferences and maintaining an inventory thereof;

to approve the list of information systems that must be integrated with the unified automated comprehensive information system “**Benefits Effectiveness**”;

to instruct interested ministries and agencies, upon request of the Statistics Agency, to enter the necessary information into the system within two months from the date of introduction of the unified automated comprehensive information system “**Benefits Effectiveness**”;

to establish that the unified automated comprehensive information system “**Benefits Effectiveness**” shall be financed from the state budget, with the Statistics Agency designated as its owner, “Uzinfocom” Unified Integrator LLC designated as its operator, state bodies and organizations designated by legislative acts as authorized bodies in the relevant sector, industry or area designated as special users, and the general public and organizations designated as users;

to establish that the necessary information shall be entered by the Statistics Agency into the unified automated comprehensive information system “**Benefits Effectiveness**” within 10 days from the date of adoption of the document granting the benefit or preference;

to provide for the automatic modification of information in the unified automated comprehensive information system “**Benefits Effectiveness**” in real time on the basis of data from special users, as well as the maintenance of digital records thereof;

to initially determine, on a pilot basis, the effectiveness of benefits and preferences granted in the fields of social protection and banking and finance;

to determine, on a pilot basis, the effectiveness of benefits and preferences granted in the fields of construction, digitalization, agriculture, transport, healthcare, education, and the economy, as well as those granted to youth and women;

based on the results of the pilot, to establish digital effectiveness mechanisms in the remaining sectors, industries and areas;

to create the following capabilities within the unified automated comprehensive information system “**Benefits Effectiveness**”:

to obtain accurate information on the number, name, value (amount), validity period of benefits and preferences, when and on the basis of which document, to which categories of entities, in which sector, industry and area (sector), and for what purposes they have been granted;

to analyze, based on accurate information, the achievements (results) attained through each benefit and preference granted, as well as the benefits and losses incurred by the budget, and to determine budget losses;

to verify whether the entities granted benefits or preferences comply with the requirements of legislation concerning conflicts of interest;

to determine whether the entities granted benefits or preferences continue to meet the requirements necessary for such benefit or preference;

to ensure transparency through the formation of an open state budget;

to establish state and public oversight over the benefits and preferences being granted;

to verify and forecast the expediency of granting additional and new benefits and preferences;

to determine whether existing benefits and preferences are justified and effective;

to generate an automated conclusion based on artificial intelligence using the identified data;

to create special chatbots and a **mobile application** of the system so that the public can view and discuss the benefits and preferences granted and submit proposals;

to automatically send notifications to individuals and legal entities regarding the benefits and preferences granted to them through the Unified Interactive Government Services Portal and the electronic government services portal of the tax authorities;

to ensure information and cybersecurity.

Information on Specialized Registers for the Accounting of Benefits and Preferences

Nº	Name of the State or Union	Name of the Registry	Purpose of the Registry	Official Link
1.	United States	Tax Expenditures List	Federal tax expenditures and their budgetary losses	https://home.treasury.gov/policy-issues/tax-policy/tax-expenditures
2.	Canada	Tax Expenditures and Evaluations	Tax expenditures, budgetary impact, and evaluation	https://www.fin.gc.ca/taxexp-depfisc/
3.	European Union	State Aid Register	All state aid, subsidies, and preferences	https://competition-policy.ec.europa.eu/state-aid/state-aid-register_en
4.	United Kingdom	HMRC Tax Reliefs	Tax reliefs and their value	https://www.gov.uk/government/statistics/hmrc-tax-expenditures-and-reliefs
5.	Australia	Tax Expenditures and Insights	Tax and customs expenditures, analysis by sector	https://treasury.gov.au/publication/p2022-295873
6.	South Africa	Tax Expenditure Report	Tax expenditures and economic impact	https://www.treasury.gov.za/
7.	Japan	Tax Expenditure Report	Tax expenditures and financial assessments	https://www.mof.go.jp/
8.	Brazil	Benefícios Tributários da União	Federal tax and tariff benefits	https://www.gov.br/economia/pt-br
9.	Chile	Informe de Gasto Tributario	Tax expenditures and budgetary impact	https://www.dipres.gob.cl
10.	Mexico	Beneficios Fiscales	Tax and tariff reliefs	https://www.shcp.gob.mx/
11.	Argentina	Gasto Tributario	Tax expenditures and economic analysis	https://www.argentina.gob.ar/
12.	Netherlands	Budget Memorandum Annex	Tax expenditure report	https://www.government.nl/
13.	Sweden	Tax Expenditures Report	Tax reliefs and financial impact	https://www.government.se/

14.	Norway	Skatteutgifter	Tax expenditures and forecasts	https://www.statsbudsjettet.no/
15.	Finland	Tax Expenditure Report	Tax expenditures and effectiveness analysis	https://vm.fi/
16.	Denmark	Skatteudgifter	Tax reliefs and budgetary losses	https://fm.dk/
17.	Germany	Subventionsbericht	Tax and financial preferences	https://www.bundesfinanzministerium.de/
18.	France	Rapport sur les dépenses fiscales	Tax expenditures and their value	https://www.impots.gouv.fr/
19.	Italy	Catalogo dei Sussidi	Tax and state aid registry	https://www.mef.gov.it/
20.	South Korea	Tax Expenditure Report	Tax expenditures and forecasts	https://www.moef.go.kr/

1.2-§. Improving the Institutions of Rotation and Attestation of Civil Servants

Over the past period, with the aim of establishing and improving the civil service system, **3** Laws of the Republic of Uzbekistan, including **1** separate special Law of the Republic of Uzbekistan, **4** Decrees of the President of the Republic of Uzbekistan, **2** Resolutions of the President of the Republic of Uzbekistan, **3** Resolutions of the Cabinet of Ministers of the Republic of Uzbekistan, and **4** departmental regulatory legal acts have been adopted²⁰.

With the adoption of these legislative acts, relations pertaining to the civil service have been duly regulated. However, the subsequent development of social relations and the advancement of the civil servant's adherence to the principle of legality and integrity are facing a number of obstacles. Among these obstacles, the existence of corruption is having a negative impact on the further advancement of the interests of the individual, society, and the state.

It should be emphasized that, during the past period, **21** regulatory legal acts directly dedicated to combating corruption have been adopted and implemented. In particular, the Republic of Uzbekistan acceded to the **United Nations Convention against Corruption** (New York, October 31, 2003) pursuant to Law № LRU-158 of the Republic of Uzbekistan dated July 7, 2008²¹.

It is well known that, pursuant to Article 7 of the United Nations Convention against Corruption, the need to improve the effectiveness of personnel through **training and rotation (replacement)** is established.

Article 39 of Law № LRP-788 of the Republic of Uzbekistan dated August 8, 2022, "On the Civil Service," provides that the rotation of a civil servant is carried out for the purpose of developing his or her personal and professional qualities, increasing the effectiveness of his or her activities, forming a reserve of managerial personnel, and preventing corruption risks.

The procedure for rotation in the civil service, the list of civil service positions subject to mandatory rotation, as well as the period of service in positions subject to rotation shall be determined by the President of the Republic of Uzbekistan.

However, to date, **no act of the President of the Republic of Uzbekistan providing for the procedure for rotation in the civil service, the list of civil service positions subject to mandatory rotation, as well as the period of service in positions subject to rotation has been adopted.**

At the same time, paragraph 3 of part two of Article 161 of the Labour Code of the Republic of Uzbekistan provides that an employee's failure to correspond to the position held or work performed due to insufficient qualifications constitutes a ground for the termination of an employment contract at the initiative of the employer.

However, while Article 9 of Law № LRP-788 of the Republic of Uzbekistan dated August 8, 2022, "On the Civil Service," establishes that state bodies shall regularly organize retraining, professional development and education of civil servants, **the procedure for conducting the attestation of civil servants has not been sufficiently regulated in legislation**²².

It should be emphasized that, at present, the procedure for the attestation of representatives of certain fields is established by legislative acts.

For information: Pursuant to Law № LRU-901 of the Republic of Uzbekistan dated February 1, 2024, "On the Status of Teachers," teachers of state preschool, general secondary, specialized secondary, professional and extracurricular educational organizations undergo attestation in accordance with the procedure established by legislative acts and, based on its

²⁰ lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²¹ Law of the Republic of Uzbekistan № LRU-158 dated 7 July 2008, "On the Accession of the Republic of Uzbekistan to the United Nations Convention against Corruption (New York, 31 October 2003)" // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²² Law of the Republic of Uzbekistan № LRU-788 dated 8 August 2022, "On Civil Service" // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

results, may obtain the relevant qualification categories²³. The procedure for attesting teachers and awarding them qualification categories is determined by the Cabinet of Ministers of the Republic of Uzbekistan. Pursuant to Resolution № 244 of the Cabinet of Ministers dated November 22, 2007, “On Approval of the Regulation on the Procedure for Attesting Legal Service Employees and Improving Their Qualifications,” the attestation of legal service employees is regulated²⁴. Pursuant to Resolution № 208 of the Cabinet of Ministers dated May 20, 2023, “On Measures to Organize the Professional Development and Rating Assessment of Employees Responsible for the Development of Information and Communication Technologies in Republican and Local Executive Authorities,” the professional literacy of employees responsible for the development of information and communication technologies in republican and local executive authorities in their respective fields is subject to rating assessment once every three years²⁵.

By Decree №DP–16 of the President of the Republic of Uzbekistan dated January 30, 2025, “On the State Program for the Implementation of the Uzbekistan–2030 Strategy in the Year of Environmental Protection and the Green Economy,” it was envisaged to introduce a competency model for leadership positions in central and local executive authorities, as well as a system for assessing professional competency models, and to foster an intolerant attitude toward corruption among civil servants, instill an “integrity vaccine” in them, and introduce preventive mechanisms in this regard²⁶.

The effective implementation of this task is of significant importance, particularly through the proper establishment of the institutions of attestation and rotation.

Drawing upon international experience, pursuant to the Czech Republic’s Act №234/2014 on Civil Service of 2014, a civil servant is required to successfully pass a civil service examination consisting of a general part and a special part. A civil servant must successfully pass the general part of the civil service examination no later than nine months after commencing civil service. The civil servant must successfully pass the special part of the civil service examination in the field in which he or she performs his or her duties at least one month prior to the date of appointment to the position. Employees of local government authorities, as well as their officials, are required to pass the relevant general and special examinations. At the same time, in order to ensure openness and transparency, an “Information System of Civil Service” is in place. This information system provides comprehensive information through the following registers and portal data, including, for example, information on civil servants contained in the register of civil servants and service employees; information on employees who are in employment relationships and occupy official positions contained in the register of civil servants and service

²³ Law of the Republic of Uzbekistan №. LRU–901 dated 1 February 2024, “On the Status of a Teacher” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁴ Resolution № 244 of the Cabinet of Ministers dated 22 November 2007, “On Approval of the Regulation on the Procedure for Attestation and Professional Development of Legal Service Employees” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁵ Resolution № 208 of the Cabinet of Ministers dated 20 May 2023, “On Measures to Organize Professional Development and Rating Assessment of Employees Responsible for the Development of Information and Communication Technologies in Central and Local Executive Authorities of the Republic” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁶ Decree № DP–16 of the President of the Republic of Uzbekistan dated 30 January 2025, “On the State Programme for the Implementation of the ‘Uzbekistan – 2030’ Strategy in the Year of Environmental Protection and the ‘Green Economy’” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

employees; information on employed personnel contained in the register of employees of civil service and service institutions; information on vacant positions in the civil service contained in the register of occupied positions of the service; information used for registration for the Civil Service Examination and indicating its results contained in the Civil Service Examination Registration Portal; and information on civil service examinations that have been passed contained in the records of completed civil service examinations. Through these mechanisms, efforts have been made to create an “integrity vaccine”, while all information relating to the employment activities of each civil servant can be accessed through this information system²⁷.

Poland’s Act of 21 November 2008 on Civil Service provides that Poland also has a dedicated information system relating to the civil service, within which 12 types of information are maintained. The Act establishes the procedure for undergoing preparatory training upon entering the civil service and stipulates that, eight months after entering the civil service, a civil servant is required to undergo attestation, with the procedure for conducting such attestation being expressly set out in the Act itself²⁸.

In the Russian Federation, pursuant to Federal Law № 58-LF of 27 May 2003 of the Russian Federation “On the System of Public Service of the Russian Federation”, the civil service is formed based on the results of attestation, while the procedure for conducting attestation is also directly established in legislation, namely, in Federal Law № 79-LF of 27 July 2004 of the Russian Federation “On the State Civil Service of the Russian Federation”²⁹.

In some countries, the conditions and procedure for undergoing attestation are established in the form of departmental regulatory legal acts. In particular, the Rules and Conditions for the Attestation of Civil Servants of the Agency of the Republic of Kazakhstan for Civil Service Affairs, approved by Order № 74 of 5 December 2016 of the Chairman of the Agency of the Republic of Kazakhstan for Civil Service Affairs and Anti-Corruption (registered on 28 December 2016 under № 14620), provide for the attestation of employees in order to assess their knowledge and ability to perform their official duties. They further stipulate that employees shall undergo attestation six months after being appointed to a position, and thereafter following each subsequent three-year period of continuous service in the civil service, while the attestation must be conducted no later than six months from the date on which the prescribed period for undergoing attestation has elapsed³⁰.

Pursuant to Federal Law №. 79-LF of 27 July 2004 of the Russian Federation “On the State Civil Service of the Russian Federation”, the rotation of civil servants is carried out for the purpose of increasing the efficiency of the civil service and combating corruption by appointing civil servants to other civil service positions in the same or another state body. Such rotation is carried out in executive authorities exercising control functions, based on a separate list established by the executive

²⁷ <https://www.zakonyprolidi.cz/cs/2014-234>.

²⁸ <https://lexlege.pl/ustawa-o-sluzbie-cywilnej/rozdzial-11-przepisy-przejsciove-i-dostosowujace/1568/>.

²⁹ https://www.consultant.ru/document/cons_doc_LAW_42413/354808bc531bbb6e57c783ceed1cfc54dedc6add/.

³⁰ <https://adilet.zan.kz/rus/docs/V1600014620#z3>.

authority in coordination with federal ministers. Rotation is carried out with the consent of the civil servant, while the legislation also establishes cases in which rotation is not permitted³¹.

Pursuant to the Rules for the Rotation of First Heads of State Organizations Providing Special Social Services, approved by Order № 194 of 14 June 2024 of the Minister of Labour and Social Protection of the Population of the Republic of Kazakhstan (registered on 15 June 2024 under № 34501), the rotation of heads of organizations shall be carried out for the purpose of ensuring the effective utilization of their professional potential. The positions subject to rotation shall be determined by the authorized body and, on the basis of the relevant list, the rotation shall be carried out by a commission annually in November, no later than 1 December³². Furthermore, pursuant to Law № 416-V of 23 November 2015 of the Republic of Kazakhstan “On Civil Service”, the rotation of civil servants belonging to categories “A” and “B” is provided for³³.

Pursuant to Estonia’s Civil Service Act of 13 July 2012, the procedure for the urgent transfer, i.e. rotation, of officials is directly established in the Act itself. According to this procedure, one organization, upon mutual agreement with another organization, may transfer an employee from one organization to another³⁴.

Pursuant to Resolution № 492 of the Cabinet of Ministers “On Measures to Improve the Human Resources Management System in the National and Local Executive Authorities” dated 22 September 2023, it was established that, starting from 1 November 2023, all information and documents relating to human resources management in national and local executive authorities shall be generated and maintained on an electronic platform. Accordingly, the electronic platform “hrm.argos.uz” was introduced for maintaining information and documents related to human resources management in national and local executive authorities³⁵.

However, *the specific types of information concerning an employee to be reflected in this electronic platform, as well as the procedure for their automated generation or generation based on artificial intelligence technologies, have not been sufficiently defined.*

Furthermore, pursuant to Decree № DP–5505 of the President of the Republic of Uzbekistan dated 8 August 2018 “On Approval of the Concept for Improving Rule-Making Activities”, the introduction of effective mechanisms for the adoption of directly applicable laws was envisaged³⁶. However, the current Law “On the State Civil Service” does not sufficiently regulate attestation and rotation, nor does it adequately establish the procedure for maintaining an information system for civil servants in an automated manner or on the basis of artificial intelligence

³¹ https://www.consultant.ru/document/cons_doc_LAW_48601/e92846ab80fa35d65ffbac3877b3267ae9735e61/.

³² <https://adilet.zan.kz/rus/docs/V2400034501>.

³³ https://kodeksy-kz.com/ka/o_gosudarstvennoj_sluzhbe/41.htm.

³⁴ <https://hartran.ee/index.php?id=64>.

³⁵ Resolution № 492 of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Improve the Human Resources Management System in the Republican and Local Executive Authorities” dated September 22, 2023 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁶ Decree № DP–5505 of the President of the Republic of Uzbekistan “On Approval of the Concept for Improving Law-Making Activities” dated August 8, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

technologies. The provisions that should be directly stipulated in the Law itself have not been sufficiently specified; moreover, the list of employees subject to rotation, which is required to be approved by a Presidential resolution, has still not been approved.

In this context, the following difficulties and problems exist, in particular:

1. Pursuant to the Labour Code, the employer is required to provide mandatory training for its employees and improve their qualifications in accordance with the legislation; however, the lack of clearly defined mandatory periods and the absence of a properly established notification system in the existing information systems are resulting in employees' qualifications not being improved in a timely and sufficient manner;

2. The insufficient amount of information concerning the qualifications required of employees and their personal data at the time of recruiting employees on a competitive basis is leading to improper recruitment processes. For example, the qualification requirements are entered in advance into the "vacancy.args.uz" system; however, the system is not fully capable of automatically verifying the candidate's qualifications and currently can only determine the candidate's work experience. This, in turn, causes the human resources development and management units to verify the qualification requirements of candidates based on the "human factor", which may result in corrupt practices whereby a qualified candidate who meets the qualification requirements is prevented from proceeding to the next stage, while another candidate whose subsequent employment has been predetermined is allowed to proceed to the next stage.

3. The prolonged employment of employees in the same position and within the same organization is hindering their professional self-development and creating conditions conducive to the intensification of corruption-related factors.

1. Based on the Law of the Republic of Uzbekistan "On the State Civil Service", to develop and adopt a Resolution of the President of the Republic of Uzbekistan "On Approval of the Regulation on the Procedure for Rotation in the State Civil Service", providing for the procedure for rotation in the state civil service, the list of state civil service positions subject to mandatory rotation, as well as the period of tenure in positions subject to rotation;

2. To supplement Law № LRU-788 of 8 August 2022 of the Republic of Uzbekistan "On the State Civil Service" with Article 42¹ in the following wording:

"Article 42¹. Attestation of a State Civil Servant

A state civil servant, regardless of his or her category, shall undergo attestation once every three years based on his or her professional competence through a commission established by the specially authorized state body.

The composition of the commission shall be approved by the specially authorized body.

The attestation questions shall be published on the official website of the specially authorized state body at least three months prior to the attestation.

The list of employees required to undergo attestation shall be compiled by the specially authorized body, and the candidate shall be notified at least one month prior to the attestation.

The candidate shall be notified by sending an SMS notification and by submitting a notification to the state organization in which the candidate performs his or her activities.

Responsibility for ensuring that the candidate undergoes attestation in a timely manner shall rest with the head of the organization in which the state civil servant performs his or her activities, the specially authorized body, and the candidate.

The attestation processes shall be broadcast live on the official website of the specially authorized body, and the attestation questions shall be provided through an automated generation (selection) system free from human intervention.

The results of the attestation shall be determined in the form of “passed” or “failed”.

A state civil servant who obtains more than 56 points in the attestation shall be deemed to have passed the attestation.

Failure of a state civil servant to pass the attestation shall constitute grounds for termination of the employment contract concluded with him or her or for transfer to a position one level lower than his or her current position.”.

3. To develop the “State Civil Service” integrated information system on the basis of the interdepartmental software and hardware complex “Unified National Labour System” and integrate within it the currently operational Unified Open Portal of Vacant Positions in the State Civil Service (“vacancy.argos.uz”), the automated information system “samaradorlik.uz” (samaradorlik.uz), and the electronic platform “hrm.argos.uz”, as well as to integrate it with the following information systems:

- the Unified Electronic Case Management System for Administrative Offenses (“E-ma’muriy ish” system) and the “Electronic Criminal Case” information systems, in order to obtain information concerning a person’s criminal record and information about the person held by law enforcement, supervisory, and judicial bodies;

- the open “E-antikorrupsiya” portal, containing information concerning a person’s involvement in corruption-related situations and conflicts of interest;

- the “Xorijda ish” electronic software complex for labour migration, containing information on whether a person has worked in a foreign country;

- the Unified Interactive Public Services Portal, containing personal and family status information, information on property, places of employment and study, and other interactive information.

The newly developed information system should incorporate artificial intelligence technologies based on neural technologies and should have the capability to automatically provide, without human intervention, all information concerning the state civil service exclusively to a limited range of authorized persons (only the employer).

Under the proposed approach, the development of an automated information system alone would require additional funding from the state budget. However, provisions providing for the redirection of funds currently allocated to the “vacancy.argos.uz”, “samaradorlik.uz”, and “hrm.argos.uz” systems towards the development, technical support, expert examination, and implementation of the new information system could be incorporated into the Resolution of the President of the

Republic of Uzbekistan “On Approval of the Regulation on the Procedure for Rotation in the State Civil Service”.

At the same time, it will also be necessary to include information concerning attestation and rotation in the “State Civil Service” integrated information system.

1.3-§. Improving Procedures for Handling Appeals Based on the Experience of Estonia and Denmark

With a view to effectively organizing interaction with the population and further improving the system for handling appeals in state bodies, the following findings were identified based on the experience of **Estonia** and **Denmark**, in particular:

The following problems exist in the handling of appeals, in particular:

1. Under the requirements of the current legislation, when submitting an appeal to each organization, the applicant is required to attach all documents and materials substantiating the issues raised in his or her appeal. This situation is resulting in negative consequences when citizens submit appeals concerning a single principal problem to two or more organizations, as they are required to submit appeals sequentially concerning the same issue. As a result, waiting for responses from the previous authorities and subsequently approaching the next organization on the basis of those responses is leading to an unjustified extension of the time limits for considering appeals. This, in turn, is creating bureaucratic factors that contribute to an increase in the number of repeated appeals and complaints within the system and result in citizens having to expend additional time and effort.

For information: In Estonia, the X-Road system, a unified secure network for information exchange between state authorities, has been introduced, which, based on the “Once-Only” principle, completely eliminates the need for other authorities to repeatedly request information once it has been provided by a citizen. Within this system, all appeals are submitted through the unified eesti.ee electronic portal, which creates the following opportunities: a citizen can monitor the processing of his or her appeal in real time, **automatically attach the necessary documents and information by integrating data and documents available in interconnected systems through the system, as well as enables the state authority itself to independently and automatically obtain from the system the information necessary for considering the appeal**³⁷.

In this context, in order to increase the efficiency of considering appeals, a systemic solution can be achieved by introducing technical modifications to murojaat.gov.uz³⁸, the “Xalq nazorati” platform³⁹, and other specialized systems. In particular, it has been established that, at the time of submitting an appeal, in addition to identifying the principal state body or organization, the applicant may simultaneously designate other relevant authorities, while these authorities may attach the necessary information to the system within 10 days without waiting for a request from the relevant state body. This would make it possible, within the overall time limit for consideration of the appeal, to provide the applicant and the relevant organization with the information pertaining to the matter under consideration. At the same time, through the full integration of these systems with the Unified Interactive Public Services Portal (UIISP)⁴⁰ and other state information resources, it would be possible to create an opportunity for both the applicant and the relevant

³⁷ eesti.ee.

³⁸ <https://murojaat.gov.uz/ru>.

³⁹ <https://xalqnazorati.uz/uz/>.

⁴⁰ <https://my.gov.uz/uz>.

organization to obtain, free of charge and in real time, all documents and materials related to the appeal.

2. At present, in our Republic, the digital KPI indicators serving as a systemic control mechanism for improving the quality of public services and services provided, as well as the procedure for assessing work performance, have not yet been fully established.

*For information: In Denmark, following the provision of each public service and response to an appeal, the applicant has the opportunity to **evaluate the quality of the service through the system or his or her personal device**. The objectivity of this evaluation is analyzed using artificial intelligence tools and **is mandatorily taken into account in assessing the KPI performance of the civil servant**. Furthermore, **the system incorporates a proactive approach, whereby citizens are automatically informed about their rights and benefits before they submit an appeal**⁴¹.*

The introduction of this advanced system in the Republic of Uzbekistan would, firstly, ensure that each appeal and service is examined in a timely and comprehensive manner, thereby contributing to a fundamental improvement in the quality of services; secondly, it would make it possible to prevent applicants from being deprived of benefits and preferences established by legislation due to their own negligence.

3. At present, cases of abuse by civil servants in relation to citizens' personal and individual data are increasing in the course of handling appeals. In particular, the leakage of such data to social networks such as Telegram without any connection to the performance of official duties is causing serious harm to the rights and legitimate interests of citizens, while the fact that the servers of such networks are located outside the territory of Uzbekistan creates technical obstacles to the timely identification and preservation of digital evidence.

For information: One of the strongest aspects of the Estonian model is the “Digital Footprint” system, through which a citizen, via the state portal (eesti.ee), can not only monitor the status of his or her appeal, but also clearly see which official accessed his or her personal data, at what time, and on what grounds⁴². Moreover, strict administrative and criminal liability is established for unjustified access, and this process is supervised by the independent institution of the Chancellor of Justice (Õiguskantsler)⁴³.

In this context, it has been established that there is a “legal gap” in the Code of the Republic of Uzbekistan on Administrative Responsibility⁴⁴ and the Criminal Code⁴⁵ concerning unjustified access to personal data through state information systems, and that the technical capabilities for monitoring such access have not been sufficiently established.

4. At a time when digital transformation processes are advancing rapidly, the possibility of establishing interaction between the state and citizens in the Republic of Uzbekistan through a **unified electronic mail system** has still not been fully created. Although Resolution № 637 of the Cabinet of Ministers dated 9 October

⁴¹ <https://www.borger.dk/>.

⁴² <https://www.eesti.ee/>.

⁴³ <https://www.oiguskantsler.ee/>.

⁴⁴ Code of the Republic of Uzbekistan on Administrative Responsibility // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴⁵ Criminal Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

2020 established the obligation of state bodies to send response letters to appeals through the “Unified National System”⁴⁶, in practice, the cost of a single postal dispatch amounts, on average, to UZS 12,000, and as of 26 June 2026, the transfer of more than **UZS 127 billion** from one budget account to another in connection with only 10,599,863 appeals considered through the Presidential Portal demonstrates that the system is **economically inefficient**.

***For information:** In Denmark, communication between the state and citizens is regulated on the basis of the Digital Post Act, under which every citizen over the age of 15 is required to have a mandatory digital mailbox⁴⁷, and letters sent by the state are considered an official legal fact equivalent to personal delivery to the citizen; no excuses, such as “I did not notice it”, have any legal effect⁴⁸.*

In this context, in the Republic of Uzbekistan, it would be advisable, on a pilot basis, to introduce the practice of **mandatorily sending response letters from state bodies to the electronic address of all citizens, except for persons with disabilities and pensioners, using their identification in the OneID system through the murojaat.gov.uz portal, and to designate such electronic address as the single official point of contact between the citizen and the state.**

The adoption of this proposal would, in turn, make it possible to save budgetary funds by eliminating the need to use the services of the Unified National Postal System and to address problems associated with delays in the delivery of postal correspondence.

5. According to the current legislation, where a state body receives an appeal that does not fall within its competence, it is required to forward the appeal to the relevant authority within five days or notify the citizen thereof. However, due to citizens’ inability to present their issues in a legally complete and well-substantiated manner, appeals often remain insufficiently examined or the number of repeated appeals increases, which, in turn, leads to the formation of negative perceptions among the public regarding the activities of state bodies.

***For information:** Under Danish legislation, a state body does not have the right simply to reject a citizen’s appeal on the grounds that the matter does not fall within its competence. Instead, the authority is required to directly forward the appeal to the relevant organization, attach a cover letter explaining the substance and legal grounds of the appeal, and notify the citizen of this process⁴⁹.*

Therefore, at present, it would be advisable to mobilize the capacities of legal service employees or legal service centers available in all state bodies, abandon the practice of returning appeals to citizens on the grounds that they fall outside the authority of the respective body, and introduce a mechanism for their high-quality direct transfer to the responsible authority.

6. Although the completeness of responses to appeals submitted to state bodies and organizations is established by legislation, in practice, response letters

⁴⁶ Resolution № 637 of the Cabinet of Ministers of the Republic of Uzbekistan dated October 9, 2020, “On Measures to Introduce a Unified National System for the Delivery of Correspondence Sent by State Bodies and Organizations, Confirmation of Its Delivery, Storage and Registration of Information” // LexUZ — National Database of Legislation of the Republic of Uzbekistan.

⁴⁷ <https://www.retsinformation.dk/>.

⁴⁸ <https://lifeindenmark.borger.dk/apps-and-digital-services/Digital-Post>.

⁴⁹ <https://www.retsinformation.dk/>.

are often general in nature and do not contain specific solutions to the issues concerning citizens.

*For information: Under Danish legislation, any decision to reject an appeal or to satisfy it in part must specify, point by point, the legal provisions and factual circumstances underlying the decision, and **each instance of rejection must be stated clearly and with appropriate justification**. Under this procedure, **providing letters that fail to fully answer the questions raised or that are general in nature entails liability of the civil servant pursuant to the legislation**⁵⁰.*

7. In the current legislation on appeals, the institution of “hearing the applicant” has not been sufficiently established, and appeals are generally considered in the form of personal, mobile, and public receptions. This, in turn, causes inconvenience to citizens and leads to an unjustified extension of the overall time limits for considering appeals due to the reception procedures.

***For information:** In Denmark, if, during the consideration of an appeal, a state body identifies new facts that may operate to the detriment of the citizen, it is required, prior to making a final decision, to provide the citizen with an opportunity to express his or her views regarding such circumstances – the “right to be heard”⁵¹.*

The implementation of this provision into national legislation would, on the one hand, ensure the fairness of decisions and, on the other hand, serve to limit the increase in unjustified repeated appeals by preventing potential dissatisfaction in advance.

8. At present, the majority of appeals being received are related to the failure to provide public services in a timely manner or to delays in services of a permitting nature.

*For information: Under the Danish practice, if no response is provided within the prescribed period in relation to applications for the provision of public services or applications concerning registration or the issuance of permits, **the system automatically generates a positive decision and provides the citizen with the relevant licence, permit, or other document***⁵².

The application of this system in Uzbekistan could further increase the responsibility and attentiveness of civil servants when considering appeals and providing public services and, consequently, could lead to a significant reduction in appeals containing complaints.

9. One of the most negative aspects of the process of handling appeals is the submission of appeals containing insulting content by applicants, and such conduct is undermining the professional reputation of state bodies and organizations.

***For information:** Under Danish legislation, if a citizen repeatedly submits unjustified appeals concerning the same matter without presenting any newly established circumstances and such appeals contain insulting content, the relevant organization has the authority to seek a temporary restriction, through judicial proceedings, of the citizen’s right to submit appeals to that organization concerning the same matter*⁵³.

The existence of such a legal mechanism would contribute to ensuring that appeals are submitted in a respectful and substantive manner, preventing disrespect towards the activities of state bodies, and ensuring the efficient allocation of administrative resources.

⁵⁰ <https://www.retsinformation.dk/>.

⁵¹ <https://www.ombudsmanden.dk/>.

⁵² <https://virk.dk/>.

⁵³ <https://www.ombudsmanden.dk/>.

10. At present, the insufficient integration of state bodies' information systems, as well as the absence of opportunities for electronic cooperation between courts and other authorities within systems for handling appeals, is causing serious problems. In particular, the continued submission of court decisions for enforcement in paper form and the failure to enforce them in a timely manner are causing serious harm to the rights and legitimate interests of citizens and other entities.

***For information:** Under the Estonian practice, when an administrative decision is challenged, the integration of judicial and appeals-handling systems automatically suspends the enforcement of that decision (demolition of a building, collection of a fine, and others) until the appeal has been considered⁵⁴.*

The introduction of this advanced system in Uzbekistan could play a decisive role in digitizing the enforcement of court decisions, eliminating bureaucratic barriers, and ensuring the legal protection of citizens.

11. At present, citizens are provided only with general information regarding the status of implementation of appeals submitted through platforms such as murojaat.gov.uz and "Xalq nazorati" (whether the appeal is under consideration, accepted, or completed). Under the new procedure introduced by the justice authorities, although the possibility of obtaining information via SMS notification concerning the full name, position, and telephone number of the official responsible for considering an appeal represents a positive step, citizens' complaints regarding the fact that such telephone numbers are frequently non-functional or incorrect are increasing.

***For information:** In Denmark, when a citizen accesses the borger.dk portal, all of his or her applications and complaints submitted to various ministries are displayed along a single chronological timeline, including a clear indication of exactly which official currently has the matter on his or her desk. This system not only ensures that citizens are adequately informed, but also makes it possible to identify officials who have failed to consider an appeal in a timely manner or have violated legislation, thereby creating an opportunity for a court to issue a fair decision in relation to such officials⁵⁵.*

The full integration of this transparency mechanism into the systems of Uzbekistan would serve as an important factor in strengthening enforcement discipline and increasing citizens' trust in state bodies.

12. At present, although the "Register of Powers" information system has been launched and the powers of ministries and agencies are being systematized by the justice authorities, in practice, the issue of properly determining the jurisdiction of appeals has still not been adequately resolved. This is causing organizational difficulties associated with the expenditure of additional time and resources by organizations when forwarding appeals to the relevant authorities.

***For information:** In Estonia, the duties and functions of each authority are fully digitized on the basis of metadata, and the system itself automatically determines which authority has jurisdiction over an appeal and even provides citizens with guidance on the appropriate direction with the assistance of artificial intelligence while the appeal is being formulated.*

⁵⁴ riigiteataja.ee.

⁵⁵ <https://www.borger.dk/>.

The introduction of this advanced approach in Uzbekistan has been identified as a decisive factor in eliminating bureaucratic barriers, improving the quality of consideration of appeals, and preventing unnecessary loss of time.

13. At present, although a mechanism for confirming appeals submitted through murojaat.gov.uz, “Xalq nazorati”, and other specialized platforms via SMS notifications has been introduced, technical malfunctions in this system are causing serious problems associated with delays in notifications, as well as an increased risk of cybercrime and inadequate protection of personal data.

*For information: In Estonia, the process of confirming citizens’ appeals is carried out through advanced identification tools such as **Mobile ID** and **Smart ID**, which not only eliminates security vulnerabilities within the system but also further simplifies the process of formalizing appeals.*

The implementation of these identification standards into Uzbekistan’s appeals-handling system has been identified as an effective solution for ensuring information security and eliminating technical barriers encountered by citizens in accessing public services.

14. In the Republic of Uzbekistan, since **Proactive Public Services** models have not yet been fully implemented in the handling of appeals, citizens are still required, in each individual case, to independently contact state bodies in order to protect their rights or access public services.

*For information: In Denmark, if the system identifies that a citizen’s rights have been violated or that the citizen is entitled to certain benefits and preferences, it automatically sends the citizen a pre-generated application form. The citizen then has the opportunity to **promptly restore his or her rights through the courts and state bodies and make use of the relevant benefits within the prescribed period** simply by clicking the “Confirm” button.*

The introduction of this proactive model in Uzbekistan has been identified as being of significant importance in preventing unnecessary inconvenience to citizens, bringing relations between state bodies and the population to a new level, and ensuring legal protection.

15. At present, in the handling of appeals, the incorrect determination of the scope of authority of state bodies and organizations, including **attempts to resolve issues at the republican or regional level at the lower, district level, or forwarding appeals to authorities whose competence does not correspond to the substance of the appeal, is leading to an increase in the number of repeated appeals and complaints.**

*For information: In Estonia, a mechanism has been introduced whereby **a single appeal is considered in parallel by several relevant state bodies and a single response letter is sent on the basis of a joint decision.** Under this system, if an appeal falls within the competence of several authorities or the level at which it should be resolved (district, regional, or republican) is complex, the possibility of sending a response letter is restricted until the parties automatically formulate a joint decision⁵⁶.*

The implementation of this approach in Uzbekistan has been identified as being of significant importance for eliminating the practice of fragmented consideration of appeals, improving the quality of decisions, and removing bureaucratic procedures that cause unnecessary inconvenience to citizens.

⁵⁶ <https://www.riigiteataja.ee/et>.

16. In Uzbekistan, the system of considering appeals based on the principle of territorial jurisdiction, which has been introduced into practice, is increasing the influence of local acquaintance and personal connection factors, thereby increasing corruption risks and creating a tendency to resolve issues raised in appeals through personal connections rather than through lawful procedures.

*For information: In Denmark, in order to ensure the impartial consideration of appeals and eliminate corrupt relationships, the system **assigns an appeal in a completely randomized manner to a representative from another region or an employee of another organization who has no territorial or organizational connection with the citizen**. In this process, it is not known in advance whose desk the appeal will reach, while the system **automatically checks for conflicts of interest**: if there is a family relationship or other affiliation between the employee considering the appeal and the citizen, the system redistributes the appeal and **removes the initial employee from the process**⁵⁷.*

The introduction of this transparent mechanism in Uzbekistan has been identified as being of decisive importance for preventing corruption in the process of considering appeals, ensuring systemic fairness, and strengthening public trust in state bodies.

17. At present, the absence of a unified legal practice in the handling of appeals is resulting in different responses being provided to appeals of the same type, which, in turn, is leading to misunderstandings among citizens and an increase in dissatisfaction with the activities of state bodies.

*For information: Under the Estonian practice, **a unified register of each appeal and the response provided thereto** is maintained, which, while ensuring the inviolability of personal data, also creates an open and transparent **precedent database** for all. Through this register, both civil servants and the general public can review previously provided responses to similar matters and, using them, submit appeals correctly⁵⁸.*

The introduction of such a unified precedent system in Uzbekistan would serve as an important factor in ensuring legal consistency in the consideration of appeals, increasing the consistency of decisions, and guaranteeing clarity regarding the outcomes that citizens may expect from state bodies.

18. At present, one of the most pressing problems on murojaat.gov.uz, “Xalq nazorati”, and other specialized platforms is the requirement to provide the personal data of individuals or legal entities in appeals concerning corruption and violations of the law, as well as the non-consideration of anonymous appeals. Such practices are leading to an increase in latent (hidden) offenses and causing citizens to refrain from submitting appeals due to concerns regarding their safety.

*For information: Under the Danish practice, an effective system of anonymization and **cryptographic protection of appeals** has been introduced for persons reporting corruption-related incidents and violations of the law. Such an approach has elevated the level of disclosure of violations in the civil service by ensuring the personal safety of citizens⁵⁹.*

The implementation of this mechanism in Uzbekistan has been identified as being of decisive importance for strengthening public oversight in the fight against

⁵⁷ <https://www.retsinformation.dk/>.

⁵⁸ <https://www.riigiteataja.ee/et>.

⁵⁹ <https://www.justitsministeriet.dk/>.

corruption, ensuring the timely detection of violations, and increasing citizens' trust in state bodies.

19. In Uzbekistan, ensuring the timely consideration of appeals is still carried out mainly through traditional administrative methods, which indicates that the potential of digital technologies is not being fully utilized and that systemic problems, such as delays in prescribed time limits, continue to persist.

*For information: Under the Estonian practice, if the prescribed time limit for considering an appeal is violated, the information system identifies the specific official responsible for the violation and automatically sends a **“red flag” (warning)** concerning the violation to the courts, law enforcement, and supervisory authorities. Such notification is not removed from the system until a decision is entered confirming that disciplinary or other measures have been taken against the responsible person or that the delay was supported by lawful grounds. This mandatory electronic monitoring mechanism has enabled Estonia to occupy leading positions in global rankings concerning the timely consideration of appeals⁶⁰.*

The implementation of this digital solution in our country has been identified as an important factor in increasing the personal responsibility of civil servants, strengthening enforcement discipline, and eliminating indifference towards citizens' appeals.

20. Insufficient attention is being paid to candidates' competencies in handling appeals during recruitment to the civil service and appointment to higher positions. In practice, this is resulting in employees who demonstrate an indifferent or superficial approach remaining within the system instead of substantively resolving citizens' issues, consequently leading to an increase in the number of complaints.

*For information: Under the Estonian practice, a **“Personal Responsibility Register”** of civil servants is maintained. According to this system, each unlawful or superficial response letter of a general nature is automatically recorded directly in the respective employee's personnel file. Such digital records constitute a **decisive factor in determining the employee's professional competence (attestation) and in the process of promotion**⁶¹.*

The implementation of such a responsibility mechanism into the civil service system of Uzbekistan has been identified as being of significant importance for increasing the responsibility of personnel, fundamentally improving the quality of consideration of appeals, and selecting professionals for positions who demonstrate a professional and respectful approach towards citizens.

21. Although response letters to appeals may be formally correct in structure, the absence of effective mechanisms for identifying and eliminating corruption-related factors or instances of incorrect interpretation of the law in their content is creating serious systemic shortcomings.

*For information: In Denmark, **responses to appeals are subject to mandatory linguistic analysis using artificial intelligence (AI) based on the principles of “completeness, substantiation, and freedom from corruption” (the triad)**. The system automatically scans the content of the response letter and identifies violations of the law, indications of corrupt arrangements, or legal errors; only **when the results of this verification are positive is the response sent to the citizen**⁶².*

⁶⁰ <https://www.ria.ee/>.

⁶¹ <https://riigikantselei.ee/>.

⁶² <https://digst.dk/>.

The implementation of this advanced technological solution in Uzbekistan has been identified as being of decisive importance for fundamentally improving the quality of responses provided by state bodies, neutralizing corruption risks at the implementation stage itself, and strengthening public trust in decisions adopted by state authorities.

22. Although a system of personal, mobile, and public receptions is currently in place, sufficient legal and organizational mechanisms have not yet been established for the official registration of appeals that have attracted widespread public attention on social media, as well as for the transparent resolution of matters of high social significance with the participation of mass media.

For information: In Denmark, a “Public Hearings” regulation applies to appeals concerning matters of significant social importance, and such appeals are mandatorily considered with the participation of the mass media. In Estonia, the procedure for officially registering and legally considering matters that have been widely discussed on social media has been fully digitized⁶³.

The implementation of these international best practices in Uzbekistan has been identified as being of strategic importance for integrating citizens’ views into public administration, resolving emerging social discontent through open and fair discussions, and increasing the transparency of the activities of state bodies.

23. Although the current legislation expressly establishes the right of minors to submit appeals to state bodies, **the absence of adapted technical functionalities that take into account the age-specific characteristics of children** on the existing platforms in Uzbekistan, including murojaat.gov.uz, “Xalq nazorati”, and other specialized platforms, is creating an obstacle to the effective exercise of this right in practice.

For information: Under the Danish practice, separate, simplified digital appeal platforms have been developed for children and young people, adapted to their language and level of comprehension. These platforms provide children with independent and convenient opportunities to protect their rights and legitimate interests⁶⁴.

The implementation of this approach into Uzbekistan’s digital appeals systems would serve as an important step towards strengthening child-oriented public policy and supporting the social engagement of the younger generation.

24. At present, the institution responsible for overseeing compliance with human rights in the process of handling appeals is operating ineffectively. It is observed that the activities of this institution remain largely limited to narrow technical and administrative functions, such as forwarding appeals to the relevant organizations according to their jurisdiction.

For information: In Denmark, every appeal and the response provided thereto is mandatorily reviewed by the Folketingets Ombudsmand (Parliamentary Ombudsman) from the perspective of ensuring human rights; where violations of the law are identified, relevant instructions are issued, and the results are publicly disclosed. In Estonia, this function is performed by the Õiguskantsler (Chancellor of Justice)⁶⁵.

The implementation of these international best practices in Uzbekistan has been identified as a decisive factor in transforming the activities of oversight bodies

⁶³ <https://hoeringsportalen.dk/>.

⁶⁴ <https://bornetelefonen.dk/>.

⁶⁵ <https://www.ombudsmanden.dk/>.

from formalistic approaches to substantive protection of rights, increasing citizens' trust in the state and the Ombudsman, and ensuring the supremacy of human rights.

25. At present, due to the insufficient integration of murojaat.gov.uz, "Xalq nazorati", and other appeal-handling systems with the Supreme Court's "Adolat" judicial systems complex, when citizens are dissatisfied with responses from state bodies, they are required to spend additional time and incur financial expenses, such as court fees, in order to apply to the court, and must submit a separate appeal through the relevant system or through traditional means. This, in turn, is leading to an increase in repeated appeals and a decline in public trust in state bodies.

*For information: Under the Estonian practice, if citizens are dissatisfied with a decision of a relevant authority or court, they have the opportunity to submit an appeal to a higher authority or court through an **"automatic appeal" button** within the system, without paying a state fee. In Denmark, with the aim of resolving disputes before they reach the courts, a **mediation mechanism has been integrated directly into the system**, allowing a citizen to select any mediator, after which the system automatically notifies the relevant organization. If the mediation process concludes unsuccessfully, the citizen retains the right to apply to the court⁶⁶.*

The introduction of these advanced digital solutions in Uzbekistan has been identified as a decisive factor in eliminating bureaucratic barriers, expanding citizens' access to justice, and strengthening the practice of resolving disputes through pre-trial mediation.

1. Amendments and additions to the Law of the Republic of Uzbekistan "On Appeals of Individuals and Legal Entities" with the inclusion of the following provisions:

- proactive appeal models;
- a system for the automatic random allocation of appeals in Uzbekistan;
- requirements for the professional competence of employees handling appeals;
- the procedure for considering appeals that have been widely discussed on social media, including the mandatory participation of press secretaries;
- the categories and procedure of appeals that must be considered with the participation of the mass media and in videoconference mode;
- mandatory requirements for specialized systems for handling appeals;
- the procedure for operating specialized systems for handling appeals;
- mandatory requirements for appeals submitted through specialized systems for handling appeals and the responses thereto, as well as their digital monitoring in real time;

- the provision of the applicant's final opportunity to state his or her position — the "right to be heard" — in decisions concerning the rejection of an appeal;

- abolishing the institution of merely explaining the law when forwarding an appeal to the relevant organization according to its jurisdiction and establishing an institution whereby, in cover letters forwarding appeals to other organizations according to their jurisdiction, the circumstances relating to the matter raised in the appeal must be comprehensively, fully, and substantiatedly stated, and the applicant's matter must be explained to the relevant authority;

⁶⁶ <https://www.riigiteataja.ee/>.

temporarily restricting, through judicial proceedings, the applicant's right to submit appeals to the relevant organization in cases involving insulting and defamatory appeals;

establishing that, in any decision to reject an appeal or satisfy it in part, the legal provisions and factual circumstances underlying such decision must be stated point by point, and each instance of rejection must be clearly and adequately substantiated;

institutional powers to conduct mandatory substantive reviews of appeals and publicly disclose the results thereof, as well as the procedure for exercising such powers;

introducing an institution whereby an appeal is considered in parallel by lower- and higher-level organizations, as well as, where the matter raised in the appeal falls within the competence of two or more organizations, the appeal is considered in parallel without forwarding it according to jurisdiction and a joint decision is adopted based on the results.

2. Establishing the mandatory introduction of the following mechanisms in systems specialized in handling appeals:

determining the jurisdiction of appeals on the basis of the "Register of Powers";

introducing a system for the automatic random allocation of appeals in Uzbekistan;

automatic preparation of the text of appeals using artificial intelligence;

automatically selecting, through the system, documents and materials related to the appeal, including previous appeals and/or responses thereto in cases of repeated appeals;

launching a mechanism for automatically logging the review of appeals and automatically notifying the applicant, through notifications, of information concerning persons who have viewed the text of the appeal, including persons who have viewed it without proper grounds, distributed it, or copied it;

enabling the applicant to view the implementation stages of an appeal in real time;

providing automatic notifications through green, yellow, and red indicators to ensure that an appeal is considered within the prescribed time limit;

automatically generating, within the system itself and without human intervention, a decision on the imposition of an administrative penalty on persons who have failed to comply with the prescribed time limit for considering an appeal and forwarding such decision for enforcement;

automatic confirmation of an appeal through the FACE-ID system;

mandatory review of the response to an appeal by artificial intelligence to determine whether each issue raised in the appeal has been addressed, whether the response is complete and substantiated, whether it is legally justified, whether it is not contrary to human rights and interests, and whether it is free from corruption-related factors, as well as conducting semantic and predictive analysis;

sending the response to an appeal, based on a positive conclusion of the artificial intelligence system, to the electronic address of an applicant who does not

have a disability and has not reached pension age, as well as to his or her telephone number in the form of an SMS notification;

in the event of dissatisfaction with the response to an appeal, enabling mediation or the automatic submission of a complaint to a court and other competent authorities without payment of a state fee;

introducing modules intended for children, persons with disabilities, and persons who have reached pension age;

establishing a cryptographically anonymized and protected subsystem for appeals relating to corruption;

launching a unified database and register of all appeals received by the system, with the personal identity of applicants anonymized, including the texts of appeals and the responses provided thereto;

introducing mandatory KPI indicators based on citizens' evaluation of civil servants with respect to the consideration of appeals and the quality of public services provided, with such evaluations being objectively assessed by artificial intelligence, as well as mechanisms for additional remuneration of civil servants based on these indicators;

establishing videoconference mode;

introducing an institution for organizing and temporarily suspending the enforcement of decisions of courts and other state bodies through the system.

3. In order to bring the provision of public services to a new level and reduce the number of systemic appeals and corruption-related factors:

establishing the provision of information-based public services and services free of charge;

restricting the collection by public service centers of additional fees approved by the justice authorities for public services and services provided by such centers, apart from the mandatory fees established by legislation for the respective service or service;

where registration, permitting, and licensing services are not provided within the prescribed period, establishing the automatic issuance of a positive conclusion through the system and, on this basis, the automatic completion of the registration, permitting, and licensing procedures;

digitizing public services and services based on the principle of a "single integrated public service" and introducing a single payment;

abolishing the requirement to obtain technical conditions and incur additional expenses for connection to electricity, water, gas, and telecommunications services, and introducing a unified public connection service.

4. Introducing, in Article 269³ of the Code of the Republic of Uzbekistan on Administrative Responsibility, the initiation of proceedings on administrative offenses based on an application by the victim in respect of the following:

Article 43 – violation of legislation on appeals of individuals and legal entities;

Article 46² – violation of legislation on personal data;

Article 212 – failure to comply with mandatory requirements of technical regulations or standards;

Article 215⁵ – violation of legislation in the field of public services.

5. Establishing administrative and criminal liability for the following:

a) in Article 46² of the Code of the Republic of Uzbekistan on Administrative Responsibility and Article 141² of the Criminal Code — unlawful viewing of personal data contained in state information systems and resources;

b) in Article 43 of the Code of the Republic of Uzbekistan on Administrative Responsibility and Article 144 of the Criminal Code —

failure to state, point by point, the legal provisions and factual circumstances underlying any decision to reject an appeal or satisfy it in part, as well as failure to clearly and adequately substantiate each instance of rejection;

violation of mandatory requirements applicable to specialized systems for handling appeals, mandatory requirements applicable to appeals submitted through specialized systems for handling appeals and the responses thereto, and their digital monitoring in real time;

failure to provide the applicant with the final opportunity to state his or her position – the “right to be heard” – concerning newly discovered circumstances and decisions to reject an appeal during the process of considering the appeal;

sending to the applicant responses to appeals that have not received a positive result from the mandatory artificial intelligence review, semantic and predictive analysis concerning whether each issue raised in the appeal has been addressed, whether the response is complete and substantiated, whether it is legally justified, whether it is not contrary to human rights and interests, and whether it is free from corruption-related factors;

unjustified consideration of an appeal, or dissemination of an appeal through telecommunications or Internet networks;

violation of the applicant’s “right to be heard” and violation of the procedure for adopting a joint decision on an appeal.

CHAPTER II. IMPROVING CIVIL SOCIETY INSTITUTIONS AND LOCAL GOVERNANCE

2.1-§. Improving Legislation on the Implementation of Socially Significant Projects through the Engagement of Civil Society Institutions and Business Entities

The procedure for implementing socially significant projects is **not directly regulated by a single (unified) law of the Republic of Uzbekistan (the absence of such a law may be recognized as a problem only if there is an actual need to adopt a single comprehensive law)**. Relations in this area are regulated by the Laws of the Republic of Uzbekistan **“On Guarantees of the Activities of Non-Governmental Non-Profit Organizations”**⁶⁷ and **“On Social Partnership”**⁶⁸, which establish general provisions concerning the implementation of socially significant projects.

The Regulation **“On the Procedure for Granting State Social Orders by State Bodies for the Implementation of Social and Socially Significant Projects,”** approved by Resolution № 135 of the Cabinet of Ministers dated February 22, 2018, establishes the procedure for state bodies to grant state social orders to non-governmental non-profit organizations and other civil society institutions for the implementation of social and socially significant projects⁶⁹.

Accordingly, **two different practices have emerged based on two distinct legislative frameworks governing the allocation of state social orders.**

First, state bodies and organizations may, in accordance with the Regulation **“On the Procedure for Granting State Social Orders by State Bodies for the Implementation of Social and Socially Significant Projects,”** approved by Resolution № 135 of the Cabinet of Ministers dated February 22, 2018, allocate state social orders annually from their extra-budgetary funds;

***For reference:** Under this Regulation, state social orders have been implemented in accordance with the requirements of legislation on public procurement through the **electronic public procurement system** (xarid.uzex.uz). In response to inquiries sent to 25 ministries and agencies, **the Ministry of Preschool and School Education** reported that 1 state social order was awarded in 2023 in the amount of UZS 500.0 million for the Republican Center for Social Adaptation of Children, on the topic “Successful Path to Vocational Training”; **the Ministry of Higher Education, Science and Innovation** reported that 1 state social order was awarded in 2025 in the amount of UZS 350.0 million to the Association of Persons with Disabilities of Uzbekistan, on the topic “Equal Opportunities in Higher Education”; **the Ministry of Justice** reported 5 state social orders totaling UZS 13,618.35 million awarded during 2023–2025; during 2024–2025, **the National Agency for Social Protection** awarded 6 state social orders totaling UZS 3,493,000 million, while **the Agency for Youth Affairs** awarded 8 state social orders totaling UZS 5,165 million. **The Tax Committee** reported that 4 projects totaling UZS 73.260 million were*

⁶⁷ Law № LRU–76 of the Republic of Uzbekistan “On Guarantees of the Activities of Non-Governmental Non-Profit Organizations” dated January 3, 2007 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁶⁸ Law № LRU–376 of the Republic of Uzbekistan “On Social Partnership” dated September 25, 2014 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁶⁹ Regulation “On the Procedure for Placing a State Social Order by State Bodies for the Implementation of Social and Projects of Social Significance,” approved by Resolution № 135 of the Cabinet of Ministers of the Republic of Uzbekistan dated February 22, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

implemented during 2024–2025 from the perspective of social protection, while 9 state bodies reported that they would consider this issue gradually.

Second, state social orders are implemented through the <https://ngo.gov.uz> platform at the expense of the funds of the Public Fund for Support of Civil Society Institutions under the Oliy Majlis of the Republic of Uzbekistan (hereinafter referred to as the **Fund**), based on proposals submitted by ministries and agencies⁷⁰.

***For reference:** During 2017–2025, state bodies and organizations in Namangan Region allocated and financed only 5 state social orders at the expense of the Fund, totaling UZS 1,136,686,000.*

A study of the practice in Namangan Region showed that, based on the requirements of the Regulation “**On the Procedure for Granting State Social Orders by State Bodies for the Implementation of Social and Socially Significant Projects**,” approved by Resolution № 135 of the Cabinet of Ministers dated February 22, 2018, **no established practice of granting state social orders has been formed, and state bodies and organizations in the region have insufficient knowledge of the nature and substance of this mechanism.**

State social orders have been formulated annually by deputies of the regional, district, and city Councils of People's Deputies based on an application submitted by the Namangan Regional Division of the Fund.

The proposals thus formulated were entered into the system by relevant specialists of the secretariats of the regional, district, and city Councils of People's Deputies, in cooperation with responsible officials of the Namangan Regional Division of the Fund. On this basis, the above-mentioned **5 state social orders** were allocated.

***For reference:** In fact, under the Regulation “On the Procedure for Granting State Social Orders by State Bodies for the Implementation of Social and Socially Significant Projects,” approved by Resolution № 135 of the Cabinet of Ministers dated February 22, 2018, the public councils established under state bodies are required to formulate state social orders for each respective state body⁷¹.*

It was established, in accordance with Annex 2, that **a number of foreign countries have positive practices in the allocation and financing of state social orders**, and that these practices can be used to improve national legislation and establish a unified legal practice.

The following are the main problems identified in the allocation and financing of state social orders:

1) There is no unified legislative framework or consistent legal practice governing the allocation of state social orders.

⁷⁰ <https://ngo.gov.uz/>.

⁷¹ Regulation “On the Procedure for Placing a State Social Order by State Bodies for the Implementation of Social and Projects of Social Significance,” approved by Resolution № 135 of the Cabinet of Ministers of the Republic of Uzbekistan dated February 22, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

***For reference:** In **Kazakhstan**⁷², **Germany**⁷³, and **Lithuania**⁷⁴, the mechanism for state support of non-governmental non-profit organizations is regulated by separate legislation.*

2) The practice of allowing citizens and business entities to submit proposals for state social orders has not been established, nor are state social orders allocated separately by category of civil society institution. This, in turn, has resulted in state social orders not being allocated to citizens' self-governing bodies or mass media organizations.

***For reference:** Although there are 1,434 civil society institutions operating in Namangan Region, no state social orders were allocated during 2017–2025 to any of the 52 mass media organizations in the region, including 1 television broadcaster, 39 print publications, and 12 electronic publications, or to any of the 788 citizens' self-governing bodies. In Finland, the provision of separate state social orders for each category of civil society institution is envisaged⁷⁵.*

3) Mechanisms for allocating state social orders at the district, regional, and national levels have not been developed, which, in turn, results in the specific characteristics and needs of the respective territories not being taken into account.

***For reference:** State social orders have been implemented in accordance with the requirements of legislation on public procurement through the **electronic public procurement system** (xarid.uzex.uz). In response to inquiries sent to 25 ministries and agencies, the **Ministry of Preschool and School Education** reported that 1 state social order was awarded in 2023 in the amount of UZS 500.0 million for the Republican Center for Social Adaptation of Children, on the topic "Successful Path to Vocational Training"; the **Ministry of Higher Education, Science and Innovation** reported that 1 state social order was awarded in 2025 in the amount of UZS 350.0 million to the Association of Persons with Disabilities of Uzbekistan, on the topic "Equal Opportunities in Higher Education"; the **Ministry of Justice** reported 5 state social orders totaling UZS 13,618.35 million awarded during 2023–2025; during 2024–2025, the **National Agency for Social Protection** awarded 6 state social orders totaling UZS 3,493,000 million, while the **Agency for Youth Affairs** awarded 8 state social orders totaling UZS 5,165 million. The **Tax Committee** reported that 4 projects totaling UZS 73.260 million were implemented during 2024–2025 from the perspective of social protection, while 9 state bodies reported that they would consider this issue gradually.*

4) Digital solutions for the formulation of projects related to state social orders have not been sufficiently introduced, and there is no system for carrying out procedures related to state social orders through a single integrated platform.

***For reference:** During 2017–2025, state social orders allocated by state bodies and organizations in Namangan Region were entered into the system by the Namangan Regional Division of the Fund based on proposals submitted by deputies of the district, city, and regional Councils of People's Deputies.*

⁷² <https://adilet.zan.kz/kaz/>.

⁷³ <https://www.gesetze-im-internet.de/>.

⁷⁴ <https://www.lrs.lt/>.

⁷⁵ <https://kansalaisyhteiskunta.fi/>.

5) No adequate measures are being taken to ensure the effectiveness of state social orders through social entrepreneurship, which, in turn, hinders the development of the attractiveness of state social orders.

For reference: During 2017–2025, none of the state social orders allocated by state bodies and organizations in Namangan Region was implemented through social entrepreneurship.

6) The sources and procedures for financing state social orders have not been sufficiently defined. As a result, it is not possible to clearly determine when and in what amount the necessary funds from the state budget will be allocated for state social orders.

For reference: During 2017–2025, all state social orders allocated by state bodies and organizations in Namangan Region were financed from the funds of the Fund; however, **there were no projects financed from the extra-budgetary funds of state bodies.**

7) There is no mechanism for public discussion and evaluation of state social orders, which, in turn, results in insufficient public engagement in the implementation of state social orders.

For reference: In **South Korea**, citizens and NGOs submit proposals aimed at addressing social problems, while budget proposals related to social orders are selected through online voting and evaluation by city councils⁷⁶. In the **United States**, each state social order is publicly announced on the relevant platform, and social services (e.g., youth centers and services for older persons) are proposed by citizens or NGOs and financed through local government budgets. NGOs may be selected **without a tender through public voting** (for example, through the PBNYC program in New York City).⁷⁷.

1. **There is no possibility of forming the results of state social orders.**

For information: In 2017–2025, all state social orders allocated by state bodies and organizations in Namangan Region were formed, statistically recorded, and monitored using traditional methods.

2. **There is no public oversight over the formation of projects related to state social orders, the allocation of state social orders, and their implementation.**

For information: In 2017–2025, none of the state social orders allocated by state bodies and organizations in Namangan Region were subjected to public discussion, and public oversight was not established.

3. **A unified digital state oversight system for state social orders has not been established.**

For information: In 2017–2025, a unified digital state oversight system over the state social orders allocated by state bodies and organizations in Namangan Region was not established.

4. **The current tax legislation does not provide for tax incentives for the implementation of state social orders through social entrepreneurship.**

⁷⁶ <https://www.mois.go.kr/ft/a01/ftMain.do>.

⁷⁷ <https://www.grants.gov/>.

For information: In 2017–2025, no tax or other incentives were provided for the implementation of state social orders allocated by state bodies and organizations in Namangan Region through social entrepreneurship.

In order to address these systemic problems through the available resources and to establish an effective mechanism for the allocation and financing of state social orders based on advanced foreign experience, the following measures are proposed:

1. To establish a working group consisting of representatives of the chambers of the Oliy Majlis, the Ministry of Justice, the Ministry of Economy and Finance, the Public Fund for Support of Civil Society Institutions under the Oliy Majlis (hereinafter referred to as the Fund), local executive authorities, the Center for Analysis of Democratic Processes, the National Association of Non-Governmental Non-Profit Organizations of Uzbekistan, the Association of Mahallas of Uzbekistan, and the Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan.

2. To designate as the principal task of the working group the development and submission to the Administration of the President of the Republic of Uzbekistan of a draft Decree of the President of the Republic of Uzbekistan aimed at further improving the allocation of state social orders in the Republic of Uzbekistan, providing for the following:

1) taking into account advanced foreign experience and the specific characteristics of state social orders, to establish a simplified unified procedure for the allocation and financing of state social orders by consolidating the provisions concerning the allocation and financing of state social orders contained in the Laws of the Republic of Uzbekistan “On Guarantees of the Activities of Non-Governmental Non-Profit Organizations” and “On Social Partnership” and Resolution № 135 of the Cabinet of Ministers dated 22 February 2018, and by directly regulating the relevant social relations in the Law “On Social Partnership”;

2) to establish a unified procedure for financing state social orders as follows:

a) the main portion of the project cost shall be financed from the Fund's resources, with equal distribution — for projects at the national level, from the extra-budgetary funds of the state body, and, with equal distribution — for projects at the district and regional levels, from the local budget funds at the respective level;

b) to accumulate funds allocated for state social orders in a separate account of the Fund and exercise control over them;

3) to establish the following practice for the formation of state social orders: citizens and deputies of Councils of People's Deputies, having passed through the Unified Identification System and Face ID, as well as business entities, civil society institutions, state bodies and organizations, through electronic digital signatures, shall formulate their proposals on a single specialized platform administered by the Fund;

proposals shall be formed by types of civil society institutions, namely non-governmental non-profit organizations, mass media, and citizens' self-government bodies, at the district, regional and national levels;

compliance of the proposals with the criteria established for state social orders, as well as their proper formation by types of civil society institutions and at the district, regional and national levels, shall be verified by justice bodies and referred for public discussion;

during the public discussion, citizens shall vote according to the principle of “one vote for one project” after passing through the Unified Identification System;

based on the results of the public discussion, taking into account the types of civil society institutions, one winning project related to state social orders at each of the district, regional and national levels, as well as candidates for implementation of such projects selected through a competitive process, shall be evaluated by members of the Parliamentary Commission under the Oliy Majlis on the platform, and, based on the results of such evaluation, referred to the relevant state body depending on the level of financing;

4) to introduce a procedure whereby the Parliamentary Commission under the Oliy Majlis determines the winners of projects and competitions through evaluation on the platform after passing through the Unified Identification System and FACE ID;

5) to establish public and state oversight, through the platform, over all stages of the allocation and financing of state social orders, public discussion of projects and the conduct of competitions, conclusion of direct contracts, and implementation of state social orders under contracts;

6) to grant the Ministry of Justice the authority to exercise unified state oversight over state social orders;

7) to establish specific deadlines for the allocation and financing of state social orders;

8) to provide that civil society institutions whose founders or heads have an unexpunged conviction as established by legislative acts, or who have been criminally prosecuted for corruption-related crimes, terrorism, or legalization of proceeds of crime, shall be prohibited from participating in competitions and shall not be permitted to become winners based on the results of such competitions;

9) with the aim of supporting social entrepreneurship, to provide tax and other incentives to entities that participate with additional funding and services in the allocation of state social orders on the basis of social partnership jointly with civil society institutions.

2.2-§. Establishing a Clear Mechanism for Interaction between Non-Governmental Non-Profit Organizations and Local Executive Authorities and Councils of People's Deputies

Defining a mechanism for interaction between non-governmental non-profit organizations and local executive authorities and Councils of People's Deputies is of particular relevance today.

At present, **2,352** legislative acts concerning the activities of non-governmental non-profit organizations have been adopted, including **271 laws**, **251 decrees** and **426 resolutions** of the President of the Republic of Uzbekistan, as well as other regulatory legal acts⁷⁸.

Article 20¹ of the Law of the Republic of Uzbekistan “On Local State Authority” contains general provisions concerning the cooperation of Councils of People's Deputies with non-governmental non-profit organizations, while Article 21¹ contains general provisions concerning the cooperation of khokimiyats with non-governmental non-profit organizations⁷⁹.

***For information:** The above-mentioned Law provides that Councils of People's Deputies cooperate with non-governmental non-profit organizations and, in accordance with legislative acts, support their activities; cooperate with non-governmental non-profit organizations on matters concerning the development of draft territorial programs and draft decisions of the Councils, as well as in exercising oversight over their implementation; and that the khokim also resolves other matters, including cooperation with enterprises, institutions and organizations of various forms of ownership within the scope of his or her powers as established by legislation.*

However, the current legislative acts do not clearly and sufficiently establish the mechanisms for implementing such cooperation.

Upon examining the state of such cooperation in Namangan Region, it was established that **in Namangan Region, no documents providing for the implementation of cooperation between local executive authorities and Councils of People's Deputies, on the one hand, and non-governmental non-profit organizations, on the other hand, have been adopted, and that procedures and measures for jointly addressing issues related to the activities of state and non-governmental bodies through programs and other measures have not been established.**

Upon examining the reasons for the absence and lack of systematic establishment of such cooperation, it was found that, due to the insufficient regulation in legislative acts of the procedures for establishing cooperation between them, there are a number of problems and shortcomings preventing them from systematically implementing such cooperation, including:

1) No state social orders have been allocated by state bodies and organizations located in the region from their own funds, and even issues concerning social and socially significant projects have not been addressed by the public councils established under them.

⁷⁸ lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁷⁹ The Law of the Republic of Uzbekistan “On Local State Authority” dated September 2, 1993, № 913-XII // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

For information: Pursuant to Decree № DR–124 of the President of the Republic of Uzbekistan dated 26 August 2024 “On Measures to Further Improve the System of State Support for Civil Society Institutions,” ministries and agencies are required to organize, on an annual basis, competitions for awarding social orders to civil society institutions from their extra-budgetary funds⁸⁰, and, pursuant to the Regulation “On the Procedure for Granting State Social Orders by State Bodies for the Implementation of Social and Socially Significant Projects,” approved by Resolution № 135 of the Cabinet of Ministers dated 22 February 2018, state bodies are required to annually organize competitions for directly awarding state social orders to non-governmental non-profit organizations from extra-budgetary funds for the implementation of social and socially significant projects, as well as to provide in their expenditure estimates for extra-budgetary funds for the amount of funds allocated for the direct granting of state social orders⁸¹. However, in Namangan Region, the expenditure estimates for the extra-budgetary funds of state bodies and organizations did not in practice provide for the necessary funds for this purpose, and no competitions were organized.

