CYBER SECURITY AND CYBER PROTECTION: THE CURRENT STATE OF PUBLIC ADMINISTRATION IN UKRAINE

Andrii Semenchenko[a][0000-0001-6482-3872], *Valentyna Pleskach*[b][0000-0002-4700-6704], *Oleh Zaiarnyi*[b][0000-0003-4549-7201], *Mariia Pleskach*[b][0000-0003-3296-5475]

[a]National Academy of Public Administration under the President of Ukraine, Kyiv, Ukraine
[b]Taras Shevchenko National University of Kyiv, 03680, Kyiv-187, Akademician Glushkov Avenue, 4d.

Abstract: The study analyzes the organizational and legal mechanisms of cybersecurity state national management in Ukraine. It provides the definition of the cybersecurity essence, its place in the strategic planning and management of security and defence sector, assessment of the particular aspects of cyber security in Ukraine. The article has identified and addressed the gaps in the conduct of cyber security reviews regarding defence sector, the national counter-terrorism system, cyber protection of the national critical information cyber-protection of critical information infrastructure, etc. Such reviews should include assessment of the state of cybersecurity, norms that regulate cyber-attacks, cyber espionage and cyberterrorism, threats to national security of Ukraine in cyberspace, provision of advancement for the national cyber security system through the supply of new specialized technologies and resources and upgrading of existing technology and equipment steamed from rethinking of the national cybersecurity strategy. Legal regulations and organizational approaches to the technical protection of the national critical infrastructure have become a specific aspect of the research. The authors have analyzed in detail the organizational, legal and information bases of implementation of state and governmental instruments of detection and counteraction to risks of encroachment on established regimes of public information, described the necessary regulatory requirements for technical protection of critical infrastructure objects in the context of ensuring national cyber security of the state. Important attention has been paid to the specifics of application of such public administration tools in the sphere of cybersecurity, as national standards of technical protection of information, audit of cybersecurity objects, monitoring of national critical infrastructure objects, etc. It is proposed to subordinate the State Service for Special Communications and Information Protection of Ukraine to the Ministry of Digital Transformation of Ukraine. In addition, the article contains recommendations for improving the system for ensuring cyber security in Ukraine. In particular, it gives proposals for eliminating existing conflicts and gaps in the main legal acts regulating the sphere of national, information and cyber security of Ukraine through the harmonization of Ukrainian legislation with international legal acts in this area.

Keywords: information sovereignty of the state, cybersecurity, cybersecurity, critical infrastructure facilities, cybersecurity system, cybersecurity strategy, cybersecurity actors.

Анотація: У дослідженні здійснено аналіз організаційно-правових механізмів державного управління забезпеченням кібернетичної безпеки та кібернетичного захисту України, надано визначення його сутності, місця в системі стратегічного планування та управління сектором безпеки та оборони, проведено оцінку аспектів забезпечення кібернетичної безпеки в Україні, зокрема авторами виявлено прогалини у порядку проведення оглядів у сфері кібернетичної безпеки (зокрема оборонного, огляду загальнодержавної системи боротьби з тероризмом, огляду стану кіберзахисту критичної інформаційної інфраструктури тощо), які повинні містити оцінку стану кібероборони, боротьби з кібершпигунством та кібертероризмом, загроз національній безпеці України у кіберпросторі, забезпечення спроможностей основних суб'єктів національної системи кібербезпеки шляхом постачання нових і модернізації наявних зразків спеціальної техніки. Окремим аспектом предмета дослідження у цій статті стали правові та організаційні особливості технічного захисту об'єктів критичної інфраструктури. Авторами детально проаналізовані організаційно-правові, інформаційні засади реалізації державно-владних інструментів виявлення і протидії ризикам посягання на встановлені режими публічної інформації, описано необхідні нормативні вимоги до технічного захисту об'єктів критичної інфраструктури у контексті забезпечення національної кібербезпеки держави. Важливу увагу приділено особливостям застосування таких інструментів публічного адміністрування у сфері забезпечення кібербезпеки як національні стандарти технічного захисту інформації, аудит об'єктів кіберзахисту, моніторинг об'єктів національної критичної інфраструктури тощо. Запропоновано з урахуванням організаційних змін в сфері кібербезпеки підпорядкувати Державну службу спеціального зв'язку та захисту інформації України Міністерству цифрової трансформації України. Крім того, у статті містяться рекомендації щодо вдосконалення системи забезпечення кібернетичної безпеки в Україні, зокрема надано пропозиції щодо усунення наявних колізій і прогалин в основних нормативно-правових актах, що регулюють сферу забезпечення національної, інформаційної та кібернетичної безпеки України, у тому числі шляхом гармонізації українського законодавства з міжнародними правовими актами у цій галузі.
Ключові слова: інформаційний суверенітет держави, кібербезпека, кіберзахист, об'єкти критичної інфраструктури, система забезпечення кібернетичної безпеки, стратегія забезпечення кібербезпеки, суб'єкти забезпечення кібербезпеки.

