LEGAL ISSUES OF INFORMATION SECURITY OF PUBLIC AUTHORITIES IN UKRAINE AND THE EUROPEAN UNION: EXPERIENCE AND REALITIES

[a]VUSAL AHMADOV, [b]NATALIIA KLIETSOVA,
[c]KONSTANTIN BIELIAKOV, [d]ALYONA KLOCHKO,
[e]TATIANA KRAVTSOVA

[a]Academy of Justice at the Ministry of Justice, 158, Vidadi Str., Nasimi district, AZ 1000, Baku, Azerbaijan Republic
[b,d,e]Sumy National Agrarian University, 160, Gerasim Kondratyev Str., 40000, Sumy, Ukraine
[c]Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine, 3, Philip Orlik Str., 01024, Kyiv, Ukraine
email: [a]vusal-ahmadov1@mail.ru,
[b]klietsovanataliia2@gmail.com, [c]kiberg1@ukr.net,
[d]alenaklocko2@gmail.com, [e]tatiana_kr1@meta.ua

Abstract: The topic of information security of public administration, and, in particular, of public authorities, is relevant all over the world. Modern public administration becomes vulnerable without ensuring an adequate level of information security on a par with the level of military equipment. The article shows that the high rates of the formation of the global information space and the informatization of all spheres of society's life have created the prerequisites for the intensive use of the information sphere for the implementation of public administration, and at the same time for the emergence of new threats to the information security of states. The steady growth of these threats necessitates the improvement of doctrinal approaches to ensuring national security in the information sphere, in particular, in the field of legal support. Generalization of the practice of creating a system of legal regulation of information security and scientific and practical research of the problems arising in this area showed numerous shortcomings associated with the lack of sufficient theoretical foundations of legal support for information security.

Keywords: Cyber threat, European Union, Information security, Public authorities, Ukraine.

1 Introduction

One of the most important factors determining the development of modern society is the ongoing information revolution, thanks to which the possibilities of realizing the human right to freedom of information activity have significantly expanded. New social relations are emerging, the objects of which are information and information infrastructure, and, as a consequence, conditions arise for the transition of society to a new, post-industrial phase of its development, often called the information society.

There have been qualitative changes in the content of national interests, which are largely associated with the active participation of Ukraine in the formation of the information society, with the development of modern information technologies and their use to ensure sustainable economic growth, increase public welfare, maintain national harmony, strengthen democracy and stability. The protection of these interests from threats increasingly determines the content of national and international information security.

In the face of global challenges, the main strategic national resource that determines the economic and defense power of the state is information and information technology, on which all spheres of life of Ukrainian society depend decisively: production and management, defense and energy, transport and communications, banking and finance, science, education, and many others [1-7]. At the same time, insufficient security of information resources leads to the leakage of the most important political, economic, scientific, and military information.

2 Literature Review

The need to improve the organization of the work of executive authorities to implement the main directions of domestic and foreign policy of the state, the steady increase in the needs of government bodies for objective, reliable and timely information about the real state of affairs in a particular industry, sector of the economy, region, city, enterprise, determines updating the processes of informatization in the field of public administration [22-24].

The urgency of the problem of ensuring the security of information in the structures of executive authorities is due, in addition, to the need to make effective, adequate to political tasks, management decisions. First, we note that dependence on information and information technology is becoming one of the qualitative conditions of the emerging society [9-13, 16, 35]. Possession of timely, accurate, reliable data is an extremely important factor in the effectiveness of managerial decision-making both at the state level and at the level of regions. Information becomes a strategic value of both the state and any administrative structure in the system of political administration. Ultimately, the quality of functioning and security of the information sphere, as well as the state of legal regulation of relations in this area, determine the level of development of the state. As a strategic resource, information requires a special state attitude, not only in terms of its development and accumulation, but also protection.