2) No decisions have been adopted by local executive authorities and the regional, district, and city Councils of People's Deputies concerning support for the activities of non-governmental non-profit organizations.

For information: Pursuant to the Law of the Republic of Uzbekistan “On Non-Governmental Non-Profit Organizations” № 763-I dated April 14, 1999, **the state** ensures compliance with the rights and legitimate interests of non-governmental non-profit organizations and creates equal legal opportunities for their participation in public life. The state may provide support for individual socially beneficial programs of non-governmental non-profit organizations⁸².

However, although **54,281** decisions of local executive authorities of the Namangan Region have been adopted and entered into the “**e-qaror**” unified electronic system⁸³, and **645** decisions of the Councils of People's Deputies of the Namangan Region have been adopted and entered into the “**kengash.gov.uz**” portal of local representative bodies⁸⁴, no necessary decisions aimed at supporting the activities of non-governmental non-profit organizations have been adopted.

3) There is no accurate statistical data on non-governmental non-profit organizations;

For information: According to the information provided by the Statistics Department of Namangan Region, there are currently **2,456** non-governmental non-profit organizations operating in the region, whereas, according to the information provided by the Namangan Regional Department of Justice, their number is **611**.

4) The majority of non-governmental non-profit organizations, including even those performing important and strategic functions, do not have their own premises, and local executive authorities and Councils of People's Deputies have not paid sufficient attention to this issue;

For information: Only **25** of the total number of non-governmental non-profit organizations in the region have their own premises, while the remainder operate on the basis of

⁸⁰ Decree № DP–124 of the President of the Republic of Uzbekistan dated August 26, 2024, “On Measures to Further Improve the System of State Support for Civil Society Institutions” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁸¹ Regulation “On the Procedure for the Provision of State Social Orders by Public Authorities for the Implementation of Socially and Publicly Significant Projects,” approved by Resolution № 135 of the Cabinet of Ministers of the Republic of Uzbekistan dated February 22, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁸² Law № 763-I of the Republic of Uzbekistan dated April 14, 1999, “On Non-Governmental Non-Profit Organizations” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁸³ <https://e-qaror.gov.uz/>.

⁸⁴ <https://kengash.gov.uz/>.

lease agreements. At the same time, the Councils of People's Deputies adopted a total of 7,948 decisions during 2017–2025. Of these, 1,558 decisions concerned information, 4,238 concerned reports, and 1,942 concerned other matters.

5) Local executive authorities and Councils of People's Deputies have not provided support for the material and technical infrastructure of non-governmental non-profit organizations.

For information: The level of depreciation of the material and technical infrastructure of non-governmental non-profit organizations in Namangan Region amounts to **50 percent**. Although it is itself a non-governmental non-profit organization, during 2024–2025, the Public Fund for Support of Civil Society Institutions under the Oliy Majlis of the Republic of Uzbekistan and its Namangan Regional Division assisted other non-governmental non-profit organizations in purchasing **25,000** units of computer equipment.

6) Financial resources are insufficient for the day-to-day activities of non-governmental non-profit organizations, and local executive authorities and Councils of People's Deputies have not carried out systematic joint activities in this regard.

For information: Financial resources are insufficient to ensure the day-to-day operations of non-governmental non-profit organizations, and social protection is scarcely provided to their employees. Although the application of labor legislation is established in the activities of non-governmental non-profit organizations operating in the region, the lack of funds even for sick leave and annual leave has resulted in staff turnover within non-governmental non-profit organizations and has created problems in the formation of a personnel reserve.

7) Modern mechanisms for implementing social partnership and public oversight have been introduced, and although a separate electronic portal was launched in 2022, the following activities have not been implemented at all:

a) participation of non-governmental non-profit organizations and other civil society institutions (hereinafter referred to as NPOs) in the development of social and economic programs and monitoring of their implementation;

b) submission to the responsible state bodies and organizations, based on the results of monitoring, of documents that are subject to mandatory consideration, as well as proposals concerning draft normative legal acts;

c) submission of proposals by NPOs or state bodies and organizations regarding the establishment of social partnership relations;

d) submission by NPOs of documents prepared based on the results of public oversight to state bodies and organizations, as well as publication of decisions adopted by state bodies and organizations based on the results of consideration of such documents.

For information: The implementation of Resolution № 208 of the Cabinet of Ministers of the Republic of Uzbekistan dated April 22, 2022, “On Measures to Further Improve the Mechanisms for Implementing Social Partnership and Public Oversight”⁸⁵ is not being adequately ensured in the region, **and prosecutorial oversight in this regard has not been carried out.**

8) The role and participation of representatives of non-governmental non-profit organizations in the activities of public councils established under state bodies and organizations located in Namangan Region are insufficient;

⁸⁵ Resolution № 208 of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Further Improve the Mechanisms for Implementing Social Partnership and Public Oversight” dated April 22, 2022 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

For information: Pursuant to Decree № PF–6181 of the President of the Republic of Uzbekistan dated March 4, 2021, “On Approval of the Concept for the Development of Civil Society in 2021–2025,” it was established that **at least 50 percent** of the composition of public councils under state bodies shall consist of representatives of non-governmental non-profit organizations⁸⁶.

However, representatives of non-governmental non-profit organizations do not constitute **50 percent** of the composition of the public councils established by state bodies and organizations in Namangan Region. Moreover, the public councils have been established merely formally, with their members consisting of the head of the respective state body or his/her deputy and employees of the existing structural divisions. Furthermore, no Public Council has been established under the Namangan Regional Hokimiyat.

During the period that has elapsed since the adoption of the above-mentioned Decree, no legal enforcement measures have been taken by **prosecutorial oversight authorities or justice bodies** to ensure compliance with the requirements of the Decree.

9) The number of offenses related to the activities of non-governmental non-profit organizations has increased due to insufficient support from state bodies for their activities and the inadequate organization of legal awareness and outreach activities;

For information: Offenses related to the activities of non-governmental non-profit organizations mainly consist of the failure of non-governmental non-profit organizations to submit reports in a timely manner and the failure to issue certificates of temporary incapacity for work to their employees. In particular, regarding the failure of non-governmental non-profit organizations to submit reports in a timely manner, there were **32 cases** in 2023 and **97 cases** in 2024; for violations of labor legislation requirements, there were **10 administrative penalties** in 2023 and **14 disciplinary penalties** in 2024, while in the first quarter of 2025, the issue of initiating **1 criminal case** was raised.

10) Digital cooperation between non-governmental non-profit organizations and state bodies has not been established; at the same time, the existing information systems in the region have not been fully integrated, and no opportunity has been created for the head of the region, at the level of district, city, and regional hokimiyats, as well as for the Councils of People's Deputies at the district, city, and regional levels, to access all available information resources from a single point through a unified information system, which has resulted in a number of negative consequences.

For information: There are **39 state information systems** in Namangan Region; however, no opportunity has been created for non-governmental non-profit organizations to access and use them. The “**E-Kengash**” **electronic system** used by the Councils of People's Deputies and the “**E-qaror**” **unified electronic system** used by local executive authorities are currently **integrated with only 6 information systems**, while they have still **not been integrated with the information systems of non-governmental non-profit organizations operating in the region**. For example, the following platforms related to the “mahalla seven” have not been integrated with the “**Unified Migration Data Base**”, despite the fact that the data contained in these information systems are of significant importance for addressing migration-related issues:

1) Digital Mahalla Platform – contains the key demographic indicators of each mahalla, accessible to the chairpersons of the respective mahallas⁸⁷;

⁸⁶ Decree № DP–6181 of the President of the Republic of Uzbekistan “On Approval of the Concept for the Development of Civil Society in 2021–2025” dated March 4, 2021 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁸⁷ <https://mahalla.ijro.uz/>.

2) **Online Mahalla Platform** – contains information accessible to the assistant hokim responsible for the respective mahalla on loans and subsidies allocated to citizens, household plots, migration, micro-projects, and other information arising from the assistant's principal functions⁸⁸.

3) **Khotin-qizlar.uz Platform** – contains information on women over 30 years of age in the respective mahalla, accessible to the mahalla women's affairs activists, as well as information on citizens included in the "Women's Register" and the assistance provided to them⁸⁹;

4) **Yoshlar balansi.uz Platform** – contains information accessible to youth leaders in the respective mahalla on the registration of young people in the "Youth Register", their migration, measures to ensure youth employment, and other relevant areas⁹⁰;

5) **IHMA.UZ Platform** – contains information on 105 types of applications and cases managed by social workers, is specialized in monitoring citizens who have found themselves in difficult social circumstances, and contains information on persons with disabilities⁹¹.

Furthermore, local leaders and responsible officials still do not have digital solutions for addressing existing problems through timely, sufficiently complete, and prompt access to the necessary data and information resources. For example:

Due to the fact that non-governmental non-profit organisations do not have their own information systems or do not have full access to state information systems, incoming appeals concerning their activities are forwarded by the People's Reception Offices to the district, city and regional hokimiyats, and the respective hokimiyats then forward the appeals in paper form to the relevant non-governmental non-profit organisations according to their jurisdiction. As a result, excessive time and resource expenditure has arisen in the hokimiyats, and problems have emerged with the timely consideration of appeals;

As another example, during 2017–2025, **9,082** appeals containing requests for information were submitted to the regional, district and city hokimiyats of Namangan Region, and in Yangiurgan District alone, **more than 15,000 appeals concerning legal clarification** were submitted. Although these appeals did not fall within the jurisdiction of the regional, district and city hokimiyats, due to the lack of an opportunity to promptly forward the appeals electronically to the organisations within the relevant territory, the appeals were not sent directly in electronic form to the competent authorities but were submitted through the People's Reception Offices to the regional, district and city hokimiyats, which then forwarded the appeals to the competent authorities in paper form according to their jurisdiction.

11) No communication has been carried out on issues concerning the activities of civil society institutions, including non-governmental non-profit organisations, or issues affecting citizens through the "Hokim Appeal" module developed on the basis of the "Ijro.gov.uz" unified interdepartmental electronic system for executive discipline.

For reference: Based on the instruction № 03-2309 of 03.12.2024 of the Administration of the President of the Republic of Uzbekistan, a Temporary Regulation on the procedure for district (city) hokims to register for meetings with heads of ministries and agencies, directly address them, and the consideration of such appeals was approved. Pursuant to this Regulation, the procedure

⁸⁸ <https://online-mahalla.uz/>.

⁸⁹ <https://xotin-qizlar.uz/>.

⁹⁰ <https://yoshlarbalansi.uz/>.

⁹¹ <https://ihma.uz/oz>.

was established for heads of local executive authorities to register for meetings with the relevant heads of ministries and agencies, directly address them, and have such appeals considered through the “Hokim Appeal” module of the “Ijro.gov.uz” unified interdepartmental electronic system for executive discipline. Based on the above, a total of 18 communications were held via the Zoom platform with the participation of district (city) hokims and heads of ministries and agencies, and 21 issues were raised by the hokimiyats of cities and districts in Namangan Region, of which 7 were positively resolved and 14 were under consideration; however, issues falling within the subject matter of public oversight were not resolved.

12) Due to the lack of clearly defined functions between the public and non-governmental sectors, the role and significance of the Councils of People's Deputies as the most important link between them have not been sufficiently established, resulting in the decisions adopted by them not being effectively and fully implemented.

For reference: In 2021–2025, a total of **838 sessions** were held by the Councils of People's Deputies of Namangan Region, cities and districts, and **7,948 decisions** were adopted. In order to ensure their implementation, **7,273 decisions** were sent to the relevant state bodies and organisations in the territory for execution; however, **174 decisions** were not implemented or were disregarded by these state bodies and organisations. As a result, a negative practice has emerged whereby issues raised and resolved at previous sessions are included in the agendas of subsequent sessions.

13) The role and significance of non-governmental non-profit organisations in the implementation of public administration by local executive authorities and Councils of People's Deputies are of particular importance, and the experience of advanced foreign countries demonstrates that the state may implement, precisely through the non-governmental sector, those important tasks undertaken before the people which the state is unable to implement through state bodies.

For reference: The Namangan Regional Division of the Association of Neighborhoods of Uzbekistan has developed the practice of establishing public registers in **788** citizens' self-governing bodies and entering them by name into the “Ombor daftar” system in the area of organising public oversight. During the past period, public oversight was ensured at **568** facilities, including the implementation of normative documents concerning the resolution of everyday problems of the population at **27** facilities, electricity supply at **79** facilities, gas supply at **25** facilities, water supply at **38** facilities, road infrastructure at **99** facilities, education at **18** facilities, the healthcare system at **34** facilities, and other areas at **253** facilities. In addition, forms of public oversight were applied in **406** cases, including the submission of appeals and requests to state bodies in **61** cases, participation in open collegial meetings of state bodies in **37** cases, public discussions in **98** cases, public hearings in **52** cases, and public monitoring in **158** cases. The Namangan Regional Division of the “Yuksalish” Movement conducted **20** public monitoring activities in 2022, **16** in 2023, **41** in 2024, and **27** in 2025; **2** public hearings in 2022, **3** in 2023, **3** in 2024, and **4** in 2025; **4** public discussions in 2022, **1** in 2023, and **9** in 2024; **25** public dialogues in 2022, **1** in 2023; **2** collective appeals in 2024; **1** public project in 2023 and **1** in 2024; **1** open dialogue and **1** discussion meeting in 2024.

In this regard, extensive work has been carried out over the past period on the allocation of state social orders, establishment of public councils, and support for the activities of non-governmental non-profit organisations, and there has arisen a need to systematically define the specific role and significance of non-governmental non-profit organisations in the implementation of public administration by local

executive authorities and Councils of People's Deputies by ensuring the continuity of these reforms and the consistency of the ongoing reforms.

Upon studying the experience of foreign countries in determining a specific mechanism for the interaction of non-governmental non-profit organisations with local executive authorities and Councils of People's Deputies, the following was identified:

1) Regarding the determination of the procedure and areas of interaction between non-governmental non-profit organisations and local executive authorities and Councils of People's Deputies:

For reference: In the United Kingdom, Estonia and Poland, through institutional mechanisms such as Local Compact, round-table and Cooperation Programme, bilateral agreements and unified programmes are established between local authorities and non-governmental non-profit organisations, and, on the basis of these documents, municipalities in each territory carry out cooperation with non-governmental non-profit organisations under a unified document⁹²;

2) In the following areas:

a) For regional, district and city hokimiyats, to create the possibility of obtaining, analysing and accessing the necessary information resources in an automated manner, without human intervention, regarding the state of development of each sector and field in the territory, as well as the public, non-governmental and private sectors, existing problems and achievements, as well as the criminogenic situation and the state of crime:

b) In order to ensure the targeted and proper use of budgetary funds and establish systematic operations, abandoning the unified electronic “E-qaror” system and creating the technical capability through the “Ijro.gov.uz” unified interdepartmental electronic system for executive discipline to, **from a single point,** enable regional, district and city hokimiyats to keep an account of the work being carried out by all state bodies and organisations in the territory, issue necessary instructions to them, monitor their “*execution steps*” in real time, and publish adopted decisions;

For reference: In the United States, through the Mayor's Office of Data Analytics (MODA) and NYC Open Data systems, more than 2,000 datasets from more than 100 agencies are integrated in real time; Hate Crime, 911, sanitation, and customs data are displayed on a single dashboard; in conjunction with “CompStat” weekly crime statistics, police patrol routes are automatically generated; through the “WindyGrid” system, more than 7 million real-time geospatial records, 911, transportation, weather, ShotSpotter, and LPR data are displayed on a single geospatial map, thereby enabling the head of the territory, as well as the head of state, to obtain accurate information in real time on the state of each sector, field and area within the territory, analyse the data, issue necessary instructions, and monitor in real time the status of implementation of those instructions⁹³; In the United Kingdom, under “One Platform, One Council”, data from more than 300 state bodies and organisations is automatically received and systematised through a “Modern Data Platform” based on Microsoft Azure⁹⁴. In Singapore, the Smart Nation Sensor Platform provides the capability to obtain and analyse information on all information resources in the state and to make accurate and effective decisions⁹⁵; In Estonia, the

⁹² <https://www.gov.uk/>.

⁹³ <https://opendata.cityofnewyork.us/>.

⁹⁴ <https://www.gov.uk/>.

⁹⁵ <https://www.smartnation.gov.sg/>.

*X-Road and MinuOmavalitsus.ee systems provide the capability to obtain the results of 99% of state services, tasks and functions*⁹⁶.

3) In the following areas related to implementing unified digital cooperation between the public and non-governmental sectors:

a) to implement cooperation between non-governmental non-profit organizations and local executive authorities and Councils of People's Deputies, reflect the results thereof in the **“Public Oversight Portal” unified information system**, fully establish its operation, and integrate it with the **“Ijro.gov.uz” unified interagency electronic system for executive discipline**;

b) to establish the technical capabilities for reflecting the results of issuing certificates of temporary incapacity for work to employees of non-governmental non-profit organizations on the Public Oversight Portal;

d) to establish the practice of entering the results of the daily, monthly, quarterly, and annual activities carried out by each non-governmental non-profit organization on the Public Oversight Portal;

e) to unify the monthly reports submitted by non-governmental non-profit organizations to tax, statistical, and justice authorities and **establish the practice of submitting a single annual report through the Public Oversight Portal**, except for reports on projects implemented with the support of state and foreign organizations;

In Tanzania, through the *NGO Digital Mapping platform*, *in Ghana*, through the *Ghana Open Data Initiative (GODI)*, *in the European Union*, through the *Joinup platform*, and *in Estonia, Benin, Kyrgyzstan, and Ukraine*, through the *X-Road system*, **the public and non-governmental sectors carry out digital cooperation with each other from a single point using one platform**. In these systems and platforms, information on the daily, weekly, quarterly, and annual activities of the non-governmental sector, its tasks carried out in cooperation with the public sector, and the results thereof is maintained in real-time.

4) In the following areas related to establishing systematic cooperation between the public and non-governmental sectors and its financing:

a) to **grant the Councils of People's Deputies** the authority to approve unified annual cooperation programmes concluded between civil society institutions and public authorities within the respective territory, thereby establishing a unified system of cooperation between the public and non-governmental sectors in the territory;

b) **in terms of granting regional, district, and city mayors the authority to make decisions on supporting the socio-economic activities of civil society institutions from additional funds of the local budget:**

For information: In the United Kingdom, cooperation between civil society institutions, including non-governmental non-profit organizations, is based on an agreement, which provides for the financing of the non-governmental sector, mutual exchange of reports, and opportunities for mutual assessment of activities⁹⁷; *In Poland*, unified working groups have been established at the regional level with the participation of representatives of public authorities and non-governmental non-profit organizations, on the basis of which a Cooperation Program has been developed and approved by city councils, and the allocation of funds from the local budget in the

⁹⁶ <https://minuomavalitsus.ee/>.

⁹⁷ <https://www.gov.uk/>.

form of grants to non-governmental non-profit organizations has been established⁹⁸. **In Croatia**, based on the national action plan, **14% of the taxes generated from risk-based games** is allocated for the cooperation and support provided by the non-governmental sector to the public sector⁹⁹.

5) regarding establishing administrative liability for failure to comply with, or improper compliance with, decisions adopted based on the results of Council inspections, and granting the Councils of People's Deputies the authority to draw up an administrative report against the offender and submit it to the court:

For information: In Latvia, administrative commissions or self-government commissions, heads of local executive authorities, and administrative inspectorates have the right to draw up administrative reports and submit them to the court in cases of violations of the law arising within their respective areas of activity¹⁰⁰.

In order to clearly define the mechanism for cooperation between non-governmental non-profit organizations and local executive authorities and Councils of People's Deputies:

1. To establish a Working Group consisting of representatives of the Ministry of Justice, the Ministry of Digital Technologies, the Ministry of Economy and Finance, the Ministry of Health, the Tax Committee, the Statistics Agency, the Senate of the Oliy Majlis, local executive authorities of the region, and Councils of People's Deputies, the Institute of Legislation and Legal Policy, and the Public Fund for Support of Civil Society Institutions under the Oliy Majlis, for the purpose of improving legislation to clearly define the mechanism for cooperation between non-governmental non-profit organizations and local executive authorities and Councils of People's Deputies;

2. To develop a draft legislative act and provide therein for the following:

1) to adopt a normative legal act providing for a clear definition of the procedure and areas of cooperation between non-governmental non-profit organizations and local executive authorities and Councils of People's Deputies, and, as an annex to this legislative act, in order to ensure systematic implementation of mutual cooperation:

a) to grant **regional, district, and city mayors** the authority to make decisions on supporting the socio-economic activities of civil society institutions from additional funds of the local budget;

b) to include provisions aimed at establishing a unified system of cooperation between the public and non-governmental sectors in the territory by granting **Councils of People's Deputies** the authority to approve unified annual cooperation programmes concluded between civil society institutions and public authorities within the respective territory;

to implement the **“Digital and Smart Territory”** project by fully and gradually integrating the existing **39** information systems in Namangan Region, thereby creating the possibility for **regional, district, and city khokimiyats** to obtain and analyze, in an automated manner without human intervention, information on the state of development of every sector and field in the territory, as

⁹⁸ <https://isap.sejm.gov.pl/>.

⁹⁹ <https://zaklada.civilnodrustvo.hr/>.

¹⁰⁰ <https://likumi.lv/>.

well as the development status of the public, non-governmental, and private sectors, existing problems and achievements, and the criminogenic situation and state of crime, and to access the necessary information resources;

2) in order to ensure the targeted and proper use of budget funds, establish systematic operations, and implement the **“Digital and Smart Territory”** project, to discontinue the use of the “E-qaror” unified electronic system, transfer its tasks and functions to the “Ijro.gov.uz” unified interagency electronic system for executive discipline, and launch its **updated version** by introducing artificial intelligence technologies therein and creating, **from a single point**, the technical capability for regional, district, and city khokimiyats to maintain an overall record of the activities carried out by all public authorities and organizations in every sector, field, and area within the territory, issue necessary instructions to them, monitor their **“implementation steps”** in real time, and publish adopted decisions;

3) to establish and fully operationalize the **“Public Oversight Portal” unified information system** for implementing the activities of non-governmental non-profit organizations and their cooperation with local executive authorities and Councils of People’s Deputies, reflecting the results thereof therein, and to integrate it with the “Ijro.gov.uz” unified interagency electronic system for executive discipline;

4) to unify the monthly reports submitted by non-governmental non-profit organizations to tax, statistical, and justice authorities and **establish the practice of submitting a single annual report through the Public Oversight Portal**, except for reports on projects implemented with the support of state and foreign organizations;

5) to fully establish the “Ijro.gov.uz” unified interagency electronic system for executive discipline in the activities of public authorities and organizations, and, for non-governmental non-profit organizations possessing important information infrastructure that have assisted in the implementation and technical support of this system, to provide an effective solution for electronic document management between public and non-governmental organizations by introducing the “Ijro.gov.uz” unified interagency electronic system for executive discipline free of charge;

6) to permit non-governmental non-profit organizations to engage in commercial activities for the purpose of assisting in the sale and marketing of products manufactured by individual entrepreneurs and to establish that the profit derived by a non-governmental non-profit organization from such activities shall not constitute an object of taxation;

to establish administrative liability for failure to comply with, or improper compliance with, decisions adopted based on the results of Council inspections and to grant Councils of People’s Deputies the authority to draw up an administrative report against the offender and submit it to the court.

As a result of the proposals aimed at clearly defining the mechanism for cooperation between non-governmental non-profit organizations and local executive authorities and Councils of People’s Deputies through advanced foreign experience and existing resources, the following will be achieved:

First, the mechanism for cooperation between non-governmental non-profit organizations and local executive authorities and Councils of People's Deputies, as well as a unified procedure for establishing cooperation between local executive authorities, Councils of People's Deputies, and non-governmental non-profit organizations, including their respective rights and obligations and liability in this area, will be clearly defined;

Second, accurate and real statistics will be established regarding the exact number of projects being implemented or having been implemented in each territory through cooperation between the public and non-governmental sectors, existing problems and specific proposals for their resolution, as well as the achievements attained;

Third, a mechanism will be created whereby the mayor, as the head of the territory, can maintain an accurate overall record of the activities being carried out by every public authority and organization, as well as by the non-governmental and private sectors within the territory, correctly identify existing problems, and effectively eliminate them;

Fourth, through the “**Digital and Smart Territory**”, the real situation in the territory for each sector, field, and area will be available at a single point, a digital geoplatform will be created, and accurate factual information will be generated regarding the actual implementation of the most important tasks assigned by the Head of State;

Fifth, cooperation between public authorities and non-governmental organizations will enter a new stage, and an effective solution will be created for the public sector and non-governmental sector to jointly and systematically resolve existing problems;

Sixth, budgetary expenditures and paper consumption will be reduced, and electronic document management through a single point will be established in the territory;

Seventh, systematic measures will be implemented to ensure the effective implementation of decisions and instructions of local executive authorities and Councils of People's Deputies, thereby raising to a new level the achievement of public satisfaction with public authorities.

2.3-§. Legal, Organizational and Digital Foundations for Improving the Mahalla Governance System

Improving the mahalla governance system can contribute not only to the expansion of infrastructure, but also to the comprehensive socio-economic development of territories. However, in practice, the mahalla governance system faces the following complex problems, in particular:

1. The number of information systems and modules introduced for the activities of the members of the “Mahalla Seven” is excessively large; they are not integrated with one another; inter-agency correspondence is still conducted using traditional methods; processes related to the provision of necessary information are based on bureaucracy or personal connections; unnecessary administrative obstacles in obtaining the necessary information still exist; and the necessary measures to preserve records of the provision of the information submitted are not being taken.

For information: The number of information systems introduced for the activities of the members of the “Mahalla Seven” is 12; however, none of them are fully integrated with one another. Members of the “Seven” obtain information using traditional methods. These information systems have an average of 19 to 54 modules, and due to the large number of modules in the interface, in some cases it is very difficult to read the modules. At present, there is a need to integrate 520 information systems with one another.

2. The members of the “Mahalla Seven” continue to use paper-based document exchange due to the complexity of the information systems introduced into their activities and problems with the exchange of information between them, the very low level of computer literacy of employees in practice, the fact that none of them fully understands the capabilities of the information systems related to their activities, insufficient efforts for self-development, the failure of agencies coordinating the activities of the “Mahalla Seven” to take the necessary measures in this area, insufficient effective measures to improve employees’ skills in using digital platforms, and the absence of digital state and public oversight mechanisms in this area. There are even negative instances in which, when there is insufficient paper, paper is purchased using their own funds or those of the population. As a result, when paper consumption was calculated within the 32 mahallas provided for examination out of 776 mahallas, and the average price of one ream of paper was estimated at 100,000 soums when purchased electronically, it was determined that, with an average consumption of 28 reams of paper per month for one mahalla, approximately **89,600,000 soums** are being directed toward unjustified paper consumption per month, and **1,075,200,000 soums** per year.

For information: When the 12 information systems introduced for the activities of the “Mahalla Seven” and their files in 776 mahallas in Kashkadarya Region alone were examined, it was established that acts, certificates, minutes, decisions, plans, reports, various tables, letters, documents related to the activities of the “Mahalla Seven”, and other documents are still being prepared on paper using a pen. Although there is an opportunity to prepare these documents through the **EDO.IJRO.UZ Interagency Electronic System for Executive Discipline**¹⁰¹, and to obtain “reports” and “tables” from the relevant agency through digital cooperation without paper

¹⁰¹ <https://edo.ijro.uz/>.

consumption, paper-based document exchange is still being maintained. It was also established that paper-based document exchange has intensified in certain divisions of the Kashkadarya Regional Territorial Division of the Association of Mahallas of Uzbekistan.

1. The majority of the data introduced into the activities of the “mahalla seven” does not correspond to reality and consists of erroneous and inaccurate information. According to the members of the “mahalla seven”, the reasons for the emergence of such data are *the failure to enter data in a timely manner due to the excessive workload, “table-making”, “report-making”, insufficient digitalization skills, the need for a person similar to a secretary, and, most importantly, the lack of inter-agency digital cooperation, the fact that accurate information is obtained from citizens’ relatives by telephone and, consequently, reliance on what they say, insufficient time and resources to verify the authenticity of the information, and, in some cases, the failure of a member of the “mahalla seven” who possesses the information to provide the necessary information to another member, hiding it or providing incorrect information.*

For information: *When the data in the “Raqamli mahalla” unified platform introduced into the activities of citizens’ assemblies and the “Online mahalla” information system introduced into the activities of the assistant to the hokim were examined, it was established that, apart from the data obtained through inter-agency digital cooperation, up to 90 percent of the data filled in traditionally and collected traditionally consisted of erroneous and inaccurate information that had no legal basis.*

2. The material and technical facilities and workplaces of the members of the “mahalla seven” do not meet the required standards. The agencies coordinating the activities of the members of the “mahalla seven” have not taken effective measures in practice to ensure that their material and technical facilities are at the required level, the members of the “mahalla seven” do not sufficiently know to whom and how to apply regarding their material and technical facilities, and the necessary measures in this regard are not being taken at the required level.

For information: *The computer of the chairman of the “Oqsaroy” MCY is completely unusable, and it is impossible to read the information displayed on the monitor; the members of the “mahalla seven” sit in one place; the members of the “Bo’shqo‘ton” MCY sit in a school building, in only two rooms; more than 60 percent of the 32 mahallas do not have a separate hall for organizing meetings with citizens; tablets have not been fully allocated, and 30 percent of the tablets are broken, do not work, or their use is limited due to other technical reasons.*

6. The daily attendance of the members of the “mahalla seven” established on the “Raqamli mahalla” unified platform is not sufficiently maintained, and the issue of paying the monthly salary of the “mahalla seven” based on its daily attendance has not been sufficiently organized;

7. It was established that, in order for the mahalla to actually become a strong support bridge between the population and the state, it is necessary to resolve a number of the following issues, in particular:

ensuring that the members of the “mahalla seven” are personnel with higher education;

establishing a professional development and attestation system on “smart mahalla governance” in order to properly organize the vertical and horizontal management of the members of the “mahalla seven”;

increasing the computer literacy and skills of the members of the “mahalla seven” in using existing platforms through their obtaining international and local IT certificates;

developing a comprehensive information system based on all information systems used by the “mahalla seven”, transforming it into a platform providing services to the population, thereby reducing citizens’ appeals, and applying artificial intelligence technologies to it;

introducing amendments and additions to certain legislative documents in connection with the establishment of the “Smart Mahalla Governance” system;

granting the “mahalla seven” permission to provide electronic public services and thereby ensuring its proximity to the population and creating an opportunity to strengthen its material and technical facilities;

implementing socio-political measures by increasing the share of appeals resolved with the assistance of the “mahalla seven” in relation to the total number of appeals and transferring 70 percent of appeals to the lower level;

increasing public trust in state bodies by allocating state social orders to mahallas and taking effective measures to further develop existing infrastructure;

increasing the share of cases in which the measure of restraint of placing an accused or defendant under the guarantee of the “mahalla seven” is selected in relation to existing criminal cases, and taking effective measures to ensure the protection of its citizens and their law-abiding conduct by increasing the number of petitions of the “mahalla seven” for the conditional early release of a convicted person from punishment or replacement of the punishment with a lighter one in relation to crimes committed within the territory of the respective mahalla;

bringing the daily attendance of the members of the “mahalla seven” to 100 percent by establishing working hours from 09:00 to 18:00 for attendance (timesheet) regarding the arrival at and departure from work of the members of the “mahalla seven”, forming a clear list of valid reasons, establishing the employee’s working time as 8 hours per day when working hours are transferred to flexible working hours, and linking all of this to the monthly salary of the members of the “mahalla seven”;

organizing close work between the mahalla and the population by bringing the level of studying the economic and social condition and needs of families to 100 percent, and organizing the daily field-based study of the problems of the population and the condition of mahalla infrastructure by the members of the “mahalla seven” using a newly established platform through a tablet;

bringing the effectiveness of decisions adopted on including individuals in the “Iron Notebook”, “Youth Notebook” and “Women’s Notebook” to 100 percent and thereby increasing the satisfaction level of the needy part of the population with the members of the “mahalla seven” to 100 percent, as well as bringing to 100 percent the effectiveness of the implementation of collegial decisions adopted on providing assistance from the “Sakhovat va Ko‘mak” Fund on the basis of a conclusion submitted by a social worker for the purpose of preventing citizens from falling into a difficult social situation and helping those who have fallen into such a situation to overcome it, and ensuring the effectiveness of material and social assistance and

state support provided to the population, as well as the proper provision of benefits and preferences, by bringing to 100 percent the level of making decisions on providing social assistance and allocating subsidies to individuals through the “Iron Notebook”, “Youth Notebook”, “Women’s Notebook”, the Fund for Involving the Population in Entrepreneurship, the State Employment Assistance Fund, and the Fund for Support of Handicrafts and Home-Based Work, and ensuring their implementation;

bringing to 100 percent the level of satisfaction, by state bodies and organizations through mutual cooperation, of citizens’ appeals submitted to members of the “mahalla seven” concerning payment of taxes, refund of overpaid taxes, improvement of road infrastructure without affecting the lawful rights and interests of other persons, provision of gas, water, electricity, sewerage and communication services, refund of overpaid debts, violations of consumer and advertising legislation, as well as matters related to the activities of the “mahalla seven”, and establishing the prompt resolution of primary appeals from the population;

further developing mahalla infrastructure and creating favorable opportunities for business representatives by increasing the number of business entities per capita up to a $\frac{1}{4}$ coefficient;

ensuring an 80 percent reduction in the number of divorces relative to the population, thereby preserving families, increasing the sense of trust in the state for the future in every family, protecting the rights and interests of minors, and ensuring their moral and harmonious development;

bringing the level of weddings, family celebrations, commemorative events and ceremonies conducted in accordance with the requirements established by legislation to 100 percent, thereby establishing effective public oversight, helping people overcome poverty, and eliminating conflict situations;

achieving an 80 percent reduction in the number of conflict-ridden families relative to the total number of families by increasing the employment level of the population and working closely with the problems of the population;

bringing the level of real-time updating of data concerning every resident and available resource within the mahalla territory in the new information system to 100 percent, thereby developing the population’s skills in using this system, sharply reducing the number of repeated appeals submitted by the population to state bodies at the regional or republican level, resolving the problems of the population through digital solutions, and obtaining a large amount of necessary, accurate and reliable information with minimal resource expenditure through the efforts of the population;

bringing the level of advance payment of property and land taxes by the population to 80 percent and the level of absence of land and property tax arrears among the population to 90 percent, and reducing the level of the population’s arrears on utility payments by 80 percent, in order to bring to a new stage the reforms carried out by the “mahalla seven” with the population regarding timely payment of taxes and other mandatory payments, and providing the necessary benefits for the population to pay taxes and other mandatory payments in advance;

granting broad powers to the “mahalla seven” in order to bring the number of mahallas in districts (cities) falling under the status of a “district (city) with the image of New Uzbekistan” to 5,000, and establishing digital state and public oversight over its activities;

ensuring inter-agency digital cooperation, widespread use of “smart and automated systems” and artificial intelligence, and resolving the technical and organizational capabilities for storing necessary information through available resources in order to support and expand the technical capabilities of the new comprehensive information system and its mobile application.

The experience of Kazakhstan, Tajikistan, Kyrgyzstan, Germany, France, Togo, the Republic of South Africa, Egypt, Saudi Arabia, Indonesia, Malaysia, Serbia, Greece, Liberia, Latvia, Lithuania, Russia, the UAE, China, the Republic of Korea, Singapore, Estonia, the USA, the United Kingdom, France, Spain, Mexico, Brazil, Azerbaijan, Georgia, India, Japan, Canada, Finland, Sweden, Rwanda, Italy, Austria, Australia, the Philippines, New Zealand, Denmark, Israel, Bangladesh, Vietnam, Colombia, Pakistan, Madagascar, Nigeria, Türkiye, Ethiopia, Switzerland, Norway, Kenya, Argentina, Romania, Chile, Portugal, Poland, Colombia, Belgium, Tanzania, Ecuador, Uganda, Papua New Guinea, the Netherlands, Jamaica, Greece and the European Union was studied in order to eliminate the problems identified above.

Based on the results of the study, a comparative table was prepared based on the solutions to the existing problems in relation to foreign experience.

In order to resolve the identified problems through foreign experience and available resources, to adopt a draft resolution of the President of the Republic of Uzbekistan entitled **“On Measures to Implement the “Servis mahalla” Strategy in 2026–2030”**, providing for the following:

- the “Servis mahalla” Strategy for 2026–2030;
- target indicators for the implementation of the “Servis mahalla” Strategy;
- a list of information systems to be integrated into the “Servis mahalla” comprehensive information system;
- a “road map” for implementing the priority tasks provided for in the “Servis mahalla” Strategy and its target indicators;
- a list of state bodies and organizations responsible for ensuring the provision of certain types of public services and services by members of the “mahalla seven”;
- a list of certain mahallas in Kashkadarya Region where the use of artificial intelligence by members of the “mahalla seven” is envisaged to be introduced on a pilot basis;
- categories of appeals to be resolved through cooperation among members of the “mahalla seven”.

As a result of the adoption of this proposal, the following target indicators will be achieved:

instead of the members of the “mahalla seven” working in separate information systems with various types of complex modules and functions, similar and repetitive functions, a comprehensive “Servis mahalla” information system and its mobile application, based on artificial intelligence and incorporating all

information systems introduced into the activities of the “mahalla seven”, will be created, and 500 information systems will be integrated into it over three years;

a “Smart Map” module will be created in the “Servis mahalla” comprehensive information system, creating the possibility of monitoring in real time data on every infrastructure facility and resident within the mahalla territory, entering necessary data, and generating 1,000 types of information in real time based on reliable, correct, accurate, prompt and free data;

the “Smart Mahalla Governance System” will be introduced 100 percent in order to ensure the proper vertical and horizontal management of the activities of the “mahalla seven” and to organize its activities at the required level;

artificial intelligence with the following capabilities in the following areas will be introduced and developed in the “Servis mahalla” comprehensive information system:

a chatbot providing information about services established in the mahalla and advising on their use;

the possibility of generating decisions adopted by the “mahalla seven” by converting audio into text;

a service for filtering the correctness, accuracy and authenticity of information generated in the “Servis mahalla” comprehensive information system and its mobile application;

the possibility of automatically generating documents necessary for the activities of the “mahalla seven” by giving instructions through text, audio and video;

the number of members of the “mahalla seven” with higher education will be brought to 100 percent;

the number of electronic public services provided by members of the “mahalla seven” will reach 500;

the following will be established 100 percent through artificial intelligence:

providing streets where asphalt roads have been laid with lamps controlled by artificial intelligence and switched on and off according to human sound;

receiving, analyzing and determining the jurisdiction of all appeals submitted to “muloqot.gov.uz”, “pm.gov.uz” and the “Servis mahalla” comprehensive information system through artificial intelligence, establishing digital control over the timely, high-quality, complete and lawful consideration of appeals, and responding to violations of the law by notifying prosecution and justice authorities;

promptly mobilizing the necessary resources to ensure the timely provision of services related to road traffic safety, bodily injury, insult, defamation, hooliganism, violations of consumer rights, advertising, violations of legislation on sanitary and epidemiological matters, communications, electricity, gas, water, sewerage, emergency medical assistance and elevators;

analyzing emergency medical assistance and law-violation-related appeals and promptly directing the necessary resources, assisting specialists through road infrastructure so that they can reach the destination in a timely and prompt manner;

forecasting offenses committed over the past period in order to prevent offenses and, by analyzing incoming appeals, clearly identifying the “red zones” of offenses;

using the “Smart Map”, providing legal explanations regarding the full activities of state bodies and organizations by every sector, network, direction, task and function, advising on which services can be obtained from them, when and how they can be obtained, and assisting in remotely obtaining public services and services through the “Servis mahalla” comprehensive information system;

sending reminders regarding citizens’ personal data, weather, natural disasters, and socio-economic conditions;

the share of appeals resolved with the assistance of the “mahalla seven” in relation to the total number of appeals will be brought to 70 percent;

the share of state social orders allocated to mahallas in relation to the total state social orders allocated will be brought to 40 percent;

the share of cases in which the measure of restraint of placing an accused or defendant under the guarantee of the “mahalla seven” is selected in relation to existing criminal cases will be increased to 70 percent;

the number of petitions by the “mahalla seven” for the conditional early release of a convicted person from punishment or replacement of the punishment with a lighter one in relation to crimes committed within the territory of the respective mahalla will be brought to a 1/3 coefficient;

the level of attendance of the members of the “mahalla seven” regarding arrival at and departure from work will be brought to 100 percent;

the level of studying the economic and social condition and needs of families will be brought to 100 percent;

the effectiveness of decisions adopted on including individuals in the “Iron Notebook”, “Youth Notebook” and “Women’s Notebook” will be brought to 100 percent, and thereby the satisfaction level of the needy part of the population with the members of the “mahalla seven” will be increased to 100 percent;

the level of making decisions on providing social assistance and allocating subsidies to individuals through the “Iron Notebook”, “Youth Notebook”, “Women’s Notebook”, the Fund for Involving the Population in Entrepreneurship, the State Employment Assistance Fund, and the Fund for Support of Handicrafts and Home-Based Work, and ensuring their implementation, will be brought to 100 percent;

the effectiveness of the implementation of collegial decisions adopted on providing assistance from the “Sakhovat va Ko’mak” Fund on the basis of a conclusion submitted by a social worker for the purpose of preventing citizens from falling into a difficult social situation and helping those who have fallen into such a situation to overcome it will be brought to 100 percent;

the share of members of the “Mahalla seven” holding international and local IT certificates will be increased to 100 percent;

the level of satisfaction, by state bodies and organizations through mutual cooperation, of citizens’ appeals submitted to the “Mahalla seven” concerning payment of taxes, refund of overpaid taxes, improvement of road infrastructure

without affecting the lawful rights and interests of other persons, provision of gas, water, electricity, sewerage and communication services, refund of overpaid debts, violations of consumer and advertising legislation, as well as matters related to the activities of the “mahalla seven”, will be brought to 100 percent;

the number of business entities per capita will be increased up to a $\frac{1}{4}$ coefficient;

an 80 percent reduction in the number of divorces will be achieved relative to the population;

the level of weddings, family celebrations, commemorative events and ceremonies conducted in accordance with the requirements established by legislation will be brought to 100 percent;

the number of conflict-ridden families will be reduced by up to 80 percent relative to the total number of families;

the level of real-time updating of data concerning every resident and available resource within the mahalla territory in the “Servis mahalla” comprehensive information system will be brought to 100 percent;

the level of advance payment of property and land taxes by the population will be brought to 80 percent;

the level of absence of land and property tax arrears among the population will be brought to 90 percent, and the level of the population’s arrears on utility payments will be reduced by 80 percent;

the number of mahallas in districts (cities) falling under the status of a “district (city) with the image of New Uzbekistan” will be brought to 5,000.

CHAPTER III. DIGITAL TRANSFORMATION OF SOCIETY AND THE STATE AND INFORMATION SECURITY

3.1-§. The Necessity and Significance of Improving the Digital New Uzbekistan

Information and communication technologies currently play a very significant role in ensuring the interests of the individual, society and the state, and particular attention is also being paid to the development of this area in our country. In particular, from the time the Republic of Uzbekistan gained independence to the present day, **2,647** legislative documents related to digitalization have been adopted. Specifically, **2,117** projects were implemented within the framework of the “Digital Uzbekistan–2030” Strategy¹⁰², **100** within the framework of the “Uzbekistan – 2030” Strategy¹⁰³, **82** within the framework of deepening reforms in the field of digital technologies and transforming the functioning of the system¹⁰⁴, **275** related to bringing the information and communication technologies sector to a new stage¹⁰⁵, **165** within the framework of increasing the coverage and quality of digital services and digitally transforming sectors, industries and territories¹⁰⁶, and **21** projects within the framework of the Strategy for the Development of Artificial Intelligence Technologies until 2030¹⁰⁷ were implemented. As a result, all important tasks envisaged in the “Digital Uzbekistan – 2030” Strategy were fulfilled, and the coverage of the territories of the Republic with the high-speed Internet global information network reached **85** percent, the coverage of populated areas with broadband mobile communication networks reached **100** percent, the share of electronic public services provided through the Unified Interactive Public Services Portal (YIDXP) in relation to public services provided by Public Service Centers reached **70** percent, the share of transactional services provided through the UIPSP reached **60** percent, the activities of more than **320** government bodies and organizations were digitized, more than **770** public services and services became available on the Unified Interactive Public Services Portal, and the number of users exceeded **11** million¹⁰⁸.

¹⁰² Decree № DP–6079 of the President of the Republic of Uzbekistan dated October 5, 2020, “On Approval of the ‘Digital Uzbekistan–2030’ Strategy and Measures for Its Effective Implementation” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁰³ Decree № DP–158 of the President of the Republic of Uzbekistan dated September 11, 2023, “On the ‘Uzbekistan – 2030’ Strategy” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁰⁴ Decree № DP–76 of the President of the Republic of Uzbekistan dated May 24, 2023, “On Measures to Effectively Organize Public Administration in the Field of Digital Technologies within the Framework of Administrative Reforms” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁰⁵ Resolution № RP–357 of the President of the Republic of Uzbekistan dated August 22, 2022, “On Measures to Bring the Information and Communication Technologies Sector to a New Level in 2022–2023” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁰⁶ Resolution № RP–162 of the President of the Republic of Uzbekistan dated May 24, 2023, “On Measures to Increase the Coverage and Quality of Digital Services and to Digitally Transform Sectors, Industries and Regions” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁰⁷ Decision № DP–358 of the President of the Republic of Uzbekistan dated October 14, 2024, “On Approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁰⁸ <https://my.gov.uz/uz>.

“Digital Uzbekistan” should serve to uphold human dignity. Therefore, it is essential to ensure that digitalization is implemented correctly and systematically! However, as a result of the failure to implement digitalization systematically, the Republic of Uzbekistan currently faces a number of problems, in particular:

First, although the “Digital Uzbekistan–2030” Strategy is, in substance, intended to remain in effect until 2030, as provided for in Decree №DP–6079 of the President of the Republic of Uzbekistan dated October 5, 2020, “On Approval of the ‘Digital Uzbekistan–2030’ Strategy and Measures for Its Effective Implementation”, the tasks set therein have already been completed; at the same time, under the New Uzbekistan Development Strategy for 2022–2026 approved by Decree №DP–60 of the President of the Republic of Uzbekistan dated January 28, 2022, or on its basis, **the concept and strategy for the digitalization of New Uzbekistan, including cybersecurity, have still not been approved and implemented in practice.** This is resulting in the work carried out in the areas of digitalization, artificial intelligence and cybersecurity not being implemented on the basis of a unified legal and technological approach.

In particular, during 2017–2025, **610** legislative acts concerning digitalization were adopted, and the majority of the tasks set forth therein consisted of repetitive and similar assignments. Moreover, digitalization was primarily focused on the activities of a particular state body or organization, while measures aimed at **comprehensive and systematic digitalization** of each sector and industry were scarcely implemented; systematic measures that were implemented accounted for less than **5 percent** of all activities. At the same time, the tasks set were not fully implemented in practice, and the necessary information systems were not developed and fully put into operation.

For example, **898** projects are currently registered in the Unified Register of Information Systems and Resources of the Digital Government¹⁰⁹. However, according to our analysis of legislative acts and other documents, more than **2,500** projects were required to be implemented, while the tasks set have not been adequately and fully fulfilled.

Secondly, although the fields of information, information and communication technologies, digital technologies, artificial intelligence, and cybersecurity are closely interrelated, the differences in their respective levels of development and the degree of attention given to them are adversely affecting the further development of the work being carried out in these areas. *For example*, although the activities of the Ministry of Digital Technologies logically encompass all of the above-mentioned fields, its name, tasks, and functions do not fully cover them in terms of the applicable legislation and its activities. Moreover, information and communication technologies constitute a considerably broader field than digital technologies, while, in practice, the Ministry is hardly engaged in any matters relating to the fields of information and cybersecurity.

¹⁰⁹ <https://reestr.uz/projects?limit=10>.

This may also be one of the reasons why the Agency for Information and Mass Communications was abolished, and its tasks and functions concerning supervision and monitoring in the field of information were transferred to the Inspectorate for Control in the Sphere of Informatization and Telecommunications under the Ministry of Digital Technologies¹¹⁰. Therefore, it is now necessary for the Ministry to clarify its tasks and functions in this area.

Due to the insufficient and unsystematic definition of the necessary tasks in this area, a number of problems are arising. For example, in accordance with Article 121 of the Law of the Republic of Uzbekistan “On Informatization”, as established by Resolution № 707 of the Cabinet of Ministers dated September 5, 2018, “On Measures to Further Improve Information Security on the World Wide Web”, the processes among state bodies related to restricting access to a website and (or) websites and (or) their pages are still being carried out using traditional methods, while adequate administrative and criminal liability measures are not being taken in respect of cases involving information attacks identified by the “Cybersecurity Center” SE, the Center for Mass Communications, authorized bodies, and the general public.

While **4,529,215** court decisions concerning administrative offenses have currently been published in the public.sud.uz information system, of these, **4,436** concern the administrative offense of producing, importing, distributing, advertising, or demonstrating pornographic products pursuant to Article 189 of the Code of the Republic of Uzbekistan on Administrative Responsibility, and **490** concern the administrative offense of producing, importing, distributing, advertising, or demonstrating products promoting coercion, violence, or cruelty pursuant to Article 1891 of the Code on Administrative Responsibility¹¹¹. Furthermore, while court decisions in **384,492** criminal cases have been published, of these, **51** concern the crime of producing, importing, distributing, advertising, or demonstrating pornographic products pursuant to Article 130 of the Criminal Code, and **46** concern criminal cases involving the production, importation, distribution, advertising, or demonstration of products promoting coercion, violence, or cruelty pursuant to Article 1301 of the Criminal Code¹¹².

At the same time, according to information provided by artificial intelligence, more than **100,000** new videos of pornographic content are currently uploaded in the Republic of Uzbekistan on average per day alone, while systematic measures to hold the offenders responsible have not been adequately established¹¹³.

In 2022, the number of cybercrimes registered in the Republic of Uzbekistan amounted to **105,215**, while in 2023 this figure amounted to **104,096**. In the city of Tashkent, this figure amounted to **22,791** in 2022 and **21,728** in 2023¹¹⁴.

¹¹⁰ Decree № DP–111 of the President of the Republic of Uzbekistan dated July 14, 2025, “On Measures to Increase Efficiency, Proactivity and Effectiveness in the Public Administration System” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹¹¹ <https://public.sud.uz/report/CONFLICT>.

¹¹² <https://public.sud.uz/report/CRIMINAL>.

¹¹³ <https://chatgpt.com/>.

¹¹⁴ https://api.siat.stat.uz/media/uploads/sdmx/sdmx_data_800.pdf.

At the same time, the data contained in the above-mentioned public.sud.uz information system were obtained not for a single year, but through an analysis of all court decisions entered into the system throughout all years. Therefore, in this situation, it can be observed that a **very significant disparity is emerging between the number of identified information security and cybersecurity incidents and the measures taken in response to them.**

Although the field of cybersecurity also encompasses measures aimed at combating cybercrime, as a result of the failure to carry out systematic work in this area, cybercriminals **stole UZS 1.9 trillion from Uzbek citizens during 2021–2024**, while in 2024 alone this figure amounted to **UZS 603 billion**. Moreover, although the terminology has been changed to digitalization or digital technologies, paper-based processes have still not been eliminated in practice. At the same time, by referring to the exchange of paper documents as digital technology or digitalization, we are deceiving ourselves; in reality, the existing exchange of paper documents has not yet been fully transferred to electronic form, and data exchange within information systems is not fully digital, but rather, **in the majority of cases, is merely conducted in electronic form.** *By using appealing terminology, we are deceiving ourselves*, thereby creating an obstacle to the systematic implementation of digitalization.

Thirdly, due to the lack of full interconnection among all existing information systems in the republic, including the **1,275** state information systems identified through the analysis, there is no clear understanding of which information system should be used, which one requires an additional subsystem or module, or in which system a particular function should be introduced. As a result, budgetary funds are being used inefficiently and for unintended purposes.

***For information:** over the past period, the “UZINFOCOM” single integrator has implemented only 21 projects¹¹⁵, including 9 information systems¹¹⁶, as well as only 3 projects based on artificial intelligence¹¹⁷.*

If all information systems had been integrated with one another and the possibility had been created to deploy artificial intelligence and intelligent systems within these systems, this would have created an opportunity not only to provide greater convenience for users, but also to save state budget funds.

Fourthly, as a result of the failure to implement digitalization systematically, cases of introducing into practice information systems that have not undergone expert examination by the “Cybersecurity Center” SE and the Ministry of Digital Technologies are increasing, while their detection is still being carried out using traditional methods. Furthermore, the **898** information systems and resources currently included in the Unified Register of Information Systems and Resources of the Digital Government¹¹⁸ have still not been fully integrated with one another, and the technical capability to manage them through a single platform has not been established.

¹¹⁵ <https://uzinfocom.uz/uz/projects?page=5>.

¹¹⁶ <https://uzinfocom.uz/uz/projects?category=3>

¹¹⁷ <https://uzinfocom.uz/uz/projects?category=2>

¹¹⁸ <https://reestr.uz/projects>.

Due to the introduction into practice of information systems whose security has not been examined, as well as the fact that even the existing information systems that have undergone expert examination have not been fully integrated with one another, the heads of local administrations, as heads of regions, and the ministries, committees, agencies, centers, and inspectorates responsible for particular sectors, industries, or areas **do not have sufficient information resources at their disposal, while automated and artificial intelligence-based analytical systems are hardly functioning at all**. As a result, the number of duplicative legislative acts and assignments continues to increase, while the security of personal data is being placed at risk.

Fifthly, systematic measures are not being implemented to determine the direction in which digitalization should proceed in order to ensure comprehensive effectiveness, ensure the proper, targeted, and efficient use of budgetary funds, save the necessary financial resources, and enable the targeted use of the funds saved. As a result, negative manifestations related to “*lobbyism*”, “*latent*” offenses, and cybercorruption are also taking root in the field of digitalization.

For example, rather than saving budgetary funds by creating a unified information system in the field of social protection and introducing the necessary modules therein, budgetary funds are currently being allocated in the same area, but through different agencies and for different purposes, through information systems with similar and duplicative tasks and functions, such as the “*Register of Low-Income Families*”, the “*Unified Register of Social Protection*”, “*Ayollar daftari*”, “*Temir daftar*”, and “*Yoshlar daftari*”. The agency may be different; however, it must not be forgotten that the funds allocated to these systems belong to the state budget.

The **kengash.gov.uz** portal of representative bodies of local authorities¹¹⁹ and the **e-qaror.gov.uz** unified electronic system¹²⁰, whose tasks and functions are similar and identical, are both operational. However, no consideration has been given to the fact that their functions are already better organized within the EDO.IJRO.UZ Interagency Electronic System for Executive Discipline¹²¹, or to the need to integrate all three into a single information system or transfer them to a single portal.

As a result, additional budgetary funds are being spent on the development, implementation, technical support, and use of information systems whose tasks and functions are virtually identical or similar. Analyses indicate that, currently, an information system is being implemented at an average cost of **UZS 5–10 billion**, while budgetary funds in the amount of UZS 5–10 million per month are allocated for its technical support and UZS 2–5 million for its use. If the total expenditure is calculated by multiplying these amounts by the number of months, years, and user organizations, it becomes evident that trillions of soums are being allocated from the budget.

¹¹⁹ <https://kengash.gov.uz/>.

¹²⁰ <https://e-qaror.gov.uz/>.

¹²¹ <https://edo.ijro.uz>.

Sixthly, the failure to implement digitalization systematically is resulting in an increase in the number of cybercrimes. No one takes into account that every user represents a potential point from which a cyber threat may originate; instead, more and more information systems are being created and introduced into practice, which benefits cybercriminals, as they carry out cyberattacks through points with low levels of security. Most regrettably, cases are also increasingly occurring in which a newly appointed head of a state organization, believing that digitalization is necessary, makes changes to the names and technical documentation of existing information systems, resulting in additional budgetary funds being spent on the same information system, while systematic oversight of such practices has not been established. This is contributing to an increase in the number of “*latent*” cyber-offenses, including offenses related to cybercorruption.

***For information:** According to data from the Central Bank, there are currently 376 commercial banks¹²², 111 microcredit organizations¹²³, the number of users of systems providing remote banking services amounts to 60,083,561¹²⁴, the number of bank cards in circulation amounts to 63,825,850, the number of installed payment terminals amounts to 426,111, and the number of ATMs and infokiosks amounts to 35,784¹²⁵, the number of payment system operators amounts to 3¹²⁶, the number of payment organizations amounts to 44¹²⁷, and there are 12 electronic money systems, demonstrating that a total of 124,371,852 points exist that may serve as potential points for the occurrence of cybersecurity incidents.*

As the number of users and information systems increases, the number of cybercrimes will also continue to increase. In the banking sector in particular, due to the large number of users, **98 percent of cybercrimes currently being committed consist of theft and fraud involving bank cards**¹²⁸. Therefore, in our view, the time has come to completely abandon information systems that perform duplicative and similar functions, conduct an inventory of such systems, and reconsider digitalization on the basis of a unified methodology.

Seventhly, the extent to which information systems proliferate does not allow full control and monitoring over their operation to be established through limited human resources or material and technical capacity. By way of analogy, due to the excessive number of **91,371**¹²⁹ normative-legal and other documents containing duplicative or similar provisions currently in existence, elements of the “*smart regulation*” model were applied in the field of law-making, measures were undertaken to transfer the provisions of departmental normative-legal acts into legislative acts having higher legal force and to apply the “*regulatory guillotine*”

¹²² <https://data.egov.uz/data/6113bd0fdb32b99538e08991>.

¹²³ <https://data.egov.uz/data/6113bde9db32b99538e0899b>.

¹²⁴ <https://data.egov.uz/data/6113c568db32b99538e08ab3>.

¹²⁵ <https://data.egov.uz/data/6113c59edb32b99538e08ab5>.

¹²⁶ <https://data.egov.uz/data/6113c68bdb32b99538e08abd>.

¹²⁷ <https://data.egov.uz/data/6113c6c0db32b99538e08abf>.

¹²⁸ [Cybercriminals Stole UZS 1.9 Trillion from Citizens in 2021–2024.](#)

¹²⁹ <https://lex.uz/>.

method¹³⁰, and a one-year moratorium was declared on the adoption of departmental normative-legal acts¹³¹.

For this reason, unless systematic measures are implemented in this area, Uzbekistan may soon be compelled to apply the “*regulatory guillotine*” method in this field as well.

Eighthly, the failure to implement digitalization systematically is having a negative impact on all sectors, including the judicial and legal sphere. In particular, a **uniform practice has still not been established** in judicial proceedings concerning the consideration of identical offenses and crimes and the adjudication of guilty persons. Although the number of “*latent*” offenses is increasing, the legislation has still not established sufficient opportunities for the practical application of precedent law (*case law*), customary law (*common law*), and statutory law (*statute law*). A simple methodology and procedure for recording cyber offenses, including cybercrimes, have not been established. While punishment for a crime is inevitable, competent authorities are attempting to take measures to reduce the number of crimes so that crime statistics do not increase, thereby themselves creating conditions for the emergence of new crimes.

According to analyses, in 2023, one cyberattack occurred every 39 seconds, whereas currently, **one cyberattack occurs every 14 seconds**¹³², while other sources indicate that **a cyberattack is carried out every second**¹³³. As a result, in 2023, 71 percent of organizations worldwide became victims of ransomware attacks, whereas currently, 80 percent of all cybersecurity incidents are associated with criminal groups¹³⁴.

The amount of damage caused to the global economy amounted to USD 3 trillion in 2018, USD 3.5 trillion in 2019, USD 4.2 trillion in 2020, USD 6 trillion in 2021, USD 7 trillion in 2022, USD 8.4 trillion in 2023, and USD 9.5 trillion in 2024¹³⁵. It is projected to amount to **USD 10.5 trillion** in 2025¹³⁶, USD 20 trillion in 2026, USD 22 trillion in 2027, USD 24 trillion in 2028, and USD 26 trillion in 2029¹³⁷.

More than **500 million** cyberattacks are carried out worldwide every year. **Every second, one in 12 people becomes a victim of attacks committed in cyberspace**. In developed countries such as the United States, France, the United Kingdom, Germany, Belgium, and Luxembourg, 60–65 percent of crimes are being committed through cyberattacks. In Uzbekistan, crimes of this type have **increased**

¹³⁰ Decree № DP–5505 of the President of the Republic of Uzbekistan dated August 8, 2018, “On Approval of the Concept for Improving Law-Making Activities” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹³¹ Decree № DP–5997 of the President of the Republic of Uzbekistan dated May 19, 2020, “On Measures to Further Improve the Activities of Justice Bodies and Institutions in the Implementation of State Legal Policy” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹³² <https://www.datensicherheit.de/2024-2025-cyber-attack-companies-14-seconds>.

¹³³ <https://cybermap.kaspersky.com/ru/stats>.

¹³⁴ <https://www.websiterating.com/ru/blog/research/cybersecurity-statistics-facts/#sources>.

¹³⁵ <https://newsletter.radensa.ru/archives/4840>.

¹³⁶ <https://www.cenlanow.com/business/press-releases/ein-presswire/674883055/cybercrime-damages-to-cost-the-world-9-5-trillion-usd-in-2024/>.

¹³⁷ <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide#:~:text=The%20global%20cost%20of%20cybercrime,trillion%20U.S.%20dollars%20in%202022.>

8.3-fold over the past three years and currently account for nearly 5 percent of total crime¹³⁸.

However, in practice, the actual number of such crimes is even higher, and they are increasingly spreading as “latent” offenses.

As is known, GDP for 2025 was projected to amount to UZS 1,630 trillion¹³⁹, and, taking into account that as of July 16, 2025, USD 1 was equivalent to UZS 12,778.12¹⁴⁰, [2] we can observe that the amount of UZS 1,630 trillion is equivalent to approximately USD 127.56 billion, while the amount of damage caused by cybercrime, totaling **USD 10.5 trillion, is nearly 82 times greater than the entire GDP of the Republic of Uzbekistan.**

Accordingly, unless digitalization is implemented properly, the problems faced by the entire population will never be fully resolved, adequate analysis will not be conducted, the opportunity to ensure the targeted and efficient use of budgetary funds will not be created, and the number, types, and scale of cyber offenses, including cybercrimes, will increase, ultimately leading the state towards decline. Therefore, in order to systematically implement work in this area, the following measures should be urgently undertaken, in particular:

Firstly, all information systems should undergo a complete inventory, and the inventory should be conducted by research institutions under the President of the Republic of Uzbekistan and the Administration of the President of the Republic of Uzbekistan jointly with the relevant executive authorities, and a final list of these information systems should be compiled. **The final list must clearly indicate the name of the information system, its tasks and functions, its digital footprints, and its owner.** On the basis of this list, it will be possible to identify information systems whose tasks and functions duplicate or resemble one another and, by optimizing them, create an opportunity to systematize them according to specific tasks and functions;

Secondly, existing information systems that are ineffective, whose tasks and functions duplicate one another, and whose ownership is unclear should be written off, and, through the response of law enforcement bodies and courts to cases of their improper involvement in practice, it will be possible to take measures to hold persons who have embezzled budgetary funds accountable and to return the funds misappropriated by them to the state budget;

Thirdly, it is necessary to fully integrate information systems whose tasks and functions are not similar to one another. In the course of this integration, it should be clearly specified what information can be obtained from each information system, and this information should be formed on the basis of a single list and transferred to a single platform, thereby creating an opportunity for users to access it from a single point. This, in turn, in addition to creating comprehensive convenience for users, will enable state bodies and organizations with clearly defined tasks and functions

¹³⁸ F. Khudoykulov. More than 500 million cyberattacks are carried out annually. <https://yuz.uz/news/bir-yilda-500-milliondan-ortiq-kiber-hujumlar-uyushtiriladi>.

¹³⁹ Law № LRU–1011 of the Republic of Uzbekistan dated December 24, 2024, “On the State Budget of the Republic of Uzbekistan for 2025” // lex.uz – National Database of Legislation of the Republic of Uzbekistan..

¹⁴⁰ <https://cbu.uz/uz/>.

to fully perform the tasks assigned to them in digital form through a single platform, establish an effective analytical system, and fundamentally improve strategic public administration;

Fourthly, it is advisable to introduce artificial intelligence into the information and communication system that has been fully integrated and transferred to a single platform, and to determine the role and status of artificial intelligence technologies in all matters relating to the activities of the relevant state body. Through their implementation, artificial intelligence will be able to predict, based on crime and the criminogenic situation, as well as on crimes and other offenses committed in previous periods, crimes and offenses that may occur in the future; effective methods for mobilizing the necessary resources to prevent them will be established; an analytical system based on automated “*smart systems*” necessary for the implementation of the tasks assigned to the state body will be created; and, through this system, public administration will become further simplified and promptness will be ensured, while acts related to cybercorruption occurring in the state, non-state, and private sectors will be exposed and prevented;

Fifthly, through the proper implementation of digitalization, it will be possible to prevent a sharp increase in the number of users; as a result of preventive measures implemented to prevent the recurrence of a cyberattack that has already been committed, a cybercriminal will hesitate to carry out another cyberattack against the same object due to the existence of the necessary cyber protection; and, most importantly, as a result of the unified efforts of all state bodies and organizations to ensure the cybersecurity of the single platform, cybersecurity can be significantly strengthened compared with the current situation through the systematic allocation of budgetary funds, the number and location of cybersecurity objects targeted by a cybercriminal planning to carry out a cyberattack can be identified, the technical capabilities for promptly ensuring cybersecurity can be created, and a sharp reduction in the number of cybercrimes can be achieved.

Sixthly, it is necessary to transfer the unified platform based on artificial intelligence and its constituent components to the Data Processing Center of the “Electronic Government” system¹⁴¹. This will enable the information resources available in state information systems to be consolidated in a single center and create an opportunity to ensure its cybersecurity. Most importantly, the performance speed of the information systems will be further increased due to the complete centralized storage of the data contained in their memory, thereby creating greater convenience for users.

Seventhly, it is necessary to create an opportunity for the Head of State, through digital solutions, to determine in real time the extent to which existing problems in the Republic can be addressed using limited resources. Currently, there are numerous information systems, while many sectors, industries, and areas have not been fully digitalized, resulting in discrepancies between statistical data and the existing reality. At the same time, negative manifestations related to “*lobbyism*” are

¹⁴¹ Resolution № 107 of the Cabinet of Ministers dated March 14, 2023, “On Measures to Organize the Activities of the Data Processing Center of the ‘Electronic Government’ System” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

arising in the proper use of limited resources. As a result, a number of problems are emerging in the full digitalization of all sectors and industries. Once a fully comprehensive state of digitalization is achieved, the Head of State will have the opportunity to determine which sector, industry, or area should receive attention at present and in the future.

Eighthly, in order to implement the systematic measures outlined above, it is necessary to develop a Concept for the Digitalization and Cybersecurity of New Uzbekistan and create mechanisms for its systematic implementation through a Strategy for its implementation and “roadmaps”. It is necessary to completely abandon approaches aimed at “digitalizing each sector independently”.

It would be appropriate to implement these tasks through a Decree or Resolution of the President of the Republic of Uzbekistan.

From a scholarly perspective, Henri Verdier, Head of France’s digitalization agency (DINUM), who advanced the “*digital republic*” model, explains transformation through the introduction of information systems in every sector as “*digitalization – the foundation of state reform*”¹⁴². Viktor Mayer-Schönberger, a leading scholar in the fields of “Big Data” and “Digital Governance”, emphasized that digitalization does not merely mean process automation, but rather the creation of a new model of digital policy, governance, and innovation¹⁴³. According to analyses, **Evgeny Kuznetsov**, one of the authors of the “Digital Transformation of the Economy” concept, recommended creating digital ecosystems in various sectors and establishing new value chains in public services, education, and healthcare, according to which digitalization means that “digitalization is equivalent to a new culture of governance”¹⁴⁴. **Satya Nadella**, in his “Tech Intensity” concept, considers it necessary to create a digital platform in every sector, that is, the internal processes of education, healthcare, logistics, and other sectors should each be implemented exclusively through a single digital infrastructure¹⁴⁵. The founder of the World Economic Forum, **Klaus Schwab**, noted in his “Fourth Industrial Revolution” concept that digitalization fundamentally transforms entire sectors and social systems, proposing the creation of a digital state and digital economy through AI, IoT, blockchain, and other technologies¹⁴⁶.

