АВАНЕСОВА Н.Е.
d-r екон. наук, професор
завідувач кафедри менеджменту та публічного адміністрування
Харківський національний університет будівництва та архітектури
вул. Сумська, 40, м. Харків, 61002
E-mail: avanesova.science@gmail.com
ORCID: 0000-0003-3636-9769

СЕРГІЄНКО Ю.І.
аспірант кафедри економіки та бізнесу
Харківський національний університет будівництва та архітектури
вул. Сумська, 40, м. Харків, 61002
E-mail: sergiienko.science@gmail.com
ORCID: 0000-0001-9957-3631

ЛЮБУШИН Р.А.
аспірант кафедри економіки та бізнесу
Харківський національний університет будівництва та архітектури
вул. Сумська, 40, м. Харків, 61002
E-mail: phd.nauka@gmail.com
ORCID: 0000-0001-7896-6524

ЗМІЩЕННЯ КІБЕРОБОРОНИ ДЕРЖАВИ І СТВОРЕННЯ КІБЕРВІЙСЬК: СТАН, ПРОБЛЕМИ ТА ОРГАНІЗАЦІЙНО-ЕКОНОМІЧНІ ЗАХОДИ ДЛЯ УКРАЇНИ


Кібероборона - сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненю збройного конфлікту та відсіч збройної агресії (пункт 10 статті 1).

Мета та завдання. Метою статті є визначення наукових засад забезпечення зміцнення кібероборони держави та створення кібервійськ. Організація ефективної кібероборони держави потребує вирішення цілієї низки важливих завдань і в першу чергу усунення прогалин у нормативно-правовій базі. Прикро визнати, що до цього часу законодавством України не визначено основи кібероборони, насамперед мета, цілі, принципи та завдання кібероборони, її суб'єкти і об'єкти, побудова, підготовка та ведення такої оборони, а також відповідні повноваження органів державної влади, основні функції та завдання органів військового управління, інших державних органів, обов'язки посадових осіб, права та обов'язки громадян України тощо. І це, на нашу думку, унеможливлює адекватне визначення завдань кібервійськ, які повинні відігравати провідну роль у
Topicality. In the last decade, cyberspace has become the fifth separate, specific and important area of armed struggle, along with four traditional ones - "Earth", "Sea", "Air" and "Space". The use of cyber troops and cyber weapons, cyber defense, cyber operations and cyber-attacks is now considered commonplace. Since 2014, Ukraine has been forced to repel hybrid Russian armed aggression, including in cyberspace. But the recognition of cyber defense as a new important component of its defense took place only in March 2016 in the Cyber Security Strategy of Ukraine [1] (hereinafter - the Strategy). At the same time, it states, in particular, that "The basis of the national cybersecurity system will be the Ministry of Defense of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Police of Ukraine, the National Bank of Ukraine."

The Strategy also for the first time for the Ministry of Defense of Ukraine (Ministry of Defense) and the General Staff of the Armed Forces of Ukraine (General Staff of the Armed Forces) identified additional new main tasks, namely: measures to prepare the state to repel military aggression in cyberspace; military cooperation with NATO related to cyber security and joint protection against cyber threats; Ensuring in cooperation with the State Service for Special
Communications and Information Protection of Ukraine and the Security Service of Ukraine cyber protection of its own information infrastructure.

Cyber defense - a set of political, economic, social, military, scientific, scientific and technical, informational, legal, organizational and other measures carried out in cyberspace and aimed at protecting the sovereignty and defense capabilities of the state, preventing armed conflict and repelling armed aggression.

Aim and tasks. The purpose of the article is to determine the scientific basis for strengthening the state’s cyber defense and creating cyber troops. The organization of effective cyber defense of the state requires the solution of a number of important tasks and, first of all, the elimination of gaps in the regulatory framework. It is unfortunate to recognize that so far, the legislation of Ukraine does not define the basics of cyber defense, especially the purpose, goals, principles and objectives of cyber defense, its subjects and objects, construction, preparation and conduct of such defense, as well as the relevant powers of public authorities, functions and tasks of military administration bodies, other state bodies, responsibilities of officials, rights and responsibilities of citizens of Ukraine, etc. And this, in our opinion, makes it impossible to adequately define the tasks of cyber troops, which should play a leading role in the implementation of cyber defense tasks and should be created to implement the aforementioned decision of the President of Ukraine.

Research results. Modern challenges and integrated threats to peace and stability have given rise to new approaches to practice cooperation in the field of cyber defense.

