ABSTRACT

The dissertation presented by Ruslan Bulatovich Dzhilkishiev, a doctoral student at the Sh. Kabyldayev Kostanay Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan, under the educational programme 8D12301 – 'Law Enforcement Activities', focuses on the following topic: The present study will examine crimes committed in the field of information technology.

General characteristics of the research. The dissertation research is devoted to a comprehensive criminalistic analysis of the investigation of crimes in the field of information technology, with an emphasis on improving methodological and organisational approaches to the detection and investigation of cybercrimes. The aim of the work is to develop and modernise practical recommendations aimed at improving the effectiveness of investigating illegal activities in this area. The object of the study is crimes committed using information and communication technologies, and the subject is the patterns of their commission, as well as the methods and means of their detection and investigation. The methodological basis consists of systemic, comparative legal, didactic and statistical methods, which ensured a comprehensive approach to the issue under study. The theoretical basis consists of scientific works by Kazakhstani and foreign authors, as well as the current legislation of the Republic of Kazakhstan and international legal acts. The scientific novelty of the research lies in the development of the author's criminalistic characteristics of cybercrimes, algorithms for investigative actions, and proposals for institutional solutions, including the creation of a National Centre for Cyber Security and Digital Forensics.

Relevance of the research topic. Claude Shannon and Robert Wiener are considered to be the founders of information technology (mid-20th century), whose work laid the foundations for understanding the processes of information transmission and processing and had a significant impact on the development of automated systems. Achievements in the field of computers, modern telecommunications and means of communication have become a kind of ‘trigger’ for the development of a completely new sector of the economy, which is currently demonstrating the fastest growth rates.

The process of improving and developing technologies is characterised by significant changes in existing communication systems. The two dominant forms of communication until the middle of the 20th century — mail and print media (newspapers, magazines, books) — were integrated and combined into a single information and communication space — cyberspace.

The advent of personal computers and the Internet in the 1970s, and later the creation of the global Internet, led to radical changes in various spheres of human life, including the economy, education, healthcare, and social interactions. This, in turn, led to the development of new forms of crime related to the use of information technology. This dissertation aims to explore the issue of illegal

activities committed through the global Internet or international communication systems.

The Internet offers a number of undeniable advantages for illegal activities. First, there is an unlimited amount of various information (text, graphics, audio, video) transmitted over the network. Secondly, it offers the possibility of using psychological techniques to manipulate users on a global scale.

According to statistical data, 407 offences were registered in Kazakhstan between 2019 and 2023: 2019 – 108, 2020 – 62, 2021 – 74, 2022 – 85, 2023 – 78, 2024 – 101 – in the field of information technology and cybercrime.

Cybercrimes have a high level of latency and cause significant damage to individual users, commercial companies and government agencies. Given the above, it is clear that traditional methods of investigating illegal activities are insufficient and ineffective. This makes the task of improving methods of combating cybercrime one of the priorities in the field of law enforcement and security, which, in turn, creates a need to develop special techniques that take into account the specifics of computer crimes.

The relevance of cybercrime on the one hand, and its insufficient development on the other (which will be discussed in detail in this dissertation), creates an urgent need for the further development of criminology as a scientific discipline, the use of knowledge from various fields of science (information technology, psychology, legal sciences, etc.), as well as the improvement of existing investigation methods and the development of new approaches.

Despite the existence of significant research in certain areas of cybercrime investigation, there is currently a lack of integrity and consistency in the work covering all aspects of criminalistic investigation methods, and there is insufficient integration of methods and knowledge, which reduces (hinders) the effective investigation of this category of cases.

Thus, given the current state of knowledge and recommendations in the field of cybercrime investigation, there is a need for in-depth, systematic research that can have a real impact on practical activities and improve the effectiveness of investigations in this area, since individual recommendations may be useful in specific cases but are not systematic in nature. Practitioners need clear, systematic and integrated working methods, and obtaining unsystematic, partial information cannot solve the main problems faced by investigators. The desire to develop a more systematic methodology and to propose new approaches based on both theory and practice prompted us to choose this topic for our dissertation.

