 DOI: https://doi.org/10.15388/OS.LAW.2020.2

# LEGISLATIVE PRINCIPLES OF INFORMATION SECURITY PROVISION IN THE EUROPEAN UNION MEMBER STATES

**Ivan Bratsuk[1], Svyatoslav Kavin[2]**

**Abstract.** The article is dedicated to the study of the information security provision in the EU Member States in the context of analyzing their state programs, national programs as well as regulatory legal acts. This study identifies priorities and gaps in the information security provision in the EU Member States, analyzes special features of the institutional and legal mechanism of information security in the EU Member States in the context of the multi-vector international security system. The expediency of developing an integral coordinated information policy of the EU Member States, aimed at unification of the approaches to information security, is substantiated, as well as the experience of the EU Member States in this field aimed at improving the domestic regulatory framework of information security provision is studied.
**Keywords:** EU Member States, information security, cyber security, information space, rule of law.

## INTRODUCTION

Currently, many EU Member States have established general national information security networks capable of rapid accumulation of the forces and means of public authorities aimed at countering a wide range of threats. And their operation is clearly regulated by the legal regulatory framework. The experience of the EU Member States (in particular, Germany, France, and Finland) shows that provision of a high level of information security is possible on condition that a thorough and effective system of legal acts in this area is adopted and the bodies that will ensure this security in a certain country function effectively.

The events of recent years clearly point to the availability of a crisis in the field of information security at both international and regional levels. Therefore, solving of the issues of proper legislative information security provision comes to the fore. At present, there are legal regulatory frameworks in this area in the EU Member States, but the problem lies in a certain inconsistency of the laws of the EU Member States in the approaches to addressing certain issues of information security provision, this significantly reducing the effectiveness of legal regulation in this area.

Thus, establishment of an effective and reliable system of information security provision in this country in the conditions of transformation of international security and foreign policy of our country before joining the European Union seems to be highly relevant. And at the forefront is the study of

1 *Associate Professor, Candidate of Law at Ivan Franko National University of Lviv, Department of European Law, Faculty of International Relations, e-mail: bratsuk@gmail.com.*

2 *Postgraduate student at Ivan Franko National University of Lviv, Department of European Law, Faculty of International Relations, e-mail: kavinsviatoslav@gmail.com.*

the experience of the EU Member States in this area, for the sake of adapting the standards available in the EU Member States in the context of information security provision.

## RESULTS OF RESEARCH AND SCIENTIFIC PUBLICATION ANALYSIS

A number of authors in domestic and foreign literature, in particular D.Vasylenko, T.Tkachuk, O.Zozulya, B.Kormych, M.Gorka, V.Pillitelli, M Niles, T. Olavsrud, R. Lucas, and others have dedicated their researches to the issue of information security provision. However, no sufficient comprehensive study aimed at researching and comparing the experience of the EU Member States in the field of information security in order to borrow their experience in domestic law has been conducted.

## GOAL OF THE ARTICLE

To study and develop holistic views of the functioning of the information security provision system in the EU Member States and their impact on the regional security system.

## STATEMENT OF BASIC MATERIALS

The study of the practice of the EU countries in the field of information security provision and cyber threats combatting gives grounds to draw a conclusion about the lack of a unified system in this area, since each of them has its own legal mechanisms for regulating this range of issues. Analyzing the national law of the EU countries, we come to the conclusion that each of them has its own unique information protection system (Vasylenko, Maslak, 2010, p. 129).

Diego Acosta Arcarazo and Cian C Murphy point out that enactment of the Treaty of Lisbon has given the EU new powers in the field of international security law, while the Stockholm Programme is the latest EU framework action program in the field of justice and home affairs, in particular, in the issues of cooperation between the national criminal justice systems. And the combination of the new Treaty and the Programme has made security and justice the key areas of legislative development in the EU (Arcarazo, Murphy, 2014, p. 17). Raphael Bossong also emphasizes this, noting that an important element of cooperation in the field of security between the European Union (EU) Member States is intensive exchange of information between security agencies. No special steps towards integration can, although, be expected in this particularly sensitive area. However, existing approaches to intelligence support of the EU security policy need to be deepened and better monitored (Bossong, 2018, p. 6).

