РОЗДІЛ 9
КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

UDC 343.1
DOI https://doi.org/10.32782/2524-0374/2024-4/137

LEGAL FRAMEWORK FOR DIGITALIZATION OF LAW ENFORCEMENT AGENCIES IN UKRAINE IN THE FIELD OF CRIMINAL JUSTICE

ПРАВОВІ ОСНОВИ ДІДЖИТАЛІЗАЦІЇ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ У СФЕРІ КРИМІНАЛЬНОЇ ЮСТИЦІЇ

Babaieva O., PhD in Law, Associate Professor,
Associate Professor at the Department of Criminal Procedure
Yaroslav Mudryi National Law University

Romantsova Ya., PhD in Philology, Associate Professor,
Associate Professor at the Department of Foreign Languages
Yaroslav Mudryi National Law University

Zelinska O., PhD in Philology, Associate Professor,
Associate Professor at the Department of Foreign Languages
Yaroslav Mudryi National Law University

The article deals with the peculiarities of regulatory framework for the digital infrastructure of law enforcement agencies of Ukraine in the field of criminal justice. The purpose of the article is to analyze the legal framework for regulating the digitalization of law enforcement agencies with the view of understanding them as a whole system. The article systematizes information and telecommunication registers in the activities of law enforcement agencies. Based on this, the authors propose a classification of the latter. In addition, the scientific works of scholars and practitioners on the problematic and positive issues of implementation and operation of relevant resources have been analyzed. The digitalization process requires a sufficient level of English due to its prevalence in professional communication and cooperation.

Thus, it is concluded that the existing registers of the activities of law enforcement agencies in the field of criminal justice can be conditionally divided into four groups. The first group of information resources includes international databases, Interpol and Europol, in particular, to which law enforcement agencies of Ukraine also have access.

The second group includes national departmental electronic information resources that are large information systems and / or contain several modules and / or separate registers, and the function of electronic communication: The Unified Information System of the Ministry of Internal Affairs of Ukraine, the Unified Judicial Information and Telecommunication System, the iCase Information and Telecommunication System, the Information Portal of the National Police of Ukraine, the Unified Register of Convicts and Detainees, etc.

According to the authors' opinion, the third group consists of registers of law enforcement agencies' document flow, such as the Unified Register of Pre-trial Investigations, the iCase Information and Telecommunication System of Pre-trial Investigation, etc.

Finally, the fourth group of resources includes "simple" registers – databases containing information on persons, property and / or procedural and administrative actions in the field of criminal justice and related activities of state bodies: The Register of Offenders (the Unified State Register of Domestic and Gender-Based Violence), the Register of Corrupt Officials (information on persons who have committed corruption offenses), the Unified Register of Seized Property (a register of assets seized in criminal proceedings).

Key words: law enforcement, law enforcement agencies, digitalization of law enforcement, criminal justice, criminal procedure, information and telecommunication systems.

У статті розглянуто питання особливості нормативного регулювання цифрової інфраструктури правоохоронних органів України у сфері кримінальної юстиції. Метою статті є аналіз правових основ регулювання діджиталізації (цифровізації) діяльності правоохоронних органів, з метою цілісного уявлення їх системи. В роботі здійснено систематизацію інформаційно-телекомунікаційних реєстрів у діяльності правоохоронних органів. На підставі чого, авторами запропоновано класифікацію останніх. Окрім того, проаналізовано наукові доробки науковців та практиків щодо проблемних й позитивних питань впровадження та роботи відповідних ресурсів. Отже, зроблено висновки, що існуючі реєстри у діяльності правоохоронних органів у сфері кримінальної юстиції можна умовно поділити на чотири групи. Так, до першої групи інформаційних ресурсів можна віднести міжнародні бази даних, зокрема, Інтерполу та Європолу, до яких мають доступ й правоохоронні органи України. До другої групи пропонується віднести національні відомчі електронні інформаційні ресурси, які є великими інформаційними системами та/або містять у собі декілька модулів та/або окремих реєстрів, та функцію електронної комунікації, зокрема: Єдина інформаційна система Міністерства внутрішніх справ України, Єдина судова інформаційно-телекомунікаційна система, Інформаційно-телекомунікаційна система «іКейс», «Інформаційний портал Національної поліції України», Єдиний реєстр засуджених та осіб взятих під варту тощо. Третю групу, на думку авторів, складають реєстри документообігу правоохоронних органів, такі як Єдиний реєстр досудових розслідувань, Інформаційно-телекомунікаційна система досудового розслідування «іКейс» та ін. Нарешті, до четвертої групи ресурсів, пропонується віднести «прості» реєстри – бази даних, які містять відомості щодо осіб, майна та/або процесуальних, адміністративних дій у сфері кримінальної юстиції та пов'язаних з нею видів діяльності державних органів, зокрема: Реєстр кривдників (Єдиний державний реєстр випадків домашнього насильства та насильства за ознакою статі), Реєстр корупціонерів (відомості про осіб, які вчинили корупційні правопорушення), Єдиний реєстр арештованого майна (реєстр активів, на які накладено арешт у кримінальному провадженні).

