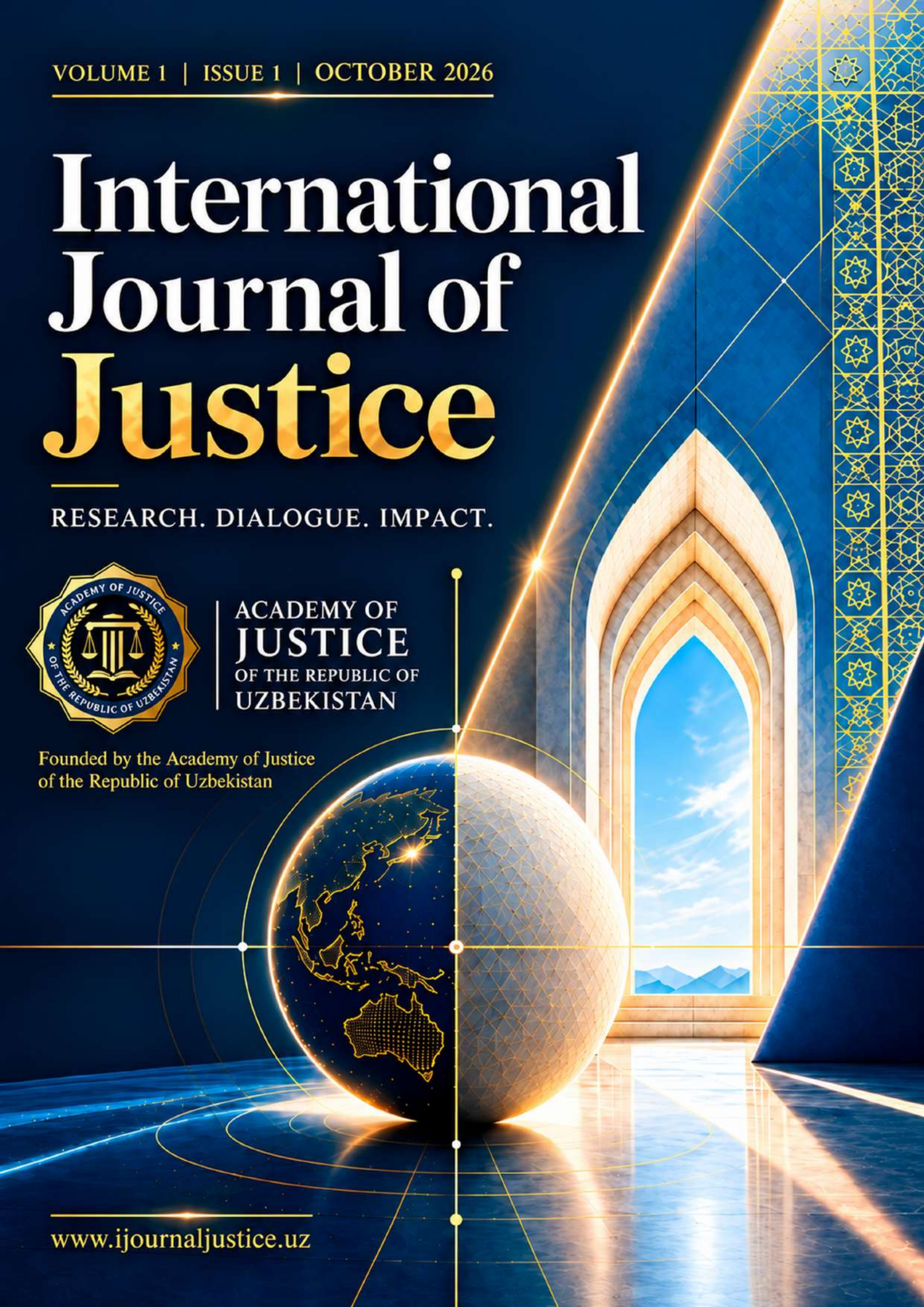
VOLUME 1 | ISSUE 1 | OCTOBER 2026

International Journal of Justice

RESEARCH. DIALOGUE. IMPACT.

