World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-53, December,-2025
ISSN: 2749-3601

AI GOVERNANCE IN UZBEKISTAN: LEGAL FRAMEWORKS AND ETHICAL CONSIDERATIONS

Ikromov Dostonbek Akhmadjon ugli
Center for Mass Communications under the Administration
of the President of the Republic of Uzbekistan
Leading Specialist

Article history:

Received: 14th September 2025
Accepted: 10th October2025

Abstract:

Global economies and governance structures are changing as a result of artificial intelligence (AI), which presents both revolutionary opportunities and serious threats to ethical standards, public trust, and data privacy. Uzbekistan ranks 70th in the AI Readiness Index and faces challenges in AI governance due to underdeveloped legal frameworks and lack of ethical standards. This article analyzes Uzbekistan's current AI regulatory environment, data privacy issues, and ethical considerations in light of global practices, proposing recommendations aligned with international standards and local needs.

Keywords: AI regulation, data privacy, ethical governance, algorithmic bias, data misuse, real-time and autonomous decision-making, disinformation, bias mitigation, human oversight, transparency, Uzbekistan.

INTRODUCTION

Globally, the swift development of artificial intelligence (AI) technologies are transforming governance, industries, and social interactions. AI offers a wide range of prospects for development and efficiency across numerous industries, from improving data-driven decision-making to automating public services. Its widespread use, however, presents serious issues, such as breaches of data privacy, moral conundrums, and the possibility of abuse, such as deepfake or false information produced by AI. For Uzbekistan, an emerging economy hoping to integrate AI into its digital transformation agenda, the timing couldn't be better. Ranking 70th in the world's AI Readiness Index[1] (Oxford Insights, 2024), Uzbekistan may fall behind developing countries due to its underdeveloped legal system, lack of technical expertise, and absence of AI-specific ethical standards. This article offers a roadmap for responsible AI governance after analyzing the current legal environment in Uzbekistan with an emphasis on data privacy and ethical issues.

CURRENT STATE OF AI REGULATION IN UZBEKISTAN

Uzbekistan's legal framework for AI is still in its early stages, and there is no specific law that deals with the technology's unique risks and uses. The Law on Personal Data[2] (2019) sets the rules for protecting data. Articles 5 and 19 say that data must be lawful, confidential, accurate, and secure. However, it doesn't take into account problems that are unique to AI, like automated data processing, algorithmic bias, or creating deepfake or falsified content. Two key policy documents signal Uzbekistan's commitment to AI development: Presidential Decree "On Measures to Create Conditions for the Rapid Introduction of Artificial Intelligence Technologies"[3]. This decree outlines priorities for AI infrastructure, workforce training, and regulatory development. A second key document is the Strategy for the Development of Artificial Intelligence Technologies until 2030 approved by Resolution No. PD-358 "On Approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030"[4] which emphasizes creating a unified normative-legal base, fostering innovation, and ensuring AI safety and transparency.

Despite these initiatives, implementation remains limited. The AI Readiness Index[5] (Oxford Insights, 2024) ranks Uzbekistan 70th globally, citing deficiencies in regulatory clarity, human capital, innovation capacity, technical expertise, and infrastructure. One of the biggest problems is that there is no AI-specific law. Uzbekistan does not have a comprehensive law to regulate AI systems, unlike the

[1] https://oxfordinsights.com/ai-readiness/ai-readiness-index/
[2] https://lex.uz/docs/4831939
[3] https://lex.uz/docs/-5297046
[4] https://lex.uz/ru/docs/-7158604
[5] https://oxfordinsights.com/ai-readiness/ai-readiness-index/

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-53, December,-2025
ISSN: 2749-3601

EU, which passed the AI Act in 2024[6]. This creates gaps in addressing algorithmic discrimination and false information. The main challenge is a fragmented regulatory framework. Current laws, like the Law on Personal Data, do not address the complexities of AI. This is especially true in areas such as real-time data processing and autonomous decision-making. According to this law, individuals have the right to avoid decisions made entirely by automated systems that could affect their rights or freedoms, unless the decision is necessary for a contract or based on clear consent. The new law on regulating relations arising from the use of AI[7] (15.03.2025) suggests a restriction stating that "decisions affecting human rights and freedoms must not be based solely on AI conclusions." The project defines the concept of "artificial intelligence", establishes the main directions of state policy in the field and the tasks of a specially authorized body, and sets out general rules for the use of artificial intelligence in the creation of information resources.