Introduction

One of the preconditions for the successful formulation and implementation of state cybersecurity policy is its systematic effective political, organizational and legal, information and analytical, technical, scientific and methodological, methodological support. Monitoring, analysis and assessment of this support and prospects for its development at the national level are carried out primarily in in a series of Ukraine's interrelated security and defence sector reviews that, according to Article 27 of the Law of Ukraine "On national security of Ukraine" include a comprehensive review of the security and defense sector and its separate components - the state of defense, public safety and security, defense industry, intelligence agencies of Ukraine, national counter-terrorism, cyber protection of

state information resources and critical information infrastructure.

Based on the results of such reviews, conceptual, strategic, planning and program documents for the development of the security and defense sector, starting from the general National Security Strategy of Ukraine and its individual components, including the Cyber Security Strategy of Ukraine and the National Intelligence Program on the basis of medium and short-term planning are formed in a sequence determined by the legislation.

The legislation defines a number of initiation factors of long-term strategic documents. Thus, according to Article 26 of the Law of Ukraine "On national security of Ukraine", the National Security Strategy of Ukraine shall be developed on behalf of President of Ukraine within six months after his assumption of office, and other strategic planning documents in the areas of national security and defence shall be formed on its basis, in particular the strategy: development of human capital, military security, public safety and security, development of defence industry, economic, environmental, informational security and sybersecurity as well as national intelligence program, foreign security strategy, state security, counterintelligence and counter-terrorism strategy.

Another reason for initiating the development of a system of interrelated strategic documents may be a sharp change in the situation and conditions of the security and defence sector functioning, which were not foreseen at the stage of its formation and, which cannot be compensated for their adjustments, for example, in 2015 and 2016 when new National Security Strategy of Ukraine, Military Doctrine of Ukraine, Doctrine of Information Security of Ukraine, Cyber Security Strategy were adopted [1,2].

Therefore, the urgency of the problem is predetermined by the imperfection of the existing theoretical and methodological apparatus of mechanisms of state management of cyber security of citizens, society and the state, in particular, in the organization and conduct of reviews in this area, the requirements of the legislation, inconsistency of requirements regarding the state of cybersecurity and the level of its provision.

Literature review

The issues of cybersecurity and cyberdefence of a person, society and state have been considered in different contexts by recognised international and Ukrainian scholars starting from K. Alexander who researches the integration of private and public sector communication systems to create the advanced level of intelligence sharing and protect society from cyberthreats worldwide [3]; J. Liepman who explores the elements of national foreign policy of a state on the example of the USA, and also highlights global and regional problems, long-term political issues, organizational, financial and diplomatic challenges to national security [4]; Bruce Schneier who researches information and cyber security [5]; R. Aldrich, whose findings have been used to develop models of cyber security management and strategic management system [6-8]; M. Schmitt, who specializes in international law regarding cyberspace [9].

Ukrainian scholars have also contributed to the research. In particular, V. Buriachok researches the influence of cyber security on the state of economic development of leading countries worldwide including Ukraine [10]; P. Grischuk analyzes the technologies of cyberattack detection [11]; A. Dovgan considers information security as a guarantor of the security of national information resources [12]; D. Myalkovskiy studies legislative and regulatory issues in the field of cryptographic information protection [13]; T. Stanislavsky highlight the state and the ways of state administration system future development regarding the implementation of the cyber security strategy of Ukraine [14].

However, not wishstanding the work of the researches mentioned above, there are not enough systematic studies covering the issues of the state of cybersecurity and cyber defense in Ukraine now.

The lack of systematic research on the issues of reviewing the state of cyber security and cyber defence in Ukraine has triggered the relevance of this study.

The aim of the article is to define the essence, place of organizational and legal mechanisms of state cyber security and cyber defence management in the strategic planning and security and defence sector management, analyze their status, interaction among organizational and legal mechanisms, justification of development and improvement priority directions.

Review and analysis of cyber security and cyber defence state

General assessment of the state of cyber security in Ukraine is given in the Cyber Security Strategy of Ukraine, which is characterized by an increase in the number and capacity of cyber attacks motivated by the interests of some states, groups and individuals, the dissemination of illegal collection, storage, use and destruction of personal data, illegal financial transactions, cybertheft and fraud on the Internet.

Cybercrime is becoming transnational and can cause significant damage to the interests of individuals, society and the state.

The level of cybersecurity and cyber protection in Ukraine is affected by a number of major negative factors, such as:

- the state of info-communications infrastructure, the level of its development and security do not meet the challenges and threats of the modern cyberspace;
- insufficient level of protection of critical infrastructure, state electronic information resources and imperfection of organizational and legal mechanisms of state management of cyber security and cyber protection make them vulnerable to cyber attacks;
- discrepancies between the national cybersecurity framework on measures of cyber protection of critical infrastructure;
- insufficient development of organizational and technical infrastructure to ensure cyber security and cyberprotection of critical infrastructure and state electronic information resources;
- insufficient effectiveness of Ukrainian security and defence sector in countering cyberthreats of military, criminal, terrorist and other nature;
- insufficient coordination, interaction and information exchange within cybersecurity framework;

- competence inconsistency among those subjected to cyber-security provision in performing certain functions and tasks of the state regarding the direction of state policy;
- lack of universal requirements to technical tasks for creation or modernization of public registers, information and telecommunication systems and databases;
- lack of special measures of administrative and criminal termination of illegal behaviour of citizens and legal entities, containing signs of cybersecurity threats in the Ukrainian legislation.