The community has arrived agreement that only by joint efforts and on the basis of international law can security be resolved problems of the global information environment in the context of countering the latest information threats.

Therefore, the need for policy research is obvious cyber defense of organizations introduced recently, practical consideration of new documents and decisions on their institutional support and implementation in the activities of member states.

Conclusion. The transformation of the information paradigm of global development, which is a reflection of new patterns of formation of the modern system of international relations, testifies to the innovations of international cooperation in the field of information and communication and accordingly needs to improve policies for international peace and stability. Modernization of international information security policies is determined by their ability to ensure a multilateral dialogue of international actors, take into account the different positions of global actors in combating the latest information threats and act in accordance with their statutory powers as universal international platforms for consensus on current security issues.

Keywords: defense, cyber defense, cyber security, cyber military, state, measures, strategy, resources, Ukraine, war, martial law, development, armed aggression, cyber resilience of the country

Problem statement and its connection with important scientific and practical tasks. The main foreign policy priority of Ukraine in the field of cybersecurity is to deepen European integration processes by unifying approaches, methods and means of cybersecurity with established EU and NATO practices, taking other measures agreed with key foreign partners to strengthen Ukraine's cyber resilience and interests in cyberspace. Ukraine will pay special attention to joint counter-terrorism with partners, detection, prevention and cessation of crimes against peace and security of mankind, other illegal actions violating international law and order and interests of the democratic world community, will develop on a contractual basis information and experience on ensuring national security in cyberspace, will use the best world practices, will actively implement other joint activities that will help strengthen the scientific, logistical base and human resources in the field of cybersecurity. Ukraine will work with international partners, organizations and other stakeholders who share our shared vision of the future of cyberspace as global, open, free, stable and secure, based on respect for human rights, fundamental freedoms and democratic values, which is the key to socio-economic and political development of Ukraine. Ukraine will continue to actively participate in the international dialogue on responsible behavior of states in cyberspace based on compliance with the principles of international law, the UN Charter, as well as voluntary non-binding norms, rules and principles of responsible state behavior. This will require greater coordination and consolidation of stakeholders in international forums, in which Ukraine will be not only a participant but also an initiator and organizer. Given that the Internet has long been a public domain, significantly beyond purely national interests, the state will support the multi-stakeholder (multilateral) model of Internet governance, promoting international, regional and national discussions on this issue, promoting private sector involvement, scientific and educational circles, civil society. Attempts by some authoritarian states to sovereignty the Internet run counter to Ukraine's long-term interests and its model of socio-economic development.

Ukraine will promote further compliance with international human rights law and standards, encourage the application of best practices, and intensify its efforts to prevent the misuse of new technologies. To this end, the state will intensify its participation and partnership in international processes of standardization and certification in the field of cybersecurity, expand its representation in international,
regional and other standardization bodies, organizations involved in the development of standards and certification in this area. In developing standards in the areas of new technologies (including artificial intelligence, cloud technologies, quantum computing and quantum communications) and the basic architecture of the Internet, Ukraine assumes that the Internet must remain global and open, technology must be human-centered and ensure basic freedoms, to guarantee non-interference in her private life, to ensure her confidentiality in cyberspace, and any restrictions in this part should be carried out only in accordance with the law.

The use of technology must be legal, safe and ethical. At the same time, due to the complexity of international security in cyberspace, Ukraine will take a more active position in UN discussions and other international forums to promote, coordinate and consolidate its position in cyberspace, reducing the dangers of militarization of cyberspace. Given the interconnectedness of modern cyberspace and in order to develop cooperation between the state, the private sector, academia and civil society in the field of cybersecurity, Ukraine will develop national cyberspace as a global, open, free, stable and, above all, secure, which is the key to successful development of the country. During the implementation of the Strategy, Ukraine will make cybersecurity one of the main issues of its international activities, strengthening the potential of its foreign policy structures and the cyber potential of the state. To this end, Ukraine will develop a network of cybersecurity partnerships, building on existing and creating new formats and mechanisms for international cooperation.

**Analysis of recent publications on the problem.** Before studying the problem of information security. In the international dimension, such well-known foreign experts as M. Libitski [3], F. Hoffman [4], J. Nai-mol. [3], A. Sebrowski, J. Garstka [4], etc., who developed the latest theories of force, theories new generation information wars and the use of information weapons in international conflicts. Common and different characteristics have also been identified in scientific papers information security, which are formed in the system of global and regional relations, analyzed tools of information and cyber threats to the international security system, considered international cooperation on information security at the level of international organizations and leading countries of the world, the institutional principles of international information security are clarified. Domestic scientists E. Makarenko [5], M. Ryzhkov [5], O. Frolova [5], G. Pocheptsov [7], M. Ozhevan [8], etc. developed theoretical positions on the problem of international cooperation in the field of information security, determined the factors of political activity of international institutions in the context of global developments, described international mechanisms to counter new challenges for the international security system.

