§4.2 LEGAL AND ORGANIZATIONAL AND TECHNICAL PRINCIPLES OF INFORMATION PROTECTION IN THE ACTIVITIES OF JUDICIAL BODIES

(**Kolesnikov A.,** West Ukrainian National University)

Introduction. In the current conditions of digital transformation of Ukraine's judicial system, information protection acquire critical importance for ensuring proper functioning of judicial bodies. The rapid development of information and communication technologies, implementation of electronic justice, and creation of the Unified Judicial Information and Telecommunication System (UJITS) actualize the need for a comprehensive approach to data protection

This issue has become particularly important under conditions of armed aggression by the Russian Federation against Ukraine, when cyber threats have become a real factor affecting the stability of the judicial system. The events of 2022, particularly the forced closure of state registers, clearly demonstrated the vulnerability of existing information protection mechanisms and the necessity for their systematic improvement.

The research of legal and organizational and technical foundations of information protection in the activities of judicial bodies is important for developing effective mechanisms to ensure information security that would guarantee confidentiality, integrity, and availability of data while preserving the principles of openness and transparency of judicial proceedings.

This study is a continuation of our scientific research in indicated direction [1; 11; 12; 3].

The main material. The perception of information as one of the defining instruments of societal development is a universally recognized fact. The effectiveness of decision-making largely depends on quality, timely, and complete information processing, as well as its professional use. However, to achieve these

goals, it is necessary to develop and implement reliable data protection mechanisms. In the activities of judicial bodies, information protection acquires critical importance, especially in the era of rapid digital technology development. A key aspect in this regard is guaranteeing confidentiality and data integrity, which not only determines trust in the justice administration system but also contributes to better protection of citizens' rights and freedoms.

Aspects of information protection in the activities of judicial bodies are the subject of several scientific studies. Researchers S. Demchenko in the work "Approaches to the Content of the Concept 'Information': Cybernetic, Philosophical, Legal" [8] and S. Banakh in the work "The Concept and Features of Information as a Theoretical Category" [4] conducted analysis of information from the theoretical concept perspective, focusing on its legal application. Legal aspects of information protection in UJITS were examined by professors V. Teremetskyi and Ye. Duliba in the work "Peculiarities of Implementation and Functioning of the Unified Judicial Information and Telecommunication System as an E-justice Tool" [26], scholar Yu. Georgievskyi in the work " Proposals for legal support of information protection in the Unified Judicial Information and Telecommunication System" [6]. M. Shepitko in the work "Criminal Law Protection of Information Security During Justice Administration" [29] conducts legal analysis of data protection in the judicial system and highlights potential risks of using AI for information protection. At the same time, specific objects of information protection and possible threats to their integrity require further study.

Ensuring effective information protection involves clear definition of objects that require such protection. These objects can be divided into two categories. The first is data stored in legal registers and protected databases. The second is information about persons involved in the process of administering justice.

Comprehensive Information Protection System (CIPS) provides for implementation of the following tools:

— regulatory-legal (application of current legislation to regulate rights and obligations of all subjects in the field of information security);

— moral-ethical (formation of organizational culture where violation of information security rules is perceived negatively by most employees);

— barrier (installation of physical obstacles to prevent unauthorized access to protected information);

— administrative (implementation of internal procedures and rules to ensure proper level of secrecy and access control);

— technical (use of specialized equipment for technical information protection);

— cryptographic (application of encryption methods for information protection during processing and transmission);

— software-technical (use of special software for control and restriction of access to information resources) [9].

Implementation of modern technologies opens new possibilities and allows optimization of judicial processes. However, realization of the electronic litigation concept must be accompanied by simultaneous development of legal and material base for electronic information protection.

This is critically important because reliable data protection directly affects the security of participants in administrative-procedural relations. Moreover, it is a guarantee of ensuring fundamental principles of judicial proceedings: fairness, equality, legality, and impartiality of both the process itself and judicial decisions.

Thus, technological progress in the judicial system must go parallel with the development of information protection mechanisms to guarantee integrity and effectiveness of the judicial process in the digital era [25, c. 46].

In the Law of Ukraine "On Information," the concept of information protection is defined as "a set of legal, administrative, organizational, technical and

other measures that ensure preservation, integrity of information and proper order of access to information" [21]. This definition will be taken as a basis when studying aspects of information protection in justice administration.