ACADEMY OF JUSTICE OF THE REPUBLIC OF UZBEKISTAN

Founded by the Academy of Justice of the Republic of Uzbekistan



www.ijournaljustice.uz

EDITORIAL BOARD

International Journal of Justice



EDITOR-IN-CHIEF

Sherzod Yoqubjonovich Abduqodirov

Rector of the Academy of Justice of the Republic of Uzbekistan

Doctor of Sciences in Law (DSc), Associate Professor



DEPUTY EDITOR-IN-CHIEF

Nodirbek Saparbaevich Salaev

Vice-Rector of the Academy of Justice of the Republic of Uzbekistan

Doctor of Sciences in Law (DSc), Professor

MEMBERS OF THE EDITORIAL BOARD



Anselmo Reyes

Doctor of Philosophy (PhD) in Law, Professor

Judge of the Singapore International Commercial Court



Dilshod Urinbaevich Aripov

Doctor of Sciences in Law (DSc), Professor

Vice-Rector of the Academy of Justice of the Republic of Uzbekistan



Akrom Ikromovich Toshpulatov

Doctor of Sciences in Law (DSc), Professor

Director of the Parliamentary Research Institute under the Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan



Shakhriyor Bakhtiyorovich Bakaev

Doctor of Philosophy (PhD) in Law

Responsible Official of the Administration of the President of the Republic of Uzbekistan



Borzu Sabahi

Doctor of Sciences in Law (DSc), Professor

International Arbitrator



Dilshod Shavkatovich Israilov

Doctor of Philosophy (PhD), Associate Professor

Head Specialist of the Department for Coordination of Research Activities of the Academy of Justice of the Republic of Uzbekistan



Yesemurat Sultamuratovich Kanyazov

Candidate of Legal Sciences in Law (PhD)

Director of the Institute for Retraining and Advanced Training of Legal Personnel under the Ministry of Justice of the Republic of Uzbekistan



Yevgeniy Vyacheslavovich Kolenko

Doctor of Philosophy (PhD), Professor

First Deputy Head of the Law Enforcement Academy of the Republic of Uzbekistan



Krisztina Karsai
Doctor of Sciences in Law (DSc), Professor
Head of the Institute of Criminal Law and Criminal Sciences at the University of Szeged



Lorenzo Mateo Bujosa Vadell
Doctor of Philosophy (PhD) in Law, Professor
Professor at the University of Salamanca



Maged Mamdouh Kamel Shebaita
Doctor of Philosophy (PhD), Professor
International Arbitrator, Doctoral Candidate at the University of London



Ivan Georgievich Nikonov
Doctor of Philosophy (PhD) in Law
Responsible Official of the Administration of the President of the Republic of Uzbekistan



Malikakhon Pirnazarovna Kalandarova
Doctor of Philosophy (PhD), Associate Professor
Deputy Chairperson of the Supreme Court of the Republic of Uzbekistan



Islambek Rustambekovich Rustambekov
Doctor of Sciences in Law (DSc), Professor
Vice-Rector of Tashkent State University of Law



Sakari Kristian Melander
Doctor of Sciences in Law (DSc), Professor
Professor at the University of Helsinki



Khurshid Primkulovich Sadikov
Judge of the Supreme Judicial Council of the Republic of Uzbekistan



Sławomir Marek Redo
Doctor of Sciences in Law (DSc), Professor
Chairperson of the Expert Council for the Development of Scientific Research at the Faculty of Law and Administration



Vigita Vėbraitė
Doctor of Philosophy (PhD) in Law, Professor
Professor at Vilnius University



MANAGING EDITOR
Azamjon Rasuljon ugli Kambaraliev
Head Specialist at the Academy of Justice of the Republic of Uzbekistan

CONTENTS

IMPROVING THE INSTITUTION OF APPEALS: TIME LIMITS, RESPONSE QUALITY, MONITORING **10**
Achilova Liliya Ilkhomovna; Rozmetova Asal Anvarzoda

LEGAL ASPECTS OF INVESTIGATIVE JOURNALISM **18**
Jahonov Shohruh Shuhrat ugli

LEGAL BASIS OF CIVIL SOCIETY INSTITUTIONS IN THE LEGISLATION OF THE REPUBLIC OF UZBEKISTAN **25**
Sharipov Asrorjon Safar ugli

DIGITAL TRANSFORMATION OF INTERNATIONAL COMMERCIAL ARBITRATION IN UZBEKISTAN: LEGAL AND INSTITUTIONAL PROSPECTS **30**
Otakhonov Foziljon Khaydarovich

THE LEGAL NATURE OF SUBSIDIARY LIABILITY IN INSOLVENCY PROCEEDINGS INVOLVING AGRICULTURAL BUSINESS ENTITIES **39**
Rakhmatjon Tojinorovich Berdiyarov