The degree of scientific development of the research topic. In recent years, the investigation of crimes committed using information and communication technologies has consistently been included in the list of priority areas of scientific research in criminal law and criminology. Issues of classification, prevention and detection of cybercrimes are covered in the works of such authoritative researchers as Zh.K. Amanov, E.O. Alaukhanov, A.N. Agibaev, K.A. Begaliyev, B.A. Beknazarov, V.B. Vekhov, R.E. Dzhansaraeva, A.A. Isaev, V.V. Krylov, E.I. Kairzhanov, I.Yu. Loskutov, V.A. Meshcheryakov, V.Yu. Rogozin, I.I. Rogov,

S.M. Rakhmetov, L.N. Solovyov, T.B. Seitov, B.Kh. Toleubekova and others, whose works reveal the theoretical and legal foundations of combating crime in the digital environment, as well as identify specific areas for improving investigative practice.

In foreign criminology, research on countering cyber threats is mainly focused on technical aspects and international cooperation. However, both domestic and international scientific sources still need to systematise knowledge about the specifics of investigating crimes in the field of information technology, as well as to develop a comprehensive criminological methodology that takes into account the national characteristics of law enforcement practice.

Thus, this dissertation research logically builds on the existing scientific base and at the same time aims to develop and expand it in the context of modern digital challenges. The work represents a step towards the formation of an integrative approach that combines the legal, forensic and technological components of the investigation process, which confirms its scientific validity and relevance.

The aim of this dissertation is to develop and modernise practical recommendations that will increase the effectiveness of the investigation of illegal activities in the field of information technology. We have set the following **tasks:**

- to analyse the current situation in the field of combating cybercrime;
- to develop classification criteria for crimes in the field of information technology;
- to reveal the content of the elemental composition of the criminalistic characteristics of cybercrimes;
- to identify the mechanisms for initiating pre-trial proceedings in the investigation of crimes in the field of information technology;
- to formulate algorithms for the initial stage of investigating crimes in the field of information technology;
- develop algorithms for the subsequent stage of investigating crimes in the field of information technology.

The object of this dissertation research is unlawful acts committed in the field of information technology, as well as the study of the practical aspects of their disclosure and investigation.

The subject of the dissertation research is to identify the patterns and unique features characteristic of illegal acts in the field under consideration, the methods and approaches used for investigation, and to determine the investigative actions that the investigator should take during the initial and subsequent investigative actions.

The methodological basis of the dissertation research includes various methods and approaches. The methodological basis involves the use of didactic principles and a systematic approach, allowing the subject of research to be considered in the context of a broader system. The application of comparative legal and statistical methods contributes to a more in-depth analysis and also allows for a

comparison of various aspects of the investigation of unlawful acts in the field under consideration.

The normative basis of the dissertation research includes the Constitution of the Republic of Kazakhstan, as well as international legal acts related to the topic of the dissertation. The current criminal and criminal procedure legislation relevant to the subject of the research was analysed, as well as the available literature on the subject, which made it possible to construct the work as a logical continuation and development of previous research in the field of information technology, taking into account new realities and comparing the results obtained with them.

The empirical basis of the dissertation research was provided by the author's analysis of statistical reports for 2019-2024 provided by the Committee for Legal Statistics and Special Records of the Republic of Kazakhstan on offences in the field of information technology, the laws 'On National Security', 'On Informatisation', 'On State Secrets', 'On Personal Data and Their Protection', 'On Electronic Documents and Electronic Digital Signatures', 'On Communications', the Criminal Code of the Republic of Kazakhstan, the Code of the Republic of Kazakhstan 'On Administrative Offences', the Unified Requirements in the Field of Information and Communication Technologies and Information Security (Decree of the Government of the Republic of Kazakhstan No. 832 of 20 December 2016), the Concept of Cybersecurity ('Cyber Shield of Kazakhstan').

In the dissertation, the author drew on his personal experience working in various positions in law enforcement agencies.