Prof. Dr. Udo Helmbrecht notes that legislative support of the European Union's network and information systems is important with a view to supporting the Internet economy through new initiatives aimed at further improvement of cyber resilience and response to cyber protection. (Helmbrecht, 2018) In this context, Marek Gorka states that a cyber security strategy is a basic document developed at the governmental level, that reflects the interests and rules of work security in cyber space. Besides that, it lays down the foundation for future legislation, policies / standards, guidelines and other security and cyber security recommendations (Gorka, 2018, p. 76).

Information security is one of the components of sustainable development of the whole state, and scientists normally apply the same approaches to the interpretation of the meaning of the term 'information security'. So, in particular, N.R. Nyzhnyk, B.T. Bilous mean by this term 'the status of legal norms and respective security institutions which guarantee constant availability of data for strategic decision-making and protection of information resources of the country' (Lipkan et. al., 2006, p. 280). In essence, a similar opinion is supported by B.A. Kormych who notes that information security should be understood as 'protection of the rules established by law, according to which information processes in the state take place, providing for constitutionally guaranteed conditions of existence and development of individuals, society as a whole and the state' (Kormych, 2004, p.384). In its turn, the opinion according to which 'information security' stands for a legislative and policy framework regulating the use of information and communication technologies by institutions and agencies of the European Union from the point of view of their information security and data confidentiality is noteworthy (Robinson, Gaspers, 2014, p.1-2). This view is supported by K. Dempsey who notes that information security stands for a legal and policy framework that regulates both the legal field and, at the same time, the use of information and communication technologies with an appropriate degree of responsibility for data confidentiality (Nieles et. al., 2017, p.2-3). Finally, Michał Mazur aptly states that 'information security, both real and legal, is a primary factor for the functioning of individuals and institutions, and especially for political bodies that are independent states and based on legal regulation that can authorize effective security of identified data' (Mazur, 2011, p. 64).

In our turn, researching the legal framework for information security, we focused primarily on countries such as Germany, France and Finland, because in our opinion, of all EU member states at the highest level, high legal standards of information security are ensured. Thus, studying legal provision of information security in Germany, we consider it necessary to note that back in 1997 Germany adopted the *Act of Information Protection in Telecommunications* (TDPA). In accordance with its general principles, collection, processing and use of information is allowed only in cases where it is permitted by law or with the user's consent. And since 2005 the so-called *Freedom of Information Act* has been in force in Germany, it regulates the right to access and receive information, in particular, everyone has the right to receive official information from the federal government agencies in accordance with the provisions of the Act. This Act expands on other federal bodies and institutions to the extent that they perform administrative tasks in accordance with public law. But the right of access to information does not apply if information disclosure may have a detrimental effect on international relations; military and other security interests of the Federal Armed Forces; internal or external security interests; external financial control matters (Tkachuk T., 2017a, p.106). The Federal Government must report to the German Bundestag on the application of this Act, while the German Bundestag must evaluate the Act scientifically.

In addition, analyzing the legal platform for information security in Germany, we tried to structure, in our opinion in terms of priority, the system of protection of the information space, in particular: The main coordinating governmental body which aims to promote information technology security, and which ensures security of information flows, systems, channel databases is the Federal Infor-

mation Security Service (BSI) of Germany. BSI is a part of the Federal Ministry of the Interior which, among other functions, ensures internal security and protection of Germany's constitutional order and fights terrorism, extremism, espionage, and sabotage.

In accordance with the Law *On the Federal Office for Information Security*, BSI collects and evaluates information on the threats posed to the state cyber security, detects new types of cyber attacks, as well as analyzes appropriate counter-measures (Klymchuk O., Tkachuk N., 2015, p.78). In our opinion, BSI is actually responsible for performing the following functions in cooperation with NATO and the EU: risk assessment of the information technology introduction; development of the criteria, methods and test tools for assessing the degree of national communication systems security; checking the degree of information systems security and issuing respective certificates; issuing permits for information systems introduction at important government facilities; taking special security measures related to information exchange in the state bodies, police, etc.; checking the reliability of existing information and technical facilities used in the field of federal authorities' activity; creating, verifying, testing and putting into operation cryptographic material for information exchange (for example, encryption of classified documents) at the federal level, etc.) (Tkachuk T., 2017a, p. 106).