The legal foundation for information protection in court activities is laid in the Law of Ukraine "On Information Protection in Information and Telecommunication Systems" [19], which plays an important role in regulating information protection in the context of court activities. Article 1 of the Law defines key concepts such as information (automated) system, information protection, unauthorized actions regarding information in the system, violation of information integrity in the system, and others that apply to judicial information systems. Article 4 establishes general requirements for information protection in systems, including judicial ones. Article 5 regulates the procedure for access to information in systems, which is important for ensuring confidentiality of judicial data. Article 8 defines responsibility for violations of information protection legislation, which also applies to judicial system employees. Article 10 establishes requirements for creating a comprehensive information protection system, which applies to the development and implementation of information systems in courts. This law creates a legal foundation for ensuring information security in the judicial system, establishing standards and requirements for protecting information processed in judicial information systems [19].

Another general document regulating features of information protection is "Rules for Ensuring Information Protection in Information, Electronic Communication and Information Communication Systems" [18]. Organizational measures include the development of information security policy, appointment of responsible persons, and conducting regular audits. These actions are aimed at creating a structured approach to information protection at the organizational level. Technical measures cover protection against unauthorized access and malicious

software, as well as ensuring backup and data recovery. They aim at technical provision of information security. The rules take into account the specifics of protection in different types of systems, establishing specific requirements for information, electronic communication and information and communication systems. This ensures an adapted approach to security depending on the nature of the system. The document also defines responsibility for violations of information protection rules and the control procedure, providing a mechanism for supervision and verification of compliance with established rules.

Conditions for protecting internal information for official use are outlined in the "Standard Instruction on the Procedure for Accounting, Storage, Use and Destruction of Documents and Other Material Information Carriers Containing Official Information" [27]. This describes certain aspects of document protection during storage in the context of the use of safes, metal cabinets and specially equipped premises. The instruction also regulates the transfer, transportation and copying of documents, which are means of their physical protection.

In general, legal regulation of relations related to informatization of the justice administration sphere is based on several basic laws: "On Electronic Documents and Electronic Document Flow," "On Information," "On Access to Public Information," "On Access to Court Decisions," "On Information Protection in Information Communication Systems," "On Personal Data Protection". These regulatory documents became the basis for developing specialized regulatory-legal acts. Thus, in the "Concept of the Program for the Informatization of Local and Appellate Courts and the Project for the Construction of the Unified Judicial Information and Telecommunications System (UJITS) for 2022-2024" [13] one of the priority directions concerns information protection and cyber protection, and provides for implementation of the following tasks: introduction of centralized management of user accounts and access rights; improvement of network

architecture to ensure control of user and administrator actions; configuration of software, hardware resources, and auxiliary equipment based on principles of mandatory duplication of all important components; introduction of a monitoring system for data center equipment operability and loading, as well as operability of critical services and load forecasting for software modules; introduction of automatic data backup system, development of procedures for quick recovery of software modules and separate data blocks; introduction of risk-oriented approach and implementation of Information Security Management System elements [13].

These organizational-technical measures are provided with optimal use of resources of main and backup data processing centers (hereinafter - DPC). This will ensure sufficient fault tolerance for UJITS needs within the Program framework and create a foundation for further expansion of technical capabilities. The ultimate goal is to guarantee uninterrupted information exchange between courts, bodies and institutions of the justice system, as well as ensure interaction with other state information resources, systems, and registers.

Development and state expertise of comprehensive information protection systems (hereinafter - CIPS) for UJITS and DPC will include implementation of a wide range of organizational, software, and technical measures. These measures are aimed at ensuring confidentiality, integrity, and availability of information resources at all stages of their storage, processing, and transmission.

Protection of UJITS and DPC information resources will be carried out through application of technical information protection means, as well as implementation of organizational and engineering-technical measures within the comprehensive information protection system. These measures aim to prevent information blocking, unauthorized access, its modification or distortion.

CIPS for UJITS and DPC undergoes state expertise in the field of technical information protection with obtaining a corresponding compliance certificate [13].