**Allocation of previously unsolved parts of the general problem.** The priority for Ukraine is to develop and implement indicators of the state of cybersecurity on the basis of systematic monitoring of detection and forecasting of cyber threats, which will allow to record the achievements or shortcomings in the functioning of the cybersecurity system.

In addition, an integrated evaluation system for the latest will be developed technologies that directly affect the cyber resilience of the state, the creation of tools (standards, protocols, certificates, etc.) to assess the effectiveness of the latest technologies to combat cyber-attacks.

The effectiveness of the implementation of the Strategy will be determined through constant monitoring of its implementation and based on a clear system of indicators of the state of cybersecurity, which will be developed during the first year of implementation of the Strategy.

Indicators should measure the progress made by actors ensuring cybersecurity in the implementation of the Strategy on such issues as: implementation of strategic tasks within the goals set by the Strategy (for each task); achieving the strategic goals set by the Strategy (for each goal); the degree of influence of the measures implemented within the Strategy on national cybersecurity system and digital transformation of the state.

The introduction of cybersecurity indicators will improve the process of monitoring the implementation of the Strategy in real time using modern web resources (online platforms), transparency of measures taken for society and the state.

Strengthening the impact of the national cybersecurity system for social development will be determined by the following criteria: increasing the level of public confidence in the state on security cyberspace; formation of a secure information society in which to take action cybersecurity in addition to public institutions involved private entities and citizens; positive impact on the protection of national interests in the field of cybersecurity. As an example, the level of influence on the development of the situation related to aggression Of the Russian Federation against Ukraine).
The state will be determined by means of an extensive system of indicators achieving conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state.

**Formulation of research objectives (problem statement).** In the framework of this study, it is advisable to make a number of goals and directions that are relevant to reflect in the study: the fight against Russian aggression and efforts to strengthen defense capabilities and restore the territorial integrity of the state; deployment and launch of anti-corruption infrastructure; introduction of effective mechanisms of social policy of the state by optimizing the pension system, initiating medical and educational reforms; entry of the country's economy on the rails of dynamic growth, attracting investment and innovation in domestic production, opening access to new markets, increasing employment and welfare; strengthening Ukraine's authority in the international arena, deepening partnerships with the EU and NATO, defining clear guidelines for our European and Euro-Atlantic integration; overcoming domestic political instability; strengthening of national identity, consolidation of the whole society around the idea of Ukrainian independence and readiness to build a common future for themselves and their descendants on their native land.

**An outline of the main results and their justification.** According to the decision of the National Security and Defense Council, the Cabinet of Ministers of Ukraine has an urgent need to create cyber troops in the system of the Ministry of Defense of Ukraine and acquire the appropriate capabilities to calculate the needs for:
- the amount of material, technical and financial resources needed to create and ensure the proper functioning of cyber troops;
- staffing of cyber troops, taking into account the optimal ratio of servicemen, employees of the Ministry of Defense of Ukraine, as well as enlisted in the reserve, reservists and other categories of persons.

Based on the results of calculations within two months, the Cabinet of Ministers must develop and submit to the Verkhovna Rada of Ukraine a bill on the establishment and operation of cyber troops in the system of the Ministry of Defense of Ukraine.

On August 26, 2021, the President also signed a decree approving Ukraine's cybersecurity strategy.

On May 14, 2021, the National Security and Defense Council supported the creation of cyber troops in Ukraine and adopted a strategy for the development of cybersecurity for the next 5 years.

Ukraine seeks to create the most open, free, stable and secure cyberspace that respects human rights and freedoms and supports social, political and economic development.

Implementing the Cyber Security Strategy of Ukraine for 2017 - 2021, the state was able to form the core of the national cyber security system. Ukraine has built up the potential that allows it to further build its national cybersecurity system on the basis of deterrence, cyber resilience, and interaction.

To this end, Ukraine will: strengthen the capacity of the national cybersecurity system to prevent armed aggression against Ukraine in cyberspace or with its use, neutralize intelligence and subversive activities, minimize the threat of cybercrime and cyberterrorism (deterrence); will be able to quickly adapt to internal and external threats in cyberspace, will support the sustainable functioning of the national information infrastructure, especially critical information infrastructure (cyber resilience); ensure the development of communication, coordination and partnership between cybersecurity actors at the national level, development of strategic cybersecurity relations with key foreign partners, especially with the European Union and NATO and their member states, cooperation in this field with other states and international organizations based on the national interests of Ukraine (interaction).