Provision of information security is associated with issues of ensuring the technological security of the country. It is also of significant interest to consider the problem of the correlation between the capabilities of protective equipment and means of unauthorized collection, processing and access to information resources, the availability of protocols for the interaction of users and information, taking into account the degree of its importance and secrecy, the state of the socio-economic and socio-political situation in the country and its subjects [26-28]. All this taken together, as well as the scientific search for comprehensive measures, means and methods for improving the information security system of political structures, increasing the management potential, mainly of national and regional executive authorities, determines a high degree of relevance of the study.

The development of the concept of an information security system for public authorities is aimed at increasing the efficiency of public authorities, protecting the interests of Ukraine, as well as protecting public authorities from unauthorized access to available information resources.

At the same time, information security of public authorities will contribute to the achievement of the following results [8, 46]:

- An increase in citizens' confidence in electronic services, which are provided on the portals of state bodies of Ukraine;
- Strengthening state guarantees of privacy when using information and telecommunication technologies;
- Strengthening cooperation between civil society, business and the state in various fields (including the use of electronic technologies);
- Information support of citizens' participation in state governance;
- Development and implementation of information technologies in government bodies; development of communication services and information processing provided to citizens and organizations; ensuring the protection of national interests in the information sphere from internal and external threats.

It should be noted that the formation of the information security system of public authorities in Ukraine should be based on the international experience of other countries, and, therefore, a comparative analysis of the situation in the field of legal support of information security of public authorities in Ukraine and the European Union, the appropriate experience and best practices seems to be highly relevant.

3 Materials and Methods

Informatization in all spheres of activity in Ukraine on the basis of the wide use of software and hardware of foreign production, in the absence of a unified centralized methodology for building departmental and territorial information and communication

systems, led to the uncontrolled creation and duplication of information resources, the emergence of many hard-to-detect access points to them [30-33]. These circumstances, in the conditions of well-developed technical means of reconnaissance and wide opportunities for their practical official use, as well as the low quality of existing means of protection, led to the emergence of a wide range of threats, the formation of unconventional technical and other channels of information leakage, as well as methods of unauthorized access to it.

Some implications of historical and comparative methods are used. The theoretical basis of the research is represented by the general theory of national security, information theory, security theory, theoretical developments of domestic and foreign scientists in the field of information, information technology and information security.

The methodological basis of the study is a system of both general scientific and special research methods of socio-political, legal and other humanitarian problems.

4 Results

According to the Doctrine of Information Security of Ukraine (hereinafter – the Doctrine), information security is an independent sphere of ensuring the national security of Ukraine and at the same time an integral component of each of its spheres. The main goal of the Doctrine is to create a developed national information space in Ukraine and protect its information sovereignty.

Recently, the term “cyber warfare” has been appearing increasingly more often in the national information space. The confrontation in the Internet space is becoming a constant companion of other, “earthly” hotbeds of tension [36, 37, 50]. The weak relevance of the defense doctrine, as well as the lack of real steps to implement the doctrine of information security of Ukraine, make the state vulnerable to cyber threats. Despite the presence of appropriate units to counteract them in individual law enforcement agencies, objective factors are gradually shaping private and public initiative in this area.

With the development of the Internet of Things, according to futurological research by Cisco Systems, we will gradually move to the Internet of Everything the inclusion of people, processes, data and things in a single network. In practice, this will mean dependence on the Network of all spheres of human life. A threat in such a network can be a direct threat to both a specific individual and groups of people. So far, cybercriminals are trying to ‘solve’ this problem with the help of existing cyberwar technologies, the main purpose of which is to disable the computer systems of government bodies and critical infrastructure facilities [25, 29].

Within the framework of the list of threats in modern cyberwar, which does not claim to be complete and consistent, the following can be distinguished [42]:

- Vandalism in relation to information resources with the aim of misinforming the audience and discrediting, incl. public authorities;
- Propaganda using fictitious social media accounts and news resources;
- Hacking of information systems and accounts in public services in order to steal sensitive information (both personal data and data from state information resources);
- Denial of Service (DoS/DDoS) attacks on public resources, in particular news sites, government portals, payment systems, telecommunications infrastructure nodes;
- Targeted attacks aimed at disabling information systems of critical infrastructure facilities and, as a result, disrupting their operation (energy facilities, housing and communal services, oil and gas pipelines, etc.).