CIVIL LAW ASPECTS OF GOODS DELIVERY BY SELF-EMPLOYED COURIERS **49**
Ruzinazarov Shukhrat Nuralievich

NATIONAL AND INTERNATIONAL EXPERIENCE IN LEGAL PROTECTION OF A COMPANY NAME: IMPROVING THE LEGISLATION OF UZBEKISTAN **63**
Allayarova Maftuna Almardanovna

ORGANIZATIONAL AND LEGAL MECHANISMS FOR COMPENSATION OF CONSTRUCTION CONTRACT DAMAGES **69**
Donayev Abduqodir Haydarovich

JURISDICTION AND VENUE OF CIVIL CASES ARISING FROM INHERITANCE RELATIONS: A NATIONAL AND FOREIGN ANALYSIS **76**
Soliyeva Kamola Rustamjon-qizi

ISSUES OF USING COURT NOTICES IN ENSURING THE OPENNESS OF CIVIL PROCEEDINGS IN COURTS **84**
Sabirov Erkinjon Kuchkarbaevich

DIGITAL EVIDENCE IN SUPPLY-CONTRACT DISPUTES BEFORE ECONOMIC COURTS: AUTHENTICATION, INTEGRITY AND EVIDENTIARY RISK IN UZBEKISTAN **91**
Mahmudova Saida Rayimjonovna

CONTENTS

FROM HUMAN CAPITAL TO INSTITUTIONAL TRANSFORMATION: A NEW STAGE IN THE STRATEGIC DEVELOPMENT OF THE JUDICIAL PERSONNEL TRAINING SYSTEM 104
Aripov Dilshod Urinbaevich

THE ROLE OF INTERNATIONAL STANDARDS IN GOVERNING ARTIFICIAL INTELLIGENCE IN JUDICIAL SYSTEMS: A COMPARATIVE AND CRITICAL ANALYSIS 109
Sadikov Khurshid Primkulovich

INDEPENDENCE — A SOLID FOUNDATION OF JUSTICE AND HUMAN DIGNITY (35 years of the evolution of the judicial and legal system of the Republic of Uzbekistan) 117
Israilov Dilshod Shavkatovich

INSTITUTIONAL MODELS OF JUDICIAL QUALIFICATION BOARDS: INTERNATIONAL STANDARDS AND FOREIGN EXPERIENCE 128
Jamolov Azizjon Nodir ugli

THE DEATH OF FREE WILL. WHO BEARS CULPABILITY WHEN ARTIFICIAL INTELLIGENCE INDUCES A PERSON TO COMMIT A CRIME? 140
Salaev Nodirbek Saparbaevich

ON EUROPEAN CRIMINAL-LAW INTEGRATION – FROM MUTUAL RECOGNITION TO LIMITED SUPRANATIONAL CRIMINAL POWER 148
Krisztina Karsai

CRIMINAL LIABILITY OF OFFICIALS OF NON-GOVERNMENTAL COMMERCIAL ORGANIZATIONS: PROBLEMS OF THEORY AND PRACTICE 158
Akramova Muazzam Turdikul qizi

DISTINGUISHING OFFENCES AGAINST SEXUAL FREEDOM FROM RELATED OFFENCES IN UZBEKISTAN 162
Achilov Izzat Tulkinovich

CRIMINAL-LAW MEASURES AGAINST THE LEGALIZATION OF PROCEEDS OBTAINED THROUGH MISAPPROPRIATION OR EMBEZZLEMENT: QUALIFICATION, EVIDENCE AND ASSET RECOVERY 170
Sadullaev Bokhodir Oybekovich

CONCEPT OF HELPLESSNESS AND ITS SIGNIFICANCE IN THE QUALIFICATION OF CRIMES 178
Khalilova Zarnigor Zafar qizi

LEGAL SIGNIFICANCE OF THE INSTITUTION OF CRIMINAL RECORDS IN PROTECTING HUMAN RIGHTS 182
Yoqubjonov Omonjon Burkhonjon ugli

CONTENTS

THE APPLICATION OF CRIMES WITH BLANKET NORMS: CURRENT STATUS AND ISSUES 189
Pulatov Bekzod Adilbaevich

THE FORMATION AND DEVELOPMENT OF THE INSTITUTION OF CRIMINAL LIABILITY IN THE FIELD OF PUBLIC PROCUREMENT: A HISTORICAL-LEGAL ANALYSIS 202
Shukurova Shahnoza Mukumjonovna