Ключові слова: правоохоронна діяльність, правоохоронні органи, діджиталізація діяльності правоохоронних органів, кримінальна юстиція, кримінальний процес, інформаційно-телекомунікаційні системи.

Introduction. Digitalization of human activity at the present stage is one of the priorities of our state. Despite the difficult times in the context of armed aggression against Ukraine, the digital transformation of public authorities, including law enforcement agencies, is gradually and steadily taking place. For example, a digital infrastructure is being created in the criminal justice system to improve efficiency. The process of digital transformation requires specialists with the sufficient level of English to enhance it.

Analysis of recent research and publications. The issues of digitalization and the use of artificial intelligence technologies in law enforcement in general, and in the field of criminal justice in particular, are the subject of scientific discussions by a wide range of scholars, such as V. Bilous, O. Verkhoglyad-Gerasimenko, M. Demura, N. Hlynska, O. Kaplina, D. Klepka, I. Krytska, T. Pavlova, O. Radutnyi, A. Stolitnyi, A. Tumanyants, L. Chygryna, V. Shevchuk. Taking into account that at the current historical stage of law enforcement activities, the digital transformation in this area is only "emerging", there are a lot of issues that require the attention of scholars and practitioners.

Statement of the problem. According to M. Demura, digitalization of criminal proceedings is no longer a novelty, it has become an integral part, the sign of its development [1, p. 2]. The law enforcement agencies have to develop in all areas of their activities taking into account the transformation in the context of digitalization. As N. Hlynska and D. Klepka rightly note, the digitalization of criminal procedure is not limited to the exclusive use of technology; it is characterized by a change in the culture and way of thinking of law enforcement officers, their acquisition of digital competence; the formation of new ways and principles of digital interaction of participants in legal relations [2, p. 25-26].

Ukraine is just beginning its journey in the use of artificial intelligence and digitalization of criminal justice, unlike some developed countries. Analyzing the relevant experience, our state, at the same time, has the opportunity to successfully use it. For example, Ukraine introduces and uses artificial intelligence technologies in the activities of law enforcement agencies, in particular in the field of criminal justice (during the investigation of war crimes, the use of the "Cassandra" system in the activities of the probation authority [3, p. 152].

In addition, our country is among the 196 countries that have 24 / 7 access to the databases of the International Criminal Police Organization (hereinafter referred to as Interpol) and the European Union Agency for Law Enforcement Cooperation (hereinafter referred to as Europol).

As of today, about one hundred information and telecommunication resources (registers) have been created in Ukraine. Therefore, in order to have a holistic view of the digital infrastructure of law enforcement agencies and the legal framework for its regulation, it is necessary to study the relevant electronic information resources which needs the English language skills development for specialists who are responsible for working with mentioned resources. In this regard, let us pay attention to those that are related to law enforcement and / or owned / managed by law enforcement agencies, and try to systematize them, taking into account their diversity.