Most of the threats are not new for Ukraine; they are being fought with varying degrees of effectiveness. However, one thing is clear: there is no unified policy to counteract them at the state level.

A natural question arises: how has the protection of state information resources been carried out so far? The only mechanism for ensuring their security, determined by the domestic regulatory and legal framework, is an integrated information protection system (hereinafter referred to as IIPS) an interconnected set of organizational and engineering measures, means and methods of information protection.

The criteria for assessing the security of information and telecommunication systems, as well as other fundamental regulatory documents in this area, date back to the end of the 90s. It is quite natural that the typical models of threats developed within the framework of such IIPS are not even close to the ones listed above. IIPS is increasingly becoming the product of some kind of creative work of the developer, directly dependent on the skill of the latter. After all, while the requirements for the design of a set of accompanying documentation are more or less defined (is it worth mentioning that often “paper” work makes up the lion's share of the work on the creation of IIPS), the physical content in the form of various means of protection, not to mention their configuration and setting, often remains behind the scenes [40, 41, 47, 48]. A separate, but no less important point is the maintenance of such systems, and again we are faced with problems, both personnel and qualifications. As a result, well-documented IIPS, with clear and detailed instructions, effective and adequate software and hardware protection, functioning along with the personnel as a truly complex and unified system, are now rare. At the same time, certificates of compliance with the requirements of the technical protection system of information are multiplying, since the process of state examination of the IIPS is in many ways not devoid of formality.

The organization of response to computer incidents, supported by an up-to-date legal framework, also deserves special attention. Of course, at the first stage, both qualitatively different financing of this activity and close interaction between the regulator, law enforcement agencies, public and commercial organizations will be required, however, everybody must understand the need to form a new defense strategy both in terms of general and cybersecurity.

5 Discussion

Cybersecurity issues are extremely relevant for Ukraine, but measures to counter challenges and threats in this area are at an early stage and are not comprehensive.

In June 2017, within one day, the “Ransom: Win32/Petya” computer virus attacked the private and public sectors of the Ukrainian economy, in particular banks, airports, the state railway company, television companies, telecommunications companies, large chain supermarkets, energy companies, state fiscal services, public authorities and local self-government bodies, etc. The virus also affected private and public entities of other states, but experts in this field agree that Ukraine has suffered the most [14].

The current version of the legislation introduces important basic concepts in the field of cyber security and cyber security and defines the rights and obligations of government agencies regarding cyber security. However, the analysis of its text shows that many provisions are of a declarative nature, it is overloaded with provisions that deal with intentions and principles, which is inappropriate for the law.

Moreover, the project duplicates the provisions of the Cybersecurity Strategy of Ukraine, approved by the Decree of the President of Ukraine dated March 15, 2016 No. 96.

Even in the opinion of the Main Legal Department of the Verkhovna Rada of Ukraine, it is necessary to finalize the conceptual apparatus of the law, since the introduction of new terminology into the legal field should be carried out in a

comprehensive manner and be consistent with the existing one. Indeed, the proposed definitions of terms are too complex, since their formulation is carried out using words, expressions and terms, the meaning of which is no more clear or known than the term itself.

With regard to the definition of the functions and powers of public authorities in the field of cyber defense, the law provides for the following distribution of scope, tasks and responsibilities [29, 34, 38]:

1. The State Service for Special Communications and Information Protection of Ukraine will provide cyber protection of critical information infrastructure facilities; coordinate the activities of other cybersecurity actors; ensure the creation and operation of the national telecommunications network; prevent, detect and respond to cyber incidents and cyberattacks and eliminate their consequences; inform about cyber threats and methods of protection against them; provide information security audit at critical infrastructure facilities, establish requirements for information security auditors, determine the procedure for their certification and recertification. The State Special Communications Service retains control over the observance of legislation in the field of information protection, the conduct of state inspection in this area in accordance with the Law on the Protection of Information in Information and Telecommunication Systems, in force today. This law also provides for the creation of the State Cyber Defense Center.

