UNIVERSALLY RECOGNIZED AND NATIONAL PRINCIPLES OF COMPETENCE OF CIVIL SERVANTS AS A BASIS FOR LEGAL PROVISION OF INFORMATION SECURITY: THE EXPERIENCE OF THE EUROPEAN UNION

[a]OLENA KRYVTSOVA, [b]MARTA KARPA, [c]KATERYNA SHVETS, [d]STANISLAV LOPATIN, [e]PYLYP YEPRYNTSEV, [f]VALENTYNA KRYVTSOVA

[a,f]Odessa Regional Institute for Public Administration of the National Academy for Public Administration under the President of Ukraine, 22, Henuezka Str., 65009, Odessa, Ukraine
[b]Vasyl Stefanyk Precarpathian National University, 57, Shevchenko Str., 76018, Ivano-Frankivsk, Ukraine
[c]Interregional Academy of Personnel Management, 2, Frometivska Str., 03039, Kyiv, Ukraine
[d,e]Donetsk State University of Internal Affaires, 21, Stepana Tilhy Str., 50065, Kryvyi Rih, Ukraine
email: [a]Lnpanyy21@yahoo.com, [b]1985kmii@ukr.net, [c]katerynachornackp1@gmail.com, [d]trianon0690@ukr.net, [e]efs81111@ukr.net, [f]vkrivtsova12@ukr.net

Abstract: The results of the analysis of the practices of the European Union in the field of the principles of competence of civil servants as a basis for legal provision of information security, the demand for methodological tools in the authorities, the analysis of regulatory and methodological support for the assessment of competencies in information security are presented. Conceptual approaches to the development of a competency model, assessment tools and evaluation procedures are given, taking into account the requirements of regulatory enactments in the field of information security, the characteristics of the target groups of the assessed governmental employees and the purpose of assessment. It is assumed that the use of methodological tools will provide an opportunity to obtain the necessary analytical information for defining tasks and choosing programs for the development of competencies of civil servants in the field of cybersecurity, which may also be in demand in educational organizations that train civil servants.

Keywords: Civil servant, Competence, Concept, Cybersecurity, Information.

1 Introduction

The development and widespread use of information and communication technologies is a global trend in world development in recent decades. The 21st century is characterized by the predominance of global and informational features of society in world civilization. The processes of convergence and interpenetration of national policies and economies are acquiring a global scale, permeating various aspects of the socio-economic, political and cultural life of the integrating countries, based on the development of computer technologies [35]. In these conditions, globalization presupposes the formation of a single world information space, as well as the formation of an international legal and cultural information field, a kind of infrastructure for interregional, including information, exchanges.

The modern stage of development of society is characterized by the increasing role of the information sphere, which represents the totality of information, information infrastructure, entities that collect, form, disseminate and use information, as well as the system of regulation of the resulting public relations. The information sphere, being a system-forming factor in the life of society, actively influences the state of political, economic, defense, and other components of security. Therefore, the information component is an important component of national security. By virtue of its versatility, information security affects various spheres of public life, in particular, it is an integral part of military security, but is not confined within its framework. Information security is not limited to purely technical and technological parameters (information and technical security) [54]. Information and psychological (psychophysical) security is no less important for both the military and non-military areas. Undoubtedly, each of the designated aspects has its own specifics, but there is no insurmountable border between them, therefore it is necessary to see their connections and interactions, which contributes to the creation of a holistic picture of the modern global and national information space.

National information security is a complex concept that is disclosed in different ways in various public documents, textbooks, and expert articles [1-8]. It is not limited only to the information security of the state, its bodies, the spheres of defense and internal politics.

The information security doctrine considers the balanced interests of the individual, society, and the state as an object of protection. Without the protection of the informational interests of the individual and the citizen, it is impossible to perceive the state as a subject of a social contract and a bearer of sovereignty, without which the protection of citizens is impossible. Also, within the concept, there is the protection of information infrastructure, carried out by software, physical and technical means, ensuring the safety of scientific developments and know-how [54].

Thus, national security in the digital space, including ensuring the information security of the individual, society, state, and infrastructure, is understood as the state of protection of the information environment, which guarantees the observance of the rights and legitimate interests of the individual, society, and the state in the information sphere, when their protection, implementation is fully ensured, as well as development opportunities regardless of the quantity and quality of internal and external threats.

The key components of information security are technology, processes, and people. At the same time, national and global experts emphasize the most important role of governmental employees in ensuring information security, the importance of developing personnel competencies in this area [10-12]. If the requirements for the technologies used are met and the processes are properly built, work to ensure information security without assessing and developing the competencies of employees in this area will always be fraught with risks.