ATTORNEY'S PARTICIPATION IN THE PRE-TRIAL STAGE OF CRIMINAL PROCEEDINGS: LEGAL AND PRACTICAL ASPECTS 214
Medetbaeva Aksungul Sharapatdin kizi

INTERNATIONAL COOPERATION IN OBTAINING ELECTRONIC EVIDENCE: THE EUROPEAN PRODUCTION AND PRESERVATION ORDERS 221
Bujosa Vadell, Lorenzo Mateo

COOPERATION BETWEEN THE SUBJECTS OF INVESTIGATION IN CROSS-BORDER INTERNET FRAUD CASES 230
Khabibiddinov Nodirjon Musinjon ugli

PROBLEMS OF PROCEDURAL REALITY IN CRIMINAL PROCEEDINGS 238
Aykhan Khankishi Rustamzade, Matanat Pasha Asgarova

DETENTION OF FOREIGN NATIONAL PRISONERS IN PENITENTIARY INSTITUTIONS: A COMPARATIVE ANALYSIS OF INTERNATIONAL PRACTICES AND NATIONAL LEGISLATION 246
Rikhsimov Komron Abrorovich

CRIMINALISTIC FOUNDATIONS FOR INTEGRATING GAIT IDENTIFICATION WITH FORENSIC PORTRAIT EXAMINATION 249
Nizomova Shahrigul Karimboy qizi

INTERNATIONAL LAW CRISIS: UN PEACE OPERATIONS AND INSTITUTIONAL REFORM 258
Kudaybergenov Bakhtiyar Abdumajit-ugli

ARTIFICIAL INTELLIGENCE AND CHILDREN'S RIGHTS: PROTECTION OPPORTUNITIES AND EMERGING LEGAL RISKS 267
Ergashev Gayrat Shavkatovich

ACTIVITIES OF INTERNATIONAL NON-GOVERNMENTAL ORGANIZATIONS IN THE FIELD OF HUMAN RIGHTS 276
Nosirova Marjona Negmat kizi

Academy of Justice of the Republic of Uzbekistan
International Journal of Justice

COOPERATION BETWEEN THE SUBJECTS OF INVESTIGATION IN CROSS-BORDER INTERNET FRAUD CASES

Khabibiddinov Nodirjon Musinjon ugli
Lecturer at the Sector of Judicial power, advocacy and law enforcement agencies, Tashkent state university of law
E-mail: nodirjonxabibiddinov@gmail.com
ORCID ID: 0000-0001-2345-6789



Abstract. *Internet fraud is often organised in one country, committed in another and cashed out in a third. For this reason, solving such cases depends on the joint work of the subjects taking part in the investigation. The article examines how the investigator, the bodies of inquiry, the prosecutor, specialists, banks and the competent authorities of foreign states cooperate with each other. The study is based on comparative legal and systemic analysis, on foreign legislation and on materials of investigative practice. The author distinguishes three levels of interaction - internal, interagency and international - and shows the main problems at each of them: the rapid loss of digital traces, the slow exchange of information and the duplication of powers. Proposals are made on joint investigation teams, expedited requests and investigative actions through videoconferencing. The results may be used in improving legislation and in practical work.*

Keywords**:** *internet fraud, cross-border crime, criminal proceedings, investigative subjects, interaction, mutual legal assistance, electronic evidence.*

Introduction

Internet fraud has become the dominant form of acquisitive crime in Uzbekistan. According to the Ministry of Internal Affairs, the number of crimes committed with the use of information technologies grew from 4,865 in 2021 to 62,440 in 2025, and the damage caused to citizens over these five years reached 3.73 trillion soums [1]. In 2024 alone, 58,800 such crimes were registered, and their share in total recorded crime rose from 6.2 to 44.4 per cent [2]. Almost every second registered offence is now committed online.

The main difficulty in investigating these crimes is their cross-border character. A single fraud episode is usually spread across several States. The offender acts from one country, the victim and the debited account are in another, the hosting provider or messenger service operates from a third, and the money is withdrawn or converted into crypto-assets in a fourth. As a result, the investigator must obtain almost all the necessary information from outside the national jurisdiction.