2. Subordinate to the State Special Communications Service, the Governmental Team of Response to Computer Emergency Events of Ukraine CERT-UA is intended to analyze data on cyber incidents and maintain their register; help prevent, detect and eliminate the consequences of cyber incidents; organize and conduct seminars on cyber defense; prepare and post on its website recommendations on countering cyber attacks and cyber threats; process information about cyber incidents; assist state bodies, local self-government bodies, military formations, enterprises, institutions and organizations, regardless of the form of ownership, as well as citizens of Ukraine in resolving issues of cyber protection and countering cyber threats. For these purposes, as the legislator plans, CERT-UA, will interact with law enforcement agencies, timely informing them about cyber attacks; with foreign and international organizations on cyber incident response; with Ukrainian teams of response to computer emergency events, as well as other entities, regardless of their form of ownership, carrying out activities to ensure the security of cyberspace.

Specialists of the Situation Center for Cybersecurity of the national security body in June of this year stopped and neutralized 76 cyber attacks on the information systems of public authorities [14]. Even under such conditions, comprehensive scientific research in the field of the theory of legal regulation of relations related to information security in Ukraine has not yet been carried out.

Meanwhile, an analysis of the experience of legal regulation of relations in the field of countering threats to the security of national interests in the information sphere shows that a correct understanding of the nature of these relations and the patterns of using methods of legal influence on them is possible only on the basis of a theoretical understanding of the entire problem area and all legislation governing actions through which threats are manifested.

Without this, the authorized state bodies are unable to correctly determine the priority areas of legislative activity. Taking into account the terminological richness of the regulatory framework governing the relations under consideration, and its importance for identifying events associated with the manifestation of information security threats, it became necessary to comprehensively assess this activity, define a number of important concepts related to the subject of legal regulation, and create a scientifically grounded system of such concepts [44, 45]. The multidimensionality of the country's interests in the information sphere, the significant variability of the manifestations of threats and the variety of mechanisms of legal regulation of the relations arising in this connection require the development of special approaches to the study of the problem [52-56]. It seems that the solution of issues arising in this area is possible on the basis of the theory of legal support of information security, as well as analysis of best practices and benchmarking. The examples of the EU countries are the best targets for this, due to some similarity of legal approaches and existing threats, respectively.

In the legal doctrine of the European Union (as well as the United States), the definition of “information security” is carried out through the enumeration of specific elements of the information sphere, which it is aimed at protecting, and is linked to the legal principles of confidentiality, integrity and accessibility of information and information systems [14, 19, 49]. The implementation of these principles makes it possible to ensure a balance of interests of various participants in legal relations, thus acting as a guarantee of human rights in the field of information security.

Subject to the principle of confidentiality, familiarization with confidential information, its processing and presentation of a request for its provision are allowed only for a person who has the right to access such information. The role of the confidentiality principle is to prevent harm that can be caused to public relations as a result of the unlawful provision and dissemination of information kept secret due to its importance for the safety of an individual, society or state. This principle corresponds to a kind of right to “conceal” information, i.e., keep it secret, restrict third party access to it, control its intended use [21].

The domestic legal literature also uses the definition of “information safety” through the state of security of the information sphere, in which it is impossible to implement known threats in relation to its constituent elements [39]. In this case, the concept of “information safety” is considered as a more general category in relation to the concept of “information security’, in which the emphasis is on a set of measures and actions aimed at ensuring the security of information [15, 17]. In this case, we are talking about the state of information security, and not the interests of the individual, society and the state.

In mid-December 2020, the European Commission presented a new EU Cybersecurity Strategy, which aims to strengthen Europe's collective resilience to cyber threats. The implementation of these principles allows ensuring a balance of interests of various participants in legal relations, thus acting as a guarantee of human rights in the field of information security and ensure that all citizens and businesses can make full use of reliable and trustworthy services and digital tools. The strategy is intended to lay down new principles for the development of the cybersecurity sector for the next decade.