The above mentioned negative factors are not only specifics of Ukrainian cyber security sphere, they are quite widespread and to some extent inherent in other countries, but the mechanisms of their neutralization, as a rule, differ and depend on the peculiarities of each country's development. Thus, for example, in case of illegal distribution of information in China and countries of the Middle East, the provider is responsible for all the actions of users, while in the EU countries the provider, under the European Directive on e-commerce, is exempt from liability if it meets certain conditions of the contract, according to the legislation of other countries. For example, in the USA, the provider is not responsible for the actions of users at all [15].

Among these negative factors, the imperfection of organizational and legal mechanisms of state management of cyber security and cyber defence is especially hazardous; in particular, their incompleteness, declarative, contradictory, blurred, fragmented, uncoordinated character and inconsistency among them.

According to the decision of the National Security and Defence Council of Ukraine approved by the Decree of the President of Ukraine "On organization of planning in the security and defence sector of Ukraine" of May 16, 2019 № 225 [16], a number of reviews are to be conducted, in particular, of defence sector, taking into account the national system of combating terrorism, the state of cyber-protection of critical information infrastructure, state information resources and information, the protection of which is required by the law.

These reviews may be conducted either as part of a comprehensive monitoring of the security and defence sector or its separate divisions. Most reviews have already been conducted.

In 2019, the decisions of the Government (Resolution of the Cabinet of Ministers of Ukraine "On approval of the procedure for review of public security and protection by the Ministry of Internal Affairs" of May 22, 2019 № 07, "On approval of the procedure for review of the defence industry" of May 22, 2019 № 490 and "On approval of the procedure for the defence review by the Ministry of Defence" of October 31, 2018 № 941 as amended by Resolution of the Cabinet of Ministers of Ukraine № 911 of November 6, 2019) and the President of Ukraine (Presidential decrees "On the order of review of intelligence agencies of Ukraine" of August 9, 2019 № 589/2019 and "On the order of review of the national system of combating terrorism" of July 9, 2019 № 506/2019) have developed and approved unified procedures and criteria for the above reviews, by which the state of readiness of the security and defence sector in the respective spheres has been assessed. However, regarding the examination of state information resources cyber defence and critical information infrastructure, the relevant orders have never been approved by the Government, and the review of the sector has not been carried out.

The results of these reviews have laid the basis for the formation of a set of interrelated long-term documents defined by the Law of Ukraine "On the national security of Ukraine", in particular, the new National Security Strategy of Ukraine and the new Military Security Strategy of Ukraine, the Strategy of Public Security and Civil Protection of Ukraine, the Strategy of Development of Defence Industry of Ukraine, the Strategy of Cyber Security of Ukraine that are the basis for targeted state programs and other medium-term and short-term planning documents on the national security and defense.

Therefore, in order to strengthen the legal, organizational and methodical support of the review of cyber defence of state information resources and critical information infrastructure it is necessary to develop and approve the procedure of its implementation by the Cabinet of Ministers of Ukraine, taking into account international and national experience, such as the defence review of the Ministry of Defence, to develop and adopt a number of the following by-laws:
- Recommendations on planning an review of the state of cyber defence of state information resources and critical information infrastructure based on its capabilities.
- The procedure of conducting reviews by law enforcement agencies of the activity of public registers, databases managers and administrators as well as information and telecommunication systems to detect and prevent threats to cyber security of the state, society, individual citizens and legal entities.
- Procedure for organization and implementation of public-private partnership projects in the sphere of ensuring cybernetic security of the State, territorial communities and international governmental organizations whose official representative offices are located on the territory of Ukraine [17].
- Procedure for ensuring cyber security of state and municipal resources that are placed or managed via cloud computing technologies.
- Action plan for the review of the cyberdefence of State information resources and critical information infrastructure, detailing and specifying tasks and measures, quantitative and qualitative indicators, performers and expected results of the review of the cyberdefence of State information resources and critical information infrastructure.

By analogy, as it is successfully implemented in the Slovak Republic and Great Britain [18].

Practical implementation of the mentioned proposals directly reflects the tasks of the state activity on enhancing the technical protection of information in public registers and information and telecommunication systems, coordination of data structures, stored or processed, as well as modernization of IT-architecture of corresponding objects in order to ensure their interoperability, technical neutrality and protection against external threats. Positive

experience of dealing with such issues was analyzed and evaluated by M. Grebenyuk. [19]

To meet these objectives the President of Ukraine issued Decree 558/2019 of July 29, 2019 "On some measures to improve access of individuals and legal entities in electronic services" with the main purpose to strengthen national electronic resources and systems security and ensure the provision of electronic administrative services or processing of personal data of Ukrainian citizens and persons who have residency in our state [20].