Here the problem of time arises. Subscriber data, IP logs and transaction records are often deleted within a few days. Traditional legal assistance procedures, however, take months. Research shows that more than half of all criminal investigations today require electronic evidence stored abroad, while the average execution time of a mutual legal assistance request is about ten months [3]. In other words, evidence usually disappears before the request reaches the foreign authority.

For this reason, the success of such cases depends less on investigative tactics and more on how well the participants of the investigation work together. This includes the investigator, the bodies of inquiry, prosecutorial supervision, specialists and

experts, banks and payment organisations, and the competent authorities of foreign States.

Uzbek legislation has already recognised the importance of this issue. Fraud committed through information systems is qualified under paragraph "g" of part three of Article 168 of the Criminal Code. Presidential Resolution No. PD-153 of 30 April 2025 "On measures aimed at further strengthening activities to counter crimes committed with the use of information technologies" designated the Ministry of Internal Affairs as the body responsible for coordinating all competent State organs in this field. At the international level, Uzbekistan cooperates on the basis of bilateral treaties, since it is not a party to the Council of Europe Convention on Cybercrime. The United Nations Convention against Cybercrime, adopted by General Assembly resolution 79/243 of 24 December 2024 and opened for signature in Hanoi on 25 October 2025, has not yet entered into force [4]. The coordinating framework has therefore been declared, but the procedural mechanisms serving it are still incomplete.

The question has been studied from two main directions. Criminological research describes the growth and under-reporting of economic cybercrime and its consequences for criminal policy [5]. Legal research analyses cross-border access to electronic evidence and the gradual shift from State-to-State cooperation towards direct cooperation with service providers [6].

Both directions, however, focus on the external channel of cooperation - between States, or between a State and a foreign company. The internal side of the question remains almost unexamined: how the domestic subjects of the investigation should distribute their functions and exchange information among themselves. In addition, the experience of countries that operate outside the Budapest system and rely on bilateral treaties has not been studied as a separate model.

The aim of this article is to develop a model of interaction between the subjects of investigation in cases of cross-border internet fraud and to propose ways of regulating it in criminal procedure. The study seeks to answer three questions: which levels of interaction exist in this category of cases and what obstacles arise at each of them; whether the instruments currently available to Uzbek investigators correspond to the short life-cycle of digital evidence; and which foreign mechanisms - joint investigation teams, expedited preservation requests and investigative actions conducted by videoconference - can be adapted to national legislation.

Materials and methods

Normative sources. The first group comprises the legislation of the Republic of Uzbekistan: the Criminal Code, the Criminal Procedure Code, and Presidential Resolutions No. PD-381 of 30 November 2023 and No. PD-153 of 30 April 2025. The second group comprises international instruments: the Council of Europe Convention on Cybercrime and its Second Additional Protocol of 12 May 2022 (CETS No. 224), the European Union legislation on production and preservation orders for electronic evidence, and the United Nations Convention against Cybercrime adopted by General Assembly resolution 79/243 of 24 December 2024. These instruments were selected because each of them regulates exactly the questions examined in this article: the expedited preservation of data, direct cooperation with service providers, joint investigation teams and permanent contact points.

Empirical materials. The empirical basis consists of the official statistical data of the Ministry of Internal Affairs on crimes committed with the use of information

technologies for the period 2021–2025, published materials of investigative and judicial practice in cases of internet fraud containing a cross-border element, and generalised information on the practice of executing requests for legal assistance in this category of cases.

Methods.

The formal-legal method was used to analyse the content of national procedural norms and to identify gaps in the regulation of interaction between the participants of the investigation.

The comparative-legal method was used to compare the national model with the mechanisms established by the Second Additional Protocol and the European instruments. The comparison was carried out according to three criteria: the time limits for executing a request, the range of subjects entitled to address a foreign service provider directly, and the procedural form of joint investigative activity.

The systemic-structural method served to construct the model of interaction and to distinguish its three levels - internal, interagency and international - as well as to determine the functional connections between them.

The statistical method was used to process the data on the dynamics of registered crimes and the damage caused, and to correlate them with the time actually required to obtain electronic evidence.

Results

The analysis of legislation and practice shows that interaction in cases of cross-border internet fraud is not a single process. It operates at three distinct levels, each with its own subjects, its own time frame and its own type of obstacle.

The internal level covers relations within one law enforcement body: between the investigator, the operational officers, the specialist in digital forensics and the head of the investigative unit. Here the decisive factor is speed at the very first hours after the report of the crime.