The strategy will also enable the EU to set international cybersecurity norms and standards and strengthen cooperation with partners around the world to promote an open, stable and secure cyberspace. The European Commission has also made proposals to improve the cybersecurity of critical physical objects and networks, including the protection of infrastructures that may be subject to cyber attacks, such as transport, energy, health care, the financial system and many other sectors [43]. Thus, the Strategy aims to address current and future online and offline risks, from cyberattacks to cybercrime or natural disasters.

The European Commission also proposed the creation of an EU cybersecurity operations department to coordinate the actions of all countries of the community, deploy a network of operations centers in the EU using AI for early detection and counteraction of cyber attacks, and develop new integrated principles for protecting the entire infrastructure of the EU countries. Primarily, the new cybersecurity strategy aims to protect the global and open Internet, but at the same time offers guarantees not only to ensure security, but also to protect European values

and fundamental rights of everyone through regulatory, investment and policy initiatives [20].

In public law relations, specialized state information systems are increasingly used, for the full functioning of which it is necessary to expand the powers of authorities in the field of processing various types of personal information in an automated mode. These processes, along with measures taken to ensure national security, lead to the formation in legislation of restrictions on the right to privacy. At the same time, the prevention of illegal interference in private life and abuse by the authorities is becoming one of the priority areas for ensuring the information security of an individual.

Currently, the document of interest is a proposal for a Directive of the European Parliament and of the council concerning measures to ensure a high common level of network and information security across the Union, submitted by the European Commission in February 2013. The directive defines the main goal of harmonizing approaches to information security in the EU member states. The directive contains requirements for private companies to provide information on information security incidents. The number of companies includes operators of critical infrastructure in the field of energy, transport, financial industry, healthcare companies providing Internet services. Annex 2 of the Directive includes in the range of regulated entities operators of critical infrastructure facilities organizations whose activities in the EU are defined by the term "information society services": e-commerce platforms; companies providing access to Internet payment systems; social networks; search engines; companies working in the field of cloud computing; application stores. In October 2014, when the draft directive was before the EU Council, the draft directive included Internet traffic exchange points, domain name registrars and web hosting companies [51].

It is expedient to note that the development of legal regulation and the harmonization of relevant standards for ensuring information security, including the security of information technology, in the countries of the European Union began to develop much earlier than in Ukraine, 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 an individual, and the like. German 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 system of classified information includes state secrets (information marked "top secret" and "secret") and departmental secrets (information marked "confidential" and "for official use"), 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 cyber attacks, and analyzes appropriate countermeasures [43]. 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.

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 result from interaction with other subjects of legal relations in the state and subjects of international law. 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.

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 ensuring cyber security. In 2013, ABW developed the Polish Cybersecurity Strategy and initiated the creation of the Cryptology Center under the Ministry of National Defense, which is tasked with information security, cyber defense and offensive cyber operations [17]. ABW has also established a Government Computer Incident Response Team (CERT) [15], whose main task is to ensure and develop the capabilities of government agencies to protect against cyber threats, in particular, from attacks on infrastructure consisting of IT systems and computer networks, or destruction which can significantly threaten the life and health of people, national wealth [20]. Civil society is actively involved in ensuring information security in Poland. An important trend that can and should be borrowed from Poland in the context of ensuring information security is the active involvement of non-state actors in this process, especially members of civil society. It is positive and common with the experience of other leading countries that information security is ensured by adopting, first of all, a key strategic document that guides the activities of all subjects of information security, determines the key areas of these activities and the tasks set for the information security mechanism.

6 Conclusion

The interests of the state in the information sphere are to create conditions for the harmonious development of the Ukrainian information infrastructure, for the implementation of constitutional rights and freedoms of man and citizen in the field of obtaining information and using it in order to ensure the inviolability of the constitutional system, sovereignty and territorial integrity of Ukraine, political, economic and social stability, in the unconditional provision of law and order, the development of equal and mutually beneficial international cooperation.