In the process of conducting the study, we come to the conclusion that in order to optimize operational cooperation between all government agencies, as well as to improve the coordination of measures aimed at cyber attacks combating, Germany has established the National Cyber Security Center (NCAZ) within the Federal Office for Information Security, which interacts directly with other cyber security actors from the EU, NATO, and international organizations. In this context, I.O. Chernukhin quite aptly points out that this center operates within the Federal Office for Information Protection (BSI) (develops requirements for information protection in the state information systems) with direct involvement of the Federal Office for the Protection of the Constitution (BfV) staff (carries out law enforcement intelligence operations to identify cyber criminals) and the Federal Office for Civil Protection and Disaster Relief (BBK) (takes measures to eliminate socially dangerous consequences of cyber attacks) (Chernukhin, 2014, p. 32).

Within the framework of the proposed structural scheme for the protection of Germany's information space, we would like to note that the Federal Office for the Protection of the Constitution (BfV) and the Office of Information Operations which includes the Information and Computer Network Operations Division (WICMO) (Abteilungder Informationund Comp uter netzwerkoperationen – AICNW) also take care of the Germany's information security. WICMO was established at the end of 2010 as a specialized unit in the Bundeswehr's command structure (since April 2017 it has been operating as the 'German Cyber Space and Information Space Forces'). In his paper *Legal Provision of Information Security in the Context of Ukraine's Integration* Tkachuk T.Y. notes that it is WICMO that is assigned the following tasks in the implementation of the concept of information security in Germany, in particular in the field of cyber defense, that stimulate the effectiveness of measures aimed at cyber crime combating. The tasks of this division include, in particular: development of new methods of cyber attacks; penetration into computer networks of foreign states and organizations

with a view to intelligence data obtaining; carrying out of operations with destructive influence on networks and automated systems or blocking their operation (Tkachuk T., 2018, p. 249).

Analysis of Germany's information security policy allows us to conclude that among the priorities in countering cyber threats Germany has chosen the tactics of the so-called 'active defense'. In our opinion, identification of the offensive component of information confrontation and development of a separate structure constitutes an adequate response to the current threats posed to Germany's information security.

Besides this we would like to note that, on May 25, 2018, a new Federal Law *On Data Protection* (BDSG) came into force in the country, and it is adapted at the national level to EU Regulation 2016/679 of April 27, 2016 on the protection of individuals with regard to the processing of personal data and free movement of such data / Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 /. In addition, this Federal Law *On Data Protection* (Part I, Chapter 4) establishes the status and forms of activity of the Federal Commissioner for Information Data Protection. The Federal Commissioner, in general, acts as an ombudsman. Anyone who considers that their right of access to information under the German Federal *Freedom of Information Act* has been violated may apply to the Federal Commissioner for freedom of information. Accordingly, the Federal Commissioner may request federal authorities subject to the *Information Act* (IFG) to apply in the relevant issues and, where appropriate, may act as a mediator and work to ensure due process. However, he cannot give instructions to the authorities. If the Federal Commissioner considers that the German Federal *Freedom of Information Act* has been violated, he may express a formal objection and notify a higher authority and, if necessary, the German Bundestag thereof (Bundesdatenschutzgesetz (BDSG)).

Analyzing the legal platform for information security in France, we come to the conclusion that similar tactics in Germany for information security work successfully in France. In this format, we would like to note that since July 17, 2014, at the level of the legislative act, the program Politique de sécurité des systèmes d'information de l'état (State Information Systems Security Policy) has been in effect, it determines the global information systems security policy. We consider that this program establishes the rules for the protection of state information systems and priority mechanisms for combating cyber threats at the state level. These rules were developed by the National Systems Security Agency (ANSSI), in collaboration with the ministries. And on March 27, 2015 *Décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense* was issued, in which the French government has formulated new provisions for the security of information systems of operators in the sectors the role of which is critical to the life of the nation. In particular, this Decree sets the terms for: determining security rules necessary for the protection of information systems of operators that are of vital importance; introducing the systems for detecting events that affect the security of these information systems; informing about incidents affecting security or information systems operation, exercising control over information systems. In addition, it sets criteria that allow operators to identify information systems,

as well as IT security rules (Publication du décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale).