Scientific novelty of the research. The systematic approach used for the first time made it possible not only to study individual issues of investigating crimes in the field of information technology, but also to conduct a comprehensive analysis of them in the context of a broader system in the interconnection and interaction of the problem under study with other elements.

This dissertation addressed a number of key issues of an organisational, tactical and methodological nature, as well as legal and ethical aspects and the work of law enforcement agencies.

New ideas were proposed that contribute to a better understanding and systematisation of knowledge about illegal activities in the field under consideration, which are of theoretical interest.

The conclusions and recommendations developed in the course of the research can be applied in the practical activities of law enforcement agencies and other organisations directly involved in the investigation of offences in the field of information technology.

Separate issues concerning preventive measures against crimes in the field of information technology are considered.

The novelty of the work is also due to significant changes in the regulatory legal framework that have taken place in recent years, as well as extensive judicial practice in the application of new legislation on offences in the field of information technology.

The following provisions have been proposed for the defence:

1. The study carried out by the author categorises the set of measures and efforts taken by law enforcement agencies and services involved in the detection and investigation of cybercrime, which includes legal regulation; specialisation of law enforcement agencies; technical tools and investigation methods; international cooperation, which, if implemented mutually, can have an effective impact on the current situation in the field of committing the type of crimes under consideration.

2. A classification of criminal offences has been proposed, the elements of which fall under the collective definition of 'Offences in the field of information technology', including: unlawful access to information, information systems or telecommunications networks (Article 205 of the Criminal Code); unlawful destruction or modification of information (Article 206 of the Criminal Code); disruption of the operation of information systems or telecommunications networks (Article 207 of the Criminal Code); unlawful acquisition of information (Article 208 of the Criminal Code); coercion to transfer information (Article 209 of the Criminal Code); creation, use or distribution of malicious computer programs and software products (Article 210 of the Criminal Code); unlawful distribution of restricted-access electronic information resources (Article 211 of the Criminal Code); provision of services for hosting Internet resources for unlawful purposes (Article 212 of the Criminal Code); unlawful alteration of the identification code of a cellular subscriber device, subscriber identification device, as well as the creation, use, or distribution of programmes for altering the identification code of a subscriber device (Article 213 of the Criminal Code).

3. An author's version of the criminalistic characteristics of crimes in the field of information technology has been created, which includes the following elements: the subject of the criminal offence; the time, place, instrument and circumstances of the offence; methods of preparation, commission and concealment of offences in the field of information technology; the evidence pattern; typological characteristics of the offender in the field of information technology; reasons and conditions contributing to the commission of offences in the field of information technology.

4. The author's well-reasoned applied tools, as applied to the beginning of pre-trial proceedings: what specific data or systems were affected by malicious actors, what is the nature of the crime, what is the structure of the object where the unlawful act may have been committed. The investigator needs to analyse the conditions in which the object operates: the method of data processing and storage; document flow (goods flow) system; equipment and software parameters that allow determining the method of interaction between computers and users; the level of security measures to protect confidential information; job descriptions of employees whose duties include the processing and storage of computers and information that has become the object of criminal encroachment.

5. The author has developed a classification of similar and dissimilar investigative situations at the initial stage of investigating offences in the field of information technology, which determine the main directions for the detection and

investigation of the offences in question, the selection of the optimal algorithm of actions for the organisation and implementation of the necessary complex of urgent investigative actions, including: a) only partial information about the fact of the offence itself, the identity of the victim, and no information about the person who committed the offence, whose motives are unclear; b) complete information about the identity of the victim, the motives for committing the offence and the persons who committed it, but the suspect claims to be uninvolved and refuses to give a confession; c) there is a complete picture of the investigation, but the suspect refuses to cooperate with the investigation, claiming that they are not involved in the unlawful act and refusing to admit their guilt; d) the suspect cooperates with the investigation, fully admitting their guilt in committing the unlawful act and giving a confession.