Another regulatory document regarding the CSI in judicial proceedings is the "Plan of measures for the creation and implementation of the CSI at the objects of information activities in the State Judicial Administration of Ukraine, territorial departments of the State Judicial Administration of Ukraine, local and appellate courts of general jurisdiction for 2014-2016" [16]. Main content of the order:

– approval of the plan of measures for building CIPS;

— determination of responsible persons and deadlines for implementing measures;

— list of objects where CIPS is implemented: SJA of Ukraine, its territorial administrations, local and appellate courts;

— main stages of CIPS implementation: object examination, development of technical documentation, implementation of protection means, system certification;

— measures for personnel training regarding work with CIPS;

— control over implementation of the action plan.

The above-mentioned Law of Ukraine "On Information Protection in Information and Communication Systems" [19] defines fundamental principles of legal protection of data stored in register form. According to this law, access to information means providing the user with the right to process it. Any actions with information performed in violation of established access rules are considered unauthorized and violating its integrity. Additionally, the Law defines the category of information processing as collection, input, recording, transformation, reading, storage, destruction, registration, acceptance, receipt, transmission, which are carried out in the system using technical and software means. Hence, we observe the presence of another factor in the information processing process: it can be carried out both automatically and with direct human participation. In this context, let us pay attention to Article 2 of the Law, where objects of information protection in the system are defined as information processed in it and software designed for

processing this information [19]. We offer to amend Article 2 of the Law, expanding its subject aspect, namely including methods and algorithms of information processing in the list of protection objects.

Considering this, we include the following among objects of legal protection in the field of information work:

1. Information resources are a set of data collected in various forms of representation, such as registers, databases, systems and other digital or paper sources. They may contain confidential information, personal data, trade secrets or other information that requires protection from unauthorized access, modification or disclosure.

Examples of information resources: registers (state registers, legal registers, property registers, etc.); databases (client databases, scientific databases, legal databases, etc.); digital archives and repositories (libraries, scientific repositories, etc.); paper documents (contracts, reports, ledgers, etc.).

2. Information systems (organizational and technical system in which information processing technology is implemented using hardware and software).

Examples of information systems: electronic document management systems; database management systems; e-commerce systems; access control and security systems.

3. Information about subjects who have access to work with information resources and information systems. An important aspect of information protection is the control of access to information resources and systems. Therefore, it is necessary to have clear information about subjects who have the right to work with such resources and systems, as well as to determine their powers and restrictions.

Examples of information about subjects of access: user credentials (names, passwords, positions, access levels); policies and procedures for access to information resources and systems; logs of user actions (audit of access and

changes); lists of persons authorized to manage information resources and systems [10, c. 9].

An important tool for secure work with information in judicial proceedings is the use of an electronic digital signature (EDS), which, in accordance with the Law of Ukraine "On Electronic Identification and Electronic Trust Services", is defined as an advanced electronic signature created using a qualified electronic signature tool and based on a qualified electronic signature certificate [15].

The law recognizes EDS as equivalent to handwritten signature in terms of legal force. Regarding qualified electronic seal, it provides presumption of inviolability of electronic information and authenticity of the source of this data to which it is attached. In other words, data sealed with such a seal are considered integral and originating from the specified source until proven otherwise.

Application of EDS increases confidentiality in transmission and storage of judicial documents. Use of qualified electronic timestamp allows precise establishment of the moment of document signing, which is important for compliance with procedural deadlines. Electronic documents with EDS are easier to store and create backup copies, which reduces the risk of losing important materials.

EDS accelerates document exchange between participants in judicial process, increasing efficiency of judicial proceedings. It also allows submitting documents and participating in hearings remotely, which improves accessibility of justice. Use of EDS facilitates audit and control over document movement, increasing transparency of the judicial system.

Overall, implementation of EDS significantly increases the level of data protection in the judicial system, ensuring authenticity, integrity, and legal force of electronic documents, as well as contributes to efficiency and accessibility of justice.

One of the means of preventing technical protection violations is the Antivirus Information Protection Center, among whose tasks is creating and implementing a unified approach to antivirus protection in information and telecommunication systems of state bodies. This includes centralized supply and implementation of antivirus software that has passed official certification according to requirements of Ukrainian legislation, which will ensure coordinated and effective protection against viral threats in all state information systems [28].