Cybersecurity issues are in almost all spheres of national security and defence as defined in Article 17 of the Constitution of Ukraine and the Law of Ukraine "On national security of Ukraine". Therefore, the most important aspect is the inclusion of the assessments of the state tasks implementation by the main subjects of the national system of cybersecurity within their competence into the reports on the results of the comprehensive review of the security and defence sector and its separate reviews, in accordance with Article 8 of the Act on basic principles of cybersecurity and the provision of such information to the State Service for Special Communications and Information Protection of Ukraine, as "a State body responsible for formulating and implementing State policy for the protection in cyberspace of State information resources and information, the protection of which is required by law, and the cyber defence of critical information infrastructure objects".

Thus, under Article 27, Paragraphs 1 and 3 to 5, of the National Security Act and Article 8 of the Basic Principles of Cyber Security of Ukraine Act, individual reviews must include assessments of the status, including the following [21]:

- cyber defence - in the defence review;
- combating cybercrime - in the review of public security and protection;
- combating cyber espionage and cyberterrorism in the review of the national system of countering terrorism.
- threats to Ukraine's national security in cyberspace - in an intelligence review;
- providing capabilities of the main subjects of the national system of cyber security through the supply of new and modernization of existing samples of special equipment - in the review of the defence industry of Ukraine, etc.

Some procedures for certain reviews (defence review by the Ministry of Defence of Ukraine, taking into account the defence-industrial complex of the Ministry of Economic Development, Trade and Agriculture of Ukraine, taking into account the national system for combating terrorism) provide for the creation of appropriate interdepartmental (working) groups, which may include representatives of the State Service for Special Communication and Information Protection of Ukraine, in the interests of, among others, formation of an overall assessment of the state of cyber security and cyber defence. However, as practice shows, the effectiveness of this mechanism of interaction is still quite low and not applied in all reviews. For example, the review of public security and civil protection of the Ministry of Internal Affairs of Ukraine, where the procedure of the review does not include representatives of other government agencies and the National Institute for Strategic Studies, makes it difficult to form an overall assessment of the state of cybersecurity, since the issue of combating cybercrime is its important part. At the same time, the international experience of some countries points to the fundamental possibility of successful solution of the above problems, which can be taken into account in Ukraine regarding the peculiarities of the country’s development [22].

It is possible to collect and summarize information on the state of cybersecurity at the level of the Government (the State Service of Special Communication and Information Protection of Ukraine), but in the conditions of organization of information interaction based on the results of reviews of intelligence agencies and the national system of combating terrorism (the Security Service of Ukraine) in terms of threats to the national security of Ukraine in cyberspace and the fight against terrorism. as well as at the level of the National Security and Defence Council of Ukraine (the main option defined by legislation) in the formation of the next Cyber Security Strategy of Ukraine, primarily on the basis of the National Coordination Centre for Cyber Security, which in accordance with legislation (Presidential Decree of June 7, 2016 № 242/2016 "On National Coordination Centre for Cyber Security") is the customer of this document and performs analysis of cyber security; the results of the review of the national system of cybersecurity; the state of readiness of cybersecurity subjects to perform tasks to counter cyberthreats; the state of compliance with the requirements of legislation on cyberprotection of state electronic information resources, information the protection of which is required by law, as well as critical information infrastructure; data on cyberincidents regarding state information resources in the information and telecommunication system

However, due to the insufficient resources of the Centre, primarily its human resources, there is a problem with the effectiveness of the tasks assigned to it. For example, in Great Britain, the Office of Cyber Security and Information Support coordinates cooperation between different subjects in cyber security, including the private sector, much more effectively. The National Infrastructure Protection Centre in the UK exchanges information with private companies that are responsible for important information infrastructure [23]. The high quality of performance of these bodies' functions was confirmed by the high British rating in GlobalCybersecurityIndex (GCI) [24]. Informational interaction of individual reviews should also be organized at the level of the National Institute for Strategic Studies, which according to the legislation (Law of Ukraine "On the National Security of Ukraine", "On Basic Principles of Cyber Security of Ukraine") is responsible for scientific and methodological support of a comprehensive review of the security and defence sector.

The proper conduct of the above reviews is extremely important not only at the national level, but also at the local one. In particular, their results can be used for effective and high-quality deployment of smart cities in Ukraine, as the ability to protect the information rights of people depends on quality review and action plans for the implementation of their results. «Problem of respect for information rights of a person has become a common prerequisite for ensuring the cybersecurity of residents of smart cities. In our opinion, its implementation could be facilitated through the

implication of the following measures by the authorities of the Council of Europe member states and businesses as recognition the ensuring of cybersecurity for smart cities at the level of national cybersecurity strategies, non-observance of fundamental human rights as a significant threat to cybersecurity of the residents of smart cities; as approval by the authorized central executive body of the national standard of cybersecurity of smart cities and formation of components of smart cities IT infrastructure based on the principle of providing cybersecurity to the residents of smart cities» [25] .