Developing the ideas of the influence of the human factor on the success of digital transformation and, in general, on information security, various studies rely on a competency-based approach to determining the state of information security in state bodies and focuses on the assessment of public civil servants in the field of information security. At the same time, the assessment is considered as a starting point for the development of programs for the development and training of state (and municipal) employees, the most important part of systemic measures in government bodies to achieve the required level of legal support in the field of information security [31].

Meanwhile, the lack of systematic work to determine the level of development of the competencies of civil servants in the field of information security in the context of digitalization increases the risks of the state authorities of nation-state in this area [13]. The existing gaps in legislation, in the methodological support by regulators, in the practice adopted in the civil service, and the urgency of the problem made it necessary to study the EU best practices in the field of the need to ensure a high level of competence of civil servants regarding, first of all, legal provision of information (cyber-) security [17-19].

2 Materials and Methods

Due to the development of the processes of informatization of public administration, civil servants are involved in the whole system of information legal relations; therefore, it is almost impossible to imagine their control and supervisory, licensing, and jurisdictional activities without obtaining and using relevant information [23, 25, 26]. Taking this into account, in the modern period, it seems necessary to develop a new model of administrative and legal regulation of information, legal relations in the system of the state civil service, which would take into account the fundamentally new problems of global informatization of modern society [27-30]. The state civil service is experiencing an ambiguous informational impact, the consequences of which do not always have a favorable effect on the efficiency of the service, and sometimes on the professional and social image of civil servants. Currently, the information support of the civil service needs to be improved, especially with regard to information exchange issues in the civil service system in general and in particular. In addition, the administrative and legal mechanism of information exchange between various types of public service, as well as between the public civil service and the municipal service, needs to be improved.

According to experts, the most important process of information globalization is informatization as an organizational socio-economic, scientific and technical process of creating optimal conditions for meeting information needs and realizing the rights of citizens, public authorities, local governments, organizations, public associations based on the formation and use of information resources [14, 15, 20, 24].

The changes taking place in the information sphere, on the one hand, cause the transition to uniform standards; on the other hand, they are characterized by the erection of new barriers associated with ensuring the safety of the individual, society, and the state as a whole.

The information security of society and the state is determined by the degree of their defence and, consequently, the stability of the main spheres of life in relation to dangerous, destabilizing, destructive information influences that infringe on the interests of the country at the level of both implementation and the level of extraction of information.

In connection with the above, the methodological basis of the study is the doctrinal foundations of information security, management theory [32-34]. The use of the descriptive-comparative method allows studying and comparing the various views of researchers, whereby it is possible to justify their own positions and views. In the course of the research, general scientific methods were also actively used - analysis, synthesis, deduction, generalization, analogy, etc [36-38]. The use of the comparative historical method made it possible to identify the general and specific in approaches to the study of information security issues. In the process of studying the policy of foreign states in the field of legal regulation of information security, the structural and functional analysis of the system approach was used.

3 Results

Information security is determined by the following abilities of the state (society, individual):

- To provide, with a certain probability, sufficient and protected information resources and information flows to maintain their life and vitality, sustainable functioning and development;
- To resist informational dangers and threats, negative informational influences on the individual and public consciousness and psyche of people, as well as on computer networks and other technical sources of information [39];
- To develop personal and group skills and skills of safe behavior;
- To maintain a constant readiness for adequate measures in information confrontation, no matter who imposed it.

Not a single sphere of life in modern society can function without a developed information structure. The national information resource is today one of the main sources of the state's economic and military power [42-44]. Penetrating into all spheres of state activity, information acquires a specific political, material, and value expression. Against this background, the issues of ensuring national information security as an integral element of national security are becoming increasingly more relevant, and information protection is turning into one of the priority state tasks [14].

An important area of improving the legal sphere of ensuring information security is the organization of activities to generalize law enforcement practice in this area.

In such circumstances, the competence of civil servants in the field of information security becomes critically important.

One of the necessary qualities of an employee during the period of digitalization in all spheres of activity, including the civil service, is the skill of working with information as a specific subject of labor. In this regard, the question of whether civil servants have skills to work with information in a digital environment, “the ability to use digital technologies, communication tools and/or networks to gain access to information, manage it, integrate, evaluate, create and transmit information in compliance with ethical and legal norms in order to successfully live and work in a knowledge society” [16, p. 37].

It is advisable to note that the development of legal regulation and harmonization of relevant standards for ensuring information security, including the security of information technology, in the European Union began to develop relatively long ago; therefore, it has a fairly systemic and thorough character. In addition, the regulation of information security in the EU is clearer and more structured: first of all, the basic concepts and categories are clearly defined, a list of relevant threats to information security has been presented, for example, personal data of a person and the like.