Building a national cybersecurity system on such a basis will make it possible to extend the proposed and recommended actions to all sectors of the economy and areas of activity. To this end, the state will involve a wide range of cybersecurity actors, including business entities, in addition to the main actors of the national cybersecurity system, which relied on at the initial stage of formation of the national cybersecurity system, public associations and individual citizens of Ukraine.

The National Cyber Security Coordination Center will play a key unifying and coordinating role in this process.

The state will build a national cybersecurity system based on:
- comprehensive understanding and analysis of the digital environment, global trends in the cybersecurity environment (while taking into account the specifics of our country), strict protection of Ukraine's national interests in the field of cybersecurity;
- permanence of measures to improve cybersecurity legislation and speed of action to update it in accordance with changing security conditions;
- focus on society, which will contribute to its economic and social growth;
- use of the principle of minimum sufficiency of the role of the state in the processes of development and security of cyberspace, setting requirements (rules, guidelines) for the safe use of the Internet;
- balanced provision of state needs and citizens' rights, observance of law, procedural guarantees and remedies, respect for fundamental values, human and individual rights to freedom of expression, and protection of universally recognized fundamental rights online as well as offline;
- condemning the practice of exceeding the established limits of the need to restrict the rights of citizens and legal entities when using cyberspace and ICT technologies; openness and creating conditions for the active participation of all stakeholders, taking into account their needs and commitments in an environment where cybersecurity of the digital environment has become paramount for the state, society and citizens;
- defining clear roles, needs, responsibilities in solving cybersecurity tasks of varying complexity, applying incentives and sharing unique knowledge and experience; risk-oriented approach in terms of cybersecurity and cybersecurity measures;
- cooperation and inclusive dialogue of all actors in cybersecurity, in particular within the framework public-private partnerships, in order to achieve strategic goals, establish initiatives, develop agreed plans and projects in the field of cybersecurity;
- implementation of modern principles, methods, approaches and mechanisms of public administration in the field of cybersecurity, including those based on strategic planning and management, crisis management, partnerships between government, business and society; balanced allocation of available material and financial resources, as well as optimal use of levers such as legislation, standardization, educational programs, mechanisms to promote and strengthen trust, exchange of information and best practices to address each specific task in the field of cybersecurity;
- proactive approach, which involves the implementation of preventive measures, including the use of cyber-attack prevention systems, shifting the organizational and technological focus from countermeasures to countering cyber-attacks in the early stages;
- ensuring democratic civilian control over the functioning of the national cybersecurity system, namely compliance with the Constitution and laws of Ukraine by cybersecurity actors, the implementation of strategic documents, concepts, government programs and plans in the field of cybersecurity, resource efficiency, including budget funds.

Accelerated development and interpenetration of information technologies, along with powerful socially significant benefits, is accompanied by scaling of cyber threats to all spheres of life, their evolution towards high-tech solutions and diversification of implementation tools. Ukraine has the necessary capacity to build cybersecurity capabilities to adequately address today's challenges and threats.

Challenges for Ukraine in the field of cybersecurity are:
- active use of cyber tools in international competition for world leadership, competitive nature of cybersecurity development and implementation of cyber threats in the process of rapid progressive changes in information and communication technologies, cloud computing, 5G networks, 5G networks, big data, Internet of Things, machine learning / artificial intelligence (AI), etc.;
- the militarization of cyberspace and the growing technological capabilities of cyber weapons, which enable the enemy to conduct covert cyberattacks and cyber operations, remote control of control systems, damage and destruction of critical information infrastructure;
- increasing the technological level of illegal encroachments on the interests of the state, society and individuals with the use of social engineering methods, the use of artificial intelligence technologies and cryptotechnologies;
- impact on economic activity and social behavior of the spread of the COVID-19 pandemic, which led to the rapid transformation and organization of a significant segment of public relations remotely with extensive use of electronic services and information and communication systems.

This has exacerbated the threat of violations of citizens' rights when using cyberspace.

Digital transformation, which is one of the priorities of Ukraine's development, creates new challenges in the field of cybersecurity. The introduction of new technologies, digital services and mechanisms of interaction between citizens and the state, including the electoral process, creates a large number of hidden relationships at the level of technology and processes. Without a systematic approach to cybersecurity and risk assessment, there is a likelihood of losing public confidence in the process of digital transformation.