In the process of conducting the study, it should be noted that the basic legal act that defines the strategic directions of French public policy in the field of security is the *White Paper on Defense and National Security* as of 2008. It names large-scale attacks on information systems among the most likely threats to France and the European community as a whole. The main ways to counter these threats mentioned in the document are cooperation in countering attacks on information systems, primarily within the EU; conducting both overt and covert active measures to counter the manifestations of aggression in information networks; training cyber troops on a professional basis (Défense et Sécurité nationale. Le Livre blanc). In 2013 the fourth White Paper was published under the supervision of Francois Hollande. In our opinion, a special feature of this document is recognition of military operations as 'the most important element of security'. The fifth document, under a slightly different title ('Strategic Defense Review and National Security'), was published in the late 2017 under the supervision of Emmanuel Macron. As noted by Shemchuk V.V. in his article 'Foreign Experience of Information Security of the State', this document pays a great attention to information threats and countermeasures, and it is also noted that some attacks in cyber space, due to their scale and severity, can be classified as armed aggression (Shemchuk, 2019, p. 189).

In order to implement the general security provision directions which are identified in the White Paper on security and defense in the information field, there has been elaborated a program regulatory act – *French Strategy on the Security and Defense of Information Systems*. Accordingly, on February 15, 2011, the National Agency for Information Systems Security published French strategy in the field of defense and security of information systems. The strategy set out in this document for the defense and security of national information systems is based on four goals, viz.: to have world-class cyber protection, to guarantee freedom of decisions in France through confidential and secret information protection, to strengthen cyber security of the critical national infrastructure, and to ensure security in civilian cyber space (La stratégie de la France en matière de cyberdéfense et cybersécurité).

Also, as it is absolutely aptly noted in this context by Shemchuk V.V. in his article 'Foreign Experience of Information Security of the State', armies must fully plan and conduct operations in the digital space up to the tactical level in the chain of planning and conducting kinetic operations. In addition, to ensure information security the Defense Review allows to conduct combat operations in cyber space, which means a defensive or offensive struggle throughout the digital environment against government or non-government opponents (Shemchuk, 2019, p. 189-190).

Accordingly, based on the research, we want to express the opinion that in order to achieve these goals, the following areas should be identified for effective information security, in particular: to protect the information systems of the state and critical infrastructure operators to improve national resilience; to adapt the legal framework with due account of the latest technological developments and new types of information systems usage; to develop international cooperation in the field of information systems security, fight against cyber crime and cyber protection for better protection of the national information systems, etc.

In addition, we would like to note that despite the general lack of organizational integrity, a single coordinating body for information security, the national system of France contains both active (development of the information sphere, obtaining of the necessary information) and passive (protection of own information resources, systems, national identity) components for the protection of national interests in the information field. Beside that, executive authorities provide for the development of their own information space and information infrastructure, while special services take measures to protect them.

It is also worth noting that in order to counter information security threats, as well as to build a single nationwide system for protecting critical infrastructure against cyber threats, the National Agency for Information Systems Security (ANSSI) was established in 2009 as part of SGDSN. In order to support the activities of governmental agencies in critical conditions, SGDSN is responsible for the reliability, confidentiality, functionality of government communication means. Taking care of state secrets, SGDSN regulates the activities aimed at the protection of national defense secrets, determines interdepartmental priorities in this area. In addition, SGDSN coordinates economic intelligence activities. Shemchuk V.V. in his article 'Foreign Experience of Information Security of the State' notes that the respective function is to obtain, process and disseminate joint strategic information, the success of which depends on clear interagency coordination that should be accompanied by concerted action of economic entities and public administration (Shemchuk, 2019, p. 190).