The invasion of the Russian Federation into Ukraine on February 24, 2022, defined qualitatively new requirements for approaches to information protection. The realization of the scale of the threats resulted in the closure of virtually all registers in the first days of the invasion. Also, the decision of the Council of Judges of Ukraine dated March 25, 2022 No. 11 states that the right to access information, guaranteed by Article 34 of the Constitution of Ukraine, is not absolute and may be subject to restrictions. Such restrictions must be exceptions provided for by law, pursue one or more legitimate goals, and be necessary in a democratic society. [24]. Thus, the Council of Judges of Ukraine determines the conditions for a more stringent application of the provision of part two of Article 6 of the Law of Ukraine "On Access to Public Information" stating that restriction of access to public information is possible in cases: in the interests of national security, territorial integrity or public order in order to prevent riots or criminal offenses, to protect public health, to protect the reputation or rights of other people, to prevent the disclosure of information received confidentially, or to maintain the authority and impartiality of justice; disclosure of information may cause significant harm to these interests; the harm from the publication of such information outweighs the public interest in obtaining it [14]. The beginning of military actions made this norm of the Law particularly relevant.

Under conditions of armed conflict, the role of law enforcement bodies has significantly increased, especially regarding investigation of war crimes and

bringing to responsibility for collaborationist activities. In this context, disclosure of information about activities of state bodies, including courts, may pose a threat to the life and health of their employees. Moreover, collection of such information during conflict may be regarded as subversive activity against Ukraine. Considering these circumstances, a decision was made about a special procedure for processing information requests. Now, when requests for obtaining public information about court work and other institutions of the justice system arrive, copies of these requests must be immediately transmitted to the Security Service of Ukraine. The SSU conducts thorough verification of persons requesting information and their motives.

The necessity of strengthening information protection in state institutions becomes obvious through numerous cyberattacks from the Russian Federation. According to data from CERT-UA (Computer Emergency Response Team of Ukraine), which operates within the State Special Communications Service, these attacks have a systematic character. Often they become possible through non-compliance with basic information security rules.

Specialists note that in most cases, malefactors obtain unauthorized access to computer systems of the attack object long before its implementation, often a year or more. To penetrate the network, they use VPN accounts, exploit software vulnerabilities and deficiencies in settings of publicly accessible information systems. The success of many cyberattacks is often related to negligence of managers and executors on the ground who do not pay proper attention to information about current cyber threats. System owners repeat typical mistakes: they do not use two-factor authentication; they do not ensure proper network segmentation, especially regarding restriction of administrative access; they do not control the attack surface, including vulnerable software, "open ports," etc.

The forced complete closure of registers in the justice sphere created problems for ensuring transparency of judicial process and realization of the right

to access public information. This situation clearly demonstrated the need to increase resilience of judicial body information systems to cyberattacks and data leaks. Under conditions of military aggression, the existing protection system proved insufficiently effective.

To solve this problem, it is necessary to apply a comprehensive approach to information security issues in the judicial system.

— technical improvement (strengthen protection of registers and databases by implementing advanced cybersecurity methods, effective encryption protocols, and regular backup systems);

— legislative changes (update legislation and develop clear procedures to ensure balance between data protection and right to information in emergency situations. Create mechanisms for selective restriction of access to sensitive information without complete closure of registers);

— educational measures (conduct training for court and law enforcement personnel on cyber hygiene and information security issues).

Thus, the experience of register closure revealed systemic deficiencies in information protection in the judicial system. To prevent similar problems in the future, it is necessary to implement comprehensive measures of technical, legislative, and educational nature in this critically important sphere.

A unified approach to building an information protection system involves building a unified system and organizational approach. In different courts, the organizational structure of the structural unit responsible for information protection is different. In the SJA of Ukraine, responsibility for information protection is assigned to the Information Technology and Information Protection Department.

Systematic information protection in the functioning of justice administration bodies involves forming a unified approach to forming the structure of such bodies. Currently, the functions of such department in individual courts are

performed by one person in most cases. In particular, among the job responsibilities of the chief specialist of the organizational-personnel department of the Commercial Court of Ternopil region are the following: manages work related to implementation of new technologies and Network development; implements organizational (control of compliance with computer equipment usage rules) and technical (regular change of network passwords, monitoring launch and termination of software use that violates normal Network operability, computers in it, and Network security) measures to stop unauthorized connection to the Network from external networks, as well as from Network computers. Provides Users with consultation assistance on issues of using Network resources; Checks integrity and security of the court's electronic information database, and in case of detecting damage or unauthorized access to it, immediately informs the head of staff and the head of court; ensures functioning of automated electronic document management system in court; prevents installation and use of third-party software and media content not directly related to court work.