Current global trends in the development of the cybersecurity environment, challenges for the country, internal processes and phenomena have formed such threats to Ukraine's cybersecurity. Since 2014, Russia has been actively using cyberspace in hybrid aggression against Ukraine by exerting destructive influence on
public authorities, military and military command and control systems, and critical infrastructure. The aggressor state is constantly increasing the arsenal of cyber weapons for offensive, reconnaissance and subversive purposes, the use of which can cause irreparable, irreversible destructive consequences. These factors require a steady increase in cybersecurity capabilities of the security and defense sector. Extremely relevant threats today are intelligence and subversive activities in cyberspace against Ukraine, which are related to the intelligence services of foreign countries, primarily the Russian Federation, intelligence activities to steal information (cyber espionage) and subversive actions to disrupt the regular operation of critical facilities information infrastructure, especially government systems, livelihoods, electricity, transport, nuclear and chemical industries, banking (cyber-sabotage acts).

The threat of cyberterrorism has increased significantly in Ukraine in recent years. First of all, this is due to the cyber capabilities of the aggressor state of the Russian Federation, which is waging a cyber war against Ukraine with the use of cyber weapons.

Incomplete measures to implement the organizational and technical model of cybersecurity, which will meet current threats, challenges in cyberspace and global trends in the cybersecurity industry; lack of a system to increase the digital literacy of citizens and the culture of safe behavior in cyberspace, raising public awareness of cyber threats and cyber defense.

The priorities of ensuring cybersecurity of Ukraine are: securing cyberspace to protect the sovereignty of the state and the development of society; protection of the rights, freedoms and legitimate interests of the citizens of Ukraine in cyberspace; European and Euro-Atlantic integration in the field of cybersecurity. The formation of a new quality of the national cybersecurity system requires a clear and understandable definition of strategic goals to be achieved during the implementation of the Strategy.

To build the capacity of deterrence (C) by 2026 we must achieve the following strategic goals:

Goal C.1. Effective cyber defense. Ukraine must not only create and develop effective (including personnel and technology) units with the authority to conduct armed conflict in cyberspace, but also to form an appropriate legal, organizational, technological model of their operation and application, which is impossible without: effective interaction of key actors national cybersecurity system and defense forces during cyber defense activities, proper training and financial support of such structures, systematic cyber training, assessment of capabilities and effectiveness of units, development and implementation of indicators to assess their performance.

Goal C.2. Strengthening capabilities in countering intelligence and subversive activities in cyberspace and cyberterrorism. Ukraine will ensure the continuous implementation of counterintelligence measures to detect, prevent and stop intelligence and subversive activities of foreign states, acts of cyber espionage and cyberterrorism, eliminate conditions conducive to them and the reasons for their occurrence to protect the interests of the state, society and individuals.

Goal C.3. Capacity building in the fight against cybercrime. Law enforcement and special purpose agencies with law enforcement functions will gain the capacity to minimize the threat of cybercrime, strengthen their technological and human resources for preventive measures and investigation of cybercrime.

Goal C.4. Development of asymmetric containment tools. We will create the necessary conditions to ensure the deterrence of aggressive actions in cyberspace against Ukraine through the use of economic, diplomatic, intelligence measures, as well as attracting the potential of the non-governmental sector.

To achieve cyber resilience (K), the national cybersecurity system must achieve the following strategic goals by 2026:

Purpose K.1. Strengthening national cyber readiness and cyber defense. Introduce and implement clear and understandable for all stakeholders’ measures to strengthen national cyber readiness in the interests of ensuring economic well-being and protecting the rights and freedoms of every Ukrainian citizen. Cyber preparedness is the ability of all stakeholders, especially the security and defense sector, to respond to cyber-attacks in a timely and effective manner, to ensure continued preparedness for real and potential cyber threats, to identify and eliminate the preconditions for their occurrence, thus ensuring cyber resilience, especially critical information infrastructure.

Purpose K.2. Professional development, cyber-knowledge society and scientific and technical support of cybersecurity. Carry out a radical reform of the system of training and retraining of specialists in the field of cybersecurity. Ensure that the existing qualified human resources of cybersecurity entities are maintained. Stimulate research and development in the field of cybersecurity, taking into account the emergence of new cyber threats and challenges, the creation of national information systems, platforms and products. Domestic scientific and technical potential will be primarily involved in solving the problems of cybersecurity of the
state. Cybergenic, digital skills, cyber awareness of and response to modern cyber threats should become an integral part of the education of every Ukrainian citizen.