However, the various levels of AI risks are not categorized, and there are no clear demands or specific rules about human oversight, though some general guidelines do exist. Considering real-time data processing, there are still no specific standards for high-risk AI that uses biometric ID and health monitoring. These systems must meet strict requirements such as accuracy, cybersecurity, risk management, and conformity assessment before they can be introduced. Additionally, mandatory data localization under the law "On Personal Data" may restrict cross-border data flows. This restriction can be reconsidered if strong safeguards for transferring personal data used in AI systems are put in place by stakeholders.

The lack of trained legal and technical professionals makes effective AI governance difficult, as noted in the AI Readiness Index. The Research Institute for the Development of Digital Technologies and Artificial Intelligence (AIRI) was established to prioritize fundamental and applied research. However, its team lacks practical experience.

While policy documents set ambitious goals, the lack of practical enforcement mechanisms reduces their effectiveness. A new law is expected to require labels for AI-generated content in media or online spaces. Moreover, labeling for high-risk AI interactions must also become legally required when users are involved. Although national laws restrict harmful autonomous decision-making, they still lack a risk-based classification system, such as the categories of unacceptable, high, limited, and minimal risk as recognized in the EU.

Current regulations aim to facilitate the quick introduction of AI technologies and their widespread use by ensuring access to digital data and its quality. They also focus on creating good conditions for training qualified professionals in this field. This approach is somewhat reasonable, as the country is still developing in terms of AI maturity and use. Nevertheless, this fact should not hinder the need to integrate international standards and policies for AI into national legislation, while also addressing the interests of the country and local users. These challenges highlight the urgent need for a strong, AI-specific regulatory framework to support Uzbekistan's digital transformation while managing risks.

DATA PRIVACY AND AI: CHALLENGES AND OPPORTUNITIES

1. Privacy Risks from AI-Driven Phishing and Data Misuse

AI systems rely on large datasets that include personal data, which pose significant privacy risks in Uzbekistan. There is a growing trend of AI-generated phishing attacks using the identities of celebrities, public figures, and high-ranking officials to trick users. Over the past five years, the number of cybercrimes in our country has increased 68-fold, and just in 2024, it increased 9.1 times compared to 2023. As a result of these crimes, funds belonging to citizens were stolen, amounting to over 1 trillion 909 billion UZS.

If in 2019, 863 crimes of 18 types were committed using information technologies and the Internet, then in 2024, 58,800 crimes of 62 types were registered. A significant increase in the share of cybercrimes in overall crime is also observed, making the need for their prevention even more urgent. If in 2023, the share of cybercrimes in overall crime was 6.2 percent, in 2024 it reached 44.4 percent, with almost every second crime being committed online or in an electronic way. The majority of cybercrimes (98%) consist of crimes related to bank cards (cyber theft and cyber fraud).

Cybercrimes are primarily committed using the following methods:

- 60% – by gaining control over a bank card or mobile device through the sending of malicious phishing links and programs;
- 16% – by obtaining an SMS code confirming control of a bank card and accounts in mobile applications, using various fraudulent schemes;

[6] https://artificialintelligenceact.eu/the-act/

[7] https://parliament.gov.uz/news/suniy-intellektni-qollash-orqali-yuzaga-keladigan-munosabatlar-tartibga-solinadi

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-53, December,-2025
ISSN: 2749-3601

- 4% – by applying for an online loan in the name of an individual;
- 11% – through fraud on online trading platforms;
- 9% – by attracting funds from citizens through various fraudulent schemes.[8]

These attacks are often disguised as social surveys, quick investment schemes, financial aid, loans, job offers, or deposit scams, and they target sensitive personal and credential information have concrete consequences reflected in official statistics.

Moreover, 2021 Voice AI Challenge Uzbekistan[9] hackathon was possible due to the creation of the first digital dataset of Uzbek voice as part of Mozilla Foundation's Common Voice initiative[10]. While this hackathon collected a large Uzbek-language voice dataset (975 total, 202 checked hours as per 03.04.2023) and brought together stakeholders, it also revealed that Uzbek-language voice and speech datasets remain under-resourced compared to global standards, limited scale of datasets may affect the quality and robustness of voice models for Uzbek language and a shortage of highly qualified AI professionals, especially in niche areas like voice-AI, speech-processing is noted. Also, robustness and potential challenges of voice models require mature regulation and governance regarding voice biometrics, data consent.