Based on the foregoing, in conclusion, in our view, as a continuation of the views expressed by the scholars mentioned above, a separate platform is not necessary for each sector, industry, and area; rather, creating an additional platform for similar and duplicative tasks and functions within such sectors, industries, and areas entails additional costs and inconvenience. Instead, it would be appropriate to develop information and communication systems for sectors, industries, and areas having similar tasks and functions, integrate them with one another, and manage them through a single platform. Only in this case will an opportunity arise to apply

¹⁴² https://media.franceintheus.org/4265/?utm_source=chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eiir.org/wp-content/uploads/2022/08/EIIR-4IR-STUDY_OVERVIEW_10_10_20_TEXT.pdf.

¹⁴³ [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eiir.org/wp-content/uploads/2022/08/EIIR-4IR-STUDY_OVERVIEW_10_10_20_TEXT.pdf](https://courses.skolkovo.ru/event/cdto-kuznetsov-2/?utm_source=chatgpt.com).

¹⁴⁴ https://courses.skolkovo.ru/event/cdto-kuznetsov-2/?utm_source=chatgpt.com.

¹⁴⁵ <https://ukstories.microsoft.com/features/microsoft-ceo-satya-nadella-on-fuelling-tech-intensity-in-the-uk/>.

¹⁴⁶ <https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab/>.

artificial intelligence technologies properly and to make more effective use of “*smart systems*” compared with other solutions.

For this purpose, a concept should be adopted, and the tasks should be systematically implemented on the basis of a strategy and programme or “roadmap”. Everyone should comply with the concept, while amendments thereto should depend on the development of information and communication technologies and the specific capabilities of the available resources and legal framework, and should be made systematically. Otherwise, the established objective may not be fully achieved. Only in this manner will it become possible to fully resolve the issues raised above, establish a unified procedure and practice for ensuring that budgetary funds are directed towards digitalization not haphazardly, but systematically and properly, and, most importantly, create an opportunity for a sharp reduction in the number of cybercrimes or, at the very least, for the increase in their number to be significantly lower than usual.

3.2-§. The Necessity and Procedure for Introducing a Strategic System for Prompt Response to Information in the Media Space that Undermines the National and Public Security of the Republic of Uzbekistan

During the period under review, a number of positive measures have been implemented in the Republic of Uzbekistan. In particular, during 2017–2025, **11,997** normative legal acts and, on the basis thereof, **more than 20,000** documents were adopted, resulting in the implementation of **nearly 100,000 positive measures** in total. Within the framework of the Action Strategy for the Further Development of the Republic of Uzbekistan, the Development Strategy of New Uzbekistan, the “Uzbekistan–2030” Strategy, and the “Digital Uzbekistan–2030” Strategy alone, **nearly one thousand high-priority tasks** were implemented under **each** of these strategies. However, due to technological development, the number of **“destructive information”** that misrepresents to the general public the reforms being implemented by the Head of State and other public officials, thereby undermining national and public security and contradicting the actual facts, is currently increasing. Since the legislation does not establish a clear distinction between “destructive information” and “well-founded critical opinion”, and relations concerning them have not been sufficiently regulated, the number of negative occurrences in this area is increasing day by day. The activities of the **information services** of state bodies and organizations have not been sufficiently **digitalized**, **solutions based on artificial intelligence and digital methods for promptly addressing information on social networks that negatively affects public sentiment or distorts the actual state of reforms are not being applied**, and the systematic dissemination of ongoing reforms and political processes in the form of content capable of becoming a **“trend”** or meaningful national content has not been properly established. The fact that, in the media space, **“destructive information”** is being addressed by responsible officials only after extensive public discussion is adversely affecting the further development of the reforms carried out by the Head of State and the actual state of the measures implemented, thereby undermining the effectiveness of the work in this area. At the same time, the number of cases in which information disseminated through channels and groups on social networks and messengers, which has been overlooked by the heads or information services of state bodies and organizations, becomes the subject of extensive public discussion, causes the reputation and role of state bodies and organizations to decline in the eyes of the general public, and distorts the actual state of the reforms being implemented by the Head of State, is increasing day by day.

According to the analysis, it has been established that **“destructive information”** may currently be discussed through **11 mobile applications** operating in the Republic of Uzbekistan, which may be **viewed by and discussed among more than 1 billion people worldwide**. Of particular concern is the fact that **nearly 90 percent of these users**, in relation to situations concerning the Republic of Uzbekistan, are becoming victims of cyberbullying **without being aware of it**, with **482,329,545 persons** potentially affected **within a single day**. Furthermore,

according to **Google Play**¹⁴⁷, in 6 mobile applications available for download from the Play Market, more than 500 million users, in 10 mobile applications more than 100 million users, in 6 mobile applications more than 50 million users, in 34 mobile applications more than 10 million users, and in 21 mobile applications more than 5 million users may discuss destructive information. The principal **subject matter** of **cyberbullying** today is **social or political issues**. Taking into account that, as of 9:35 a.m. on 28 August 2025, the permanent population of the Republic of Uzbekistan had reached 38,000,000 persons, these figures demonstrate that the **number of cyberbullying victims is 12.69 times greater**¹⁴⁸. In this regard, the legislation of the Republic of Uzbekistan, in particular, the Constitution of the Republic of Uzbekistan, Law № LRU–369 of the Republic of Uzbekistan dated 5 May 2014¹⁴⁹, Decree № DP–154 of the President of the Republic of Uzbekistan dated 14 June 2022¹⁵⁰, and Resolutions of the Cabinet of Ministers № 910 dated 30 December 2024¹⁵¹, №81 dated 19 February 2021¹⁵², № 54 dated 31 January 2025¹⁵³, № 137 dated 26 March 1999¹⁵⁴, № 27 dated 20 February 2006¹⁵⁵, and № 373 dated 15 June 2021¹⁵⁶, partially establish traditional solutions for addressing the above-mentioned issues. However, due to the lack of systematization thereof and the absence of a procedure for resolving specific problems through clearly defined solutions, there is currently a **“legal, political, and technical gap”** in this area.

When the experience of foreign countries was studied, it was established that in **South Africa**, through the **National Communication Strategy Framework for 2025–2030**¹⁵⁷, the **GCIS – Media Rapid Response (Government Communication**

¹⁴⁷ <https://play.google.com/store/games?hl=ru&pli=1>.

¹⁴⁸ https://t.me/statistika_rasmiy/6256.

¹⁴⁹ Law № LRU–369 of the Republic of Uzbekistan “On Openness of the Activities of State Authorities and Administration” dated 5 May 2014 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁵⁰ Methodology for Monitoring and Assessing the Openness of the Activities of State Bodies and Organizations, approved by Decree № DP–154 of the President of the Republic of Uzbekistan dated 14 June 2022 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁵¹ Regulation “On the Procedure for Remote Monitoring of Compliance by State Bodies and Organizations with Obligations Established in Normative Legal Acts in the Field of Ensuring Openness”, approved by Resolution № 910 of the Cabinet of Ministers dated 30 December 2024 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁵² Regulation “On Requirements for the Official Websites of Business Entities with State Participation and State Unitary Enterprises”, approved by Resolution № 81 of the Cabinet of Ministers dated 19 February 2021 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁵³ Regulation “On the Procedure for Establishing and Maintaining the Activities of Official Websites of State Bodies on the Government Portal of the Republic of Uzbekistan Based on the ‘Single Window’ Principle, Ensuring the Relevance and Security of Information Therein, and the Procedure for Submission by State Bodies of Information to Be Posted on the Government Portal”, approved by Resolution № 54 of the Cabinet of Ministers dated 31 January 2025 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁵⁴ Regulation “On the Procedure for Preparing Information Resources of the Republic of Uzbekistan and Disseminating Them through Data Transmission Networks, Including the Internet”, approved by Resolution № 137 of the Cabinet of Ministers dated 26 March 1999 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁵⁵ List of state information resources and state bodies responsible for their formation, use, and maintenance, approved by Resolution № 27 of the Cabinet of Ministers dated 20 February 2006 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁵⁶ Basic Requirements for the Official Websites of State Bodies, Business Associations, and Local Executive Authorities, approved by Resolution № 373 of the Cabinet of Ministers dated 15 June 2021 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁵⁷ <https://www.gov.za/documents/other/national-communication-strategy-framework-2025-2030-26-feb-2025>.

and Information System) system¹⁵⁸; in the United Kingdom, the GCS – Government Communication Service system¹⁵⁹ (formerly, the Rapid Response Unit¹⁶⁰ and the Counter Disinformation Unit (CDU)¹⁶¹; in France, the Service d'Information du Gouvernement (SIG)¹⁶² and VIGINUM¹⁶³; in Germany, the Presse- und Informationsamt / Federal Press Office (BPA) system¹⁶⁴ and the Netzwerkdurchsetzungsgesetz (NetzDG) – Network Enforcement Act¹⁶⁵; in the Philippines, the 8888 Citizens' Complaint Center (Presidential Hotline) system¹⁶⁶; in Australia, the ACMA (Australian Communications and Media Authority)¹⁶⁷; in the United States, the Global Engagement Center (GEC)¹⁶⁸; in Brazil, the Programa de Enfrentamento à Desinformação (Program to Combat Disinformation) of the Superior Electoral Court (TSE)¹⁶⁹; in the Republic of Korea, the Korea Communications Standards Commission (KCSC)¹⁷⁰; in Canada, The Canadian Centre for Cyber Security¹⁷¹; in Latvia, NATO's NATO Strategic Communications Centre of Excellence (NATO StratCom COE)¹⁷²; in Lithuania, Debunk.eu as a public-private partnership model¹⁷³; in Singapore, the Protection from Online Falsehoods and Manipulation Act (POFMA) and the POFMA Office¹⁷⁴; in Taiwan, the Taiwan FactCheck Center (TFC)¹⁷⁵; and in Sweden, the Myndigheten för psykologiskt försvar (Psychological Defence Agency)¹⁷⁶ have been established, through which digital methods for addressing existing problems have been implemented by means of **comprehensive interagency information systems based on artificial intelligence, legislative acts, and the necessary organizations or collegial bodies**, and positive results have been achieved.

It is well known that a number of positive reforms have also been implemented in the Republic of Uzbekistan to ensure information security. In particular, pursuant to Resolution № 555 of the Cabinet of Ministers of the Republic of Uzbekistan dated

¹⁵⁸ <https://www.gcis.gov.za/content/about-us/chief-directorates/media-rapid-response/>

¹⁵⁹ <https://gcs.civilservice.gov.uk/about-us/what-we-do/>.

¹⁶⁰ <https://www.gov.uk/government/news/fact-sheet-on-the-cdu-and-rru?>.

¹⁶¹ <https://www.gov.uk/government/news/fact-sheet-on-the-cdu-and-rru>.

¹⁶² <https://www.info.gouv.fr/organisation/service-d-information-du-gouvernement-sig>.

¹⁶³ <https://www.sgdsn.gouv.fr/viginum>.

¹⁶⁴ <https://www.bundesregierung.de/breg-en/federal-government/federal-press-office?>.

¹⁶⁵ https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html.

¹⁶⁶ <https://8888.gov.ph/>.

¹⁶⁷ <https://www.acma.gov.au/digital-platforms-and-misinformation>.

¹⁶⁸ <https://www.state.gov/gec/>.

¹⁶⁹ <https://www.tse.jus.br/imprensa/noticias-tse/2024/Marco/programa-de-enfrentamento-a-desinformacao-completa-cinco-anos-de-atuacao>.

¹⁷⁰ <https://www.kocsc.or.kr/eng/main.php>.

¹⁷¹ <https://cyber.gc.ca/en/guidance/disinformation>.

¹⁷² <https://stratcomcoe.org/>.

¹⁷³ <https://www.debunk.eu/>.

¹⁷⁴ <https://www.pofmaoffice.gov.sg/>.

¹⁷⁵ <https://tfc-taiwan.org.tw/>.

¹⁷⁶ <https://www.mpi.se/en/>.

24 November 2004, the **Monitoring Center in the Field of Mass Communications was established**¹⁷⁷.

Pursuant to Resolution № 132 of the Cabinet of Ministers dated 28 June 2007, a procedure was established for the **systematic monitoring by the Center for Mass Communications Issues of compliance with legislation in the field of production and distribution of print and book products, television and radio products, audiovisual products, and information resources on the Internet**, as well as for cooperation between the Center and the Expert Commission in the Field of Information and Communications with ministries, agencies, and local government authorities¹⁷⁸.

Pursuant to Resolution № 228 of the Cabinet of Ministers dated 5 August 2011, the **Expert Commission in the Field of Information and Communications was established**, and its regulations and composition were approved¹⁷⁹.

Pursuant to Resolution № 707 of the Cabinet of Ministers dated 5 September 2018, the Regulation on the procedure for restricting access to websites and/or web pages on the Internet containing information prohibited for dissemination under the legislation of the Republic of Uzbekistan; the scheme for restricting access to websites and/or web pages on the Internet containing information prohibited for dissemination under the legislation of the Republic of Uzbekistan; the Regulation on the procedure for exercising state control over compliance with special requirements for the processing of personal data of citizens of the Republic of Uzbekistan; as well as the procedure for **sending notifications** to the owner of a website, the owner of a website and/or messenger page, as well as to a blogger, concerning the removal of information prohibited for dissemination under the legislation of the Republic of Uzbekistan, were approved¹⁸⁰.

Pursuant to Resolution № RP-4452 of the President of the Republic of Uzbekistan dated 14 September 2019, Uzkomnazorat was designated to cooperate with the Agency for Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan on matters relating to ensuring compliance with the requirements of legislative acts and, upon the submission of the Agency for Information and Mass Communications, to take measures in accordance with the established procedure against entities in the

¹⁷⁷ Resolution № 555 of the Cabinet of Ministers of the Republic of Uzbekistan dated 24 November 2004 “On Measures to Improve the Management Structure in the Field of Mass Communications” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁷⁸ Regulation “On the Procedure for Monitoring Compliance with Legislation in the Republic of Uzbekistan in the Field of Production and Distribution of Print and Book, Television and Radio, Audiovisual Products and Information Resources of the Internet”, approved by Resolution № 132 of the Cabinet of Ministers dated 28 June 2007 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁷⁹ Resolution № 228 of the Cabinet of Ministers of the Republic of Uzbekistan dated 5 August 2011 “On Additional Measures to Improve the Monitoring System in the Field of Mass Communications” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁸⁰ Resolution № 707 of the Cabinet of Ministers of the Republic of Uzbekistan dated 5 September 2018 “On Measures to Further Improve Information Security on the World Wide Web” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

information sector that violate the requirements of the legislation of the Republic of Uzbekistan¹⁸¹.

Furthermore, pursuant to Decree № DP–111 of the President of the Republic of Uzbekistan dated 14 July 2025, the **Agency for Information and Mass Communications was abolished**, and its functions and responsibilities in the field of information-sector oversight and monitoring were **transferred to the Inspection for Control in the Sphere of Informatization and Telecommunications**¹⁸².

However, all processes provided for in the above-mentioned documents are carried out by state bodies and organizations using traditional methods. In particular, apart from the **“Digital Control” integrated information system**, no other information systems have officially been put into operation at Uzkomnazorat. **It does not have specialized systems designed specifically for monitoring the information space.**

For this reason, in order to fully address the problems identified above, expose cyber-corruption, ensure transparency, eliminate violations of the law, make effective use of information services and digitalize their activities, as well as transform traditional mechanisms that have not been sufficiently effective into digital form, it is proposed to implement the following measures on the basis of the Resolution of the President of the Republic of Uzbekistan “On Measures to Introduce a Strategic System for Rapid Response to Information in the Media Space that Undermines the National and Public Security of the Republic of Uzbekistan”:

- to approve the Regulation on the Strategic System for Rapid Response to Information in the Media Space that Undermines the National and Public Security of the Republic of Uzbekistan;
- to establish the following:

The system shall be implemented through the **“Digital Public” Interagency Comprehensive Cooperation Information and Communication System** (hereinafter referred to as the **“Digital Public” information system**), introduced at the expense of the Digital Technologies Development Fund and based on artificial intelligence technologies, while meeting information and cybersecurity requirements;

The **“Digital Public” information system** shall constitute a rapid-response system for information disseminated on websites, social networks and messengers that may have a negative impact on public sentiment or misrepresent the actual state of reforms, using artificial intelligence, automated systems and traditional methods (hereinafter referred to as **destructive information**);

The owner of the **“Digital Public” information system** shall be the Ministry of Digital Technologies. Its special users shall include the Expert Commission in the Field of Information and Mass Communications, the Center for Monitoring in the

¹⁸¹ Resolution № RP–4452 of the President of the Republic of Uzbekistan dated 14 September 2019 “On Additional Measures to Improve the System for Monitoring the Implementation of Information Technologies and Communications and Ensuring Their Protection” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁸² Decree № DP–111 of the President of the Republic of Uzbekistan dated 14 July 2025 “On Measures to Increase Efficiency, Proactivity and Effectiveness in the Public Administration System” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

Field of Mass Communications, heads and information service units or persons performing their functions of all bodies, organizations, enterprises and institutions, regardless of their organizational and legal form, in the system of state bodies and organizations in which the state has a share (hereinafter referred to as **state bodies and organizations**), the Inspectorate for Control in the Field of Informatization and Telecommunications, the administrator of the .uz domain, registrars, operators and providers. Their activities shall be fully digitalized through this system;

The **“Digital Public” information system** shall operate on a **24/7** basis. Information and materials generated within and transmitted through the system shall, depending on the required response time, be reviewed by the relevant state body or organization and the results shall be entered into the system no later than **24 hours under the red regime, 48 hours under the yellow regime, and 72 hours under the green regime**;

Clear criteria shall be established to distinguish **“destructive information”** from **“well-founded critical opinion”**, while ensuring the guarantees of freedom of speech and access to information guaranteed to citizens by the Constitution of the Republic of Uzbekistan;

Information services of state bodies and organizations shall exclusively use the **“Digital Public” information system** to fully create, edit, process and perform other necessary actions with any materials and information relating to the activities of the organization in audio, video, textual, graphical and other forms, and shall be able to publish the necessary information on social networks exclusively through this system, while preserving its digital traces;

30 percent of the performance of employees of the information services of state bodies and organizations shall be assessed based on their activities related to working with destructive information through the **“Digital Public” information system**. In addition, reporting to the general public on the work carried out with regard to destructive information shall be established as a separate component of each briefing;

The activities of state bodies and organizations, as well as political processes, shall be conducted in real time through the **“Digital Public” information system**;

Through the **“Digital Public” information system**, the activities of state bodies and other organizations shall be digitalized on the basis of any political or ideological information relevant to the system arising on social networks, while creating the possibility of automatically filtering harmful information and identifying offenders through artificial intelligence;

Using the **“Digital Public” information system**, administrative offense cases and criminal cases shall be processed, the results of necessary inquiries, investigations, prosecutorial supervision and judicial actions shall be entered into the system, and a systematic and unified approach shall be established for communicating the results to the general public.

The adoption of this proposal shall contribute to:

1. improving the activities of information services of state bodies and organizations;

2. enabling the information services of state bodies and organizations to systematically communicate to the population the reforms being implemented by state bodies and organizations, rather than doing so arbitrarily;
3. enabling the information services of state bodies and organizations to create, modify, cancel, remove, edit and perform other necessary actions with information required for content creation in various forms and by various methods within a single information system;
4. generating digital traces of corrupt practices occurring in cyberspace and thereby facilitating the detection of cyber-corruption;
5. enabling the general public, as well as higher-level bodies and officials, to obtain the necessary information concerning the activities of state bodies and organizations and their officials on the basis of well-founded critical opinions expressed in the media space;
6. creating an opportunity for the relevant sector, industry, field or issue to find a lawful and well-founded solution on the basis of necessary critical information;
7. detecting disinformation and destructive information through artificial intelligence and introducing a modern method for determining, by digital means, whether such information falls within the legally established criteria of destructive information;
8. exposing unlawful actions of persons attempting to misrepresent to the population the genuine results of reforms being implemented by the Head of State and officials under the pretext of “destructive information”, preventing violations of the law and ensuring the inevitability of liability for each violation of the law;
9. filling the existing “**legal gap**” and creating an opportunity, through a unified information system based on artificial intelligence, to determine whether matters that have hitherto been carried out through traditional methods and whose actual functioning could not be properly assessed are functioning in practice, are not functioning, or are functioning inadequately, and to promptly implement the necessary reforms;
10. bringing the development of the institution of public oversight to a new stage on the basis of well-founded critical opinions;
11. transforming functions currently performed through traditional methods into digital form;
12. introducing a strategic system for rapid response to information in the media space that undermines the national security of the Republic of Uzbekistan.

The mechanism and basis for implementing this proposal

As a mechanism and basis for implementing this issue, the Head of State could also emphasize it in his Address to the Oliy Majlis in the following wording:

“By a Resolution of the President of the Republic of Uzbekistan, a strategic system for rapid response to information in the media space that undermines the national security of the Republic of Uzbekistan shall be introduced. Through the ‘Digital Public’ Interagency Comprehensive Cooperation Information and Communication System, the activities of state bodies and other organizations, operators and providers, registrars, as well as information services, shall be fully

digitalized on the basis of a unified system, and their activities in dealing with destructive information shall be brought to a new level. Clear criteria distinguishing 'destructive information' from 'well-founded critical opinion' shall be established on the basis of the Law 'On Informatization', creating opportunities for working with such information, identifying and exposing offenses, combating them, automatically restricting harmful information, conducting proceedings on offenses, and communicating the results of administrative and criminal cases to the general public through the system. An opportunity shall also be created to communicate any political situations occurring in our country to the general public through a unified system."

3.3-§. The Social Necessity and Organizational and Legal Mechanisms for Restricting Artificial Intelligence in the Republic of Uzbekistan

Nowadays, artificial intelligence technologies, like digital technologies, are permeating all areas. On the one hand, the fact that they are penetrating all spheres and making users' work easier is commendable; however, life itself dictates the need to exercise caution in using this technology due to a number of factors. In particular:

firstly, they cannot be fully relied upon, and information generated by artificial intelligence as a result of errors or "hallucinations" may lead to serious consequences. Artificial intelligence does not understand truth in the conventional sense; it is considered "artificial" precisely because it operates solely on probabilities and patterns of this kind. For example, artificial intelligence may provide an incorrect conclusion, as a result of which a physician may make an incorrect diagnosis for a patient based on the results of MRI, MSCT, and other medical examinations, potentially even resulting in the loss of the patient's life;

secondly, artificial intelligence systems are considered a prominent manifestation of algorithmic injustice. The provision stipulated in Article 19 of the Constitution of the Republic of Uzbekistan, according to which all citizens in the Republic of Uzbekistan have equal rights and freedoms and are equal before the law regardless of their sex, race, nationality, language, religion, beliefs, social origin, or social status¹⁸³, does not apply in this context at all. Due to deficiencies in training data, such equality may be directly violated;

thirdly, as a result of artificial intelligence engaging in malicious activities, deception through Deepfake videos and images and phishing attacks may arise, disinformation may become widespread, reality may give way to illusion, and hallucinations may occur;

fourthly, from a social perspective, the risk of job losses or reductions due to artificial intelligence emerges and will continue to increase. As a result of automation, many professions and positions may lose their significance and give way to artificial intelligence, thereby further contributing to unemployment and, consequently, giving rise to social inequality;

fifthly, users will increasingly provide artificial intelligence systems with control over their personal data, personal information, and confidential information, while the likelihood that such information will be used by persons pursuing malicious purposes will continue to increase; consequently, the disclosure of such information may undermine the security of individuals, society, and the state;

sixthly, from a psychological and emotional perspective, artificial intelligence may not only suppress an individual's sense of self, but also make the individual dependent on it, causing the person to become accustomed to acting in accordance with its opinions. As a result, children may remain insufficiently protected from information harmful to their health, the psychological well-being and development of young people may be adversely affected, and the risk of the degradation of society

¹⁸³ Constitution of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

may emerge and gradually intensify. Critical thinking may fail to develop among children and young people, which may lead to dependence on ready-made answers and a decline in the quality of education;

seventhly, artificial intelligence systems are considered the primary enemy of security, including information and cybersecurity, and they may enable malicious viruses to spread across networks and systems, causing their complete disruption, information to be seized and destroyed, networks and systems to become completely inoperable, and even other serious consequences to arise, including the commission of crimes;

eighthly, due to content created through artificial intelligence that cannot be distributed across networks, there is a risk that negative information of a pornographic, violent, or other harmful nature may cause damage to society. These technologies may create an inability of humanity to make moral decisions, thereby contributing to the loss of conscience, responsibility, and human values, or causing them to deteriorate;

ninthly, due to artificial intelligence, control over virtually all areas, sectors, fields, infrastructures, and other domains may be lost, which, in turn, may result in serious consequences. Since the decision-making logic of complex models is incomprehensible (black box), and humans may fail to understand why a particular decision has been made, both users and administrators may fail to recognize the emerging risks and may become victims of crime;

tenthly, as a result of artificial intelligence carrying out social manipulation, serious negative phenomena related to political disinformation, market manipulation, and the moral degradation of society may emerge, causing individuals to lose confidence in themselves and potentially become victims of this technology;

eleventhly, laws prepared with the assistance of artificial intelligence may fail to take into account the specific characteristics of a particular territory and field, which may result in “conflicting” norms, as well as mutual misunderstandings and disputes between the population and those responsible for implementation;

twelfthly, due to the absence of strict regulations governing artificial intelligence, copyright, property rights, and other rights and freedoms may be directly violated by it;

thirteenthly, the use of artificial intelligence generates the consumption of very large amounts of energy and water resources, thereby causing environmental degradation;

fourteenthly, as artificial intelligence gradually makes humanity dependent on it, people may begin to use independent thinking, analysis, writing, and calculation less frequently, thereby giving rise to intellectual dependence.

In brief, artificial intelligence is not inherently neutral and safe or fully consistent with human values. If left uncontrolled, it may cause serious harmful consequences; if used irresponsibly, it may create dangerous situations; and if it completely replaces human beings, it may pose a threat to society.

It should not be forgotten that artificial intelligence does not become inherently evil; it is a tool. As a result of introducing harmful information into this tool and giving it harmful instructions, the aforementioned alarming situations may

arise and continue to increase, and if we were to attempt to enumerate them, many more such cases could be identified.

For this reason, serious attention must be paid to this issue. Today, citizens, state bodies, and organizations of the Republic of Uzbekistan are increasingly becoming victims of these risks and cybercrimes. According to data from Cybersecurity Ventures, while the countries of the world suffered losses amounting to USD 6 trillion due to cybercrimes in 2021, this figure amounted to USD 10.5 trillion in 2025¹⁸⁴. The most alarming aspect is that, at present, one out of every 80 prompts submitted by users of artificial intelligence is being used for malicious (illegal or harmful) purposes. Approximately 7.5 percent of all communications contain personal, private, family, or confidential information. At the same time, 12 percent of employees are using artificial intelligence tools such as DeepSeek in the workplace. Notably, 33 percent of the information being disseminated is being assessed as disinformation¹⁸⁵.

The subsequent development of artificial intelligence in the Republic of Uzbekistan has been promoted by the Decree of the President of the Republic of Uzbekistan “On Measures to Increase Efficiency, Proactivity and Effectiveness in the Public Administration System” № DP–111 dated July 14, 2025¹⁸⁶, Resolutions № RP–4996 “On Measures to Create Conditions for the Accelerated Introduction of Artificial Intelligence Technologies” dated February 17, 2021¹⁸⁷, № RP–5234 “On Measures to Introduce a Special Regime for the Application of Artificial Intelligence Technologies” dated August 26, 2021¹⁸⁸, № RP–358 “On Approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030” dated October 14, 2024¹⁸⁹, № RP–320 “On Additional Measures to Support Projects Based on Artificial Intelligence Technologies” dated October 30, 2025¹⁹⁰, Resolutions of the Cabinet of Ministers № 717 “On Approval of the Regulation on the Procedure for Establishing a Special Regime for Supporting Artificial Intelligence Technologies and Organizing Its Activities” dated November 29, 2021¹⁹¹, № 475 “On Organizing the Activities of the Research Institute for the Development of

¹⁸⁴ <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>.

¹⁸⁵ <https://engage.checkpoint.com/2025-ai-security-report/>.

¹⁸⁶ Decree of the President of the Republic of Uzbekistan “On Measures to Increase Efficiency, Proactivity and Effectiveness in the Public Administration System” № DP–111 dated July 14, 2025 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁸⁷ Resolution of the President of the Republic of Uzbekistan “On Measures to Create Conditions for the Accelerated Introduction of Artificial Intelligence Technologies” № RP–4996 dated February 17, 2021 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁸⁸ Resolution of the President of the Republic of Uzbekistan “On Measures to Introduce a Special Regime for the Application of Artificial Intelligence Technologies” № RP–5234 dated August 26, 2021 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁸⁹ Resolution of the President of the Republic of Uzbekistan “On Approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030” № RP–358 dated October 14, 2024 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁹⁰ Resolution of the President of the Republic of Uzbekistan “On Additional Measures to Support Projects Based on Artificial Intelligence Technologies” № RP–320 dated October 30, 2025 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁹¹ Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Approval of the Regulation on the Procedure for Establishing a Special Regime for Supporting Artificial Intelligence Technologies and Organizing Its Activities” № 717 dated November 29, 2021 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

Digital Technologies and Artificial Intelligence” dated July 31, 2021¹⁹², № 425 “On Measures to Implement Priority Projects in the Field of Artificial Intelligence Technologies in 2025–2026” dated July 10, 2025¹⁹³, and other legislative acts. Due to the special attention being paid to this field by the President and the Government, the use of these technologies by the general public has increased, which, in turn, creates a risk that the quantitative and qualitative indicators of the associated risks may reach a new level.

At present, due to this technology, cybercriminals are generating the voices of victims and extorting money from their relatives and acquaintances, creating fake profiles and accounts and carrying out illegal actions on behalf of the victims, and damaging the honor and dignity of victims based on photographic and video information. In brief, while artificial intelligence technologies are, on the one hand, making people’s lives easier, on the other hand, they are becoming one of the greatest threats to humanity.

There are the following three ways to prevent these risks:

it is necessary to properly train and adapt artificial intelligence technology;

persons involved in these technologies, that is, both the technology administrator and the user, must use this technology for its proper purposes and exercise proper control over it;

it is necessary to create the possibility of restricting this technology or (and) its resources and to implement such restrictions properly in practice.

While the implementation of the first and second methods above depends on the administrator and the user, the third depends on the administrator and relevant organizations. It is precisely in this process that, as the practical implementation of the high-level provisions of Article 2 of the Constitution of the Republic of Uzbekistan, according to which the state expresses the will of the people and serves its interests, and state bodies and officials are responsible to society and citizens, the organizational, legal, and technical capabilities for procedures to restrict artificial intelligence technologies or (and) their resources must be fully established.

At present, a number of reforms have also been implemented in Uzbekistan in this regard, in particular:

By the Law of the Republic of Uzbekistan “On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan in Connection with the Regulation of Relations Arising from the Use of Artificial Intelligence” № LRU–1115 dated January 21, 2026¹⁹⁴, with the aim of further developing artificial intelligence technologies, establishing the general framework for the use of artificial

¹⁹² Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Organizing the Activities of the Research Institute for the Development of Digital Technologies and Artificial Intelligence” № 475 dated July 31, 2021 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁹³ Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Implement Priority Projects in the Field of Artificial Intelligence Technologies in 2025–2026” № 425 dated July 10, 2025 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁹⁴ Law of the Republic of Uzbekistan “On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan in Connection with the Regulation of Relations Arising from the Use of Artificial Intelligence” № LRU–1115 dated January 21, 2026 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

intelligence technologies, and protecting the rights and freedoms of citizens in relations arising in this field, the Law of the Republic of Uzbekistan № 560-II “On Informatization” adopted on December 11, 2003, provides for the definition of the concept of “artificial intelligence”; the requirement that information resources created using artificial intelligence and information systems operating on the basis of artificial intelligence technologies must not cause harm to a person, his or her life, health, freedom, honor, dignity, or violate his or her other inalienable rights; the prohibition of relying solely on the conclusions of information resources created using artificial intelligence and information systems operating on the basis of artificial intelligence technologies when making legally significant decisions affecting human rights and freedoms; and the provision that unlawful processing of personal data using artificial intelligence technologies, as well as their dissemination through mass media, telecommunications networks, or the global Internet information network, entails liability. Accordingly, Article 46² of the Code of the Republic of Uzbekistan on Administrative Responsibility establishes administrative liability for the unlawful processing of personal data using artificial intelligence technologies and their dissemination through mass media, telecommunications networks, or the global Internet information network.

Pursuant to Resolution № RP–371 of the President of the Republic of Uzbekistan “On Measures to Improve the System of State Control in the Areas of Information and Digital Technologies” dated December 11, 2025, the Inspection for Control in the Sphere of Informatization and Telecommunications under the Ministry of Digital Technologies was designated as a specially authorized state body responsible for monitoring and controlling activities in the field of artificial intelligence, information systems and resources, databases, digital services, and software¹⁹⁵.

However, despite the establishment of oversight and liability in this field today, the absence of a procedure for restricting the technology and its resources, as well as the lack of sufficient resources and human capacity within the authorized body for this purpose, necessitates a number of reforms in this area.

In particular, although the Rules of Ethics for the Development, Implementation, and Use of Artificial Intelligence-Based Solutions were approved by Order № 284-mh of the Minister of Digital Technologies of the Republic of Uzbekistan dated February 24, 2026 (registered on March 14, 2026, № 3787), establishing the principles and requirements for the development, implementation, and use of artificial intelligence-based solutions, as well as the rights and obligations of participants in artificial intelligence-related activities¹⁹⁶, the fact that specific mechanisms for their implementation and oversight have not yet been established demonstrates the need for necessary reforms in this area.

¹⁹⁵ Resolution of the President of the Republic of Uzbekistan “On Measures to Improve the System of State Control in the Areas of Information and Digital Technologies” № RP–371 dated December 11, 2025 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁹⁶ Rules of Ethics for the Development, Implementation, and Use of Artificial Intelligence-Based Solutions, approved by Order № 284-mh of the Minister of Digital Technologies of the Republic of Uzbekistan dated February 24, 2026 (registered on March 14, 2026, № 3787) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

Therefore, in order to prevent the risks associated with artificial intelligence, to combat them systematically and comprehensively in a timely manner, to protect the future of humanity, and to eliminate serious adverse consequences, the following is proposed:

Adoption of the Law of the Republic of Uzbekistan “On Artificial Intelligence” and, on its basis, introduction of amendments and additions to legislative acts, including Resolution № 707 of the Cabinet of Ministers “On Measures to Further Improve Information Security on the World Wide Web” dated September 5, 2018¹⁹⁷, as well as other relevant documents. In particular, in the aforementioned Resolution of the Government:

To supplement paragraph 1 with a separate paragraph stating: “unlawful processing of personal data using artificial intelligence technologies and their dissemination through mass media, telecommunications networks, or the global Internet information network”;

Taking into account that restricting artificial intelligence differs in certain respects from restricting access to an Internet website and/or web pages, a Regulation or Procedure providing for a separate procedure for such restriction should be approved, and these processes should also be reflected in a corresponding scheme.

It is also advisable to establish in the current legislative acts the organizational and legal measures for ensuring information and cybersecurity in information systems, platforms, websites, and other technical means incorporating artificial intelligence, including the regulation of relations concerning all forms of logging and storage of digital traces, as well as the collection, storage, submission, and processing of electronic information and digital evidence.

In addition, the Register of Internet networks containing information whose dissemination is prohibited under the legislation of the Republic of Uzbekistan should contain a separate section (column) specifically related to artificial intelligence, through which accurate statistics on restricted artificial intelligence systems and the information contained therein should be maintained.

When working with artificial intelligence, the fact that a significant portion of the servers and databases of these technologies are located in foreign countries and that their management is carried out by representatives of the private, state, or non-governmental sectors may create numerous problems in ensuring the security of personal and private data of citizens of the Republic of Uzbekistan. Therefore, it is extremely important that relations in this area be regulated by our legislation and international instruments.

Adoption of these proposals would:

enable citizens, when faced with an error or unfairness of artificial intelligence, to clearly understand under which legal provision they can protect their rights, thereby ensuring their legal protection;

¹⁹⁷ Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Further Improve Information Security on the World Wide Web” № 707 dated September 5, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

create a systematic mechanism for combating Deepfake, phishing, and disinformation (through registers and restrictions), thereby making it possible to achieve a significant reduction in the number of victims of fraud;

prevent algorithmic unfairness and discrimination, while establishing human oversight over artificial intelligence decisions would prevent technological judgments from being made in vital areas such as medicine and the judiciary;

establish a system for protecting young people and children from the negative effects of artificial intelligence (intellectual dependence and harmful content), thereby making it possible to preserve critical thinking and independent decision-making skills in society;

ensure that, even when citizens' personal data is stored on foreign servers, legal guarantees at the international and national levels and a technical logging system are established for their security, thereby preventing threats to national security.

3.4-§. Strategic Provision of Protection of Children from Information Harmful to Their Health and Social Protection

The rapid development of information and communication technologies and the advancement of artificial intelligence technologies necessitate the improvement of methods for ensuring guarantees of the child's right to information, which, in turn, requires the improvement of legislation. In particular, the need to improve legislation concerning the provision of guarantees of the child's right to information is as follows:

Over the past period, extensive work has been carried out to ensure guarantees of the child's right to information. In particular, for the purpose of ensuring guarantees of the child's right to information, **10** Laws of the Republic of Uzbekistan, **1** Decree and **2** Resolutions of the President of the Republic of Uzbekistan, and **3** Resolutions of the Cabinet of Ministers have been adopted, and the necessary reforms have been implemented in this area.

In particular, the Law of the Republic of Uzbekistan "On the Protection of Children from All Forms of Violence" № LRU-996 dated November 14, 2024 regulates the area of protecting children from all forms of violence and establishes the powers of more than 10 agencies in protecting children from all forms of violence¹⁹⁸.

However, the implementation of the current legislative acts demonstrates that a number of reforms still need to be continued in order to fully ensure the rights of children.

In particular, Article 16 of the Law of the Republic of Uzbekistan "On Guarantees of the Rights of the Child" № LRU-139 dated January 7, 2008 provides that every child has the right to seek, receive, and disseminate any information, **except for restrictions provided for by law**, while Article 17 of the Law stipulates that the child's freedom of thought and expression may be restricted in accordance with the procedure established by law¹⁹⁹.

However, the current law does not contain **specific provisions prohibiting the dissemination of information that is harmful to the child's health, moral and spiritual development** through telecommunications networks, including the global Internet information network, social networks, and messengers, **nor does it contain specific provisions for restricting the child's freedom of thought and expression or a mechanism for implementing such restrictions and preventing the child from accessing such information.**

The restriction provided for by law is partially stipulated in Article 21 of the Constitution of the Republic of Uzbekistan²⁰⁰, Article 12¹ of the Law of the Republic

¹⁹⁸ Law № LRU-996 of the Republic of Uzbekistan "On the Protection of Children from All Forms of Violence" dated November 14, 2024 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

¹⁹⁹ Law № LRU-139 of the Republic of Uzbekistan "On Guarantees of the Rights of the Child" dated January 7, 2008 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁰⁰ Constitution of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

of Uzbekistan “On Informatization”²⁰¹, and Resolution № 707 of the Cabinet of Ministers “On Measures to Further Improve Information Security on the World Wide Web” dated September 5, 2018, adopted on its basis²⁰². This restriction, however, is established generally not only for children but also for individuals, society, and the state.

However, these legislative acts do not provide guarantees of the preferential rights of children in relation to other persons or a mechanism for exercising such rights.

As a result, today the amount of information on telecommunications networks and the Internet that may adversely affect the psychological well-being, future, moral development, and maturation of children has increased excessively, and its direct access and use by the younger generation is giving rise to a number of problems, in particular:

1) the absence of a legally established procedure for exercising children’s rights to their own image is resulting in an increase in cases of abuse of children’s images by parents or third parties.

For information: Today, it has become common to use children’s images on Instagram, Telegram, and other popular social networks without the joint consent of the parents in order to obtain additional income; however, the failure to direct the resulting income toward the child’s future places issues related to the child’s education and upbringing at risk. It should be emphasized that, **under Law № 2024-120 of the French Republic “On Guaranteeing Respect for Children’s Right to Their Image” dated February 19, 2024**, the following provisions have been established, including:

*Parents must jointly protect the right of their minor child to his or her image, while respecting it as a **right relating to the child’s private life**.*

Parents may involve the child in exercising his or her right to an image, taking into account the child’s age and level of maturity.

***In exercising the child’s right to his or her image, the parents must reach an agreement with each other.** If the parents cannot reach an agreement regarding the exercise of the child’s right to his or her image, the court may prohibit one of the parents seeking consent from disseminating any content concerning the child without the consent of the other parent.*

If the dissemination of the child’s image by the parents causes serious harm to the child’s dignity or moral integrity**, the person who has taken the child into care, an institution, a child social protection service, or a family member may apply to the court **to request the authority to exercise the child’s right to his or her image²⁰³.

Under the legislation of California (the Coogan Act²⁰⁴), earnings of child influencers must be held for them in a trust account, and its administration is carried out jointly by the parents.

2) The absence of a minimum age limit for children’s use of social networks and content, as well as the lack of mechanisms for monitoring compliance with such a limit, increases the likelihood of children becoming dependent on phones, smartphones, and other gadgets, exposing them to harmful information through telecommunications networks and the Internet.

²⁰¹ Law № 560-II of the Republic of Uzbekistan “On Informatization” dated December 11, 2003 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁰² Resolution № 707 of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Further Improve Information Security on the World Wide Web” dated September 5, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁰³ <https://www.legifrance.gouv.fr/download/pdf?id=wSCtx11Gzpq9uWOcYXc7s1sDFihSq-tW46KWa2ISZzs=>.

²⁰⁴ <https://www.sagafta.org/membership-benefits/young-performers/coogan-law/coogan-law-full-text>.

For information: In Australia, children under the age of 16 are prohibited from opening accounts on social networks. All social networks and messengers are required to use a dedicated platform for age verification, and information collected without the user's explicit, informed, and voluntary consent may not be used for purposes other than those for which it was collected. The **eSafety Commissioner** and the **Information Commissioner** have been granted powers to request information from users and other entities for the purpose of monitoring compliance, issue warnings to platforms that fail to comply with the rules, make such non-compliance public, and impose fines²⁰⁵.

Under French Law № 2023-566 of July 7, 2023, on the introduction of a digital age of majority and combating online hate, the right to self-expression, privacy, security, and protection against threats and harassment of any kind is recognized as a right of the child. Online social network services operating in France may register children under the age of 15 only with the consent of one of their legal representatives. Platforms providing online social network services must provide users under the age of 15 and their parents with information about digital risks and means of protection. The law allows legal representatives to request the temporary suspension of the account of their child under the age of 15. The user's activity time must be monitored, and their parents must be informed thereof through notifications. Age and consent verification must be carried out through technical solutions specified by the regulator (in cooperation with ARCOM and CNIL). If social network services fail to comply with these requirements, the President of ARCOM may issue an official warning and subsequently apply to the Paris Court, and the offender may be subject to a fine of up to 1% of its worldwide annual turnover. With regard to complaints concerning children's access to content, measures must be taken within 10 days after receipt of the complaint, and where serious risks to individuals are involved, within 8 hours²⁰⁶.

For example, France, Spain, Italy, Denmark, and Greece are currently testing applications designed to determine the age at which children may access online networks. In 2024, ***Australia made an age-verification system mandatory for users under the age of 16, based on biometric data or government-issued identification***²⁰⁷

In Italy, the use of smartphones and tablets by students in schools is prohibited²⁰⁸; ***in the Netherlands,*** the use of smartphones in classrooms is prohibited in certain cases²⁰⁹; ***while in Germany,*** schools have been granted the authority to prohibit the use of smartphones²¹⁰.

3) There is no separate liability for violating the age classification requirements for information products on telecommunications networks, including the global Internet, violating the age requirement for children's registration on social networks and messengers, unlawfully posting a child's image on telecommunications networks or deriving profit therefrom, as well as permitting such acts to be committed, and posting and disseminating information on telecommunications networks that is harmful and detrimental to the child's identity, development, and moral well-being. This, in turn, is resulting in the non-compliance with the generally binding norms and principles established in this area.

²⁰⁵ chrome-

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.infrastructure.gov.au/sites/default/files/documents/social-media-minimum-age-and-age-assurance-trial-fact-sheet.pdf.

²⁰⁶ https://www.legifrance.gouv.fr/download/pdf?id=uixn4vDFFJU_veW4xSVamq3PzXyh2U2x_naRfEud_Wg=.

²⁰⁷ https://www.reuters.com/sustainability/boards-policy-regulation/five-eu-states-test-age-verification-app-protect-children-2025-07-14/?utm_source=

²⁰⁸ <https://www.mim.gov.it/web/guest/home>.

²⁰⁹ <https://www.rijksoverheid.nl/>.

²¹⁰ <https://www.km.bayern.de/>.

For information: Articles 189 and 189¹ of the Code of the Republic of Uzbekistan on Administrative Responsibility establish separate liability only for the production, import, distribution, advertising, and demonstration of products promoting pornography, coercion, violence, or cruelty; however, **there is no separate liability for the dissemination of information that does not fall within these categories but is harmful to the health and moral well-being of children, or for deriving profit therefrom, nor for the unlawful use of a child's image.**

In the Russian Federation, Article 151.2 of the “Criminal Code” provides for a fine of 100,000 rubles, compulsory community service for up to 440 hours, corrective labor for up to 2 years, or imprisonment for up to 3 years for involving minors in the commission of acts that pose a danger to their lives or demonstrating such acts through mass media²¹¹.

Article 33 of the Law of the People's Republic of China “On the Protection of Minors” establishes criminal liability for persons who sell, rent, and/or distribute materials harmful to minors. This includes audiovisual products, electronic publications, and online information concerning pornography, violence, murder, terrorism, and gambling. Violation of the requirements of the legislation of the Russian Federation on the protection of children from information that may affect their health and development constitutes an administrative offense under Article 6.17 of the Code of Administrative Offenses of the Russian Federation.

At the same time, violation by the owner of an audiovisual service of the established procedure for disseminating information that may affect the health and development of children constitutes grounds for administrative liability under Article 13.36 of the Code²¹².

Article 156-1 of the Code of the Republic of Kazakhstan on Administrative Offenses provides for liability for violating legislation on the protection of children from information that may affect their health and development, namely:

1. Dissemination of publications without an age-group designation;
2. Failure to comply with the established time restrictions when distributing information products containing information intended for persons aged “18 and over” through television and radio broadcasting;
3. Distribution of information products without announcing the age category at the beginning of a television or radio program, as well as without indicating the age-group designation for each subsequent broadcast after the end of interruptions;
4. Dissemination of audiovisual and/or printed products without age-related designations²¹³.

Furthermore, in France²¹⁴, the United States²¹⁵, the United Kingdom²¹⁶, Belgium²¹⁷, the Netherlands²¹⁸, Norway²¹⁹, Germany²²⁰, Australia²²¹, Italy²²², and Spain²²³, the age of children must be subject to mandatory technical verification when they access their own profiles or accounts. Violation of this requirement entails liability. In particular, in France, the joint consent of the parents is required for children under the age of 15 to open their own accounts on social networks, and violation of this requirement may result in a fine imposed by ARCOM amounting to

²¹¹ <http://pravo.gov.ru/>.

²¹² <http://en.npc.gov.cn.cdurl.cn/>.

²¹³ <https://adilet.zan.kz/kaz/>.

²¹⁴ <https://www.arcom.fr/>.

²¹⁵ https://www.ft.com/content/846e8253-85f0-4666-9655-d9689eb0843f?utm_source.

²¹⁶ <https://www.legislation.gov.uk/ukpga/2023/50/contents>.

²¹⁷ <https://www.dataprotectionauthority.be/citizen>.

²¹⁸ <https://www.autoriteitpersoonsgegevens.nl/>.

²¹⁹ <https://www.medietilsynet.no/>.

²²⁰ <https://www.bzkg.de/>.

²²¹ <https://www.esafety.gov.au/>.

²²² <https://www.garanteprivacy.it/>.

²²³ <https://www.aepd.es/>.

1% of the offender's global revenue²²⁴. In Australia, children under the age of 16 are prohibited from using social networks, and violation of this requirement may result in a fine of up to USD 50 million being imposed on the respective platform operators²²⁵.

4) No specific mechanism has been established for the application of separate liability for violating the age classification requirements for information products on telecommunications networks, including the global Internet, violating the age requirement for children's registration on social networks and messengers, unlawfully posting a child's image on telecommunications networks or deriving profit therefrom, as well as permitting such acts to be committed, and posting and disseminating information on telecommunications networks that is harmful and detrimental to the child's identity, development, and moral well-being. This, in turn, means that the lack of clearly defined tasks in this area is resulting in the relevant authorities failing to adequately fulfil the goals and objectives that have been established.

For information: In Germany, indicating the age rating of information products in content is mandatory, and compliance is monitored by the Federal Working Group for the Protection of Youth and Kommission für Jugendmedienschutz (KJM) – Commission for the Protection of Minors in the Media²²⁶. In the United Kingdom, measures of liability arising in relation to children's information rights are applied by the ICO (Information Commissioner's Office)²²⁷; in the United States, by the Federal Trade Commission (FTC)²²⁸; in South Korea, by the Korea Communications Standards Commission (KCSC)²²⁹; in France, by ARCOM²³⁰; and in Germany, by KJM²³¹.

Pursuant to Resolution № RP-4452 of the President of the Republic of Uzbekistan dated September 14, 2019, "On Additional Measures to Improve the System for Monitoring the Implementation of Information Technologies and Communications and Their Protection," and other legislative acts, the traditional methods-based processes between the Ministry of Digital Technologies, the Ministry of Internal Affairs, the Inspection for Control in the Sphere of Informatization and Telecommunications, the Agency of Information and Mass Communications, the Center for Mass Communications, relevant operators and providers, and registrars of the .uz domain are currently proving ineffective due to the absence of prompt digital interagency communication among them, the lengthy periods for reviewing violations, the increasing number of similar violations during such periods, and the insufficiently defined powers and obligations of the competent authorities in identifying offenders and bringing them to liability.

At the same time, following the monitoring conducted by the Center for Mass Communications, a conclusion is prepared; however, the audio, video, and other necessary evidence substantiating the circumstances stated in the conclusion is not actually submitted to the competent authorities. In practice, the processes for suspending the activities of telecommunications providers do not operate in an automated manner, the level of response to violations of the law remains highly passive, and the implementation of insufficiently substantiated

²²⁴ https://www.reuters.com/technology/what-countries-do-regulate-childrens-social-media-access-2024-11-28/?utm_source.

²²⁵ https://www.theguardian.com/media/2024/nov/29/how-australias-tough-social-media-ban-compares-to-laws-in-other-countries?utm_source.

²²⁶ <https://www.kjm-online.de/>.

²²⁷ <https://ico.org.uk/>.

²²⁸ <https://www.ftc.gov/>.

²²⁹ <https://service.kocsc.or.kr/eng/mainPage.do>.

²³⁰ <https://www.arcom.fr/>.

²³¹ <https://www.die-medienanstalten.de/organisation/kjm/>.

violation-related materials submitted to the internal affairs bodies is not adequately ensured due to the failure to identify the offender and the lack of sufficient evidence proving the commission of the violation.

5) There is no system for detecting violations of children's information rights on the Internet using artificial intelligence (AI). As a result, cases arise in which children's information rights are not restored in a timely manner.

For information: There are currently international and national platforms involved in protecting or monitoring children's information rights, including Google's Google Family Link, which provides tools for monitoring children's activities and managing content access; YouTube Kids, which offers age-appropriate content, filtering, and parental control tools; EU Kids Online, which conducts research on children and Internet safety in the European Union; Net Nanny, which provides online content filtering and safe browsing for children in the United States; Qustodio, which provides child activity monitoring and online activity control in the United States and Spain; UNICEF Child Online Protection Guidelines, which provide worldwide guidelines for protecting children in the digital environment; CyberTipline, which enables reporting of child abuse and violations of children's rights in the United States; and Be Internet Awesome, a program developed by Google and UNICEF to teach children information literacy.

"Microsoft Security AI" and "Microsoft AI for Anti-Terrorism," developed by Microsoft²³²; "AI-Powered Government Systems," developed by Interpol²³³; "Google Jigsaw," developed by Google Jigsaw²³⁴; in **China**, "Smart Policing AI," developed by Alibaba; and in the **United Kingdom**, "Gato," developed by Google DeepMind, and "Moonshot CVE," developed by Moonshot CVE, are examples of artificial intelligence technologies that serve precisely to fulfil the above-mentioned requirements²³⁵.

At the same time, **in China**, through artificial intelligence technologies such as "AI-Powered Computing & Big Data Analysis," "Alibaba Cloud AI Speech & Image Recognition," and "Smart Policing AI," developed by Alibaba At the same time, **in China**, through artificial intelligence technologies such as "AI-Powered Computing & Big Data Analysis," "Alibaba Cloud AI Speech & Image Recognition," and "Smart Policing AI," developed by Alibaba²³⁶; "Tencent YouTu AI" and "Tencent Speech AI," developed by Tencent AI²³⁷; and **in the Republic of Korea**, "Face Recognition & Voice Control," developed by Samsung AI, it is possible to protect the interests of individuals, society, and the state, prevent crimes, and detect and solve crimes²³⁸.

In the **United Kingdom**, an automated monitoring system has been established through the "**Children's Code**" (**Age-Appropriate Design Code**).²³⁹

However, the Republic of Uzbekistan has not yet established mechanisms for the operation of artificial intelligence technologies in this area, which results in all processes being carried out through traditional methods and contributes to an increase in the number of violations.

6) Reforms aimed at ensuring children's right to quality information have not yet proved sufficiently effective. In particular, pursuant to Resolution № RP–191 of the President of the Republic of Uzbekistan dated September 28, 2005, "**On the Establishment of the Public Education Information Network of the Republic of Uzbekistan**," the "**ZiyoNET**" information network was established,

²³² <https://www.microsoft.com/en-us/security>.

²³³ <https://www.interpol.int/>.

²³⁴ jigsaw.google.com.

²³⁵ <https://moonshotteam.com/>.

²³⁶ <https://www.alibabacloud.com/>.

²³⁷ <https://www.tencent.com/en-us/articles/2202171.html>.

²³⁸ <https://research.samsung.com/>.

²³⁹ <https://ico.org.uk/>.

and “Uzinfocom” LLC was designated as its operator²⁴⁰. The main functions of this network include the following:

1. **For young people, to create and develop national information resources** aimed at increasing the effectiveness of their patriotic education and fostering mature individuals with an active civic position;
2. **Taking into account the national interests of Uzbekistan, to ensure broad access to social and political, socio-economic, analytical, spiritual and educational, scientific and educational, as well as other information** that contributes to the spiritual and intellectual development of young people;
3. **To promote a healthy lifestyle among young people** and assist in the **introduction of distance learning methods and a comprehensive range of other information and communication services into the education system** for pupils and young people of the Republic.

The aforementioned Presidential Resolution stipulates that **the connection of schools, academic lyceums, colleges, higher education institutions, youth organizations, libraries, museums, and other scientific, educational, cultural, and educational institutions of the country to international information networks, including the Internet, shall be carried out exclusively through the “ZiyoNET” network. However, in practice, the network has not been adequately developed.**

For reference: the network has 47,802 users, 117,594 information resources, 8,274 audio resources, and is interconnected with 5,455 websites. As of January 1, 2025, the permanent population of Uzbekistan had reached 37.5432 million. Relative to the population of Uzbekistan, the number of resources available on the network is approximately 320 times lower, the number of audio resources 4,538 times lower, and the number of users 786 times lower.

The further development of this network at the level of legislative and regulatory acts **has been neglected since 2019.**

At a time when there are **more than 15,000 online platforms for learning foreign languages**, the “ZiyoNET” network still contains predominantly educational materials based on outdated and traditional approaches.

For reference: in China, a highly advanced neural network has been developed for pupils and students, incorporating almost all available educational materials, including books, articles, theses, monographs, teaching and methodological manuals, dissertations, reports, and databases on a wide range of subjects. Access to this resource is completely free, and its extensive opportunities for users are reportedly contributing to a reduction in the number of negative perceptions of China expressed on social media. By providing users with broad educational opportunities and encouraging their engagement in learning, the platform may also help reduce their susceptibility to radical ideas²⁴¹. Despite the possibility of creating similar opportunities in the Republic of Uzbekistan, the existing problems have still not been adequately addressed, even through the “ZiyoNET” network.

At the same time, the information resources available on the “ZiyoNET” network are not sufficiently systematized according to age groups, and users are not provided with adequate convenience when accessing and using the network. In

²⁴⁰ Resolution № RP–191 of the President of the Republic of Uzbekistan “On Establishing the Public Education Information Network of the Republic of Uzbekistan” dated September 28, 2005 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁴¹ <https://www.bohrium.com/>.

particular, the network lacks **AI-powered chatbots**, its **search functionality is insufficiently effective**, and the number of available **relevant educational and academic resources is limited**. As a result, the number of users of the network has been declining year by year. Even among those who remain registered, actual use of the network is extremely limited, with many users having merely completed authorization or registration in order to access the system when necessary.

*For reference: the “Duolingo” platform has **more than 700 million users**²⁴², whereas the number of users of the “ZiyoNET” network is **48,463**, which means that the former has nearly **15,000 times more users** than the latter²⁴³.*

It should be emphasized that, currently, there are more than **1,000 mobile applications** in the Republic that can be downloaded through the “Google Play” application and contain social-network content in the form of dating, conversation, interpersonal communication, chatbots, video, audio, text, and videoconferencing, and the technical capacity to disseminate information harmful to children’s health through these messengers is fully available, i.e. **100 percent**. Since the databases of a very large proportion of these applications are physically located in the territories of other states, and the requirements of legislation concerning personal data are being violated on a continual basis, information harmful to children’s health is becoming increasingly widespread.

*For information: among the aforementioned mobile applications, **11** have more than **1 billion** users, **6** mobile applications have more than **500 million**, **10** mobile applications have more than **100 million**, **6** mobile applications have more than **50 million**, **34** mobile applications have more than **10 million**, and **21** mobile applications have more than **5 million** users, which may expose the global population to radicalism. Through these mobile applications alone, **482,329,545 people** become victims of cyberbullying in a single day. When compared with the population of Uzbekistan, these figures are almost **13 times** higher.*

7) Currently, the digital ecosystem in the Republic of Uzbekistan is highly developed; however, there are no clear standards for content created on websites, messengers and their pages, social networks, and other information resources, and no rules of conduct for using the network have been established, which contributes to an increase in the number of network users.

*For information: the number of mobile communication users (subscribers) was **26,566,759** in 2020, **26,953,435** in 2021, **31,981,910** in 2022, **34,217,491** in 2023, and **35,798,804** in 2024. According to the Speedtest Global Index ranking, the average speed of mobile Internet increased from **6.6 Mbps** in 2020 to **12.1 Mbps** in 2021, **13.7 Mbps** in 2022, **21.3 Mbps** in 2023, and **38.96 Mbps** in 2024. In this context, the Republic of Uzbekistan ranks **74th** in the global ranking in terms of **mobile communication speed** and **72nd** in terms of **wired communication**. **95.5 percent** of the population of the Republic of Uzbekistan **fully use mobile communications**.*

In order to ensure guarantees of children’s information rights and protect them from information harmful to their health, it is proposed to adopt a Resolution of the President of the Republic of Uzbekistan providing for the implementation of the following measures:

1. Establish 16 years as the minimum age for children to create personal accounts on social networks and messengers, assign responsibility for ensuring compliance with this requirement to their parents and persons acting in their place,

²⁴² <https://ru.duolingo.com/>.

²⁴³ <https://ziyonet.uz/uzc>.

as well as educational organizations, and reflect these provisions in the Laws of the Republic of Uzbekistan “**On Guarantees of the Rights of the Child**” and “**On Protecting Children from Information Harmful to Their Health**”;

2. Define a child’s image as his or her personal data and ensure its protection, provide for the rights and obligations concerning the use of a child’s image by the child’s parents and persons acting in their place, as well as third parties, in the Law of the Republic of Uzbekistan “On Guarantees of the Rights of the Child” and, based on this, introduce amendments and additions to the Law of the Republic of Uzbekistan “On Personal Data” and the Family Code;

3. With regard to violations of guarantees of children’s information rights:

a) establish liability for violating the age classification of information products on telecommunications networks, including the worldwide Internet, violating the age requirement for children to register on social networks and messengers, unlawfully posting their personal data on telecommunications networks or deriving profit therefrom, as well as allowing operators and providers to permit the commission of such acts;

b) in addition to those provided for in Articles 189–189¹ of the Code of Administrative Responsibility, **establish administrative liability** in Articles 189³–189⁴ of the Code of Administrative Responsibility for posting and disseminating information on telecommunications networks that harms the child’s personality, development, and morality and is harmful to the child;

4. Provide for the following by a Government resolution:

approve and introduce mandatory technical requirements for determining a child’s age and the age classification of information products on social networks and messengers, as well as the procedure for determining them through a mobile application using artificial intelligence technologies;

establish a **personal bank account for a child for the use of the child’s image, including for its advertising**, determine the procedure for using and disposing of these funds, while imposing on the child’s parents and persons acting in their place the obligation to open a separate bank account for the child for the use of the child’s personal data, including for its advertising;

bring the Resolution of the Cabinet of Ministers № 137 dated March 26, 1999 “On Approval of the Regulation on the Procedure for Preparing Information Resources of the Republic of Uzbekistan and Distributing Them through Data Transmission Networks, Including the Internet” into line with current requirements, providing for the procedure for posting and disseminating a child’s personal data on the network and the rules for using the network;

5. Instruct the Ministry of Digital Technologies to carry out the following measures at the expense of the Digital Technologies Development Fund:

ensure the development and implementation by “Uzinfocom Unified Integrator” LLC of the “**Child Protection**” information system and provide for its permanent technical support;

establish the operation of the “**Child Protection**” **mobile application**, incorporating artificial intelligence technologies and “smart systems” that automatically detect cases of violating the age classification of information products

on telecommunications networks, including the worldwide Internet, violating the age requirement for children to register on social networks and messengers, unlawfully posting their personal data on telecommunications networks or allowing profit to be derived therefrom;

receive, on a 24/7 basis, applications concerning violations of children's information rights through the **“President's Virtual Reception”** system and the **“112” unified dispatch service**,

and introduce a separate module in the **“President's Virtual Reception”** system for mandatory posting of the results of their consideration by authorized agencies and integrate it with the **“Child Protection”** information system;

ensure full integration with the information systems of interested agencies and complete the implementation of this information system in the activities of interested ministries and agencies;

establish a system whereby monitoring of children's access to social networks inappropriate for their age is carried out using artificial intelligence through the **“Child Protection”** information system and its mobile application, with parents and persons acting in their place, as well as authorized agencies, being notified;

establish in the **“Child Protection”** information system the automatic generation of drafts of expert opinions, conclusions, requests, instructions, and other documents, an analysis system based on artificial intelligence, as well as, through the **“Protection from Harmful Information”** module, interagency digital cooperation between state bodies and other organizations concerning the protection of children's rights; through the **“Legal Representative Control”** module, provide parents with the ability to monitor their children's use of the network and authorized agencies with the ability to conduct monitoring; and through the **“Child Rights Monitoring”** module and other modules, establish a system for maintaining a summary of the activities carried out by state bodies and other organizations to protect children's rights;

on the **“ZiyoNET”** educational portal, form the necessary information resources through the Unified Identification System of citizens of the Republic of Uzbekistan, transfer all useful information resources available in the Republic to this portal, integrate it with the necessary websites, information systems, and other social networks, place information resources taking into account children's age in relation to information products, and launch an updated version of the artificial-intelligence-based **“ZiyoNET”** educational portal, which is highly convenient for users and provides the ability to find and use the necessary information through artificial intelligence technology;

take necessary measures to develop all necessary information resources on the **“ZiyoNET”** educational portal for children under 16 years of age that are not harmful to their health.

6. The Ministry of Higher Education, Science and Innovation, the Ministry of Preschool and School Education, and all organizations within whose systems educational organizations operate:

shall be obliged to identify the information resources necessary for users and take the necessary measures to place them on the **“ZiyoNET”** educational portal,

with control thereof being carried out by the Inspectorate for Control in the Sphere of Informatization and Telecommunications;

issue the necessary instructions to ensure, together with parents, that the “Child Protection” mobile application is active on the smartphone used by a child under 16 years of age, or that it is integrated with the “Child Protection” information system.

7. In order to ensure guarantees of children’s information rights, establish the following new system:

parents and persons acting in their place, as well as third parties, shall have the opportunity to submit applications concerning violations of children’s rights through the “**Child Protection**” mobile application, the “**President’s Virtual Reception**” system, the “**112**” unified dispatch service, or other means;

the Ministry of Internal Affairs, the National Agency for Social Protection, the Inspectorate for Control in the Sphere of Informatization and Telecommunications, the Center for Mass Communications Issues, telecommunications operators and providers, and registrars shall regularly monitor violations of children’s information rights on telecommunications networks and the worldwide Internet information network, receive applications, and post the monitoring results and their conclusions concerning applications in the “**Child Protection**” information system;

the Inspectorate for Control in the Sphere of Informatization and Telecommunications shall, **within 10 days**, obtain information concerning the offender in the uz. domain from the Registrar through its instruction and enter the results into the “**Child Protection**” information system;

if it is established that the information and documents requested by the Inspectorate for Control in the Sphere of Informatization and Telecommunications have not been provided in full, the Ministry of Digital Technologies shall temporarily suspend the activities of the relevant operator or provider for violating legislation in the telecommunications sphere until the violation is eliminated and shall enter the results into the “**Child Protection**” information system;

the National Agency for Social Protection shall review the conclusion and the materials indicated as the basis thereof **within 5 days**, place its expert opinion in the “**Child Protection**” information system, and carry out the procedures provided for by legislation concerning the issuance of a protection order to a child who has suffered violence;

within 10 days from the time the expert opinion is posted, the Ministry of Digital Technologies shall ensure the restriction of the relevant information in accordance with the requirements of legislation on informatization

and enter the results into the “**Child Protection**” information system;

the Ministry of Internal Affairs shall fully establish the identity of the offender and, having carried out inquiry actions, ensure that the administrative offence report and submission based on the results thereof are made available in the “**Child Protection**” information system;

courts and compulsory enforcement bodies shall be responsible for ensuring that court decisions concerning offences involving violations of guarantees of

children's information rights and their enforcement are made available in the **“Child Protection”** information system;

the Children's Ombudsman shall monitor the implementation of legislative acts concerning guarantees of children's rights by the relevant state bodies and organizations and shall take the necessary measures in cases of violations of the law;

the Ministry of Digital Technologies shall, within the framework determined by the Children's Ombudsman, ensure the technical capability for the Children's Ombudsman, the Ministry of Internal Affairs, the National Agency for Social Protection, the Inspectorate for Control in the Sphere of Informatization and Telecommunications, the Center for Mass Communications Issues, the Supreme Court, the Bureau of Compulsory Enforcement, telecommunications operators and providers, as well as registrars, to fully and adequately use the **“Child Protection”** information system.

8. In order to ensure the full and adequate implementation of guarantees of children's information rights at the local level, instruct the Ministry of Justice, the National Agency for Social Protection, the Children's Ombudsman, the Prosecutor General's Office, the Ministry of Internal Affairs, the Ministry of Preschool and School Education, and the Committee on Family and Women to properly organize the explanation at the local level of the substance and significance of the new procedure concerning guarantees of children's information rights.

The adoption of these proposals will serve to guarantee the information rights of children who are citizens of the Republic of Uzbekistan and ensure their protection from harmful information.

CHAPTER IV. ENSURING JUSTICE AND COMBATING CYBERCRIME

4.1-§. Improving the Criminal-Law and Organizational Framework for Combating Cybercorruption

The development of information and communication technologies, particularly artificial intelligence technologies, is affecting all sectors and fields, and the fact that these technologies, while bringing benefits to all sectors and fields, are also causing harm is affecting the further development of the reforms being implemented.

***For information:** While cybercrime caused USD 8.27 trillion in damage to the countries of the world in 2023 and USD 9.5 trillion in 2024, this figure is projected to reach USD 10.5 trillion in 2025²⁴⁴.*

For this reason, at the meeting of the National Council for Combating Corruption held on 5 March 2025, the Head of State issued a specific instruction to establish a strong legal framework for combating cybercorruption, and extensive work is being carried out in this regard²⁴⁵.