The above legislative steps taken by Germany and France clearly confirm that special attention is paid to information security issues in these countries. However, according to Politanskyy, Finland has some particularly useful experience in the field of information security, as it is a successful example of implementing the optimal model of information society, establishing a developed information technology infrastructure and ensuring a high level of public access to them (Politanskyy, 2017, p. 35). Here again, it is important to note that participation in the EU imposes on these countries the obligations to comply with the standards of this organization related to the information society development and information security provision.

According to our research, the structural scheme of information security in Finland is as follows: the key state institutions responsible for the development and implementation of Finland's information security policy are the Ministry of Transport and Communications of Finland, the Data Protection Ombudsman. The Ministry of Transport and Communications is responsible for the development of legislation on communication networks, data security, ensuring access to communication services, as well as for the development and implementation of the national policy in the field of information security. A structural subdivision of the Ministry of Transport and Communications is the Finnish Communications Regulatory Authority (FICORA), the mandate of which includes control and state regulation in the field of information and communication technologies, as Tkachuk T.Y. notes in his article 'Ensuring Information Security in Non-Aligned Countries" (Tkachuk T., 20176, p. 62). The author notes that FICORA structure includes CERT-FI (Computer Emergency Response Team of Finland) – a Finnish rapid response computer team the main task of which is to prevent, detect and respond to cyber incidents, as well as to disseminate information about information security threats. In 2013

the Government of Finland approved the National Information Security Strategy which outlined the following priorities for improving the management of threats and the effectiveness of strategically important information systems maintenance, in particular: raising the basic knowledge of the population and business in the field of information security through provision of confidential and secure network services; developing and implementing professional training at all levels in order to strengthen information security; investing into international cooperation and participation in international research activities focused on information security (Finland Cyber Security Strategy (2013)).

In this context, we share the view expressed by Zozulya O.S., that it is the Finnish model of information society that has a strong social orientation, with combination of dynamic interaction between business and society with an active mediatory role of the state. The state retains two functions: development management and deregulation. Its main goals include establishment of the national information infrastructure to help raise public awareness among the country residents. Because of that, as the author notes, since 2003 the Government of Finland has been implementing measures to inform the citizens of the country about the methods and ways of protection against the negative information impact within the framework of the Information Security Strategy (Zozulya, 2016, p. 35).

It should also be noted that in 2013 the Government of Finland approved the National Information Security Strategy, which identifies the following priorities: establishment of the national information security center for comprehensive data collection and analysis, general situational awareness as well as national and international cooperation; excellence of threat management and service efficiency for strategically important information systems; raising of the basic knowledge of the population and business in the field of information security through provision of confidential and secure network services; development and implementation of professional training at all levels in order to strengthen information security; investing into international cooperation and participation in the international research activities focused on information security (Finland Cyber Security Strategy (2013). In our opinion the Finnish National Security Strategy presupposes thus minimizing of the risks involved, which is an important task in ensuring global information security, since cyber attacks can be used as a tool of political and economic pressure, including in combination with traditional military means.

During the research a special attention was focused on the features of legal information security of the EU Germany, France and Finland in the context of studying their national cyber strategies as an inherent component of national security, in particular in terms of diversification of external relations in a multi-vector system of international security. The peculiarities of the functioning of the institutional and legal mechanism of cyber defense in the context of the legislative regulation of international cooperation between state institutions and national security structures were analyzed. The need to develop a coherent cyber defense policy of the European Union in the context of EU information policy in order to unify approaches to information protection and improve the regulatory framework for information security was also justified.

In general, having studied the specifics and features of information security in the EU, Germany, France and Finland, we concluded that in general the issue of information security in these EU countries is heterogeneous and contains a number of differences depending on the country. Thus,

Germany has a comprehensive cybersecurity strategy, complemented by a strong legal framework in the field of cybersecurity. In particular, the existence of the Federal Office for Information Security (BSI), which is responsible for managing the computer and communication security of the German government, is a clear demonstration that information security is at a high level. In this turn, France has a national cybersecurity strategy that focuses heavily on defense and national security. In particular, the National Agency for Information Systems Security (ANSSI) is a well-established information security body integrated with the country's CERT-FR computer emergency response team. And the implementation of specific sectoral security measures makes France one of the few EU countries that has taken such a focused approach to governance, including information security.