The interagency level covers relations between different national institutions: the investigative bodies, prosecutorial supervision, the Cybersecurity Centre, banks, payment organisations and mobile operators. Here the decisive factor is access to information held by third parties.

The international level covers relations with the competent authorities of foreign States and with foreign service providers. Here the decisive factor is the legal form through which a request can be made and executed.

These levels are not independent. A delay at the internal level makes the interagency stage meaningless, because by the time the request is prepared the data no longer exists. In this sense the three levels form a chain in which the weakest link determines the result of the whole investigation.

The first problem is the loss of digital traces caused by delay. Session logs,

IP addresses and device identifiers are stored by providers for a limited period and are overwritten in the ordinary course of business. The national procedure does not provide for a simplified preservation measure that could be applied immediately, before the collection of the data itself is authorised. As a result, the investigator is obliged to follow the full procedure for obtaining evidence at a moment when the only realistic task is to prevent the evidence from disappearing.

The second problem is the uneven distribution of technical competence. The qualification of an act under Article 168 of the Criminal Code requires the establishment of the mechanism of unauthorised access to the account,

which is a technical question. Where a specialist is involved only at the stage of the expert examination, and not at the stage of planning the investigation, the initial investigative actions are performed without an understanding of where the traces are actually located.

The main obstacle is the absence of a single channel for exchanging information on fraudulent accounts, cards and telephone numbers. Each bank responds to requests separately and within its own time frame, although the same fraudulent scheme usually involves accounts in several institutions at once. Consequently, the picture of the movement of funds is assembled from fragments received at different moments, by which time the money has already been withdrawn or converted.

Presidential Resolution No. PD-153 of 30 April 2025 addressed precisely this problem by designating the Ministry of Internal Affairs as the body responsible for coordinating all competent State organs in this field. This established the institutional centre of coordination. However, coordination as an administrative function and interaction as a procedural relationship are not the same thing. The Criminal Procedure Code does not define the procedural form in which the results of such coordinated activity are recorded and introduced into the case file. The coordinating mechanism therefore exists, while the procedural mechanism serving it does not.

At this level the results confirm the conclusions reached in the international literature. The lifetime of electronic evidence is measured in days, whereas the execution of a request for legal assistance is measured in months [3]. The mismatch is structural rather than organisational: the procedure was designed for documents and physical objects, which do not disappear while the request is being transmitted.

Three specific difficulties follow from this.

First, there is no legal basis for addressing a foreign service provider directly. Since the Republic of Uzbekistan is not a party to the Council of Europe Convention on Cybercrime and its Second Additional Protocol, the mechanism of direct cooperation with providers and registrars for obtaining subscriber information is unavailable. Every such request must pass through the full chain of central authorities.

Second, there is no permanent contact point operating on a continuous basis. The Second Additional Protocol and the United Nations Convention against Cybercrime both proceed from the assumption that an emergency request can be sent and received at any hour. Where communication is possible only during working hours and through the central authority, the very idea of an expedited request loses its meaning.

Third, the joint investigation team is not regulated as a procedural institution. Where officials of two States work on connected episodes, each of them acts within its own case, and the results obtained by one party must be transferred to the other through the ordinary channel of legal assistance. The advantage of joint work - the simultaneous performance of actions in several jurisdictions - is thereby lost.

The results can be summarised as follows.

The effectiveness of the investigation of cross-border internet fraud depends on the speed of interaction at all three levels, and the national procedural law currently regulates the first level in detail, the second level partially, and the third level by reference to general provisions on legal assistance.

The principal reason is not a lack of coordination between institutions, but the

absence of procedural instruments adapted to the short life-cycle of digital evidence. Coordination has been established at the level of executive regulation, whereas the corresponding procedural forms have not been introduced into the Criminal Procedure Code.

Accordingly, three instruments are required to close this gap: an expedited measure for the preservation of data pending the decision on its collection, a procedural form for joint investigative activity with foreign authorities, and the regulation of investigative actions conducted by videoconference in cases involving participants located abroad.

Discussion

The findings presented above lead to a conclusion that deserves to be stated directly: in cases of cross-border internet fraud, the decisive procedural resource is not authority but time. This is what distinguishes the present category of cases from other forms of transnational crime. In an investigation of drug trafficking or money laundering, the object of evidence - the substance, the account, the property - continues to exist while the request for legal assistance travels through the central authorities. In internet fraud it does not. Session logs, subscriber records and device identifiers are erased in the ordinary course of the provider's business, without any intention to conceal the crime.