Researchers O. Hyliaka S. and A. Mernyk define personal data security breaches as an incident that negatively affects confidentiality, integrity, or availability of personal information. Such breaches occur in various situations: when data is lost, destroyed, damaged, or unauthorized disclosed; when someone gains unauthorized access to information or transmits it without proper permission; or when data becomes inaccessible, for example, due to encryption by ransomware or accidental loss or destruction. In case of a security incident, it is critically important to promptly determine whether a personal data breach has actually occurred. Quick reaction and effective actions can significantly reduce negative consequences of such incident [7, c. 164].

Scientists V. Barannik, V. Vlasov, and V. Tarnopolov, using the example of videoconferencing system security, define three groups of threats. The first

includes risks caused by actions of access subjects. Security measures against these threats can be controlled, and they depend on accuracy of assessment and forecasting. The second category covers less predictable threats that depend more on technical characteristics of equipment. Potential security risks for videoconferencing system related to technical means may also have external or internal origin. The third category consists of threats caused by natural phenomena. These potential risks for security of video information resource of videoconferencing usually have external character [5].

When detecting personal data security breach during justice administration, the primary task is risk assessment, which should consider possible negative consequences for all participants in judicial process. Inability to timely and properly eliminate the breach may have serious consequences, namely loss of control over use of confidential information, violation of equal treatment principle, discrimination, theft of personal data or fraud. In the judicial sphere, such breaches may have additional consequences: undermining trust in judicial system, compromising witnesses or experts, influencing impartiality of judges, or even threatening security of process participants. Thus, quick and effective response to detected facts of personal data security breaches is important for preserving integrity of judicial process and protecting rights of all involved parties.

Processing personal data of judicial power representatives requires a balanced approach to maintain balance between privacy protection and ensuring transparency in state body work. Thus, in the "Strategy for Reforming Judicial System, Judicial Proceedings and Related Legal Institutions for 2015-2020," among tasks is indicated the need to establish balance between information protection and right to fair trial in the interests of justice transparency, including establishment of clear legislative criteria for closed case consideration [22].

Persons holding public positions must understand that their special status involves a certain level of publicity, which naturally narrows the sphere of their private life. However, this does not mean that their personal data can be used and distributed uncontrollably.

The Constitutional Court of Ukraine in its decision of January 20, 2012, emphasized the necessity of publishing certain information about state authorities and their officials. This is due to their public status and need to maintain public trust and authority of power. However, the issue is complicated by the fact that personal data may concern not only officials themselves but also members of their families. The latter have constitutional right to protection of private and family life. Therefore, each case requires individual consideration to find balance between public interest in information disclosure and protection of human rights. It is necessary to determine when publication of personal data serves important public interests and when it may violate person's rights.

Personal data of judges and court staff may contain sensitive information, particularly about their political views, religious beliefs, or health status. Disclosure of this information may compromise a judge and thus affect his independence and impartiality when considering cases. Given this, it is critically important to ensure reliable protection of this data from unauthorized access, leakage, or improper use. This requires implementation of effective information protection mechanisms in the judicial system.

Ukrainian legislation establishes specific norms regarding publication of personal data of persons working in the judicial system. For candidates for elected positions and civil servants of first category, most personal data is not considered information with restricted access, except for data defined by law as confidential. Instead, personal data of family members of judges and court employees are usually protected from illegal disclosure. Declarations of income of persons

applying for positions in judicial bodies or already holding them, as well as their personal data (except those that law defines as information with restricted access) are not considered confidential. Such approach aims to ensure a certain level of transparency in official activities, making part of their personal data accessible to the public, which contributes to power accountability.