In particular, a working group consisting of 29 specialists was established, and a roadmap for the implementation of 17 key tasks was approved²⁴⁶. The implementation of this task requires the comprehensive and full-scale execution of the objectives set from scientific, practical, theoretical, legal, organizational, economic and financial perspectives.

It should be emphasized that, although the definition of the term **“cybercorruption”** is not currently provided for in the legislation of any state, including the legislation of the Republic of Uzbekistan, the necessary practice and legal framework in this regard have been established in foreign countries. In particular,

France’s LOPMI (Loi d'Orientation et de Programmation du Ministère de l'Intérieur) Law dated 24 January 2023 defined the activities of the Ministry of the Interior in the field of cybersecurity for the subsequent five-year period²⁴⁷.

***For information:** Under this Law, the penalties for unlawfully accessing automated data processing systems have been increased, and liability has been established for owners of information technology platforms. In particular, the founder of Telegram, Pavel Durov, was also investigated under this Law. The issue of insurance in relation to cyberattacks has also been adequately regulated; in particular, specific provisions establish that a victim may file a claim against the owners of the platforms at fault within 72 hours from the moment their rights and interests have been violated.*

²⁴⁴ cybersecurityventures.com.

²⁴⁵ <https://president.uz/uz/lists/view/7924>.

²⁴⁶ Joint Resolution № 04/4-03-01/17 of the Committee on Innovative Development and Information Technologies of the Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan and the Committee on Youth, Women, Culture and Sports of the Senate of the Oliy Majlis of the Republic of Uzbekistan dated 25 March 2025.

²⁴⁷ <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047046768>.

The **Atlantic Council**, in its **report** entitled “*The Impact of Corruption on Cybersecurity: Rethinking National Strategies in the Global South*”, published in July 2024, addresses instances of corruption in the field of information and communication technologies, as well as cases involving the procurement of software that have a negative impact on cybersecurity²⁴⁸.

A **webinar** on the topic “*Examining the Interrelationship between Corruption and Cybercrime*” was conducted by the **SANS Institute** on 21 August 2024²⁴⁹.

The **European Union Agency for Law Enforcement Cooperation (Europol)**: in its report published in March 2025, **warned that the development of artificial intelligence** could intensify organised crime and, consequently, contribute to the development of cybercrime, including **cybercorruption**²⁵⁰.

Among scholars from the United States and Western countries, R. Peacock, Ch. Binns, S. Likhova, T. Lisko, O. Kosilova, O. Kirichenko, A. Shamara, S. Bortnik, T. Kuznetsova, V. Orlov, Yu. Bortnik, and among national scholars, S. Gulyamov, R. Raimberdiyev, S. Eshkabilov, S. Hamroyev, R. O‘rinboyev, Sh. Eraliyev, and other scholars have studied general information relating to cybercorruption.

Cybercorruption has the following essential characteristics, in particular:

1. this act is committed in cyberspace or through its use in a mixed form as a cybersecurity incident;
2. cyber-technical means are used to carry out a cybersecurity incident;
3. cyber-technical means may include a program, software, hardware-software means, software-hardware means, software product, telecommunications network, including the Internet, artificial intelligence, telecommunications infrastructure (telecommunications means), software, information system and resource, including a website, web application, messenger, various technical means, and other means created through other information technologies, including artificial intelligence technologies;
4. cybercorruption may be committed in a form that is broader than “digital corruption” but narrower than “corruption”, or in a mixed form;
5. specific liability for cybercorruption must be established in the legislation of the respective states.

The following forms and methods of cybercorruption exist, in particular:

1) Electronic (digital) receipt or giving of a bribe or mediation:

receiving, giving, or mediating a bribe through electronic (digital) payments or cryptocurrency, including other anonymous cryptocurrencies;

electronic gift cards – giving bribes through gift cards instead of ordinary bank transfers, for example, providing cards with discounts for purchases;

receiving discounts, online rewards, gifts through lotteries, games based on risk or gambling, or cashback cards, sending monetary amounts to cashback cards, and providing benefits;

²⁴⁸ www.atlanticcouncil.org.

²⁴⁹ <https://www.sans.org/emea/>.

²⁵⁰ <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>.

obtaining benefits through the organization of electronic document management;

2) Illegal use of information resources:

illegal access, with or without authorization, to personal databases of civil servants or representatives of the private sector contained in information systems and personal data databases;

illegal sale of databases;

altering personal data, including a person's credit history, tax information, or identification data;

disseminating false information on behalf of a state body or its official through a fake website;

conducting campaigns against civil servants or business competitors through social networks;

influencing government decisions through digital propaganda and fake voting systems;

committing illegal acts in the name of officials or prominent persons through digital propaganda and fake voting systems;

3) Corruption in public procurement:

illegally ensuring, through an information system, that certain companies win public procurement, auction, tender, or competitive selection processes through corruption schemes;

influencing users by providing false information for procurement or entering false information into the system;

illegally assisting certain companies through an information system in public procurement, auction, tender, or competitive selection processes through corruption schemes; obstructing users in the procurement process; partially disabling information systems; suspending some of their functions; issuing unlawful instructions to the system; and creating conditions or opportunities that prevent the procurement process from being carried out properly;

failing to align the information system with the criteria established for public procurement, auction, tender, or competitive selection processes;

carrying out cyberattacks against information systems designated for public procurement, auction, tender, or competitive selection processes, or creating conditions for such attacks to be carried out;

entering the system of ministries and agencies or establishing public-private partnerships for the purpose of directly providing benefits for the development of information systems;

obtaining the status of a sole operator or integrator for the preferential development of information systems;

modifying the program code in order to predetermine procurement winners;

manipulating through fake participants (bots);

introducing fake companies into procurement processes and eliminating genuine and fair competition;

discrediting a competitor;

- altering digital data and documents relating to users in procurement processes, and obstructing their sufficient use of the system;

- altering digital documents related to the conduct and process of procurement;

- selecting another winner by making changes to or falsifying digital documents concerning procurement results;

- entering into the system information that fully corresponds to the capabilities of a company agreed in advance to win directly;

4) Implementation of cyberextortion, cyberblackmail and other cyberthreats

- stealing data from the public and private sectors through cybertheft and cyberespionage and carrying out cyberextortion, cyberblackmail, and other cyberthreats;

- altering, deleting, and concealing information in an information system for the purpose of hiding digital traces of corruption schemes;

- “*Ransomware Attacks*” – encrypting government agencies’ or business systems, restricting access to them, and unlocking them in exchange for a ransom;

- phishing and fake messages – obtaining confidential information by deceiving government officials or company employees;

- extortion through insiders, i.e., carrying out extortion by disclosing information belonging to persons working in a company or government agency;

- establishing illegal information exchange involving employees working in government or private organizations;

- providing procurement-related information in advance;

- corporate espionage, i.e., disclosing company information for use by competitors;

- transmitting data through software companies, i.e., obtaining government or private data through fake IT companies;

- obtaining illegal funds by entering into contractual relations for the purpose of preventing certain information from being disclosed to the general public, while in practice not providing the service;

- initiating unjustified inspections;

5) Legalization of criminal proceeds and carrying out illegal operations through cryptocurrency:

- laundering illegal funds using cryptocurrencies;

- carrying out illegal financial transactions through payment systems that are difficult to detect;

- illegal use of blockchain technologies;

- mixing funds to make it difficult to trace cryptocurrency;

- money laundering through NFTs (non-fungible tokens), i.e., legalizing illegal funds by purchasing books, scientific works, intellectual property works, copyright and related rights, works of art, or digital property advertised, displayed, or sold in information systems, websites, and electronic payment systems or electronic wallets;

- crypto-offshores – transferring illegal funds by establishing crypto-companies in different countries;

6) Falsification of digital identification:

creating false identity data of persons in the information systems or resources of organizations in the public or private sectors;
 illegal use of identification and electronic digital signature means;
 illegal alteration of personal data;
 altering, taking over, and illegally using data in authentication, authorization, FACE-ID, and other biometric identification systems;
 illegal exchange of information between competitors or government agencies;
 breaching bioidentification or digital passport (ID-card) systems;
 creating fake documents through Deepfake, i.e., altering personal data using technologies involving manipulated faces, voices, or videos;
 forging electronic signatures;
 creating opportunities for the illegal use of public services through the creation of multiple personal profiles.

However, the current Criminal Code does not provide sufficient criminal liability for this.

***For information:** in the field of corruption alone, 5,716 crimes were committed in 2024, however, with regard to preventing such crimes, sufficient preventive measures were not taken to ensure that persons who were subsequently held liable did not attempt to commit these acts before actually committing corruption-related crimes; as a result, 6,898 persons were held criminally liable and caused damage to state interests in the amount of UZS 12.4 trillion, while only UZS 4.2 trillion was recovered, and the most important issues affecting people remained unresolved²⁵¹.*

At the same time, due to the presence of corruption factors and insufficient transparency in the areas of public procurement, healthcare, education, social protection, the judicial and legal system, and public services, the number and proportion of cybercorruption-related acts involving electronic payments, information systems, and websites are also increasing in practice.

According to the Law of the Republic of Uzbekistan “On Combating Corruption” dated January 3, 2017, № LRU–419, **corruption** is the unlawful use by a person of his or her official or service position for the purpose of obtaining material or non-material benefits for personal interests or the interests of other persons, as well as the unlawful provision of such benefits²⁵².

According to the Law of the Republic of Uzbekistan “On Cybersecurity” dated April 15, 2022, № LRU–764, **cybercrime** is a set of crimes committed **in cyberspace** using software and technical means for the purpose of acquiring, modifying, or destroying information, or disabling information systems and resources;

In this context, **cyberspace** is a virtual environment created using information technologies, while a **cybersecurity incident** is an incident in cyberspace that results in disruptions to the functioning of information systems and/or violations of the availability, integrity, and free access to information contained therein²⁵³.

²⁵¹ file:///C:/Users/%D0%B37/Downloads/https_yuz.uz_file_newspaper_1501d499b4f544b9a3d8408d878d4fb8.p df.

²⁵² Law № LRU–419 of the Republic of Uzbekistan “On Combating Corruption” dated January 3, 2017 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁵³ Law № LRU–764 of the Republic of Uzbekistan “On Cybersecurity” dated April 15, 2022 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

Thus, **cybercorruption** is corruption involving an official or civil servant using cyberspace through cyber-technical means to commit a cybersecurity incident for which liability is provided by legislation.

Cybercorruption may take the form of an offense or a crime.

For information: According to the Law of the Republic of Uzbekistan “On Prevention of Offenses” dated May 14, 2014, № LRU–371, **an offense** is a culpable unlawful act (action or omission) for which administrative or criminal liability is provided²⁵⁴;

According to Article 14 of the Criminal Code, a culpable socially dangerous act (action or omission) prohibited by this Code and punishable under threat of punishment shall be deemed a **crime**²⁵⁵.

Cybercrime, in turn, is committed against an object of cybersecurity, and today this object is defined very narrowly.

For information: According to the Law of the Republic of Uzbekistan “On Cybersecurity” dated April 15, 2022, № LRU–764, **an object of cybersecurity** is a set of information systems used in activities aimed at ensuring the cyber protection of information and the cybersecurity of national information systems and resources, including critical information infrastructure facilities²⁵⁶.

However, in addition to information systems, the cyber-technical means identified above by scholars may also constitute an object of cybercorruption.

For information: The “Cybersecurity Center” State Unitary Enterprise has established a system for reporting cyber incidents through its official website, csec.uz. During the first half of 2024, the Center recorded **63** cyber incidents within the .uz domain zone and **22** cyber incidents on the websites of government bodies and organizations.

Defining the object of cybersecurity more broadly and precisely makes it possible to implement specific measures to combat cybercorruption; **otherwise, the object of cybersecurity may potentially be formulated as follows:**

Object of cybercorruption – a set of information systems used in activities aimed at ensuring the cyber protection of information and the cybersecurity of national information systems and resources, including critical information infrastructure facilities, in which a cybercorruption act may be committed.

According to the Regulation “On the Procedure for Incentivizing Persons Who Report Corruption-Related Offenses or Otherwise Assist in Combating Corruption”, approved by Resolution № 829 of the Cabinet of Ministers dated December 31, 2020, a list of administrative offenses and crimes related to corruption has been approved. According to this Regulation:

administrative offenses related to corruption include offenses provided for in Articles 61¹, 193¹, and 193² of the Code of the Republic of Uzbekistan on Administrative Responsibility;

crimes related to corruption include crimes provided for in paragraph “g” of Part 2 of Article 167, paragraph “v” of Part 3 of Article 168, Articles 192⁹ and 192¹⁰, Articles 205, 209–214 of the Criminal Code of the Republic of Uzbekistan,

²⁵⁴ Law № LRU–371 of the Republic of Uzbekistan “On the Prevention of Offenses” dated May 14, 2014 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁵⁵ Criminal Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁵⁶ Law № LRU–764 of the Republic of Uzbekistan “On Cybersecurity” dated April 15, 2022 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

the commission of the crime provided for in Article 243 through the use of official position, as well as the crimes specified in Article 301²⁵⁷.

However, the acts provided for in **Articles 133, 135, 141, 141¹, 141², 141³, 143, 145–147, 149, 156–157, 160, 165, 167–168, 170–186³, 188, 188¹, 189, 191, 192, 192¹, 202, 207, 228, 229⁶, 244¹–244⁴, 244⁶, 2781¹–278⁹** of the Criminal Code may also constitute corruption-related crimes.

In this situation, taking into account advanced foreign experience and the views of scholars concerning **cybercorruption**, it would be appropriate to fill the existing legal gap.

The act provided for in **Article 168 of the Criminal Code** may take the form of information fraud (cyberfraud); the act provided for in **Article 175** may involve creating corruption schemes using blockchain technologies, concealing criminal proceeds, or falsifying tender processes, as well as entering into corruption agreements through social networks and messengers; the act provided for in **Article 192** may involve manipulating public procurement and the market through digital platforms; the acts provided for in **Articles 210–212** may involve receiving, giving, and mediating bribes through electronic financial platforms, electronic payment systems, social networks, and blockchain systems, using cryptocurrency and other digital assets, as well as electronic payments; the acts provided for in **Articles 228 and 230¹** may involve forging and using electronic (digital) documents, forging digital identification means (electronic signatures, biometrics, NFT documents), or using them as forged documents; the act provided for in **Article 243** may involve the legalization (money laundering) of criminal proceeds through cryptocurrency, NFTs, blockchain, and digital assets; the act provided for in **Article 244¹** may involve committing corruption-related acts through digital manipulation and cyber-propaganda; and the act provided for in **Article 278** may additionally be committed in the form of corruption-related activities and corruption agreements through the Dark Web, Dark Net, and other illegal Internet platforms, as well as through artificial intelligence, and influencing officials through social engineering methods.

In foreign countries, sufficient liability measures have been established for cybercrimes. In particular, **Section 201 of Title 18 of the United States Code**²⁵⁸, the **UK Bribery Act**²⁵⁹, and the **Criminal Code of the Republic of Korea** and the **Act on the Aggravated Punishment of Specific Crimes** prohibit public officials, as well as witnesses and other persons, from **receiving, giving, or mediating bribes in any manner**, including through electronic means, and establish specific liability for such acts²⁶⁰.

Even, in **Article 131 of the Criminal Act of the Republic of Korea**, criminal liability is established for improper acts after accepting a bribe and for subsequent bribery; **Article 132** provides liability for accepting a bribe through the use of one's

²⁵⁷ Regulation “On the Procedure for Encouraging Persons Who Report Corruption-Related Offenses or Otherwise Assist in Combating Corruption,” approved by Resolution № 829 of the Cabinet of Ministers of the Republic of Uzbekistan dated December 31, 2020 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁵⁸ <https://www.justice.gov/criminal/criminal-fraud/file/1292051/dl>.

²⁵⁹ <https://www.legislation.gov.uk/ukpga/2010/23/contents>.

²⁶⁰ https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=62179&type=sogan&key=9.

good offices; **Article 134** provides for the confiscation of property received as a bribe or, where confiscation is impossible, the collection of its value; **Article 355** establishes criminal liability for embezzlement and breach of trust; and **Article 356** establishes criminal liability for occupational embezzlement and occupational breach of trust²⁶¹.

***For information:** In the Republic of Uzbekistan, there is no separate special law specifically concerning bribery; there are only the laws “On Combating Corruption” and “On Conflict of Interests”, as well as legislative acts adopted on their basis and the Resolution of the Plenum of the Supreme Court “On Judicial Practice in Cases of Bribery”. However, Article 167 of the Criminal Code has not been brought into line with the requirements of the present day and the current legislative acts. In particular, **Part 3, paragraph “g”, of Article 167 of the Criminal Code** establishes criminal liability for the misappropriation or embezzlement of another person’s property entrusted to or under the control of the offender **through the use of computer technology**, but does not take into account the possibility that such acts may be committed using other information technologies, in addition to computer technology, or through artificial intelligence technologies. Therefore, it is necessary to reconsider this Article.*

Germany: Articles 202a, 202b, and 202c of the Criminal Code establish criminal liability for unauthorized access to data not intended for the offender and specially protected against unauthorized access, unauthorized interception of information using technical means, and the production, acquisition, sale, supply, dissemination, or other provision of passwords or other security codes that restrict access to data, as well as computer programs intended for committing such offenses. Criminal liability is also established for **computer fraud** under Article 263a²⁶².

According to **Article 323-1 of the Criminal Code of France**, fraudulent access to, or fraudulent remaining in, all or part of an automated data processing system is subject to liability; where such conduct results in the deletion or modification of data contained in the system or an alteration of the functioning of the system, an aggravated penalty is provided. Where these offenses are committed against an automated data processing system containing personal data implemented by the State, liability is further aggravated²⁶³.

***For information:** Under the Criminal Code of the Republic of Uzbekistan, **Article 278¹** provides for criminal liability for violating the rules of informatization, **Article 278⁴** for modifying computer information, **Article 278⁵** for computer sabotage, **Article 278⁶** for creating, using, or distributing harmful programs when committed through the use of one’s official or professional position; however, separate criminal liability for **computer fraud** has not been established in a separate article.*

Japan: Article 96-6 of the Criminal Code establishes criminal liability for obstructing an auction; Article 161-2 for falsifying or altering electronic data and documents; Article 163-2 for causing errors in the processing of another person’s financial transactions and documents without the requisite authorization, creating improperly encoded credit cards or other cards for making payments for goods or services, and obtaining unauthorized access; Article 248 for constructive fraud;

²⁶¹ <https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%ED%98%95%EB%B2%95>.

²⁶² <https://www.gesetze-im-internet.de/stgb/>.

²⁶³ https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/.

Article 246-2 for computer fraud; Article 250 for attempts against property; Article 254 for theft of lost property; and Article 256 for receiving stolen property²⁶⁴.

For information: *The Criminal Code of the Republic of Uzbekistan does not establish direct liability for obstructing the conduct of procurement processes, including competitive selection, tenders, and auctions, or for the circumstances provided for under Japanese legislation.*

Canada: Article 322 of the Criminal Code establishes criminal liability for theft; Article 335 for offenses similar to theft; Article 347 for criminal interest rates; Article 348 for unlawful breaking and entering; Article 361 for false pretenses; Article 402.1 for the theft of personal information and the use of personal information for fraudulent purposes; Article 406 for counterfeiting trademarks and trade descriptions; Article 437 for interference with property; and Article 460 for advertising and selling counterfeit money and counterfeit items of value²⁶⁵.

For information: *The Criminal Code of the Republic of Uzbekistan does not sufficiently provide for the provisions stipulated in the Criminal Code of Canada.*

Australia: Pursuant to Section 474.17 of the Criminal Code, criminal liability is established for making threats²⁶⁶.

For information: *Liability under Article 112 of the Criminal Code arises only where there are sufficient grounds to fear that a threat to kill or use violence will be carried out; however, **the possibility that a cyberthreat may be made for purposes other than threatening to kill or use violence** is not provided for in this Article.*

Singapore's "Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act" provides for strict criminal liability for corruption, drug trafficking, and other serious crimes committed through cryptocurrency²⁶⁷.

For information: *In the Criminal Code of the Republic of Uzbekistan or in a separate law, a direct list of corruption-related crimes has not been established, and matters relating to cryptocurrency have not been regulated at the legislative level.*

Switzerland's "Anti-Money Laundering Act" prohibits any form of corruption, as well as money-laundering activities carried out using cryptocurrency, and establishes strict criminal liability for such acts²⁶⁸.

For information: *Article 243 of the Criminal Code of the Republic of Uzbekistan establishes criminal liability for the legalization of proceeds derived from criminal activity; however, **provisions relating to cryptocurrency** are not provided for in this Article. Furthermore, under the Law of the Republic of Uzbekistan "On Combating the Legalization of Proceeds from Criminal Activities, the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction" dated August 26, 2004, № 660-II, persons carrying out activities in the field of crypto-asset circulation are included in the list of organizations conducting transactions involving funds or other property; however, relations concerning such persons are not sufficiently regulated by this Law.*

Italy: Article 476 of the Criminal Code²⁶⁹ and **Spain:** Article 390 of the Criminal Code²⁷⁰ establish liability for forgery, including the forgery of official identification.

²⁶⁴ <https://www.japaneselawtranslation.go.jp/ja>.

²⁶⁵ <https://laws-lois.justice.gc.ca/eng/acts/c-46/>.

²⁶⁶ https://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/cca1995115/sch1.html.

²⁶⁷ <https://sso.agc.gov.sg/Act/CDTOSCCBA1992>.

²⁶⁸ https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/en.

²⁶⁹ <https://www.brocardi.it/codice-penale/>.

²⁷⁰ <https://www.brocardi.it/codice-penale/>.

For information: *It is necessary to establish criminal liability under Article 228 of the Criminal Code of the Republic of Uzbekistan for the falsification of digital (electronic) documents, and under Article 230^l for the falsification of electronic (digital) evidence, including when such acts are committed through the use of one's official position²⁷¹.*

The Netherlands: Article 350 of the Criminal Code establishes criminal liability for intentionally and unlawfully destroying, damaging, rendering unusable, or taking away any property wholly or partly belonging to another person; Article 350a establishes criminal liability for intentionally and unlawfully modifying or deleting data stored, processed, or transmitted by means of an automated system or telecommunications facility, rendering such data unusable or unavailable, or intentionally and unlawfully introducing or disseminating data intended to damage automated operations; Article 350b establishes criminal liability for committing acts involving the unlawful modification, deletion, rendering unusable, or addition of other data during the storage, processing, or transmission of data through an automated system or telecommunications facility; Article 350c establishes criminal liability for intentionally destroying, damaging, or rendering unusable any automated or telecommunications system, disrupting its functioning or use, or violating security measures applied to such systems, as well as causing malfunctions in data processing or transmission or in the functioning of a telecommunications network or the provision of telecommunications services; Article 350d establishes criminal liability for manufacturing, selling, using, importing, or exporting technical devices designed to obstruct the operation of an automated system, as well as manufacturing, providing, obtaining, selling, purchasing, importing, distributing, or providing passwords, access codes, or similar data that enable access to such a system; Article 359 establishes criminal liability for usurping official powers by using one's official position or documents in one's possession, or enabling other persons to usurp such powers; Article 361 establishes criminal liability for altering data in documents and registers; Article 363 establishes criminal liability for engaging in corruption; Article 365 establishes criminal liability for creating conditions or opportunities for the commission of an act through abuse of official position; Article 366 establishes criminal liability for extortion by a public official; Articles 364 and 367–368 establish criminal liability for corruption-related offenses committed by officials who are investigators, judges, or officials of bodies responsible for enforcing court decisions; and Article 371 establishes criminal liability for the disclosure of letters, correspondence, and other communications by officials or allowing such disclosure to occur²⁷².

For information: *The Criminal Code of the Republic of Uzbekistan does not sufficiently provide for the necessary provisions concerning damage to property, which is treated as a civil matter; almost none of these acts are linked to cybercorruption.*

For cyber-propaganda and digital manipulation, liability is established under **Section 130 of the Criminal Code of Germany²⁷³**, the **Internet Ethics Code of China**, France's **Law against the Manipulation of Information (Loi contre la**

²⁷¹ Criminal Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁷² <https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vi32nmht6cz9>.

²⁷³ <https://www.gesetze-im-internet.de/stgb/>.

manipulation de l'information)²⁷⁴, and the United Kingdom's Malicious Communications Act 1988²⁷⁵ and Communications Act 2003²⁷⁶.

For information: Article 156 of the Criminal Code of the Republic of Uzbekistan establishes criminal liability for inciting national, racial, ethnic, or religious hatred, while paragraph “g” of Part 3 of Article 244¹ establishes criminal liability for producing, storing, distributing, or demonstrating materials that threaten public safety and public order through telecommunications networks or the Internet; however, **liability for market manipulation is not provided for.**

Pursuant to Article 345 of the Criminal Procedure Code²⁷⁷:

In cases concerning crimes under **paragraph “g” of Part 2 of Article 167 and Article 243 of the Criminal Code**, the preliminary investigation is conducted by the preliminary investigation body that initiated the criminal case. If a criminal case concerning these crimes is initiated by a body conducting a pre-investigation examination or by an inquiry body, the prosecutor determines the preliminary investigation body that will conduct the investigation in the case²⁷⁸.

The preliminary investigation of cases concerning crimes under **paragraph “v” of Part 3 of Article 168 of the Criminal Code** is conducted by **investigators of the internal affairs bodies.**

The preliminary investigation of cases concerning crimes under **Articles 192⁹ and 192¹⁰, 205, and 209–214 of the Criminal Code** is conducted by **investigators of the prosecutor's offices.**

In cases concerning crimes provided for in **Article 301 of the Criminal Code**, the **preliminary investigation is conducted by investigators of the military prosecutor's offices.**

At the same time, **Article 245 of the Code of the Republic of Uzbekistan on Administrative Responsibility** does not specify which state body is responsible for conducting inquiry proceedings in cases involving corruption-related offenses; however, it merely provides that **such cases are subject to consideration by the court.**

In foreign countries, the issue of territorial jurisdiction over the investigation of cybercrimes is addressed as follows:

According to **Article 706-72-1 of the French Code of Criminal Procedure**, the acts provided for in Article 706-72 of the Code, namely offenses against information systems (cybercrimes), are heard by the **Tribunal de grande instance de Paris**²⁷⁹.

France has granted special powers to the **Tribunal de grande instance de Paris** for the purpose of combating cybercrime, comprising specialized divisions or courts for the investigation and judicial centralization of cybercrimes. This court has

²⁷⁴ <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/>.

²⁷⁵ <https://www.legislation.gov.uk/ukpga/1988/27/section/1>.

²⁷⁶ <https://www.legislation.gov.uk/ukpga/2003/21/contents>.

²⁷⁷ Criminal Procedure Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁷⁸ Criminal Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁷⁹ <https://www.tribunal-de-paris.justice.fr/75>.

separate jurisdiction over criminal intelligence and investigation, investigative authorities, the prosecution system, and the judicial system²⁸⁰.

For information: this court was established by France's Law № 2016-731 of June 3, 2016 "Strengthening the Fight against Organized Crime, Terrorism and Their Financing, and Improving the Effectiveness and Guarantees of Criminal Procedure Law". The issue of territorial jurisdiction in an investigation is determined on the basis of the place where the crime was committed, the place where the offender was apprehended, or the offender's place of residence, through the aforementioned court²⁸¹.

A similar practice exists in **Thailand**, as follows:

On March 18, 2024, the President of the Supreme Court of Thailand announced the establishment of the **Technology Crime Division** within the Criminal Court of Thailand, which commenced operations on April 1, 2024. The division has jurisdiction over technology-related crimes, including cybercrime, computer-related fraud or extortion, and offenses related to personal data protection laws. It also considers requests from competent law-enforcement officers for court orders under Thailand's Computer Crimes Act, Personal Data Protection Act, and Cybersecurity Act²⁸².

This division hears cybercrimes and technology-related offenses under the following laws:

1. **Computer-Related Crime Act B.E. 2550 (2007)**²⁸³;
2. **Personal Data Protection Act B.E. 2562 (2019)**²⁸⁴;
3. **Cyber Security Maintenance Act B.E. 2562 (2019)**²⁸⁵.

This **division** considers not only **cybercrimes**, but also **cyber-offenses**, and:

1. issues **court orders** – for example, to block websites and to carry out procedural actions against cybercriminals;
2. makes **rulings/decisions** – it may issue procedural decisions in relation to the case under consideration;
3. delivers **judgments/sentences** – if a case proceeds to trial, it issues criminal judgments against persons found guilty.

For information: An investigation is conducted in the territory where the crime was committed or where it was anticipated to be committed, or where the accused was apprehended.

In Germany, the issue of investigation is organized somewhat differently, namely:

For the purpose of combating cybercrime, detecting and solving cybercrimes, introducing new technologies to combat cybercrime, pooling and allocating

²⁸⁰ https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154/.

²⁸¹ <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032627231>.

²⁸² https://tel.directory.gov.hk/index_HKPF_ENG.html.

²⁸³ <https://www.icj.org/wp-content/uploads/2012/12/Thailand-Computer-Crime-Act-2007-eng.pdf>.

²⁸⁴ https://data.thailand.opendevelopmentmekong.net/en/laws_record/2562/resource/ec616be5-9fbf-4071-b4b5-cb1f3e46e826.

²⁸⁵ https://data.opendevelopmentmekong.net/dataset/329b4f41-f309-4348-9015-23c6f62d5fb4/resource/ea9a61bc-fba9-41ae-9dd0-d31ca5f36ff5/download/843708_0001.pdf.

capabilities and resources, as well as developing them, the **Cybercrime Division**²⁸⁶ was established on April 1, 2020, within the **German Federal Criminal Police Office (BKA)**²⁸⁷, which also includes the following units:

1) Central Contact Point for Cybercrime (ZAC)²⁸⁸;

***For information:** ZAC ensures cooperation between the private sector and law enforcement agencies.*

2) Department for Operational Analysis of Cybercrimes²⁸⁹.

***For information:** this department analyzes data on cybercrimes and coordinates international cooperation. The issue of investigative jurisdiction is resolved on the basis of the place where the crime was committed, the place of residence of the accused, or the place where the accused was detained or arrested.*

In the United States, which is based on Anglo-Saxon law, for example, specialized prosecutors dealing with cybercrimes operate in the District Attorney's Office of Santa Clara County, State of California²⁹⁰, In the Office of the Attorney General of California, there is a specialized unit for the investigation and legal prosecution of cybercrimes — the Cybercrime Unit. This unit investigates crimes such as unauthorized access to information systems, internet fraud, and cyberstalking²⁹¹.

For information: In the United States, the issue of territorial jurisdiction is determined as follows: investigation is conducted in the territory where the federal laws were violated, or in the federal state to which the respective law applies.

In the Philippines, the procedure for organizing and conducting raids against cybercrimes and illegal online activities, as well as the obligations of the participating state bodies and organizations, is established in Republic Act № 10175 – the “Cybercrime Prevention Act” adopted in 2012, and the fight against these crimes through raids has been widely implemented there²⁹².

***For information:** it falls under the jurisdiction of the investigation at the place where the cybercrime was committed.*

The body authorized in the field of cybersecurity to exercise oversight and inspection, conduct operational-search activities, pre-investigation checks, and investigative actions is the **State Security Service of the Republic of Uzbekistan**, pursuant to Law № LRU–764 of the Republic of Uzbekistan “On Cybersecurity” dated April 15, 2022²⁹³.

Articles 279 and 280 of the Code of the Republic of Uzbekistan on Administrative Responsibility provide that a report on an administrative offense

²⁸⁶ https://www.bka.de/EN/Home/home_node.html.

²⁸⁷ <https://www.fbi.gov/investigate/cyber>.

²⁸⁸ https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html.

²⁸⁹ <https://nj.gov/njsp/division/investigations/cyber-crimes.shtml>.

²⁹⁰ <https://da.santaclaracounty.gov/home>.

²⁹¹ <https://www.ca.gov/departments/223/>.

²⁹² https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/philippines/pop_up.

²⁹³ Law of the Republic of Uzbekistan No. LRU–764 dated 15 April 2022, **“On Cybersecurity”* // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

shall be drawn up by the body exercising supervision and inspection in the respective field in which the administrative offense was committed²⁹⁴.

However, the following powers covering matters within the competence of the State Security Service are provided for in legislative acts regulating the activities of certain ministries and agencies, in particular:

powers relating to inquiry and investigation of cyber offenses and cybercrimes – the Prosecutor General’s Office, the Ministry of Internal Affairs, the Ministry of Justice, and the Inspection for Control in the Field of Informatization and Telecommunications;

powers to exercise oversight and conduct inspections in the field of information security and cybersecurity – the National Agency for Prospective Projects, the Ministry of Digital Technologies, the Central Bank, the Ministry of Justice, the Inspection for Control in the Field of Informatization and Telecommunications, the Personalization Agency, and the Center for Mass Communications.

This situation, in turn, hinders the effective ensuring of cybersecurity of cybersecurity subjects.

Pursuant to **Article 346 of the Criminal Procedure Code of the Republic of Uzbekistan**, the issue of territorial jurisdiction of investigation is resolved as follows:

As a general rule, **a criminal case falls under the jurisdiction of the investigator of the district (city) where the crime was committed.**

At the same time, in the following cases, **the investigation may also be conducted in other territories**, namely:

a preliminary investigation may, **if this contributes to a significantly faster, thorough, complete, objective, and comprehensive examination of the circumstances of the case**, be conducted at the place where the case was initiated or at the place where the majority of the suspects, accused persons, or witnesses are located;

on the basis of an order of a superior prosecutor or the head of a higher investigative unit, a preliminary investigation may also be conducted territorially **without observing the rules of territorial jurisdiction of investigation**²⁹⁵.

However, there are a number of problems in applying the general rules concerning territorial jurisdiction of investigation of cybercrimes in the **Republic of Uzbekistan**, in particular:

1. when a cybercrime is committed in cyberspace against a relevant information system, the user may be located in one territory, while the server or database where the information system is located may be situated in another territory;

²⁹⁴ Code of the Republic of Uzbekistan on Administrative Responsibility // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁹⁵ Criminal Procedure Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

2. a cybercrime may be committed from the territory of a foreign state against information systems, means of payment, or payment systems located in one or more territories of the Republic of Uzbekistan;

3. the victim may not know that a cybercrime has been committed at the time it occurs and may become aware of it later, when the integration of information systems is being carried out or when other technical operations are performed after the system has been moved to another territory, while not knowing in which territory, i.e., district (city), the crime was committed;

4. some of the victims may be located in the Republic of Uzbekistan, while others may be located in the territory of a foreign state.

Pursuant to **Article 11 of the Criminal Code**, acts committed in such circumstances shall be subject to the legislation of the Republic of Uzbekistan and the perpetrator shall be held liable, except for the cases provided for in part four of this Article.

Therefore, it is important to resolve, through law-making, the existing problems concerning not only the territorial jurisdiction of investigation of cybercorruption-related crimes, but also that of cybercrimes.

It should be emphasized that the current legal framework concerning cybercorruption has been formed in two areas, namely:

1) on combating corruption:

24 Laws, **60** Presidential Decrees, **72** Presidential resolutions, **138** Resolutions of the Cabinet of Ministers, **30** departmental regulatory legal acts, **324 legislative acts in total.**

2) on cybersecurity:

12 Laws, **20** Presidential Decrees, **29** Presidential resolutions, **40** Resolutions of the Cabinet of Ministers, **12** departmental regulatory legal acts, **113 legislative acts in total.**

The legal relationship that currently connects these two areas is administrative and criminal legislation.

The concept of administrative offenses related to cybercorruption and the offenses falling within this category are not directly defined in legislation.

***For information:** Pursuant to the Code of the Republic of Uzbekistan on Administrative Responsibility, an administrative offense is an unlawful, culpable act or omission (committed intentionally or through negligence) that infringes upon an individual, the rights and freedoms of citizens, property, state and public order, or the natural environment, for which administrative liability is provided for by legislation.*

It is well known that, pursuant to Law № LRU–419 of the Republic of Uzbekistan “On Combating Corruption” dated January 3, 2017²⁹⁶,

corruption — the unlawful use by a person of his or her official or service position for the purpose of obtaining material or non-material benefits in his or her own interests or in the interests of other persons, as well as the unlawful provision of such benefits;

²⁹⁶ Law № LRU–419 of the Republic of Uzbekistan “On Combating Corruption” dated January 3, 2017 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

corruption-related offense — an act having the characteristics of corruption, for the commission of which liability is provided for by legislation.

Pursuant to Law № LRU-764 of the Republic of Uzbekistan “On Cybersecurity” dated April 15, 2022, a **cybersecurity incident** is an incident that has resulted in disruptions in the functioning of information systems in cyberspace and/or violations of the availability, integrity, and free access to information contained therein.

In this regard, **cyberspace** is a virtual environment created using information technologies²⁹⁷.

Thus, an **administrative offense related to cybercorruption** is a corruption-related offense committed by an official or civil servant through cyber-technical means using cyberspace, aimed at causing a cybersecurity incident for which liability is provided for by the Code of the Republic of Uzbekistan on Administrative Responsibility.

It should be noted that, under the Regulation “On the Procedure for Encouraging Persons Who Report Corruption-Related Offenses or Otherwise Assist in Combating Corruption,” approved by Resolution № 829 of the Cabinet of Ministers dated December 31, 2020, **administrative offenses related to corruption** include the offenses provided for in **Articles 61¹, 193¹ and 193² of the Code of the Republic of Uzbekistan on Administrative Responsibility**.

However, the acts provided for in Articles 40–41¹, 46–46², 47⁸, 51², 51⁴, 51⁷, 52, 55, 56², 56⁴, 59², 59⁴, 60, 61, 61², 72, 75, 76, 82, 89¹, 91, 94, 98–99, 102, 107–109, 151, 155–155⁵, 164, 165–167, 170, 171¹, 175⁸, 176, 177–177², 178, 178¹, 179, 179³, 185¹, 185⁴–186¹, 188–188¹, 188³, 189–189², 191, 193, 195², 200, 201¹, 202¹, 202², 203¹, 210¹, 212–214, 215⁵, 215⁸, 216, 219–223, 241¹, 241⁶ and 241⁷ of the Code of the Republic of Uzbekistan on Administrative Responsibility may also be committed in the form of cyber offenses and/or cybercorruption.

For this reason, **it is necessary to define the concept of a corruption-related cyber offense in legislation and clarify the list of corruption-related cyber offenses**.

The authorized body exercising oversight and inspection and conducting operational-search activities in the field of cybersecurity is the **State Security Service of the Republic of Uzbekistan**, pursuant to Law № LRU-764 of the Republic of Uzbekistan “On Cybersecurity” dated April 15, 2022. Pursuant to Article 11 of this Law, the State Security Service has the authority to **establish a working body for ensuring cybersecurity**, as well as **to delegate part of its powers to it**.

At the same time, pursuant to Article 22 of this Law, cybersecurity incidents are investigated by officials of the authorized state body or the working body for ensuring cybersecurity²⁹⁸.

²⁹⁷ Law № LRU-764 of the Republic of Uzbekistan “On Cybersecurity” dated April 15, 2022 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

²⁹⁸ Law № LRU-764 of the Republic of Uzbekistan “On Cybersecurity” dated April 15, 2022 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

It should be emphasized that the existence of overlapping powers and functions of state bodies constitutes, pursuant to Law № LRU–860 of the Republic of Uzbekistan “On Anti-Corruption Examination of Regulatory Legal Acts and Their Drafts” dated August 8, 2023²⁹⁹, **a corruption-generating factor related to powers, rights, and obligations.**

Pursuant to the Concept for Improving Law-Making Activities approved by Decree № DP–5505 of the President of the Republic of Uzbekistan dated August 8, 2018, it is necessary to introduce effective mechanisms for the adoption of directly applicable laws³⁰⁰.

Pursuant to the List of Bodies Authorized to Exercise Control over the Activities of Business Entities and Their Areas of Control³⁰¹, approved by Decree № DP–184 of the President of the Republic of Uzbekistan dated November 14, 2024, **control over information** falls within the competence of the Agency for Information and Mass Communications; **control in the areas of crypto-asset circulation, the capital market and insurance market, e-commerce, and regulation of the organization of lotteries and risk-based games on the Internet and bookmaker activities** falls within the competence of the National Agency for Prospective Projects; and **control over compliance with communication, informatization, and telecommunications requirements** falls within the competence of the Inspection for Control in the Field of Informatization and Telecommunications.

However, pursuant to Article 11 of the Law of the Republic of Uzbekistan “On Cybersecurity,” **exercising control over the implementation of legislation on cybersecurity and conducting operational-search activities, pre-investigation checks, and investigative actions in relation to cybersecurity incidents fall within the competence of the State Security Service.**

Therefore, pursuant to the Law, which has higher legal force than a Presidential Decree, and pursuant to the Code of the Republic of Uzbekistan on Administrative Responsibility, administrative reports on cyber offenses, including offenses related to cybercorruption, should be drawn up by officials of the State Security Service.

For information: Pursuant to Law № LRU–682 of the Republic of Uzbekistan “On Normative Legal Acts” dated April 20, 2021, *a normative legal act must comply with normative legal acts having higher legal force than it*³⁰².

However, the officials of the Border Troops of the State Security Service of the Republic of Uzbekistan and the Sanitary and Epidemiological Station of the Military Medical Service of the State Security Service of the Republic of

²⁹⁹ Law № LRU–860 of the Republic of Uzbekistan “On Anti-Corruption Examination of Regulatory Legal Acts and Their Drafts” dated August 8, 2023 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁰⁰ Concept for Improving Law-Making Activities, approved by Decree № DP–5505 of the President of the Republic of Uzbekistan dated August 8, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁰¹ List of Bodies Authorized to Exercise Control over the Activities of Business Entities and Their Areas of Control, approved by Decree № DP–184 of the President of the Republic of Uzbekistan dated November 14, 2024 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁰² Law № LRU–682 of the Republic of Uzbekistan “On Normative Legal Acts” dated April 20, 2021 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

Uzbekistan, whose names are specified in the Code of the Republic of Uzbekistan on Administrative Responsibility, do not have such powers; moreover, their specialization does not enable them to draw up administrative offense reports concerning acts of this category. Furthermore, imposing an additional workload on an organization fully engaged in addressing internal and external threats may affect its subsequent activities.

Second, pursuant to Resolution № RP–4452 of the President of the Republic of Uzbekistan “On Additional Measures to Improve the System for Monitoring the Implementation of Information Technologies and Communications and Their Protection” dated September 14, 2019, **Uzkomnazorat**, together with the **Cybersecurity Center SE, conducts monitoring, oversight, examination, and inspection of the implementation and development of information and communication technologies and the state of information security** in state and economic management bodies, local government authorities, and other organizations and agencies³⁰³.

For information: Through the official website of the **Cybersecurity Center SE**, csec.uz, a system for reporting cyber incidents has been established. During the first half of 2024, the Center identified **63** cyber incidents within the .uz domain and **22** cyber incidents on the websites of state bodies and organizations, while Uzkomnazorat drew up **64** administrative offense reports for violations of legislation concerning personal data.

However, this provision is also contrary to Article 11 of the Law “On Cybersecurity.”

Third, the Central Bank currently has the “CERT-CBU” Cybersecurity Center, while a Cybersecurity Center has been established within the Department of Operational Search Activities of the Ministry of Internal Affairs.

For information: The **Central Bank’s “CERT-CBU” Cybersecurity Center** performs the following functions:

ensuring information security and cybersecurity in the activities of payment system operators, credit and payment organizations, as well as ensuring cybersecurity in their information systems and resources and at critical information infrastructure facilities;

examining factors contributing to the emergence of information security and cybersecurity risks, introducing risk prevention systems, and taking measures for their implementation and application;

monitoring and analyzing offenses committed through digital technologies in banking and payment systems and combating offenses committed through digital technologies in the regions.

The **Cybersecurity Center** within the **Department of Operational Search Activities of the Ministry of Internal Affairs** carries out operational-search activities relating to cybercrimes.

However, pursuant to the Law “On the Central Bank,” its activities are provided for contrary to the principal sectoral law, namely, information and cybersecurity oversight is to be administered by the Central Bank rather than by the State Security Service.

³⁰³ Resolution № RP–4452 of the President of the Republic of Uzbekistan “On Additional Measures to Improve the System for Monitoring the Implementation of Information Technologies and Communications and Their Protection” dated September 14, 2019 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

Fourth, the National Agency for Prospective Projects of the Republic of Uzbekistan regulates matters relating to mining and cryptocurrency, issues licenses and permits, and **applies to authorized bodies regarding cases of violations of the law.**

It should be emphasized that the existence of overlapping powers and functions of state bodies constitutes, pursuant to Law № LRU–860 of the Republic of Uzbekistan “On Anti-Corruption Examination of Regulatory Legal Acts and Their Drafts” dated August 8, 2023³⁰⁴, **a corruption-generating factor related to powers, rights, and obligations.**

Fifth, Uzkomnazorat cooperates with the Agency for Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan on matters concerning ensuring compliance with the requirements of legislative acts and, upon the submission of the Agency for Information and Mass Communications, takes measures in accordance with the established procedure against information sector entities that violate the requirements of the legislation of the Republic of Uzbekistan.

However, the failure to take any effective measures in this regard in practice is resulting in an increase in offenses related to telecommunications networks.

For information: this provision was established pursuant to Resolution № RP–4452 of the President of the Republic of Uzbekistan “On Additional Measures to Improve the System for Monitoring the Implementation of Information Technologies and Communications and Their Protection” dated September 14, 2019³⁰⁵.

Sixth, the main tasks of the Ministry of Justice include implementing a unified state policy in the field of personal data, as well as monitoring and coordinating the activities of state bodies and organizations in the field of processing personal data.

However, the State Inspectorate “Uzkomnazorat” draws up administrative offense reports against owners and/or operators who process personal data of citizens using information technologies, including on the Internet, for violations of the special conditions for processing personal data of citizens of the Republic of Uzbekistan, and submits them to the court for consideration.

For information: The provisions of Resolution № RP–3666 of the President of the Republic of Uzbekistan “On Organizational Measures to Further Improve the Activities of the Ministry of Justice of the Republic of Uzbekistan” dated April 13, 2018³⁰⁶ and the Regulation “On the Procedure for Exercising State Control over Compliance with the Special Conditions for

³⁰⁴ Law № LRU–860 of the Republic of Uzbekistan “On Anti-Corruption Examination of Regulatory Legal Acts and Their Drafts” dated August 8, 2023 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁰⁵ Resolution № RP–4452 of the President of the Republic of Uzbekistan “On Additional Measures to Improve the System for Monitoring the Implementation of Information Technologies and Communications and Their Protection” dated September 14, 2019 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁰⁶ Resolution № RP–3666 of the President of the Republic of Uzbekistan “On Organizational Measures to Further Improve the Activities of the Ministry of Justice of the Republic of Uzbekistan” dated April 13, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

Processing Personal Data of Citizens of the Republic of Uzbekistan,” approved by Resolution № 707 of the Cabinet of Ministers dated September 5, 2018³⁰⁷, are mutually contradictory.

Seventh, pursuant to Article 245 of the Code of the Republic of Uzbekistan on Administrative Responsibility, the **court** is sufficiently defined in legislation as the body that considers corruption-related offenses; however, the **absence of its authority to conduct an inquiry under the legislation** necessitates the establishment of a specialized body authorized in this field.

Eighth, in the United States³⁰⁸, Germany³⁰⁹, France³¹⁰, India³¹¹, Canada³¹², Singapore³¹³, and South Korea³¹⁴, a separate state body is responsible for cybersecurity.

For example, cybersecurity agencies operate in Singapore³¹⁵ and South Korea³¹⁶.

Ninth, pursuant to Resolution № RP–81 of the President of the Republic of Uzbekistan “On Measures to Introduce a Rating Assessment System for the Effectiveness of Anti-Corruption Efforts” dated January 12, 2022, along with the introduction of a rating assessment system aimed at analyzing and evaluating the effectiveness of anti-corruption measures and eliminating shortcomings in state bodies and organizations, including local executive authorities, a system for submitting reports of corruption has also been established³¹⁷.

For information: Through the “e-anticor.uz” platform, a total of 686 applications were submitted by citizens, 562 of which were resolved, while 124 applications are under consideration³¹⁸.

Tenth, the Ministry of Internal Affairs has introduced the Unified Information System “Electronic Criminal-Legal Statistics” for registering criminal cases and maintaining their database, as well as the Unified Electronic Case Management System for Administrative Offenses for registering cases of administrative offenses and maintaining their database.

For information: The Unified Information System “Electronic Criminal-Legal Statistics” was introduced into practice by Decree № DP–5566 of the President of the Republic of Uzbekistan “On Measures to Fundamentally Improve the Criminal-Legal Statistics System and Increase the Effectiveness of Systematic

³⁰⁷ Regulation “On the Procedure for Exercising State Control over Compliance with the Special Conditions for Processing Personal Data of Citizens of the Republic of Uzbekistan,” approved by Resolution № 707 of the Cabinet of Ministers dated September 5, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁰⁸ <https://www.cisa.gov/>.

³⁰⁹ https://www.bsi.bund.de/EN/Home/home_node.html.

³¹⁰ <https://cyber.gouv.fr/en>.

³¹¹ <https://www.bsc-icc.com/service/cert-in>.

³¹² <https://www.cse-cst.gc.ca/en>.

³¹³ <https://www.csa.gov.sg/contact-us>.

³¹⁴ <https://www.kisa.or.kr/EN>.

³¹⁵ <https://www.csa.gov.sg/contact-us>.

³¹⁶ <https://www.kisa.or.kr/EN>.

³¹⁷ Resolution № RP–81 of the President of the Republic of Uzbekistan “On Measures to Introduce a Rating Assessment System for the Effectiveness of Anti-Corruption Efforts” dated January 12, 2022 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³¹⁸ <https://e-anticor.uz/oz>.

Analysis of Crimes” dated October 31, 2018³¹⁹, while the *Unified Electronic Case Management System for Administrative Offenses* was introduced into practice by Resolution № 431 of the Cabinet of Ministers “On Additional Measures to Introduce an Electronic System for the Processing of Administrative Offense Cases” dated July 8, 2021³²⁰.

However, the above information systems are not integrated with each other.

Eleventh, Article 7 of the Law “On Combating Corruption” lists 7 state bodies that directly carry out activities to combat corruption.

However, the Law “On Cybersecurity” provides only for the **State Security Service** as the authorized body exercising oversight and regulation in the field of cybersecurity.

At the same time, Article 14 of this Law establishes the rights and obligations of state bodies and organizations in ensuring cybersecurity.

Accordingly, it is necessary to clearly define, among the powers of the authorized bodies under Articles 8¹–13 of the Law “On Combating Corruption,” including the powers of the State Security Service in the field of combating corruption, its powers to combat cybercorruption.

Twelfth, Article 15 of the Law “On Combating Corruption” provides for the participation of mass media in combating corruption. However, given that artificial intelligence technologies may create broad opportunities for corruption-related crimes, particularly crimes associated with organized crime, it would be appropriate to reflect the participation of artificial intelligence in combating corruption in the Law “On Combating Corruption.”

Based on the foregoing, it would be appropriate to instruct the State Security Service, the Anti-Corruption Agency, the Prosecutor General’s Office, the Ministry of Internal Affairs, the Ministry of Justice, the National Agency for Prospective Projects, the Agency for Information and Mass Communications, the Ministry of Digital Technologies, the Central Bank, and the Supreme Court, in cooperation with the Senate and the Legislative Chamber, to develop the following draft legislative acts and submit them to the Presidential Administration:

1. To adopt the Decree of the President of the Republic of Uzbekistan “On Measures to Improve the Organizational and Criminal-Legal Framework for Combating Cybercorruption,” providing for:

approval of a “road map” providing for combating corruption through digitalization in the areas of healthcare, education, public administration, mahalla, social protection, digitalization, including digital assets, and public procurement;

in accordance with the requirements of the Law “On Cybersecurity,” transferring the powers of the Prosecutor General’s Office and the Ministry of

³¹⁹ Decree № DP–5566 of the President of the Republic of Uzbekistan “On Measures to Fundamentally Improve the Criminal-Legal Statistics System and Increase the Effectiveness of Systematic Analysis of Crimes” dated October 31, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³²⁰ Resolution № 431 of the Cabinet of Ministers of the Republic of Uzbekistan “On Additional Measures to Introduce an Electronic System for the Processing of Administrative Offense Cases” dated July 8, 2021 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

Internal Affairs of the Republic of Uzbekistan to investigate cybercrimes to the State Security Service;

reorganizing the “Cybersecurity Center” SE and establishing the Cybersecurity Agency of the Republic of Uzbekistan within the State Security Service;

establishing the Agency’s operations on a 24/7 basis and clearly defining its powers to combat cyber offenses and cybercrimes at the national and international levels;

transferring the Center for Mass Communications and the Republican Center for Management of Telecommunication Networks to the Agency;

reducing overlapping and similar powers by transferring to the Agency the functions and tasks of the Ministry of Internal Affairs, the Ministry of Justice, the Ministry of Digital Technologies, the National Agency for Prospective Projects, the Agency for Information and Mass Communications, the Central Bank, the Anti-Corruption Agency, and the Inspection for Control in the Field of Informatization and Telecommunications concerning oversight and inspection in the areas of informatization, personal data, including information security and cybersecurity;

reducing overlapping and similar powers by transferring to the Agency the functions and tasks of the Ministry of Internal Affairs and the Inspection for Control in the Field of Informatization and Telecommunications concerning proceedings on administrative offenses in the areas of informatization, personal data, including information security and cybersecurity, including drawing up administrative offense reports and submitting them to the court;

introducing the positions of **cyber specialist** and **cyber investigator** within the State Security Service, responsible for conducting operational crime-search activities, investigative actions, and court proceedings concerning cybercrimes;

forming a separate “**corps of judges**” specializing in considering cyber-administrative offenses and cybercrimes within the Criminal Judicial Panel of the Supreme Court of the Republic of Uzbekistan and within the courts of the Republic of Karakalpakstan, regions, and the city of Tashkent;

transferring the Unified Electronic Case Management System for Administrative Offenses, the Unified Information System “Electronic Criminal-Legal Statistics,” and the “e-anticor.uz” platform to a unified platform;

developing the “**Cybersecurity**” information system for the prompt consideration and resolution of reports concerning cyber offenses, including cybercorruption, and ensuring its integration with the information systems on the unified platform and all information systems in the Republic;

introducing into practice the automated, artificial intelligence-based “**CCA**” platform and approving its Regulations, enabling the automatic receipt and analysis of reports concerning cyber offenses and cybercrimes, including reports concerning cyber offenses submitted through the pm.gov.uz website and the “eanticor.uz” information system, and enabling the consideration of reports in real time;

establishing, through artificial intelligence technologies, the prediction of cyber offenses and cybercrimes; enabling investigators and courts to use artificial intelligence as an advisory and analytical tool in reviewing decisions, identifying

and exposing cyber offenses and cybercrimes, imposing sentences, and analyzing and evaluating the effectiveness of measures implemented to combat corruption;

transforming the organizational and legal form of the Limited Liability Company “Center for Development of Information Technologies and Information Resources” into a state institution and reorganizing it as the “Republican Center for Digital Technologies and Technical Equipment Expertise”;

developing a draft normative document on unified technical regulation for combating cybercorruption;

defining specific tasks for improving Uzbekistan’s position in international rankings and indices concerning combating cybercorruption;

introducing amendments and additions to Decree № DP–38 of the President of the Republic of Uzbekistan “On Defining the Cybersecurity Strategy of the Republic of Uzbekistan and Improving the System for Preventing Cybercrime” dated March 10, 2026;

simultaneously bringing subordinate legislation into compliance with this Decree.

2. To adopt the Law of the Republic of Uzbekistan “On Amendments and Additions to Certain Legislative Acts in Connection with the Improvement of Combating Cybercorruption-Related Offenses,” providing for:

1) in the Law “On Combating Corruption”:

providing for the concepts of cybercorruption, corruption-related offense, corruption-related crime, cybercorruption-related offense, cybercorruption-related crime, cybersecurity incident, cyberspace, and cybersecurity object;

clarifying the powers of authorized bodies based on cybercorruption;

establishing the procedure for the participation of artificial intelligence in combating corruption;

approving the list of corruption-related and cybercorruption-related offenses and crimes;

2) amending and supplementing the Law “On Cybersecurity” to clarify the cybersecurity object based on cybercorruption;

3) amending and supplementing the Criminal Code based on advanced foreign experience and the information-analytical material attached from a scientific and legal perspective concerning cybercorruption, and providing for the concepts of cybercrime, cyberspace, cybercorruption, and corruption in Section VIII;

4) clarifying the investigation and territorial jurisdiction of cybercrimes in Articles 345 and 346 of the Criminal Procedure Code;

5) granting the Cybersecurity Agency the authority to draw up administrative offense reports, conduct inquiries, and, pursuant to Article 282 of the Code of the Republic of Uzbekistan on Administrative Responsibility, submit them to the court concerning offenses committed in or through telecommunications and Internet networks, as well as offenses provided for in Articles 46–46¹, 56² and 56⁴ of the Code of the Republic of Uzbekistan on Administrative Responsibility (cases committed through telecommunications and Internet networks), Article 61¹ (the part concerning cybercorruption), Articles 151, 155–155³, and Articles 193¹–193² (the part concerning cybercorruption), and other cyber-administrative offenses;

6) introducing amendments and additions to the following laws:

in the Law “On Informatization,” incorporating the concepts of “artificial intelligence” and “artificial intelligence technologies” and establishing information and cybersecurity requirements for artificial intelligence;

in the Laws “On the Central Bank,” “On Banks and Banking Activities,” “On Payments and Payment Systems,” “On Electronic Commerce,” “On Telecommunications,” “On Personal Data,” “On Electronic Digital Signature,” “On Electronic Government,” “On Electronic Document Management,” “On Guarantees for the Protection of Deposits in Banks,” “On Non-Bank Credit Organizations and Microfinance Activities,” “On Conflict of Interests,” “On the Prosecutor’s Office,” “On Courts,” “On the State Security Service of the Republic of Uzbekistan,” “On the Cabinet of Ministers of the Republic of Uzbekistan,” “On Internal Affairs Bodies,” “On the Status of a Deputy of the Legislative Chamber and a Member of the Senate of the Oliy Majlis of the Republic of Uzbekistan,” “On the Status of a Deputy of the Regional, District and City Councils of People’s Deputies,” and “On the Openness of the Activities of State Authorities and Administration Bodies,” establishing specific obligations of state bodies and organizations as cybersecurity subjects to ensure information security and cybersecurity and to combat cyber offenses and cybercrimes, including cybercorruption.

4.2-§. Legal Aspects of International Instruments on Combating Cybercrimes, Including Cybercorruption

In today's globalized era, the development of digital technologies is also contributing to the increased activity of forces that use them for malicious purposes, and this global problem is currently referred to as cybercrime. While these crimes caused **USD 8.27 trillion** in damage to countries worldwide in 2023 and **USD 9.5 trillion** in 2024, this figure is projected to reach **USD 10.5 trillion** in 2025. The increase in these crimes is leading not only to such damage but also to a number of other negative consequences, and in this regard, combating cybercrime gives rise to the following necessities, including:

1) ensuring information and cybersecurity;

*for example, medical information systems store sensitive information such as personal data, medical records, and medical histories. As a result of cyberattacks, this information may be stolen or altered, which poses a serious threat to patients and medical institutions. It should be emphasized that, pursuant to the Law of the Republic of Uzbekistan "On Protection of Citizens' Health," information concerning a citizen's seeking medical assistance, the state of his or her health, the diagnosis of his or her illness, as well as other information obtained during examination and treatment, constitutes a medical secret. Persons who become aware of information constituting a medical secret in the course of education, professional, official, or other duties are not permitted to disclose such information without the consent of the citizen or his or her legal representative, and persons to whom information constituting a medical secret has been provided in accordance with the procedure established by law shall be held liable, in accordance with the law, for disclosure of medical secrets on an equal basis with medical and pharmaceutical workers*³²¹.

2) reducing financial and economic risks;

for example, cyberattacks may result in significant economic losses for the public and private sectors. Through ransomware viruses, data may be locked, and a ransom may be demanded for its restoration.

3) compliance with legislation and international standards;

for example, in accordance with the rules of the World Health Organization (WHO)³²² and the European Union's GDPR (General Data Protection Regulation)³²³, the protection of medical data is considered one of the key requirements.

4) maintaining the stability of information systems;

for example, information systems may become inoperable as a result of cyberattacks, which may lead to disruptions in the provision of medical services.

5) ensuring public security

for example, cybercrimes pose threats not only to healthcare but also to other sectors and public services.

Accordingly, ensuring overall national security can be achieved by strengthening the protection of systems based on information and communication technologies. For this reason, the Republic of Uzbekistan is also paying particular attention to this area, in particular:

³²¹ Law № 265-I of the Republic of Uzbekistan "On Protection of Citizens' Health" dated August 29, 1996 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³²² <https://www.who.int/>.

³²³ <https://gdpr-info.eu/>.

in the national legislation, the concepts of cybercrime and cybersecurity were first used in an official normative legal act in paragraph 297 of the State Programme on the Implementation of the Action Strategy for the Five Priority Areas of Development of the Republic of Uzbekistan for 2017–2021 in the “Year of Dialogue with the People and Human Interests”, approved by Decree № DP–4947 of the President of the Republic of Uzbekistan dated February 7, 2017³²⁴;

Ensuring cybersecurity of the Republic of Uzbekistan in the field of ensuring cybersecurity and introducing modern technologies for the protection of networks, software products, information systems and resources; developing and implementing a unified state policy in this area; implementing a mechanism for ensuring information security of websites in the national segment of the worldwide Internet information network through the use of methods and means for timely notification of and response to unauthorized access attempts and computer virus attacks in the information space of the Republic of Uzbekistan; monitoring violations in the areas of telecommunications, e-government, postal services, informatization and the radio-frequency spectrum, interacting with law enforcement bodies in terms of identifying and preventing such violations; identifying and combating threats to information security and cybersecurity; developing and implementing effective mechanisms to combat the use of information and communication technologies for criminal, intelligence and terrorist purposes and to prevent their use for such purposes; collecting and analyzing information on threats to information security and cybersecurity; and organizing and conducting research, experimental design, project, exploratory and technological developments in the field of ensuring information security and cybersecurity were established as one of the main tasks of the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan (currently the Ministry of Digital Technologies)³²⁵;

The Concept for Enhancing the Participation of State and Economic Management Bodies in Virtual Space was approved³²⁶;

The State Inspectorate for Control in the Sphere of Informatization and Telecommunications of the Republic of Uzbekistan was granted the authority to monitor, study, and inspect compliance by business entities with technical and technological requirements concerning information security and cybersecurity³²⁷;

³²⁴ State Programme on the Implementation of the Action Strategy for the Five Priority Areas of Development of the Republic of Uzbekistan for 2017–2021 in the “Year of Dialogue with the People and Human Interests”, approved by Decree № DP–4947 of the President of the Republic of Uzbekistan dated February 7, 2017 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³²⁵ Regulation “On the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan”, approved by Resolution № 318 of the Cabinet of Ministers of the Republic of Uzbekistan dated May 1, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³²⁶ Concept for Enhancing the Participation of State and Economic Management Bodies in Virtual Space, approved by Resolution № 622 of the Cabinet of Ministers of the Republic of Uzbekistan dated August 7, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³²⁷ Regulation “On the State Inspectorate for Control in the Sphere of Informatization and Telecommunications of the Republic of Uzbekistan”, approved by Resolution № RP–4024 of the President of the Republic of Uzbekistan dated November 21, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

Sharda University was established in Uzbekistan to ensure the training of highly qualified specialists in the fields of information technologies and cybersecurity at the level of international standards³²⁸;

The State Security Service of the Republic of Uzbekistan was designated as the authorized body in the field of cybersecurity regulation³²⁹;

A procedure was developed for restricting access to websites and/or web pages containing information whose dissemination is prohibited under the legislation of the Republic of Uzbekistan³³⁰;

In the criminal legislation of the Republic of Uzbekistan, when the Criminal Code was adopted in 1994, criminal liability for violation of the rules of informatization was established under Article 174, namely, for unauthorized access to an information network or, where access was authorized, failure to take appropriate protective measures, or unlawfully obtaining information from an information network; as well as for intentionally altering, losing, removing or destroying data contained in an informatization system by a person authorized to use the system, where this resulted in substantial damage; for developing and disseminating computer viruses or programs without the appropriate authorization for the purpose of modifying data or programs stored in computer systems; and for using an information system without authorization where this resulted in the alteration, removal or destruction of data or the failure of the system.

However, due to the strengthening of liability for unlawful acts committed in the field of informatization and data transmission, this article was removed from the Criminal Code of the Republic of Uzbekistan, and **Chapter XX¹ “Crimes in the Sphere of Information Technologies”** was incorporated into the Criminal Code. This Chapter established criminal liability for violation of the rules of informatization; unlawful (unauthorized) access to computer information; the preparation or transfer and dissemination of special means intended for unlawful (unauthorized) access to a computer system; modification of computer information; computer sabotage; and the creation, use or dissemination of malicious programs³³¹. However, although these crimes were referred to under the general title of crimes in the sphere of information technologies, in 2001, criminal liability was established under paragraph “g” of Part 3 of Article 167 of the Criminal Code for embezzlement or misappropriation of another person’s property entrusted to or under the control of the guilty person through the use of computer technology; under paragraph “g” of Part 2 of Article 168 of the Criminal Code for fraud, that is, obtaining another

³²⁸ Resolution №RP-4278 of the President of the Republic of Uzbekistan “On the Establishment of Sharda University in Uzbekistan” dated April 10, 2019 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³²⁹ Resolution №RP-4452 of the President of the Republic of Uzbekistan “On Additional Measures to Improve the System for Monitoring the Implementation of Information Technologies and Communications and Ensuring Their Protection” dated September 14, 2019 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³³⁰ Resolution №707 of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Further Improve Information Security on the World Wide Web” dated September 5, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³³¹ Law №LRU-137 of the Republic of Uzbekistan “On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan in Connection with the Strengthening of Liability for Committing Unlawful Acts in the Field of Informatization and Data Transmission” dated December 25, 2007 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

person's property or the right to another person's property through deception or abuse of trust; and under paragraph "b" of Part 3 of Article 169 of the Criminal Code for theft, that is, the secret appropriation of another person's property³³²; in 2007, under Part 2 of Article 278 of the Criminal Code, criminal liability was established for providing services by providers of the worldwide Internet information network through telecommunication networks, including for organizing or conducting gambling and other games based on risk, reproducing, duplicating and distributing the relevant software, as well as for organizing and conducting gambling and other games based on risk through providers of the worldwide Internet information network after the imposition of an administrative penalty for such acts³³³; in 2016, under Article 188¹ of the Criminal Code, unlawful activities involving the attraction of funds and/or other property of individuals and legal entities through the assumption of obligations to provide property benefits, with the fulfillment of previously assumed obligations using newly attracted funds and/or other property of individuals and legal entities, as well as managing and facilitating such activities and advertising such activities for the purpose of involving persons in participation therein, including advertising through mass media, telecommunication networks, as well as the worldwide Internet information network, were defined as unlawful activities involving the attraction of funds and/or other property³³⁴; under paragraph "g" of Part 3 of Article 244¹ of the Criminal Code, criminal liability was established for preparing or storing materials using telecommunication networks, as well as the worldwide Internet information network, for the purpose of distributing them or preparing, storing, distributing or displaying attributes or symbols of religious-extremist or terrorist organizations, containing ideas of religious extremism, separatism and fundamentalism, calling for mass violence or the forced displacement of citizens, or aimed at creating panic among the population, as well as for using religion for the purpose of disrupting civil harmony, spreading defamatory or destabilizing fabrications and committing other acts directed against established rules of conduct and public safety, namely, for preparing, storing, distributing or displaying materials that threaten public safety and public order³³⁵; in 2017, criminal liability was established under paragraph "g" of Part 2 of Article 103 of the Criminal Code for bringing a person to the level of suicide through the use of telecommunication networks, as well as the worldwide Internet information

³³² Law № 254-II of the Republic of Uzbekistan "On Amendments and Additions to the Criminal, Criminal Procedure Codes and the Code of Administrative Responsibility of the Republic of Uzbekistan in Connection with the Liberalization of Criminal Penalties" dated August 29, 2001 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³³³ Law № LRU–109 of the Republic of Uzbekistan "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan in Connection with the Regulation of the Organization and Conduct of Gambling and Other Games Based on Risk" dated September 14, 2007 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³³⁴ Law № LRU–411 of the Republic of Uzbekistan "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan" dated September 23, 2016 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³³⁵ Law № LRU–405 of the Republic of Uzbekistan "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan" dated April 25, 2016 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

network, and under paragraph “v” of Part 2 of Article 103¹ for inducing a person to commit suicide³³⁶.