Results of the study. Thus, the *first group of* information resources includes international databases, in particular, Interpol and Europol. Interpol manages 19 police databases (Criminal databases) with information on crimes and criminals available to countries in real time. The average response time in the Interpol database from anywhere in the world is half a second. The relevant databases contain information on: individuals, child abuse, DNA profiles, facial recognition, stolen property, works of art, etc. Each search in 19 databases is a potential breakthrough for police around the world. For example, the *INTERPOL* Facial Recognition System*(IFRS*) contains facial images from more than 179 countries, making it a unique global criminal database. Combined with an automated biometric software application, the system is able to identify or verify a person by comparing and analyzing the patterns, shapes and proportions of their facial features and contours. Since the launch of Interpol's facial recognition system in late 2016, nearly 1,500 terrorists, criminals, fugitives, persons of interest, or missing persons have been identified [4].

Europol, among other things, also has several platforms, including the Europol Platform for Experts (EPE). This platform is a secure network for collaboration. Specifically, it is a platform for professionals working in various areas of law enforcement. Its purpose is to facilitate and support the exchange of non-personal data on crimes.

It provides content management and communication, messaging and file sharing. Europol has 60 platforms and 19 thousand experts. The EUROPOL Information System (EIS) is its core system, a reference system that exists to support Europol member states and its partners in the fight against organized crime, terrorism and other serious crimes. It contains information on offenses, persons involved, data related to suspects and / or convicts, etc. [5, p. 10].

The *second group* consists of a list of national departmental, so-called "complex" electronic information resources, which are large information systems and / or containing several modules and / or separate registers, and an electronic communication function. The second group of registries includes, in particular, the following: the Unified Information System of the Ministry of Internal Affairs of Ukraine, the Unified Judicial Information and Telecommunication System, the iCase Information and Telecommunication System, the Information Portal of the National Police of Ukraine, the Unified Register of Convicts and Detainees. Let us consider some of them.

The Unified Information System of the Ministry of Internal Affairs (hereinafter referred to as the UIS of the MIA) is an integrated information system that directly ensures the implementation of the functions of its subjects, information support and of their activities and constitutes a set of interconnected functional subsystems, services, software and information complexes, and technical means of electronic communication that ensure the logical combination and integration of electronic information resources of the Unified Information System of the MIA, processing and protection of information, interaction of internal and external information through the use of a functional subsystem of the Unified Information System of the Ministry of Internal Affairs with special functions [6].

The owner and manager of the Unified Information System of the MIA is the state represented by the MIA. The owner of information processed in the central subsystem of the Unified Information System of the MIA is the MIA. The owners of information processed in functional subsystems of the Unified Information System of the MIA are relevant subjects of the Unified Information System of the MIA that ensure protection of information from accidental loss or destruction, unlawful processing and access to information.

The purpose of information processing in the functional subsystems of the MIA Unified Information System is established by the regulatory acts governing the activities of the relevant entities of the MIA Unified Information System separately for each electronic information resource of the MIA Unified Information System (Clause 3 of the Regulation on the MIA UIS).

According to Clause 6 of the Regulation on the UIS MIA, the system is designed to automate and technologically support the data exchange between the entities of the Unified Information System of the MIA in the interests of national security, protection of the rights and legitimate interests of citizens, society and the state in the following areas: ensuring the protection of human rights and freedoms, combating crime, and maintaining public security and order; protection of the state border and safeguarding the sovereign

rights of Ukraine in its exclusive (maritime) economic zone; civil defense, protection of the population and territories from emergencies and prevention of their occurrence, liquidation of the consequences of emergencies, rescue, firefighting, fire and industrial safety, activities of emergency services, as well as hydrometeorological activities; migration (immigration and emigration), including combating illegal migration, citizenship, registration of individuals, refugees and other categories of migrants defined by law.