Purpose K.3. Secure digital services. We will achieve a balance between the needs of Ukrainian society, the domestic market, the state economy and the need to ensure security in cyberspace. We will ensure the reliability and security of digital services from the moment of creation and throughout their life cycle.

Interaction (B) will be improved by achieving the following strategic goals by 2026:

Goal B.1. Strengthening the coordination system. The state will create conditions for effective cooperation of cybersecurity actors in the process of building and functioning of the national cybersecurity system, as well as for effective joint actions in preventing, repelling and neutralizing the consequences of cyber-attacks and cyber incidents. We coordinate the activities of all stakeholders to overcome cybersecurity crises.

Goal B.2. Formation of a new model of relations in the field of cybersecurity. We will introduce a service model of state participation in cybersecurity measures, in which the state will be perceived not as a source of requirements, but as a partner in building a national cybersecurity system.

Goal B.3. Pragmatic international cooperation. We focus our relations with international partners both on the development of mutual trust for joint response to cyber-attacks and overcoming cyber security crises, and on purely practical cooperation: exchange of information on cyber-attacks and cyber incidents, joint cyber operations and investigation of international cybercrimes, regular cybercrimes, regular cybercrime experience and best practices.

Strengthening the capacity of the national cybersecurity system is carried out by fulfilling strategic objectives aimed at achieving certain goals. On the basis of deterrence: Ukraine will form a system of effective cyber defense by (goal C.1):

- formation of a separate type of troops within the Armed Forces of Ukraine - cyber defense forces, providing it with adequate financial, human and technical resources to deter armed aggression in cyberspace and repel the aggressor; introduction of effective mechanisms of interaction between the main actors of the national cybersecurity system and the defense forces in terms of joint implementation of cyber defense tasks; ensuring constant monitoring of electronic communications networks and information resources of the "ua" domain, analysis of intrusions on these networks and resources, as well as real-time detection of anomalies in their functioning; development and implementation of the cyber defense plan as an integral part of the Defense Plan of Ukraine;
- conducting joint thematic exercises at least twice a year with relevant units of NATO member states to achieve interoperability; creation of MIL.CERT-UA in the interests of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine, establishing on a permanent basis cooperation with the European Military CERT-Network (Military CERT-Network);
- ensuring the assessment of the capabilities of the security and defense sector in terms of joint implementation of cyber defense tasks, in particular during defense and cyber security reviews;
- introduction into the system of military-patriotic education and the system of territorial defense of training programs for the preparation and conduct of practical exercises in the field of cybersecurity.

Ukraine will ensure effective counteraction to intelligence and subversive activities in cyberspace and cyberterrorism by (Objective C.2):

- creation in accordance with the approved conceptual framework of the national system of detecting cyberattacks, combating acts of cyberterrorism and cyber espionage on critical information infrastructure designed to monitor cyberspace for timely detection, prevention and neutralization of cyber threats and scalability, and operational response;
- improving the analytical and forensic support of counterintelligence protection of cybersecurity of the state through the introduction of innovative methods of processing and evaluation of digital data, the formation of electronic evidence; ensuring maximum coverage of critical infrastructure facilities by secretly checking the state of their readiness for possible cyber-attacks and cyber incidents in order to prevent the elimination of preconditions for the implementation of cyber threats;
- ensuring constant monitoring of the development of cyber capabilities of international terrorist groups, aimed at timely detection and neutralization of real and potential threats of acts of cyberterrorism in Ukraine;
- strengthening counterintelligence protection in the field of electronic communications, IT industry, the environment affiliated with them, aimed at detecting, preventing and stopping intelligence and subversive encroachments of foreign intelligence services on national security of Ukraine in the field of cybersecurity;
- creation of technological capabilities for automatic detection of cyber-attacks in real time in the data flows of national information and communication systems and individual critical infrastructure, their blocking and prioritization; improving the legal, organizational and personnel support of the national system of combating terrorism in the part related to the involvement of law enforcement agencies in the implementation of measures to prevent, detect and stop acts of cyberterrorism.