At the same time, for the purpose of ensuring cybersecurity, provisions were established whereby the registration and implementation of information systems and databases developed as a result of the implementation of information projects in the Unified Register of Information Systems and Resources of the “Digital Government” are permitted only after obtaining positive conclusions from the Ministry of Digital Technologies and the “Cybersecurity Center” SUE regarding their compliance with technical specifications and information security requirements³³⁷;

The procedure for complying with information security and cybersecurity requirements was incorporated into the rules of the payment system; it was established that a user of payment services shall have the right to use the remote service system of the payment service provider servicing the user’s bank account or to use the services of another payment service provider, provided that the payment service provider has the technical capability for such use, subject to compliance with the requirements for ensuring information security and cybersecurity and equal access to all payment service providers; a payment service provider shall ensure compliance with this condition when providing payment services; violations affecting the provision of information security and cybersecurity shall be remedied within three months from the date of dispatch of the Central Bank’s initial instruction; the Central Bank shall establish requirements for software tools that ensure interaction with the Central Bank’s interbank payment and clearing systems, including automated banking systems, as well as requirements for ensuring information security and cybersecurity measures in payment systems; a document on the security policy, including a detailed risk assessment, as well as a description of the measures to be taken to mitigate risks, including the risks of fraud and unlawful use of confidential and personal data, in order to ensure information security and cybersecurity and the protection of payment service users, shall be attached to the application for a license submitted by a legal entity that is not a bank; where violations affecting the uninterrupted operation of the payment system, as well as the provision of information security and cybersecurity, are not remedied by the operator of the payment system within three months from the date of dispatch of the Central Bank’s initial instruction, the Central Bank shall have the right to decide on the revocation of the license of the payment system operator; supervision over payment system operators and payment service providers in the field of information security and cybersecurity shall be carried out by the Central Bank; in the event of a breach of the information security and cybersecurity regime, payment system operators and payment service providers shall promptly notify the Central Bank

³³⁶ Law № LRU-436 of the Republic of Uzbekistan “On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan, as well as Declaring Certain Legislative Acts to Have Lost Force” dated June 13, 2017 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³³⁷ Resolution №RP-4328 of the President of the Republic of Uzbekistan “On Measures to Improve the Quality of Development and Implementation of Projects in the Field of Information and Communication Technologies within the Framework of the ‘Electronic Government’ System” dated May 21, 2019 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

thereof after the violation is identified, as well as of the measures being taken to mitigate its consequences. The Central Bank shall establish and maintain a database of information on breaches of the information security and cybersecurity regime of payment systems; violations of the requirements of legislation on banking secrecy, on combating the legalization of proceeds from criminal activities, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, as well as violations of legislative requirements resulting in the occurrence of a cyber threat or cybersecurity incident in banking information systems, were classified as serious violations³³⁸;

It was established that the specialized platforms of business entities for the remote control of outdoor advertising facilities equipped with video screens (electronic displays) shall be integrated into the electronic system, and that such specialized platforms shall undergo a comprehensive assessment at the “Cybersecurity Center” State Unitary Enterprise for compliance with cybersecurity requirements³³⁹;

It was provided that a positive opinion shall be obtained from the Ministry of Digital Technologies of the Republic of Uzbekistan and the “Cybersecurity Center” State Unitary Enterprise confirming that the electronic exchange trading system and the settlement and clearing system comply with the requirements stipulated in the Regulation on General Requirements for Electronic Trading Systems of Commodity Exchanges³⁴⁰.

In order to regulate relations pertaining to cybersecurity directly at the legislative level, the Law of the Republic of Uzbekistan “On Cybersecurity” № LRU–764 dated April 15, 2022, was adopted³⁴¹.

The legislation established provisions stipulating that an opinion of the authorized bodies confirming the existence of violations of the requirements of legislation on information security and cybersecurity shall constitute grounds for the temporary suspension or termination of connection to the Interagency Integration Platform³⁴².

The Regulation on the Procedure for Ensuring the Cybersecurity of Critical Information Infrastructure Objects of the Republic of Uzbekistan and the General

³³⁸ Law №LRU–964 of the Republic of Uzbekistan “On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan in Connection with the Improvement of Legislation in the Field of Ensuring Cybersecurity” dated September 20, 2024 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³³⁹ Resolution №695 of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Increase the Effectiveness of the Public Oversight System over the Activities of State Bodies and Organizations in Addressing Problems of the Population” dated October 24, 2024 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁴⁰ Resolution №570 of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Widely Introduce Advanced Information Technologies into Exchange Trading and Consistently Continue Digitalization Processes in the Sector” dated September 12, 2024 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁴¹ Law №LRU–764 of the Republic of Uzbekistan “On Cybersecurity” dated April 15, 2022 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁴² Resolution №516 of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Further Improve the Interagency Electronic Cooperation System and Information Exchange of Data” dated September 20, 2022 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

Cybersecurity Requirements for Critical Information Infrastructure Objects of the Republic of Uzbekistan were approved³⁴³;

Services for cybersecurity testing and protection (including cryptographic protection) of information systems and software were included among the types of services in the field of information technology consulting, as well as cybersecurity testing and protection of information systems and software³⁴⁴;

The assessment of the level of cybersecurity of the Republic of Uzbekistan and the level of cybersecurity of critical information infrastructure facilities was established³⁴⁵;

The procedures for ensuring information security and cybersecurity in the payment systems of payment system operators and payment service providers, as well as for taking measures to prevent offenses committed through digital technologies³⁴⁶, categorizing critical information infrastructure objects of the Republic of Uzbekistan and establishing a unified register thereof³⁴⁷, conducting expert assessments for compliance with cybersecurity requirements³⁴⁸, and certifying hardware, hardware-software, and software tools used to ensure the cybersecurity of information systems and resources³⁴⁹ were established;

In the banking and financial sector, the prevention of fraud, assessment of users' creditworthiness, and forecasting of market trends were identified as one of the priority areas for the introduction of artificial intelligence technologies³⁵⁰.

³⁴³ Resolution №RP-167 of the President of the Republic of Uzbekistan "On Additional Measures to Improve the System for Ensuring the Cybersecurity of Critical Information Infrastructure Objects of the Republic of Uzbekistan" dated May 31, 2023 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁴⁴ Resolution №447 of the Cabinet of Ministers of the Republic of Uzbekistan "On Approval of the List of Types of Services in the Field of Information and Communication Technologies" dated September 4, 2023 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁴⁵ Order №91 of the Chairman of the State Security Service of the Republic of Uzbekistan "On Approval of the Regulation on the Procedure for Assessing the Level of Cybersecurity of the Republic of Uzbekistan and Critical Information Infrastructure Objects" dated September 4, 2023 (registered on September 22, 2023, registration №3458) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁴⁶ Resolution №13/1 of the Board of the Central Bank of the Republic of Uzbekistan "On Approval of the Regulation on Ensuring Information Security and Cybersecurity in the Payment Systems of Payment System Operators and Payment Service Providers and Taking Measures to Prevent Offenses Committed through Digital Technologies" dated April 24, 2024 (registered on May 21, 2024, registration №3513) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁴⁷ Order №118 of the Chairman of the State Security Service of the Republic of Uzbekistan "On Approval of the Temporary Regulation on the Procedure for Categorizing Critical Information Infrastructure Objects of the Republic of Uzbekistan and Establishing a Unified Register Thereof" dated October 24, 2024 (registered on November 11, 2024, registration №3570) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁴⁸ Order №113 of the Chairman of the State Security Service of the Republic of Uzbekistan "On Approval of the Regulation on the Procedure for Conducting Expert Assessments for Compliance with Cybersecurity Requirements" dated October 15, 2024 (registered on November 14, 2024, registration №3573) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁴⁹ Order №114 of the Chairman of the State Security Service of the Republic of Uzbekistan "On Approval of the Regulation on the Procedure for Certifying Hardware, Hardware-Software, and Software Tools Used to Ensure the Cybersecurity of Information Systems and Resources" dated October 15, 2024 (registered on November 14, 2024, registration №3574) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁵⁰ Resolution №RP-358 of the President of the Republic of Uzbekistan "On Approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030" dated October 14, 2024 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

During the period under review, the “Cybersecurity Center” State Unitary Enterprise was established³⁵¹.

A separate special Law of the Republic of Uzbekistan directly concerning the provision of cybersecurity was adopted; **30** articles of the Criminal Code of the Republic of Uzbekistan and **389** articles of the Criminal Procedure Code of the Republic of Uzbekistan were reviewed, and certain aspects of liability for cybercrimes and the procedures for their consideration were established;

Pursuant to **one special Decree and three Resolutions** of the President of the Republic of Uzbekistan, it was established that the State Security Service is the authorized body regulating cybersecurity, and separate cybersecurity divisions and centers were established within the “Cybersecurity Center” State Unitary Enterprise, the Central Bank, the Ministry of Internal Affairs, and other agencies;

A system of open financing for the activities of the “Cybersecurity Center” State Unitary Enterprise was established³⁵².

In 4 educational organizations, a **system for training personnel** in cybersecurity was established as a separate field at the bachelor’s and master’s levels, and 3 **higher education organizations** specializing in training cybersecurity professionals were established;

a cybercrime notification system (<https://csec.uz/uz/>) and a unified node were put into operation, and a unified communication network for cybersecurity of state bodies and organizations was established;

a system for conducting expert assessments, certification, and audits of state information systems and resources for compliance with information security and cybersecurity requirements, as well as digital forensics activities, was established; the legal status of electronic (digital) evidence was defined, and procedures for protecting personal data and intellectual property rights were developed and implemented in practice;

reforms were carried out in the banking and financial system, and mechanisms for ensuring the cybersecurity of banks and payment organizations were established.

The preparation of reports on the cybersecurity of the Republic of Uzbekistan and public disclosure of cybersecurity information were put into practice;

A secure electronic identification system was created (<https://id.egov.uz/>);

A competition for the Presidential Award for Ensuring Cybersecurity was established (<https://awards.gov.uz/>);

The foundation was laid for international cooperation in the field of cybersecurity.

There are a number of problems in ensuring the cybersecurity of the Republic of Uzbekistan at the national and international levels, and the failure to resolve these problems, as well as the insufficient level of cybersecurity, is having a particularly

³⁵¹ Resolution №RP–4452 of the President of the Republic of Uzbekistan “On Additional Measures to Improve the System for Monitoring the Implementation of Information Technologies and Communications and Ensuring Their Protection” dated September 14, 2019 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

³⁵² Law №LRU–1011 of the Republic of Uzbekistan “On the State Budget of the Republic of Uzbekistan for 2025” dated December 24, 2024 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

negative impact on the further development of the ongoing reforms, especially on the protection of the interests of the individual, society, and the state.

In particular, according to the Global Cybersecurity Index — the ranking of countries by level of cybersecurity prepared annually by experts of the International Telecommunication Union of the United Nations — the **Republic of Uzbekistan** ranked **64th**, while it ranked **40th** in the National Cyber Security Index.

The following were identified as **shortcomings** preventing it from achieving a higher position, including:

- 1) the procedure for coordinating cybersecurity policy has not been established;
- 2) the cybersecurity strategy of the Republic of Uzbekistan has not been developed and approved;
- 3) the implementation plan (roadmap) for the cybersecurity strategy of the Republic of Uzbekistan is not officially and publicly available;
- 4) there is no official position or guarantee of the Republic of Uzbekistan regarding the application of international legal norms and compliance with human rights during cyberattacks committed in cyberspace; the Republic of Uzbekistan is not a party to any of the international conventions on cybersecurity and has not itself initiated such an instrument;
- 5) the Republic of Uzbekistan has made no contribution to ensuring cybersecurity at the international level;
- 6) cybersecurity competencies are not taught in primary, secondary, and secondary specialized education, and there is no system of continuing education in this area;
- 7) there is no association of cybersecurity specialists (a non-governmental non-profit organization);
- 8) there is an insufficient number of studies, developments, and textbooks on cybersecurity, as well as significant differences between articles in the technical and legal fields, which are not presented in mutually comprehensible language;
- 9) there are no cybersecurity trust services, such as a helpline, a call center receiving such calls, and agencies responsible for their prompt consideration;
- 10) there is no body responsible for supervising the activities of trust services;
- 11) cybersecurity requirements for cloud technologies have not been established;
- 12) there is no system establishing a clear and prompt mechanism for ensuring cybersecurity; there is no clear mechanism specifying who responds, when, where, and how, through which the problem is resolved, and the tasks and functions of state bodies have not been clearly defined;
- 13) the responsibility of cybersecurity centers in the event of a cyber threat against the Republic of Uzbekistan or national security has not been clearly defined;
- 14) there is no system for coordinating efforts to raise cybersecurity awareness; that is, all state bodies and organizations independently conduct legal awareness activities and communicate to the public the work they have carried out,

but their activities are not coordinated and no specific state body has been designated for this purpose;

15) there is no system establishing a clear and prompt mechanism for ensuring cybersecurity; there is no clear mechanism specifying who responds, when, where, and how, through which the problem is resolved, and the tasks and functions of state bodies have not been clearly defined;

16) no single point of contact has been designated for international cooperation in the field of cybersecurity;

17) there has been no participation in international cyber crisis exercises;

18) a cyber crisis management plan has not been developed;

19) national cyber crisis management exercises have not been developed;

20) the Convention of the Council of Europe on Cybercrime has not been ratified or acceded to;

21) law enforcement bodies do not have special functions and powers to prevent and investigate cybercrimes;

22) there is no 24/7 point of contact for international cybercrime;

23) there is no military cyber defense capability;

24) military cyber defense exercises are not being conducted;

25) a military cyber doctrine has not been adopted.

Implementation of a very large number of these tasks does not require additional funding from the state budget; in particular, additional funding from the state budget may be required for the following areas, while implementation of the remaining tasks does not require additional budgetary funding:

1) cybersecurity competencies are not taught in primary, secondary, and secondary specialized education, and there is no system of continuing education in this area;

2) no single point of contact has been designated for international cooperation in the field of cybersecurity;

3) there has been no participation in international cyber crisis exercises;

4) national cyber crisis management exercises have not been developed;

5) the Convention of the Council of Europe on Cybercrime has not been ratified or acceded to;

6) there is no 24/7 point of contact for international cybercrime;

7) there is no military cyber defense capability;

8) military cyber defense exercises are not being conducted.

Implementation of the tasks identified under these rankings will contribute to the creation of the organizational, legal, and institutional foundations for establishing a secure cyberspace.

Today, in the Republic of Uzbekistan, the following may become victims of cybercriminals, which is contrary to the interests of individuals, society, and the state:

136,404 uz. domain administrators³⁵³;

2,273 information systems and resources;

³⁵³ <https://cctld.uz/stat/>.

1,768 telecommunications licensees³⁵⁴;
35,763,980 mobile users;
731 services available through the Unified Interactive Public Services Portal³⁵⁵;
376 banks and their branches³⁵⁶;
9,149 ATMs³⁵⁷;
2 payment system operators³⁵⁸;
257 bank plastic cards and customers' accounts associated with them³⁵⁹;
44 payment organizations³⁶⁰;
99 microfinance organizations³⁶¹;
402,802 business entities³⁶²;
1,150 personal data databases, and others.

The large-scale nature of this crime, as well as its speed and effectiveness compared with other crimes in terms of economic and time considerations, creates a number of problems in ensuring the interests of individuals, society, and the state in cyberspace through cross-border relations. In particular:

Administrative reforms are being carried out; however, administrative reforms aimed at ensuring cybersecurity have not been implemented sufficiently. For example, under the Law of the Republic of Uzbekistan "On Cybersecurity" №LRU-764 dated April 15, 2022, and pursuant to Resolution №RP-4452 of the President of the Republic of Uzbekistan "On Additional Measures to Improve the System for Monitoring the Implementation of Information Technologies and Communications and Ensuring Their Protection" dated September 14, 2019, the State Security Service was designated as the state body regulating the field of cybersecurity and the authorized body in this field; however, the body responsible for supervising this field has not been sufficiently defined.

Only by the aforementioned Resolution of the President of the Republic of Uzbekistan and Resolution №RP-167 of the President of the Republic of Uzbekistan "On Additional Measures to Improve the System for Ensuring the Cybersecurity of Critical Information Infrastructure Objects of the Republic of Uzbekistan" dated May 31, 2023, was it established that Uzkomnazorat, jointly with the "Cybersecurity Center" State Unitary Enterprise, shall monitor, conduct monitoring, study, and inspect the implementation and development of information and communication technologies and the state of information security in state and economic management bodies, local government bodies, and other organizations and agencies. However, in practice, it has not been clearly and sufficiently determined which state body is

³⁵⁴ https://license.gov.uz/registry?filter%5Bdocument_id%5D=4603&filter%5Bdocument_type%5D=LICENSE&page=177.

³⁵⁵ <https://oldmy.gov.uz/ru/>.

³⁵⁶ <https://cbu.uz/oz/credit-organizations/banks/branches/>.

³⁵⁷ <https://cbu.uz/oz/credit-organizations/banks/atm/>.

³⁵⁸ <https://cbu.uz/oz/payment-systems/documents-license-applicati/operators-of-payment-systems/>.

³⁵⁹ https://bank.uz/uz/cards?PAGEN_4=18/.

³⁶⁰ <https://cbu.uz/oz/payment-systems/documents-license-applicati/payment-organizations/>.

³⁶¹ <https://cbu.uz/oz/credit-organizations/microcredit/>.

³⁶² <https://www.sirstat.uz/uz/matbuot-markazi/qo-mita-yangiliklar/15232-qaysi-sohalarda-tadbirkorlik-subyektlari-ko-proq>.

responsible for protecting the interests of individuals, society, and the state in cyberspace in the field of cybersecurity, coordinating cybersecurity-related relations, and supervising this field.

At the same time, a number of tasks and functions of the current Ministry of Digital Technologies, as well as of the former Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan, as a regulator in the field of cybersecurity, have been omitted from Resolution №318 of the Cabinet of Ministers “On Approval of the Regulations on the Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan and the Inspectorate for Control in the Sphere of Communications, Informatization and Telecommunication Technologies under the Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan” dated May 1, 2018, which has lost its relevance.

Today, the field of cybersecurity in Uzbekistan is studied and personnel are trained primarily on the basis of technical theory, separately from the information sector; however, there is no qualified specialist who possesses comprehensive knowledge of this field from both the legal and technical perspectives.

At the same time, international instruments demonstrate that cybersecurity is considered as a single field based on both technical and legal theory, and cyber-offenses relating to the information sector and cybersecurity are addressed as a single area.

According to Article 15 of the Constitution of the Republic of Uzbekistan in its new edition, international treaties of the Republic of Uzbekistan, along with universally recognized principles and norms of international law, constitute an integral part of the legal system of the Republic of Uzbekistan. If an international treaty of the Republic of Uzbekistan establishes rules different from those provided for by the law of the Republic of Uzbekistan, the rules of the international treaty of the Republic of Uzbekistan shall apply. Accordingly, pursuant to this provision, the provisions of the draft Information Code should comply with the provisions of the Law “On Cybersecurity”, and this area should be systematized.

The initiative of the Republic of Uzbekistan is of significant importance in ensuring that it has sufficient experience and capabilities at both the national and international levels. In particular, when provisions of an international instrument are developed by representatives of a particular state, it is natural that, first and foremost, the rights and interests of that state are protected. Therefore, as a developing state, it would be natural for the Republic of Uzbekistan to initiate the adoption of an international Convention to be recognized and ratified by the Member States of the United Nations. This would enhance Uzbekistan’s role among the countries of the world, particularly as a centrally located state in Central Asia, by recognizing the cyberspace of all states as a single cyberspace and contributing to ensuring its security.

Furthermore, the development and maintenance of international cybersecurity ranking indices by the Republic of Uzbekistan would contribute to further enhancing the prestige of Uzbekistan among Russia, the United States, China, Türkiye, the United Arab Emirates, Saudi Arabia, Western and Eastern European countries, the

Republic of Korea, Japan, Singapore, Malaysia, Indonesia, Estonia, as well as among the Central Asian states.

The cybersecurity reforms being carried out in the Republic of Uzbekistan are fragmented, and the fact that reforms in this field are not developing on the basis of a unified medium-term strategy is causing systemic problems to arise.

From a technical perspective, the absence of unified special cybersecurity requirements for personal data databases, critical information infrastructure, and cloud technologies, based on cybersecurity considerations, as well as the fact that the register of critical information infrastructure has not yet been approved, is negatively affecting the effectiveness of the work being carried out. This is weakening the attention of cybersecurity entities to ensuring the security of classified objects and, as a result, is causing 1 percent of all cybercrimes committed in cyberspace not to be fully detected.

With regard to cybercrimes, the failure to ensure the inevitability of punishment is caused by the absence of an effective principle of inevitability of liability for systemic offenses in the field of communications and informatization under the Criminal Code and the Code of Administrative Responsibility.

For example, while Chapter XX¹ of the Criminal Code is recognized as “Crimes in the Sphere of Information Technologies”, there is no separate chapter concerning administrative offenses in this field in the Code of Administrative Responsibility. Moreover, no amendments or additions concerning liability have been introduced to the provisions establishing liability for offenses in the field of communications during the period under review. Despite the development of artificial intelligence and the increase in the number of offenses committed using this technology in practice, liability for such offenses has still not been provided for at all under either of the two codes governing liability.

In the personnel training system, instead of establishing continuous education in stages, a system for training cybersecurity specialists has been introduced in higher education. However, in order to develop the competencies of personnel in this field, specific programs and subjects for training personnel in cybersecurity have not yet been developed and implemented in primary (general), secondary, and secondary specialized education, and a unified educational system for training specialists in both legal and technological aspects of cybersecurity has still not been established.

Insufficient reforms have been implemented in the cybersecurity sector in terms of its material and technical base and financial support. Moreover, it has been established that the “Cybersecurity Center” State Unitary Enterprise itself is financed not from the state budget, but by the Digital Technologies Development Fund under the Ministry of Digital Technologies.

Today, there are 1,203 state information systems and resources and 1,150 personal data databases, almost all of which are maintained by individuals and legal entities. There are virtually no clear rules governing their technical and legal protection, leaving personal data and information resources at risk.

The fact that this risk is currently developing in close interaction with corruption is causing the existing problem to expand even further. For this reason,

at the meeting of the National Council for Combating Corruption held on March 5, 2025, the Head of State issued an instruction to create a strong legal framework for combating cybercorruption³⁶³.

In order to ensure the implementation of this instruction, a joint Resolution №04/4-03-01/17 dated March 25, 2025, was adopted by the Committee on Innovative Development and Information Technologies of the Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan and the Committee on Youth, Women, Culture and Sports of the Senate of the Oliy Majlis of the Republic of Uzbekistan. Pursuant to this Resolution, the task of studying the issue of the Republic of Uzbekistan's accession to international instruments on combating cybercrime was assigned.

At present, although the definition of the term “**cybercorruption**” is **not provided for in the legislation of any state, including the legislation of the Republic of Uzbekistan**, the necessary practices and legal frameworks in this area have been developed in foreign countries. In particular,

France's LOPMI (Loi d'Orientation et de Programmation du Ministère de l'Intérieur) Law dated January 24, 2023, established the framework for the activities of the Ministry of the Interior in the field of cybersecurity for the subsequent five-year period.

***For information:** Under this Law, the amount of liability for unlawful access to automated data processing systems was increased, liability of owners of information technology platforms was established, including the founder of Telegram, Pavel Durov, who was also investigated under this Law; issues related to insurance against cyberattacks were also sufficiently regulated. In particular, special provisions were established under which victims may file claims against the owners of platforms responsible for the violation within 72 hours from the time their rights and interests were violated.*

The **Atlantic Council** (www.atlanticcouncil.org), in its report entitled “*The Impact of Corruption on Cybersecurity: Rethinking National Strategies in the Global South*,” published in July 2024, addressed instances of corruption in the field of information and communication technologies, including cases involving the procurement of software that adversely affect cybersecurity.

A **webinar** on the topic “Studying the Interrelationship between Corruption and Cybercrime” was held by the **SANS Institute** on August 21, 2024.

The **European Union Agency for Law Enforcement Cooperation (Europol)**, in its report published in March 2025, warned that the **development of artificial intelligence** could intensify organized crime and thereby contribute to the development of cybercrime, including **cybercorruption**³⁶⁴.

Researchers from the United States and Western countries, including R. Peacock, C. Binns, S. Likhova, T. Lisko, O. Kosilova, O. Kirichenko, A. Shamara, S. Bortnik, T. Kuznetsova, V. Orlov, Yu. Bortnik, as well as national scholars S. Gulyamov, R. Raimberdiev, S. Eshkabilov, S. Hamroyev, R. Urinboyev, Sh.

³⁶³ <https://president.uz/uz/lists/view/7924>.

³⁶⁴ <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>.

Eraliyev and other scholars, have studied general information related to cybercorruption.

Cybercorruption has the following essential characteristics, in particular:

- 1) this act is committed in cyberspace or in a mixed form using cyberspace, as a cybersecurity incident;
- 2) cyber-technical means are used for the occurrence of a cybersecurity incident;
- 3) cyber-technical means may include a program, software, hardware-software means, software-hardware means, software product, telecommunications network, including the Internet, artificial intelligence, telecommunications infrastructure (telecommunications means), software, information system and resource, including a website, web application, messenger, various technical means and other means created through other information technologies, including artificial intelligence technologies;
- 4) cybercorruption may be committed in a narrower form than “corruption” in a broader sense, in the form of “digital corruption,” or in a mixed form;
- 5) specific liability for cybercorruption must be established in the legislation of the respective countries.

According to their view, the following forms and methods of cybercorruption exist, in particular:

1) electronic (digital) receipt and giving of bribes or mediation:

receiving, giving or mediating bribes through electronic (digital) payments or cryptocurrency, including other anonymous cryptocurrency;

electronic gift cards – giving bribes through gift cards instead of ordinary bank transfers, for example, providing cards with discounts for purchases;

obtaining discounts through lotteries, games based on risk or gambling, or cashback cards, online rewards, gifts, sending monetary amounts to a cashback card, and providing benefits;

obtaining benefits through the organization of electronic document circulation;

2) illegal use of information resources:

illegal access, with or without authorization, to personal databases of civil servants or representatives of the private sector contained in information systems and personal data databases;

illegal sale of databases;

altering personal data, including a person’s credit history, tax information or identification data;

disseminating false information on behalf of a state body or its official through a fake website;

conducting campaigns against civil servants or business competitors through social networks;

influencing state decisions through digital propaganda and fake voting systems;

carrying out illegal actions on behalf of officials or well-known persons through digital propaganda and fake voting systems;

3) corruption in public procurement:

illegally awarding a win through an information system to certain companies by means of corrupt schemes in public procurement, auction, tender and competitive selection processes;

influencing users by providing false information for procurement or entering false information into the system;

illegally assisting certain companies through an information system by means of corrupt schemes in public procurement, auction, tender and competitive selection processes, obstructing users during the procurement process, partially shutting down information systems, suspending some of their functions, giving illegal instructions to the system, and creating conditions or opportunities to prevent the procurement from being carried out properly;

failing to align the information system with the criteria established for public procurement, auction, tender and competitive selection processes;

carrying out cyberattacks against information systems designated for public procurement, auction, tender and competitive selection processes, or creating conditions for such an attack to be carried out;

entering the system of ministries and agencies or implementing public-private partnership for the purpose of providing advantages for the direct development of information systems;

obtaining the status of a sole operator or integrator for the preferential development of information systems;

modifying software code in order to predetermine procurement winners;

manipulation through fake participants (bots);

introducing fake companies into procurement processes and eliminating genuine and fair competition;

discrediting a competitor;

altering digital data and documents relating to users in procurement processes and obstructing their access to the system sufficiently;

altering digital documents relating to the conduct and process of procurement;

selecting another winner by making changes to or falsifying digital documents concerning the results of procurement;

entering into the system data fully corresponding to the capabilities of a pre-agreed company in order to ensure its direct victory;

4) implementation of cyberextortion, cybershamtage and other cyberthreats

stealing data in the public and private sectors through cybertheft and cyberespionage and carrying out cyberextortion, cybershamtage and other cyberthreats;

altering, deleting and concealing information in an information system for the purpose of hiding digital traces of corruption schemes;

“*ransomware*” attacks (Ransomware Attacks) – encrypting government agencies’ or business systems, restricting access to them, and unlocking them in exchange for a ransom;

phishing and fake messages – obtaining confidential information by deceiving government officials or company employees;

extortion through insiders, that is, carrying out extortion by disclosing information of persons working in a company or government agency;

establishing illegal exchange of information by employees working in government or private organizations;

providing procurement-related information in advance;

corporate espionage, that is, disclosing company information for use by competitors;

sending information through software companies, that is, obtaining government or private data through fake IT companies;

obtaining illegal funds by entering into contractual relations for the purpose of preventing certain information from being disclosed to the general public, while in practice not providing the service;

initiating unjustified inspections;

5) legalization of criminal proceeds and carrying out illegal operations through cryptocurrency:

laundering illegal funds using cryptocurrencies;

carrying out illegal financial operations that are difficult to detect through payment systems;

illegal use of blockchain technologies;

mixing funds in order to limit the possibility of tracing cryptocurrency;

money laundering through NFTs (non-fungible tokens), that is, legalizing illegal funds by purchasing books, scientific works, samples of intellectual property, copyright and related rights, works of art or digital property advertised, displayed or sold in information systems, on websites and in electronic payment systems or electronic wallets;

crypto-offshores – transferring illegal funds by opening crypto-companies in different countries;

6) Falsification of digital identification:

creating personal data of fictitious persons in the information systems or resources of organizations in the public or private sector;

illegal use of identification and electronic digital signature means;

illegal alteration of personal data;

altering, obtaining control over and illegally using data in authentication, authorization, FACE-ID and other biometric identification systems;

illegal exchange of information among competitors or state agencies;

breaching bioidentification or digital passport (ID-card) systems;

preparing fake documents through Deepfake, that is, altering personal data using combined face, voice or video technologies;

forging electronic signatures;

establishing opportunities for illegal use of public services by creating multiple personal profiles.

However, the current Criminal Code does not provide sufficient criminal liability for this.

***For information:** in the field of corruption alone, 5,716 crimes were committed in 2024, however, for the purpose of preventing them, no **preventive measures were taken at all** regarding persons who were subsequently held liable, in terms of preventing them from attempting to commit corrupt crimes before committing such acts; as a result, **6,898 persons** were held criminally liable and caused damage to state interests in the amount of **12.4 trillion soums**, while only **4.2 trillion soums** of monetary funds were recovered, and the most important issues affecting people remained unresolved.*

At the same time, due to the presence of corruption factors and insufficient transparency in the areas of public procurement, healthcare, education, social protection, judicial and legal affairs, and public services, the number and proportion of cybercorruption acts related to electronic payments, information systems and websites are also increasing in practice.

The current legal framework related to cybercorruption has been formed in two ways, namely:

1) on combating corruption:

24 Laws, **60** Presidential Decrees, **72** Presidential resolutions, **138** resolutions of the Cabinet of Ministers, **30** departmental normative legal acts, **324 legislative acts in total.**

2) on combating cybercrime:

12 Laws, **20** Presidential Decrees, **29** Presidential resolutions, **40** resolutions of the Cabinet of Ministers, **12** departmental normative legal acts, **113 legislative acts in total.**

The relationship that currently unites them is administrative and criminal legislation.

Currently, there is no international instrument that directly unites all relations concerning cybercorruption; however, there are numerous international instruments specializing in corruption or cybercrime, or regulating similar or mutually related relations, in particular:

1. List of the most important international instruments on combating corruption:

1) United Nations Convention against Corruption³⁶⁵;

For information:** this instrument applies to the prevention of international corruption, investigation and criminal prosecution for corruption, as well as the suspension (freezing), seizure, confiscation and return of proceeds recognized as having been obtained through criminal means in accordance with this Convention, and **Uzbekistan is a party to this Convention.

2) United Nations Convention against Transnational Organized Crime³⁶⁶;

***For information:** the Republic of Uzbekistan ratified this Convention in 2004. The Convention establishes the necessary provisions in **Articles 8–9** concerning corruption-related*

³⁶⁵ <https://lex.uz/docs/1461329>.

³⁶⁶ <https://lex.uz/docs/1304112>.

crimes, including **extortion** or **corruption-related crimes** involving the acceptance by a public official personally or through intermediaries, as well as measures to combat them.

At the same time, while **Part 2, Paragraph “c” of Article 210 of the Criminal Code of the Republic of Uzbekistan, in its Uzbek-language version**, provides for “receiving a bribe through extortion,” in the **Russian-language version** it provides for “receiving a bribe through extortion.” In foreign countries³⁶⁷, in particular, in **Article 290, Part 5, Paragraph “b” of the Criminal Code of the Russian Federation**, criminal liability is provided not for “receiving a bribe through extortion,” but for “receiving a bribe through extortion”³⁶⁸.

Likewise, Paragraph 18 of Resolution № 24 of the **Plenum of the Supreme Court of the Russian Federation** “On judicial practice in cases of bribery and other corruption-related crimes” dated 9 July 2013 states that receiving a bribe (Article 290, Part 5, Paragraph “b” of the Criminal Code) or the subject of commercial bribery (Article 204, Part 7, Paragraph “b” of the Criminal Code) may be associated with the threat of obtaining illegal remuneration, committing actions (inaction) that may harm the lawful interests of a person, or deliberately creating conditions conducive to a corrupt situation and creating opportunities for corruption to arise; **the situation of demanding a bribe, that is, the situation of extortion in addition to extortion, is also indicated as being related to extortion**³⁶⁹.

M. Rustamboyev, in his commentaries on the Criminal Code of the Republic of Uzbekistan, with regard to **Article 210, Part 2, Paragraph “c”**, also noted **that the crime of receiving a bribe through extortion is committed through extortion**³⁷⁰.

3) United Nations International Code of Conduct for Public Officials³⁷¹;

For information: this document establishes ethical rules, standards and norms of conduct for UN public officials. It is based on the principles of integrity and impartiality, independence and objectivity, responsibility and accountability, professional ethics and rules of conduct, avoidance of conflicts of interest, confidentiality and information security, international cooperation and cultural respect.

According to it, public officials are required to comply with the following:

- not to allow personal interests to interfere with their professional activities;
- to take into consideration only the public interest when making decisions;
- to take a firm stance against bribery and corruption;
- not to come under the influence of external influences or national interests;
- to be objective and impartial in any matter;
- to faithfully serve the goals and objectives of international organizations;
- to ensure accountability for any actions and decisions;
- to observe professionalism, fairness and transparency in their activities;
- to treat other colleagues, supervisors and clients with respect when performing their official duties;
- to avoid conflicts between personal and professional interests;
- not to accept gifts or special privileges from external organizations;
- not to unlawfully disclose confidential information;
- to protect information belonging to states and international organizations;
- persons working in international organizations shall respect different nations, cultures and beliefs;
- to oppose any discrimination or unfair treatment.

4) Resolutions of the United Nations Congresses on Crime Prevention and Criminal Justice³⁷²;

³⁶⁷ <https://lex.uz/docs/111453?otherlang=1>.

³⁶⁸ https://www.consultant.ru/document/cons_doc_LAW_10699/6411e005f539b666d6f360f202cb7b1c23fe27c3/.

³⁶⁹ https://www.consultant.ru/document/cons_doc_LAW_149092/.

³⁷⁰ https://drive.google.com/file/d/1ctKcLoMP8UaC5BgGscM_S-AI0i8fjYlh/view.

³⁷¹ <https://icsc.un.org/Resources/General/Publications/standardsE.pdf>.

³⁷² <https://www.un.org/ru/library/page/databases>.

For information: the first Congress session was held in 1955, and 14 sessions have been held over the ensuing period. In 2018, the Congress discussed **cybercrime** and **terrorism**, as well as effective methods of combating them, and the resolutions on this issue were aimed at strengthening the system for **identifying offenders** and imposing lawful penalties on them. Uzbekistan has participated in the sessions as a member state since 1992.

5) Inter-American Convention against Corruption of the Organization of American States³⁷³;

For information: adopted in Caracas (Venezuela) on 29 March 1996 and entered into force on 6 March 1997. This Convention is considered one of the first international instruments aimed at strengthening cooperation in combating corruption among the member states of the Organization of American States, combating the illicit enrichment of public officials, combating the receipt and giving of bribes by public officials, and strengthening cooperation among states in providing mutual legal assistance and carrying out extradition requests. Uzbekistan is not a party to this instrument.

6) African Union Convention on Preventing and Combating Corruption and Related Offences³⁷⁴;

For information: all member states of the Convention are obliged to implement norms and measures related to combating corruption, and this covers combating all forms of corruption – corrupt activities involving officials, individuals and legal entities. This Convention establishes cooperation in cross-border relations to combat economic manipulation and financial crimes. Uzbekistan is not a party to this instrument.

7) Arab Convention against Corruption³⁷⁵;

For information: this is a legal instrument adopted in 2010 for the purpose of combating corruption among the states of the Middle East and North Africa. It provides for joint efforts by the states that are members of the Arab League to combat corruption, cooperation, and the development of anti-corruption strategies in each state. The Convention is aimed at conducting public education and awareness-raising activities to prevent corruption and explaining the importance of preventing corruption. Member states are obliged to take strict measures against all forms of corruption. Uzbekistan is not a party to this Convention.

8) Mecca Al-Mukarramah Convention on Cooperation in Enforcing Anti-Corruption Laws among the Member States of the Organization of Islamic Cooperation³⁷⁶;

For information: The Mecca Al-Mukarramah Convention is an international treaty established with the aim of strengthening cooperation in combating corruption among the member states of the Organization of Islamic Cooperation (OIC). This Convention was adopted at the first ministerial meeting of the heads of anti-corruption law enforcement agencies of the OIC member states, held in Jeddah, Saudi Arabia, on 20–21 December 2022. At the second ministerial meeting held in Doha, Qatar, on 27 November 2024, 21 OIC member states — the Kingdom of Saudi Arabia, Qatar, the Hashemite Kingdom of Jordan, the Islamic Republic of Pakistan, the Kingdom of Bahrain, the People's Republic of Bangladesh, the Republic of the Sudan, the Republic of Sierra Leone, the Federal Republic of Somalia, the Republic of Iraq, the Sultanate of Oman, the Union of the Comoros, the State of Kuwait, the Lebanese Republic, the State of Libya, Malaysia, the Republic of Niger, the Republic of Yemen, the Islamic Republic of Mauritania, Guinea and the Republic of Chad — signed this Convention. The main purpose of the Convention is to establish a legal framework for cooperation among the anti-corruption law enforcement agencies of OIC member states. This includes, in particular, improving communication mechanisms, exchanging

³⁷³ https://www.oas.org/en/sla/dil/inter-american-treaties_B-58_against_Corruption.asp.

³⁷⁴ <https://au.int/en/treaties/african-union-convention-preventing-and-combating-corruption>.

³⁷⁵ <https://star.worldbank.org/sites/star/files/Arab-Convention-Against-Corruption.pdf>.

³⁷⁶ <https://www.oic-oci.org/docdown/?docID=9774&refID=4268>.

information, expediting investigations, and collecting evidence to ensure criminal justice. At the second ministerial meeting held in Doha in November 2024, a decision was also made to establish an open-ended group of government experts to consider the mechanisms and methods for implementing the Convention. This group will be responsible for monitoring the implementation of the Convention and developing technical and legislative guidelines. The Convention is of significant importance in strengthening cooperation among OIC member states in combating corruption and coordinating efforts in this area.

9) OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions³⁷⁷;

For information: it is the first international legal instrument aimed at criminalizing the bribery of foreign public officials in the commercial sector, with **44 states as parties**. *The Republic of Uzbekistan is not a party to this instrument. According to the requirements of this instrument, bribery of foreign public officials must be recognized as a criminal offense; penalties related to bribery must be effective, proportionate and deterrent in nature, and must be implemented through the confiscation of proceeds obtained from bribery or their recovery in full in favor of the state in the form of a fine.*

10) OECD Recommendations and Guidelines on Combating Corruption³⁷⁸;

For information: the following are included in the recommendations on combating corruption, in particular:

political will and leadership: heads of state should demonstrate strong political will against corruption and support reforms in this area;

strengthening the legal framework: improving anti-corruption legislation, including establishing criminal liability for giving and receiving bribes, regulating conflicts of interest and ensuring transparency;

institutional mechanisms: establishing special anti-corruption bodies and ensuring their independence;

openness and transparency: ensuring openness in public administration, freely providing information to the public and increasing transparency in public procurement;

ensuring public participation: encouraging the participation of civil society, the mass media and the private sector in combating corruption;

The following are included in the guidelines:

preventive measures: assessing risks for the prevention of corruption, ensuring compliance by employees with ethical standards and managing conflicts of interest;

education and awareness: conducting anti-corruption awareness-raising activities among public servants and the public, and organizing training courses on ethical rules and standards;

monitoring and evaluation: regularly evaluating and monitoring the effectiveness of anti-corruption measures and reviewing policies based on the results;

international cooperation: strengthening cooperation with international organizations and other states in combating corruption, exchanging experience and jointly implementing measures;

11) Council of Europe Criminal Law Convention on Corruption³⁷⁹;

For information: the Council of Europe Criminal Law Convention on Corruption of 27 January 1999 was adopted in Strasbourg for the purpose of identifying corruption-related crimes and establishing criminal liability for them, strengthening legal cooperation between states, and establishing common standards and norms in combating corruption, however, Uzbekistan has not acceded to this Convention. This Convention provides for the recognition and punishment of

³⁷⁷ <https://www.oecd.org/en/topics/fighting-foreign-bribery.html>.

³⁷⁸ <https://legalinstruments.oecd.org/public/doc/205/205.en.pdf>.

³⁷⁹ <https://rm.coe.int/168007f3f5>.

bribery of public officials of each state and foreign states as a criminal offense, and for the member states to cooperate with each other³⁸⁰.

12) Council of Europe Civil Law Convention on Corruption³⁸¹;

For information: this Convention was adopted on 4 November 1999 and provides for a mechanism for compensation for material and moral damage caused to persons affected by corruption. However, Uzbekistan is not a party to this Convention. According to the requirements of Article 3 of the Convention, it is specified that the damage consists of material and moral damage and lost profit. According to Article 4 of the Convention, this damage arises only when the responsible person has committed or authorized the corruption, or has failed to take the necessary measures to prevent corruption, the affected person has suffered damage, and there is a causal relationship between the corruption and the damage. According to Article 5 of the Convention, it is also provided that persons who have suffered damage from corruption may claim compensation from the state. Furthermore, the limitation period for claims concerning corruption-related cases is established as 4 years, and there are clear restrictive provisions stating that cases concerning corruption that has occurred more than 10 years previously shall not be initiated.

13) Documents of the Council of Europe's Group of States against Corruption (GRECO)³⁸²;

For information: this group was established in 1999 with the aim of ensuring compliance with international standards by assessing the activities of member states in the field of combating corruption and providing them with recommendations. GRECO membership includes 47 member states of the Council of Europe, Belarus and the United States, a total of 49 states. GRECO's activities are aimed at strengthening the capacity of member states to combat corruption by monitoring compliance with the standards of the Council of Europe, and it provides a platform for exchanging best practices in the prevention and detection of corruption. GRECO country reports are published with the consent of the respective state.

14) Council of Europe Convention on "Laundering, Search, Seizure and Confiscation of the Proceeds from Crime" (Strasbourg)³⁸³;

For information: this Convention was adopted on 8 November 1990 as ETS № 141 and is aimed at strengthening international cooperation in combating the legalization of proceeds from criminal activity, their tracing, seizure and confiscation, and Uzbekistan is not a party to it.

15) EU Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering (10 June 1991)³⁸⁴;

For information: this Directive requires financial institutions and other organizations to take the necessary measures to prevent money laundering and terrorist financing, and its fifth Directive provides for the inclusion of cryptocurrency operators and electronic money services as part of combating money laundering and terrorist financing, accordingly, it establishes Know Your Customer (KYC) requirements for cryptocurrency exchange platforms and electronic money services, furthermore, the financing of terrorism and the procedure for the mutual exchange of financial information by member states are regulated, however, the Republic of Uzbekistan is not a member of it.

16) Paris Declaration against Money Laundering (Final Declaration of the European Union Parliamentary Conference against Money Laundering, 8 February 2002)³⁸⁵;

³⁸⁰ <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=173>.

³⁸¹ <https://rm.coe.int/168007f3f6/>

³⁸² <https://www.coe.int/en/web/greco/publications>.

³⁸³ <https://rm.coe.int/168007bd23>.

³⁸⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024L1640>.

³⁸⁵ <https://docs.cntd.ru/document/901934984>.

***For information:** this document is aimed at increasing the transparency of financial transactions and preventing confidential accounts and activities in offshore zones, according to which, all financial transactions, including bank transactions, transfers of funds between companies and purchase and sale transactions, accounting records must be complete and accurate, access to this information by authorized state bodies must be freely ensured, and strong mechanisms must be established to prevent confidential accounts in offshore zones and monitor their operation, however, the Republic of Uzbekistan has not acceded to this document.*

17) Twenty Guiding Principles for the Fight against Corruption of the Committee of Ministers of the Council of Europe³⁸⁶;

***For information:** these principles were adopted on 6 November 1997, among which the principles of political will, the rule of law, encouragement of public participation, personal responsibility, personal independence and an effective judicial system, financial control and international cooperation are considered important principles, however, Uzbekistan has not acceded to these principles.*

18) Model Code of Conduct for Public Officials of the Committee of Ministers of the Council of Europe³⁸⁷;

For information:** this Code was adopted on 11 May 2000 and establishes the ethical norms and conduct of public officials and is aimed at regulating the professional and personal conduct of public officials and increasing their role in combating corruption, however, **the Republic of Uzbekistan is not a party to it.

19) Common Rules against Corruption in the Funding of Political Parties and Electoral Campaigns of the Committee of Ministers of the Council of Europe³⁸⁸;

***For information:** this Convention was adopted on 8 April 2003 and is aimed at reducing and preventing corruption in the field of political financing, however, the Republic of Uzbekistan has not acceded to it either.*

20) Anti-Corruption Documents Adopted within the Frameworks of the Economic Cooperation Organization (ECO) and the Shanghai Cooperation Organization (SCO)³⁸⁹;

***For information:** The Economic Cooperation Organization (ECO) does not have a specific document addressing cyber-corruption; however, it has adopted a number of documents aimed at combating corruption. As for the Shanghai Cooperation Organization (SCO), two agreements on cybersecurity were signed in 2017 and 2018, respectively. Pursuant to these agreements, mechanisms for monitoring and ensuring security against cyber threats have been developed among SCO member states. These initiatives promote information exchange and establish roadmaps for ensuring cybersecurity in order to prevent cyber-corruption and cyberattacks. In addition, mechanisms for the exchange of experts and training among member states have also been established. Furthermore, by Decision № 16 of the Council of Heads of State of the Shanghai Cooperation Organization, dated 4 July 2024, “On the Plan for Cooperation among the Member States of the Shanghai Cooperation Organization on Issues of Ensuring International Information Security,” the Plan for Cooperation among the Member States on Issues of Ensuring International Information Security was approved³⁹⁰. The Republic of Uzbekistan, as a member of the SCO, cooperates with other member states in this area.*

³⁸⁶ <https://rm.coe.int/0900001680910ecf>.

³⁸⁷ <https://rm.coe.int/16805e2e52>.

³⁸⁸ <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=198>.

³⁸⁹ <https://sectsco.org/>.

³⁹⁰ <https://rus.sectscsco.org/20240704/1600099.html>.

21) Agreement on Cooperation among the States Parties to the Commonwealth of Independent States in Combating Crime (Moscow, 25 November 1998)³⁹¹;

For information: This Agreement is aimed at strengthening cooperation among the CIS member states in the field of combating crime. Pursuant to Article 2 of the Agreement, the member states are required to cooperate with one another in the detection and investigation of crimes. Within this framework, the participating states undertake to provide close practical assistance in preventing crimes, conducting operational-search activities, locating and apprehending offenders, and bringing them to justice.

22) Agreement on the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (Moscow, 16 June 2011)

For information: This Agreement was signed in Moscow on 16 June 2011 and aims to strengthen cooperation in the Eurasian region in combating the legalization of proceeds of crime and the financing of terrorism. The Republic of Uzbekistan ratified this Agreement on 14 December 2011. The purpose of the Agreement is to develop and implement effective measures to combat money laundering and the financing of terrorism. The Group primarily focuses on financial crimes, while issues of cyber-corruption are not directly addressed.

2. List of the Most Important International Instruments Specifically Addressing Cybercrime:

1) United Nations Convention against Cybercrime;

For information: This Convention was adopted by Resolution № 79/243 of the United Nations General Assembly on 24 December 2004. At present, 38 states are parties to the Convention; however, the Republic of Uzbekistan is not a party to it. This international instrument was adopted to strengthen international cooperation in combating certain crimes committed through the use of information and communication systems and in the exchange of electronic evidence relating to serious crimes. The Convention classifies the following acts as cybercrimes:

- illegal access to an information and communication system;
- illegal interception of data transmitted to, from or within an information and communication system;
- damaging, deleting, altering or blocking electronic data;
- causing serious hindrance to the functioning of an information and communication system through the input, transmission, damaging, deletion, alteration or suppression of data, by intentionally and without right, by access to the system;
- the illegal use of devices connected to an information and communication system or parts thereof;
- forgery committed through the use of an information and communication system;
- theft or fraud committed through the use of an information and communication system;
- making available through the Internet of materials depicting sexual abuse or sexual exploitation of children;
- soliciting or grooming a child for the purpose of committing a sexual offence against the child;
- non-consensual distribution of intimate images;
- laundering of proceeds derived from crime.

Furthermore, the Convention regulates matters relating to the jurisdiction over cybercrimes, as well as the obtaining and collection of electronic (digital) evidence³⁹².

2) Resolutions of the United Nations General Assembly:

³⁹¹ <https://lex.uz/uz/docs/1801724>.

³⁹² <https://documents.un.org/doc/undoc/gen/n24/426/76/pdf/n2442676.pdf>.

For information: Within the framework of the United Nations, the following resolutions of the United Nations General Assembly have been adopted concerning combating cybercrime, information and communication technologies, and cybersecurity, including:

Resolution № 68/167 of 2013 on international cooperation aimed at strengthening cybersecurity and combating cybercrime³⁹³;

Resolution № 68/198 of 20 December 2013 on the development of information and communication technologies³⁹⁴;

Resolution № 69/204 of 19 December 2014 on the development of information and communication technologies³⁹⁵;

Resolution № 70/237 of 2015 on international cooperation in the field of cybersecurity and information security³⁹⁶;

Resolution № 70/184 of 22 December 2015 on the development of information and communication technologies³⁹⁷;

Resolution № 71/212 of 21 December 2016 on the development of information and communication technologies³⁹⁸;

Resolution № 70/200 of 20 December 2017 on the sustainable development of information and communication technologies³⁹⁹;

Resolution № 72/186 of 19 December 2017 on global developments in the field of information and communication technologies⁴⁰⁰;

Resolution № 70/218 of 20 December 2018 on the sustainable development of information and communication technologies⁴⁰¹.

3) Council of Europe Convention on Cybercrime⁴⁰²;

For information: This document, adopted on 23 November 2001, is one of the most important international instruments addressing cybercrime. It has been ratified by more than 65 states and was developed with the aim of harmonizing national legislation on cybercrime, criminalizing offences related to cybercrime, strengthening cooperation among states in combating cybercrime, and protecting information systems and personal data. The Convention recognizes the following acts as criminal offences:

illegal access to computer systems (hacking);

illegal collection and use of data;

interference with information systems (malware, DDoS attacks);

computer-related fraud (online fraud, phishing);

distribution of pornography and illegal content (cyber grooming, child pornography);

infringement of intellectual property rights (piracy, illegal file sharing).

The Convention establishes international standards for the expedited preservation and regulation of data, the collection and preservation of electronic evidence, and the prompt response to cyberattacks for the purposes of investigating cybercrime and gathering evidence. Accordingly, it establishes specific rules concerning the provision of electronic data between states, cooperation among law enforcement agencies, and extradition procedures. In addition, the Convention has been supplemented by two additional protocols: the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, adopted on 28 January 2003, and the Second Additional Protocol on enhanced cooperation and disclosure of electronic evidence, adopted on 17 November 2021. These protocols were adopted

³⁹³ <https://www.un.org/en/ga/68/resolutions.shtml>.

³⁹⁴ https://www.itu.int/en/ITU-D/Regional-Presence/UN/Documents/GA_Resolutions_ICTs/ares68d198_en.pdf.

³⁹⁵ https://www.itu.int/en/ITU-D/Regional-Presence/UN/Documents/GA_Resolutions_ICTs/ares69d204_en.pdf.

³⁹⁶ <https://www.un.org/en/ga/70/resolutions.shtml>.

³⁹⁷ https://www.itu.int/en/ITU-D/Regional-Presence/UN/Documents/GA_Resolutions_ICTs/ares70d184_en.pdf.

³⁹⁸ https://www.itu.int/en/ITU-D/Regional-Presence/UN/Documents/GA_Resolutions_ICTs/ares71d212_en.pdf.

³⁹⁹ https://www.itu.int/en/ITU-D/Regional-Presence/UN/Documents/GA_Resolutions_ICTs/ares72d200_en.pdf.

⁴⁰⁰ file:///C:/Users/%D0%B37/Downloads/A_RES_72_186-RU.pdf.

⁴⁰¹ https://www.itu.int/en/ITU-D/Regional-Presence/UN/Documents/GA_Resolutions_ICTs/ares73d218_en.pdf.

⁴⁰² <https://www.coe.int/ru/web/impact-convention-human-rights/convention-on-cybercrime>.

to combat the dissemination of terrorist-related information and the promotion of terrorism through the Internet, as well as to strengthen cooperation among states in combating cybercrime at both the national and international levels. They establish specific provisions concerning the criminalization of the dissemination of information related to terrorist activities, monitoring the dissemination via the Internet of information that facilitates terrorism, strengthening information exchange among states and facilitating the expedited exchange of electronic evidence, enhancing cooperation between the private sector and public authorities, and strengthening international cooperation among investigative and law enforcement authorities⁴⁰³. **The Republic of Uzbekistan is not a party to this Convention.** The most significant concern associated with the Convention is that it may require Uzbekistan to **exchange information with other states**. This could potentially affect national security, personal data, or information constituting state secrets.

4) European Union Directive on Security of Network and Information Systems (NIS Directive, 2016)⁴⁰⁴;

For information: The Directive was adopted to strengthen measures against cyber threats and enhance the security of information systems in the Member States of the European Union. It requires the establishment of Computer Security Incident Response Teams (CSIRTs) in the EU Member States to facilitate the exchange of cybersecurity-related information and cooperation. The European Union Agency for Cybersecurity (ENISA) strengthens international standards and cooperation in the field of information security among Member States. Uzbekistan is not a member of the European Union and is therefore not a party to this instrument.

5) Agreement of the Shanghai Cooperation Organization (SCO) on Information Security⁴⁰⁵.

For information: The Agreement was adopted in 2009 and is aimed at strengthening cooperation among the SCO member states in combating cybercrime and ensuring information security.

The document contains specific provisions concerning ensuring information security, establishing national and international cybersecurity standards, strengthening cooperation in the field of information security, combating cyber threats, taking measures against such threats as viruses, hacking, and the activities of Internet hackers, protecting the information systems of SCO member states, and information exchange and cooperation, including the exchange of relevant information on information security among SCO member states, the protection of electronic data, and strengthening liability for hackers and offences threatening cybersecurity.

The Agreement provides for strengthening international cooperation in the field of information security, applying legal measures against offences involving electronic security, and establishing procedures for mutual assistance among SCO member states in combating terrorism, extremism, and threats to cybersecurity. The states that have joined the Agreement include China, Russia, India, Kazakhstan, Kyrgyzstan, Uzbekistan, Tajikistan, Pakistan, and Belarus. The Agreement also approves the principal concepts in the field of international information security, as well as lists of the main types of threats to international information security, their sources, and their characteristics.

According to the Agreement, the following are recognized as threats to international information security:

- the development and use of information weapons, and the preparation for and conduct of information warfare;
- information terrorism;
- information-related crime;
- the use of a dominant position in the information space to harm the interests and security of other countries;

⁴⁰³ <https://www.coe.int/en/web/cybercrime/home>.

⁴⁰⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016L1148>.

⁴⁰⁵ <https://rus.sectsc.org/documents/?offset=420>.

the dissemination of information harmful to the socio-political and socio-economic systems and the moral, ethical, and cultural environment of other states;
threats to the secure and stable functioning of global and national information infrastructures of natural and/or technological origin.

6) International Standards and Technical Instruments in the Field of Cybersecurity

For information: These instruments include:

ISO/IEC 27001:2013 – Information security management systems (ISMS) – Requirements, developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which constitutes an international standard for information security management systems (ISMS)⁴⁰⁶;

ITU-T X.1205 – Security Framework for Information and Communication Technologies (ICT), developed by the International Telecommunication Union (ITU), the United Nations specialized agency for information and communication technologies, provides a security framework for information and communication technologies (ICT) and establishes cybersecurity guidelines for ICT⁴⁰⁷;

The Cybersecurity Framework, developed by the National Institute of Standards and Technology (NIST), is a standard for managing cybersecurity⁴⁰⁸;

ISO 22301:2019 – Security and resilience — Business continuity management systems — Requirements, developed by ISO and IEC, is a standard for business continuity management systems that helps enhance security and minimize risks⁴⁰⁹;

ISO/IEC 27032:2023 – Cybersecurity — Guidelines for Internet security, developed by ISO and IEC, provides guidelines for ensuring cybersecurity, establishes international standards for cybersecurity, and supports their implementation⁴¹⁰;

The General Data Protection Regulation (GDPR), developed by the European Union (EU), is a regulation designed to protect personal data⁴¹¹;

Control Objectives for Information and Related Technologies (COBIT), developed by ISACA, is an international framework for information technology and governance that helps organizations manage cybersecurity and make informed decisions⁴¹².

The general requirements contained in these international instruments on combating cyber-corruption are as follows:

- defining clear boundaries of corruption-related relations and identifying the range of relevant subjects;
- establishing a clear list of cybercrimes;
- incorporating into national legislation provisions aimed at combating the identified cybercrimes;
- designating a dedicated body responsible for combating cybercrime, including cyber-corruption;
- designating a body responsible for international cooperation in combating cybercrime at the international level;
- establishing the exchange of documents relating to international cooperation;

⁴⁰⁶ <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>.

⁴⁰⁷ [https://store.accuristech.com/standards/itu-t-x-](https://store.accuristech.com/standards/itu-t-x-1205?product_id=2874775&srsId=AfmBOooDhzvjNp457MgaYJ9Djr4G7oOmb_gVFAPeCmB2o9ji_KjSUH5F)

[1205?product_id=2874775&srsId=AfmBOooDhzvjNp457MgaYJ9Djr4G7oOmb_gVFAPeCmB2o9ji_KjSUH5F](https://store.accuristech.com/standards/itu-t-x-1205?product_id=2874775&srsId=AfmBOooDhzvjNp457MgaYJ9Djr4G7oOmb_gVFAPeCmB2o9ji_KjSUH5F).

⁴⁰⁸ <https://www.nist.gov/cyberframework>.

⁴⁰⁹ <https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en>.

⁴¹⁰ <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27032:ed-2:v1:en>.

⁴¹¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.

⁴¹² <https://www.isaca.org/resources/cobit/cobit-5>.

- establishing a unified information system and ensuring access to information through such a system;
- establishing jurisdiction over cybercrime, limitation periods, and general rules governing extradition;
- submission of reports;
- compliance with the requirements of international regulatory and technical instruments.

The following are the advantages of acceding to the international instruments on cyber-corruption envisaged in the information and analytical material:

1) Cybersecurity will be strengthened and opportunities will be created to align with international standards.

For information: This would mean that:

- *cybercrime is transnational in nature, and accession to (ratification of) the international instruments envisaged in the information and analytical material would provide substantial assistance in detecting and exposing cyberattacks carried out against the Republic of Uzbekistan from the territory of states that are parties to these instruments, or against a state party to the relevant international instrument from the territory of the Republic of Uzbekistan, as well as in apprehending and extraditing cybercriminals;*
- *common concepts and terminology would be established at the international level;*
- *the harmonization or approximation of criminal and criminal-procedural legislation would contribute to the development of common legal and technological practices.*

2) It will help prevent cyber-offences and combat corruption:

For information: This would mean that:

- *measures aimed at preventing cyber-offences would be established at the international level;*
- *a systematic and comprehensive framework for combating corruption would be created.*

3) A unified approach to cybersecurity and international cooperation would be established at the international level:

For information: This would mean that:

- *it would contribute to the development of information and communication technologies;*
- *it would create unified legal and technological solutions for ensuring cybersecurity based on consistency and logical sequencing and taking into account the specific characteristics of information and communication technologies;*
- *it would enhance the international standing of Uzbekistan.*

The following are the disadvantages of acceding to the international instruments on cyber-corruption envisaged in the information and analytical material:

1) It may limit the independence and sovereignty of Uzbekistan;

For information: Continuous alignment of domestic legislation with international instruments and the obligation to submit regular reports may create a form of indirect dependence.

2) It may result in additional economic and human-resource costs:

For information: This would mean that:

- *after acceding to an international instrument, at least one dedicated body would need to operate on behalf of Uzbekistan in this area at the international level, which would entail additional expenditure from the state budget for the material and technical infrastructure, remuneration, and other forms of support for such a body;*

- even if a dedicated body were established, it would need to obtain the information necessary to ensure cybersecurity from other government agencies, which could result in time and human resources being diverted from other areas;
- additional time and financial resources would be required for personnel training and capacity building.

3) It may give rise to cultural and legal differences:

***For information:** Until a secure cyberspace based on unified legal and technological cybersecurity standards is established, each state, based on its own legislation, culture, and practices, may seek to influence other states by harmonizing international instruments with its own legislation and practices. This may create a highly difficult and complex process and affect the independence of the legislative, executive, and judicial branches of government.*

4) International monitoring and oversight in the field of cybersecurity may affect internal security:

***For information:** Alignment with international standards may result in external monitoring and oversight of Uzbekistan, which could potentially lead to negative influence by foreign states on the implementation of Uzbekistan's domestic policies.*

Among these instruments, the **United Nations Convention against Cybercrime** has been identified as being of particular importance due to its broad scope and coverage of relevant contemporary issues.

Accordingly, based on the proposal of the author, **A. Anorboev**, Uzbekistan has acceded to this Convention.

Based on the foregoing, it is proposed as follows:

1. To establish a special working group comprising representatives of the Prosecutor General's Office, the State Security Service, the Anti-Corruption Agency, the Ministry of Digital Technologies, the Ministry of Internal Affairs, the Ministry of Justice, the Ministry of Foreign Affairs, the National Agency of Perspective Projects, the Agency for Information and Mass Communications, the Central Bank, the Supreme Court, the Senate and Legislative Chamber of the Oliy Majlis, and the Institute of Legislation and Legal Policy, for the purpose of developing and submitting to the Presidential Administration a draft Resolution of the President of the Republic of Uzbekistan **“On Measures to Improve the Organizational and Criminal-Law Framework for Combating Cyber-Corruption”**, providing for:

- 1) designation of the body or bodies responsible for matters relating to combating cyber-corruption at the national and international levels;
- 2) assignment of tasks to the newly established Cybersecurity Agency of the Republic of Uzbekistan and other interested ministries and agencies concerning the issue of acceding to the following international instruments, as well as legal consolidation of the ongoing reforms through the adoption of a separate legislative instrument in connection with Uzbekistan's accession to the United Nations Convention against Cybercrime:
 - a) Council of Europe Criminal Law Convention on Corruption (1999);
 - b) Council of Europe Civil Law Convention on Corruption (1999);
 - d) Organization of American States Inter-American Convention Against Corruption (1996);
 - e) African Union Convention on Preventing and Combating Corruption (2003);
 - f) Arab Convention on Combating Corruption;

- g) Makkah Al-Mukarramah Convention;
- h) Budapest Convention (Council of Europe Convention on Cybercrime);
- i) international cybersecurity standards and technical instruments.

5. introduction into practice of an automated, real-time, national artificial intelligence-based “CCA” platform and approval of its Regulations;

6. connection of all information systems in the Republic to the “CCA” platform and establishment of a powerful, mutually protected and integrated system operating in real time and providing information on developments occurring within the Republic and at the international level;

7. designation of the owner and operator of the “CCA” platform;

8. alignment of the legislation of the Republic of Uzbekistan with the United Nations Convention against Cybercrime and other international instruments.

2. For the special working group:

To organize official or study visits to examine on-site the experience of the United States, the Republic of Korea, Japan, Viet Nam, China, Singapore, Estonia, Germany, France, the United Kingdom, Italy, Romania, Spain, Saudi Arabia, the United Arab Emirates, Qatar, Egypt, South Africa, Malaysia, and Indonesia in greater depth for the purpose of studying the measures proposed to be included in the Presidential Resolution.

It is considered advisable to instruct the special working group to submit the initial draft of the Resolution of the President of the Republic of Uzbekistan “**On Measures to Improve the Organizational and Criminal-Law Framework for Combating Cyber-Corruption**” to the Presidential Administration.

4.3-§. Improvement of the Mediation Institution

The institution of mediation is currently regulated by **53 normative legal acts**, including a separate dedicated Law. However, a number of problems remain with regard to the widespread application of this institution, in particular:

1) There is no clear list of disputes subject to mandatory mediation. As a result, this institution is not being widely applied in the Republic, since the parties do not have a clear understanding of the matters in respect of which they may seek the assistance of a mediator.

***For information:** The Law of the Republic of Uzbekistan “On Mediation” dated 3 July 2018, № LRU–482, provides that, unless otherwise stipulated by law, it applies to relations arising from civil-law matters, including disputes arising in connection with entrepreneurial activities, as well as individual labour disputes and disputes arising from family-law relations.⁴¹³ However, the specific social relations to which these provisions apply have not been clearly defined. This, in turn, is resulting in the limited application of this institution and preventing the development of a “uniform legal practice” in this area.*

2) The mediation institution has not been sufficiently digitalized;

***For information:** A Register of Professional Mediators is maintained pursuant to legislation by the Ministry of Justice of the Republic of Karakalpakstan and the justice departments of the regions and the city of Tashkent. The Register is published on their official websites, as well as on the official website of the Ministry of Justice of the Republic of Uzbekistan. However, it contains only information about mediators, while no mechanism has been established for providing information on their actual activities, and such activities have not been digitalized.*

Clearly defining in legislation the list of disputes subject to mandatory mediation and adequately establishing the mechanism for its implementation will contribute to the following:

- *establishing a clear list of disputes arising from civil-law relations, including disputes arising in connection with entrepreneurial activities, as well as individual labour disputes and disputes arising from family-law relations;*
- *creating opportunities for the wider application of this institution in administrative and criminal-law relations;*
- *resolving a number of existing problems concerning the pre-trial settlement of disputes between state bodies and organizations and other entities.*

The digitalization of the mediation institution, in turn, will contribute to the following:

1. In the field of investment and investment activities

Pursuant to the Law of the Republic of Uzbekistan “On Investments and Investment Activities” dated 25 December 2019, № LRU–598, social relations concerning the digitalization of the settlement of investment disputes through mediation will be established where a dispute involving foreign investment and arising in the course of investment activities carried out by a foreign investor within the territory of the Republic of Uzbekistan cannot be resolved through negotiations.

2. In the field of enforcement of judicial acts and acts of other bodies:

⁴¹³ Law of the Republic of Uzbekistan № LRU–482 dated 3 July 2018, “On Mediation” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

Pursuant to the Law of the Republic of Uzbekistan “On Enforcement of Judicial Acts and Acts of Other Bodies” dated 29 August 2001, № 258-II, the obligations of a state enforcement officer to suspend enforcement proceedings in accordance with the mediation procedure, as well as the mechanisms for its implementation and supervision⁴¹⁴, will be digitalized;

3. In the field of notarial services:

Pursuant to the Law of the Republic of Uzbekistan “On Notariat” dated 26 December 1996, № 343-I⁴¹⁵, the Rules for Notarial Record-Keeping in State Notarial Offices approved by Order № 308-mh of the Minister of Justice of the Republic of Uzbekistan dated 22 December 2010 (registration № 2170, 22 December 2010)⁴¹⁶, and the Instruction on the Procedure for Performing Notarial Acts by Notaries approved by Order № 2-mh of the Minister of Justice of the Republic of Uzbekistan dated 4 January 2019 (registration № 3113, 4 January 2019)⁴¹⁷, the rights of notaries to perform the functions of mediators, as well as documents relating to the conduct of mediation proceedings, will be digitalized.