To tackle this, Uzbekistan should adopt AI governance framework aligned with OECD/UNESCO AI Ethics principles, which maintains the balanced oversight and mandate informed consent for collecting voice data and standardizing of anonymization. This would ensure that personal data used in training or inference meets strict privacy standards. Public awareness campaigns, promoting media literacy and public education on identifying phishing and synthetic voices and AI-driven fraud detection tools developed under AIRI's direction could also help reduce phishing risks.

2. Disinformation and Deepfake Manipulation

Another major concern is disinformation, especially deepfake and misleading AI-generated content that manipulate public opinion during global conflicts like those in Gaza and Ukraine. These campaigns often target religious communities in Uzbekistan, taking advantage of cultural sensitivities to create division or sway views on international issues. The lack of strong content verification mechanisms makes this threat worse. Additionally, there is a troubling amount of disinformation in video platforms like YouTube and RuTube, where misleading thumbnails, titles, and hashtags promote undisclosed AI-generated content aimed at manipulating public perceptions of political figures, or sensitive socio-political issues like migration policy, elections, or referendums.

To combat disinformation, Uzbekistan should set up a task force with online platforms (similar to the AI Content Verification Taskforce in the USA) to create real-time detection tools for deepfake and false narratives. Following the EU AI Act's requirements for transparency in high-risk AI systems, Uzbekistan could mandate watermarking and tracking the source of AI-generated content to improve traceability and trust.

3. Transparency Gaps in AI Regulation

Current regulations in Uzbekistan, which fall under the "Digital Uzbekistan - 2030" strategy, require only basic labeling of AI systems. They do not mandate clear processes for AI decision-making or documentation of AI logic and data use. This lack of transparency increases the risk of opaque AI systems that can undermine user trust and enable data misuse. To meet global standards, such as the EU AI Act, Uzbekistan should require technical transparency from developers. This would involve providing clear explanations of AI decision-making and keeping auditable records. AIRI could take the lead in creating a National AI Transparency Framework, which would include tools for understanding AI models and regular compliance audits, particularly for high-risk areas like healthcare or public administration.

4. Dataset Quality and Fairness

The quality of datasets used in AI systems directly affects their fairness, gender bias, regional disparities and reliability. Uzbekistan currently does not have standards for dataset quality, bias testing, or fairness metrics. When it comes to formal standards for data quality in AI systems, there is not yet a clearly articulated or publicly accessible standard framework. Existing standards for processing personal data includes the following principles:

- compliance with the constitutional rights and freedom;
- the lawfulness of the purposes and methods of processing;

[8] https://gov.uz/ru/iiv/news/view/57775

[9] https://it-park.uz/en/itpark/news/in-uzbekistan-mitc-it-park-and-undp-organize-hackathon-called-voice-ai-challenge-uzbekistan

[10] https://www.undp.org/uzbekistan/stories/young-people-develop-ai-solutions-uzbek-language

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-53, December,-2025
ISSN: 2749-3601

- the accuracy and reliability;
- the confidentiality and protection;
- the equality of rights of subjects, owners and operators;
- the security of the individuals, society and the state.

As it can be seen, there is no core standards for AI dataset quality, but some principles exist for personal data. Internationally adopted main requirements like completeness, consistency, currency, representativeness, validity, relevance, fairness, traceability should be determined by legislation. Lack of unified framework creates a risk of biased AI outputs that could discriminate against specific groups, such as ethnic or religious minorities. For instance, during the Voice AI Challenge Uzbekistan hackathon lots of experts identified that speech datasets collected during the hackathon remain under-resourced compared to global standards with its deficiencies in quantity, quality and representativeness which may lead to the higher error rates, poor handling of accents, unnatural Text-to-Speech (TTS), limited vocabulary in training AI.

To tackle this issue, Uzbekistan should implement mandatory bias audits and fairness metrics, such as demographic parity or equal opportunity for AI systems, perhaps using UNESCO's AI Ethics Recommendations as a guideline. AIRI could create a Dataset Quality Certification Program to ensure datasets meet international standards for diversity, accuracy, and ethical sourcing.

5. Sector-Specific Regulation and Accountability

AI's quick adoption in Uzbekistan's public and private sectors, including finance, healthcare, cadaster, and media, calls for regulations specific to each sector for autonomous and real-time data processing. Existing laws do not address potential nuances, which could create gaps in accountability. For example, real-time AI in financial services could misuse sensitive data without proper oversight. When fraud detection tools, credit scoring algorithms, or trading bots — process huge amounts of personal and financial data instantly. If these systems are not properly supervised, they can misuse or expose sensitive data in several ways. Potential risks entail the following consequences:

- insecure storage or share of information used credit scoring to third-parties,
- discriminatory decision-making in healthcare service basing on specific backgrounds (area, gender, race, religion and etc.),
- non-official track for ownership histories in cadastral databases,
- user profiling and micro-targeting of audiences in case of privacy breach of behavioral data, viral spread of deepfake and misinformation made by using the identities of highest public officials or information of public importance, biased content recommendation prioritizing sensational or politically biased stories caused from more clicks in media.