The objectives of the UIS MIA are:

1) creating a unified information space of the MIA system and central executive authorities, whose activities are directed and coordinated by the Cabinet of Ministers of Ukraine through the Minister of Internal Affairs, by logically combining their electronic information resources, and optimization of the processes of sharing technical and software resources;

2) information support of the activities of the subjects of the Unified Information System of the MIA in the performance of the tasks and functions assigned to them by the legislation in order to increase its efficiency;

3) creating the conditions for electronic interaction between the subjects of the Unified Information System of the Ministry of Internal Affairs in order to promptly fulfill the tasks in the interests of national security, assigned to them by the legislation, and reducing time and financial costs for administrative, managerial, search for information, calculation, analytical work, and reporting;

4) integration of electronic information resources of the Unified Information System of the MIA, registration of subjects of the UIS MIA in the System and provision of access to it (Clause 7 of the Regulation on the UIS MIA).

The functions of the unified information system of the MIA are: integration of electronic information resources of the Unified Information System of the MIA; processing of the information generated in the course of activities of the subjects of the UIS MIA using the central subsystem of the Unified Information System of the MIA; verification of the timeliness, accuracy and completeness of information processed by the entities of the MIA Unified Information System in accordance with the law; systematization and generalization of information, its transformation into a format suitable for further analysis and ensuring the operation of the automated decision support subsystems, signal and control services; automation and verification of the processes of information activities of the MIA Unified Information System entities in an interactive real-time mode; providing the electronic document flow in cases stipulated by law between the entities of the Unified Information System of the MIA using the central subsystem of the UIS MIA; providing the electronic information interaction of the subjects of the Unified Information System of the MIA with the services (means) of the central subsystem of the UIS MIA and/or the System of Electronic Interaction of the State Electronic Information Resources "Trembita"; delimitation of the access rights and provision for the controlled access to the functional subsystems and electronic information resources of the MIA Unified Information System to the users of the UIS MIA; ensuring the backup, storage and comprehensive protection of information contained in the electronic information resources of the MIA Unified Information System (Clause 8 of the Regulation on the MIA UIS).

The functional subsystems of the Unified Information System of the MIA are: 1) National System of Biometric Verification and Identification of Ukrainian Citizens, Foreigners and Stateless persons; 2) Information Portal of the National Police of Ukraine; 3) Unified State Register of Vehicles; 4) Register of Administrative Offenses in the Field of Road Safety; 5) System for Recording Administrative Offenses in the Field of Road Safety in an automatic mode; 6) Integrated Interagency Information and Communication System for Controlling Persons, Vehicles and Cargo Crossing the State Border; 7) "Gart-1" Border Control Information and Communication System; 8) 112 Information and Communication System; 9) Electronic Register of Human Genomic Information; 10) Unified Register of Persons Missing in Special Circumstances; 11) Unified Register of Weapons; 12) System of Management of Civil Defense Forces and Means and other systems, registers and databases created by the subjects of the Unified Information System of the MIA within the framework of their powers exercising.

The structure and operation of the functional subsystems of the MIA Unified Information System are determined by the regulations on such subsystems, which are developed by the subjects of the UIS MIA, taking into account the Model Regulation on the Functional Subsystem of the MIA Unified Information System approved by the MIA and approved in accordance with the procedure established by the law (Clause 12 of the Regulation on the UIS MIA).

The next information and telecommunication system we will focus on is the Information and Telecommunication System of Pre-trial Investigation iCase (hereinafter referred to as the iCase System). This system is the digital infrastructure of the triad of anti-corruption agencies – the National Anti-Corruption Bureau of Ukraine (NABU), the Specialized Anti-Corruption Prosecutor's Office (SAP), the High Anti-Corruption Court (HACC), and the Office of the Prosecutor General of Ukraine.

The implementation of the iCase System began in 2021. The purpose, main tasks and functions, structure, subjects, users, as well as general principles of functioning of the iCase information and telecommunication system of pre-trial investigation in criminal proceedings in which the pre-trial investigation is carried out by detectives of the National Anti-Corruption Bureau of Ukraine are determined by the Regulation on the iCase System [7].