- Ukraine will strengthen its capacity to combat cybercrime (goal C.3), for this purpose it is necessary to: audit the implementation of the provisions of the Cybercrime Convention into Ukrainian legislation and complete this process by making the necessary changes to the laws of Ukraine; to regulate the issue of electronic evidence at the legislative level, using the best practices and approaches of EU member states on these issues; to improve the legislation of Ukraine, providing for the necessary changes taking into account current challenges and trends in the field of cybersecurity;

- Introduce a nationwide awareness-raising campaign on citizens’ actions in the face of cyber-fraud, the distribution of malicious software or pornographic content, and other cybercrimes, and clarify procedures for appealing to law enforcement;

- develop a methodology for collecting cyber statistics and annually publish statistical information on cyber-attacks, cyber incidents and countermeasures in the areas of responsibility of the main actors of the national cyber security system on their official websites; to develop a methodology for conducting annual sociological surveys on cyber threats faced by the population of Ukraine, with assessments of the effectiveness of government agencies in combating them and to ensure the conduct of such surveys;

- to develop a method of communication between the state and society to counter large-scale cyber-attacks and cyber incidents, to create all necessary conditions for its practical implementation; introduce mechanisms for the identification of e-commerce entities in cyberspace, ensuring appropriate amendments to the legislation of Ukraine;

- regulate at the legislative level the legal status of cryptocurrencies, define legal mechanisms for cryptocurrency transactions and market creation;

- conduct joint activities with the EU in the framework of the EU External Cyberspace Building Program and support partners to increase their resilience in cyberspace and their ability to investigate, prosecute cybercrime and respond to cyber threats;

- to ensure the improvement of the level of qualification, logistical support of forensic experts in the areas of research of computer hardware and software products, communication systems and tools; to promote the development of innovative methods and technologies of digital forensics; to ensure an increase in the level of knowledge of operatives, employees of pre-trial investigation bodies, prosecutors, judges in the field of information technology and cybersecurity, primarily in the areas of collection and research of digital (electronic) evidence;

- Facilitate the involvement of private experts in computer and telecommunications research and expertise, software research needed to respond quickly to cyber incidents and effectively investigate cybercrime.

The state will introduce asymmetric deterrence instruments (goal C.4), for this purpose it will be:

- a permanent working group on cyber intelligence was established, its effective cooperation with the EU Intelligence and Situation Center (INTCEN) was established in order to promote strategic cooperation of Ukraine in the field of intelligence on cyber threats and cybersecurity activities;

- improved the system of intelligence support of cyber security of the state in terms of creation, development of forces, means and tools to prevent threats to national security in cyberspace;

- measures to ensure cybersecurity of information infrastructure and cyber protection of information resources of diplomatic missions, consular posts and state-owned objects of Ukraine abroad were strengthened; created technological opportunities for connection by suppliers of electronic communications networks and / or services of technical means for the implementation of operational and investigative, counterintelligence and intelligence activities;

- a harmonized approach with the Euro-Atlantic community to impose sanctions in response to subversive activities in cyberspace, developed and agreed with foreign partners a mechanism for joint diplomatic and economic action and measures, including the introduction of restrictive measures in the form of economic sanctions in response to destructive cyberactivity;

- a clear procedure for a comprehensive diplomatic response with the use of internationally available tools to combat malicious activity in cyberspace against Ukraine;

- systematic exchange of information on destructive activities in cyberspace with international partners, primarily EU and NATO member states, established platforms for such exchange; the issue of full
involvement of the private sector and civil society in the implementation of measures to deter destructive activities in cyberspace has been regulated at the legislative level;
- effective mechanisms have been developed to involve private sector specialists in cybersecurity in participating in deterring and counteracting aggression against Ukraine in cyberspace