This is precisely why the international literature has for the past decade treated the mutual legal assistance system as structurally unsuited to digital evidence rather than merely slow. Casino and co-authors demonstrate that more than half of all criminal investigations now require access to data held abroad, while the ordinary channel of judicial cooperation operates on a scale of months. Abraha reaches the same conclusion from a different direction, showing that the proliferation of reform initiatives across jurisdictions is itself evidence that the traditional system is no longer considered sustainable by the States that created it.

The author shares this assessment, but with one qualification. The literature tends to present the problem as an external one - as a question of relations between States. The present study suggests that the external channel is only the final segment of a chain, and that the same loss of time occurs earlier, inside the national procedure, where no request has yet been sent to anyone. If the initial hours are spent on the ordinary procedure for collecting evidence rather than on preserving it, the deficiencies of the international mechanism become irrelevant, since there is nothing left to request.

Three responses to this problem have emerged internationally, and it is useful to distinguish what each of them genuinely achieves.

The first is the acceleration of the request itself. The European Union has replaced negotiation between authorities with an order addressed directly to the service provider, with strict deadlines for compliance. Sachoulidou describes this as a paradigm shift, in which cooperation that had previously been informal and voluntary was given binding legal form [7]. The gain in speed is considerable, but the mechanism operates within a single integrated legal space and presupposes that provider maintain legal representatives in the requesting jurisdiction.

The second is direct cooperation with foreign providers under the Second Additional Protocol to the Convention on Cybercrime. Here, however, caution is warranted. Davies and Kennedy-Mayo, having examined the substantive provisions of the Protocol and their anticipated implementation, conclude that it is unlikely to remove the persistent barriers faced by authorities seeking data stored overseas [8].

Their argument is important for the present study because it warns against a common error in comparative research: treating the adoption of an instrument as equivalent to the solution of the problem it addresses.

The third is joint investigative activity. Its advantage is qualitatively different from the first two. An expedited request accelerates the transfer of information; a joint investigation team removes the need for transfer altogether, since officials of both States act within a single case. Comparative analysis indicates that this form offers greater flexibility than a request-based mechanism, though it requires substantially more coordination and a prior agreement between the parties.

Abraha distinguishes four approaches to cross-border data access - reformist, unilateralist, internationalist and nuanced. This typology is useful for determining the position of the Republic of Uzbekistan.

The unilateralist approach, under which a State extends its own enforcement jurisdiction to data stored abroad, is unacceptable: it presupposes economic leverage over global providers that few States possess, and it generates conflicts of law rather than resolving them. The internationalist approach, which relies on a universal treaty, is in principle the most appropriate, but the United Nations Convention against Cybercrime has not yet entered into force, and the number of ratifications required means that its practical effect cannot be expected in the immediate future.

The realistic path is therefore the reformist one: adapting national procedure so that it is capable of operating at the speed the evidence requires, and doing so without waiting for the international framework to mature. This conclusion has a practical consequence. The instruments proposed in this study - an expedited preservation measure, a procedural form for joint investigative activity, and investigative actions conducted by videoconference - do not require prior accession to any particular convention. They can be introduced into national law as autonomous procedural institutions and will then be compatible with whichever international instrument the State subsequently joins.

A separate observation concerns the internal level, which the comparative literature largely leaves aside.

Research on offender organisation shows that cybercriminal groups are not purely virtual formations: they combine offline social ties with digitally acquired technical specialisation, and their members occupy clearly differentiated roles [9]. This finding has a direct methodological consequence. If the criminal group is functionally differentiated, an investigation conducted by a single investigator supported by an occasional expert opinion is structurally weaker than its object. The composition of the investigating side must correspond to the composition of the offending side - which means the early and permanent participation of a specialist in the planning of investigative actions, not merely at the stage of expert examination.

The same logic applies to financial institutions. Banks and payment organisations are not simply holders of information subject to request; they are the only participants able to observe the movement of funds in real time. Their role in the model proposed here is therefore closer to that of a participant in interaction than to that of a source of evidence.

Two objections must be acknowledged.

The first concerns sovereignty. Any mechanism permitting an authority of one State to address a private company situated in another shifts the traditional boundary between territorial jurisdictions. The criticism directed at such

mechanisms in the literature is well founded, and the response cannot be to disregard it, but to accompany every acceleration of procedure with a corresponding guarantee: judicial authorisation for the collection of content data, and strict limitation of the expedited measure to preservation, which does not disclose the content of communications to anyone.