The implementation of this system is a breakthrough in the execution of electronic criminal proceedings in Ukraine and is carried out pursuant to Clause 5.12 of the Strategy for Reforming the Judiciary, Judicial Proceedings and Related Legal Institutions for 2015–2020, approved by the Decree of the President of Ukraine No. 276/2015 dated 20.05.2015, to ensure proper coordination of the legal institutions and the unity of information system. According to the President's Press Service, the Strategy for Sustainable Development of the Judicial System for 2021-2025 (hereinafter referred to as the Strategy), developed by the Legal Reform Commission with the involvement of representatives of the expert community, was submitted to President V. Zelensky for consideration.

The second block of the Strategy specifically emphasizes the need for the fastest possible development of the electronic justice. For example, A. Stolitnyi believes that "The introduction of Electronic Criminal Proceedings is the most expedient organizationally and technically on the basis of the URPTI in four stages: 1) improvement of the URPTI functionality; 2) involvement of an investigating judge in electronic criminal proceedings; 3) involvement of all subjects of criminal proceedings in electronic criminal proceedings through external resources of digital messaging (e-mail); 4) transition to electronic criminal procedures using personal virtual offices [8, p. 24].

The purpose of the System is to automate pre-trial investigation processes, including creation, collection, storage, search, processing and transmission of materials and information (data) in criminal proceedings, as well as the processes that ensure organizational, managerial, analytical, information and telecommunication and other needs of the System users (Clause 4 of the Regulation on iCase).

The main tasks of the System include:

1) creation of a unified electronic space for the System's participants, which stores materials and information on criminal proceedings;

2) creation of the conditions for electronic interaction and automation of the work of the System's participants in order to increase the efficiency of performing the tasks assigned to them by law, reduce the time and financial costs for pre-trial investigation, management, information search, analytical work, and reporting;

3) providing accurate analytical data for making effective managerial decisions based on facts;

4) ensuring information interaction with other information (automated), information and telecommunication systems (Clause 5 of the Regulation on iCase).

The functions of the System are: 1) creation, collection, storage, search, processing and transfer of the materials and information (data) in criminal proceedings; 2) centralized secure storage of criminal proceedings materials, procedural and other documents; 3) secure storage, automated analytical processing of information; 4) exchange of documents and information (sending and receiving documents and information, joint work with documents) in electronic form between the System subjects; 5) System users access to any information stored in it in electronic form in accordance with the granted access rights; 6) automated interaction (integration) of the System with other information (automated) and telecommunication systems; 7) automatic generation of analytical reports from data sets contained in the System; 8) other functions provided for by the Regulation (Clause 6 of the Regulation on iCase).

The System consists of: 1) the System core; 2) telecommunication network; 3) automated workstations of the System users; 4) comprehensive information security system (Clause 7 of the Regulation on iCase).

The core of the System includes: 1) servers; 2) virtualization systems; 3) data storage systems; 4) a cluster of programs and services; 5) a cluster of databases; 6) integration gateway (Clause 8 of the Regulation on iCase).

The telecommunication network includes: 1) telecommunication access networks; 2) technical means of telecommunications; 3) means of cryptographic protection of information (Clause 9 of the Regulation on iCase).

The system interacts with the Unified Register of Pre-trial Investigations and the system operating in the court in accordance with Article 35 of the Criminal Procedure Code of Ukraine, and can also interact with other information, information and telecommunication systems in cases provided for by law.

The procedure for interaction of the System with the Unified Register of Pre-trial Investigations, other information and telecommunication systems is determined by the holders of the respective Systems in accordance with the requirements of the current legislation of Ukraine (Clause 10 of the Regulation on iCase) [7].

It should be noted that although the implementation of the iCase System is rather slow, it does not stop and is constantly evolving. In particular, on March 1, 2024, the HACC expands the operation of the Pre-trial Investigation Information and Telecommunication System (iCase). In addition to the already successfully functioning acceptance of applications for permission to search a person's home or other property from NABU detectives and SAPO prosecutors in electronic format, the HACC is starting to accept the applications for temporary access to things and documents. According to the court, saving resources, reducing time and logistical needs, as well as their rational use under martial law are priorities in the activities of HACC [9].