In the Constitutional Court of Ukraine decision in the case on constitutional petition of Zhashkiv District Council of Cherkasy region regarding official interpretation of provisions of parts one, two of Article 32, parts two, three of Article 34 of the Constitution of Ukraine, it is stated: When resolving issues regarding confidentiality of information about a person holding a position related to performing functions of state or local self-government bodies and members of her family, the CCU proceeds from the fact that belonging of information about a physical person to confidential is determined in each specific case. Being in a position related to performing functions of state or local self-government bodies involves not only guarantees of protecting this person's rights but also additional legal burdens. Public character of both the bodies - subjects of power authorities and their officials requires publication of certain information for forming public opinion about trust in power and supporting its authority in society [23].

The processing of personal data of persons holding public office, as well as all other individuals, must comply with the principles and requirements of personal data protection legislation. Authorities should have clearly defined purposes for data processing and established procedures for their collection, storage, use and deletion. It is important to distinguish between general personal data and data of special categories that require enhanced protection.

Courts should ensure sufficient transparency of their activities and decisions for public scrutiny. At the same time, the information published is depersonalized to protect the personal data of participants in legal proceedings. This approach

allows balancing the need for transparency of the judicial system with the need to protect personal data.

It is necessary to introduce strict control over access to personal data of representatives of the judiciary to prevent their misuse. All employees working with personal data must strictly follow internal instructions. At the same time, there are specific features of personal data protection and responsibility for their dissemination in different areas.

State authorities should ensure transparency of their activities, while protecting the privacy of officials and their families. This requires compliance with the principles of legality, justification of purposes, necessity and proportionality. Achieving a balance between protecting confidential data and ensuring the openness of the judicial system requires a comprehensive approach that includes organizational measures, technical solutions and legal mechanisms. Only such a comprehensive approach can guarantee proper data protection without compromising the principles of transparency and accountability of the judiciary.

Effective information protection plays an important role in ensuring the proper functioning of the judicial system. Precise definition of objects of protection will increase the effectiveness of security measures. It is important to protect not only information resources and systems, but also data about individuals who have access to them. In addition to observing procedural aspects, it is critically important to implement basic principles of information hygiene. To achieve these goals, it is necessary to apply a comprehensive approach to information security in the judicial system, which will cover all aspects of data protection and ensure the system's resilience to various threats. Such an approach will allow creating a reliable information protection system that will support the integrity and efficiency of the judicial system as a whole.

Another vector for developing information protection tools in the justice system is their compliance with international regulations. One of these is the General Data Protection Regulation (GDPR), adopted in 2016 [2], which defines the features of the protection of personal data of an individual at a qualitatively new level. The GDPR regulation significantly expanded the scope of data protection legislation, covering almost all international organizations that collect or process personal information. This document defined a comprehensive set of new legal requirements that require the implementation of organizational and technological measures.

Such approach forced global companies and institutions to review their data handling practices, regardless of their geographical location. GDPR established new personal data protection standards that became mandatory not only for European but also for many global organizations working with information about physical persons.

GDPR influence determined several requirements for data protection in justice administration system.

Raising personal data processing standards. GDPR establishes strict requirements for personal data processing, which can be applied to information of judicial process participants, witnesses, victims, and other persons involved in justice system.

Data minimization principle. According to GDPR, only data necessary for specific purpose should be collected and processed. In judicial system, this means limiting collection of personal information to minimum necessary for justice administration. Point 3 of Article 6 of the Law of Ukraine "On Personal Data Protection" states that composition and content of personal data must be relevant, adequate, and not excessive regarding determined purpose of their processing [20]. We consider the term "not excessive" incorrect. We believe that according to GDPR norms, it should be changed to "minimally necessary."

Strengthening security measures. GDPR provides for implementation of adequate technical and organizational measures for data protection. This may include data encryption, access control, regular security audits in judicial information systems. In the context of implementing this task, we consider it appropriate to add a function for developing detailed protocol of actions in case of detecting data security breaches, including mandatory notification of data subjects, in the second section of "Regulation on the Procedure for Functioning of Individual Subsystems of the Unified Judicial Information and Telecommunication System" [17].