Despite this multitude of possible synergies between separate cybersecurity reviews, none of them have been effective so far. Therefore, taking into account organizational changes in cybersecurity, in particular the foundation of the Ministry of Digital Transformation of Ukraine with the subordination of the State Service for Special Communications and Information Protection of Ukraine, it is necessary to clarify their powers, primarily by making appropriate changes to the Laws of Ukraine "On State Service for Special Communications and Information Protection of Ukraine", "On the basic principles of cybersecurity of Ukraine" [26] and "On the national security of Ukraine", including the legal mechanism for review of cyber security of state information resources and critical information infrastructure, in particular, the mechanism of interaction of such reviews on cybersecurity issues (defense review, review of cyber security of critical information infrastructure, state information resources and information, the protection of which is required by law, review of the national anti-terrorism system, review of intelligence agencies, review of public security and protection), and in general the mechanism of formation and implementation of the Cyber Security Strategy of Ukraine. There is a nessecity to determine National Coordination Center for Cyber Security of Ukraine as a main coordinator of these reviews.

In the context of the practical implementation of these changes, an important problem that needs to be addressed is the regulatory definition of criteria for the delimitation of competences of authorized entities. In our opinion, such criteria may include the tasks of activity of authorized subjects of power, direct connection of their powers with legal instruments, that are used for the objectives of organization and preparation of reviews, in particular: normative regulation, monitoring of cybersecurity, requests for official information, review of critical infrastructure objects, etc. At the same time, an important condition for further implementation of the above recommendations is to ensure that the managers of public registers and information and telecommunication systems perform functions of expertise and technical examination of the relevant category of information objects in order to form reviews, conduct their proper technical, managerial and security audits, to establish their ability to withstand possible cyberthreats and cyber attacs.

Unlike all other reviews (complex and its separate components), which are defined either directly in the Law of Ukraine "On the national security of Ukraine" or in the relevant procedures for carrying out separate reviews, the legislation does not provide a clear definition of both "examination of the state of cyber-protection of state information resources and critical information infrastructure" and "review of the national cybersecurity system", which is provided for in the subparagraphs below. Article 8.3 of the Law of Ukraine "On basic principles of cyber security in Ukraine" and the current Cyber Security Strategy of Ukraine, as well as their interrelationship.

There are two main approaches regarding the understanding of the relationship between these inconclusive terms, but according to the National Security Strategy of Ukraine, in order to form the Strategy of Cyber Security of Ukraine it is necessary to conduct either appropriate reviews or consider "reviews of the state of cybersecurity of state information resources and critical information infrastructure is "a component of a more general" considering the national system of cybersecurity". According to the first approach, these timelines are considered to be identical, i.e. different laws refer to the same review procedure differently. In our opinion, this approach is not justified, primarily because these reviews, in accordance with the Law of Ukraine "On basic principles of cyber security of Ukraine", cover mainly the objects of review that are different in scope and function. Thus, the main objects of the review of the national cybersecurity system are the following:

- constitutional human and civil rights and freedoms;
- society, sustainable development of information society and digital communication environment;
- the state, its constitutional system, sovereignty, territorial integrity and inviolability;
- national interests in all spheres of life of an individual, society and state;
- objects of critical infrastructure.

The objects of cyberdefence are defined by the above Law of Ukraine:

- Communication systems of all forms of ownership where national information resources are processed and/or used in the interests of government bodies, local authorities, law enforcement agencies and military units established in accordance with the law;
- objects of critical information infrastructure;
- communication systems subjected to meet public needs and/or implement legal relations in the areas of e-government, e-government services, e-commerce and electronic document management.

The comparison of these sets of objects shows that the second list is an integral part of the first one, where objects of critical infrastructure incorporate objects of critical information infrastructure, and communication systems are important elements of the organizational and technical system of the state, as well as objects of critical infrastructure.

The same can be applied to the actors of ensuring these procedures. The list of cybersecurity actors is clearly defined by legislation and systematically presented in the form of a hierarchical model of three interacting lists of cybersecurity participants: a list of participants at the national level of coordination (the President of Ukraine, the National Security and Defense Council of Ukraine, the National Coordination Center for Cyber Security of Ukraine, the

Cabinet of Ministers of Ukraine), a list of actors that directly implement measures to ensure cybersecurity within their competence.

The list of cybersecurity actors is not specifically defined by legislation, but its model also has a hierarchical structure and covers the same upper parts of the list of actors, and in the model of lists of cybersecurity actors. The lowest link of this list of actors, based on their functions, including the State Service for Special Communications and Information Protection of Ukraine with the State Center for Cyber Defence and the Government team for response to computer emergency events in Ukraine CERT-UA subordinated to it.