Since the beginning of active discussions in the mid-1990s about the development of the information society in the European Union, the issue of emerging risks and threats has certainly been raised, which has led to the development of appropriate political and legal instruments to counter these risks and threats. Constant attention was paid to the issues of ensuring the security of the information society [46, 47]. The active activity of the EU institutions in this area was carried out primarily within the framework of the first (European Community) and third pillars (cooperation between the police and courts in the criminal sphere). In connection with the entry into force of the Lisbon Treaty on December 1, 2009, the system of three pillars was eliminated and the European Community was abolished; the full successor of it was the European Union [31]. Further development of EU legislation in the field of information security is carried out within the framework of the unified system of EU legal regulation.

An important stage in the development of European policy in the field of network and information security was the adoption of the European Commission Communication “Security Strategy for the Information Society: Dialogue, Partnership and Empowerment” in 2006 [22]. This Strategy accumulates an overview of the current state of threats to the security of the information society and highlights additional measures to ensure network and information security. The section “Key Threats” of this Strategy notes the fact that despite all efforts, both at the international, regional and national levels, increasingly more new security challenges arise, including attacks on information systems for mercenary purposes, active distribution of malicious software, spyware viruses. Within the framework of this Strategy, the Commission also focused on the growth of the use of mobile devices and network mobile services as potential targets of cyber attacks [49-52]. The document rightly notes that any form of new means of communication and information systems will inevitably create new opportunities for various types of malicious attacks.

In the EU, the practice of organizing the activities of state authorities in the external and internal information environment demonstrates the existing technology in the prevention of information risks and incidents. The implemented measures are aimed at the formation of a complex of knowledge, skills, behavioral stereotypes of civil servants as those among the most important factors in ensuring information security [55].

Germany legislation is characterized by a detailed development of a system of various types of information with limited access, clear formulations of their definitions in federal legislation. In particular, according to the Law “On Security Verification”, the secret information system includes state secrets (information marked “top secret” and “secret”) and departmental secrets (information marked “confidential” and “for official use”), the protection of which, unlike other types of secrets concerning the confidential sphere of individuals, is due to the interests of the external security of the state. Confidential information is considered especially important and subject to special protection. The leading role in ensuring information security in Germany is played by the Federal Information Security Service (BSI). According to the Law “On the Federal Office for Information Systems Security”, BSI collects and evaluates information regarding cybersecurity threats of the state, detects new types of cyberattacks, analyzes the appropriate countermeasures [45]. Also, BSI, in cooperation with NATO and the EU, is responsible for the following functions: risk assessment of the introduction of information technologies; development of criteria, methods and test tools for assessing the degree of security of national telecommunication systems; checking the degree of security of information systems and issuing appropriate certificates; issuance of permits for the implementation of information systems in important state facilities; implementation of special security measures for information exchange; propaganda of the need to ensure information security [45]. In early 2011, Germany adopted a new Federal Cyber Security Strategy, which outlines the following main areas of cybersecurity: 1) The main priority of cybersecurity is the protection of critical information structures and ensuring cooperation defined by the CIP; 2) IT security in Germany is carried out on the basis of joint activities of society and the state based on the correlation of threats and measures [45]. The National Cyber Response Center optimizes operational collaboration between all government agencies and improves the coordination of security and IT incident response.

As we can see from the above, in order to achieve the goal of ensuring information security in any sphere of public life, a clear and well-coordinated functioning of the subject of ensuring such security, which is endowed with exclusively specialized powers, is necessary. It is a specialized body (department, institution, enterprise) that can most effectively observe information security, since it accumulates special experience, improves the educational, technical, material, practical basis, as well as the knowledge and competence from interaction with other subjects of legal relations in the state and subjects of international law [56-59]. Also, using the example of Germany, it is clearly possible to determine that the proper basis for the further effective functioning of the administrative and legal mechanism for ensuring information security in the state is, first of all, effective and high-quality legal regulation, implemented by highly qualified civil servants.

In Poland, the national information policy is focused on building a free open society, introducing the concept of free cross-border circulation of information, ensuring human rights. The Homeland Security Agency (ABW) plays a key role in cyber security. In 2013, ABW developed the Cybersecurity Strategy of Poland and initiated the creation of the Cryptology Center under the Ministry of National Defense, which is tasked with information protection, cyber defense and offensive cyber operations [40]. ABW has also established a Government Computer Incident Response Team (CERT), whose main task is to ensure and develop the capabilities of governments to protect against cyber threats, in particular, from attacks on infrastructure consisting of IT systems and computer networks, or those the destruction of which could significantly threaten the life and health of people, national wealth [40].