At the same time, based on our research, we would like to note that the approaches to information security adopted in the European Union are currently not unified. Therefore, research, evaluation and implementation of the positive experience of each EU country in this area are important in building the information security system of the European Union.

In addition, our analysis of the regulatory framework of the cyber security system of the EU countries Germany, France and Finland allows us to demonstrate the dominant role of intelligence services in ensuring cyber security. In this regard, in our opinion, international cooperation on unified approaches to combating cyber threats in the information space is somewhat limited.

Finally, we would like to note that the practical experience of the EU countries Germany, France and Finland is especially important in the formation of the domestic legal framework in the field of information security. Thus, the adaptation of legal standards that take place in these EU countries in this area is a priority of our country in the context of development and development of the national information security system.

## Bibliography

**Legal acts**

1. Act on the Federal Office for Information Security (BSI Act - BSIG). Accessed 9 July 2020. Available via the internet at: <https://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz.html>.

2. Act on the Protection of Privacy in Electronic Communications. Accessed 9 July 2020. Available via the internet at: <https://www.finlex.fi/en/laki/kaannokset/2004/en20040516>.

3. Adequate and effective cybersecurity: state of play. Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht – Cybersecurity Conference organized by the Austrian Presidency of the Council of the European Union. Vienna, Austria 3rd December 2018.

4. Bundesdatenschutzgesetz (BDSG). Accessed 9 July 2020. Available via the internet at: <https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html>.

5. Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI). Accessed 9 July 2020. Available via the internet at: <https://www.bfdi.bund.de/DE/Home/home_node.html>.

6. Bundesministerium Inneres Austria. (undated) [online]. Available via the internet at: https://bundeskriminalamt.at/306/start.aspx [Accessed 09 July 2020].

7. Défense et Sécurité nationale. Le Livre blanc. Accessed 9 July 2020. Available via the internet at: <http://archives.livreblancdefenseetsecurite.gouv.fr>.

8. Finland Cyber Security Strategy (2013). Accessed 9 July 2020. Available via the internet at: <http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40finlandas-cyber-security-strategy>.

9. Government Decree on information security in central government (681/2010). Accessed 9 July 2020. Available via the internet at: <https://www.finlex.fi/en/laki/kaannokset/2010/20100681>.

10. La stratégie de la France en matière de cyberdéfense et cybersécurité. Accessed 9 July 2020. Available via the internet at: <https://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite/>.

11. Politique de sécurité des systèmes d'information de l'état. Accessed 9 July 2020. Available via the internet at: <http://circulaire.legifrance.gouv.fr/pdf/2014/08/cir_38641.pdf>.

12. Publication du décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale. Accessed 9 July 2020. Available via the internet at: <https://www.ssi.gouv.fr/publication/publication-du-decret-n-2015-351-du-27-mars-2015-relatif-a-la-securite-des-systemes-dinformation-des-operateurs-dimportance-vitale/>.

**Special literature**

13. Василенко Д.П., Маслак В.І. (2010). Законодавство провідних країн світу в сфері захисту інформації. Вісник КДУ імені Михайла Остроградського. Випуск № 61, частина 1. Частина 1. С.129. [Vasylenko D. and Maslak V. A Legislation of Leading Countries of the World is in Sphere of Defence of Information. Scientific journal "Transactions of Kremenchuk Mykhailo Ostrohradskyi National University" 61(2) part1].

14. Зозуля О. С. (2016). Зарубіжний досвід державного управління забезпеченням інформаційної безпеки в умовах інформаційнопсихологічного протиборства. Науково-інформаційний вісник Академії національної безпеки. № 1-2. С. 35 [Zozulya O. 2016. Foreign Experience of Public Administration Ensuring Information Security in Conditions of Information-Psychological Confrontation. Scientific journal the Academy of National Security 9-10 (1-2)].

15. Кормич Б.А. (2004). Інформаційна безпека: організаційно-правові основи [Текст] : навч. посібник для студ. вищих навч. закл. / Б.А. Кормич. – К.: Кондор, 2004. – 384 с. – (Юридична книга). [Kormych B. 2004. Information Security: Organizational-Legal Basis. Kiev: Condor.]