Therefore, according to the second approach, it is considered that the relationship between the above procedures and concepts is characterized by a ratio of general and private, where "review of the state cyberdefense of State information resources and critical information infrastructure" should be considered as an integral specific technical and technological component of a more general procedure, namely "review of the national system of cyber security". Other components of " review of the national system of cybersecurity" are aimed at assessing the state of readiness of the cybersecurity system. That inplies the readiness of its main subjects in the national system of cybersecurity to carry out their tasks, including combating cybercrime, cyberterrorism, cyber espionage, military aggression in cyberspace (cyberdefence), execution of intelligence activities addressing threats to Ukraine's national security in cyberspace, and the like. Their evaluation should be carried out within the framework of the abovementioned reviews in order to assess the state of cybersecurity in the relevant areas.

The Act “On the basic principles of cybersecurity in Ukraine” defines the terms “cybersecurity” and “cyberdefence”, their objects and subjects, the concept of the national cybersecurity system, its main subjects, their objectives and the ways of ensuring the efficient functioning of the system. Analysis of these principles makes it possible to assert that cyberdefence is part of a more general concept of cybersecurity. According to the Law of Ukraine "On basic principles of cybersecurity of Ukraine", cyberdefence is mainly limited to measures of cryptographic and technical protection of information resources, cyberdefence of objects of critical information infrastructure, cyber security as protection of vital interests of a person and citizen, society and state in the use of cyberspace, which ensures sustainable development of information society and digital communication environment, timely identification, prevention and neutralization of real and potential threats to Ukraine's national security in cyberspace and "cyber defence - a set of organizational, legal, engineering and technical measures, as well as measures of cryptographic and technical protection of information aimed at preventing cyberincidents, detection and protection against cyberattacks, elimination of their consequences, restoration of stability and reliability of communication and technological systems", that also means that cybersecurity is more general concept than cyberdefence.

Lack of definition or ambiguity of these terms makes it difficult and hinders the development of such reviews and realisation of the action plan of its implementation.

It should be noted that in Ukraine the legislative base on cyber security and cyber defence has been created in general. It has a hierarchical structure and is in permanent dynamic development, trying to meet modern global tendencies, new challenges and threats in this sphere, the needs and requirements of citizens, society and state, international obligations of Ukraine on reliable protection of vital interests of a person and citizen, society and state in cyberspace. Such process is also being observed in other countries, first of all in the EU, the USA, Canada [23].

In previous studies, it was proposed to define "review of the state of cyberdefense of state information resources and critical information infrastructure" [27] as a procedure for periodic observation, measurement, analysis and evaluation of the state and readiness of cyberdefense of critical information infrastructure, information and telecommunication systems, that process and store information resources and information, the protection requirement for which is established by law; as well as information regarding surveillance of the state of cyberdefense - active, systematic, purposeful, and study of the real state of cyberdefense aimed at prevention of cyber-incidents, detection, prevention and suppression of cyberattacks, liquidation of their consequences, the ability of critical information infrastructure to restore their operation after cyberattacks and cyberincidents.

There is a requirement to legislatively regulate the relationship to ensure cybersecurity of cyberdefense actors and owners (managers) of critical information infrastructure objects at the prevention, detection and suppression of cyberattacks and cyberincidents, as well as during the elimination of their consequences that should be formalized in the State Service for Special Communications and Information Protection of Ukraine. The draft resolution of the Cabinet of Ministers of Ukraine "On approval of the Protocol of joint actions of the main subjects of cybersecurity, subjects of cyberdefence and owners (managers) of critical information infrastructure objects at the prevention, detection and suppression of cyberattacks and cyberincidents, as well as during the elimination of their consequences" was developed but was not approved. The absence of this document significantly reduces the effectiveness of the state policy to ensure cybersecurity.

However, the state policy on cybersecurity has made significant progress over the past five years, and as of 2020, it contains a number of important pieces of national legislation - Constitution of Ukraine, laws of Ukraine "On information", "On national security of Ukraine", "On basic principles of cybersecurity of Ukraine", "On information protection in information and telecommunication systems", "On electronic trust services", "On protection of personal data", etc., as well as by laws approved by the President of Ukraine and the Government, in aprticilar the law “On the national security strategy of Ukraine, On the concept of development of the security and defense sector of Ukraine; On the strategic defense bulletin of Ukraine, On the national coordination center for cyber cecurity, On the threat to the state cybersecurity and urgent measures to neutralize it, on some issues of organization of interdepartmental information exchange in the National System of Confidential Communication, On approval of the Concept of creation of the state

system of protection of critical infrastructure [29], On approval of the General requirements to cyber protection of objects of critical infrastructure.

Ukraine's international obligations in this area consist primarily of the Budapest Convention (Convention on Cybercrime of the Council of Europe), ratified by Ukraine in 2005. An extremely important international document in this area is the Directive on security of network and information systems (NIS Directive or The Directive on security of network and information systems), adopted by the European Parliament in 2016, which provides for a number of organizational, legal and communication measures aimed at improving the overall level of cybersecurity in the EU [28]. Although the NIS Directive is not binding on Ukraine as a non-EU member state, its basic provisions are useful for the development of the national public policy and administration in cybersecurity and cyber protection.