In 2008, Estonia, for the first time among the members of the European Union, published a national cybersecurity strategy [45]. Since the indicated time, the phenomenon has acquired an avalanche-like character – the Strategies are adopted by most of the EU countries, and some specific features are reflected in the national strategies. Specifically, the Swedish Government has commissioned the Agency for Civil Protection and Preparedness MSB to administer the national cyber security action plan, which was drawn up in 2008 and updated in 2010. The plan is based on the national security information strategy and was created in collaboration with a number of other authorities and organizations in this area. Four main areas have been identified as priorities [41]:

- The need to improve multisectoral and intersectoral work on social information and security. Comprehensive information security rules can be designed in such a way as to apply them in all instances under government control;
- A basic level of security for the security of public information should be created, which is a prerequisite for the provision of information resources, that are increasingly becoming fundamental for the trade and public sector; society must be able to process the vast amount of information related to IT riots and crises [60, 61]. At the same time, operational national coordination functions should be established;
- There is a lack of expertise on information security at all levels of society.

In 2016, the European authorities agreed to introduce the Network and Information Security (NIS) Directive in the field of information security, which will be valid in all EU countries after formal approval by the European Parliament and the European Council. The directive sets requirements for all members of the European Union. Each country's government is obliged to comply with its requirements and establish its own Computer Security Incident Response (CERT) and Directive Compliance Center in each State. In addition, according to the directive, a single coordination center for information security will be created in the European Union, which will serve as a platform for interaction between EU members. The leadership of this center will be appointed by the European Commission [21].

The innovation is due to the need to prevent incidents in the field of information security, affecting computer networks, servers, storage systems and network nodes, on the proper functioning of which people's lives depend. At the same time, according to government officials, protection must be provided not only from hacker attacks, but also from technical problems, human errors, and natural disasters. Given the growing number of incidents and the role of information systems in the life of modern society, these measures have become urgent [21].

In general, in the EU, qualification requirements for information security are formed for several target groups of civil servants (depending on the degree of their involvement in the processes of information security provision, for example, information security specialists, IT specialists, managers of all levels, all other civil servants).

In the European Union, efforts to develop information security skills are systemic in nature and are being implemented sequentially: from defining a competency model, developing training programs to creating a toolkit for assessing competencies, including self-assessment [9, 41]. A modern civil servant of any level must be ready every hour, every minute for a situation of mobile, competent response to requests from citizens and organizations, which presupposes professionalism and a high level of information competence. The insufficient level of information competence of civil servants becomes a natural reason for the inefficiency of the civil service in terms of the interaction of this institution with citizens, the slow pace of change in the existing bureaucratized management style, and the lack of a system for providing public services to citizens as one of the results of administrative reforms. The efficiency of the ongoing administrative reforms and the optimization of administrative processes in this regard, the development of democracy and the formation of civil society also directly depend on the increase in the level of information competence of civil servants.

In the EU, an acmeological concept for the development of information technology competence of civil servants has been developed, which gives a holistic picture of a comprehensive solution to the problem of integrating science and practice in the field of improving professionalism and optimizing the work of civil service personnel in the context of universal informatization [48]. The acmeological concept of the development of information technology competence of civil servants is of a general nature and is meaningfully a system of views on the subject of research, mechanisms for the development of this type of competence, as well as a system of ideas about the ways and methods of optimizing the process of this development. It expresses a conceptual scheme for the synthesis of theoretical, methodological, and applied foundations and combines a number of interrelated components [48]. In accordance with this concept, effective information technology training of a civil servant is based on a three-component model for the development of information technology competence, including the following: motives, integrated knowledge, skills in computer science, as well as skills in using new information technologies in their professional activities, understanding all potential cybersecurity threats and ways to eliminate them.

4 Discussion

The acmeological model of the development of information technology competence of civil servants reflects the conceptual scheme of the pedagogical system, in which the interaction of the teacher and the student is carried out through technical means of communication. It provides for the integration of the developed theoretical provisions and conclusions into an integral system of ideas about the productive development of information technology competence of students. The model includes interrelated theoretical, technological, and procedural components. This made it possible to implement an iterative and technological approach to the personal and professional development of the information technology competence of civil servants. The model is innovative, as it reflects the process of qualitative changes in the development of a person as a subject of the process of informatization of public administration, thanks to which he acquires the ability to achieve higher personal and professional results. The model contains the stages of productive development of information technology competence: problem-oriented analysis, design of a reference state, planning of changes, implementation of changes. The acmeological system for the development of information technology competence of civil servants is presented in accordance with the model of its productive development, which includes the following content directions: motivational, general psychological, pedagogical, in particular, didactic.