Thus, information security of a country is a state of protection from internal and external threats to national interests in the information sphere, which is determined by a set of balanced needs in ensuring the sustainable development of the individual, society and the state [18].

The information security of Ukraine is inextricably linked with the information security of the state bodies of the country, and namely the state authorities represent the force for ensuring the information security of Ukraine, using technological, legal, and organizational means.

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.V1I24.128340.
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. Andresson, K.J. (2011). *Cybersecurity: Public Sector Threats and Responses*. CRC Press.
9. 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.
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. Bratel, S., Makarenko, N., Bortnyk, V., & Levchenko, Y. (2021). The role of rule-of-law institutions in ensuring information security of Ukraine. *Revista Amazonia Investiga*, 19(39), 238-244.
15. Christou, G. (2016). *Cybersecurity in the European Union: resilience and adaptability in governance policy, New Security Challenges Series.* Palgrave Macmillan UK, London.
16. 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.
17. ENISA. (2017). *Principles and opportunities for a renewed EU cyber security strategy.* Available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-input-to-the-css-review-b.
18. European Court of Auditors. (2019). *Challenges to effective EU cybersecurity policy*. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_ EN.pdf.
19. Furashev, V. (2012). Essence of informative safety and determination of "informative safety" and "safety of information" concepts. *Legal Information*, 2(34), 51-59.
20. Fuster, G., & Jasmontaite, L. (2020). Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In: M. Christen et al. (Eds.). *The Ethics of Cybersecurity*, 97-115.
21. Getman, A., Danilyan, O., Dzeban, A., Kalinovsky, Y., & Hetman, Y. (2020). Information security in modern society: Sociocultural aspects. *Amazonia Investiga*, 9(25), 6-14.
22. Grama, J. (2014). *Legal Issues in Information Security: Print Bundle.* Jones & Bartlett Learning.
23. Grama, J. (2020). *Legal and Privacy Issues in Information Security*. Jones & Bartlett Learning.
24. 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.
25. Jasmontaite, L., et al. (2018). Data protection by design and by default: framing guiding principles into legal obligations in the GDPR. *European Data Protection Law Review*, 4(2), 168–89.
26. 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.
27. 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.
28. 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.
29. Kukharska, N., & Polotai, O. (2019). Cyber security as a component of information security of Ukraine. *Information Technology and Security*, 7(13), 136-148.
30. 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.
31. 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.
32. 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.
33. 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.
34. Makarchuk, V., Nikitenko, O., Dotsenko, O., Kopan, O., & Kitsul, S. (2021). Tasks and Powers of the National Police of Ukraine in Ensuring Information Security of the State. *Amazonia Investiga*, 10(37), 86-92.
35. 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.

36. 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.
37. 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.
38. Nashynets-Naumova, A. (2017). *Information security: issues of legal regulation*. Kyiv: Helvetika.
39. Nimyshchenko, O.A. (2016). Information security of Ukraine at the current stage of state and society development. *Nashe Pravo*, 1, 17-23.
40. 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.
41. 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.
42. Porcedda, M.G. (2018). *Patching the patchwork: appraising the EU regulatory framework on cyber security breaches*. Elsevier.
43. Robinson, N., & Gaspers, J. (2014). *Information Security and Data Protection Legal and Policy Frameworks Applicable to European Union Institutions and Agencie*s. RAND Corporation.
44. 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.
45. 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.
46. Solms, R.V., & Niekerk, J.V. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.
47. 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
48. 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.
49. Vedder, A., et al. (2019). *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*. Intersentia.
50. 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.
51. Wessel, R.A. (2015). Towards EU cybersecurity law: regulating a new policy field. In: Tsagourias, N. and Buchan, R. (Eds.). *Research handbook on international law and cyberspace*. Edward Elgar Publishing.
52. 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.
53. 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.
54. 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.
55. 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.
56. 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: AG