The second concerns the limits of the present study. The comparison undertaken here is doctrinal, and it establishes what foreign norms provide rather than how effectively they operate. Levi has repeatedly observed that in the field of economic cybercrime the available data are shaped by reporting practices as much as by criminal activity itself. The same caution applies to the conclusions of this article: they identify gaps in legal regulation, and empirical verification of the proposed model would require data on the execution of requests that is not currently published.

Conclusion

The investigation of cross-border internet fraud has become a problem of organisation rather than of tactics. The study has shown that interaction in this category of cases operates at three levels - internal, interagency and international - and that these levels form a chain in which the weakest link determines the outcome. Time is the decisive resource at every one of them, because digital traces disappear in the ordinary course of a provider's business, without any action on the part of the offender.

The principal conclusion is that the gap in the national system lies not in coordination but in procedure. Presidential Resolution No. PD-153 of 30 April 2025 established the institutional centre of coordination by designating the Ministry of Internal Affairs as the authorised body in this field. What has not yet been introduced is the set of procedural forms through which such coordinated activity can be conducted and recorded. Coordination exists at the level of executive regulation; the corresponding instruments are absent from the Criminal Procedure Code.

Three amendments are therefore proposed.

First, to introduce an expedited measure for the preservation of computer data, applied by decision of the investigator with subsequent notification of the prosecutor, limited in duration and not entailing disclosure of the content of communications. Its purpose is to stop the destruction of data while the question of its collection is being decided.

Second, to regulate the joint investigation team as a procedural institution, defining the grounds for its creation, the composition of its participants and the procedural status of the results obtained by the foreign party.

Third, to establish the procedure for conducting investigative actions by videoconference where a participant is located outside the territory of the Republic, together with the requirements for recording such actions and verifying the identity of the participants.

These instruments do not depend on accession to any particular international treaty and can be introduced as autonomous provisions of national law. They will remain compatible with the United Nations Convention against Cybercrime once it enters into force.

The results may be used in the preparation of amendments to the Criminal Procedure Code, in the practical work of investigative bodies, and in the training of specialists in this field.

References

1. *This Year, Cybercriminals Stole UZS 1.9 Trillion from Citizens of Uzbekistan. Spot.uz, 23.12.2025. Available at: https://www.spot.uz/oz/2025/12/23/cyber-crime (accessed: 01.08.2026).*

2. *Cybercrime Accounts for Almost Half of All Crimes in Uzbekistan. Gazeta.uz, 05.11.2025. Available at: https://www.gazeta.uz/oz/2025/11/05/cybercrime/ (accessed: 01.08.2026).*

3. *Casino F., Pina C., López-Aguilar P., Batista E., Solanas A., Patsakis C. SoK: cross-border criminal investigations and digital evidence. Journal of Cybersecurity, 2022, vol. 8, no. 1, tyac014. doi: 10.1093/cybsec/tyac014.*

4. *The United Nations Convention against Cybercrime opens for signature in Hanoi. United Nations Office of Legal Affairs, 2025. Available at: https://www.un.org/ola/en/news/united-nations-convention-against-cybercrime-opens-signature-hanoi (accessed: 01.08.2026).*

5. *Levi M. Assessing the trends, scale and nature of economic cybercrimes: overview and issues. Crime, Law and Social Change, 2017, vol. 67, no. 1, pp. 3–20. doi: 10.1007/s10611-016-9645-3.*

6. *Abraha H.H. Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives. International Journal of Law and Information Technology, 2021, vol. 29, no. 2, pp. 118–153. doi: 10.1093/ijlit/eaab001.*

7. *Sachoulidou A. Cross-border access to electronic evidence in criminal matters: the new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation. New Journal of European Criminal Law, 2024, vol. 15, no. 3, pp. 256–274. doi: 10.1177/20322844241258649.*

8. *Davies G., Kennedy-Mayo D. The promise and pitfalls of the Second Protocol to the Budapest Convention: assessing its impact on EU and UK cross-border criminal investigations. New Journal of European Criminal Law, 2026. doi: 10.1177/20322844261419413.*

9. *Leukfeldt E.R., Kleemans E.R., Stol W.P. A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. Crime, Law and Social Change, 2017, vol. 67, no. 1, pp. 21–37.*