The principles of the construction and functioning of the acmeological system for the development of information technology competence of civil servants in the EU as an open system functioning under conditions of intensive informatization of state power (principles of dynamic balance, structural stability, feedback) have been determined. A normative model of the subject area has been developed, built on the basis of coordinating the factors of the objective necessity of the civil service in the use of a number of information technologies, the subjective need of civil servants in the development and use of information technologies in their professional activities and a real opportunity to master and use these technologies. The necessary psychological-pedagogical and information-technological conditions for building an acmeological developmental environment have been substantiated [53]:

- Organization of a didactically oriented system of distance interaction to higher levels of development of information competence, both vertically (teacher - trainee) and horizontally (between trainees of the same level) (mode of demonstration of elements of “correct” activity, direct transition from informing and demonstrations for self-repetition of actions by trainees, built-in diagnostic systems, the use of screen animation and multimedia, the creation of electronic textbooks, information and control materials for distance learning, simulation models of situational management processes);
- The presence of pedagogical and developmental technologies based on the joint use of a modular approach and the theory of the stage-by-stage formation of mental actions with the maximum possible consideration of the individual-personal, status, age and professional characteristics of civil servants for the implementation of their individual trajectory of development;
- Availability of organizational and methodological support corresponding to the peculiarities of informatization of the student's activity (scenario approach to the organization of educational tasks for working out certain elements of professional activity, the development of specially organized “end-to-end” educational tasks to combine meaningfully related elements and types of professional activity);
- Structuring of educational data, aimed at the gradual complication and variability of educational tasks (modularity in the organization of educational material, which involves not so much the fragmentation of the content, but rather the allocation of elements and connections of the studied system of professional activity, the most significant for the result of this activity).

When determining the qualification requirements for civil servants in the field of information security, as the basis for creating an assessment toolkit, the features of the activities of employees and the levels of responsibility in their positions are taken into account. In addition, the assessed knowledge, skills and abilities should reflect the current trends in digitalization as a promising area for the development of competencies.

5 Conclusion

In conclusion, it is important to note that the algorithms being introduced today that formalize the decision-making process in the selection and recruitment of a candidate for a civil servant position, including with the involvement of neural networks and artificial intelligence capabilities, will transfer the process of standard recruiting from conducting an interview that gives a subjective assessment, to an objectively compiled map of applicants with a rating of their best qualities and characteristics, including in relation to competence in the field of information security.

The same competency map can become a good tool for motivating an employee for professional development, and most importantly, for constantly monitoring the competencies of civil servants, selecting employees who have shown the best results in the talent pool, to create their individual development plan and develop training and advanced training programs in the information (cyber) security. An integrated technological system for the development of information and technological competence of civil servants has been introduced in EU, which is the basis for continuous education, distance learning, diagnostics of the state, simulation of real management activities, and developmental trainings in various areas.

Literature:

1. Akimova, L., Akimov, O., & Liakhovich, O. (2017). State regulation of foreign economic activity. *Scientific Bulletin of Polissia,* 4(12), P. 1, 98-103. DOI: 10.25140/2410-9576-2017-1-4(12)-98-103.
2. Akimova, L., Akimov, O., Mihus, I., Koval, Y., & Dmitrenko, V. (2020). Improvement of the methodological approach to assessing the impact of public governance on ensuring the economic security of the state. *Financial and Credit Activity-Problems of Theory and Practice*, 4(35), 180-190. DOI: https://doi.org/10.18371/fcaptp.v4i35.221969.
3. Akimova, L., Levytska, S., Pavlov, C., Kupchak, V., & Karpa, M. (2019). The role of accounting in providing sustainable development and national safety of Ukraine. *Financial and credit activity: problems of theory and practice,* 30 (3), 64-70. DOI: 10.18371/FCAPTP.V3I30.179501.

4. Akimova, L., Osadcha, O., & Akimov, O. (2018). Improving accounting management via benchmarking technology. *Financial and Credit Activity-Problems of Theory and Practice,* 1(24), 64-70. DOI: 10.18371/FCAPTP.V1I24.1 28340.

5. Akimova, L., Osadcha, O., Bashtannyk, V., Kondratska, N., & Fedyna, C. (2020). Formation of the system of financial-information support of environmentally-oriented management of the enterprise. *Financial and credit activity: problems of theory and practice,* 32(1), 434–443. DOI: 10.18371/FCAPTP.V1I32. 200606.

6. Akimova, L., Reinska, V., Akimov, O., & Karpa, M. (2018). Tax preferences and their influence on the investment in Ukraine. *Financial and Credit Activity-Problems of Theory and Practice,* 3(26), 91-101. DOI: 10.18371/FCAPTP.V3I26.144117.

7. Akimova, N., & Akimova, Al. (2018). Text Understanding as a Special Kind of Understanding. *Psycholinguistics,* 24(1), 27-46. DOI: https://doi.org/10.31470/2309-1797-2018-24-1-27-46.

8. Andros, S., Akimova, L., & Butkevich, O. (2020). Innovations in management of banks deposit portfolio: structure of customer deposit. *Marketing and Management of Innovations,* 2, 206-220. DOI: 10.21272/MMI.2020.2-15.