Appointment of responsible persons. According to GDPR, a special data protection officer may be appointed in judicial system to supervise compliance with data protection rules and procedures. This involves making changes to the Standard Regulation on Court Staff. For this purpose, in the Court Staff Structure section, it is appropriate to add a point with the following content: "The court staff structure includes the position of personal data protection officer. The officer is directly subordinated to the head of court staff and interacts with the person responsible for data protection in judicial system. The officer ensures compliance with personal data protection legislation in court, conducts consultations and training for staff members, participates in implementing technical and organizational data protection measures. The head of court staff ensures conditions for effective performance of officer's duties."

Data processing transparency. GDPR requires informing data subjects about processing their information. In judicial system, this may mean greater transparency regarding how personal data of judicial process participants is used.

Increased responsibility. GDPR establishes significant fines for violations, which may stimulate judicial system to more serious attitude toward data protection.

Conclusions. The conducted analysis of legal and organizational-technical foundations of information protection in activities of justice administration bodies demonstrates complexity and multi-aspect nature of this issue. The study revealed that modern information protection system in judicial sphere is based on comprehensive combination of regulatory-legal, moral-ethical, technical, and organizational measures, but requires substantial improvement.

Analysis of current legislation showed existence of extensive regulatory-legal base regulating information protection issues in judicial system. At the same time, certain gaps and inconsistencies were revealed, particularly in defining protection objects and distributing responsibility between different structural subdivisions. Special attention is needed for bringing national legislation into compliance with international standards, particularly GDPR requirements, which involves making changes to personal data processing procedures and strengthening their protection measures.

Organizational aspects of information protection are characterized by fragmentation and lack of unified approach. In different courts, information protection functions are performed by different structural subdivisions, often with limited resources and qualifications. This creates risks for ensuring proper level of information security and requires systematic reform of organizational structure.

Technical aspects of information protection develop toward implementation of modern cryptographic protection means, electronic digital signature, and comprehensive information protection systems. However, their effectiveness largely depends on compliance with basic principles of information hygiene and professional staff training.

Special attention is needed for personal data protection of judicial process participants and judicial system employees. The necessity of ensuring judicial transparency must be combined with guarantees of personal information

confidentiality, which requires developing balanced approaches to data processing and publication.

References:

1. Kolesnikov, A. (2023). Cybersecurity as a necessary condition for the functioning of the justice administration system. *Entrepreneurship, Economy and Law*, 5, 101-107. https://doi.org/10.32849/2663-5313/2023.5.15

2. European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation). Official Journal of the European Union, L 119/1https://gdpr-text.com/uk/read/article-25/

3. Teremetskyi V., Kovalchuk O., Kolesnikov A., Bogdanov R., Korniienko M., Dir I. (2024). Improving the information and legal support of the judicial system of Ukraine: experience of the European Court of human rights. *Journal of Ecohumanism*, Vol. 3, No. 3. Pp. 61-74. DOI: https://doi.org/10.62754/joe.v3i3.3349

4. Banakh, S. (2019). The Concept and Features of Information as a Theoretical Category. *Actual Problems of Jurisprudence*, 2019. № 4(20), 226-231.

5. Barannik, V. V., Vlasov, A. V., & Tarnopolov, R. V. (2014). Security threat model for video information resource of videoconferencing systems. *Science-Intensive Technologies*, 1(21), 55-60.

6. Georgievskyi, Yu. V. (2020). Proposals for legal support of information protection in the Unified judicial information and telecommunication system. *Legal Scientific Electronic Journal*, 3, 204-208.

7. Hyliaka, O. S., & Mernyk, A. M. (2023). Some issues of implementation of the right to privacy and confidentiality in the conditions of modern digital technologies. *Bulletin of the National Academy of Legal Sciences of Ukraine*, 30(3), 156-172.

8. Demchenko, S. (2016). Approaches to the content of the concept "information": cybernetic, philosophical, legal. *Jurnalul juridic national: teorie şi practică* , 1/2 (17) C. 35-38.

9. Kyryliuk, R. I. (2011). Legal nature of relations regarding organizational support of court activities with participation of the State Judicial Administration of Ukraine: problematic issues of definition. *Viche: Public-Political Journal of the Verkhovna Rada of Ukraine*, 19, 28-32.