Lawyers also expect the iCase System to work in full, hoping for positive changes in general, namely: transparency of criminal proceedings for the parties and the court; the possibility of stricter compliance with deadlines, since updates (procedural decisions, etc.) in the system will be sent immediately to an authorized e-mail, not three months later or not at all; electronic document flow: the defense counsel submits a motion to the investigator through an authorized account in a matter of minutes and from that date counts down three days for the investigator to respond; the investigator does not travel halfway across the city to approve the motion with the prosecutor, having waited several hours for it to be approved by the prosecutor's office. He or she also immediately sends the motion to the prosecutor for approval; preventing procedural decisions of the investigator or prosecutor from being made "retroactively" and attached to the criminal proceedings; the discipline of both parties to the CP (in terms of time, ownership of the subject of the motion, who the documents are sent to) ensuring real competitiveness of the process, objectivity at the pre-trial investigation stage and prompt response to actions and inactions of the investigator by both parties, and not after the fact after opening the materials in accordance with Article 290 of the CPC of Ukraine; no need for the investigating judge to wait for months for the criminal proceedings from the investigator to consider a complaint about his or her inaction or unlawfulness of actions; preventing the fact that the documents of the CP are "lost" and others appear (I personally saw a fake resolution on changing the group of prosecutors / investigators, which introduced the "necessary" persons who actually participated in the investigative actions but were not initially included in the groups); speed of familiarization: when opening materials in accordance with Article 290 of the CPC of Ukraine, the parties can fully familiarize themselves with the scanned CP, audio and video recordings. At the same time, the possibility of familiarization with the materials of the CP (in paper version and material evidence) by the investigator or prosecutor is also guaranteed to the parties [10].

Also, in our opinion, it would be advisable to distinguish the electronic document management systems of law enforcement agencies, which would constitute the *third group* of resources, and include such systems as the Unified Register of Pre-trial Investigations, the iCase Information and Telecommunication System of Pre-trial Investigation, etc.

Finally, the *fourth group of* resources includes the "simple" registers – databases containing information on persons, property and / or procedural, administrative actions in the field of criminal justice and related activities of law enforcement agencies, in particular: The Register of Offenders (the Unified State Register of Domestic and Gender-Based Violence), the Register of Corrupt Officials (information on persons who have committed corruption offenses), the Unified Register of Seized Property (a register of assets seized in criminal proceedings), and others.

Turning to the issue of legal regulation of the digitalization of law enforcement activities in the field of criminal justice, it is necessary to point out a wide range of legal acts that regulate the relevant legal relations.

Thus, firstly, it is necessary to distinguish the international legal acts that must be complied with both law enforcement agencies in the context of digital transformation and national regulations, in particular the Convention on Cybercrime, the European Ethical Charter on the Use of Artificial Intelligence in the Judiciary and its Environment, the concept of the Digital Agenda for Europe within the framework of the European economic development strategy "Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth", Recommendation CM / Rec (2020) 1 of the Committee of Ministers to Member States on the impact of algorithmic systems on human rights [2, p. 27].

When developing conceptual issues of digitalization of the criminal procedure, the scholars also advise to take into account the relevant conclusions of the Advisory Council of European Judges on Justice and Information Technology, in particular: Recommendation No. R (95) 11 of the Committee of Ministers of the Council of Europe to Member States on the selection, processing, presentation and archiving of judgments in legal information and retrieval systems (Septem-

ber 11, 1995); Recommendation Rec (2001) 2 of the Committee of Ministers of the Council of Europe to Member States on the development and restructuring of the judicial systems and legal information in an economical manner (February 28, 2001); Recommendation Rec (2001) 3 of the Committee of Ministers of the Council of Europe to Member States on the provision of judicial and other legal services to citizens using the latest technologies (February 28, 2001); Recommendation Rec (2003) 14 of the Committee of Ministers of the Council of Europe to Member States on the interoperability of information systems in the justice sector (September 9, 2003); Recommendation Rec (2003) 15 of the Committee of Ministers of the Council of Europe to Member States on the archiving of electronic documents in the legal sector (September 9, 2003); Opinion No. 14 (2011) of the Consultative Council of European Judges to the attention of the Committee of Ministers of the Council of Europe on Justice and Information Technology (November 9, 2011) [2, p. 27].