9. Bannykh, G., & Kostina, S. (2021). Formation of Digital Competence of State Servants in the Conditions of Government Digitalisation: The Problem Statement. *KnE Social Sciences*. XXIII International Conference Culture, Personality, Society in the Conditions of Digitalization: Methodology and Experience of Empirical Research Conference Volume 2020. DOI: http://dx. doi.org/10.18502/kss.v5i2.8357.

10. Bashtannyk, A., Akimova, L., Kveliashvili, I., Yevdokymov, V., Kotviakovskyi, Y., & Akimov, O. (2021). Legal bases and features of public administration in the budget sphere in Ukraine and foreign countries. *Ad Alta: Journal of interdisciplinary research*, 1(1), XVIII, 63-68.

11. Bilan, S., Mishchuk, H., Bilan, Y., & Mishchuk, V. (2019). *Empirical Study of Migration Caused by Well-being in Living and Working Environment.* Paper presented at the Proceedings of the 34th International Business Information Management Association Conference, IBIMA 2020: Vision 2025: Education Excellence and Management of Innovations through Sustainable Economic Competitive Advantage, 11159-11169.

12. Bilan, S., Mishchuk, H., Samoliuk, N., & Ostasz, G. (2019). *Effectiveness of Social Dialogue in the System of Sustainable Economic Development Factors.* Paper presented at the Proceedings of the 34th International Business Information Management Association Conference, IBIMA 2020: Vision 2025: Education Excellence and Management of Innovations through Sustainable Economic Competitive Advantage, 13303-13313.

13. Bobrovska O.Y., Lysachok A.V., Kravchenko T.A., Akimova LM., & Akimov O.O. (2021). The current state of investment security in Ukraine in the context of covid-19 and its impact on the financial and economic situation of the state. *Collection of scientific papers Financial and Credit Activity-Problems of Theory and Practice,* 1(36), 233-242. DOI: 10.18371/FCAPTP.V1I36.227770.

14. Bodrunov, S., Plotnikov, V., &Vertakova, Y. (2017). *Technological Development as a Factor of Ensuring the National Security.* In: Proceedings of the 30th International Business Information Management Association Conference. Vision 2020: Sustainable Economic development, Innovation Management, and Global Growth, Madrid, Spain, 2666-2674.

15. Christou, G. (2016). *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. Palgrave Macmillan.

16. Clarker, R., & Knake, R. (2011). *Cyber War: The Next Threat to National Security and What to Do About It*. Ecco.

17. Committee on National Security Systems (2015). *National Information Assurance*. CreateSpace Independent Publishing Platform.

18. Denysov, O., Litvin, N., Lotariev, A., Yegorova-Gudkova, T., Akimova, L., & Akimov, O. (2021) Management of state financial policy in the context of the Covid-19 pandemic. *Ad Alta: Journal of interdisciplinary research,* 11(2), XX, 52-57.

19. European Commission. (2018). *State of Union 2018: Building strong cybersecurity in Europe (P.1)*. Available at: https://ec.europa.eu/commission/sites/beta-political/files/soteu2 018-factsheet- cybersecurity_en.pdf.

20. GAO. (2013). *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*. Available at: https://www.gao.gov/assets/660/ 652170.pdf 2013.

21. Gary, S. (2018). *Understanding Cybersecurity: Emerging Governance and Strategy*. Rowman & Littlefield Publishers.

22. Giantas, D., & Liaropoulos, A. (2019). *Cybersecurity in the EU: Threats, frameworks and future perspectives*. Laboratory of Intelligence and Cyber-Security, Working Paper Series No. 1.

23. Harafonova, O., Zhosan, G., & Akimova, L. (2017) The substantiation of the strategy of social responsibility of the enterprise with the aim of providing efficiency of its activities. *Marketing and Management of Innovations,* 3, 267 – 279. DOI: 10.21272/MMI.2017.3-25.

24. Helmbrecht, U., Purser, S., & Ritter Klejn, M. (2012). *Cyber Security: Future Challenges and Opportunities*. ENISA.

25. HM Government. (2020). *Initial National Cybersecurity Skills Strategy*. Available at: https://assets.publishing.service.go v.uk/government/uploads/system/uploads/attachment_data/file/9 49209/Cyber_security_skills_strategy_executive-summary_21 1218_V2.pdf.

26. Isaieva, N., Akimova, Al., & Akimova, A. (2020). Categorization of Personality Traumatic Experience in Chinese Women's Diary Narrative: The Frame-Scenario Model. *Psycholinguistics,* 28(2), 56-81. DOI: 10.31470/2309-1797-2020-28-2-56-81.

27. Kalyayev, A., Efimov, G., Motornyy, V., Dzianyy, R. & Akimova, L. (2019). *Global Security Governance: Conceptual Approaches and Practical Imperatives.* Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020, 10-11 April 2019, Spain, Granada, 4484-4495.