10. Kolesnikov, A. (2024). Features of information protection in the activity of justice enforcement bodies. *Economy. Finance. Law*, 5, 8-12. https://doi.org/10.37634/efp.2024.5.1

11. Kolesnikov A. P. (2024). Legal tech in Ukraine under conditions of global digitalization. Scientific Notes. Series: Law, 16, 98-102. https://pravo.cusu.edu.ua/index.php/pravo/article/view/406

12. Kolesnikov A. P. (2024). Implementation and interaction features of the Unified Judicial Information and Telecommunication System modules. *Bulletin of Luhansk Educational and Scientific Institute Named After E.O. Didorenko*, 2(106), 71-81. https://doi.org/10.33766/2786-9156.106.1.71-81

13. State Judicial Administration of Ukraine. (2022, January 1). *Concept of the Program for the Informatization of Local and Appellate Courts and the Project for the Construction of the Unified Judicial Information and Telecommunications System (UJITS) for 2022-2024*. https://zakon.rada.gov.ua/rada/show/n0001750-22#Text

14. Verkhovna Rada of Ukraine. (2011, January 13). *On access to public information* (Law No. 2939-VI). https://zakon.rada.gov.ua/laws/show/2939-17#Text

15. Verkhovna Rada of Ukraine. (2017, October 5). On electronic identification and electronic trust services (Law No. 2155-VIII). https://zakon.rada.gov.ua/laws/show/2155-19#Text

16. State Judicial Administration of Ukraine. (2014, January 23). *On approval of the Plan of measures for the creation and implementation of the CSI at the objects of information activities in the State Judicial Administration of Ukraine, territorial departments of the State Judicial Administration of Ukraine, local and appellate courts of general jurisdiction for 2014-2016* (Order No. 14). https://zakon.rada.gov.ua/rada/show/v0014750-14#n14

17. High Council of Justice. (2021, August 17). On approval of Regulation on the procedure for functioning of individual subsystems of the Unified Judicial Information and Telecommunication System (Decision No. 1845/0/15-21). https://zakon.rada.gov.ua/rada/show/v1845910-21#Text

18. Cabinet of Ministers of Ukraine. (2006, March 29). *On approval of Rules for ensuring information protection in information, electronic communication and information communication systems* (Resolution No. 373). https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text

19. Verkhovna Rada of Ukraine. (1994, July 5). *On information protection in information and communication systems* (Law No. 80/94-VR). https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

20. Verkhovna Rada of Ukraine. (2010, June 1). *On personal data protection* (Law No. 2297-VI). https://zakon.rada.gov.ua/laws/show/2297-17#Text

21. Verkhovna Rada of Ukraine. (1992, October 2). *On information* (Law No. 2657-XII). https://zakon.rada.gov.ua/laws/show/2657-12#Text

22. President of Ukraine. (2015, May 20). *On the Strategy for reforming judicial system, judicial proceedings and related legal institutions for 2015-2020* (Decree No. 276/2015). https://zakon.rada.gov.ua/laws/show/276/2015#Text

23. Constitutional Court of Ukraine. (2012, January 20). *Decision in the case on constitutional petition of Zhashkiv District Council of Cherkasy region regarding official interpretation of provisions of parts one, two of Article 32, parts two, three of Article 34 of the Constitution of Ukraine* (No. 2-rp/2012).

24. Council of Judges of Ukraine. (2022, March 25). *Decision No. 11*. https://rsu.gov.ua/uploads/news/richenarsu11250322-f68cadf705.pdf

25. Smokovich, M. I. (2020). Electronic litigation. In O. V. Shcherbaniuk & L. G. Bzova (Eds.), *Modern challenges and current problems of judicial reform in Ukraine: Materials of IV International scientific-practical conference* (pp. 43-47). VAITE Publishing House.

26. Teremetskyi, V. I., & Duliba, Ye. V. (2023). Features of implementation and functioning of the Unified Judicial Information and Telecommunication System as an electronic justice tool. *Forum of Law*, 2(75), 130-143. http://doi.org/10.5281/zenodo.10007341

27. Cabinet of Ministers of Ukraine. (2016, October 19). *Standard instruction on the procedure for accounting, storage, use and destruction of documents and other material information carriers containing official information* (Resolution No. 736). https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF#Text

28. Antivirus Information Protection Center. (n.d.). *Official website*. https://cazi.gov.ua/uk

29. Shepitko, M. (2022). Criminal law protection of information security during justice administration. *Issues of Crime Prevention*, 4, 69-75.