4. In the field of monitoring limitation periods:

Pursuant to Article 156 of the Civil Code of the Republic of Uzbekistan, opportunities will be created to digitally monitor the conclusion of an agreement to conduct mediation proceedings and the suspension of the limitation period⁴¹⁸.

5. In the field of arbitration courts:

Pursuant to the Law of the Republic of Uzbekistan “On Arbitration Courts” dated October 16, 2006, № LRU–64, in arbitration proceedings, mediation procedures will be digitized, arbitration courts will be able to monitor the termination of arbitration proceedings due to the parties having concluded a mediation agreement, and the submission of unfounded claims to civil and economic courts will be prevented⁴¹⁹.

6. In the field of mediation:

Pursuant to Order № 53-mh of the Minister of Justice of the Republic of Uzbekistan dated March 2, 2012 “On Approval of the General Legal Classifier of Branches of Legislation of the Republic of Uzbekistan” (registration № 2333, March 2, 2012)⁴²⁰, the field of 17.07.00.00 Mediation will be digitized;

7. In the field of the sale of state shares:

⁴¹⁴ Law of the Republic of Uzbekistan “On Enforcement of Judicial Acts and Acts of Other Bodies” dated 29 August 2001, № 258-II // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴¹⁵ Law of the Republic of Uzbekistan “On Notariat” dated 26 December 1996, № 343-I // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴¹⁶ Rules for Notarial Record-Keeping in State Notarial Offices, approved by Order № 308-mh of the Minister of Justice of the Republic of Uzbekistan dated 22 December 2010 (registration № 2170, 22 December 2010) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴¹⁷ Instruction on the Procedure for Performing Notarial Acts by Notaries, approved by Order № 2-mh of the Minister of Justice of the Republic of Uzbekistan dated 4 January 2019 (registration № 3113, 4 January 2019) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴¹⁸ Civil Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴¹⁹ Law of the Republic of Uzbekistan № LRU–64 dated 16 October 2006, “On Arbitration Courts” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴²⁰ Order № 53-mh of the Minister of Justice of the Republic of Uzbekistan dated 2 March 2012, “On Approval of the General Legal Classifier of the Legislative Branches of the Republic of Uzbekistan” (registration № 2333, dated 2 March 2012) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

Pursuant to the Regulation “On the Procedure for the Sale of State Shares”, approved by Resolution № 279 of the Cabinet of Ministers dated October 6, 2014⁴²¹, in relation to disputes and claims arising in the sale of state shares, an opportunity will be created to monitor through digital methods whether the mediation procedure has been carried out as a matter of priority.

8. In civil cases:

Pursuant to Article 70 of the Civil Procedure Code of the Republic of Uzbekistan, it will be possible to digitally monitor that a mediator may not act as a representative in court; pursuant to Article 122, to digitally monitor the leaving of an application without consideration in three cases under the mediation procedure; pursuant to Articles 166 and 226, to conclude a mediation agreement;

pursuant to Article 203, to digitally monitor whether the judge has determined the possibility of the parties concluding a mediation agreement and explained its legal consequences to them; and pursuant to Article 2709, to digitally monitor the non-conclusion of a mediation agreement in cases concerning the return of a land plot arbitrarily occupied and owned by the state and the demolition of an arbitrarily constructed structure⁴²².

9. In economic cases:

Pursuant to Article 53 of the Economic Procedural Code of the Republic of Uzbekistan, it will be possible to monitor that a mediator is not interrogated as a witness;

pursuant to Article 65, that a mediator may not act as a representative in court;

pursuant to Article 2039, to monitor the non-conclusion of a mediation agreement in cases concerning the return of a land plot arbitrarily occupied and owned by the state and the demolition of an arbitrarily constructed structure; and pursuant to Article 131, the processes of concluding a mediation agreement and accepting it by the court will be digitized⁴²³.

10. Regarding the mediation procedure of the Tashkent International Arbitration Centre (TIAC) under the Chamber of Commerce and Industry of the Republic of Uzbekistan:

Pursuant to Resolution № RP-4001 of the President of the Republic of Uzbekistan dated November 5, 2018 “On Establishment of the Tashkent International Arbitration Centre (TIAC) under the Chamber of Commerce and Industry of the Republic of Uzbekistan”, the rights of the Tashkent International Arbitration Centre (TIAC) under the Chamber of Commerce and Industry of the Republic of Uzbekistan⁴²⁴ concerning the mediation procedure will be digitized;

11. In the field of training mediators and entering them into the register:

⁴²¹ Regulation “On the Procedure for the Sale of State Shares”, approved by Resolution № 279 of the Cabinet of Ministers dated 6 October 2014 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴²² Civil Procedure Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴²³ Economic Procedure Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴²⁴ Resolution № RP-4001 of the President of the Republic of Uzbekistan dated 5 November 2018, “On Establishing the Tashkent International Arbitration Centre (TIAC) under the Chamber of Commerce and Industry of the Republic of Uzbekistan” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

Based on Resolution № 171 of the Cabinet of Ministers dated March 19, 2025 “On Measures to Organize the Activities of the Institute for Retraining and Advanced Training of Legal Personnel under the Ministry of Justice of the Republic of Uzbekistan”⁴²⁵, the Order № 54-mh of the Minister of Justice of the Republic of Uzbekistan dated January 31, 2019 (registration № 3134, January 31, 2019), and the Mediator Training Programme approved thereby, the area of mediator training⁴²⁶ and, pursuant to Resolution № 544 of the Cabinet of Ministers dated October 17, 2023 “On Approval of the Administrative Regulation for the Provision of Public Services for Inclusion in the Register of Professional Mediators”⁴²⁷, the field of entering mediators into the register will be fully digitized;

12. Regarding labor disputes:

Pursuant to Articles 542, 545, 554, 560, 570, 573–576, and 579 of the Labor Code of the Republic of Uzbekistan⁴²⁸, the Model Regulation on a Permanently Operating Labor Arbitration, approved by Order № 62-2023/B of the Minister of Poverty Reduction and Employment of the Republic of Uzbekistan dated July 20, 2023 (registration № 3449, July 26, 2023)⁴²⁹, and Resolution № RP–347 of the President of the Republic of Uzbekistan dated October 4, 2024 “On Measures to Improve and Increase the Effectiveness of State Policy in the Field of Poverty Reduction and Employment”⁴³⁰, procedures relating to labor disputes and proceedings conducted in videoconference mode will be digitized;

13. In the field of crypto-shop activities:

Pursuant to Order № 43 of the Director of the National Agency of Perspective Projects of the Republic of Uzbekistan dated September 29, 2022 “On Approval of the Rules for Carrying Out Crypto-Shop Activities” (October 31, 2022, registration № 3395)⁴³¹, customers dissatisfied with the actions (inaction) of a crypto-shop located on the electronic platform and/or at the trading facility will be provided with the opportunity to obtain information from a single point regarding methods and measures for resolving the dispute through mediation;

⁴²⁵ Resolution № 171 of the Cabinet of Ministers dated 19 March 2025, “On Measures to Organize the Activities of the Institute for Retraining and Advanced Training of Legal Personnel under the Ministry of Justice of the Republic of Uzbekistan” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴²⁶ Mediator Training Programme, approved by Order № 54-mh of the Minister of Justice of the Republic of Uzbekistan dated 31 January 2019 (registration № 3134, dated 31 January 2019) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴²⁷ Resolution № 544 of the Cabinet of Ministers dated 17 October 2023, “On Approval of the Administrative Regulation for the Provision of Public Services for Inclusion in the Register of Professional Mediators” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴²⁸ Labour Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴²⁹ Order № 62-2023/B of the Minister of Poverty Reduction and Employment of the Republic of Uzbekistan dated 20 July 2023 (registration № 3449, dated 26 July 2023), approving the Model Regulation on a Permanent Labour Arbitration Tribunal // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴³⁰ Resolution № RP–347 of the President of the Republic of Uzbekistan dated 4 October 2024, “On Measures to Improve and Increase the Effectiveness of State Policy in the Field of Poverty Reduction and Employment” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴³¹ Order № 43 of the Director of the National Agency of Perspective Projects of the Republic of Uzbekistan dated 29 September 2022, “On Approval of the Rules for Conducting Crypto-Store Activities” (31 October 2022, registration № 3395) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

14. Regarding the performance of obligations under a sale and purchase agreement for state property subject to privatization:

Pursuant to the Law of the Republic of Uzbekistan “On Privatization of State Property” dated February 14, 2024, № LRU–907, in the event of non-performance or improper performance of obligations under a sale and purchase agreement for state property subject to privatization, the processes relating to the parties conducting mediation procedures will be digitized⁴³².

15. In the field of advocacy activities:

Pursuant to Order № 30-mh of the Minister of Justice of the Republic of Uzbekistan dated December 20, 2024 “On Approval of the Regulation on the Procedure for Submission of Statistical Information by Bar Associations” (December 23, 2024, registration № 3588), the participation of an attorney in mediation processes will be digitized⁴³³.

16. In the field of public procurement:

Pursuant to Resolution № 476 of the Cabinet of Ministers dated July 30, 2025 “On Additional Measures to Expand the Use of Information and Communication Technologies in Public Procurement and Further Improve the Activities of Operators of the Electronic Public Procurement System”, mediation processes in the pre-trial resolution of disputes in the field of public procurement will be digitized and general monitoring thereof will be established⁴³⁴.

1. Regarding a specific list of disputes to which mandatory mediation applies:

In Italy, the principal instrument regulating mediation in civil and commercial disputes is Legislative Decree № 28/2010 dated March 4, 2010. Pursuant to this instrument, in certain categories of disputes, it is mandatory to undergo a mediation procedure before applying to court.

The list of disputes to which mandatory mediation applies:

Disputes relating to condominiums (common property in multi-apartment buildings);

Disputes concerning rights in rem;

Division of property;

Disputes relating to inheritance;

Family agreements (settlements);

Lease and tenancy;

Commodate (gratuitous use);

Business leasing;

⁴³² Law of the Republic of Uzbekistan № LRU–907 dated 14 February 2024, “On Privatization of State Property” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴³³ Order № 30-mh of the Minister of Justice of the Republic of Uzbekistan dated 20 December 2024, “On Approval of the Regulation on the Procedure for Submission of Statistical Data by Bar Associations” (23 December 2024, registration № 3588) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴³⁴ Resolution № 476 of the Cabinet of Ministers dated 30 July 2025, “On Additional Measures to Expand the Use of Information and Communication Technologies in Public Procurement and Further Improve the Activities of Operators of the Electronic Public Procurement System” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

Compensation for damage caused as a result of medical and healthcare malpractice;

Defamation through the press or other advertising media;

Disputes relating to insurance, banking, and financial contracts.

According to amendments introduced recently, this list has been expanded to include:

Company (association) agreements;

Consortia;

Franchising;

Work (service) contracts;

Network contracts;

Supply and sub-supply contracts⁴³⁵.

In Turkey, the institution of mandatory mediation has been introduced in several stages and primarily covers commercial and labor disputes.

Pursuant to Law № 7036 “On Labor Courts”, adopted on October 25, 2017, mediation is mandatory before applying to court in claims arising from individual or collective labor agreements, claims by an employee or employer relating to wages and compensation payments, as well as claims for reinstatement⁴³⁶.

Pursuant to the Turkish Commercial Code dated February 14, 2011, in most commercial disputes concerning the collection of money or compensation for damages, it is mandatory to apply to a mediator before filing a statement of claim⁴³⁷.

Pursuant to Law № 6502 “On Consumer Protection”, adopted on November 28, 2013, mandatory mediation has also been introduced for consumer disputes exceeding a certain amount⁴³⁸.

The principal legislative instrument is Law № 6325 “On Mediation in Civil Disputes” (Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu), adopted on June 22, 2012⁴³⁹.

In Australia, the approach to mandatory mediation differs somewhat. Although there is no single list at the federal level, this procedure is strictly established in certain areas. In particular, pursuant to the Family Law Act 1975, in matters concerning parenting (children), the parties are required to undergo Family Dispute Resolution before applying to court. In practice, this constitutes mandatory mediation⁴⁴⁰.

In certain states, mediation is mandatory for specific types of disputes. For example, in the State of New South Wales, mandatory mediation exists in the following areas:

Retail leases (Retail Leases Act 1994)⁴⁴¹;

Farm debt (Farm Debt Mediation Act 1994)⁴⁴².

⁴³⁵ [https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2010-03-04:28!vig=.](https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2010-03-04:28!vig=:)

⁴³⁶ <https://www.resmigazete.gov.tr/eskiler/2017/10/20171025-8.htm>.

⁴³⁷ <https://www.resmigazete.gov.tr/eskiler/2011/02/20110214-1-1.htm>.

⁴³⁸ <https://resmigazete.gov.tr/eskiler/2013/11/20131128-1.htm>.

⁴³⁹ <https://resmigazete.gov.tr/eskiler/2012/06/20120622-1.htm>.

⁴⁴⁰ <https://www.legislation.gov.au/C2004A00275/2019-03-10/text>.

⁴⁴¹ <https://legislation.nsw.gov.au/view/html/inforce/current/act-1994-046>.

⁴⁴² <https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1994-091>.

In Greece, pursuant to Article 6 of Law № 4640/2019 (Νόμος 4640/2019, Άρθρο 6), the disputes to which mandatory mediation applies include the following:

family disputes:

division of property acquired by the spouses during the marriage;
maintenance of minor children (alimony);
determination of with whom the children will live;
determination of the arrangements for communication between parents and children.

property disputes:

all disputes exceeding EUR 30,000 in value.

contractual disputes:

disputes relating to the invalidity or performance of contracts.

compensation for damages:

compensation for damage caused as a result of road traffic accidents involving motor vehicles;

compensation for damage caused by medical errors (malpractice);

compensation for damage associated with professional malpractice in the activities of attorneys, notaries, and court enforcement officers.

disputes relating to insults to a person's honor and dignity (through the press or otherwise).

disputes relating to the stock market⁴⁴³.

In Romania, pursuant to Article 60¹ of Law № 192/2006 “On Mediation and the Organization of the Mediator Profession” (Legea nr. 192/2006, Articolul 60¹), an obligation to undergo mediation is established for certain categories of disputes, in particular:

family disputes:

divorce;

exercise of parental rights;

determination of the child's place of residence;

determination of the arrangements for communication with the child;

division of property acquired during the marriage.

civil disputes:

protection of ownership rights;

disputes relating to neighborhood rights;

compensation for damages associated with professional malpractice (malpractice) valued at less than 50,000 lei (the national currency of Romania).

criminal cases: only crimes initiated upon the victim's complaint and permitting **reconciliation between the parties** (for example, **defamation, insult, and minor bodily injury**)⁴⁴⁴.

In Lithuania, pursuant to the requirements of the Law “On Mediation” dated June 29, 2017, all family disputes, including cases concerning dissolution of marriage (divorce), cases concerning legal separation, determination of the place of

⁴⁴³ <https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4640-2019/arthro-6-nomos-4640-2019-ypohreotiki-arhiki-synedria>.

⁴⁴⁴ <https://legislatie.just.ro/Public/DetaliiDocument/71928>.

residence of a minor child, determination of the procedure for visiting a minor child, disputes concerning child support (alimony), amendment or termination of a marriage contract, and division of the spouses' common property must initially be considered through mandatory mediation⁴⁴⁵.

In Montenegro, pursuant to the Law on Alternative Dispute Resolution dated June 5, 2025 (Zakon o alternativnom rješavanju sporova), categories of disputes have been established in which the parties are required to participate in a first mediation meeting before applying to court, including the following:

commercial disputes:

disputes concerning indebtedness between business entities;
disputes relating to banking, leasing, and insurance services;
disputes arising from construction contracts;

labor disputes:

disputes concerning termination of an employment contract;
disputes concerning compensation for damages;

family disputes:

property relations between parents and children;

other disputes:

disputes concerning compensation for damage caused to property;
disputes concerning protection of honor, dignity, and business reputation⁴⁴⁶.

Furthermore, **in the United States**, pursuant to the Federal Alternative Dispute Resolution Act (1988), mediation is applied in administrative and certain criminal cases⁴⁴⁷, **in the United Kingdom** – in cross-border disputes, certain types of public-law disputes, and criminal cases involving minors⁴⁴⁸, **in France** – in certain administrative disputes (tax disputes and disputes relating to financial market relations)⁴⁴⁹, **in the Republic of Kazakhstan** – in administrative disputes, as well as in cases involving administrative offenses⁴⁵⁰ or criminal cases (less serious, moderately serious, and serious crimes)⁴⁵¹.

2. Regarding the digitalization of the mediation institution:

The **European Union**, through the EU ODR Platform (European Online Dispute Resolution), which operated until 2025⁴⁵², created an opportunity to receive online applications concerning disputes related to consumers' rights and interests and to connect them with a mediator/ODR body, while new opportunities are currently being created through the "Consumer Redress in the EU" platform⁴⁵³. **In Turkey**, the UYAP (Ulusal Yargı Ağı Projesi) information system⁴⁵⁴, the E-Hearing

⁴⁴⁵ <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/95539982609f11e7a53b83ca0142260e>.

⁴⁴⁶ <https://me.propisi.net/zakon-o-alternativnom-rjesavanju-sporova/>.

⁴⁴⁷ <https://www.congress.gov/bill/105th-congress/house-bill/3528>.

⁴⁴⁸ <https://www.legislation.gov.uk/ukxi/2011/1133/contents/made>.

⁴⁴⁹ https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070933/.

⁴⁵⁰ <https://adilet.zan.kz/rus/docs/K1400000234>.

⁴⁵¹ <https://adilet.zan.kz/rus>.

⁴⁵² https://consumer-redress.ec.europa.eu/site-relocation_en.

⁴⁵³ https://consumer-redress.ec.europa.eu/index_en.

⁴⁵⁴ <https://bilirkisi.uyap.gov.tr/giris>.

mobile application⁴⁵⁵, and the E-Arabulucu platform⁴⁵⁶ have been created, through which a “mediator” interface provides opportunities to monitor the status of mediators, receive and review cases, and maintain an online mediation register. **In Singapore**, through the CJTS (Community Justice & Tribunals System) / eLitigation platform, e-Negotiation and e-Mediation capabilities are available (online negotiation and mediation elements, the ability to submit applications online and view documents, conduct video meetings, and create and upload electronic agreements)⁴⁵⁷. **In Estonia**, through the e-File (E-toimik) / e-Justice ecosystem⁴⁵⁸, opportunities have been created for electronic conduct of court proceedings (e-filing), receipt of electronic statements and decisions by all parties, obtaining information through interagency data exchange (X-Road)⁴⁵⁹, and personal authentication through the national e-ID (ID-card / Mobile-ID), including its use for verifying participants in mediation and court hearings. **In the Republic of Korea**, the Korean ODR and Supreme Court e-Litigation platforms provide opportunities for electronic filing, remote hearings, and online mediation⁴⁶⁰. **In the UAE**, online mediation has been established through the DIFC Courts Virtual Hearing and Smart Courts⁴⁶¹ systems, and **in the United States**, through the Utah State Courts ODR Platform⁴⁶².

For the purpose of improving the mediation institution, the following is proposed:

- 1) approval of a specific list of disputes to which mandatory mediation applies;
- 2) full digitalization of the mediation institution and ensuring its transparency.

Therefore, for the purpose of implementing these tasks, the following is proposed:

I. Establishment of a Working Group consisting of representatives of the Ministry of Justice of the Republic of Uzbekistan, the Institute of Legislation and Legal Policy, the Ministry of Economy and Finance, the Tax Committee, and the Ministry of Digital Technologies;

II. To define the tasks of the Working Group, after the Working Group has been fully formed, as the **implementation of the following**:

1. formation of a specific list of disputes to which mandatory mediation applies;
2. submission to the Presidential Administration of the draft resolution of the President of the Republic of Uzbekistan “On Improving the Regulation of Relations in the Field of Mediation”, providing for:

⁴⁵⁵ <https://play.google.com/store/apps/details?id=tr.gov.adalet.edurusma&hl=ru>.

⁴⁵⁶ <https://arabulucu.uyap.gov.tr/main/arabulucu/index.jsp?v=3785>.

⁴⁵⁷ <https://cjts.judiciary.gov.sg/home>.

⁴⁵⁸ <https://e-estonia.com/e-estonia-briefing-centre-services/about-us/>.

⁴⁵⁹ <https://www.rik.ee/en/international/ai-solutions>.

⁴⁶⁰ <https://eng.scourt.go.kr/eng/judiciary/eCourt/eTrials.jsp>.

⁴⁶¹ <https://www.difccourts.ae/rules-decisions/practice-directions/practical-guidance-note-no-1-2023-difc-courts-virtual-hearing-and-bundling-protocol>.

⁴⁶² <https://www.utcourts.gov/en/about/miscellaneous/law-library/research/utah.html>.

inclusion, among the areas in which mediation procedures are applied, of civil, tax, public procurement disputes, disputes in cases where one of the parties is a state body, organization, or business entity, as well as cases involving damage caused in administrative offense and criminal cases, as a method of securing obligations;

introduction of amendments and additions to the Code of Administrative Responsibility and the Criminal Procedure Code arising from the refusal to initiate an administrative offense or criminal case and the termination of an ongoing case due to the application of the mediation procedure in an administrative offense or criminal case;

approval of a unified list of disputes to which mediation applies;

establishment of the practice whereby courts, in disputes to which mediation applies, offer the parties mandatory mediation and, based on its outcome, terminate or continue the proceedings;

establishment of procedures for incentivizing mediators in disputes resolved by courts as a result of cases in which mediation was applied;

establishment of an opportunity to automatically notify the mediator about state bodies and organizations, as well as disputes to which mediation applies that are under consideration by a court;

establishment that remuneration paid to professional mediators shall not constitute an object of taxation;

introduction of the AI-based “**Digital Mediation**” integrated information system and its mobile application;

approval of the Regulation on the procedure for conducting mediation procedures using the “**Digital Mediation**” integrated information system;

establishment of a mechanism for conducting mediation procedures with mandatory use of the “**Digital Mediation**” integrated information system in full;

creation, through the “**Digital Mediation**” integrated information system and its mobile application, of the following opportunities for implementation in real time:

obtaining information in the “**Digital Mediation**” integrated information system concerning the identity, property, residential and current address of the mediator and the parties, as well as other information relating to the subject matter of the dispute, through interagency electronic cooperation, and filling in information through traditional methods;

information on the list of disputes to which mediation applies and, based on this list, mediation agreements concluded in the Republic, the mediators who certified them, and the results of the agreements;

education on the digital learning platform necessary for training professional mediators;

the register of professional mediators;

the register of mediation agreements and cases completed through mediation procedures;

obtaining, through interagency electronic cooperation, information concerning the mediator and the parties, mediation agreements concluded by them and certified by a QD-code, and information on their implementation;

sending an offer to conclude a mediation agreement, accepting it, reviewing and discussing offers and proposals;

providing the mediator with the information and evidence necessary for concluding a mediation agreement, and enabling the mediator to submit alternative proposals to the parties;

sending summonses to the parties and conducting discussions of the mediation agreement between the parties through videoconference communication with the participation of the mediator;

editing a draft mediation agreement, concluding a mediation agreement, making amendments and additions thereto, terminating it, approving it, and downloading the mediation agreement certified by a QD-code;

payment of remuneration to the mediator;

obtaining information on the rights and obligations of the mediator, the parties, and platform users, their liability arising from these obligations, the procedure for filing complaints, and the consequences of concluding a mediation agreement;

receiving notifications concerning actions carried out in real time through the Single Interactive Public Services Portal, the electronic public services portal of tax authorities, the “Digital Mediation” integrated information system, and its mobile application;

through integration with the interactive services portal of the Supreme Court of the Republic of Uzbekistan, enabling courts to obtain, from a single platform, mediation agreements, as well as rulings on termination of proceedings or leaving a case without consideration due to the acceptance of mediation agreements by interested parties;

conducting mediation procedures in a simple and convenient manner through the conversion of video, audio, and voice recordings into text;

establishment of an opportunity to automatically notify the mediator about state bodies and organizations, as well as disputes to which mediation applies that are under consideration by a court;

enabling the parties and mediator, after registering through the Single Interactive Public Services Portal, the electronic public services portal of tax authorities, and using the QD-code on the ID card and Face ID authentication methods, to review the processes relating to the mediation procedures in which they participated and obtain the necessary information through the “Digital Mediation” integrated information system and its mobile application, as well as to work with the necessary information in the system.

4.4-§. Further Strengthening the Role of Forensic Examination in the Detection of Crimes and Cybercrimes Committed Using Information and Communication Technologies

The number of crimes and cybercrimes committed using information and communication technologies is increasing day by day.

For information: In Uzbekistan, **863** acts were registered in 2020, **785** in 2021, **7,570** in 2022, **6,450** in 2023, and **58,800** acts in 2024 as having been committed using information technologies. The number of ***cybercrimes in 2024 increased by approximately 68.13 times compared to 2020.***

Determining when, how, and by whom these socially dangerous acts were committed, detecting crimes, and identifying and locating the perpetrators make the **role and significance of forensic examination** extremely important.

At present, forensic computer-technical examinations are appointed in cases concerning crimes and cybercrimes committed using information and communication technologies.

However, forensic computer-technical examination does not currently meet the requirements of the present day and is not sufficiently effective for the following reasons, in particular:

first, during the forensic examination, experts are initially unable to determine whether the evidence was properly obtained with the participation of a specialist, or whether any technical errors occurred at the time the evidence was collected.

It is known that, pursuant to Law № LRU–1003 of the Republic of Uzbekistan dated November 21, 2024 “On Introducing Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan Aimed at Improving the System of Handling Digital Evidence”, amendments were introduced to the Criminal Procedure Code of the Republic of Uzbekistan establishing the procedure for voluntarily providing **electronic data** to an official of the body conducting the pre-investigation examination, an inquiry officer, an investigator, a prosecutor, or a court, and for attaching items, documents, and electronic data to a case as material, documentary, and digital evidence⁴⁶³.

Pursuant to Article 69 of the Criminal Procedure Code of the Republic of Uzbekistan, a **specialist shall be called to assist** the inquiry officer, investigator, prosecutor, and court in **finding and securing evidence** during the conduct of an investigation and court proceedings. A physician, teacher, or other person possessing the necessary knowledge and qualifications may be called as a specialist⁴⁶⁴.

Accordingly, the aforementioned Law established, in the current Criminal Procedure Code of the Republic of Uzbekistan, the **necessity of the participation of a specialist in attaching electronic data to a case as material, documentary, and digital evidence.**

⁴⁶³ Law of the Republic of Uzbekistan № LRU–1003 dated 21 November 2024, “On Introducing Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan Aimed at Improving the System for Handling Digital Evidence” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴⁶⁴ Criminal Procedure Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

At the same time, pursuant to Resolution № RP–153 of the President of the Republic of Uzbekistan dated April 30, 2025 “On Measures Aimed at Further Strengthening Activities to Combat Crimes Committed Using Information Technologies”, a procedure has been introduced whereby the **Cybersecurity Center** State Unitary Enterprise issues an opinion on compliance with cybersecurity requirements in relation to cybercrimes committed during the pre-investigation examination and preliminary investigation⁴⁶⁵.

However, the mandatory requirements imposed on such specialists and their conclusions, as well as the specific duties of specialists, have not been established in the current legislation. Article 70 of the CPC also contains no provisions in this regard.

For information: In practice, law enforcement agencies engage specialists from the Ministry of Digital Technologies, the Inspectorate for Control in the Field of Informatization and Telecommunications and its territorial and system organizations, as well as specialists from the “Cybersecurity Center” State Unitary Enterprise, and the issue of initiating criminal proceedings is decided on the basis of materials prepared based on their explanations.

As a result, opportunities for the timely detection of cybercrimes remain unrealized due to the fault of the inquiry officer, investigator, prosecutor, judge, and specialist;

second, due to the insufficient technical knowledge of inquiry officers, investigators, prosecutors, and judges, particularly their insufficient knowledge of cybertechnologies, they are unable to determine whether a specialist has made an error during investigative actions, while the fact that a specialist, unlike an expert, is not warned under Articles 238 and 240 of the Criminal Code causes the specialist not to consider the consequences of his or her actions;

third, although **forensic computer-technical examination** is appointed in cases concerning crimes and cybercrimes committed using information and communication technologies, in terms of its scope, it addresses matters relating to computer technology and equipment.

The **objects of examination** may include:

- computer equipment (processors, memory, disks, and others);
- computer devices (printers, scanners, flash drives, and others);
- technical aspects of software.

The **examination questions** concern:

- the operability of the device;
- determining whether data on a data carrier has been deleted;
- the legality or licensing of software;
- issues relating to the causes of technical malfunctions.

However, it is, in fact, unable to resolve the following issues, in particular:

issues relating to the examination that must be appointed to determine the quality of communication and whether, as a result thereof, a communication-related

⁴⁶⁵ Resolution № RP–153 of the President of the Republic of Uzbekistan dated 30 April 2025, “On Measures Aimed at Further Strengthening Efforts to Combat Crimes Committed Using Information Technologies” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

crime provided for under Articles 186 and 263 of the Criminal Code has been committed;

issues relating to the condition of telecommunications networks, in particular matters concerning telecommunications networks provided for under Articles 143, 186, 163, 278³, and 278⁷ of the Criminal Code;

cryptographic issues, in particular circumstances provided for under Articles 141¹–141³, 143, 150–151, 154–155, 155², 156, 157–162, 165, 168–169, 210, 278¹–278⁴, and 278⁶–278⁸ of the Criminal Code;

issues relating to information systems, websites, networks, messengers, electronic mail, log files, IP addresses, and “digital traces”, in particular circumstances provided for under Articles 141¹–141³, 143, 150–151, 154–155, 155², 156, 157–162, 165, 168–169, 210, 278¹–278², 278⁴, and 278⁸–278⁹ of the Criminal Code that are not related to computer systems, computer technology, and equipment.

Therefore, since forensic computer-technical examination **covers only matters related to computer technology**, it is considered impossible, through such examination, to:

prove the commission of cybercrimes;

determine who, when, and by what method modified data in a network or information system;

recover data deleted or encrypted in a network or information system;

detect digital traces related to corruption and fraud;

prepare evidence having legal force in court.

fourth, the formulation of questions submitted to an expert and the proper appointment of an examination are of great importance in detecting a crime and identifying the actual perpetrator. A forensic computer-technical examination can provide answers based on its area of expertise only when questions relating exclusively to computer technology are submitted to the expert; however, it cannot answer questions concerning **networks, communication quality**, or matters beyond computer technology; moreover, **it may not address legal issues**.

The reason for this is that personnel training in this field in the Republic is still being carried out using outdated methods.

In particular, there is currently no expert or forensic examination center in the Republic capable of providing an opinion specifically on communication quality. **The H. Suleymanova Republican Forensic Examination Center, the Institute of Scientific Research on Digital Forensics of the Law Enforcement Academy, and its Center for Assistance in Combating Cybercrime and Digital Investigation also do not have such capabilities.**

As a single example, where an offense or crime arises directly as a result of **communication quality** under Articles 153 and 164 of the Code of Administrative Responsibility and Articles 186 and 263 of the Criminal Code, none of the forensic examination centers or experts in the Republic is able to determine, by technical methods, the causes of such offense or crime.

Therefore, **when the period from 2017 to 2025 was analyzed**, it was established that employees of the Inspectorate for Control in the Field of Informatization and Telecommunications took measures based solely on the

conclusion of the “Electromagnetic Compatibility Center” State Unitary Enterprise regarding communication coverage and violations of regulatory documents in the field of technical regulation concerning the continuity of communications, while **no measures were taken in relation to offenses arising directly from the quality of the communication being provided.**

According to the Decrees of the President of the Republic of Uzbekistan “On Approval of the “Digital Uzbekistan – 2030” Strategy and Measures for Its Effective Implementation” № DP–6079 dated October 5, 2020 ⁴⁶⁶, “On Measures to Effectively Organize Public Administration in the Field of Digital Technologies within the Framework of Administrative Reforms” № DP–76 dated May 24, 2023⁴⁶⁷, and the Resolutions “On Measures for the Widespread Introduction of the Digital Economy and E-Government” № RP–4699 dated April 28, 2020⁴⁶⁸, “On Measures to Bring the Information and Communication Technologies Sector to a New Level in 2022–2023” № RP–357 dated August 22, 2022⁴⁶⁹, and “On Measures to Increase the Coverage and Quality of Digital Services and Digitally Transform Sectors, Industries and Regions” № RP–162 dated May 24, 2023⁴⁷⁰, it has been established that the coverage of the regions of the Republic by the high-speed Internet global information network shall be increased to **100 percent by 2030.**

Furthermore, pursuant to Resolution № RP–357 of the President of the Republic of Uzbekistan “On Measures to Bring the Information and Communication Technologies Sector to a New Level in 2022–2023” dated August 22, 2022, it was envisaged that, **by the end of 2022**, the level of coverage of residential areas by broadband mobile communication networks would **reach 98 percent**⁴⁷¹.

However, **there is no forensic institution in the Republic capable of verifying whether these tasks have actually been implemented in practice, and, consequently, the extent to which these tasks have actually been fulfilled has still not been verified or made known to the general public.**

Moreover, today, approximately 20 higher education institutions related to the fields of cybersecurity and cybercrime train specialists; however, their educational programmes **are not specialised in simultaneously providing comprehensive training of specialists in both legal and technical fields**, and the specialists

⁴⁶⁶ Decree № DP–6079 of the President of the Republic of Uzbekistan “On Approval of the “Digital Uzbekistan – 2030” Strategy and Measures for Its Effective Implementation” dated October 5, 2020 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴⁶⁷ Decree № DP–76 of the President of the Republic of Uzbekistan “On Measures to Effectively Organize Public Administration in the Field of Digital Technologies within the Framework of Administrative Reforms” dated May 24, 2023 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴⁶⁸ Resolution № RP–4699 of the President of the Republic of Uzbekistan “On Measures for the Widespread Introduction of the Digital Economy and E-Government” dated April 28, 2020 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴⁶⁹ Resolution № RP–357 of the President of the Republic of Uzbekistan “On Measures to Bring the Information and Communication Technologies Sector to a New Level in 2022–2023” dated August 22, 2022 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴⁷⁰ Resolution № RP–162 of the President of the Republic of Uzbekistan “On Measures to Increase the Coverage and Quality of Digital Services and Digitally Transform Sectors, Industries and Regions” dated May 24, 2023 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴⁷¹ Resolution № RP–357 of the President of the Republic of Uzbekistan dated 22 August 2022, “On Measures to Bring the Information and Communication Technologies Sector to a New Level in 2022–2023” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

implementing the educational process are likewise not considered specialists capable of simultaneously working in both fields.

***For information:** While educational institutions such as Tashkent State University of Law, the Institute of Criminology Research, the Academy of the Ministry of Internal Affairs, and the Law Enforcement Academy train specialists with greater emphasis on the legal field and less on technical fields, Tashkent University of Information Technologies, Amity University in Tashkent, and Inha University in Tashkent mainly train specialists in technical fields. However, they do not train specialists specifically specialised in conducting forensic examinations of cyber-offences and cybercrimes.*

Furthermore, in the Republic, there is no specialised higher education institution, preschool, secondary, specialised secondary, or professional education institution that specifically trains experts specialised in detecting cybercrimes, nor are the necessary educational programmes, retraining and professional development programmes, specialised educational areas, or courses available or sufficiently established. Only from the 2025–2026 academic year, permanent specialised training courses in the field of “Digital Forensics” will be organised in distance-learning format through the educational information portal of the Law Enforcement Academy for **inquiry officers, investigators, and employees of prosecution authorities engaged in operational-search activities.** However, this **does not cover operational-search officers, judges, or experts.**

***For information:** At the Cyber University State University, instruction of students in the speciality **Jurisprudence: Digital Forensics (60420100)** will commence from the 2025–2026 academic year. However, its educational programme is not sufficiently oriented towards training modern cyber experts; rather, its implementation is planned based on the existing classifier.*

In addition, the fact that the **methodology for calculating damage caused as a result of cybercrimes has still not been adopted** is creating a number of problems in determining the exact amount of the damage and serious harm caused, incorporating such amount into the case materials, and providing it with a legal assessment. At the same time, **for cybercrimes, including those provided for under Articles 278¹–278⁹ of the Criminal Code, the amount of damage and serious harm is of significant importance.**

For information:** During 2017–2025, no forensic examination was appointed by the courts to determine the amount of serious harm and actual damage caused by crimes committed using information and communication technologies, including cybercrimes, and **the damage caused was determined on the basis of documents provided by the relevant organisations.

For example, the damage provided for under Article 278⁷ of the Criminal Code is based solely on a certificate provided by operators.

These circumstances, in turn, demonstrate the need for separate and independent institutions capable of ensuring the proper collection and preservation of digital evidence, monitoring the proper conduct of investigative actions, referring the information and technical devices obtained for forensic examination, and enabling judges to assess digital information as evidence and draw appropriate conclusions.

1) Requirements imposed on the competence of specialists and experts engaged in and working with cases involving cybercrimes:

In Germany, the national standard DIN ISO/IEC 27037:2013-10⁴⁷²; **in Italy**, the national standard UNI 11742:2019 – “Figure professionali operanti nel settore ICT – Esperto in informatica forense”⁴⁷³; **in France**, the NSSI – *Référentiel d'exigences pour la qualification “PRIS” (Prestataires de Réponse aux Incidents de Sécurité)* requirements framework⁴⁷⁴; **in Spain**, the CCN-STIC 817 – *Gestión de Incidentes (CCN-CERT)*⁴⁷⁵ and CCN-STIC 820/821⁴⁷⁶ national technical guidelines; **in Austria**, the national standard ÖNORM ISO/IEC 27037⁴⁷⁷; **in Poland**, the national standard PN-ISO/IEC 27037⁴⁷⁸; **in Portugal**, the national standard NP ISO/IEC 27037⁴⁷⁹; and **in Switzerland**, the national standard SN ISO/IEC 27037⁴⁸⁰ provide for qualification and experience requirements, training and competencies, tasks and functions, as well as the rights and obligations of professional specialists and experts engaged in crimes committed using information and communication technologies and cybercrimes.

2) Regarding the methodology for calculating damage caused as a result of cybercrimes:

In Russia, the *Methodology for Determining the Amount of Damage Caused by Crimes in the Sphere of Computer Information*; **in the European Union**, *EUROPOL IOCTA (Internet Organised Crime Threat Assessment)*⁴⁸¹ and *ENISA – Methods for Estimating Economic Impact of Cyber Incidents*⁴⁸²; **in the United States**, *NIST Special Publication 800-30 – Guide for Conducting Risk Assessments*⁴⁸³ and *NIST SP 800-55 – Performance Measurement Guide for Information Security*⁴⁸⁴; **in China**, *Guidelines for Calculating Economic Losses from Cybercrime*⁴⁸⁵; **in India**, *Methodology for Estimation of Loss due to Cybercrime*⁴⁸⁶; **in the Republic of Korea**, *Guidelines on the Calculation of Damages from Cybercrime*⁴⁸⁷; and **in Kazakhstan**, *Methodological Recommendations for Determining Material Damage Caused as a Result of Cybercrimes*⁴⁸⁸, damage caused as a result of cybercrimes is calculated on the basis of the respective documents.

⁴⁷² <https://webstore.ansi.org/standards/ds/dsisoiec270372013>.

⁴⁷³ <https://http.uni.com/en/uni-11742-2019>.

⁴⁷⁴ <https://www.lsti-certification.fr/fr-FR/Nos-offres-entreprises/Cybersecurite/Qualification-PRIS>.

⁴⁷⁵ https://www.aec.es/wp-media/uploads/DPD-00266.SEG-GUI-004-CCN-STIC-817_Gestion_de_Ciberincidentes_ENS.pdf.

⁴⁷⁶ <https://access.redhat.com/compliance/ccn-stic>.

⁴⁷⁷ <https://webstore.iec.ch/en/publication/11317>.

⁴⁷⁸ <https://meganorm.ru/Data2/1/4293768/4293768989.pdf>.

⁴⁷⁹ <https://standards.iteh.ai/catalog/standards/iso/1a0f0032-a18e-4c41-baef-932b9c410aa5/iso-iec-27037-2012>.

⁴⁸⁰ <https://www.iso.org/standard/44381.html>.

⁴⁸¹ <https://www.europol.europa.eu/publications-events/main-reports/iocta-report>.

⁴⁸² <https://www.enisa.europa.eu/news/enisa-news/determining-the-real-economic-impact-of-cyber-incidents-a-mission-almost-impossible>.

⁴⁸³ <https://csrc.nist.gov/pubs/sp/800/30/r1/final>.

⁴⁸⁴ <https://csrc.nist.gov/pubs/sp/800/55/r1/final>.

⁴⁸⁵ <https://www.court.gov.cn/>.

⁴⁸⁶ <https://www.meity.gov.in/>.

⁴⁸⁷ <https://www.kcc.go.kr/>.

⁴⁸⁸ <https://www.gov.kz/>.

3) The types of examinations to be appointed in cases involving cybercrimes, in terms of foreign countries and the Republic of Uzbekistan, are provided for in accordance with **Annex 1**;

4) The list of countries, organizations, and programmes providing training, retraining, advanced training, and specialized education for cyber-experts in foreign countries is set out in **Annex 2**;

5) The list of specialized forensic examination centres that exclusively provide expert opinions in respect of cyber-offences and cybercrimes is set out in **Annex 3**.

In order to further strengthen the role of forensic examination in detecting crimes and cybercrimes committed using information and communication technologies and to bring cyber-forensic examination to a new stage, the following is proposed:

1. To establish a working group comprising representatives of the Ministry of Justice of the Republic of Uzbekistan, the Ministry of Internal Affairs, the Ministry of Higher Education, Science and Innovations, the Ministry of Preschool and School Education, the Ministry of Digital Technologies, the Ministry of Economy and Finance, the Prosecutor General's Office, the State Security Service, the Agency for Strategic Reforms, the Agency for Technical Regulation, the Central Bank, the "Cybersecurity Center" SUE, the Law Enforcement Academy, the Institute of Criminology, Tashkent State University of Law, CYBER University, Tashkent University of Information Technologies, the Academy of the Ministry of Internal Affairs, Inha University in Tashkent, Amity University in Tashkent, the Institute of Legislation and Legal Policy, and other interested ministries and agencies;

2. Upon formation of the working group and commencement of its activities, to designate as its task the development and submission to the Presidential Administration of the Republic of Uzbekistan of a draft Resolution of the President of the Republic of Uzbekistan **"On Measures to Systematize Digital Forensics and Bring It to a New Stage"**, providing for the following:

a) to establish a system of forensic examinations applicable to crimes and offences committed using information and communication technologies, including cybercrimes, and to include therein telecommunications network examination, telecommunications infrastructure examination, information systems examination, computer information and electronic data examination, software and software-related examination, cryptographic examination, communications coverage and quality examination, cyber-forensic examination, and forensic economic cyber-examination;

b) to establish the practice of conducting **forensic cyber-examinations** that provide a comprehensive legal and technical opinion concerning the legality and reliability of specialist opinions and expert conclusions obtained in cases involving crimes and cybercrimes committed using information and communication technologies, as well as the legality and reliability of evidence and the accuracy of the sources from which such evidence was obtained, including digital evidence, electronic documents and data, and technical devices;

c) to reorganize the limited liability company “Information Technologies and Information Resources Development Center” as a state institution under the name **“Republican Center for Digital Technology Forensic Examinations”**;

d) to establish a unified legal and technical practice for expert conclusions and specialist opinions in this field throughout the Republic by granting the **Republican Center for Digital Technology Forensic Examinations** the authority to issue forensic cyber-examination conclusions concerning conclusions and specialist opinions issued in cases involving crimes and cybercrimes committed using information and communication technologies;

e) to develop and introduce a specialized **“Cyber-Criminalist”** educational programme encompassing the system of preschool, school, higher and post-higher education for the training of specialized experts and specialists in cybercrimes, fully incorporating both legal and technical knowledge;

f) to establish a specialization in **“Cyber Forensics”** fully encompassing criminal, civil and international law, as well as specialized technical disciplines, and to critically review the existing classifier and curriculum;

g) to introduce mandatory instruction in Cyber Forensics textbooks at the preschool, school, higher and post-higher education levels, taking into account the age and interests of learners;

h) to establish and maintain an online database and register of specialists and experts engaged in cases involving crimes and cybercrimes committed using information and communication technologies, and to create an opportunity to view the amounts of remuneration payable to them on an open platform;

k) to establish that expert examinations in cases involving crimes and offences committed using information and communication technologies, including cybercrimes, may be conducted exclusively by **certified experts**;

l) to approve the following:

- a list of mandatory requirements applicable to organizations, experts and specialists issuing specialist and expert opinions and conclusions in cases involving crimes and cybercrimes committed using information and communication technologies;

- a regulation on the special procedure for engaging specialists and experts and obtaining specialist opinions and expert conclusions in criminal cases involving crimes and cybercrimes committed using information and communication technologies;

- a list of types of forensic examinations applicable to crimes and cybercrimes committed using information and communication technologies;

- a methodology for calculating damage resulting from cybercrimes;

- a regulation on the procedure for appointing forensic cyber-examinations and obtaining expert conclusions;

m) taking into account categories of critical information infrastructure facilities for which direct assessment is impossible, to establish a practice of determining the amount of damage by multiplying the value attributable to each facility by the respective categories of **“significant,” “large,” and “very large”** amounts;

n) to issue instructions on introducing amendments and additions to the Criminal Procedure Code and the Code of Administrative Responsibility concerning the mandatory conduct of **forensic cyber-examinations** in cases involving crimes and cybercrimes committed using information and communication technologies, for the purpose of determining the legality and reliability of evidence and the accuracy of the sources from which it was obtained, as well as the mandatory conduct of **communications coverage and quality examinations** in respect of acts and offences related to communications quality, for the purpose of determining the quality and coverage of communications and their adverse impact on the population and living organisms.

NATIONAL AND FOREIGN EXPERIENCE IN THE USE OF FORENSIC EXAMINATIONS IN CYBERCRIME CASES

№	Country	Types of Forensic Examinations Used in Cybercrime Cases									
		Telecommuni- cation networks	Viruses and malicio- us softwar- e	Computer equipment, hardware and devices	Qualit- y and cover- age of commu- nicat- ion servic- es	Legal and technical verificati- on of evidence , involve- ment of specialis- ts, and supervisi- on of the forensic examinat- ion process	Electro- nic docume- nts and data	Digital evidence and traces	Telecommuni- cation devices and information storage media	Informa- tion systems and softwar- e	Determinat- ion of the amount of damage caused
1.	USA	Telecommuni- cation Forensics, Cell Site Analysis, IP Traffic Analysis	Malwar- e Forensi- cs, Reverse Engineer- ing,	Computer Forensics	Cell Site Analy- sis, Radio Frequ- ency	Forensic authentic- ation / Digital evidence validatio- n	Electro- nic docume- nt authenti- cation; Metadat	Digital Forensic s, Digital Evidenc- e	Network Forensics, Telecommuni- cation Forensics, Mobile Device Forensics	Softwar- e Forensi- cs / Source Code	Economic Loss Assessment , Risk/Impac- t

			Cyber Forensics		Analysis		a analysis ; E-signature verification; Forensic imaging ; File system analysis ; Email header & server log analysis , E- Discovery	Examination		Analysis	Assessment , Economic Impact Assessment of Cybercrime
2.	Russia		Software and Technical Examination	Computer Forensic Examination	Forensic Telecommunications		Examination of Electronic Documents;	Electronic Evidence Examination	Telephone and Computer Forensic Examination	Information and Technical Examination	Economic Examination

					Exam ination		Digital Tracing ; Verifica tion of Digital Signatu res; Examin ation of Logs and Storage Media				
3.	United Kingdom	Mobile Device Forensics, Telecoms Forensics, Call Detail Records (CDR) Analysis	Malicio us Softwar e Analysi s, Digital Forensi cs	Computer Forensics, Computer Hardware Examinati on	Telec omm unicat ions Foren sics	Forensic Cyber Examina tion; Expert Evidenc e – Digital Evidenc e Authenti cation.	Digital docume nt examin ation; e-mail forensic s; metadat a & timesta mp analysis ;	Data Recover y / E- Discover y, Digital Evidenc e Forensic Analysis	Network Forensics, Telecoms Data Forensics	Networ k Forensi cs, Softwar e & Informa tion System Forensi cs	Economic Loss Assessment

							e-signature checks, Data Recovery / E-Discovery				
4.	Germany	Netzwerkforensik	Schadsoftware-Forensik	Computertechnik-Forensik	Telekommunikationsforensik	Forensic Cyber Examination; Electronic Evidence Authentication.	Elektronische Dokumentenprüfung; Dateisystem- und Metadatenanalyse; Signaturprüfung; Forensische Abbilder	Digitale Spurenanalyse / Digitale Beweisuntersuchung	Datenträgeruntersuchung, Telekommunikationsspuren-Analyse	IT-Forensik	Wirtschaftsexpertise zur Schadensberechnung

5.	Singapore	Network Forensics, Telecommunications Forensics	Malware Forensics, Code Reverse Engineering	Computer Hardware Forensics	Telecommunications Forensics	Authentication of electronic records	Electronic document authentication; e-signature verification; log and metadata forensic s; document provenance analysis	Digital Evidence Examination, Digital Evidence Authentication / Digital Forensic s	Mobile & Telecom Forensics	Software Forensics / Information System Analysis	Financial Cybercrime Assessment, Cybercrime Financial Impact Assessment
6.	South Korea	Mobile & Network Forensics, Telecommunications Forensics	Malware Forensics, Code Reverse Engineering	Computer Hardware Forensics	Coverage Analysis	Digital forensic authentication	Digital document forensic s; metadata/timestamp	Digital Forensic Examination, Digital Evidence Authentication	Mobile & Network Forensics	Software Forensics / Information System	Economic Loss Estimation, Cybercrime Financial Impact Assessment

							analysis ; electron ic signatur e and certifica te checks; mail/log forensic s	cation / Digital Forensic s		Analysi s	
7.	China	Telecommuni cation and Network Forensics	Malicio us Code Forensi c Examin ation	Computer Hardware Forensic Examinati on		Electroni c data judicial authentica tion	Judicial appraisa l of electron ic docume nts; metadat a analysis ; e-signat ure and certifica te validati	Digital Evidenc e Judicial Authenti cation	Electronic Media Forensics	Informa tion System Forensi c Analysi s	Economic Loss Calculation Guidelines, Cybercrime Loss Assessment

							on; log and server data examin ation				
8.	Kazakhst an		Informa tion Technol ogy Forensi c Examin ation	Informatio n and Computer Technolog y Forensic Examinati on	Foren sic Telec omm unicat ions Exam inatio n	Electroni c Docume nt Forensic Examina tion	Electro nic Docum ent Examin ation; Metadat a and Log Analysi s; Digital Signatu re Verifica tion	Informat ion and Comput er Forensic Examina tion	Forensic Examination in the Field of Information and Communicatio n Technologies, Forensic Examination of Telecommunic ation Devices		Economic Examination, Forensic Examination for the Assessment of Damage Caused by Cybercrime
9.	Uzbekista n			Forensic Computer Technical Examinati on			Forensi c Technic al Examin ation of	Forensic Comput er Technic al	Forensic Electrical Engineering Examination, Forensic Computer	Forensi c Comput er Technic al	Forensic Economic Examination, Forensic Accounting

							Documents, Forensic Examination of Video Materials	Examination	Technical Examination	Examination	Examination, Forensic Economic and Statistical Examination
10.	Poland	Analiza sieci		Informatyka śledcza		Суд-киберэкспертиза	Informatyka śledcza (digital document authentication); metadata & e-signature verification		Ekspertyza nośników danych		
11.	Tajikistan			Computer Forensic Examination			Examination of Electronic Documents			Forensic Information	Economic Examination

							ents; Log/Me tadata Analysi s; Digital Signatu re Verifica tion			Examin ation	
12.	Turkmeni stan			Computer Forensic Examinati on			Comput er and Electro nic Docum ent Examin ation; Analysi s of Storage Media	Electron ic Evidenc e Examina tion			Economic Examinatio n
13.	Kyrgyzst an			Computer Forensic Examinati on			Examin ation of Electro nic Docum ents and	Electron ic Evidenc e Examina tion		Informa tion System s Forensi c	Economic Examinatio n

							Files; Metadat a, Timesta mp and Log Analysi s			Examin ation	
14.	India	Telecom and Network Forensics	Cyber Forensi cs, Malwar e Analysi s	Digital / Computer Hardware Forensics	Mobil e Netw ork Foren sics	Expertis e Digital Forensic, Electroni c records authentic ation, Cyber Forensic s	Digital docume nt authenti cation; e-signat ure validati on (where applica ble); email/se rver log analysis ; metadat a examin ation,	Digital Forensic s, Digital Evidenc e Analysis	Cyber Forensics	Cyber Forensi cs, Softwar e Forensi cs / IT System Examin ation	Cybercrime Financial Impact Assessment

							E- Discove ry				
15.	Georgia			Computer Forensic Examinati on			Electro nic docume nt forensic ; timesta mp end metadat a checks; file integrit y analysis	Digital Tracing			
16.	Belarus		Softwar e and Technic al Examin ation	Computer Forensic Examinati on		Forensic Cyber Examina tion	Informa tion Forensi c Examin ation			Softwar e and Technic al Examin ation	
17.	France	Expertise en logiciels malveillants,		Expertise en informatiq ue,	Exper tise téléco m	Expertis e en cybercri minalité,	Expertis e électron ique des	Analyse des traces numériq	Expertise en télécommunica tions et	Expertis e des système s	Expertise économiqu e,

		Expertise télécom		Expertise en matériel informatique		Expertise judiciaire des documents électroniques	documents; signature électronique validation; forensic imaging ; metadata analysis	ues / expertise en preuves électroniques	supports numériques	d'information et logiciels	Évaluation des préjudices liés à la cybercriminalité
18.	Italy			Informatica forense		Forensic Cyber Examination, Perizia informatica – autenticazione documenti elettronici	Informatica forense; document metadata & signature checks; file system and	Peritaje informático forense / Perizia informatica	Perizia informatica su dispositivi mobili e supporti digitali	Pericia informática sobre programas y sistemas de información / Perizia informatica sui	Pericia económica de delitos informáticos

							format analysis			softwar e	
19.	Spain	Análisis de redes				Forensic Cyber Examina tion, Peritaje informát ico – autentica ción de documen tos electróni cos	Informá tica forense; e-docu ment authenti cation; metadat a & e-signat ure checks	Análisis de redes, Peritaje informát ico forense / Perizia informat ica	Análisis de redes, Perizia informatica su dispositivi mobili e supporti digitali	Análisis de redes, Pericia informá tica sobre progra mas y sistema s de informa ción / Perizia informa tica sui softwar e	Pericia económica de delitos informático s
20.	Portugal					Forensic Cyber Examina tion	Forense informá tica; electron ic docume nt verificat	Peritaje informát ico forense / Perizia informat ica	Perizia informatica su dispositivi mobili e supporti digitali	Pericia informá tica sobre progra mas y sistema s de	Pericia económica de delitos informático s

							ion; signatur e checks			informa ción / Perizia informa tica sui softwar e	
21.	Malaysia	Mobile & Network Forensics		Digital Forensics			Digital docume nt forensic ; metadat a analysis ; e-signat ure verificat ion where applica ble	Digital Forensic s	Mobile & Network Forensics	Digital Forensi cs	

LIST OF COUNTRIES, ORGANIZATIONS AND PROGRAMMES PROVIDING TRAINING, RETRAINING, PROFESSIONAL DEVELOPMENT AND SPECIALIZED EDUCATION FOR CYBER EXPERTS

№	Country	Specialized higher education institution providing training for experts specializing in the detection of cybercrime	Specialized training programme	Specialized field of study	Specialized retraining and professional development course
1	Estonia	TalTech & University of Tartu	“Tiger Leap” Programme – cartoons and educational activities on Internet safety for children		
2	Singapore	Singapore Institute of Technology, LSBF Singapore, University of East London	Cyber Wellness Programmes for Preschools (TOUCH); the “Cyber Wellness” Programme introduces children from preschool age to basic concepts of online risks		1) NUS-ISS; 2) Temasek Polytechnic (CET)
3	USA	George Mason University, University of New Haven, Champlain College, University of Arizona, Utica College, Stevenson University, Pace University, University of Advancing Technology, Regent	1. Common Sense Media, FBI Safe Online Surfing – teaching children about online safety through cartoons and games. 2. CISA (Cybersecurity and Infrastructure Security Agency) for K–5 students: guidance for children, teachers and parents on	Robert Morris University, University of Central Florida	1) USSS – National Computer Forensics Institute (NCFI); 2) CISA / NICCS Catalogue

№	Country	Specialized higher education institution providing training for experts specializing in the detection of cybercrime	Specialized training programme	Specialized field of study	Specialized retraining and professional development course
4	Ukraine	University, DeVry University, Oklahoma State University, ECPI University	security and protection of online information; certified activities and comics through the “CYBER.ORG” platform (featuring Pascal and Python characters).3. CyberPatriot (USA, Air Force Association) – the largest cyber defense competition programme for school students. Students learn to protect Windows/Linux systems and networks in virtual laboratories. The objective is to prepare future cyber experts and forensic specialists.4. GenCyber Camps – a programme for children aged 10–18 focused on cryptography and cyber defense. Ukraine – Diia.Education: Online Safety for Children – an online educational series developed through cooperation between the Ministry of Digital Transformation of Ukraine		

№	Country	Specialized higher education institution providing training for experts specializing in the detection of cybercrime	Specialized training programme	Specialized field of study	Specialized retraining and professional development course
5	China		and the Swatch-Ukrainian EGAP programme. It is aimed at educating children about harmful online content, blackmail, bullying and fraud, as well as developing a culture of gadget use Worldwide – DQ Every Child (#DQEveryChild) – a global digital citizenship and digital literacy initiative created in China and implemented by the DQ Institute. It has been introduced in 107 countries, involved more than 700,000 children, and translated into 21 languages		
6	Canada		Canada – MediaSmarts – provides resources and educational programmes for children and young people on media literacy, digital identity and Internet safety. It also develops materials for teachers,		1) Canadian Police College – TCLI;2) RCMP / CPC cooperation

№	Country	Specialized higher education institution providing training for experts specializing in the detection of cybercrime	Specialized training programme	Specialized field of study	Specialized retraining and professional development course
7	Latvia		including videos, time-management resources and quizzes 1. “Superheroes on the Internet” initiative, implemented through cooperation between Net-Safe Latvia and the State Police, promotes media literacy, online safety and digital citizenship among children		
8	Australia	Edith Cowan University	1. “Digital Thumbprint” Programme – designed for primary school students and implemented in a roadshow format across a number of schools, as well as through seminars with parents, providing guidance on online safety, effective communication and cyberbullying.2. Schools Cyber Security Challenges – a programme organized through cooperation between Australian universities and		1) TAFE NSW (with ACSC);2) AFP (Australian Federal Police)

№	Country	Specialized higher education institution providing training for experts specializing in the detection of cybercrime	Specialized training programme	Specialized field of study	Specialized retraining and professional development course
9	United Kingdom	Cranfield University, University of South Wales, University College Dublin	the government to teach school students online forensics and cyber analysis Cyber Discovery – a national government programme for students aged 14–18 (2017–2021). Digital Forensics, Ethical Hacking, Cryptography, Law & Cybercrime were taught. It has now been replaced by the Cyber Explorers platform	Cranfield University, London Metropolitan University, University of Wales Trinity Saint David	College of Policing
10	India	National Forensic Sciences University, Institute of Forensic Science, Lok Nayak Jayaprakash Narayan NICFS	Cyber Shikshaa Junior / Cyber Peace Foundation – a programme comprising specialized courses for school students on cybersecurity and digital ethics	Institute of Forensic Science	1) NFSU – National Forensic Sciences University; 2) CBI Academy / CyTrain

№	Country	Specialized higher education institution providing training for experts specializing in the detection of cybercrime	Specialized training programme	Specialized field of study	Specialized retraining and professional development course
11	New Zealand	University of Waikato, Auckland University of Technology			
12	Saudi Arabia	Naif Arab University for Security Sciences			NAUSS (Naif Arab University for Security Sciences)
13	Switzerland	University of Lausanne, École des sciences criminelles			1) University of Lausanne (UNIL) – ESC; 2) Bern University of Applied Sciences (BFH)
14	Germany	Ruhr-Universität Bochum, Horst Görtz Institute, Saarland University / CISP A			
15	Myanmar	Info Myanmar University			

№	Country	Specialized higher education institution providing training for experts specializing in the detection of cybercrime	Specialized training programme	Specialized field of study	Specialized retraining and professional development course
16	Norway	Noroff University College			Noroff University College
17	Iraq			Leiden University of Applied Sciences	
18	Netherlands				1) Netherlands Forensic Institute (NFI) Academy; 2) Police Academy of the Netherlands
19	UAE				Dubai Police Academy

**LIST OF SPECIALIZED FORENSIC EXAMINATION CENTERS THAT
PROVIDE FORENSIC OPINIONS EXCLUSIVELY IN RELATION TO
CYBER OFFENSES AND CYBERCRIMES**

№	Country	Names of Forensic Examination Centers
1.	USA	FBI Regional Computer Forensics Laboratory (RCFL) тармоғи
2.	Canada	RCMP National Digital Forensics Program / Digital Forensics Services
3.	United Kingdom	National Crime Agency (NCA) / Forensic Capability Network (FCN) рақамли криминалистикаси
4.	France	Institut National de Police Scientifique (INPS) (Polices Scientifiques)
5.	Germany	Bundeskriminalamt (BKA) – IT-Forensik
6.	Netherlands	Netherlands Forensic Institute (NFI) – Digital & Biometric Traces
7.	Sweden	Nationellt Forensiskt Centrum (NFC)
8.	Norway	Kripos – National Cybercrime Centre (NC3)
9.	Spain	Policía Nacional – Scientific Police (BIT/Информатика форензика бўлимлари), Guardia Civil лабораториялари
10.	Italy	Polizia Postale e delle Comunicazioni; Carabinieri RaCIS/RIS ва Reparto Tecnologie Informatiche
11.	Poland	Centralne Laboratorium Kryminalistyczne Policji (CLKP) – IT-форензика
12.	Belgium	NICC/INCC (Institut National de Criminalistique et de Criminologie)
13.	Finland	National Bureau of Investigation (KRP) Forensic Laboratory – Digital Forensics
14.	Australia	Australian Federal Police Forensics (ва штат лабораториялари) – Digital Forensics
15.	Japan	National Research Institute of Police Science (NRIPS)

16.	South Korea	Supreme Prosecutors' Office – Digital Forensic Center
17.	Singapore	Home Team Science & Technology Agency (HTX) Forensics Centre; Singapore Police Force DF бўлинмалари
18.	UAE	Dubai Police Forensic Science Dept. – Digital Forensics
19.	India	National Cyber Forensic Laboratory (NCFL) – I4C (MHA)
20.	China	Institute of Forensic Science (MPS)
21.	Kazakhstan	Ministry of Justice – Forensic Examinations Centre
22.	Italy	Carabinieri – RaCIS/RIS таркибида Reperto Tecnologie Informatiche

CHAPTER V. IMPROVEMENT OF SCIENTIFIC RESEARCH AND CYBERALOGY METHODOLOGY

5.1-§. The Concept of Cyberalogy, Its Content and Essence, and Its Significance

The rapid development of information and communication technologies, the digitalization of all sectors, and the penetration of artificial intelligence and innovative technologies into all areas are creating a need to study the cyber environment, including relations pertaining to cyberspace.

In the Address of the President of the Republic of Uzbekistan, particular emphasis was placed on the need to increase high-income services such as IT, artificial intelligence, fintech, consulting, and transport and logistics. It was stated that in 2026, the operation of 4 “Data Centers”, 2 supercomputers, and artificial intelligence laboratories at 15 higher education institutions would be launched in the city of Tashkent, Bukhara, Fergana and Tashkent regions, which would serve to implement more than 100 artificial intelligence projects in such important areas as healthcare, transport, agriculture, geology, banking and finance, and public safety⁴⁸⁹. This indicates that attention to information and communication technologies is being elevated to a new level, creating a need for a unified discipline to systematically study the broad range of relations in this area. This discipline will make it possible to study the methods and conditions for implementing reforms in a systematic manner. The Head of State emphasized that wherever there are new technologies and highly qualified professionals, there is growth and development in that sector⁴⁹⁰.

Thus, in order to ensure the availability of new technologies and qualified professionals, there is a need for a discipline that systematically studies all relevant relations. Furthermore, the Decree of the President of the Republic of Uzbekistan “On the Strategy “Uzbekistan – 2030” dated 11 September 2023 № DP–158 also attaches particular importance to information and communication technologies, and the development of these technologies, in turn, necessitates the training of qualified professionals. However, due to the autonomy granted to higher education institutions, education in the public and private sectors is developing on the basis of different approaches. This, in turn, is creating a number of difficulties in ensuring the timely, high-quality and proper implementation of the tasks envisaged by the “Uzbekistan – 2030” Strategy and adopted legislative acts, as well as in providing personnel whose qualifications are comprehensively aligned with practical requirements.

Firstly, there is a lack of systemicity in education, that is, at present, there is no single officially recognized methodology or textbook for systematically teaching cyberspace-related relations. Existing curricula are not specialized in practical professions (cyber-investigator, cyber-prosecutor, cyber-expert, etc.). Even though the number of existing textbooks has increased and their content has also become

⁴⁸⁹ <https://president.uz/uz/lists/view/8834>.

⁴⁹⁰ <https://president.uz/uz/lists/view/8834>.

diverse, none of them is oriented toward a comprehensive, broad-based and consistent system of personnel training; it is not possible to independently train a specialist in the field of cybersecurity, such as an officer of an operational-search body, cyber-inquirer, cyber-investigator, cyber-prosecutor, cyber-judge or cyber-expert, through the complete mastery of any single textbook or set of textbooks at educational institutions.

Secondly, there are inconsistencies in legislation, namely, there is a need to clarify the relationship between certain concepts in the Law of the Republic of Uzbekistan “On Cybersecurity” dated 15 April 2022 № LRU–764. In particular, Article 3 of this Law does not establish a relationship between the concepts of “cybersecurity”, “cybercrime” and “cybersecurity objects”, and the logical relationship between these three concepts is not sufficiently disclosed. For example, although cyberattacks are directed not only at information systems but also at other resources, the Law itself defines cybersecurity as the state of protection of the interests of individuals, society and the state in cyberspace from external and internal threats, while identifying only information systems as an object, thereby failing to take into account the fact that, in practice, cyberattacks are carried out not only against information systems but also against other resources. In addition, the concept of “cyberspace” is also defined incorrectly, as the definition refers to a virtual environment created using information technologies, while it remains unclear what type of space an environment created using artificial intelligence and telecommunications technologies constitutes. Moreover, the definition given to cyberspace is linked to the concept of an environment; taking into account that there is a significant distinction between the concepts of “space” and “environment” from an etymological and lexical perspective, certain provisions of the Law of the Republic of Uzbekistan “On Cybersecurity” dated 15 April 2022 № LRU–764 do not fully cover the practical needs of the present day. In our view, training specialists under legislation that does not sufficiently meet the relevant requirements is creating all the necessary conditions for the emergence of the various one-sided approaches listed above.

Thirdly, there is a lack of practical skills, namely, there are no artificial “cyber ranges” necessary for training specialists, which limits the ability of personnel to counter real threats. In foreign countries, a cyber range is fully artificially prepared for future cybersecurity personnel, and specialists become qualified professionals by performing practical tasks. In our Republic, however, there are not sufficient cyber ranges to ensure that the personnel being trained become superior to cybercriminals and acquire comprehensive and all-round skills for working with them.

Fourthly, ineffective awareness-raising, namely, awareness-raising activities among the population sometimes serve to indirectly teach methods of committing cybercrimes or to cause unjustified panic among the population. As a result, one of the factors contributing to the increase in the number of registered cybercrimes in our Republic from 863 in 2020 to 58,800 in 2024, representing a 68.13-fold increase, is precisely this awareness-raising. In our view, the situations arising from this incorrect approach based on excessive meetings and being disseminated through networks are also contributing to the fact that, after frightening the population into

panic and alarm by telling them not to give out their code (password), social media personal accounts can now be taken over without a password or code, with a second user gaining access, subsequently obtaining full control and carrying out unlawful actions in the account holder's name, as well as causing damage to business entities by generating counterfeit receipts from terminals. The need to improve these forms of awareness-raising in full is creating the necessity of changing the public mood in a positive direction. No one can guarantee that, by holding meetings under the name of cyber-awareness and teaching everyone the methods of committing cybercrimes, a criminal will not attend such meetings or watch them on social networks and acquire these skills free of charge. It should be noted that in developed countries, cyber-awareness is mainly conveyed to the population in the form of cartoons and films, or by exposing and apprehending criminals, from the perspective that the state's resources and capabilities are sufficient to ensure comprehensive cybersecurity.