28. Karpa, M., Akimova, L., Akimov, O., Serohina, N., Oleshko, O., & Lipovska, N. (2021). Public administration as a systemic phenomenon in society. *Ad Alta: Journal of interdisciplinary research*, 11(1), XV, 56-62.

29. Kitsios, F., et al. (2018). *National Cybersecurity Strategy: A Conceptual Framework for Greece.* Proceedings of 11th International Conference for Entrepreneurship, Innovation and Regional Development (ICEIRD 2018) At: Doha, Qatar.

30. Kostiukevych, R., Mishchuk, H., Zhidebekkyzy, A., Nakonieczny, J., & Akimov, O. (2020). The impact of European integration processes on the investment potential and institutional maturity of rural communities. *Economics and Sociology*, 13(3), 46-63. DOI:10.14254/2071-789X.2020/13-3/3.

31. Kovacs, L. (2018). Cyber Security Policy and Strategy in the European Union and NATO. *Land Forces Academy Review,* 23(1), 16-24.

32. Levytska, S., Krynychnay, I., Akimova, A., & Kuzmin, O. (2018). Analysis of business entities' financial and operational performance under sustainable development *Financial and credit activity: problems of theory and practice*, 25(2), 122–127. DOI: 10.18371/FCAPTP.V2I25.136476.

33. Levytska, S.O., Akimova, L.M., Zaiachkivska, O.V., Karpa, M.I., & Gupta, S.K. (2020). Modern analytical instruments for controlling the enterprise financial performance. *Financial and Credit Activity-Problems of Theory and Practice*, 2(33), 314-323. DOI: 10.18371/FCAPTP.V2I33.206967.

34. Liubkina, O., Murovana, T., Magomedova, A., Siskos, E., & Akimova, L. (2019). Financial instruments of stimulating innovative activities of enterprises and its improvements. *Marketing and Management of Innovations,* 4, 336-352. DOI: 10.21272/MMI.2019.4-26.

35. Lopez, J., Setola, R., & Wolthusen, S. (2012). *Critical Infrastructure Protection: Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense*. Springer.

36. Lyulyov, O., Pimonenko, T., Kwilinski, A., Us, Y., Arefieva, O., Akimov, O., & Pudryk, D. (2020). Government Policy on Macroeconomic Stability: Case for Low-and Middle-Income Economies. *Proceedings of the 36th International Business Information Management Association (IBIMA)*. ISBN:

978-0-9998551-5-7. Dated on November, 4-5, 2020. Granada, Spain, 8087-8101.

37. Marchenko, A., Akimova, L., & Akimov O. (2021) The current state of ensuring the effectiveness of coordination of anticorruption reform. *Ad Alta: Journal of interdisciplinary research*, 11(2), XX, 78-83.

38. Mihus, I., Denysenko, M., Rumyk, I., Pletenetska, S., Laptiev, M., & Kupriichuk, V. (2021) Methodology of corporate financial diagnostics in the period of a crisis. *Ad Alta: Journal of interdisciplinary research*, 11(1), XV, 52-55.

39. Mihus, I., Laptev, S., Parashchenko, L., Koval, Ya., Odarchyk, K., & Panchenko, O. (2021). The impact of the covid-19 pandemic on the loyalty of employees. *Ad Alta: Journal of interdisciplinary research*, 11(1), XVII, 38-41.

40. Ministry of Digital Affairs. (2017). *National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022.* Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/govermental-program-for-protection-of-cyberspace-for-the- years-2011-2016-2013.

41. Ministry of Finance Finland. (2016). *Competence required by digitalization – The way the Finnish government looks at it.* Competence model presented by Marjaana Laine at the EUPAN Working Level meeting on 8-9 April 2019, Focsani, Romania. Available at: https://www.innokyla.fi/documents/3575377/8c10fd f2-4be1-4c89-9dcd-5c18cb48e303.

42. Mishchuk, H., Bilan, S., Yurchyk, H., Akimova, L., & Navickas, M. (2020). Impact of the shadow economy on social safety: The experience of Ukraine. *Economics and Sociology,* 13(2), 289-303. DOI:10.14254/2071-789X.2020/13-2/19.

43. Mordvinov, O., Kravchenko, T., Vahonova, O., Bolduiev, M., Romaniuk, N., & Akimov, O. (2021). Innovative tools for public management of the development of territorial communities. *Ad Alta: Journal of interdisciplinary research*, 11(1), XVII, 33-37.

44. National Research Council. (2014). *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. *National Academies Press.*

45. OECD *(2010). Managing Competencies in Government: State of the Art Practices and Issues at Stake for the Future.* Available at: https://www.oecd.org/gov/pem/paper-managing-competencies-in-government-state-of-the-art-practices-and-issues.pdf.