The Constitution of Ukraine defines national values that are transformed into national interests - the vital interests of an individual, society and the State, the implementation of which ensures the State sovereignty of Ukraine, its progressive democratic development, as well as safe living conditions and the well-being of its citizens as stated in Article 17. This is due to the proclamation in the norms of Art. 3 of the Basic Law of direct meaning of human rights and freedoms for determination of directions of state activity, determination of bases of its legal responsibility to the person for its activity. "Accordingly, as social values, human rights and freedoms not only determine the measure of possible (permitted) behavior, conditions of satisfaction of individual interests and needs in public legal relations, but also serve as a means of establishing the content and direction of state activity, determine the range of responsibilities of subjects of public administration objects, as well as reflect the criteria of social significance of specific values that must be protected by the state" [30, p. 136].

It is the Law "On basic principles of cybersecurity in Ukraine" that defines the main objects of cyberdefense that create the critical infrastructure of the country, normatively fixes the conceptual apparatus in cybersecurity at the highest level, regulates the principles of cybersecurity and the national system of cybersecurity, defines public-private cooperation in cybersecurity and establishes liability for violation of legislation in this sphere and control over the legality of measures to ensure cyberdefense [26]. This Law also defines the legal and organizational basis for ensuring the protection of the vital interests of individuals and citizens, society and the State, and the national interests of Ukraine in cyberspace; the main goals, directions and principles of State policy in the area of cybersecurity; the power of State bodies, enterprises, institutions, organizations, individuals and citizens in this area; and the basic principles for coordinating their activities to ensure cybersecurity.

The Law of Ukraine "On basic principles of ensuring cyber security of Ukraine" is a main framework document, it legally defines the key concepts in the field of cybersecurity and attempts, in our opinion, to allocate areas of responsibility of government agencies in the field of information protection, although a part of the Law simply translates the key provisions of the Cyber Security Strategy. The law determines the need to introduce a single (universal) system of indicators of cyber threats, taking into account international standards on cyber security and cyber protection.

Conclusions and recomendations

1. It is necessary to provide simultaneous development and mutually agree on the content of the amendments to the Law of Ukraine "On basic principles of ensuring cyber security of Ukraine" and the draft Law of Ukraine "On critical infrastructure facilities and their protection" should
2. It is necessary to amend the Law of Ukraine "On the fundamental principles of ensuring cyber security of Ukraine" regarding its detailed elaboration and specification of mechanisms for implementing public-private partnership in the sphere of cybersecurity and conducting reviews of cybersecurity and cyber defence.
3. To take into consideration the changes that have occurred in the field of cybersecurity, namely the emergence of the Ministry of Digital Transformation of Ukraine and subordination to it of the State Service for Special Communications and Information Protection of Ukraine, should be considered in the Laws of Ukraine "On the basic principles of cybersecurity in Ukraine", "On the national security of Ukraine", "On the state service for special communications and Information protection of Ukraine"
4.To consider, in accordance with paragraph 4 of Article 10 of the Law of Ukraine "On national security of Ukraine" the development of the "White Paper on Cyber Security" at least once every three years, as well as to transfer of this norm in the new version of the Law of Ukraine "On the basic principles of cyber security in Ukraine.
5. To develop and adopt a procedure for conducting "reviews of the national cybersecurity system" and "review of cybersecurity of state information resources and critical information infrastructure".
6. To adapt national cybersecurity legislation in line with the international cybersecurity legislation, primarily NIS Directive (The Directive on security of network and information systems).
7. To establish special panels in courts of general jurisdiction of Ukraine to consider cases related to IT and cyber security issues.
8. To develop and adopt the draft of the State Target Program on Cyber Security Development.
9. To harmonize international standards in cybersecurity sphere.
10. To codify, develop and adopt an Information Code of Ukraine (Information Code of Ukraine).
11. To adapt the existing infrastructure of public institutions to the requirements of cybersecurity, primarily with regard to the work of public servants with electronic means (e-mails, etc.), fixed and mobile communications, and use of the global Internet open segment.
12. To develop a mechanism for regular audits of critical infrastructure and the training and development programmes on cybersecurity for public services, authorized officials of enterprises - administrators of public registers and

information systems.
13. To develop, implement and update various educational programmes in higher education institutions on cyber security and cyber hygiene with round tables, international conferences and symposiums.
14. To stimulate the development of public-private partnership programs in the sphere of cybersecurity, including aspects of updating national information infrastructure, except for critical ones.

Compliance with ethical standards

The authors declare that all the data used in the research and analysis is in open access.