As T. Pavlova noted, the relations connected to the use of information and telecommunication systems by criminal justice authorities at the national level are regulated by the Constitution of Ukraine, Civil Code of Ukraine, and the Law of Ukraine "On Information" of October 02, 1992, No. 2657-XII; "On protection of information in automated systems" of 05.07.1994, № 80/94-BP; "On state secret" of 21.07.1994, № 3855-XII; "On obligatory copy of documents" of 09.04.1999, № 595-XIV; "On electronic documents and electronic document flow" of 22. 05.2003, No. 861-IV; "On the National Archival Fond and Archival Institutions" of 24.12.1993, No. 3814-XII; "On Electronic Trust Services" of 05.10.2017, No. 2155-VIII, as well as other legal acts [11, p. 2–3].

The Law of Ukraine No. 2147-VIII dated 03.10.2017 amended part 1 of Article 35 of the Criminal Procedure Code of Ukraine (hereinafter – the CPC of Ukraine) to improve the automated court document management system, which regulates: objective and impartial distribution of criminal proceedings materials between judges in compliance with the principles of priority and the same number of proceedings for each judge; selection of jurors for the trial from the list of jurors; provision of information to individuals and legal entities on the status of consideration of criminal proceedings in accordance with the procedure provided for by the Criminal Procedure Code of Ukraine; centralized storage of texts of verdicts, rulings and other procedural documents; preparation of statistical data; issuance of verdicts, court rulings and enforcement documents based on the data available in the system; transfer of materials to the electronic archive.

The current CPC of Ukraine also contains provisions that partially regulate "the issues of electronic procedures and their recording, namely:

1) electronic form of pre-trial investigation concerning entering information about a criminal offense into the URPTI (Article 214 of the CPC of Ukraine);

2) entering procedural decisions in criminal proceedings into the URPTI (Article 218(4), Article 278(4), Article 280(4), Article 282(3), Article 281(2), Article 283 of the CPC of Ukraine);

3) use of electronic documents as a source of evidence (Articles 84, 99 of the CPC of Ukraine);

4) use of modern telecommunication means to summon a person (Article 134 of the CPC of Ukraine);

5) conducting investigative (detective) actions in the mode of video or telephone conference (Article 232 of the CPC of Ukraine) etc." [11, p. 2–3].

Taking into consideration the challenges faced by the state during the COVID-19 pandemic, and even more so during martial law, "the need for further digital transformation of criminal proceedings in Ukraine with a significant modification of the criminal procedural form through introduction of digital technologies, transition to full electronic document management is no longer in doubt and is only a matter of time" [2, p. 28].

Conclusions. Summing up, it is worth noting that the existing information and communication systems in the activities of law enforcement agencies in the field of criminal justice can be divided into four groups. Thus, the first group of information resources includes international databases, in particular, Interpol and Europol, the law enforcement agencies of Ukraine have access to.

The second group includes national departmental electronic information resources, which are large information systems and / or contain several modules and / or separate registers, and the function of electronic communication, in particular: The Unified Information System of the Ministry of Internal Affairs of Ukraine, the Unified Judicial Information and Telecommunication System, the iCase Information and Telecommunication System, the Information Portal of the National Police of Ukraine, the Unified Register of Convicts and Detainees.

In our opinion, the third group consists of registers of document flow and electronic management of law enforcement agencies, such as the Unified Register of Pre-trial Investigations, the iCase Information and Telecommunication System of Pre-trial Investigation, etc.

Finally, the fourth group of resources includes "simple" registers – databases containing information on persons, property and / or procedural and administrative actions in the field of criminal justice and related activities of state bodies, in particular: The Register of Offenders (the Unified State Register of Domestic and Gender-Based Violence), the Register of Corrupt Officials (information on persons who have committed corruption offenses), the Unified Register of Seized Property (a register of assets seized in criminal proceedings).