6. The algorithm for conducting investigative verification activities at the subsequent stage of investigating crimes in the field of information technology is justified in order to overcome contradictions, eliminate inconsistencies and discrepancies according to the following formula: investigative experiment – subsequent interrogations – additional examinations.

7. Taking into account the current challenges in the field of digital security, it is proposed to initiate the creation of a National Centre for Cyber Security and Digital Forensics (hereinafter referred to as the NCSDF) in Kazakhstan as an interdepartmental coordinating body. The centre will bring together the efforts of law enforcement and special state bodies (the Ministry of Internal Affairs, the National Security Committee, the Financial Monitoring Agency and other interested state bodies), the private sector and international partners, ensuring the exchange of information on cyber incidents through a unified digital platform based on blockchain technology. Key functions include the creation of a cybercrime database, rapid data exchange, the development of digital forensics using AI and big data, the establishment of a cyber investigation institute, and the establishment of mechanisms for international cooperation. Legislative support is proposed to be implemented through the adoption of a special law ‘On Combating Cybercrime.’

8. In order to improve the effectiveness of investigations into crimes in the field of information technology, it is proposed to introduce a specialised software and analytical complex (hereinafter referred to as SPAC) that provides automated collection, analysis and storage of digital evidence using artificial intelligence. SPAC will allow for the systematisation of data, accelerate the formation of expert opinions and improve interdepartmental interaction. Its implementation on the basis of the Centre for Forensic Expertise and, in the future, within the framework of the National Centre for Cybersecurity, will ensure a reduction in investigation times, improve the qualifications of specialists and enhance the quality of digital forensics in Kazakhstan. There is also an alternative: the future SPAC could be used in the new National Centre for Cybersecurity and Digital Forensics, which we proposed earlier.

9. Given the rapid growth of contactless drug sales via the internet, messengers and the darknet, it is proposed to develop a strategy in Kazakhstan to combat digital forms of drug crime, with a focus on drug dealers. Key measures include: improving legislation with the introduction of special qualifying criteria, creating digital platforms for monitoring and data exchange, and introducing intelligent systems for analysing digital traces and metadata. It is envisaged that the public will be actively involved, mobile applications for reporting drug stashes will be developed, operational activities on the darknet will be expanded, and AI will be used to identify criminal schemes. A comprehensive approach will reduce drug threats and increase the effectiveness of law enforcement activities.

The main results of the dissertation are reflected in 8 scientific publications.

Published in an international peer-reviewed journal (with a non-zero impact factor or included in the Scopus database, JSTORE): Problems of Investigation of Crimes in the Field of Information Technology. Pakistan Journal of Criminology Vol. 16, No. 03, July—September 2024 (97-114).

The present publication has been included in the List of Scientific Publications recommended for publication of the main results of scientific activity. This list has been approved by the Committee for Control in the Field of Education and Science of the Ministry of Education and Science of the Republic of Kazakhstan.

1. The current state and prospects of combating cybercrime. Khabarsky-Vestnik, No. 4(86) 2021.

2. The content and essence of the elements of the criminalistic characteristics of offences in the field of information technology and cybercrime. Scientific works of the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov, No. 4(81) 2024.

3. Circumstances subject to proof and tasks of investigation in criminal cases involving information technology and cybercrime. Scientific Works of the M. Esbulatov Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan, No. 4(81) 2024.

The material has been published in the proceedings of international conferences.

1. Problems of investigating crimes in the field of information technology. 'Aubakirov Readings' Materials of the international scientific and practical conference 19.02.2018.

2. Cybercrime in the field of social networks. Legal scientific and practical journal 'Zan zhan' No. 12 (216), December 2018, pp. 28-31.

3. On the Forensic Characterisation of the Identity of the Subjects of Crimes in the Field of High Technologies - 'Journal of Advanced Research in Law and Economics', Fall 2018 Volume IX issue 6 (36), pp. 2011-2015.

4. Classification of offences in the field of cybercrime. ‘Aubakirov Readings’. Materials of the international scientific and practical conference, pp. 68-72. 19 February 2025.