References

1.Decree of the President of Ukraine (2016). On the decision of the National Security and Defense Council of Ukraine dated On the Cyber Security Strategy of Ukraine. Government Courier (52).(in Ukrainian).
2.Decree of the President of Ukraine (2015) № 287. On the decision of the National Security and Defense Council of Ukraine On the National Security Strategy of Ukraine. Government Courier (95) (in Ukrainian).
3. BRANDOM, RUSSELL (2020). Former NSA chief Keith Alexander has joined Amazon's board of directors.
4. DOBBINS JAMES & SOLOMON RICHARD H. & CHASE MICHAEL S. et al (2015). Choices for America in a Turbulent World: Strategic. 5. SCHNEIER BRUCE (2008). Schneier on Security.
6. ALDRICH RICHARD J.& CORMAC RORY & GOODMAN MICHAEL S. (2013). Spying on the World: The Declassified Documents of the Joint Intelligence Committee.
7. SINGER PETER & FRIEDMAN A. (2014). Cybersecurity and Cyberwar.
8. PUYVELDE DAMIEN VAN & BRANTLY AARON (2019). Cybersecurity: Politics, Governance and Conflict in Cyberspace.
9. YUVAL SHANY & DAN EFRONY & MICHAEL SCHMITT (2018). The Tallinn Manual on Cyber Operations and the Laws of War: Towards Customary International Law.
10. BURIACHOK VOLODYMYR (2015). The impact of cyber security on the economic development of the world's leading countries and Ukraine. (4) P.29-43. (in Ukrainian).
11. HRYSHCHUK R. & OKHRIMCHUK V (2015). Formulation of the scientific tasks for the potentially dangerous patterns of cyberattacks development. (3) P.276-282. (in Ukrainian).
12. DOVHAN OLEKSANDR (2015). Information security as a guarantor of the national information resources safety. (2) P.130-134. (in Ukrainian).
13. MYALKOVSKY DANYLO (2017). Analysis of the subject area of identification and authentication. (191) P.120-127. (in Ukrainian).
14. STANISLAVSKYI TARAS (2019). State and improvement of planning of measures on implementation of the cyber security strategy of Ukraine. (4) P.99-103. (in Ukrainian).
15. MIKHAILOVA ALINA (2014). Cybersecurity problems in Russia and ways to solve them. (in Russian).
16. Decree of the President of Ukraine (2019) №225. On the decision of the National Security and Defense Council of Ukraine. On the organization of planning in the security and defense sector of Ukraine. Government Courier (92) (in Ukrainian).
17. DUBOV DMYTRO (2018). Public-private partnership in the field of cybersecurity: international experience and opportunities for Ukraine. Kyiv: NISD (in Ukrainian).
18. European Union Agency for Network and Information Security (ENISA). (2014) An evaluation Framework for National Cyber Security Strategies.
19. GREBENYUK MAXYM (2020) Some issues of organizational and legal support of cybersecurity: a review of best practices of foreign experience.(2) P.203-207.
20. Decree of the President of Ukraine (2019) № 558 On some measures to improve access of individuals and legal entities to electronic services. Government Courier (144) (in Ukrainian).
21. On National Security of Ukraine: Law of Ukraine (2018). Bulletin of the Verkhovna Rada of Ukraine. (31). - St. 241 (in Ukrainian).
22. ARDIELLI EVA, ARDIELLI JIŘÍ (2017) Cyber security in public administration of the Czech Republic.
23. European Information and Research Center (EIRC). (2016) Legislation and cyber security strategy in the European Union, USA, Canada.
24. Global Cybersecurity Index (2018).
25. PLESKACH MARIIA & ZAIARNYI OLEH & PLESKACH VALENTYNA (2020) Respect for Information Rights of a Person as a Condition for Cybersecurity of Smart Cities Residents.P. 759-764.
26. On the basic principles of cybersecurity of Ukraine: Law of Ukraine (2017). Bulletin of the Verkhovna Rada of Ukraine (45). - St.403 (in Ukrainian).
27. SEMENCHENKO ANDRII&MIALKOVSKYI DANYLO &STANYSLAVSKYI TARAS (2018). Scientific and methodological approaches to the review of cyber protection of state information resources and critical information infrastructure. Investments: practice and experience (18). P. 87-95. (in Ukrainian).
28. The Directive on security of network and information systems Avaibale from: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive(in English)[Accessed 15/03/2020].
29. The concept of creating a state system of critical infrastructure protection (2017) № 1009-r. Government Courier dated 10.01.2018-№ 5.(in Ukrainian).
30. ZAYRNYI OLEH (2017). Legal support of the development of the information sphere of Ukraine: administrative-tort aspect. Kyiv: Vidavnichyi dim Gelvetika (in Ukrainian)

About the authors:
Semenchenko A. I.,
Doctor of Science in Public Administration, Professor,
National Academy of Public Administration
under the President of Ukraine
Andrii.Semencenko@gmail.com
ORCID ID 0000-0001-6482-3872

Pleskach V.L.,
Dr. Habil. (Economics)
Candidate of Technical Sciences,
Head of the Department of Applied Information Systems
Faculty of Information Technologies
Taras Shevchenko national University of Kyiv
v_pleskach@ukr.net
ORCID ID 0000-0002-4700-6704.

Zaiarnyi O.A, Doctor of Law, Associate Professor
Institute of Law
Taras Shevchenko national University of Kyiv
ORCID ID
e-mail: oleganalitik.knu@gmail.com

Pleskach M.V, postgraduate sdudent
Taras Shevchenko national University of Kyiv
pleskachmarija@gmail.com
ORCID ID 0000-0003-3296-5475.