To address these, Uzbekistan should develop sector-specific AI guidelines, prioritizing high-risk areas like healthcare (e.g., AI diagnostics) and finance (e.g., credit scoring). Relevant authorities should conduct conformity assessments, establish risk management frameworks, and ensure ongoing monitoring. These guidelines could reflect the EU AI Act's risk-based approach by categorizing AI systems based on their risk level and imposing stricter controls on high-risk applications.

6. Building a Robust Compliance Ecosystem

To overcome enforcement challenges, Uzbekistan needs a solid compliance system, starting with a dedicated AI regulatory body under Ministry of Digital Technologies to handle audits and enforce standards. This body should require AI developers to submit risk assessments before deployment, based on AIRI's research on high-risk AI systems. Next, there should be public reporting requirements; national legislation must require annual transparency reports from AI providers that outline data use, bias mitigation efforts, and compliance actions. Finally, international collaboration is crucial. By accelerating joint projects with global organizations like UNDP and adopting best practices—such as the GDPR's adequacy framework or the EU's MCC-AI for high-risk AI procurement—Uzbekistan can strengthen its position among global leaders in this field.

ETHICAL FRAMEWORKS FOR AI: LOCAL NEEDS AND GLOBAL LESSONS

As AI systems become more independent and driven by data, they raise important ethical issues about privacy, fairness, accountability, transparency, and human rights. Without ethical oversight, AI can unintentionally increase social inequalities, promote algorithmic bias, and allow for mass surveillance or manipulation of public opinion. Establishing global ethical frameworks for AI is crucial to ensure that technological advancements benefit humanity rather than just profit or control. These frameworks promote values such as trust, non-discrimination, and responsible innovation, enabling societies to balance progress with protection. Because digital systems are interconnected, AI ethics must be a global effort; one

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-53, December,-2025
ISSN: 2749-3601

country's misuse of AI can impact others through data sharing, misinformation, or cross-border platforms.

In short, AI ethics are important worldwide because they define how humanity can use smart technologies safely, fairly, and sustainably, keeping humans at the center of AI development.

Ethical governance is vital to ensure AI systems reflect societal values and uphold fundamental rights. Principles like human oversight, transparency, technical reliability, and fairness are becoming increasingly important for the responsible use of AI. Currently, Uzbekistan lacks enforceable ethical guidelines for AI, which makes it susceptible to misuse.

Uzbekistan's local needs in creating an Ethical Framework for AI fall into five key areas: institutional oversight, data quality, localization and access, transparency and understanding, and ethical education and digital literacy, as well as cultural and social context. The absence of an independent body in charge of AI ethics and risk assessment creates gaps in accountability and oversight. Without an independent ethics authority, AI governance may be reactive, only addressing issues after harm has occurred. Therefore, establishing a national AI Ethics body to evaluate AI systems, ensure compliance, and coordinate with global organizations is a potential solution.

Next, the current Law on Personal Data mandates that citizens' data be stored locally, which limits access to diverse datasets for AI training. Local datasets often lack representativeness in terms of gender, region, and language. Consequently, poor data quality can lead to biased algorithms and reduce the reliability of AI systems, ultimately undermining public trust. To address this, policymakers should create trusted data-sharing frameworks and standards that protect privacy while enabling responsible innovation, allowing for anonymized, cross-border research collaborations.

Additionally, many digital systems in governance and banking in Uzbekistan implement automated decision-making without clear public explanations. The lack of clarity and accessibility erodes trust and citizens' rights, especially when AI influences access to services or justice. To tackle this, authorities should require that AI-driven decisions affecting individuals include a "human-in-the-loop" review and a right to explanation, similar to the EU's AI Act and GDPR.