46. Oliinyk, O., Bilan, Y., Mishchuk, H., Akimov, O., & Vasa, L. (2021). The Impact of Migration of Highly Skilled Workers on The Country's Competitiveness and Economic Growth. *Montenegrin Journal of Economics*, 17, 3, 7-19. DOI: 10.14254/1800-5845/2021.17-3.1.

47. Osadcha, O.O., Akimova, A.O., Hbur, Z.V., & Krylova, I.I. (2018). Implementation of accounting processes as an alternative method for organizing accounting. *Financial and credit activity: problems of theory and practice,* 27(4), 193–200. DOI: 10.18371/FCAPTP.V4I27.154194.

48. Pantiru, M. (2019). *Competencies necessary for eGovernment*. National Agency of Civil Servants, Romania.

49. Shpektorenko, I., Vasylevska, T., Bashtannyk, A., Piatkivskyi, R., Palamarchuk, T., & Akimov, O. (2021). Legal bases of public administration in the context of European integration of Ukraine: questions of formation of a personnel reserve. *Ad Alta: Journal of interdisciplinary research*, 11(1), XVIII, 76-81.

50. Smyrnova, I., Akimov, O., Krasivskyy, O., Shykerynets, V., Kurovska, I., Hrusheva, A., & Babych, A. (2021). Analysis of The Application of Information and Innovation Experience in The Training of Public Administration Specialists. *IJCSNS International Journal of Computer Science and Network Security,* 21, 3, March 2021, 120-126.

51. Sysoieva, I., Poznyakovska, N., Balaziuk, O., Miklukha, O., Akimova, L., & Pohrishchuk, B. (2021). Social innovations in the educational space as a driver of economic development of modern society. *Financial and Credit Activity: Problems of Theory and Practice, 3*(38), 538–548. DOI: https://doi.org/10.18371/fcaptp.v3i38.237486.

52. Uygun, S.V., & Gupta, S.K. (2020). Leadership and accountability for social development: intellectual leadership and rectors. *International Journal of Indian Culture and Business Management*, 21(2), 171-180. DOI: 10.1504 / IJICBM.2020.109750.

53. Van Puyvelde, D., & Brantly, A. (2017). *US National Cybersecurity: International Politics, Concepts and Organization*. Routledge.

54. Vasilieva, E. V., Pulyaeva, V. N. and Yudina, V. A. (2018). Development of digital competencies of state civil servants of the Russian Federation. *Business Informatics,* 4(46), 28-42.

55. Vasylovych, Z., et al. (2021). Legal basis for ethical behavior of civil servants in Ukraine: some problematic issues. *Cuestiones Politicas*, 39(68), 882-895.

56. Vorobei, O., Akimova, A., & Akimova, A. (2021). Metaphorical Conceptualization of WAR in Chinese Sports Discourse. *Psycholinguistics*, 29(2), 25-45. DOI: https://doi.org/10.31470/2309-1797-2021-29-2-25-45.

57. Yakymchuk, A.Y., Valyukh, A.M., & Akimova, L.M. (2017). Regional innovation economy: aspects of economic development. *Scientific Bulletin of Polissia*, 3(11), P.1, 170-178. DOI: 10.25140/2410-9576-2017-1-3(11)-170-178.

58. Yakymchuk, A.Y., Akimova, L. M., & Simchuk, T.O. (2017) Applied project approach in the national economy: practical aspects. *Scientific Bulletin of Polissia*, 2(10), P.2, 170-177. doi: 10.25140/2410-9576-2017-2-2(10)-170-177.

59. Yakymchuк, A.Y., Akimov, O.O., & Semenova, Y.M. (2017). Investigating key trends of water resources attraction into economic turnover. *Scientific Bulletin of Polissia,* 1(9), P.2, 70-75. DOI: 10.25140/2410-9576-2017-2-1(9)-70-75.

60. Zahorskyi, V., Lipentsev, A., Mazii, N., Bashtannyk, V., & Akimov, O. (2020). Strategic directions of state assistance to enterprises development in Ukraine: managerial and financial aspects. *Financial and Credit Activity-Problems of Theory and Practice,* 2(33), 452-462. DOI: https://doi.org/10.18371/fcaptp.v2i33.207230.

61. Zahorskyi, V.S., Lipentsev, A.V., Yurystovska, N.Ya., Mazii, N.H., & Akimov, O.O. (2019). Financial and administrative aspects of small business development in Ukraine. *Financial and Credit Activity-Problems of Theory and Practice*, 3(30), 351-360. DOI: https://doi.org/10.18371/fcaptp.v3i30.179717.

Primary Paper Section: A

Secondary Paper Section: AE, AD, AG