Fifthly, today it has become common practice to use numerous words associated with the word "cyber", while no organization has shown interest in, or sufficiently addressed, the question of whether this term is being used correctly and how its etymological and lexical aspects should properly be applied; despite speaking about "cybercrime" every day, the definition of this concept is still absent from our legislation. This naturally raises the question: how, then, are the criminal-law, civil-law and other legal aspects of cybercrime being studied?! At present, the legal aspects of something that does not exist in legislation are being taught.

Sixthly, a student ultimately learns a field based on the techniques taught by their teacher. However, it should also be noted that the number of specialists whose scientific works have been placed on the Ziyonet network does not even reach 20; due to the lack of a sufficient number of teaching personnel, the number of specialists possessing sufficient knowledge and skills in cybersecurity is extremely small, and their place is currently being taken in the training of national personnel by specialists who lack knowledge in this field but possess skills in working with artificial intelligence, in other words, who simply know "computers", as well as foreign specialists who do not know national legislation and the specific characteristics of the sector and the region.

Failure to resolve the above problems will create systemic and strategic problems for the Republic of Uzbekistan in the future. In this regard, we consider it appropriate to implement the following solutions to address these problems:

Firstly, in order to resolve the above problems, it is appropriate to introduce the fundamental discipline of "Cyberology". This discipline integrates such areas as cyberlaw, cybersecurity, cyberpsychology, cybertechnology and sociology, and personnel trained on its basis will be developed not only as IT specialists, but also as cyber judges, cyber investigators, cyber inquirers, cyber prosecutors and experts and specialists in digitalization. As a result, the textbooks currently taught, such as cybersecurity, fundamentals of cybersecurity, cybersecurity law, cybercrime law, fundamentals of information security, information security, cyberlaw, data science, digital law and other similar disciplines, will be fully integrated and adapted into a single methodology. Most importantly, the classifier should be fully reviewed and

adapted accordingly. This discipline is a single fundamental discipline that systematically teaches cyber relations, in which the word “cyber” means “control”, the abbreviation “a” represents a unified abbreviation of the words information, informatization and communication, while “logy” is derived from the word “logos” and means “science, doctrine”. In addition to being the fundamental discipline integrating all of the above-mentioned disciplines, Cyberalogy is considered the key to all cyber-related disciplines. Within this discipline, all relations relating to cybercrime, cybersecurity, cyberlaw, technology, psychology and political science are studied systematically with a focus on practical personnel training. A specialist who completes this discipline will not only be qualified to work in the fields of public services, digitalization and cybersecurity, but will also acquire comprehensive skills to work as a cyber officer of an operational-search body, cyber inquirer, cyber investigator and cyber judge.

Secondly, the Law of the Republic of Uzbekistan “On Cybersecurity” dated 15 April 2022 № LRU–764 should include provisions on Cyberalogy and establish that the cyber education system should be based on it; the definition of the concept of “cybercrime” should be provided for in this Law and the Criminal Code; furthermore, the concept of “cyber environment” should be introduced into this Law, while the definitions of “cyberspace” and “cybersecurity object” should be reconsidered; the specific types of cybercrimes should be taken from the UN Convention against Cybercrime of 2024 and further developed on its basis.

Thirdly, Uzbekistan needs to carry out a number of reforms in order to fully expose and apprehend cybercriminals. In particular, today the majority of cybercriminals are women, while the punishment applicable to them under our legislation is very lenient; although gender equality is emphasized, the crime is also increasing because, in applying punishment for a crime, we treat women as vulnerable. Therefore, it is necessary to fully revise the Criminal Code, provide for specific types of cybercrimes, strengthen their sanctions, and remove from the mitigating circumstances the fact that a cybercrime was committed by a woman, or introduce an appropriate addition. It is also necessary to create an artificial cyber range and, through artificial traps, make effective use of Article 69 of the Criminal Code to temporarily delay the commencement of investigations against criminals for a period of two years, while preserving their exact number, location and all evidence of the acts they have committed, and to study them closely. Furthermore, a temporary moratorium should be declared on liability for persons who have committed cyberattacks against the websites of state bodies and organizations and fully disclosed how such attacks were committed; through this, it would be possible to further strengthen the cybersecurity of websites. Most importantly, it is necessary to establish the lawful activities of “white hackers” and introduce mechanisms for incentivizing persons who assist in exposing individuals who have committed cybercrimes. This would make it possible to create a genuine practical cyber range; if a cybercriminal communicates with a cybersecurity specialist, it would be possible to understand their inner world and determine the level of threat they pose.

Fourthly, it is necessary to abandon empty meeting-based activities and, by instilling a culture of cybersecurity through cartoons, films and infographics,

increase and demonstrate materials showing the capabilities and strength of state bodies; in order to prevent cybercrime, the best approach against a cybercriminal is psychological pressure. It should be explained that a cybercriminal committing a cybercrime in Uzbekistan may be subject to liability under aggravating circumstances, and that it is preferable to follow the path of “white hackers”. It is appropriate to act promptly, understanding that attacking a minority is preferable to protecting the majority. It should be emphasized and demonstrated through mass media and web resources that cybercriminals are apprehended and held liable and that mitigation is not applied; only then can cybercrime be sharply reduced, and education and doctrine should be structured accordingly.

Fifthly, it is appropriate to clearly establish that the word “cyber” is linked to “cyber environment, including cyberspace” and “information and communication technologies”, and to clearly define that information technologies, artificial intelligence, telecommunications technologies and other technologies constitute information and communication technologies, while specifying not only the precise subject matter, purpose and objectives of the discipline of Cyberalogy, but also those of other disciplines. This would enable users to learn to use the word “cyber” correctly and ensure that education is also carried out systematically.

Sixthly, it is appropriate to establish and maintain an accurate register of practical and academic specialists who have conducted scientific research on cyber-related relations, systematically improve their qualifications, and transition to systematic training of specialists by imposing on them the obligation to teach and engage in scientific activities at higher education institutions in return for the free professional development they have received. By ensuring free professional development abroad for qualified specialists and directing their knowledge toward the training of national personnel, it will be possible to train specialists who meet both national and international requirements.

Properly conducted education will serve not only to ensure cybersecurity, but also to train specialists capable of ensuring the full protection of the Republic of Uzbekistan from internal and external threats, as well as ensuring human rights and interests and the rule of law. Therefore, the practical application of these subjective views constitutes an urgent task today. The adoption of this proposal will ensure that both legislation and education are directed toward a correct, systematic, comprehensive and broad-based methodology. The introduction of the discipline of Cyberalogy and the systematization of legislation in this field will serve to strengthen Uzbekistan’s sovereignty in cyberspace, ensure human rights and uphold the rule of law.

5.2-§. Methodology for Preparing Information and Analytical Materials, Articles, and Theses Based on the Cyberalogy Method and Its Significance for the Development of Science

Today, the state is carrying out the necessary reforms by employing various methods and forms of its regulatory function. One such method is the **approach of adopting the relevant legislative act on the basis of an information and analytical material**, which is currently being used by nearly all state research institutions to present the results of their research by submitting them to the Government, relevant state bodies, and other entities.

At the same time, with regard to how information and analytical materials should be developed and the requirements applicable to them, based on the proposal of the Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan, a **scientific manual** on the preparation of scientific research and analytical materials was approved by Minutes No. 8 of the Coordinating Council for Strategic Planning and Development under the President of the Republic of Uzbekistan dated March 12, 2026.

Accordingly, the requirements for information and analytical materials to be prepared for research conducted within the scope of the activities of the **10 analytical centers and research institutions** whose activities are organized by the Coordinating Council for Strategic Planning and Development under the President of the Republic of Uzbekistan, as approved by Decree № DP–201 of the President of the Republic of Uzbekistan dated October 30, 2025, have been established⁴⁹¹.

As a result, the opportunity has been created to establish a unified legal practice by adapting at least ten different forms of information and analytical materials prepared by the 10 analytical centers and research institutions to a single format.

Although important steps have thus been taken toward unifying the activities of the analytical centers and research institutions operating within the Coordinating Council for Strategic Planning and Development under the President of the Republic of Uzbekistan, certain shortcomings still remain in practice. This also affects the further development of reforms, as the **process** lacks a sufficiently developed **comprehensive, integrated, and systematic approach**.

In particular, the **insufficient harmonization of theory and practice**, as well as differences in the scope of knowledge and mutual understanding between researchers and implementers, result in advanced ideas not being fully reflected in strategic documents and in the emergence of conflicts and legal gaps in adopted legislation. In addition, the conclusions of materials often propose establishing another working group; however, a **draft legislative act that constitutes a concrete, existing or future problem-oriented, idea- and data-based solution to**

⁴⁹¹ List of analytical centers and research institutions whose activities are organized by the Coordinating Council for Strategic Planning and Development under the President of the Republic of Uzbekistan, approved by Decree №. DP–201 of the President of the Republic of Uzbekistan dated October 30, 2025 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

the actual problem, that is, a ready-made product, is not attached. At the same time, the fragmented use by researchers of various approaches, such as IMRAD, Case Study, or Narrative without any particular structure, is leading to **methodological fragmentation**.

The most effective way to eliminate these problems and transform the ongoing reforms into a digital format is to introduce the **Cyberalogy Method** as a unified standard. At a time when information and communication technologies have penetrated all areas and artificial intelligence operates on the basis of precise algorithms, analytical materials must also be written in an algorithmic format that can be automatically understood not only by humans but also by technologies. The **science of Cyberalogy** unifies the cyber environment and the relations associated with it under a single fundamental umbrella. According to its golden rule, any reform or proposal must be presented in the fastest, technologically flawless, and algorithmically sequential manner, and must be sufficiently simple, precise, and concise to be firmly retained in the reader's memory.

The difference between the traditional method and the Cyberalogy method can be clearly demonstrated through a specific legal and practical situation. For example, when an authorized body analyzes crimes committed through the use of information and communication technologies as provided for in the Criminal Code, the traditional method involves presenting dozens of pages of abstract text, general information about the history of the Internet, and statistics, followed simply by a proposal to establish a commission or strengthen oversight.

Under the Cyberalogy method, this process is carried out in a highly concentrated form, and the information and analytical materials specify the following:

the existing situation and the problem;

algorithmic national and international **analyses and their results;**

as an **exact solution**, a ready-made draft law specifying exactly what wording or provision should be added to the relevant article of the Criminal Code is attached. If such an approach were widely applied, particularly in the activities of research institutes, institutions, and even councils of young scientists and analytical groups operating under them, it would ensure that subjects authorized to adopt legislative acts receive comprehensive, well-developed, finalized solutions that are substantiated from both legal and technological perspectives.

According to the **Cyberalogy method**, any information and analytical material, article, or thesis must consist of strictly defined algorithmic structural components. In the **Introduction** section, the document on the basis of which, or the instruction pursuant to which, it is being prepared, the purpose of the research, the participants, and the relevant period are indicated, thereby forming, as it were, the **metadata** of the document. This enables the decision-making entity to understand the purpose within seconds. Then, in the **Main Part**, in order to systematically diagnose the problem, the existing state of legislation, the real symptoms and causes of the problem, theoretical proposals of scholars, foreign experience, and available national resources are compared and analyzed, resulting in the formulation of a specific data-based idea. The **Conclusion** section, in turn, is directly oriented toward

implementation. Here, a cost-effective and highly effective **specific proposal** for resolving the problem – necessarily together with the text of the relevant draft legislative act – as well as the **implementation mechanism**, including the distribution of tasks, deadlines, responsible implementers, and the **socio-economic benefits to be achieved** as a result of the proposal, are clearly and understandably specified. At the same time, if the relevant legislative act specified in the concrete proposal section of the conclusion is a highly complex, time-consuming, or comprehensive instrument aimed at regulating new relations, it would be appropriate to present a model of the draft, together with its structural components, instead of the full text.

In conclusion, preparing information and analytical materials, articles, and theses **on the basis of the Cyberalogy method** and introducing it as a unified national standard will serve to save time and resources and eliminate unnecessary bureaucracy and excessive paperwork. This method will not only accelerate genuine innovative reforms but will also, in the near future, create a **strong fundamental basis for continuously analyzing the system of public administration and law-making through artificial intelligence and digital technologies**.

Now, as a practical application of this proposal, let us provide a solution to one particular issue. It is well known that all citizens working in the public, non-governmental, and private sectors pay taxes on their income; however, unfortunately, bloggers engaged in advertising activities still do not pay taxes. Admittedly, there are cases where this issue is addressed through registration as a business entity or as a self-employed person. However, this approach can also constitute tax evasion. The reason is that everyone knows the amount of a particular advertising post, its duration, audience size, and so forth. While bloggers do not pay taxes, citizens who are barely making ends meet do pay taxes, and bloggers or influencers also use the infrastructure created as a result of those tax payments. The violation of the principles of rationality, fairness, and equality requires an in-depth study of this issue.

Many organizations have conducted research on this issue and have put forward their proposals. Based on the above, we intend to propose an entirely different approach.

Title of the research: *“Taxation and Regulation of Influencers: Problems and Solutions”*.

Introduction:

“Pursuant to paragraph 12 of the 2026 Scientific and Practical Research Plan of the Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan, in cooperation with the responsible representatives of 10 interested ministries and agencies in accordance with the annex, 5 non-governmental non-profit organizations, 8 mass media outlets, and approximately 3,500 informatization entities, and through the discussion process conducted in the form of a **brainstorming session** on March 12, 2026, with the participation of responsible representatives of 21 ministries and agencies, 13 mass media outlets, and 54 prominent user-bloggers with more than 10,000 subscribers, the issue of taxing informatization entities deriving income from advertising activities through the use

of telecommunications networks and the Internet during January–April 2026 was studied.”

Main Part:

1) Current situation and problem:

“Nowadays, influencers are exerting a strong influence on the market economy and consumer culture. Their advertisements and recommendations are not only managing demand, but also affecting price formation in the market and consumers’ selection of quality and necessary goods.

For information: According to statistical data, approximately 60–70 percent of buyers trust influencers’ recommendations more than traditional advertising. Therefore, while the share of this type of activity in the global market amounted to 24 billion US dollars in 2024, this figure amounted to 35 billion US dollars in 2025. The main share of influencers’ income still comes from the *Instagram* platform (approximately 30 percent share) and the rapidly growing *TikTok* platform.

At the same time, the rapid development of the digital economy and the transformation of the advertising market into the Internet segment necessitate the legal regulation of influencer activity and the improvement of the system of their taxation. This necessity is substantiated by the following factors:

Firstly, the absence in national legislation of the concept of “influencer”, their legal status, as well as the scope of their obligations, is creating a “legal gap”. This, in turn, is leading to high-income individuals not being subject to taxation, consequently resulting in the violation of the principle of social justice among bona fide taxpayers, as well as the formation among the general public of destructive views aimed at “earning money effortlessly and easily”;

Secondly, the fact that goods and services promoted by influencers in most cases do not comply with the requirements of the current legislation and cause harm to the material and moral interests of consumers is having a negative impact on the environment of “fair competition”. This, in turn, is leading to an increase in systemic disputes in relations between producers, advertising distributors and consumers;

Thirdly, the lack of clear legal delineation of the boundaries of liability among participants in the advertising process (advertiser, performer and influencer) is creating difficulties in restoring the interests of citizens whose rights have been violated. As a result, there is a growing number of justified objections among the population regarding the effectiveness of the supervisory functions of authorized state bodies”;

2) Algorithmic national and foreign analyses and their results:

“The most effective way of regulating this activity is taxation; however, a comprehensive tax mechanism for this purpose has not been formed in Uzbekistan, and the shadow economy continues to exist.

There are some incorrect approaches in this regard. For example, the former Agency for Information and Mass Communications had proposed defining an influencer as “a blogger with more than 10,000 subscribers”. Some experts propose taking only the number of subscribers or views as the basis for the tax base. However, these criteria do not justify themselves for the following reasons:

firstly, on some platforms, it is technically possible to conceal statistics from third parties;

secondly, it is possible to artificially manipulate and increase indicators (views, subscribers, information transmissions, etc.) through certain bot systems;

thirdly, in practice, there are also resources that have a small audience but high commercial conversion and conduct large-scale sales.

At the same time, it was determined that, when taxing influencers, it would be appropriate to take into account the following existing resources and reforms, including:

registering influencers as business entities may give rise to negative public discussions due to the influence of bloggers on the general public;

registering influencers as business entities and licensing their activities is not consistent with the reforms being carried out in this area and with the legal status of a “blogger” under the Law “On Informatization”;

the most effective way of taxing influencers is to establish the following, using the accumulated practice and foreign experience in product marking through the “Asl belgisi” system, marking through a tax partner, and using broad public participation in reporting violations of tax legislation, in particular:

a) marking or digital tokenization through the “Asl belgisi” system before influencers place advertising-related information on the telecommunications or Internet network;

b) establishing mandatory registration with the tax authorities, through the electronic public services portal of the tax authorities, of contracts concluded between advertisers and distributors;

c) establishing the practice of submitting monthly tax reports by advertisers and distributors for each advertisement distributed on the telecommunications or Internet network;

d) establishing liability for placing unmarked advertising-related information on the telecommunications or Internet network and for failure to register an advertising contract, and determining the effective use by the general public of the tax cooperation system through the Electronic Public Services Portal of the Tax Authorities (Soliq-mobile).

In foreign countries, this concept and related relations are regulated by separate laws. For example, this term is reflected in the legislation of **more than 30** countries as “commercial influencers” in **France**, “influencer” in **Kazakhstan**, “advertising distributor” in **Russia**, “users of particular significance” in **Spain**, and “media service providers” in **Germany**.

In more than **40** countries of the world, **digital marking of Internet advertising** has been firmly established for the purpose of taxing influencers.

For information: *Austria, Australia, the United States, Argentina, Belgium, the United Kingdom, the UAE, Brazil, Hungary, Vietnam, Germany, Greece, Denmark, South Korea, Ireland, Spain, Italy, Indonesia, India, Canada, China, Kazakhstan, Qatar, Latvia, Lithuania, Luxembourg, Malaysia, Mexico, the Netherlands, Norway, Poland, Portugal, Russia, Romania, Saudi Arabia, Singapore, Thailand, Türkiye, Ukraine, the Philippines, Finland, France, the Czech Republic, Switzerland, Sweden, Estonia, and Japan are considered countries that strictly apply digital marking of Internet advertising.*

In addition, in **more than 80 foreign countries**, the activities of influencers are licensed or carried out on the basis of a permit, and they are registered with the state as **business entities and submit tax reports**.

***For information:** Austria, Australia, the United States, Argentina, Albania, Andorra, Armenia, Azerbaijan, Belgium, Bulgaria, Brazil, the United Kingdom, the UAE, Hungary, Vietnam, Germany, Greece, Georgia, Denmark, Egypt, Israel, India, Indonesia, Ireland, Spain, Italy, Jordan, Kazakhstan, Canada, Cyprus, China, Colombia, the Republic of Korea, Kyrgyzstan, Kuwait, Qatar, Latvia, Lithuania, Luxembourg, Malaysia, Malta, Morocco, Mexico, Moldova, the Netherlands, Norway, Oman, Pakistan, Poland, Portugal, Russia, Romania, Saudi Arabia, Serbia, Singapore, Slovakia, Slovenia, Thailand, Türkiye, Turkmenistan, Ukraine, the Philippines, Finland, France, Croatia, the Czech Republic, Chile, Switzerland, Sweden, Estonia, the Republic of South Africa, Japan, Algeria, Bahrain, Ecuador, Ethiopia, Ghana, Iceland, Kenya, Liechtenstein, Mauritius, Nigeria, New Zealand, Panama, Peru, Seychelles, Tunisia, and Uruguay require the licensing of influencers' advertising activities and their state registration as business entities, as well as the submission of tax reports.*

*At the same time, in **Russia**, before placing advertising-related information on a telecommunications or Internet network, **tokens** are obtained from a special automated system. In **Kazakhstan**, advertising distributed through the network must first be marked and subsequently distributed through a special mark (tag), while bank transactions of advertising distributors are monitored. In **Belarus**, advertising distributors are required to be entered into a mandatory register in advance and only thereafter may they distribute advertising information; taxation is also withheld by cross-referencing advertising distributors with their bank transactions.*

In all three states, comprehensive liability is provided for violations of advertising requirements.

Accordingly, it was determined that, in international practice, **4 main models** of taxing influencers have currently emerged:

1) "Tax agent – platform" or automated control model. Under this model, the principal tax burden is imposed not on the influencer, but on the digital platform making the payment (YouTube, TikTok, Instagram) or its advertising agency, and the influencer is required to conclude a contract with them. According to this model, the influencer's taxes are mandatorily directed to the budget based on the principle of mandatory withholding of tax from income earned before the income is credited to the influencer's bank account (Tax Deducted at Source);

***For information:** 25 countries in North and South America, including the United States, Canada, Mexico, Brazil, Argentina, Chile, Colombia, Peru, Uruguay, Paraguay, Ecuador, Bolivia, Costa Rica, Panama, Guatemala, Honduras, El Salvador, the Dominican Republic, Jamaica, Trinidad and Tobago; 22 countries in Europe and Oceania, including the United Kingdom, Germany, Japan, Australia, Austria, Belgium, the Netherlands, Luxembourg, Switzerland, Sweden, Norway, Denmark, Finland, Iceland, Ireland, New Zealand, Papua New Guinea, Fiji; and 58 countries in Asia and Africa, including South Africa, Nigeria, Kenya, Ethiopia, Ghana, Tanzania, Uganda, Senegal, Pakistan, Bangladesh, Sri Lanka, Vietnam, the Philippines, Malaysia, Israel, Jordan and other countries operate on the basis of this model.*

2) Model of special digital and simplified regimes. According to this model, with the aim of reducing the shadow economy, a separate legal status and preferential tax rates have been introduced for bloggers. In particular, a system has been created for registering activities without a declaration through special mobile applications and paying taxes at low rates (usually from 1% to 15%); furthermore, mandatory withholding of tax by banks and platform owners is provided for. The United States taxes Uzbek bloggers through this mechanism;

For information: In Kazakhstan, Belarus, India, China, South Korea, Türkiye, Indonesia, Taiwan, Thailand, Egypt and France, advertising must be distributed on the basis of a contract, and the bank must withhold tax from each transaction. For example, in Türkiye, 15% of the blogger's tax for advertising is withheld by the bank; in China, by the platform owner (Google, Meta, TikTok) or local banks; in Kazakhstan, a 1% mobile regime has been introduced; while in Belarus, the "State Register of Advertising Distributors" and a 10% professional income tax have been introduced.

3) Model of assessing not only commercial but also barter relations and in-kind income – full tax coverage model. Under this model, the focus is on taxing non-monetary income characteristic of influencer activity (gifts, travel, services, etc.); the market value of any product (PR packages) or service provided for advertising purposes is assessed as commercial income and included in the general tax base;

For information: In the United States, Germany and the United Kingdom, bloggers are required to pay income tax on the value of free gifts received from brands. Concealing this is considered tax evasion.

4) Professional entrepreneurship and expense deduction model – commercialized approach model. According to this model, blogging activity is regarded as a professional business generating high income, and they are granted the benefits provided for business entities; in order to encourage the transparency of income, influencers are granted the right to deduct production expenses (equipment, Internet, editing services) from their total income.

For information: In Australia, Canada and the Scandinavian countries, bloggers pay tax on net profit at progressive rates (from 10 percent to 50 percent).

Conclusion:

A) In the section on specific proposals:

"Based on the above, taking into account practice and making effective use of existing resources on the basis of foreign experience, it is proposed to adopt legislative acts providing for the following:

The Law of the Republic of Uzbekistan "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan", taking into account the following:"

The Law of the Republic of Uzbekistan "**On Advertising**"⁴⁹² shall define the concept of an "influencer" and clarify their role as an advertising distributor, establish requirements for advertising-related information disseminated on telecommunications or Internet networks, including its marking or digital tokenization, provide for the possibility of distributing advertising on the basis of a smart contract, and determine the rights and obligations of the advertiser and distributor in relation to advertising placed on the network, as well as their liability to consumers;

The **Tax Code** of the Republic of Uzbekistan⁴⁹³ shall provide, for the purpose of creating favorable conditions for influencers, for granting them relief when they advertise the works, goods and services of business entities by reflecting such

⁴⁹² Law of the Republic of Uzbekistan "On Advertising" dated 7 June 2022 № LRU-776 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴⁹³ Tax Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

activities in the monthly tax reports of the business entities, ensuring the prevention of duplicate tax reporting, and, in other cases, creating an opportunity for the influencer to reflect the profit received through their advertising in their monthly tax report and to eliminate discrepancies in the annual aggregate declaration upon its submission, as well as providing for tax liability of the taxpayer in cases where advertising-related information that has not been marked or digitally tokenized is allowed to be disseminated on telecommunications or Internet networks;

The **Code of the Republic of Uzbekistan on Administrative Liability** shall establish the administrative liability of individuals for the dissemination, through the Unified Automated Information System of the tax authorities, of unmarked or digitally untokenized advertising information on telecommunications or Internet networks, failure to submit tax reports, and failure to register an advertising contract with the tax authorities;

2) A special resolution of the Cabinet of Ministers concerning the following:

- approval of the procedure for maintaining an electronic automated register of influencer taxpayers engaged in advertising activities;

- establishing that the advertiser and the distributor shall bear equal responsibility for ensuring that it is visible to the user that the information being disseminated is advertising and that the possibility of using it is provided, and that the advertiser and distributor shall be required to conclude a smart contract or agreement concerning the distribution of advertising;

- taking into account the prevention of cyber incidents, introduction of a mandatory digital marking system through the “Asl belgisi” system for concluding a smart contract for the distribution of advertising and assigning a digital token to advertising information, as well as for concluding an electronic contract between informatization entities that do not conclude a smart contract and automatically generating a QR code;

- approval of the procedure and control rules for digital marking and tokenization of information resources, conclusion of smart contracts and other contracts concerning advertising, while providing for taxpayers, tax authorities and other organizations to determine, through the electronic public services portal of the tax authorities and the “Soliq mobile” application, whether an information resource disseminated on the telecommunications or Internet global information network has been marked or digitally tokenized through the “Asl belgisi” system, to combat inappropriate advertising, and to establish procedures for the digital marking of information resources;

- launching a system for incentivizing citizens who report unmarked Internet advertising through the electronic public services portal of the tax authorities and the “Soliq mobile” application;

- approval of an action plan for implementing the tasks established by the Government resolution and ensuring that the new procedures are sufficiently explained to the population and performers;

Amendments and additions shall be made to Resolution № 707 of the Cabinet of Ministers dated 5 September 2018 “On Measures to Further Improve Information

Security on the World Wide Web”⁴⁹⁴, providing for the restriction of access to an information resource containing unmarked and/or inappropriate advertising;

3. An order of the **Ministry of Digital Technologies of the Republic of Uzbekistan** “On Approval of the Rules for Provision of Services in the Field of Informatization” in accordance with Annex 3, providing for the procedure for the provision of services in the field of informatization by influencers alongside informatization entities.

B) In the section on the implementation mechanism:

“Assigning the Cabinet of Ministers to submit, in accordance with the established procedure, a draft legislative act to the Legislative Chamber of the Oliy Majlis on the basis of this proposal and, following its adoption, to adopt a Government resolution;

Assigning the Ministry of Digital Technologies, in coordination with the Representative for the Protection of the Rights and Legitimate Interests of Business Entities under the President of the Republic of Uzbekistan, the Prosecutor General’s Office, the State Security Service, the Committee for Development of Competition and Protection of Consumer Rights, the Tax Committee, and the Chamber of Commerce and Industry, to adopt an internal regulatory legal act;

Assigning the Tax Committee and the Ministry of Digital Technologies to introduce the technical capabilities provided for in the proposal into the “Asl belgisi” system, the electronic public services portal of the tax authorities, the “Soliq mobile” application, and the Single Interactive Public Services Portal;

Assigning the Ministry of Justice, the Chamber of Commerce and Industry, the Center for Preparation of Public Content, the National Television and Radio Company, and the Informatization Agency, together with the interested ministries and agencies, to take the necessary measures to explain the substance and significance of the legislative acts adopted as a result of this proposal;

C) Socio-economic benefits to be achieved:

the incomes of influencers will become transparent through the digital marking or tokenization of advertising information, which will ensure additional revenues to the budget;

the taxation of influencers, as representatives of all other sectors, will eliminate inequality and social discontent among bona fide taxpayers;

the marking or tokenization of each advertisement and its integration with the “Asl belgisi” system will enable consumers to clearly identify who is responsible for the quality of the product;

the promotion of low-quality and unlawful goods will decrease, thereby creating equal opportunities for local producers and bona fide entrepreneurs.

Accordingly, in conclusion, an information-analytical material, article and thesis consist of a specific problem, analysis and conclusion within the cyberalogy method; an information-analytical material does not include quotations from the resources analyzed, a list of references, or an abstract, and is aligned with the

⁴⁹⁴ Resolution № 707 of the Cabinet of Ministers dated 5 September 2018 “On Measures to Further Improve Information Security on the World Wide Web” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

technical requirements of newspapers and journals. General proposals give way to specific proposals. However, complex and incomprehensible methods such as IMRAD, IRDAC, systems analysis, case study, quantitative, qualitative, and Narrative are not applied in this method. At the same time, since the introduction of an article and thesis sets out the achievements attained and/or the tasks identified, the content of the introduction of an information-analytical material is changed; articles and theses do not envisage the editing of lengthy legislative texts, but rather indicate their content and model.”

It should be emphasized that the above-mentioned algorithmic format based on the cyberalogy method will serve as a solid fundamental basis in the future for the automatic monitoring of the implementation of legislation using artificial intelligence. At the same time, information-analytical materials, articles and theses created with the assistance of or by artificial intelligence will prevent plagiarism and research conducted on the basis of incorrect approaches. Our innovative proposal concerning the taxation of income derived from bloggers’ advertising can be applied not only to the advertising or tax sector, but also to other areas. For example, Article 12¹ of the Law “On Informatization” contains 13 prohibitive criteria⁴⁹⁵, and, based on the fact that all of them, including the Criminal Code⁴⁹⁶ and the Code of the Republic of Uzbekistan on Administrative Liability⁴⁹⁷, provide for liability for disseminating religious materials through telecommunications or Internet networks without undergoing religious studies examination, if someone intends to disseminate religious materials on the network, they may simply mark them, thereby creating greater convenience for believers in exercising freedom of conscience, reducing cases of using religion as a cover that threaten national security, and, most importantly, resolving existing problems related to inquiry and investigation concerning proof and evidence.

In this respect, it can also be stated that the cyberalogy method and discipline are distinguished by their distinctive features and advantages in all respects compared to the methods and disciplines of all other fields. Conducting scientific research in this area leads to the prompt resolution of the problem raised, finding its proper place, and, most importantly, its systematic solution, as well as ensuring that it is understandable to the population and implementers. Therefore, we need to give special consideration to the necessity of conducting research based on the cyberalogy method.

⁴⁹⁵ Law of the Republic of Uzbekistan “On Informatization” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴⁹⁶ Criminal Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

⁴⁹⁷ Code of the Republic of Uzbekistan on Administrative Liability // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

CONCLUSION

During the course of our research conducted on the topic “**Strategic-Digital Transformation of the State and Society: Problems and Solutions (under the section ‘Global Challenges: Problems and Strategic Solutions’)**”, the following fundamental scientific and practical conclusions were reached:

Chapter 1. On the Institutional Foundations of Public Administration and Administrative Reforms

1.1. Adoption of a separate Law of the Republic of Uzbekistan “On Executive Bodies of the Republic”, which would establish in detail a clear procedure for the establishment, reorganization and liquidation of ministries and agencies, criteria for the distribution of their functions, as well as the boundaries of their powers;

1.2. Development of the concept of “Gradual Elimination of Manual Management” in public administration, including a clear delineation of the powers and responsibilities of civil servants at each level; approval of a gradual roadmap for transition from “manual management” in decision-making to management based on legislation and normative documents;

1.3. For the purpose of improving the decentralization process:

Adoption of the Law of the Republic of Uzbekistan “On Administrative Decentralization” and establishment therein of the gradual procedure, timeframes and sources of financing for the transfer of powers of state bodies and organizations from the central to the local level;

Approval, on the basis of the “Uzbekistan – 2030” Strategy, of a clear roadmap for transferring at least 30 percent of the tasks and functions of republican executive bodies to local executive bodies;

1.4. Creation of a unified integrated platform and, through it, integration of the information systems of all state bodies on the basis of unified standards, as well as introduction of a system based on the principle of entering data once and enabling all agencies to use such data; acceleration of the launch of the Unified Digital Platform stipulated in the Address of the President dated December 26, 2025;

1.5. Introduction of a unified system for assessing the efficiency of public administration, including further improvement of the KPI system consisting of no more than 5–7 criteria, establishment of key indicators for each ministry and agency, and determination of the amount of financing, number of employees and incentive measures for ministries based on the results of KPI assessment;

1.6. Strengthening systematic efforts to eliminate bureaucratic barriers within the framework of the “Bureaucracy Elimination – 2030” Program – reducing the timeframes for consideration of proposals received through the “Zero Bureaucracy” digital platform and establishing specific target indicators for each ministry and agency regarding the elimination of bureaucratic barriers; taking prompt measures to eliminate bureaucratic barriers most frequently identified by citizens and entrepreneurs;

2.1. Creation of a unified digital register of benefits and preferences and, through the integration of the necessary information systems, including all information systems related to the accounting of benefits and preferences, introduction of the unified automated comprehensive information system **“Effectiveness of Benefits”**, based on artificial intelligence technologies and operated as an open platform, specialized in granting benefits and preferences, summarizing their results, and maintaining records of digital traces automatically in real time;

2.2. Approval by normative documents of a regulation on the procedure for granting benefits and preferences and determining their effectiveness;

2.3. Initially, on a pilot basis, determining the effectiveness of benefits and preferences granted in the areas of social protection and banking and finance, followed at the next stage by construction, digitalization, agriculture, transport, healthcare, education, the economy, as well as benefits and preferences granted to youth and women, and based on the pilot results, establishing digital assessment of effectiveness in the remaining sectors, industries and areas;

2.4. Creation of the following capabilities in the unified automated comprehensive information system “Effectiveness of Benefits”:

- obtaining accurate information on the number, name, value (amount), validity period of benefits and preferences, when and on the basis of which document, to which categories of entities, in which sector, industry and area (sector), and for what purposes they were granted;

- analysis, based on accurate data, of the achievements (results) obtained from each benefit and preference granted and the benefit and loss generated for the budget, as well as identification of budgetary losses;

- verification of whether entities granted benefits or preferences comply with the requirements of legislation on conflicts of interest;

- determination of whether entities granted benefits or preferences continue to meet the requirements necessary for such benefit or preference;

- ensuring transparency through the formation of an open state budget;

- establishing state and public oversight over the benefits and preferences being granted;

- checking and forecasting the expediency of granting additional and new benefits and preferences;

- determining whether existing benefits and preferences are justified and effective;

- formation of an automated conclusion based on artificial intelligence using the identified data;

- creation of special chatbots and a **mobile application** of the system to enable the public to view and discuss granted benefits and preferences and submit proposals;

- sending automatic notifications to individuals and legal entities regarding benefits and preferences granted to them through the Unified Interactive Public Services Portal and the electronic public services portal of tax authorities;

- ensuring information and cybersecurity;

3.1. Based on the Law of the Republic of Uzbekistan “**On Civil Service**”, development and adoption of a resolution of the President of the Republic of Uzbekistan “**On Approval of the Regulation on the Procedure for Rotation in the Civil Service**”, providing for the procedure for rotation in the civil service, a list of civil service positions subject to mandatory rotation, as well as the period of service in positions subject to rotation;

3.2. Supplementing the Law of the Republic of Uzbekistan “**On Civil Service**” dated August 8, 2022, № **LRU–788**, with Article 42¹ in the following wording:

“Article 42¹. Certification of a Civil Servant

Regardless of the category of a civil servant, he or she shall undergo certification once every three years based on professional competence through a commission established by the specially authorized state body.

The composition of the commission shall be approved by the specially authorized body.

The certification questions shall be published on the official website of the specially authorized state body at least three months before the certification.

The list of employees required to undergo certification shall be formed by the specially authorized body, and the candidate shall be notified at least one month before the certification.

Notification of the candidate shall be carried out by sending an SMS notification and submitting a notification to the state organization where the candidate performs his or her activities.

Responsibility for ensuring that the civil servant undergoes certification in a timely manner shall rest with the head of the organization where the civil servant performs his or her activities, the specially authorized body and the candidate.

Certification processes shall be broadcast live on the official website of the specially authorized body, and certification questions shall be provided through an automated selection process free from human intervention.

The results of certification shall be determined in the form of “passed” or “failed.”

A civil servant who scores more than 56 points in the certification shall be considered to have passed.

Failure of a civil servant to pass certification shall constitute grounds for termination of the employment contract concluded with him or her or transfer to a position one level lower than his or her current position.”;

3.3. Development of the “Civil Service” comprehensive information system on the basis of the interagency software and hardware complex “**Unified National Labor System**”, and integration within it of the existing unified open portal of vacant civil service positions (“vacancy.argos.uz”), the automated information system “samaradorlik.uz” (samaradorlik.uz), and the electronic platform “hrm.argos.uz”, as well as integration with the following information systems:

the unified electronic case management system for administrative offenses (“E-ma’muriy ish” system) and the “Electronic Criminal Case” information systems,

in order to obtain information on a person's criminal record and information concerning the person held by law enforcement, supervisory and judicial bodies;

the "E-antikorrupsiya" open portal for information concerning corruption and conflicts of interest involving the person;

the "Xorijda ish" electronic software complex for information concerning the person's employment in a foreign state;

the Unified Interactive Public Services Portal for personal and family status, property, places of employment and study, and other interactive information concerning the person;

3.4. The newly developed information system shall consist of artificial intelligence technologies based on neural technologies and shall have the capability to automatically provide all information concerning the civil service, without human intervention, only to authorized persons with restricted access (only to the employer);

4.1. Creation of a unified digital platform for human capital monitoring, including launching a unified digital platform for human capital monitoring based on the OECD's "lifetime income approach" and PIAAC methodology;

4.2. Improvement of the regional labor resources balance, in particular, by encouraging internal migration and directing surplus labor resources (from the Fergana Valley) to areas where demand for labor is high (new industrial zones);

4.3. Strengthening the integration of science and production, including establishment of dual education clusters through cooperation among higher education institutions, research institutes and enterprises, and establishing mechanisms for the rapid implementation of scientific developments into production;

4.4. Reforming the system of retraining and professional development, in particular, establishing that each employee must undergo professional development at least 3–4 times during his or her employment;

4.5. Introduction of a system for assessing the effectiveness of investments in human capital, including development of indicators determining the contribution of state budget funds to human capital;

4.6. Annual forums under the slogan "**Human Capital – the Pillar of the Motherland**" should be held in each region, where local talents are introduced and their achievements are widely publicized;

5.1. Amendments and additions to the Law of the Republic of Uzbekistan "On Appeals of Individuals and Legal Entities" providing for the following:

proactive appeal models;

a system for automatic random distribution of appeals in Uzbekistan;

requirements for the professional competence of employees handling appeals;

the procedure for considering appeals widely discussed on social networks and mandatory participation of press secretaries therein;

categories and procedures of appeals subject to mandatory consideration with the participation of mass media and through videoconferencing;

mandatory requirements for specialized systems for handling appeals;

the procedure for using specialized systems for handling appeals;

mandatory requirements for appeals submitted through specialized systems for handling appeals and responses thereto, as well as their digital monitoring in real time;

granting the applicant the right to be heard as the applicant's final statement regarding decisions on rejection;

abolishing the institution of explaining the right to refer an appeal to another competent organization and, in cover letters forwarding appeals to other competent organizations, mandatorily providing detailed, complete and substantiated information concerning the issue raised in the appeal and explaining the applicant's issue to the relevant body;

temporarily restricting through court proceedings the applicant's right to apply to the relevant organization in cases of insulting and defamatory appeals;

establishing that in any decision on rejecting or partially satisfying an appeal, the legal norms and factual circumstances serving as the basis for the decision shall be stated point by point, and each case of rejection shall be clearly and duly substantiated;

institutional powers and mechanisms for conducting mandatory substantive reviews of appeals and publicly announcing the results;

introducing an institution for considering an appeal simultaneously by lower and higher organizations, as well as, where the issue raised in the appeal falls within the competence of two or more organizations, jointly considering the appeal without forwarding it according to competence and adopting a joint decision based on the results;

5.2. Establishing the mandatory implementation of the following in specialized systems for handling appeals:

determining the competence of appeals on the basis of a **“Register of Powers”**;

introducing a system for automatic random distribution of appeals in Uzbekistan;

automatic preparation of the text of an appeal through artificial intelligence;

automatic selection through the system of documents and materials related to the appeal, including previous appeals and/or response letters thereto in cases of repeated appeals;

introducing automatic logging of the consideration of appeals and the capability to automatically notify the applicant through a notification of the information concerning persons who viewed, including unjustifiably viewed, distributed or copied the text of the appeal;

providing the capability to monitor the steps taken in processing an appeal in real time;

providing automatic notifications through green, yellow and red indicators to ensure that the appeal is considered within the prescribed period;

automatically generating within the system, without human intervention, a decision on the imposition of an administrative penalty on persons who failed to comply with the deadline for considering an appeal and forwarding it for execution;

automatic verification of an appeal through the FACE-ID system;

mandatory review of the response to an appeal by artificial intelligence to determine whether each issue raised in the appeal has been addressed, whether the response is complete and substantiated, lawful, consistent with human rights and interests, and free from corruption factors, as well as conducting semantic and predictive analysis;

sending the response to an appeal, based on a positive conclusion of artificial intelligence, to the electronic address of an applicant who does not have a disability and has not reached retirement age, and to the applicant's telephone number in the form of an SMS notification;

in the event of disagreement with the response to an appeal, conducting mediation or enabling an automatic appeal to a court and other competent bodies without payment of a state duty;

introducing modules intended for children, persons with disabilities and persons who have reached retirement age;

establishing a cryptographically anonymized and protected subsystem for appeals concerning corruption;

launching a unified database and register of all appeals received by the system in an anonymized form, including the text of appeals and responses sent thereto;

introducing mandatory KPI indicators under which the quality of appeals considered and public services provided is assessed by the population, and the objectivity of such assessment is verified by artificial intelligence, as well as mechanisms for additional remuneration of civil servants based on such indicators;

establishing videoconferencing;

organizing through the system the execution of decisions of courts and other state bodies and introducing an institution for their temporary suspension;

5.3. Taking public service provision to a new level and reducing the number of systemic appeals and corruption factors, in particular:

establishing free provision of public services and services of an informational nature;

restricting the collection by Public Service Centers of additional fees for the public services and services they provide, except for mandatory fees established by legislation for the relevant service and additional fees approved by justice authorities;

in cases where registration, permitting and licensing services are not provided within the prescribed period, automatically issuing a positive conclusion through the system and ensuring registration, granting of permits and licensing through such conclusion;

digitizing public services and services based on the principle of a **“single appeal comprehensive service”** and making a single payment;

abolishing the requirement to obtain technical conditions and incur additional expenses for connection to electricity, water, gas and communications, and introducing a unified public service and service for connection;

5.4. Introducing, in Article 269³ of the Code of the Republic of Uzbekistan on Administrative Responsibility, proceedings on an administrative offense based on an application by the victim in relation to:

Article 43 – violation of legislation on appeals of individuals and legal entities;

Article 46² – violation of legislation on personal data;

Article 212 – failure to comply with mandatory requirements of technical regulations or standards;

Article 215⁵ – violation of legislation in the field of public services;

5.5. Establishing administrative and criminal liability for the following:

a) in Article 46² of the Code of the Republic of Uzbekistan on Administrative Responsibility and Article 141² of the Criminal Code – unlawful access to personal data in state information systems and resources;

b) in Article 43 of the Code of the Republic of Uzbekistan on Administrative Responsibility and Article 144 of the Criminal Code –

failure to state, point by point, the legal norms and factual circumstances serving as the basis for any decision to reject or partially satisfy an appeal, as well as failure to clearly and duly substantiate each case of rejection;

violation of mandatory requirements imposed on specialized systems for handling appeals, mandatory requirements for appeals submitted through specialized systems for handling appeals and responses thereto, and their digital monitoring in real time;

failure to grant the applicant the right to be heard as the applicant's final statement regarding newly discovered circumstances and decisions on rejection during the consideration of an appeal;

sending to the applicant responses to appeals that have not received a positive result from mandatory artificial intelligence verification, semantic and predictive analysis as to whether each issue raised in the appeal has been addressed, whether the response is complete and substantiated, lawful, consistent with human rights and interests, and free from corruption factors;

unjustifiably considering an appeal, distributing an appeal through telecommunications or the Internet;

violation of the applicant's **"right to be heard"** and violation of the procedure for adopting a joint decision on an appeal;

6.1. Adoption of the National Strategy for Crisis Resilience of the Republic of Uzbekistan;

6.2. Introduction of a national system of indicators for assessing the resilience of critical infrastructure;

6.3. Development of a National Resilience Index enabling regular assessment of the level of national crisis resilience in Uzbekistan, integration thereof into the state strategic planning system, and, through this, coverage of indicators in key areas such as public administration, the economy, digital infrastructure, energy, social stability and cybersecurity;

6.4. It is necessary to develop national educational programs on the preparedness of the population for crises.

Chapter 2. On Improving Civil Society Institutions and Local Governance

1.1. Taking into account advanced foreign experience and the specific characteristics of state social orders, by consolidating the provisions concerning the allocation and financing of state social orders contained in the Laws “**On Guarantees of Activities of Non-Governmental Non-Profit Organizations**” and “**On Social Partnership**”, as well as Resolution № 135 of the Cabinet of Ministers dated February 22, 2018, provide directly in the Law “**On Social Partnership**” for a simplified unified procedure for the allocation and financing of state social orders;

1.2. Establish a unified procedure for financing state social orders as follows:

a) of the project value:

the main portion – funds of the Public Fund for Support of Civil Society Institutions under the Oliy Majlis of the Republic of Uzbekistan (hereinafter – the Fund);

in equal distribution – extrabudgetary funds of the state body for projects at the republican level;

in equal distribution – local budget funds at the relevant level for projects at the district and regional levels.

b) formation of funds for state social orders in a separate account of the Fund and exercise of control over them;

1.3. Establish the following practice for the formation of state social orders:

citizens and deputies of local Councils of People's Deputies, after passing through the Unified Identification System and Face-ID, as well as business entities, civil society institutions, state bodies and organizations through electronic digital signatures, shall formulate their proposals on a unified special platform managed by the Fund;

proposals shall be formulated by types of civil society institutions, namely non-governmental non-profit organizations, mass media, citizens' self-governing bodies, at district, regional and republican levels;

compliance of proposals with the criteria established for state social orders and their proper formulation by types of civil society institutions and at district, regional and republican levels shall be verified by justice authorities and forwarded for public discussion;

during public discussion, citizens shall vote according to the principle of “**one vote per project**” after passing through the Unified Identification System;

based on the results of public discussion, taking into account the types of civil society institutions, one winning project related to state social orders at each of the district, regional and republican levels, as well as candidates to implement them through competition, shall be evaluated by members of the Parliamentary Commission under the Oliy Majlis on the platform, and the results shall be forwarded to the relevant state body depending on the level of financing;

1.4. Introduce a procedure under which the Parliamentary Commission under the Oliy Majlis determines project and competition winners through

evaluation on the platform after passing through the Unified Identification System and FACE-ID;

1.5. Through the platform, establish public and state oversight over all stages of allocation and financing of state social orders, public discussion of projects and holding of competitions, conclusion of direct contracts, and implementation of state social orders under contracts;

1.6. Grant the Ministry of Justice the powers to exercise unified state control over state social orders;

1.7. Establish specific deadlines for the allocation and financing of state social orders;

1.8. Provide that civil society institutions whose founder or head has an unexpunged conviction under legislation or has been subject to criminal liability for corruption, terrorism, or legalization of criminal proceeds shall be prohibited from participating in competitions and shall not be allowed to become winners based on the results of such competitions;

1.9. In order to support social entrepreneurship, provide tax and other benefits to entities that participate, together with civil society institutions, in the allocation of state social orders on the basis of social partnership by contributing additional funds and services;

2.1. Adoption of a normative legal act providing for a clear definition of the procedure and areas of cooperation between non-governmental non-profit organizations and local executive authorities and Councils of People's Deputies, and additionally, in the draft of this legislative act, in order to ensure systematic cooperation:

a) grant **regional, district and city khokims** the powers to adopt decisions on supporting the socio-economic activities of civil society institutions from additional local budget funds;

b) grant **Councils of People's Deputies** the powers to approve annual unified cooperation programs concluded between civil society institutions and state bodies within the respective territory, thereby introducing provisions aimed at establishing a unified system of cooperation between the state and non-state sectors in the territory;

as an experiment, gradually and fully integrate the existing **39 information systems** in Namangan Region and implement the **“Digital and Smart Region”** project for regional, district and city khokimiyats, creating the capability to automatically, without human intervention, obtain information on and analyze the state of development, existing problems and achievements in every sector and area, as well as the criminogenic situation and state of crime in the territory, and to access necessary information resources;

2.2. For the purpose of targeted and proper use of budget funds, establishment of systematic operations and implementation of the **“digital and smart region”** project, abandon the unified electronic system **“E-qaror”** and transfer its tasks and functions to the interagency unified electronic system for executive discipline **“Ijro.gov.uz”**, introduce artificial intelligence technologies therein, and launch its **updated version** by creating the technical capability for regional, district and city

khokimiyats, from a single point, to maintain an overall record of activities carried out by all state bodies and organizations in every sector, industry and area within the territory, issue necessary instructions, monitor their **“execution steps”** in real time, and publish adopted decisions;

2.3. Reflect the activities of non-governmental non-profit organizations and their cooperation with local executive authorities and Councils of People's Deputies, as well as the results thereof, in the unified information system **“Public Oversight Portal”**, fully establish its operation, and integrate it with the interagency unified electronic system for executive discipline **“Ijro.gov.uz”**;

2.4. Unify the monthly tax, statistical and justice authority reports submitted by non-governmental non-profit organizations and establish the practice of submitting a **single annual report through the Public Oversight Portal**, except for reports on projects implemented with the support of state and foreign organizations;

2.5. Fully implement the interagency unified electronic system for executive discipline **“Ijro.gov.uz”** in the activities of state bodies and organizations, and implement an effective solution for electronic document management between state and non-governmental organizations by providing non-governmental non-profit organizations possessing important information infrastructure that have assisted in the implementation and technical support of this system with free access to the interagency unified electronic system for executive discipline **“Ijro.gov.uz”**;

2.6. Permit non-governmental non-profit organizations to engage in commercial activities aimed at assisting in the sale and marketing of products developed by individual entrepreneurs, and establish that profits received by non-governmental non-profit organizations from such activities shall not constitute a taxable object;

2.7. Establish administrative liability for failure to comply or improper compliance with decisions adopted based on the results of Council inspections, and grant Councils of People's Deputies the authority to draw up administrative protocols against offenders and submit them to court;

3.1. Adoption of a resolution of the President of the Republic of Uzbekistan “On Measures to Implement the ‘Servis mahalla’ Strategy for 2026–2030”, providing for:

the **“Servis mahalla” Strategy for 2026–2030**;

target indicators for implementation of the **“Servis mahalla” Strategy**;

a list of information systems to be integrated into the **“Servis mahalla” comprehensive information system**;

a **roadmap** for implementing the priority tasks provided for by the **“Servis mahalla” Strategy** and its target indicators;

a list of state bodies and organizations responsible for ensuring the provision of certain types of public services and services by members of the **“mahalla seven”**;

a list of certain mahallas in Kashkadarya Region where the use of artificial intelligence by members of the **“mahalla seven”** is envisaged on a pilot basis;

categories of appeals to be resolved through cooperation among members of the **“mahalla seven”**;

4.1. Increasing the effectiveness of the “mahalla seven” by optimizing the staffing positions of the “Youth Leader”, initially implementing this on a pilot basis in Tashkent, Namangan and Kashkadarya regions, and subsequently in other territories based on the pilot results;

4.2. Distributing the duties and functions of the “Youth Leader” among the members of the “mahalla seven”, and fully digitizing the functioning of the social protection institution by integrating youth, women and “Iron Notebook” systems with one another.

Chapter 3. On the Digital Transformation of Society and the State and Information Security

1.1. Adoption of the Decree of the President of the Republic of Uzbekistan “On Approval of the ‘Digital New Uzbekistan’ Strategy”, and approval together with the Strategy of a “roadmap”; complete abandonment of approaches aimed at “digitizing each sector separately” and transition to a systematic digitalization trend, in particular, establishment, on the basis of this Decree, of a Unified Integrated Information System providing for:

reflecting the total number of all information systems in the Republic of Uzbekistan, their names by sector, industry and area, their tasks and functions, digital traces, and ownership;

decommissioning existing information systems that are ineffective, whose tasks and functions duplicate one another, or whose ownership is unclear;

clarifying ownership of information systems through the creation of information system passports;

introducing an automated system for taking measures to hold accountable persons who have misappropriated budget funds and ensuring the return to the state budget of funds appropriated by them, through responses by law enforcement bodies and courts to cases of improper involvement of information systems in practice;

providing, in real time, a clear indication of the need for full integration of information systems whose tasks and functions are similar;

introducing artificial intelligence into information and communication systems that have been fully mutually integrated and transferred to a unified platform, and determining the role and status of artificial intelligence technologies in all matters relating to the activities of the relevant state body;

creating the capability for the Head of State to determine, in real time, through digital solutions, the possibility of resolving existing problems in the Republic with limited resources;

2.1. On the basis of the resolution of the President of the Republic of Uzbekistan “On Measures to Introduce a Strategic System for Rapid Response to Information in the Media Space that Undermines the National and Public Security of the Republic of Uzbekistan”, implementing the following:

(a) approval of the Regulation on the strategic system for rapid response to information in the media space that undermines the national and public security of the Republic of Uzbekistan;

(b) establishing the following:

the system shall be implemented through the **“Digital Public” interagency comprehensive cooperation information and communication system** (hereinafter referred to as the **“Digital Public” information system**), based on artificial intelligence and meeting information and cybersecurity requirements, financed from the Digital Technology Development Fund;

the **“Digital Public” information system** shall constitute a rapid response system for information obtained from websites, social networks and messengers through artificial intelligence, automated systems and traditional methods regarding information that negatively affects the mood of the general public or distorts the actual state of reforms (hereinafter referred to as destructive information);

the owner of the **“Digital Public” information system** shall be the Ministry of Digital Technologies, and its special users shall include the Expert Commission in the field of Information and Mass Communications, the Center for Monitoring in the Field of Mass Communications, all bodies, organizations, enterprises and institutions with state participation in the system of state bodies and organizations regardless of their organizational and legal form (hereinafter referred to as state bodies and organizations), their heads and information services or persons performing their functions, the Inspection for Control in the Field of Informatization and Telecommunications, the administrator of the **.uz** domain, registrars, operators and providers, and their activities shall be fully digitized through this system;

the **“Digital Public” information system** shall operate **24/7**, and information and materials formed in and transmitted through it shall be reviewed by the relevant state body or organization according to the urgency of response, no later than **24 hours** in red mode, **48 hours** in yellow mode, and **72 hours** in green mode, with the results entered into the system;

clear criteria shall be established distinguishing **“destructive information”** from **“substantiated critical opinion”**, while ensuring the guarantees of freedom of speech and access to information guaranteed to citizens by the Constitution of the Republic of Uzbekistan;

the information services of state bodies and organizations shall have the capability to create, edit, process and perform other necessary actions with any materials and information relating to the activities of the organization, including audio, video, text, graphic and other forms, exclusively through the **“Digital Public” information system**, and to publish necessary information on social networks exclusively through this system with the preservation of digital traces;

30 percent of the work performance of employees of information services of state bodies and organizations shall be assessed through their activities in handling destructive information in the **“Digital Public” information system**, and information on work carried out concerning destructive information shall be communicated to the general public as a separate area at each briefing;

the activities of state bodies and organizations and political processes shall be carried out in real time through the **“Digital Public” information system**;

the activities of state bodies and other organizations shall be digitized on the basis of any political or ideological information related to the system occurring on

social networks through the **“Digital Public” information system**, with the creation of capabilities for automatically restricting harmful information and identifying offenders on the basis of artificial intelligence;

using the **“Digital Public” information system**, administrative offense cases and criminal cases shall be considered, the results of necessary inquiries, investigations, prosecutorial supervision and judicial actions shall be entered into the system, and a systematic unified approach shall be established for communicating the results to the general public;

3.1. Adoption of the Law of the Republic of Uzbekistan “On Artificial Intelligence”;

3.2. In connection with the adoption of the Law of the Republic of Uzbekistan “On Artificial Intelligence,” it is necessary to introduce amendments and additions to legislative acts, including Resolution № 707 of the Cabinet of Ministers of the Republic of Uzbekistan dated September 5, 2018, “On measures to further improve information security on the World Wide Web”⁴⁹⁸ and other documents. In particular, in the aforementioned Government Resolution:

To supplement paragraph 1 with a separate paragraph to the effect of “unlawful processing of personal data using artificial intelligence technologies and dissemination thereof through mass media, telecommunications networks or the global Internet information network”;

taking into account that restricting artificial intelligence differs in part from restricting access to an Internet website and/or web pages, to approve Regulations or Rules providing for a separate procedure for such restriction, and to ensure that these processes are also reflected in the scheme;

3.3. To establish in the current legislative acts the organizational and legal measures for ensuring information and cybersecurity in information systems, platforms, websites and other technical means containing artificial intelligence, including relations concerning all forms of logging digital traces, storing them, collecting, storing, presenting and processing electronic information and digital evidence;

3.4. To ensure that the Register of Internet information containing information prohibited for dissemination under the legislation of the Republic of Uzbekistan has a separate section (column) specifically related to artificial intelligence, and through this mechanism to maintain accurate statistics on restricted artificial intelligence systems and the information contained therein;

3.5. In working with artificial intelligence, the fact that a significant portion of the servers and databases of these technologies are located in foreign countries and that their management is carried out by representatives of the private, public or non-governmental sectors may create numerous problems in ensuring the security of the personal and private data of citizens of the Republic of Uzbekistan. Therefore, to regulate these relations in the legislation of our country and in international instruments;

⁴⁹⁸ Resolution № 707 of the Cabinet of Ministers of the Republic of Uzbekistan dated September 5, 2018, “On measures to further improve information security on the World Wide Web” // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

4.1. In order to ensure guarantees of children's information rights and protect them from information harmful to their health, it is necessary to adopt a resolution of the President of the Republic of Uzbekistan providing for the implementation of the following measures, and through this resolution to implement the following:

(a) to establish that the minimum age for opening a personal account for children on social networks and messengers is **16** years of age, to assign responsibility for ensuring compliance with this requirement to their parents and persons acting in their place, as well as educational organizations, and to reflect this requirement in the Laws of the Republic of Uzbekistan “**On Guarantees of the Rights of the Child**” and “**On Protection of Children from Information Harmful to Their Health**”;

(b) to define a child's image as his or her personal data and ensure its protection, to provide in the Law of the Republic of Uzbekistan “**On Guarantees of the Rights of the Child**” for the rights and obligations relating to the use of a child's image by his or her parents and persons acting in their place, as well as third parties, and, based on this, to introduce amendments and additions to the Law of the Republic of Uzbekistan “**On Personal Data**” and the **Family Code**;

(c) with regard to violations of guarantees of children's information rights:

to establish liability for violations of the age classification of information products on telecommunications networks, including the global Internet, violations of the age requirement for children's registration on social networks and messengers, and the unlawful placement of their personal data on telecommunications networks or deriving profit therefrom, as well as permitting such actions by operators and providers;

in addition to those provided for in Articles 189–189¹ of the Code of Administrative Responsibility, to **establish administrative liability** in Articles 189³–189⁴ of the Code of Administrative Responsibility for placing and disseminating information on telecommunications networks that harms the personality, development and morality of a child and for harmful information;

(d) to instruct the **Ministry of Digital Technologies**, at the expense of the funds of the Digital Technologies Development Fund, to implement the following:

to develop and introduce into practice by “Uzinfocom Single Integrator” LLC the “**Child Protection**” information system and ensure its continuous technical support;

to launch the “**Child Protection**” **mobile application**, relating to the operation of artificial intelligence technologies and “smart systems” that automatically detect cases of violation of the age classification of information products on telecommunications networks, including the global Internet, violations of the age requirement for children's registration on social networks and messengers, and unlawful placement of their personal data on telecommunications networks or deriving profit therefrom;

to establish the acceptance, on a 24/7 basis, of appeals concerning violations of a child's information rights through the “**Prezidentning virtual qabulxonasi**” system and the “**112**” **Unified Dispatch Service**,

and to introduce a separate module for mandatory placement in the **“Prezidentning virtual qabulxonasi”** system of the results of consideration of such appeals by authorized bodies and to integrate it with the **“Child Protection”** information system;

to complete full integration with the information systems of interested agencies and to establish the operation of this information system within the activities of the interested ministries and agencies;

to establish a system whereby access by a child to social networks inappropriate for his or her age is detected using artificial intelligence through the **“Child Protection”** information system and its mobile application, and the child’s parents and persons acting in their place, as well as authorized agencies, are notified;

to establish, within the **“Child Protection”** information system, the automatic generation of drafts of specialist opinions, conclusions, requests, instructions and other documents, an analysis system based on artificial intelligence, as well as interagency digital cooperation between state bodies and other organizations concerning the protection of children's rights through the **“Protection from Harmful Information”** module, the ability of parents to monitor their children's use of the network and the ability of authorized agencies to monitor it through the **“Legal Representative Control”** module, and the recording of the overall results of the work carried out by state bodies and other organizations to protect children's rights through the **“Child Rights Monitoring”** module and other modules;

to launch an updated version of the artificial intelligence-based **“ZiyoNET”** educational portal, highly convenient for users, providing for the formation of necessary information resources through the Unified Identification System of citizens of the Republic of Uzbekistan, the transfer of all useful information resources available in the Republic to this portal, its integration with the necessary websites, information systems and other social networks, the placement of information resources taking into account the age of children in relation to information products, and the ability to find and use the necessary information through artificial intelligence technology;

to continuously take necessary measures to create all necessary information resources for children under 16 years of age on the **“ZiyoNET”** educational portal that do not cause harm to their health;

(e) the Ministry of Higher Education, Science and Innovation, the Ministry of Preschool and School Education, and all organizations having educational institutions within their systems:

shall be obliged to identify the information resources necessary for users and take the necessary measures to place them on the **“ZiyoNET”** educational portal, with supervision thereof carried out by the Inspection for Control in the Sphere of Informatization and Telecommunications;

to issue the necessary instructions to ensure, together with parents, that the **“Child Protection”** mobile application is active on the smartphone used by a child under 16 years of age, or that it is integrated with the **“Child Protection”** information system;

(f) in order to ensure guarantees of children's information rights, to establish the following new system:

the child's parents and persons acting in their place, as well as third parties, shall have the opportunity to submit appeals concerning violations of children's rights through the **“Child Protection”** mobile application, the **“Prezidentning virtual qabulxonasi”** system, the **“112” Unified Dispatch Service**, or other means;

the Ministry of Internal Affairs, the National Agency for Social Protection, the Inspection for Control in the Sphere of Informatization and Telecommunications, the Center for Mass Communications, telecommunications operators and providers, and registrars shall regularly monitor violations of children's information rights in telecommunications and the global Internet information network, accept appeals, and continuously place the results of monitoring and their conclusions regarding appeals in the **“Child Protection”** information system;

the Inspection for Control in the Sphere of Informatization and Telecommunications shall, through its instruction, obtain from the Registrar information concerning the offender under the uz. domain and enter the results into the **“Child Protection”** information system;

if it is established that the information and documents requested by the Inspection for Control in the Sphere of Informatization and Telecommunications have not been fully provided, the Ministry of Digital Technologies shall temporarily suspend the activities of the relevant operator or provider for violating legislation in the telecommunications sector until the violation is eliminated and shall enter the result thereof into the **“Child Protection”** information system;

the National Agency for Social Protection shall review the conclusion and the materials indicated as its basis within **5** days, place its professional opinion in the **“Child Protection”** information system, and carry out the procedures provided for by legislation concerning the issuance of a protection order to a child who has suffered violence;

within **10** days from the time the professional opinion is placed, based on the requirements of legislation on informatization, the Ministry of Digital Technologies shall ensure the restriction of the relevant information and enter the result into the **“Child Protection”** information system;

the Ministry of Internal Affairs shall fully establish the identity of the offender and, after conducting inquiry proceedings, ensure that the administrative offense report and submission based on the results are displayed in the **“Child Protection”** information system;

courts and compulsory enforcement bodies shall be responsible for ensuring that court decisions concerning offenses involving violations of guarantees of children's information rights and their enforcement are displayed in the **“Child Protection”** information system;

the Children's Ombudsman shall monitor the implementation by relevant state bodies and organizations of legislative acts concerning guarantees of children's rights and shall take necessary measures in cases of violations of the law;

the Ministry of Digital Technologies shall, within the framework determined by the Children's Ombudsman, ensure the technical capacity for the Children's

Ombudsman, the Ministry of Internal Affairs, the National Agency for Social Protection, the Inspection for Control in the Sphere of Informatization and Telecommunications, the Center for Mass Communications, the Supreme Court, the Bureau of Compulsory Enforcement, telecommunications operators and providers, as well as registrars, to fully and sufficiently use the “**Child Protection**” information system;

(g) in order to ensure the full and sufficient implementation of guarantees of children's information rights at the local level, to instruct the Ministry of Justice, the National Agency for Social Protection, the Children's Ombudsman, the General Prosecutor's Office, the Ministry of Internal Affairs, the Ministry of Preschool and School Education, and the Committee on Family and Women to properly organize explanatory activities at the local level regarding the substance and significance of the new procedure concerning guarantees of children's information rights;

4.2. The following should be provided for by a resolution of the Government:

to approve and introduce mandatory technical requirements for determining the age of a child and the age classification of information products on social networks and messengers, as well as the procedure for determining them through a mobile application using artificial intelligence technologies;

to establish the procedure for creating a personal bank account for a child, including for the use of a child's image, including its use in advertising, and the procedure for using and disposing of these funds, while stipulating the obligation of the child's parents and persons acting in their place to open a separate bank account for the child for the use of the child's personal data, including its use in advertising;

to bring Resolution No. 137 of the Cabinet of Ministers of the Republic of Uzbekistan dated March 26, 1999 “On Approval of the Regulation on the Procedure for Preparing Information Resources of the Republic of Uzbekistan and Disseminating Them in Data Transmission Networks, Including the Internet” into line with current requirements, providing for the procedure for placing and disseminating a child's personal data on the network and rules for using the network;

