The Academy held another dissertation defence

At the meeting of the Scientific Council DSc.24/2026.31.01.Yu.01.02, authorised to award academic degrees under the Law Enforcement Academy of the Republic of Uzbekistan, held on 12 November 2026, **Gayrat Farkhadovich Musaev** defended his dissertation entitled **"Improving the Methodology for Investigating Crimes Committed through the Use of the Hidden Segment of the Internet (Darknet)"** for the degree of Doctor of Philosophy (PhD) in Law in the speciality 12.00.09 – "Criminal Procedure. Criminalistics, Operational-Search Law and Forensic Examination".

The aim of the research is to develop scientifically substantiated proposals and recommendations aimed at improving the methodology for investigating crimes committed through the use of the hidden segment of the Internet (Darknet).

The object of the research is the body of social and legal relations arising in the process of improving the methodology for investigating crimes committed through the use of the hidden segment of the Internet (Darknet).

The subject of the research comprises the regulatory legal acts governing relations concerning the methodology for investigating crimes on the Darknet and the tactics of conducting investigative actions; current trends in combating this category of crimes; practices involving the use of specialised technical tools; as well as conceptual approaches and scientific and theoretical views developed in digital forensics and legal science.

The scientific novelty of the research consists of the following:

The study substantiates that the establishment of a Digital Forensics Research Institute will contribute to improving the scientific and methodological foundations for detecting crimes committed in the hidden segment of the Internet, collecting digital evidence and formalising it in accordance with procedural requirements;

It substantiates that the establishment of an interagency automated system, the "Unified Register of Digital Evidence", covering information not related to state secrets, photographs, video and audio recordings, electronic wallets, crypto-asset addresses, IP addresses, Internet addresses (domains), social media accounts, information on the place and time of their identification, as well as other significant characteristics of digital evidence, will facilitate the collection, registration, storage and examination of materials relating to this

category of criminal cases received from law enforcement agencies, contribute to solving crimes, improve the effectiveness of investigations and enable the prompt identification of organised criminal groups;

It is scientifically substantiated that electronic data identified and recorded during seizure and inspection investigative actions without the participation of a person possessing specialised knowledge (a specialist) should be deemed inadmissible evidence, and that this requirement should be enshrined in criminal procedure legislation;

It is substantiated that electronic data containing information relevant to the case, including electronic files, audio and video recordings, messages stored on the global Internet, as well as other electronic digital information, constitute independent digital evidence, and that this provision should be enshrined in the criminal procedure legislation of the Republic of Uzbekistan.

The practical results of the research are as follows:

A draft regulation on the procedure for conducting forensic examinations of digital evidence at the Digital Forensics Research Institute has been developed. It comprehensively covers the procedures for appointing and conducting examinations, submitting examination materials, extending examination periods, formalising expert opinions and returning the examined materials;

A draft joint interagency resolution aimed at approving the Regulation on the “Unified Register of Electronic (Digital) Evidence” has been developed;

A specialised training course (module) has been developed for the master's degree programme in “Legal Support for Cybersecurity” and introduced into the educational process, with the aim of training personnel to combat cybercrime, including crimes committed through the use of the Darknet;

A methodology has been developed for the forensic examination and analysis of large volumes of data (Big Data) obtained from the Darknet;

A teaching and methodological guide entitled “Specific Features of Investigating Crimes in the Field of Crypto-Asset Circulation” has been prepared and introduced into the education system and research activities.