Furthermore, the level of ethical education and digital literacy is low compared to leading AI countries. Lack of proper digital ecosystem with unreliable electricity and internet access would hinder the balanced and rapid growth in AI education. Digital divide between the capital and regions excludes the edge areas from this type of education. Next big challenge related to localization crisis. There is a critical shortage of educational content that reflects local languages, cultural values, and socio-cultural norms of Uzbekistan. Without this contextualization, there is a risk of imposing Western-centric ethical frameworks, which can be irrelevant or even harmful when applied to local contexts. This is closely tied to a lack of local data, as AI models trained only on data from the developed world will perform poorly as for now.

Public understanding of AI, algorithms, and data privacy remains limited despite some projects and university programs. AI ethics is not systematically taught in most universities or in public administration training. Including AI ethics modules in university programs and public and private sector training could boost awareness and interest among the public. Promoting media and digital literacy campaigns for citizens can help develop informed judgment regarding AI ethics.

Lastly, Uzbekistan's cultural values, such as social harmony, respect for elders, and family roles, should be reflected in AI ethics. Simply importing ethical models from culturally different regions may not align well with local societal norms. To gain legitimacy, ethical principles must resonate culturally, be acceptable, and not seen as externally imposed. In this context, creating a hybrid ethical framework—combining international standards (like human rights, transparency, and accountability) with local values such as social responsibility ("mahalla" values)—should be a priority in establishing ethical guidelines. For instance, collective responsibility value shifts focus from purely individual harm to community-level impact and before deploying a high-risk AI system (e.g., in hiring, credit scoring, or public services), companies must assess and mitigate its potential impact on social equity and community structures in specific mahallas. Another example could be the case when implementing AI hiring systems in public administration, mahalla-based principles could require that hiring decisions are reviewed by community representatives before final implementation, ensuring algorithmic decisions don't undermine social cohesion. Mediation in Uzbek communities prioritizes reconciliation over purely punitive measures or conflict, so create a non-judicial, community-based body where citizens can bring complaints about AI systems can be considered in policy-making. AI-powered products leveraging mahalla values means building an AI governance model that is decentralized, community-focused, restorative, and deeply rooted in local trust and values.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-53, December,-2025
ISSN: 2749-3601

Global approaches to AI ethics differ widely. Key international models to consider include the UNESCO Recommendation on the Ethics of AI[11] (2021), OECD AI Principles (2019), EU AI Act (2024), and U.S. AI Bill of Rights (2022). Unanimously adopted by 193 Member States in November 2021, the UNESCO Recommendation on the Ethics of Artificial Intelligence is the first global framework for AI ethics. It offers a universal set of principles and policy guidelines to ensure that AI development and use stay human-centered, rights-based, and inclusive.

The Recommendation highlights four key ethical principles:

• Respect for Human Rights and Dignity. AI design and use should support fundamental human rights and dignity, including privacy, freedom of expression, and equality.

• Environmental and Social Well-being. AI should help achieve sustainable development, ecological balance, and the well-being of societies.

• Fairness and Non-discrimination. AI applications must be designed to reduce social or gender bias and promote equal opportunities for all groups.

• Transparency and Accountability. Developers and governments must ensure AI systems are understandable, traceable, and subject to human oversight.

To implement these principles, UNESCO recommends:

• Establishing ethical impact assessments before deploying AI.

• Creating independent oversight bodies for AI governance.

• Promoting data governance and privacy protection.

• Supporting education and capacity-building in AI ethics.

The EU's AI Act and Singapore's Model AI Governance Framework[12] require ethical compliance for high-risk systems. They emphasize human oversight, transparency, and accountability, striking a balance between innovation and ethics while supporting startups. Key elements of these approaches include mandatory disclosure of AI processes to users to ensure informed consent. They also regulate algorithmic bias to prevent discrimination, especially in public service applications, and establish mechanisms to investigate and address ethical violations. There are penalties for non-compliance to ensure the rules are followed. In contrast, Japan (Act on the Promotion of Research, Development and Utilization of Artificial Intelligence-Related Technologies)[13] and South Korea (South Korean AI Act[14]) focus on innovation and collaboration between public and private sectors. However, they lack thorough ethical regulations and rely on industry self-regulation along with some oversight of AI content platforms.

For Uzbekistan, these recommendations provide a base model for developing national AI policies that align with universal values while respecting local circumstances. The aim is to balance rapid digital transformation with ethical responsibility, ensuring AI benefits people and does not infringe on their rights or cultural diversity. These points should be included in a broader AI law to ensure they are enforceable, taking cues from the EU and Singapore's mandatory approach while adjusting to Uzbekistan's innovation-driven environment.