Thus, today, we can talk about the creation of digital infrastructure in the activities of law enforcement agencies in the field of criminal justice. The digitalization process in the law enforcement agencies of Ukraine and the status of the English language as the language of international communication according to bill #9432 adopted as a basis by Verkhovna Rada of Ukraine require the sufficient training of the personnel for successful professional communication in English.

At the same time, some scholars emphasize that "the analysis of the current criminal procedural legislation shows chaotic regulation of certain issues of digital technologies implementation in the field of criminal proceedings, in particular, the implementation and recording of electronic procedures, the creation of electronic criminal proceedings and other areas of the CCP. This level of regulation is mostly unsatisfactory due to certain legal uncertainty, which also gives rise to differences in law enforcement practice. ...Therefore, there is an obvious need for a conceptual development of the CCC issues, which includes a study of both the process of digital transformation of criminal proceedings and the quality of the current criminal procedural legislation in this area" [2, p. 29].

REFERENCES

1. Демура М. До питання про цифрову трансформацію кримінального провадження в умовах воєнного стану. *Науковий вісник ДДУВС*. 2022 р. Спеціальний випуск № 2. С. 374–381. DOI: 10.31733/2078-3566-2022-6-374-381.

2. Глинська Н. В., Клепка Д. І. Цифровізація кримінального провадження: сучасні аспекти концептуалізації. Ч.1. *Питання боротьби зі злочинністю*. 2022. № 43. Т. 1. С. 24–42. DOI: 10.31359/2079-6242-2022-43-24.

3. Kaplina O., Tumanyants A., Krytska I., Verhoglyad-Gerasymenko O. Application of Artificial Intelligence Systems in Criminal Procedure: Key Areas, Basic Legal Principles and Problems of Correlation with Fundamental Human Rights. *Access to Justice in Eastern Europe*. № 6 (3). 2023, 147–166. References : p. 165–166. DOI: 10.33327/AJEE-18-6.3-a000314. URL: https://ajee-journal.com/upload/attaches/att_1690877650.pdf

4. Офіційна веб-сторінка Міжнародної організації кримінальної поліції – Інтерпол. URL: https://www.interpol.int/How-we-work/Databases
5. Europol in Brief / The European Union Agency for Law Enforcement Cooperation. Luxembourg: Publications Office of the European Union, 2022. 21 p. URL:|https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20in%20Brief.pdf
6. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку пріоритетних електронних інформаційних ресурсів її суб'єктів: Постанова Кабінету Міністрів України від 14 листопада 2018 р. № 1024. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF#Text
7. Про затвердження Положення про інформаційно-телекомунікаційну систему досудового розслідування «іКейс»: Наказ Національного антикорупційного бюро України, Офісу Генерального прокурора, Ради суддів України, Вищого антикорупційного суду від 15 грудня 2021 р. № 175/390/57/72. URL: https://zakon.rada.gov.ua/laws/show/v0390886-21#Text
8. Столітній А. Концепція електронного кримінального провадження в Україні. *Вісник Національної академії прокуратури України*. 2018. № 4(56). С. 24–35.
9. 'ВАКС розширює експлуатацію ІКейс' (Вищий антикорупційний суд 01 березня 2024 р.) < URL: https://first.vaks.gov.ua/publications/vaks-rozshyriuie-ekspluatatsiiu-ikeys/ > (дата звернення – 21.04.2024)
10. Седун Д. 'Електронне кримінальне провадження: очікування адвокатів' (Just talk 17 березня 2023 р.) < URL: https://justtalk.com.ua/post/elektronne-kriminalne-provadzhennya-ochikuvannya-advokativ > (дата звернення – 21.04.2024)
11. Павлова Т.О. Діджиталізація як напрям трансформації кримінального провадження. *Правова держава*. 2021. № 41. С. 96–106. DOI: https://doi.org/10.18524/2411–2054.2021.41.225612