16. Климчук О.О., Ткачук Н.А. (2015). Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. Інформаційна безпека людини, суспільства, держави. № 3 (19). С.75-83. [ Klymchuk O., Tkachuk N. 2015. Role of law enforcement bodies and special services in national cyber security systems of leading countries. Scientific Journal Series «Juridical sciences», Information Security of the Person, Society and State 19 (3)].

17. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. (2006). Інформаційна безпека України в умовах євроінтеграції / Навчальний посібник. - К.: КНТ. [Lipkan V., Maksymenko Y., and Jelihovsky V. 2006. Information security of Ukraine in the conditions of European integration. Kiev: KNT].

18. Політанський В.С. (2017). Світові моделі та фундаментальні принципи інформаційного суспільства. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 43, том 1. [Politanskyy V. 2017. World Models and Fundamental Principles Information Society. Scientific Bulletin of UzhNU. The "Law" 43 part1].

19. Ткачук Т. Ю. Забезпечення інформаційної безпеки у країнах центральної Європи. Юридичний науковий електронний журнал. 2017 № 5. Ст.106 [Tkachuk T. 2017. Information security ensuring in the countries of central Europe. [Juridical scientific and electronic journal, accessed 9 July 2020. Available via the internet at: <http://lsej.org.ua/index.php/arkhiv-nomeriv?id=80>.

20. Ткачук Т.Ю. Забезпечення інформаційної безпеки в країнах позаблокового статусу. Прикарпатський

юридичний вісник. 2017. № 4 (19). Ст. 62 [Tkachuk T. 2014. Information security ensuring in the non-aligned countries», Subcarpathian Law Herald 19 (4), pp.61-65].

21. Ткачук Т. Ю. (2018). Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: моногр. К.: ВД «АртЕк». [Tkachuk T. 2018. Legal providing of information security in conditions of European integration of Ukraine: legal dimension. Kiev: ph-artec].

22. Чернухін І. О. (2014). Досвід Федеративної Республіки Німеччини в побудові системи захисту інфраструктури / І. О. Чернухін // Інформаційна безпека людини, суспільства, держави. – 2014. – № 1(14). – С. 32 [Chernouhin I.The experience of the Federal Republic of Germany in the field critical infrastructure protection from cyber threats. Scientific Journal Series «Juridical sciences» Information Security of the Person, Society and State 14(1)].

23. Шемчук В.В. (2019). Зарубіжний досвід забезпечення інформаційної безпеки держави. Порівняльно-аналітичне право. 2019, № 2 Ст.189 [Shemchuk V. 2019. Foreign Experience in Providing Information Security of State. Comparative analytical law 2 part1].

24. Murphy C. C., Acosta Arcarazo D., (2014). Rethinking Europe's Freedom, Security and Justice. In: Cian C Murphy and Diego Acosta Arcarazo ed. 2014. EU Security and Justice Law. After Lisbon and Stockholm, Oxford and Portland, Oregon: Hart Publishing.

25. Gorka, M. (2018). The Cybersecurity Strategy of the Visegrad Group Countries. Politics in Central Europe 14(2).

26. Nieles, M., Dempsey K., Yan Pillitteri, V. (2017). An Introduction to Information Security. Special Publication 800-12 Revision 1. Gaithersburg: National Institute of Standards and Technology (NIST).

27. Mazur, M. (2011). The Legal Basis of Informational Security in Face of Modem World Reality or Only a Myth. In: The Academy of Economic Studies of Moldova, Information Security Laboratory, International Conference (8th edition), Security Information 2011. Kishinev, Republic of Moldova, 4 May, Kishinev: Editorial-Polygraphic Department of ASEM.

28. Robinson N., Gaspers, J. (2014). Information Security and Data Protection Legal and Policy Frameworks Applicable to European Union Institutions and Agencies. Brussels: RAND Corporation.

29. Robinson, R. (2018). Intelligence Support for EU Security. Options for Enhancing the Flow of Information and Political Oversinght. SWP Comment 2018/C51, December 2018, 8.