CONCLUSION

A comparison of global AI governance frameworks shows various approaches that Uzbekistan can use in its situation. Based on these findings, the following recommendations are suggested:

- Develop a dedicated new version AI Law (current version was adopted but not open to public use and lacks comprehensive framework in regulation) as soon as possible as the deadline (by late 2021) set in accordance with Presidential Resolution "On measures for creating conditions for the accelerated introduction of artificial intelligence technologies" for establishing a regulatory framework in the field of artificial intelligence already expired and the field itself continues developing. This law should classify systems by risk, such as high, medium, or low. It should also set specific requirements for data protection, ethical compliance, transparency.
- Add auditing provisions for AI systems to ensure they meet legal and ethical standards.
- Strengthen data privacy regulations by updating the Law on Personal Data. This update should tackle AI-related risks like unauthorized data sharing, deepfake misuse, and algorithmic bias.
- Require risk assessments for AI systems that handle personal data, especially in public services, healthcare, and media.
- Create an authorized state body in the field of AI to oversee compliance and investigate any breaches.
- Set ethical guidelines by forming an AI ethics board. This board should create and enforce principles such as human oversight, transparency, and fairness.

[11] https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence
[12] https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework
[13] https://www.ibanet.org/japan-emerging-framework-ai-legislation-guidelines
[14] https://www.linkedin.com/pulse/united-korean-ai-act-bill-contents-comparison-eu-english-min-h98kc/

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-53, December,-2025
ISSN: 2749-3601

Balancing ethical requirements with local cultural values and innovation incentives is essential. Support for AI startups—through tax breaks, grants, or regulatory sandboxes—can accelerate adoption without compromising regulatory standards.

- Create a regulatory sandbox similar to Singapore's. This space will allow startups to test AI applications under controlled conditions, reducing costs and risks.
- Invest in training programs for legal and technical experts to address gaps identified in the AI Readiness Index through secondary and higher education.

REFERENCES:

1. Oxford Insights. *Government AI readiness index 2024* [Electronic resource]. URL: https://oxfordinsights.com/ai-readiness/ai-readiness-index/
2. Law of the Republic of Uzbekistan "On Personal Data," No. LRU-547, 02.07.2019 [Electronic resource]. URL: https://lex.uz/docs/4831939
3. Resolution of the President of the Republic of Uzbekistan "On measures for creating conditions for the accelerated introduction of artificial intelligence technologies" No. RP-4996, 17.02.2021 [Electronic resource]. URL: https://lex.uz/docs/7573787
4. Resolution of the President of the Republic of Uzbekistan "On the approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030" No. RP-358, 14.10.2024 [Electronic resource].URL: https://lex.uz/ru/docs/7159258
5. European Commission. *The Act: Full text of the AI Act 2024* [Electronic resource]. URL: https://artificialintelligenceact.eu/the-act/
6. Legislative Chamber of the Parliament (Oliy Majlis) of the Republic of Uzbekistan. *News* Relations arising from the use of AI are regulated, 15.03.2025 [Electronic resource]. URL: https://parliament.gov.uz/news/suniy-intellektni-qollash-orqali-yuzaga-keladigan-munosabatlar-tartibga-solinadi
7. Ministry of Internal Affairs of the Republic of Uzbekistan. *News* [Electronic resource]. URL: https://gov.uz/ru/iiv/news/view/57775
8. IT Park Uzbekistan. *News* MITC, IT Park and UNDP organize hackathon called "Voice AI Challenge Uzbekistan" [Electronic resource]. URL: https://it-park.uz/en/itpark/news/in-uzbekistan-mitc-it-park-and-undp-organize-hackathon-called-voice-ai-challenge-uzbekistan
9. UNESCO. *Recommendation on the ethics of artificial intelligence* [Electronic resource]. URL: https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence
10. United Nations Development Programme. (31.03.2022). *Young people develop AI solutions in Uzbek language* [Electronic resource]. URL: https://www.undp.org/uzbekistan/stories/young-people-develop-ai-solutions-uzbek-language
11. Personal Data Protection Commission (Singapore). (2020, January). *Model AI governance framework* [Electronic resource]. URL: https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework
12. International Bar Association. *Japan: Emerging framework for AI legislation & guidelines* [Electronic resource]. URL: https://www.ibanet.org/japan-emerging-framework-ai-legislation-guidelines
13. LinkedIn. *United Korean AI Act bill: Contents & comparison (EU/English)* [Electronic resource].URL: https://www.linkedin.com/pulse/united-korean-ai-act-bill-contents-comparison-eu-english-min-h98kc/