CHAPTER 4. ON ENSURING JUSTICE AND COMBATING CYBERCRIME

1.1. To adopt the Decree of the President of the Republic of Uzbekistan “**On Measures to Improve the Organizational and Criminal-Legal Foundations for Combating Cybercorruption**”, providing for the following:

to approve a “road map” providing for combating corruption through digitalization in the areas of healthcare, education, public administration, mahalla, social protection, digitalization, including digital assets, and public procurement;

based on the requirements of the Law “On Cybersecurity”, to transfer the authority to investigate cybercrimes from the General Prosecutor's Office of the Republic of Uzbekistan and the Ministry of Internal Affairs to the State Security Service;

to reorganize the State Unitary Enterprise “Cybersecurity Center” and establish the Cybersecurity Agency of the Republic of Uzbekistan within the State Security Service;

to define the Agency's specific powers to combat cyber-offenses and cybercrimes at the national and international levels by transferring its activities to a 24/7 operational mode;

to transfer the Center for Mass Communications and the Republican Center for Management of Telecommunication Networks to the Agency;

to reduce overlapping and similar powers by transferring to the Agency the functions and powers of the Ministry of Internal Affairs, the Ministry of Justice, the Ministry of Digital Technologies, the National Agency of Prospective Projects, the Agency for Information and Mass Communications, the Central Bank, the Anti-Corruption Agency, and the Inspection for Control in the Sphere of Informatization and Telecommunications concerning informatization, personal data, including control and inspection in the fields of information and cybersecurity;

to reduce overlapping and similar powers by transferring to the Agency the functions and powers of the Ministry of Internal Affairs and the Inspection for Control in the Sphere of Informatization and Telecommunications concerning proceedings on administrative offenses in the fields of informatization, personal data, including information and cybersecurity, including the preparation and submission to court of administrative offense reports;

to introduce the positions of **cyber specialist** and **cyber investigator** within the structure of the State Security Service responsible for conducting operational investigative activities, investigative actions and judicial proceedings in relation to cybercrimes;

to establish a specialized “**corps of judges**” within the Criminal Judicial Collegium of the Supreme Court of the Republic of Uzbekistan and the courts of the Republic of Karakalpakstan, regions and the city of Tashkent for the consideration of cyber-administrative offenses and cybercrimes;

to transfer the unified electronic case management system for administrative offenses, the unified information system “Electronic Criminal-Legal Statistics”

and the “e-anticor.uz” platform to a single platform;

to develop the “**Cybersecurity**” information system for the prompt consideration and resolution of appeals concerning cyber-offenses, including cybercorruption, and to integrate it with the information systems on the single platform and all information systems in the Republic;

to introduce into practice and approve the Regulations for the “**CCA**” platform, which automatically receives and analyzes appeals concerning cyber-offenses and cybercrimes, including appeals concerning cyber-offenses in the pm.gov.uz website and the “eanticor.uz” information system, and enables the consideration of appeals in real time, as an operational automated, artificial intelligence-based platform;

to establish the prediction (forecasting) of cyber-offenses and cybercrimes through artificial intelligence technologies, and provide investigators, inquiry

officers and judges with the ability to review decisions, receive recommendations for identifying, detecting, exposing and sentencing cyber-offenses and cybercrimes, analyze them, as well as analyze the measures implemented to combat corruption and assess their effectiveness;

to transform the organizational and legal form of the Limited Liability Company “Center for Development of Information Technologies and Information Resources” into a state institution and reorganize it as the “Republican Center for Expertise of Digital Technologies and Technical Means”;

to develop a draft normative document on unified technical regulation for combating cybercorruption;

to define specific tasks for improving the Republic of Uzbekistan's position in international rankings

and indices on combating cybercorruption;

to introduce amendments and additions to Decree № DP–38 of the President of the Republic of Uzbekistan dated March 10, 2026 “On Defining the Cybersecurity Strategy of the Republic of Uzbekistan and Improving the System for Preventing Cybercrime”;

based on this decision, simultaneously bring subordinate legislation into compliance with this decision;

1.2. To adopt the Law of the Republic of Uzbekistan “On Amendments and Additions to Certain Legislative Acts in Connection with the Improvement of Combating Cybercorruption-Related Offenses”, providing for the following:

1) in the Law “On Combating Corruption”:

to provide for the concepts of cybercorruption, corruption-related offense, corruption-related crime, cybercorruption-related offense, cybercorruption-related crime, cybersecurity incident, cyberspace, and cybersecurity object;

to clarify the powers of authorized bodies arising from cybercorruption;

to establish the procedure for the participation of artificial intelligence in combating corruption;

to approve the list of corruption and cybercorruption-related offenses and crimes;

2) to introduce amendments and additions to the Law “On Cybersecurity” and, based on cybercorruption, clarify the cybersecurity object;

3) to introduce amendments and additions to the Criminal Code based on advanced foreign experience concerning cybercorruption and the attached information-analytical material from the scientific and legal perspective, and to provide in Section VIII for the concepts of cybercrime, cyberspace, cybercorruption and corruption;

4) to clarify the investigation of cybercrimes and issues of territorial jurisdiction in Articles 345–346 of the Criminal Procedure Code;

5) to grant the Cybersecurity Agency the authority to prepare administrative offense reports, conduct inquiries and submit them to court in accordance with Article 282 of the Code of Administrative Responsibility concerning offenses and other cyber-administrative offenses committed on telecommunications and Internet networks or using such networks, as well as offenses under Articles 46–46¹, 56² and

56⁴ of the Code of Administrative Responsibility of the Republic of Uzbekistan (cases committed using telecommunications and Internet networks), Article 61¹ (in the part concerning cybercorruption), Articles 151, 155–155³, 193¹–193² (in the part concerning cybercorruption);

6) to introduce amendments and additions to the following laws:

in the Law “On Informatization”, to reflect the concepts of “artificial intelligence” and “artificial intelligence technologies” and establish information and cybersecurity of artificial intelligence;

in the Laws “On the Central Bank”, “On Banks and Banking Activities”, “On Payments and Payment Systems”, “On Electronic Commerce”, “On Telecommunications”, “On Personal Data”, “On Electronic Digital Signature”, “On Electronic Government”, “On Electronic Document Management”, “On Guarantees of Protection of Bank Deposits”, “On Non-Bank Credit Organizations and Microfinance Activities”, “On Conflict of Interests”, “On the Prosecutor's Office”, “On Courts”, “On the State Security Service of the Republic of Uzbekistan”, “On the Cabinet of Ministers of the Republic of Uzbekistan”, “On Internal Affairs Bodies”, “On the Status of a Deputy of the Legislative Chamber and a Member of the Senate of the Oliy Majlis of the Republic of Uzbekistan”, “On the Status of a Deputy of a Regional, District and City Council of People's Deputies”, and “On the Openness of the Activities of State Authorities and Administration”, to establish the specific obligations of state bodies and organizations as cybersecurity subjects to ensure information and cybersecurity and to combat cyber-offenses, cybercrimes, including cybercorruption;

2.1. To adopt a resolution of the President of the Republic of Uzbekistan “**On Measures to Improve the Organizational and Criminal-Legal Foundations for Combating Cybercorruption**” and, on its basis:

1) in connection with accession to the UN Convention against Cybercrime, to legally consolidate the ongoing reforms by adopting a separate legislative act in this regard:

- (a) Council of Europe Criminal Law Convention on Corruption (1999);
- (b) Council of Europe Civil Law Convention on Corruption (1999);
- (c) Organization of American States Inter-American Convention Against Corruption (1996);
- (d) African Union Convention on Preventing and Combating Corruption (2003);
- (e) Arab Convention on Combating Corruption;
- (f) Makka Al-Mukarrama Convention;
- (g) Budapest Convention (Council of Europe Convention on Cybercrime);
- (k) international cybersecurity standards and technical documents;

2) to introduce into practice the operational automated national artificial intelligence-based “CCA” platform and approve its Regulations;

3) to connect all information systems of the Republic to the “CCA” platform and establish the operation of a powerful, mutually protected and integrated system providing real-time information on situations occurring at the national and international levels;

4) to determine the owner and operator of the “CCA” platform;

5) to bring the legislation of the Republic of Uzbekistan into compliance with the United Nations Convention against Cybercrime and other international instruments;

3.1. To approve, by a separate Law of the Republic of Uzbekistan, a specific list of disputes subject to mandatory mediation;

3.2. In order to fully digitalize the mediation institution and ensure its transparency, to submit to the Presidential Administration a draft resolution of the President of the Republic of Uzbekistan “On Improving the Regulation of Relations in the Field of Mediation”, providing for the following:

to include among the areas in which mediation procedures are applied civil, tax and public procurement disputes, disputes in which one of the parties is a state body, organization or business entity, as well as cases involving damage caused by an administrative offense or criminal offense, as a means of securing an obligation;

to introduce amendments and additions to the Code of Administrative Responsibility and the Criminal Procedure Code based on the refusal to initiate an administrative offense or criminal case and the termination of pending proceedings due to the application of a mediation procedure in an administrative offense or criminal case;

to approve a unified list of disputes subject to mediation;

to establish the practice whereby courts offer the parties mandatory mediation in disputes subject to mediation and, based on its outcome, terminate or continue the proceedings;

to establish procedures for incentivizing mediators for disputes resolved by courts as a result of the application of mediation;

to establish the possibility of automatically notifying mediators about state bodies and organizations, as well as disputes subject to mediation being considered by courts;

to establish that remuneration paid to professional mediators shall not constitute an object of taxation;

to introduce the artificial intelligence-based “**Digital Mediation**” integrated information system and its mobile application;

to approve the Regulation on the procedure for conducting mediation procedures using the “**Digital Mediation**” integrated information system;

to establish a mechanism for conducting mediation procedures entirely through the mandatory use of the “**Digital Mediation**” integrated information system;

to create the following opportunities for implementation in real time through the “**Digital Mediation**” integrated information system and its mobile application:

to obtain through interagency electronic cooperation and enter manually into the “**Digital Mediation**” integrated information system information concerning the identity, property, residential and current address of the mediator and the parties, as well as other information relating to the subject matter of the dispute;

the list of disputes subject to mediation and, based on this list, mediative settlements concluded in the Republic, the mediators who approved them, and the results of the settlements;

to receive education through a digital educational platform necessary for the training of professional mediators;

the register of professional mediators;

the register of mediative settlements and cases completed through mediation procedures;

to obtain through interagency electronic cooperation information about mediators and parties, mediative settlements concluded by them and confirmed by a QD code, and information concerning their implementation;

to send an offer for concluding a mediative settlement, accept it, review and discuss offers and proposals;

to provide the mediator with the information and evidence necessary for concluding a mediative settlement, and for the mediator to provide alternative proposals to the parties;

to send summonses to the parties and conduct discussions of a mediative settlement between the parties through video conferencing with the participation of the mediator;

to edit a draft mediative settlement, conclude a mediative settlement, introduce amendments and additions thereto, cancel and approve it, and download the mediative settlement confirmed by a QD code;

to pay remuneration to the mediator;

to know and analyze the rights and obligations of the mediator, the parties and platform users, their liability arising from such obligations, the procedure for filing complaints, and the consequences of concluding a mediative settlement;

to receive, through the Unified Interactive Government Services Portal, the Electronic Government Services Portal of the Tax Authorities, the “**Digital Mediation**” integrated information system and its mobile application, notifications in real time regarding actions carried out;

to obtain from a single platform, through integration with the interactive services portal of the Supreme Court of the Republic of Uzbekistan, mediation settlements submitted to courts, as well as rulings of courts terminating proceedings or leaving cases without consideration due to the acceptance of mediation settlements by interested parties;

to conduct mediation procedures in a simple and convenient manner by converting video, audio and voice recordings into text;

to establish the possibility of automatically notifying mediators about state bodies and organizations, as well as disputes subject to mediation being considered by courts;

to enable the parties and the mediator, after registering through the Unified Interactive Government Services Portal, the Electronic Government Services Portal of the Tax Authorities, and using the QD code on the ID card and Face ID methods of authentication, to familiarize themselves through the “Digital Mediation” integrated information system and its mobile application with the processes of the

mediation procedures in which they participated, obtain the necessary information, and work with the necessary information in the system;

4.1. In order to further strengthen the role of forensic examination in detecting crimes and cybercrimes committed using information and communication technologies and to bring cyber-forensic examination to a new level, it is necessary to adopt a resolution of the President of the Republic of Uzbekistan “On Measures to Systematize Digital Forensics and Bring It to a New Level”, providing for the following:

(a) to create a system of forensic examinations applicable to crimes and offenses committed using information and communication technologies, including cybercrimes, and to include in it telecommunications network examination, telecommunications infrastructure examination, information system examination, computer information and electronic data examination, software and software products examination, cryptographic examination, communication coverage and quality examination, forensic cyber examination, and forensic economic cyber examination;

(b) to establish the operation of **forensic cyber examination**, providing a complete unified legal and technical conclusion concerning digital evidence, including electronic documents and data and technical means, addressing the legality and reliability of specialist opinions and appointed expert conclusions obtained in cases involving crimes and cybercrimes committed using information and communication technologies, as well as the legality and reliability of evidence and the authenticity of the sources from which it was obtained;

(c) to reorganize the Limited Liability Company “Center for Development of Information Technologies and Information Resources” as a state institution under the name “Republican Center for Expertise of Digital Technologies”;

(d) to grant the “Republican Center for Expertise of Digital Technologies” the authority to issue forensic cyber examination conclusions concerning conclusions and specialist opinions issued in cases involving crimes and cybercrimes committed using information and communication technologies, thereby establishing a unified legal and technical practice for all expert conclusions and specialist opinions in this field throughout the Republic;

(e) to develop and introduce a special educational program “**Cybercriminologist**” encompassing the preschool education–school–higher education–postgraduate education system for the training of specialized experts and specialists in cybercrime, fully covering legal and technical knowledge;

(f) to establish the specialty “**Cybercriminology**”, fully encompassing criminal, civil and international law and specialized technical disciplines, and to critically review the existing classifier and curriculum;

(g) to establish mandatory teaching of Cybercriminology textbooks at the preschool education, school, higher education and postgraduate education levels, depending on the age and interests of the learner;

(h) to establish and maintain an online database and register of specialists and experts engaged in cases involving crimes and cybercrimes committed using

information and communication technologies, and to create the possibility of viewing the amounts of payments made to them on an open platform;

(i) to establish that expert examinations in cases involving crimes and offenses committed using information and communication technologies, including cybercrimes, may be conducted only by certified experts;

(j) to approve the following:

a list of mandatory requirements for organizations, experts and specialists issuing specialist opinions and expert conclusions concerning crimes and cybercrimes committed using information and communication technologies;

a Regulation on the special procedure for engaging specialists and experts in cases involving crimes and cybercrimes committed using information and communication technologies and obtaining specialist opinions and conclusions in criminal cases;

a list of types of expert examinations applicable to crimes and cybercrimes committed using information and communication technologies;

a methodology for calculating damage caused as a result of cybercrimes;

a Regulation on the procedure for appointing forensic cyber examinations and obtaining expert conclusions;

(k) based on the categories of critical information infrastructure facilities whose value cannot be assessed, to establish the practice of determining the amount of damage by multiplying each facility by a significant, large or very large amount;

(l) to instruct the introduction of amendments and additions to the Criminal Procedure Code and the Code of Administrative Responsibility concerning the mandatory conduct of forensic cyber examinations in cases involving crimes and cybercrimes committed using information and communication technologies provided for in the Criminal Code and the Code of Administrative Responsibility, in order to determine the legality and reliability of evidence and the authenticity of the sources from which it was obtained, as well as the mandatory conduct of communication coverage and quality examinations in relation to acts and offenses concerning communication quality for the purpose of determining communication coverage and quality and the negative impact of communications on the population and living organisms;

5.1. It is necessary to introduce the following amendments and additions to the legislation of the Republic of Uzbekistan:

to supplement Article 68 of the Law of the Republic of Uzbekistan “On Courts”, concerning the mandatory education of candidates at the Higher School of Judges, with a provision establishing mandatory continuous education on artificial intelligence technologies and their legal consequences;

to introduce amendments to Articles 249–270 of the Civil Procedure Code concerning court decisions, making it mandatory for a judge to clearly indicate that artificial intelligence assistance was used when adopting a decision in accordance with Article 204 or preparing drafts of procedural documents;

to establish in the Code of Judicial Ethics the procedure for judges' participation in the development and improvement of artificial intelligence systems

used in the judicial system, while ensuring that ethical considerations in technological advances remain a priority;

to introduce amendments to Articles 176–179 of the Economic Procedural Code concerning court decisions, making it mandatory to disclose information on the use of artificial intelligence assistance in resolving economic disputes;

to introduce amendments to Articles 154–164 of the Code of Administrative Court Proceedings concerning court decisions, making it mandatory to clearly disclose the use of artificial intelligence assistance in making administrative decisions.

Chapter 5. On Improving Scientific Research and the Cyberalogy Methodology

1.1. It is advisable to introduce the fundamental science of “**Cyberalogy**”;

1.2. The Law of the Republic of Uzbekistan No. LRU–764 “On Cybersecurity” dated April 15, 2022, should address cyberalogy and establish that the cybersecurity education system should be based on it; the definition of the concept of “**cybercrime**” should be provided in this Law and the Criminal Code; furthermore, the concept of “**cyber environment**” should be introduced into this Law, while the definitions of the concepts of “**cyberspace**” and “**cybersecurity object**” should be reconsidered; this area should be further developed by deriving specific types of cybercrime from the **2024 United Nations Convention against Cybercrime**, thereby establishing a comprehensive list of all specific types of cybercrime;

1.3. To abolish all benefits and preferences established by legislation with respect to women who have committed cybercrimes, including all mitigating measures established by legislation for ordinary crimes;

1.4. To create artificial cyber ranges and, through artificial traps, make effective use of Article 69 of the Criminal Code by temporarily delaying the commencement of investigations against offenders for a period of two years, while preserving information on their exact number, location, and all evidence of the acts they have committed, and applying a tactic of obtaining comprehensive knowledge about them;

1.5. It is necessary to declare a temporary moratorium on holding persons liable for having committed cyberattacks against the websites of state bodies and organizations and for fully disclosing how such attacks were carried out; through this, the cybersecurity of websites can be further strengthened; most importantly, it is necessary to establish the lawful activities of “**white hat**” **hackers** and introduce mechanisms for encouraging persons who assist in exposing individuals who have committed cybercrimes;

1.6. It is necessary to abandon mere formal meetings and, by instilling a culture of cybersecurity through cartoons, films, and infographics, increase and disseminate materials demonstrating the capabilities of state bodies;

1.7. To prevent cybercrime, the best approach toward a cybercriminal is psychological pressure; it should be explained that committing a cybercrime in

Uzbekistan may result in liability under aggravating circumstances, and that it is preferable to follow the path of “**white hat**” **hackers**. It is advisable to act promptly, understanding that attacking a minority is preferable to protecting the majority. The mass media and web resources should emphasize and demonstrate that cybercriminals have been apprehended and held liable and that mitigation measures are not applied; only then may cybercrime decrease sharply, and education and instruction should be organized accordingly;

1.8. The word “**cyber**” should be linked to “**cyber environment, including cyberspace**” and “**information and communication technologies**”, with a clear determination that information technologies, artificial intelligence, telecommunications technologies, and other technologies constitute information and communication technologies; the specific subject matter, goals, and objectives should be clearly defined not only for the science of cyberalogy but also for other academic disciplines;

1.9. To maintain a specific register of scientific and practical specialists who have conducted scientific research in the field of cyber-related relations, systematically improve their qualifications, and transition to systematic training of specialists by imposing an obligation on them to teach and engage in scientific activities at higher education institutions in return for the free professional development training they have received;

2.1. Analytical and information materials, articles, theses, monographs, training manuals, teaching and methodological manuals, textbooks, dissertations, and other scientific works submitted to the President of the Republic of Uzbekistan, the Administration, the Government, and other agencies should be developed on the basis of the **Cyberalogy method**;

2.2. Scientific works developed on the basis of the **Cyberalogy method** are not only understandable, precise, and simple for the reader, but this algorithmic format will also serve in the future as a strong fundamental basis for the automated monitoring of the implementation of legislation with the assistance of artificial intelligence, enabling the education system of the Republic of Uzbekistan to reach a new level and become comprehensively systematized.

List of References

I. Regulatory and Legal Documents

1. Constitution of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
2. Civil Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
3. Code of the Republic of Uzbekistan on Administrative Responsibility // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
4. Criminal Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
5. Labour Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
6. Tax Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
7. Criminal Procedure Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
8. Civil Procedure Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
9. Economic Procedure Code of the Republic of Uzbekistan // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
10. Law of the Republic of Uzbekistan “On Local State Authority” dated September 2, 1993, № 913-XII // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
11. Law of the Republic of Uzbekistan “On Protection of Citizens’ Health” dated August 29, 1996, № 265-I // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
12. Law of the Republic of Uzbekistan “On Notariat” dated December 26, 1996, № 343-I // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
13. Law of the Republic of Uzbekistan “On Non-Governmental Non-Profit Organizations” dated April 14, 1999, № 763-I // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
14. Law of the Republic of Uzbekistan “On Introducing Amendments and Additions to the Criminal, Criminal Procedure Codes and the Code of the Republic of Uzbekistan on Administrative Responsibility in Connection with the Liberalization of Criminal Penalties” dated August 29, 2001, № 254-II // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
15. Law of the Republic of Uzbekistan “On Execution of Judicial Acts and Acts of Other Bodies” dated August 29, 2001, № 258-II // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
16. Law of the Republic of Uzbekistan “On Informatization” dated December 11, 2003, № 560-II // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

17. Law of the Republic of Uzbekistan “On Arbitration Courts” dated October 16, 2006, № LRU–64 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
18. Law of the Republic of Uzbekistan “On Guarantees of the Activities of Non-Governmental Non-Profit Organizations” dated January 3, 2007, № LRU–76 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
19. Law of the Republic of Uzbekistan “On Introducing Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan in Connection with the Regulation of the Procedure for Organizing and Conducting Gambling and Other Games Based on Risk” dated September 14, 2007, № LRU–109 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
20. Law of the Republic of Uzbekistan “On Introducing Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan in Connection with Strengthening Liability for Illegal Acts Committed in the Field of Informatization and Data Transmission” dated December 25, 2007, № LRU–137 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
21. Law of the Republic of Uzbekistan “On Guarantees of the Rights of the Child” dated January 7, 2008, № LRU–139 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
22. Law of the Republic of Uzbekistan “On the Accession of the Republic of Uzbekistan to the United Nations Convention against Corruption (New York, October 31, 2003)” dated July 7, 2008, № LRU–158 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
23. Law of the Republic of Uzbekistan “On Openness of the Activities of State Authorities and Administration” dated May 5, 2014, № LRU–369 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
24. Law of the Republic of Uzbekistan “On Prevention of Offenses” dated May 14, 2014, № LRU–371 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
25. Law of the Republic of Uzbekistan “On Social Partnership” dated September 25, 2014, № LRU–376 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
26. Law of the Republic of Uzbekistan “On Introducing Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan” dated April 25, 2016, № LRU–405 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
27. Law of the Republic of Uzbekistan “On Introducing Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan” dated September 23, 2016, № LRU–411 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
28. Law of the Republic of Uzbekistan “On Combating Corruption” dated January 3, 2017, № LRU–419 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.
29. Law of the Republic of Uzbekistan “On Introducing Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan, as well as

Recognizing Certain Legislative Acts as Having Lost Their Force” dated June 13, 2017, № LRU-436 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

30. Law of the Republic of Uzbekistan “On Mediation” dated July 3, 2018, № LRU-482 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

31. Law of the Republic of Uzbekistan “On Normative Legal Acts” dated April 20, 2021, № LRU-682 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

32. Law of the Republic of Uzbekistan “On Cybersecurity” dated April 15, 2022, № LRU-764 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

33. Law of the Republic of Uzbekistan “On Advertising” dated June 7, 2022, № LRU-776 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

34. Law of the Republic of Uzbekistan “On Civil Service” dated August 8, 2022, № LRU-788 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

35. Law of the Republic of Uzbekistan “On Anti-Corruption Examination of Normative Legal Acts and Their Drafts” dated August 8, 2023, № LRU-860 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

36. Law of the Republic of Uzbekistan “On the Status of a Teacher” dated February 1, 2024, № LRU-901 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

37. Law of the Republic of Uzbekistan “On Privatization of State Property” dated February 14, 2024, № LRU-907 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

38. Law of the Republic of Uzbekistan “On Introducing Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan in Connection with the Improvement of Legislation in the Field of Ensuring Cybersecurity” dated September 20, 2024, № LRU-964 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

39. Law of the Republic of Uzbekistan “On Protection of Children from All Forms of Violence” dated November 14, 2024, № LRU-996 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

40. Law of the Republic of Uzbekistan “On Introducing Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan Aimed at Improving the System for Handling Digital Evidence” dated November 21, 2024, № LRU-1003 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

41. Law of the Republic of Uzbekistan “On the State Budget of the Republic of Uzbekistan for 2025” dated December 24, 2024, № LRU-1011 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

42. Law of the Republic of Uzbekistan “On Introducing Additions and Amendments to Certain Legislative Acts of the Republic of Uzbekistan in

Connection with the Regulation of Relations Arising from the Use of Artificial Intelligence” dated January 21, 2026, № LRU–1115 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

43. Decree of the President of the Republic of Uzbekistan “On the Strategy of Actions for the Five Priority Areas of Development of the Republic of Uzbekistan in 2017–2021” dated February 7, 2017, № DP–4947 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

44. Concept for Improving Rulemaking Activities, approved by Decree of the President of the Republic of Uzbekistan № DP–5505 dated August 8, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

45. Decree of the President of the Republic of Uzbekistan “On Measures for Radical Improvement of the Criminal-Legal Statistics System and Increasing the Effectiveness of Systematic Analysis of Crimes” dated October 31, 2018, № DP–5566 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

46. Decree of the President of the Republic of Uzbekistan “On Measures to Further Improve the Activities of Justice Bodies and Institutions in Implementing State Legal Policy” dated May 19, 2020, № DP–5997 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

47. Decree of the President of the Republic of Uzbekistan “On Approval of the Strategy ‘Digital Uzbekistan – 2030’ and Measures for Its Effective Implementation” dated October 5, 2020, № DP–6079 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

48. Decree of the President of the Republic of Uzbekistan “On Approval of the Concept for the Development of Civil Society for 2021–2025” dated March 4, 2021, № DP–6181 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

49. Decree of the President of the Republic of Uzbekistan “On the Development Strategy of New Uzbekistan for 2022–2026” dated January 28, 2022, № DP–60 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

50. Methodology for Monitoring and Evaluating the Openness of the Activities of State Bodies and Organizations, approved by Decree of the President of the Republic of Uzbekistan № DP–154 dated June 14, 2022 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

51. Decree of the President of the Republic of Uzbekistan “On Measures to Implement the Administrative Reforms of New Uzbekistan” dated December 21, 2022, № DP–269 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

52. Decree of the President of the Republic of Uzbekistan “On Priority Organizational Measures to Effectively Organize the Activities of the Republic’s Executive Authorities” dated January 25, 2023, № DP–14 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

53. Decree of the President of the Republic of Uzbekistan “On Measures to Effectively Organize Public Administration in the Field of Digital Technologies within the Framework of Administrative Reforms” dated May 24, 2023, № DP–76 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

54. Decree of the President of the Republic of Uzbekistan “On the Strategy ‘Uzbekistan – 2030’” dated September 11, 2023, № DP–158 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

55. Decree of the President of the Republic of Uzbekistan “On Measures to Further Improve the System of State Support for Civil Society Institutions” dated August 26, 2024, № DP–124 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

56. List of Bodies Authorized to Exercise Control over the Activities of Business Entities and Their Areas of Control, approved by Decree of the President of the Republic of Uzbekistan № DP–184 dated November 14, 2024 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

57. Decree of the President of the Republic of Uzbekistan “On the State Program for the Implementation of the Strategy ‘Uzbekistan – 2030’ in the Year of Environmental Protection and the ‘Green Economy’” dated January 30, 2025, № DP–16 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

58. Decree of the President of the Republic of Uzbekistan “On Measures to Increase Efficiency, Proactivity and Effectiveness in the Public Administration System” dated July 14, 2025, № UP–111 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

59. List of Analytical Centers and Research Institutions Whose Activities Are Organized by the Coordinating Council for Strategic Planning and Development under the President of the Republic of Uzbekistan, approved by Decree of the President of the Republic of Uzbekistan № DP–201 dated October 30, 2025 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

60. Decree of the President of the Republic of Uzbekistan “On Additional Measures to Consistently Continue Reforms and Bring Them to a New Stage within the Framework of the Priority Areas of the Country’s Development until 2030” dated February 16, 2026, № DP–21 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

61. Resolution of the President of the Republic of Uzbekistan “On Establishment of the Public Education Information Network of the Republic of Uzbekistan” dated September 28, 2005, № RP–191 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

62. Resolution of the President of the Republic of Uzbekistan “On Organizational Measures to Further Improve the Activities of the Ministry of Justice of the Republic of Uzbekistan” dated April 13, 2018, № RP–3666 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

63. Resolution of the President of the Republic of Uzbekistan “On Measures to Radically Improve the Procedure for Granting Benefits and Preferences” dated May 31, 2018, № RP–3756 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

64. Resolution of the President of the Republic of Uzbekistan “On Establishment of the Tashkent International Arbitration Centre (TIAC) under the Chamber of Commerce and Industry of the Republic of Uzbekistan” dated

November 5, 2018, № RP–4001 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

65. Regulation “On the State Inspectorate for Control in the Sphere of Informatization and Telecommunications of the Republic of Uzbekistan”, approved by Resolution of the President of the Republic of Uzbekistan № RP–4024 dated November 21, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

66. Resolution of the President of the Republic of Uzbekistan “On Establishment of Webster University in Uzbekistan” dated April 10, 2019, № RP–4278 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

67. Resolution of the President of the Republic of Uzbekistan “On Measures to Improve the Quality of Development and Implementation of Projects in the Field of Information and Communication Technologies within the ‘Electronic Government’ System” dated May 21, 2019, № RP–4328 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

68. Resolution of the President of the Republic of Uzbekistan “On Additional Measures to Improve the System for Monitoring the Implementation and Protection of Information Technologies and Communications” dated September 14, 2019, № RP–4452 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

69. Resolution of the President of the Republic of Uzbekistan “On Measures for the Widespread Introduction of the Digital Economy and Electronic Government” dated April 28, 2020, № RP–4699 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

70. Resolution of the President of the Republic of Uzbekistan “On Measures to Create Conditions for the Accelerated Introduction of Artificial Intelligence Technologies” dated February 17, 2021, № RP–4996 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

71. Resolution of the President of the Republic of Uzbekistan “On Measures to Introduce a Special Regime for the Application of Artificial Intelligence Technologies” dated August 26, 2021, № RP–5234 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

72. Resolution of the President of the Republic of Uzbekistan “On Measures to Introduce a Rating Assessment System for the Effectiveness of Anti-Corruption Efforts” dated January 12, 2022, № RP–81 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

73. Resolution of the President of the Republic of Uzbekistan “On Measures to Bring the Information and Communication Technologies Sector to a New Level in 2022–2023” dated August 22, 2022, № RP–357 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

74. Resolution of the President of the Republic of Uzbekistan “On Measures to Increase the Coverage and Quality of Digital Services and to Digitally Transform Sectors, Industries and Regions” dated May 24, 2023, № RP–162 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

75. Resolution of the President of the Republic of Uzbekistan “On Additional Measures to Improve the System for Ensuring Cybersecurity of Critical Information Infrastructure Facilities of the Republic of Uzbekistan” dated May 31, 2023, № RP–167 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

76. Resolution of the President of the Republic of Uzbekistan “On Measures to Improve State Policy and Increase Effectiveness in the Field of Poverty Reduction and Employment” dated October 4, 2024, № RP–347 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

77. Resolution of the President of the Republic of Uzbekistan “On Approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030” dated October 14, 2024, № RP–358 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

78. Resolution of the President of the Republic of Uzbekistan “On Measures Aimed at Further Strengthening Activities to Combat Crimes Committed Using Information Technologies” dated April 30, 2025, № RP–153 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

79. Resolution of the President of the Republic of Uzbekistan “On Additional Measures to Support Projects Based on Artificial Intelligence Technologies” dated October 30, 2025, № RP–320 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

80. Resolution of the President of the Republic of Uzbekistan “On Measures to Improve the System of State Control in the Fields of Information and Digital Technologies” dated December 11, 2025, № RP–371 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

81. Order of the President of the Republic of Uzbekistan “On Organizational Measures Aimed at the Digital Transformation and Increasing the Efficiency of Public Administration” dated November 28, 2025, № O–68 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

82. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Improve the Management Structure in the Field of Mass Communications” dated November 24, 2004, № 555 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

83. List of State Information Resources and State Bodies Responsible for Their Formation, Use and Maintenance, approved by Resolution of the Cabinet of Ministers of the Republic of Uzbekistan № 27 dated February 20, 2006 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

84. Regulation “On the Procedure for Monitoring Compliance with Legislation in the Sphere of Production and Distribution of Printed and Book, Television and Radio, Audiovisual Products and Information Resources on the Internet in the Republic of Uzbekistan”, approved by Resolution of the Cabinet of Ministers of the Republic of Uzbekistan № 132 dated June 28, 2007 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

85. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Approval of the Regulation on the Procedure for Attestation and Advanced

Training of Legal Service Employees” dated November 22, 2007, № 244 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

86. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Additional Measures to Improve the Monitoring System in the Field of Mass Communications” dated August 5, 2011, № 228 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

87. Regulation “On the Procedure for Granting State Social Orders by State Bodies for the Implementation of Socially Significant Projects”, approved by Resolution of the Cabinet of Ministers of the Republic of Uzbekistan № 135 dated February 22, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

88. Regulation “On the Ministry for Development of Information Technologies and Communications of the Republic of Uzbekistan”, approved by Resolution of the Cabinet of Ministers of the Republic of Uzbekistan № 318 dated May 1, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

89. Concept for Activating the Participation of State and Economic Administration Bodies in the Virtual Space, approved by Resolution of the Cabinet of Ministers of the Republic of Uzbekistan № 622 dated August 7, 2018 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

90. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Further Improve Information Security on the World Wide Web” dated September 5, 2018, № 707 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

91. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Introduce a Unified National System for Delivery of Correspondence Sent by State Bodies and Organizations, Confirmation of Delivery, Storage and Recording of Information” dated October 9, 2020, № 637 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

92. Regulation “On the Procedure for Encouraging Persons Who Reported a Corruption-Related Offense or Otherwise Assisted in Combating Corruption”, approved by Resolution of the Cabinet of Ministers of the Republic of Uzbekistan № 829 dated December 31, 2020 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

93. Regulation “On Requirements for Official Websites of Business Entities with State Participation and State Unitary Enterprises”, approved by Resolution of the Cabinet of Ministers of the Republic of Uzbekistan № 81 dated February 19, 2021 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

94. Basic Requirements for Official Websites of State Bodies, Economic Associations and Local Executive Authorities, approved by Resolution of the Cabinet of Ministers of the Republic of Uzbekistan № 373 dated June 15, 2021 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

95. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Additional Measures for the Introduction of an Electronic System for

Proceedings in Cases of Administrative Offenses” dated July 8, 2021, № 431 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

96. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Organization of the Activities of the Research Institute for the Development of Digital Technologies and Artificial Intelligence” dated July 31, 2021, № 475 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

97. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Further Improve the Registration of Taxpayers and Simplify the Procedure for Reimbursement of Value Added Tax” dated September 22, 2021, № 595 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

98. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Approval of the Regulation on the Procedure for Establishing a Special Regime to Support Artificial Intelligence Technologies and Organizing Its Activities” dated November 29, 2021, № 717 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

99. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Further Improve the Mechanisms of Social Partnership and Public Control” dated April 22, 2022, № 208 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

100. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Further Improve the Interagency Electronic Cooperation System and Information Exchange” dated September 20, 2022, № 516 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

101. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Organize the Activities of the Data Processing Center of the Electronic Government System” dated March 14, 2023, № 107 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

102. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Organize Advanced Training and Rating Assessment of Employees Responsible for the Development of Information and Communication Technologies in Republican and Local Executive Authorities” dated May 20, 2023, № 208 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

103. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Approval of the List of Types of Services in the Field of Information and Communication Technologies” dated September 4, 2023, № 447 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

104. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Improve the Human Resources Management System in Republican and Local Executive Authorities” dated September 22, 2023, № 492 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

105. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Approval of the Administrative Regulation for Providing Public Services for Inclusion in the Register of Professional Mediators” dated October 17, 2023, № 544 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

106. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Widely Introduce Advanced Information Technologies into Exchange Trading and to Consistently Continue Digitalization Processes in the Sector” dated September 12, 2024, № 570 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

107. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Increase the Effectiveness of the Public Control System over the Activities of State Bodies and Organizations in Resolving Problems of the Population” dated October 24, 2024, № 695 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

108. Regulation “On the Procedure for Remote Monitoring of Compliance by State Bodies and Organizations with Obligations Established in Normative Legal Acts in the Field of Ensuring Openness”, approved by Resolution of the Cabinet of Ministers of the Republic of Uzbekistan № 910 dated December 30, 2024 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

109. Regulation “On the Procedure for Preparing Information Resources of the Republic of Uzbekistan and Distributing Them through Data Transmission Networks, Including the Internet”, approved by Resolution of the Cabinet of Ministers of the Republic of Uzbekistan № 137 dated March 26, 1999 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

110. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Improve the Management Structure in the Field of Mass Communications” dated November 24, 2004, № 555 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

111. Regulation “On the Procedure for Sale of State Shares”, approved by Resolution of the Cabinet of Ministers of the Republic of Uzbekistan № 279 dated October 6, 2014 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

112. Regulation “On the Procedure for Establishing and Maintaining Official Websites of State Bodies on the Government Portal of the Republic of Uzbekistan Based on the ‘Single Window’ Principle, Ensuring the Relevance and Security of Information Therein, and the Procedure for the Submission by State Bodies of Information to Be Posted on the Government Portal”, approved by Resolution of the Cabinet of Ministers of the Republic of Uzbekistan № 54 dated January 31, 2025 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

113. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Organize the Activities of the Institute for Retraining and Advanced Training of Legal Personnel under the Ministry of Justice of the Republic of Uzbekistan” dated March 19, 2025, № 171 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

114. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Measures to Implement Priority Projects in the Field of Artificial Intelligence Technologies in 2025–2026” dated July 10, 2025, № 425 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

115. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan “On Additional Measures to Expand the Use of Information and Communication Technologies in Public Procurement and Further Improve the Activities of Operators of the Electronic Public Procurement System” dated July 30, 2025, № 476 // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

116. Order of the Minister of Justice of the Republic of Uzbekistan № 308-mh dated December 22, 2010 (registration № 2170, December 22, 2010), approving the Rules for Notarial Record-Keeping in State Notary Offices // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

117. Order of the Minister of Justice of the Republic of Uzbekistan № 53-mh dated March 2, 2012 “On Approval of the General Legal Classifier of the Branches of Legislation of the Republic of Uzbekistan” (registration № 2333, March 2, 2012) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

118. Instruction on the Procedure for Performing Notarial Acts by Notaries, approved by Order of the Minister of Justice of the Republic of Uzbekistan № 2-mh dated January 4, 2019 (registration № 3113, January 4, 2019) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

119. Mediation Training Program, approved by Order of the Minister of Justice of the Republic of Uzbekistan № 54-mh dated January 31, 2019 (registration № 3134, January 31, 2019) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

120. Order of the Director of the National Agency for Perspective Projects of the Republic of Uzbekistan “On Approval of the Rules for Conducting Crypto-Store Activities” dated September 29, 2022, № 43 (October 31, 2022, registration № 3395) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

121. Methodology for Assessing the Performance of Civil Servants Based on Key Performance Indicators, approved by Order of the Director of the Agency for Development of Public Service under the President of the Republic of Uzbekistan № 2-2022 dated November 21, 2022 (registration № 3407, December 28, 2022) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

122. Model Regulation on a Permanent Labour Arbitration, approved by Order of the Minister of Poverty Reduction and Employment of the Republic of Uzbekistan № 62-2023/B dated July 20, 2023 (registration № 3449, July 26, 2023) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

123. Order of the Chairman of the State Security Service of the Republic of Uzbekistan “On Approval of the Regulation on the Procedure for Assessing the Level of Cybersecurity of the Republic of Uzbekistan and the Cybersecurity of Critical Information Infrastructure Facilities” dated September 4, 2023, № 91 (September 22, 2023, registration № 3458) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

124. Resolution of the Board of the Central Bank of the Republic of Uzbekistan “On Approval of the Regulation on Ensuring Information Security and Cybersecurity in Payment Systems of Payment System Operators and Payment Service Providers and Taking Measures to Prevent Offenses Committed Using

Digital Technologies” dated April 24, 2024, № 13/1 (May 21, 2024, registration № 3513) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

125. Order of the Chairman of the State Security Service of the Republic of Uzbekistan “On Approval of the Regulation on the Procedure for Conducting an Examination for Compliance with Cybersecurity Requirements” dated October 15, 2024, № 113 (November 14, 2024, registration № 3573) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

126. Order of the Chairman of the State Security Service of the Republic of Uzbekistan “On Approval of the Regulation on the Procedure for Certification of Hardware, Hardware-Software and Software Tools Used to Ensure Cybersecurity of Information Systems and Resources” dated October 15, 2024, № 114 (November 14, 2024, registration № 3574) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

127. Order of the Chairman of the State Security Service of the Republic of Uzbekistan “On Approval of the Temporary Regulation on the Procedure for Categorizing Critical Information Infrastructure Facilities of the Republic of Uzbekistan and Establishing Their Unified Register” dated October 24, 2024, № 118 (November 11, 2024, registration № 3570) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

128. Order of the Minister of Justice of the Republic of Uzbekistan “On Approval of the Regulation on the Procedure for Submission of Statistical Data by Bar Associations” dated December 20, 2024, № 30-mh (December 23, 2024, registration № 3588) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

129. Rules of Ethics for the Creation, Implementation and Use of Artificial Intelligence-Based Solutions, approved by Order of the Minister of Digital Technologies of the Republic of Uzbekistan № 284-mh dated February 24, 2026 (March 14, 2026, registration № 3787) // lex.uz – National Database of Legislation of the Republic of Uzbekistan.

130. Joint Resolution № 04/4-03-01/17 of the Committee on Innovative Development and Information Technologies of the Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan and the Committee on Youth, Women, Culture and Sports of the Senate of the Oliy Majlis of the Republic of Uzbekistan dated March 25, 2025.

II. Works and Speeches by the President of the Republic of Uzbekistan Sh.M. Mirziyoyev

1. Ш.М. Мирзиёев. Янги Ўзбекистон тараққиёт стратегияси. — Тошкент: “O‘zbekiston”, 2021. — Б. 45, 464.

2. Ш.М. Мирзиёев. Миллий тараққиёт йўлимизни қатъият билан давом эттириб, янги босқичга кўтарамиз. — Тошкент: “O‘zbekiston”, 2017. — Б. 592.

3. Ш.М. Мирзиёев. Буюк келажагимизни мард ва олижаноб халқимиз билан бирга қурамиз. — Тошкент: Ўзбекистон, 2017. — Б. 78.

4. Ўзбекистон Республикаси Президенти Шавкат Мирзиёевнинг 2025 йил 26 декабрдаги Олий Мажлис ва Ўзбекистон халқига Мурожаатномаси // <https://president.uz/uz/lists/view/8834>.

III. Scientific Literature

1. Абдуллаев Ф.А. Кибержиноятларни тергов қилиш методикаси: ўқув қўлланма. – Т.: ТДЮУ нашриёти, 2023. – Б.180.
2. Гуломов С.С., ва б. Рақамли иқтисодиётда инновациялар. – Т.: Иқтисодиёт, 2022. – Б.312.
3. Исмоилов И.А. Криминалистика ва ахборот технологиялари. – Т.: Академия, 2024. – Б.250.
4. Каримов А.К. Ахборот хавфсизлигининг ҳуқуқий асослари: монография. – Т.: Фан ва технология, 2025. – Б.210.
5. Расулов А.Т. Рақамли ҳуқуқ ва киберхавфсизлик. – Т.: Юрист медиа, 2026. – Б.290.
6. Турғунов М. Ахборот тизимларида содир этиладиган ҳуқуқбузарликлар квалификацияси. – Т.: Янги аср авлоди, 2025. – Б. 150.
7. Ҳасанов Б.М. Сунъий интеллект ва ҳуқуқ: муаммолар ва истиқболлар. – Т.: ТДЮУ, 2026. – Б. 195.
8. Сафаев С.К. вопросу о децентрализации и совершенствования государственного управления // Жамият ва бошқарув. 2013. №1. – Б. 25.
9. Муродуллаева Г. Давлат бошқарув тизимида коррупцияни олдини олишнинг асосий усули сифатида манфаатлар тўқнашувини ҳал этиш: юрид. фан. докт. (PhD) дисс. автореферати. – Тошкент, 2024. – Б. 16.
10. Жураев А. Давлат фуқаролик хизматида рағбатлантириш чораларини қўллашнинг ташкилий-ҳуқуқий асослари: юрид. фан. докт. (PhD) дисс. – Тошкент, 2023. – Б. 86.
11. Цифровая гуманитаристика и технологии в образовании (DHTE 2025): сб. статей VI Международной научно-практической конференции. 13-14 ноября 2025 г. | Digital Humanities and Technology in Education (DHTE 2025): Collection of Articles of the VI International Scientific and Practical Conference. November 13-14, 2025. / Под ред. В.В.Рубцова, М.Г.Сороковой, Н.П.Радчиковой. – М.: ФГБОУ ВО МГППУ, 2025. – 607 с.
12. Аганбегян А.Г. Человеческий капитал и его главная составляющая – сфера «экономики знаний» как основной источник социально-экономического роста // Экономические стратегии. – 2017. – №3. – С.66-79.
13. Божечкова А.В., Клячко Т.Л., Кнобель А.Ю., Лощенкова А.Н., Любимов И.Л., Синельников-Мурылев С.Г. Образование и экономический рост. – М.: Издательский дом «Дело» РАНХ и ГС, 2019. – 120 с.
14. Ижтимоий соҳа иқтисодиёти // И.ф.д., проф. Қ.Х. Абдурахмонов таҳрири остида. – Т.: Иқтисодиёт, 2013. – 418 б.
15. Masuda Y. Managing in the Information Society: Releasing synergy Japanese style. Oxford, 1990. – P. 44.
16. Бекмуродов А.Ш. и автор. колл. Человеческое развитие. Учебник. – Т.: Фан ва технология, 2012. – 376 с.

17. Ижтимоий соҳа иқтисодиёти // И.ф.д., проф. Қ.Х. Абдурахмонов таҳрири остида. – Т.: Иқтисодиёт, 2013. – 418 б.
18. Вахабова Д.Х. Социальные инвестиции в человеческий интеллектуальный капитал и оценка их эффективности // Молия. – Т.: 2016. №6. – С. 94-101.
19. Саттикулова Г.А. Инсон капиталини ривожлантириш Ўзбекистонда давлат ижтимоий сиёсатининг муҳим йўналиши сифатида. "XXI asr: fan va ta'lim masalalari" ilmiy elektron jurnali. №2, 2024. – Б. 132-143.
20. Мансурова М.М. Инсон капитали назариясининг шаклланиши ва ривожланиши. – СамИСИ, 2020. Eurofound (2024). Role of human capital inequalities in social cohesion and convergence.
21. A.V.Vaxabov, Zaxidova Sh.Sh., Xajibakiyev va boshqalar. Ijtimoiy siyosat. – Т.: MUMTOZ SO'Z, 2019. – 312 б.
22. Качество образования, эффективность НИОКР и экономический рост: количественный анализ и математическое моделирование / В.А.Садовничий, А.А.Акаев, А.В.Коротаев, С.Ю.Малков. – М.: URSS: ЛЕНАНД, 2016. – 347 с.

IV. Internet Sources

1. https://www.legis.md/cautare/getResults?doc_id=95089&lang=ro.
2. <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000186714>.
3. <https://cbd.minjust.gov.kg/4-4864/edition/1219811/ru>.
4. lex.uz – National Database of Legislation of the Republic of Uzbekistan.
5. <https://home.treasury.gov/policy-issues/tax-policy/tax-expenditures>.
6. <https://www.canada.ca/en/department-finance/services/publications/federal-tax-expenditures.html>.
7. <https://competition-cases.ec.europa.eu/search>.
8. <https://portal.datransparencia.gov.br/>.
9. <https://treasury.gov.au/publication/p2024-489823>.
10. <https://www.treasury.gov.za/documents/national%20budget/2020/>.
11. https://www.mof.go.jp/english/policy/tax_policy/index.html.
12. <https://reestr.uz/>.
13. <https://singlewindow.uz/>.
14. <https://eco.gov.uz/>.
15. <https://agroplatforma.uz/>.
16. <https://gov.uz/uz/ssv>.
17. <https://akkred.uz/uz>.
18. <https://my.soliq.uz/>.
19. <https://www.zakonyprolidi.cz/cs/2014-234>.
20. <https://lexlege.pl/ustawa-o-sluzbie-cywilnej/rozdzial-11-przepisy-przejscowe-i-dostosowujace/1568/>.
21. https://www.consultant.ru/document/cons_doc_LAW_42413/354808bc531bbb6e57c783ceed1cfc54dedc6add/.
22. <https://adilet.zan.kz/rus/docs/V1600014620#z3>.

23. https://www.consultant.ru/document/cons_doc_LAW_48601/e92846ab80fa35d65ffbac3877b3267ae9735e61/.
24. <https://adilet.zan.kz/rus/docs/V2400034501>.
25. https://kodeksy-kz.com/ka/o_gosudarstvennoj_sluzhbe/41.htm.
26. <https://hartran.ee/index.php?id=64>.
27. eesti.ee.
28. <https://murojaat.gov.uz/ru>.
29. <https://xalqnazorati.uz/oz/>.
30. <https://my.gov.uz/uz>.
31. <https://www.borger.dk/>.
32. <https://www.eesti.ee/>.
33. <https://www.oiguskantsler.ee/>.
34. <https://www.retsinformation.dk/>.
35. <https://lifeindenmark.borger.dk/apps-and-digital-services/Digital-Post>.
36. <https://www.ombudsmanden.dk/>.
37. <https://virk.dk/>.
38. <https://www.ombudsmanden.dk/>.
39. riigiteataja.ee.
40. <https://www.borger.dk/>.
41. <https://www.riigiteataja.ee/et>.
42. <https://www.justitsministeriet.dk/>.
43. <https://www.ria.ee/>.
44. <https://riigikantselei.ee/>.
45. <https://digst.dk/>.
46. <https://hoeringsportalen.dk/>.
47. <https://bornetelefonen.dk/>.
48. <https://www.ombudsmanden.dk/>.
49. <https://www.riigiteataja.ee/>.
50. <https://ngo.gov.uz/>.
51. <https://adilet.zan.kz/kaz/>.
52. <https://www.gesetze-im-internet.de/>.
53. <https://www.lrs.lt/>.
54. <https://kansalaisyhteiskunta.fi/>.
55. <https://www.mois.go.kr/frt/a01/frtMain.do>.
56. <https://www.grants.gov/>.
57. <https://e-qaror.gov.uz/>.
58. <https://kengash.gov.uz/>.
59. <https://mahalla.ijro.uz/>.
60. <https://online-mahalla.uz/>.
61. <https://xotin-qizlar.uz/>.
62. <https://yoshlarbalansi.uz/>.
63. <https://ihma.uz/oz>.
64. <https://www.gov.uk/>.
65. <https://opendata.cityofnewyork.us/>.
66. <https://www.gov.uk/>.

67. <https://www.smartnation.gov.sg/>.
68. <https://minuomavalitsus.ee/>.
69. <https://www.gov.uk/>.
70. <https://isap.sejm.gov.pl/>.
71. <https://zaklada.civilnodrustvo.hr/>.
72. <https://likumi.lv/>.
73. <https://edo.ijro.uz/>.
74. <https://my.gov.uz/uz>.
75. <https://reestr.uz/projects?limit=10>.
76. <https://public.sud.uz/report/CONFLICT>.
77. <https://public.sud.uz/report/CRIMINAL>.
78. <https://chatgpt.com/>.
79. https://api.siat.stat.uz/media/uploads/sdmx/sdmx_data_800.pdf.
80. <https://uzinfocom.uz/uz/projects?page=5>.
81. <https://uzinfocom.uz/uz/projects?category=3>.
82. <https://uzinfocom.uz/uz/projects?category=2>.
83. <https://reestr.uz/projects>.
84. <https://kengash.gov.uz/>.
85. <https://e-qaror.gov.uz/>.
86. <https://edo.ijro.uz>.
87. <https://data.egov.uz/data/6113bd0fdb32b99538e08991>.
88. <https://data.egov.uz/data/6113bde9db32b99538e0899b>.
89. <https://data.egov.uz/data/6113c568db32b99538e08ab3>.
90. <https://data.egov.uz/data/6113c59edb32b99538e08ab5>.
91. <https://data.egov.uz/data/6113c68bdb32b99538e08abd>.
92. <https://data.egov.uz/data/6113c6c0db32b99538e08abf>.
93. <https://www.datensicherheit.de/2024-2025-cyber-attack-companies-14-seconds>.
94. <https://cybermap.kaspersky.com/ru/stats>.
95. <https://www.websiterating.com/ru/blog/research/cybersecurity-statistics-facts/#sources>.
96. <https://newsletter.radensa.ru/archives/4840>.
97. <https://www.cenlanow.com/business/press-releases/einpresswire/674883055/cybercrime-damages-to-cost-the-world-9-5-trillion-usd-in-2024/>.
98. <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide#:~:text=The%20global%20cost%20of%20cybercrime,trillion%20U.S.%20dollars%20in%202022>.
99. Ф. Худойкулов. Бир йилда 500 миллиондан ортиқ кибер ҳужумлар уюштирилади. <https://yuz.uz/news/bir-yilda-500-milliondan-ortiq-kiber-hujumlar-uyushtiriladi>.
100. <https://cbu.uz/uz/>.
101. https://media.franceintheus.org/4265/?utm_source.

102. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eiir.org/wp-content/uploads/2022/08/EIIR-4IR-STUDY_OVERVIEW_10_10_20_TEXT.pdf.
103. https://courses.skolkovo.ru/event/cdto-kuznetsov-2/?utm_source=chatgpt.com.
104. <https://ukstories.microsoft.com/features/microsoft-ceo-satya-nadella-on-fuelling-tech-intensity-in-the-uk/>.
105. <https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab/>.
106. <https://play.google.com/store/games?hl=ru&pli=1>.
107. https://t.me/statistika_rasmiy/6256.
108. <https://www.gov.za/documents/other/national-communication-strategy-framework-2025-2030-26-feb-2025>.
109. <https://www.gcis.gov.za/content/about-us/chief-directorates/media-rapid-response/>
110. <https://gcs.civilservice.gov.uk/about-us/what-we-do/>.
111. <https://www.gov.uk/government/news/fact-sheet-on-the-cdu-and-rru?>
112. <https://www.gov.uk/government/news/fact-sheet-on-the-cdu-and-rru>.
113. <https://www.info.gouv.fr/organisation/service-d-information-du-gouvernement-sig>.
114. <https://www.sgdsn.gouv.fr/viginum>.
115. <https://www.bundesregierung.de/breg-en/federal-government/federal-press-office?>
116. https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html.
117. <https://8888.gov.ph/>.
118. <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>.
119. <https://engage.checkpoint.com/2025-ai-security-report/>.
120. <https://www.acma.gov.au/digital-platforms-and-misinformation>.
121. <https://www.state.gov/gec/>.
122. <https://www.tse.jus.br/imprensa/noticias-tse/2024/Marco/programa-de-enfrentamento-a-desinformacao-completa-cinco-anos-de-atuacao>.
123. <https://www.kocsc.or.kr/eng/main.php>.
124. <https://cyber.gc.ca/en/guidance/disinformation>.
125. <https://stratcomcoe.org/>.
126. <https://www.debunk.eu/>.
127. <https://www.pofmaoffice.gov.sg/>.
128. <https://tfc-taiwan.org.tw/>.
129. <https://www.mpi.se/en/>.
130. <https://www.legifrance.gouv.fr/download/pdf?id=wSCtx11Gzpq9uWOcYXc7s1sDFihSq-tW46KWa2ISZzs=>.
131. <https://www.sagafta.org/membership-benefits/young-performers/coogan-law/coogan-law-full-text>.

132. chrome-extension://efaidnbnmnibpcajpcglclefindmkaj/https://www.infrastructure.gov.au/sites/default/files/documents/social-media-minimum-age-and-age-assurance-trial-fact-sheet.pdf.
133. https://www.legifrance.gouv.fr/download/pdf?id=uixn4vDFFJU_veW4xSVamq3PzXyh2U2x_naRfEud_Wg=.
134. https://www.reuters.com/sustainability/boards-policy-regulation/five-eu-states-test-age-verification-app-protect-children-2025-07-14/?utm_source=.
135. <https://www.mim.gov.it/web/guest/home>.
136. <https://www.rijksoverheid.nl/>.
137. <https://www.km.bayern.de/>.
138. <http://pravo.gov.ru/>.
139. <http://en.npc.gov.cn.cdurl.cn/>.
140. <https://adilet.zan.kz/kaz/>.
141. <https://www.arcom.fr/>.
142. https://www.ft.com/content/846e8253-85f0-4666-9655-d9689eb0843f?utm_source=.
143. <https://www.legislation.gov.uk/ukpga/2023/50/contents>.
144. <https://www.dataprotectionauthority.be/citizen>.
145. <https://www.autoriteitpersoonsgegevens.nl/>.
146. <https://www.medietilsynet.no/>.
147. <https://www.bzkg.de/>.
148. <https://www.esafety.gov.au/>.
149. <https://www.garanteprivacy.it/>.
150. <https://www.aepd.es/>.
151. https://www.reuters.com/technology/what-countries-do-regulate-childrens-social-media-access-2024-11-28/?utm_source=.
152. https://www.theguardian.com/media/2024/nov/29/how-australias-tough-social-media-ban-compares-to-laws-in-other-countries?utm_source=.
153. <https://www.kjm-online.de/>.
154. <https://ico.org.uk/>.
155. <https://www.ftc.gov/>.
156. <https://service.kocsc.or.kr/eng/mainPage.do>.
157. <https://www.arcom.fr/>.
158. <https://www.die-medienanstalten.de/organisation/kjm/>.
159. <https://www.microsoft.com/en-us/security>.
160. <https://www.interpol.int/>.
161. jigsaw.google.com.
162. <https://moonshotteam.com/>.
163. <https://www.alibabacloud.com/>.
164. <https://www.tencent.com/en-us/articles/2202171.html>.
165. <https://research.samsung.com/>.
166. <https://ico.org.uk/>.
167. <https://www.bohrium.com/>.
168. <https://ru.duolingo.com/>.

169. <https://ziyonet.uz/uzc>.
170. <https://president.uz/uz/lists/view/7924>.
171. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047046768>.
172. www.atlanticcouncil.org.
173. <https://www.sans.org/emea/>.
174. <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>.
175. file:///C:/Users/%D0%B37/Downloads/https___yuz.uz_file_newspaper_1501d499b4f544b9a3d8408d878d4fb8.pdf.
176. <https://www.justice.gov/criminal/criminal-fraud/file/1292051/dl>.
177. <https://www.legislation.gov.uk/ukpga/2010/23/contents>.
178. https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=62179&type=soga n&key=9.
179. <https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%ED%98%95%EB%B2%95>.
180. <https://www.gesetze-im-internet.de/stgb/>.
181. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/.
182. <https://www.japaneselawtranslation.go.jp/ja>.
183. <https://laws-lois.justice.gc.ca/eng/acts/c-46/>.
184. https://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/cca1995115/sch1.html.
185. <https://sso.agc.gov.sg/Act/CDTOSCCBA1992>.
186. https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/en.
187. <https://www.brocardi.it/codice-penale/>.
188. <https://www.brocardi.it/codice-penale/>.
189. <https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vi32nmht6cz9>.
190. <https://www.gesetze-im-internet.de/stgb/>.
191. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/>.
192. <https://www.legislation.gov.uk/ukpga/1988/27/section/1>.
193. <https://www.legislation.gov.uk/ukpga/2003/21/contents>.
194. <https://www.tribunal-de-paris.justice.fr/75>.
195. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154/.
196. <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032627231>.
197. https://tel.directory.gov.hk/index_HKPF_ENG.html.
198. <https://www.icj.org/wp-content/uploads/2012/12/Thailand-Computer-Crime-Act-2007-eng.pdf>.
199. https://data.thailand.opendevdevelopmentmekong.net/en/laws_record/2562/resource/ec616be5-9fbf-4071-b4b5-cb1f3e46e826.
200. https://data.opendevdevelopmentmekong.net/dataset/329b4f41-f309-4348-9015-23c6f62d5fb4/resource/ea9a61bc-fba9-41ae-9dd0-d31ca5f36ff5/download/843708_0001.pdf.
201. https://www.bka.de/EN/Home/home_node.html.

202. <https://www.fbi.gov/investigate/cyber>.
203. https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html
204. <https://nj.gov/njsp/division/investigations/cyber-crimes.shtml>.
205. <https://da.santaclaracounty.gov/home>.
206. <https://www.ca.gov/departments/223/>.
207. https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/philippines/pop_up.
208. <https://www.cisa.gov/>
209. https://www.bsi.bund.de/EN/Home/home_node.html.
210. <https://cyber.gouv.fr/en>.
211. <https://www.bsc-icc.com/service/cert-in>.
212. <https://www.cse-cst.gc.ca/en>.
213. <https://www.csa.gov.sg/contact-us>.
214. <https://www.kisa.or.kr/EN>.
215. <https://www.csa.gov.sg/contact-us>.
216. <https://www.kisa.or.kr/EN>.
217. <https://www.who.int/>.
218. <https://gdpr-info.eu/>.
219. <https://cctld.uz/stat/>.
220. https://license.gov.uz/registry?filter%5Bdocument_id%5D=4603&filter%5Bdocument_type%5D=LICENSE&page=177.
221. <https://oldmy.gov.uz/ru/>
222. <https://cbu.uz/oz/credit-organizations/banks/branches/>
223. <https://cbu.uz/oz/credit-organizations/banks/atm/>
224. <https://cbu.uz/oz/payment-systems/documents-license-applicati/operators-of-payment-systems/>
225. https://bank.uz/uz/cards?PAGEN_4=18/
226. <https://cbu.uz/oz/payment-systems/documents-license-applicati/payment-organizations/>
227. <https://cbu.uz/oz/credit-organizations/microcredit/>.
228. <https://www.sirstat.uz/uz/matbuot-markazi/qo-mita-yangiliklar/15232-qaysi-sohalarda-tadbirkorlik-subyektlari-ko-proq>.
229. <https://president.uz/uz/lists/view/7924>.
230. <https://lex.uz/docs/1461329>.
231. <https://lex.uz/docs/1304112>.
232. <https://lex.uz/docs/111453?otherlang=1>.
233. https://www.consultant.ru/document/cons_doc_LAW_10699/6411e005f539b666d6f360f202cb7b1c23fe27c3/.
234. https://www.consultant.ru/document/cons_doc_LAW_149092/.
235. https://drive.google.com/file/d/1ctKcLoMP8UaC5BgGscM_SAIOi8fjYlh/view.
236. <https://icsc.un.org/Resources/General/Publications/standardsE.pdf>.
237. <https://www.un.org/ru/library/page/databases>.

238. https://www.oas.org/en/sla/dil/inter_american_treaties_B-58_against_Corruption.asp.
239. <https://au.int/en/treaties/african-union-convention-preventing-and-combating-corruption>.
240. <https://star.worldbank.org/sites/star/files/Arab-Convention-Against-Corruption.pdf>.
241. <https://www.oic-oci.org/docdown/?docID=9774&refID=4268>.
242. <https://www.oecd.org/en/topics/fighting-foreign-bribery.html>.
243. <https://legalinstruments.oecd.org/public/doc/205/205.en.pdf>.
244. <https://rm.coe.int/168007f3f5>.
245. <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=173>.
246. <https://rm.coe.int/168007f3f6/>
247. <https://www.coe.int/en/web/greco/publications>.
248. <https://rm.coe.int/168007bd23>.
249. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024L1640>.
250. <https://docs.cntd.ru/document/901934984>.
251. <https://rm.coe.int/0900001680910ecf>.
252. <https://rm.coe.int/16805e2e52>.
253. <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=198>.
254. <https://sectsco.org/>.
255. <https://rus.sectsco.org/20240704/1600099.html>.
256. <https://lex.uz/uz/docs/1801724>.
257. <https://documents.un.org/doc/undoc/gen/n24/426/76/pdf/n2442676.pdf>.
258. <https://www.un.org/en/ga/68/resolutions.shtml>.
259. https://www.itu.int/en/ITU-D/Regional-Presence/UN/Documents/GA_Resolutions_ICTs/ares68d198_en.pdf.
260. https://www.itu.int/en/ITU-D/Regional-Presence/UN/Documents/GA_Resolutions_ICTs/ares69d204_en.pdf.
261. <https://www.un.org/en/ga/70/resolutions.shtml>.
262. https://www.itu.int/en/ITU-D/Regional-Presence/UN/Documents/GA_Resolutions_ICTs/ares70d184_en.pdf.
263. https://www.itu.int/en/ITU-D/Regional-Presence/UN/Documents/GA_Resolutions_ICTs/ares71d212_en.pdf.
264. https://www.itu.int/en/ITU-D/Regional-Presence/UN/Documents/GA_Resolutions_ICTs/ares72d200_en.pdf.
265. file:///C:/Users/%D0%B37/Downloads/A_RES_72_186-RU.pdf.
266. https://www.itu.int/en/ITU-D/Regional-Presence/UN/Documents/GA_Resolutions_ICTs/ares73d218_en.pdf.
267. <https://www.coe.int/ru/web/impact-convention-human-rights/convention-on-cybercrime>.
268. <https://www.coe.int/en/web/cybercrime/home>.

269. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016L1148>.
270. <https://rus.sectesco.org/documents/?offset=420>.
271. <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>.
272. https://store accuristech.com/standards/itu-t-x-1205?product_id=2874775&srsltid=AfmBOooDhzvjNp457MgaYJ9Djr4G7oOmb_gVFAPeCmB2o9ji_KjSUH5F.
273. <https://www.nist.gov/cyberframework>.
274. <https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en>.
275. <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27032:ed-2:v1:en>.
276. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.
277. <https://www.isaca.org/resources/cobit/cobit-5>.
278. <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2010-03-04;28!vig=>.
279. <https://www.resmigazete.gov.tr/eskiler/2017/10/20171025-8.htm>.
280. <https://www.resmigazete.gov.tr/eskiler/2011/02/20110214-1-1.htm>.
281. <https://resmigazete.gov.tr/eskiler/2013/11/20131128-1.htm>.
282. <https://resmigazete.gov.tr/eskiler/2012/06/20120622-1.htm>.
283. <https://www.legislation.gov.au/C2004A00275/2019-03-10/text>.
284. <https://legislation.nsw.gov.au/view/html/inforce/current/act-1994-046>.
285. <https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1994-091>.
286. <https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4640-2019/arthro-6-nomos-4640-2019-ypohreotiki-arhiki-synedria>.
287. <https://legislatie.just.ro/Public/DetaliuDocument/71928>.
288. <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/95539982609f11e7a53b83ca0142260e>.
289. <https://me.propisi.net/zakon-o-alternativnom-rjesavanju-sporova/>.
290. <https://www.congress.gov/bill/105th-congress/house-bill/3528>.
291. <https://www.legislation.gov.uk/uksi/2011/1133/contents/made>.
292. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070933/.
293. <https://adilet.zan.kz/rus/docs/K1400000234>.
294. <https://adilet.zan.kz/rus>.
295. https://consumer-redress.ec.europa.eu/site-relocation_en.
296. https://consumer-redress.ec.europa.eu/index_en.
297. <https://bilirkisi.uyap.gov.tr/giris>.
298. <https://play.google.com/store/apps/details?id=tr.gov.adalet.edurusma&hl=ru>.
299. <https://arabulucu.uyap.gov.tr/main/arabulucu/index.jsp?v=3785>.
300. <https://cjts.judiciary.gov.sg/home>.
301. <https://e-estonia.com/e-estonia-briefing-centre-services/about-us/>.
302. <https://www.rik.ee/en/international/ai-solutions>.
303. <https://eng.scourt.go.kr/eng/judiciary/eCourt/eTrials.jsp>.

304. <https://www.difccourts.ae/rules-decisions/practice-directions/practical-guidance-note-no-1-2023-difc-courts-virtual-hearing-and-bundling-protocol>.
305. <https://www.utcourts.gov/en/about/miscellaneous/law-library/research/utah.html>.
306. <https://webstore.ansi.org/standards/ds/dsisoiec270372013>.
307. <https://http.uni.com/en/uni-11742-2019>.
308. <https://www.lsti-certification.fr/fr-FR/Nos-offres-entreprises/Cybersecurite/Qualification-PRIS>.
309. https://www.aec.es/wp-media/uploads/DPD-00266.SEG-GUI-004-CCN-STIC-817_Gestion_de_Ciberincidentes_ENS.pdf.
310. <https://access.redhat.com/compliance/ccn-stic>.
311. <https://webstore.iec.ch/en/publication/11317>.
312. <https://meganorm.ru/Data2/1/4293768/4293768989.pdf>.
313. <https://standards.iteh.ai/catalog/standards/iso/1a0f0032-a18e-4c41-baef-932b9c410aa5/iso-iec-27037-2012>.
314. <https://www.iso.org/standard/44381.html>.
315. <https://www.europol.europa.eu/publications-events/main-reports/iocta-report>.
316. <https://www.enisa.europa.eu/news/enisa-news/determining-the-real-economic-impact-of-cyber-incidents-a-mission-almost-impossible>.
317. <https://csrc.nist.gov/pubs/sp/800/30/r1/final>.
318. <https://csrc.nist.gov/pubs/sp/800/55/r1/final>.
319. <https://www.court.gov.cn/>.
320. <https://www.meity.gov.in/>.
321. <https://www.kcc.go.kr/>.
322. <https://www.gov.kz/>.
323. <https://e-anticor.uz/oz>.
324. https://www.uzedu.uz/y3/page/press_reliz.