On the basis of cyber resilience, the State, in cooperation with the private sector, academia and the public, will ensure the achievement of national cyber preparedness and cyber defense (Objective K.1). This requires:
- develop a National Cyber Emergency Response Plan, which will define the mechanisms for responding, with further recovery, to large-scale cyber-attacks and cyber incidents on critical information infrastructure, define the roles and responsibilities of all cybersecurity actors and critical infrastructure during an emergency, key processes and measures to overcome an emergency, criteria for classifying a situation as an emergency, mechanisms for informing citizens, conducting exercises to check the state of emergency preparedness; develop basic requirements and recommendations on cybersecurity and cybersecurity;
- to expand the system of information exchange on cyber incidents between all subjects of cyber security; implement a risk-oriented approach in terms of cybersecurity and cybersecurity measures for critical infrastructure and government agencies, in particular develop methods for identifying and assessing cyber risks at the national level and for critical infrastructure sectors of the state, regulate at the legislative level mandatory risk assessment based on the developed methods; to introduce a system of product certification, which is used for the functioning and cyber protection of information and communication systems, first of all objects of critical information infrastructure; to ensure the development of organizational and technical model of cyber defense,
- introduce mechanisms for timely identification of threats, tools for detecting cyberattacks to respond to them quickly and quickly restore stable operation during and after cyberattacks;
- complete the process of identifying critical infrastructure and critical information infrastructure, create and ensure the functioning of the state register of critical information infrastructure, constantly review and update the requirements for their cyber security in accordance with modern international standards on cyber security;
- to introduce a national program to identify vulnerabilities of information and communication systems, to conduct regular audits of the security of communication and technological systems of critical infrastructure for vulnerabilities; to introduce a permanent assessment of the state of protection of critical information infrastructure and state information resources, to establish incentives, mandatory and periodicity of such assessment taking into account the criticality categories of objects, to provide for the participation of private sector cybersecurity specialists;
- implement an information security audit system, primarily at facilities critical infrastructure, define mechanisms and basic methods of conducting independent audits, set requirements for information security auditors, their certification, certification (re-certification), training and retraining, as well as the mandatory and periodicity
- conducting audits, providing generalized information on the results of audits to the National Cyber Security Coordination Center; to ensure the development of systems of technical and cryptographic protection of information, the priority of the use of technical and cryptographic protection of domestic information for cyber protection of state information resources and critical information infrastructure; to promote the use of domestic means of cryptographic protection of information in the interests of private companies; to conduct annual command and staff cyber exercises of strategic level with the participation of representatives of the public and private sectors; to ensure the development of a network of sectoral (sectoral) centers for responding to cyber-attacks and cyber incidents;
- to create the National Center for Reservation of State Information Resources, to modernize the system of secure access of state bodies to the Internet; complete the deployment of the National Telecommunication Network, increase its capacity, and provide for the use of exclusively domestic means of cryptographic protection of information during its operation.

Ukraine will conduct research in the field of cybersecurity, reform the system of training and retraining, as well as develop curricula, courses, training in cyber learning for all segments of the population (goal K.2), for which there will be:
- stimulated research and development in the field of cybersecurity, taking into account the development of new information and communication technologies, 5G, artificial intelligence, Internet of
Things, cloud and quantum computing technologies, as well as the emergence of new tools for cyber threats to create domestic systems, platforms and products. cybersecurity;

- analysis and assessment of the current state of training of specialists in the field of cybersecurity, developed on the basis of the analysis of proposals for reforming the system of training and retraining of such specialists, approved the relevant concept;
- developed the National Cybergenic Program aimed at increasing the level of cyber literacy of the population of Ukraine; centers have been established to generalize and exchange experience in the field of cybersecurity, support innovation and domestic developments in this field;
- requirements are set for the need to improve the skills of employees of the security and defense sector, critical infrastructure and civil servants on cyber security and cybersecurity with the introduction of short- and long-term courses and programs on these issues; Periodic training, including at the expense of the state, and obtaining at least one certificate (as well as a new one every three years) in cybersecurity is provided for specialists of state bodies directly performing cybersecurity and cybersecurity functions, as well as carry out training of cybersecurity specialists;
- mechanisms for training cybersecurity specialists have been created both at the level of higher education and at the level of secondary and vocational education;
- periodic carrying out, taking into account the departmental specifics of attestation (re-attestation) of specialists responsible for ensuring cybersecurity and cybersecurity of state bodies and critical infrastructure facilities;
- provides material incentives for cybersecurity professionals who serve in the military, civil service (including special services), law enforcement or contract employment in the public sector and directly perform cybersecurity and cybersecurity functions, taking into account levels remuneration of such specialists in the private sector; launched annual national cyber competitions for high school students and students as a tool for selecting the best young professionals in the field of cybersecurity;
- the inclusion of the cybersecurity component in the training program for school teachers in higher educational institutions of all levels of accreditation is ensured, with the simultaneous introduction of advanced training of the current teaching staff on cybersecurity;
- included issues of cybergenic, digital skills, cyber awareness of modern cyber threats and their response to secondary, vocational and higher education programs; coordination of the scientific community during scientific research in the field of cybersecurity and its involvement in the implementation of state policy in the field of cybersecurity;
- identified long-term areas of research and development in the field of cybersecurity, as well as developed an effective program of state support (based on a project approach) strategically important for cybersecurity research institutions and organizations, research on cybersecurity and cybersecurity for national security and defense;

The main actors of the national cybersecurity system are involved in EU-supported training and development programs for staff, in particular the EU Cybersecurity Agency (ENISA), gradually covering other cybersecurity actors.

Recognizing secure digital services as a guarantee of economic development, the state will take the following measures (goal K.3):

- strengthen the confidence of the private sector and individual citizens in digital services provided by the state, unconditionally fulfilling the requirements for cybersecurity and cyber security during their provision and informing the public about their security and reliability;
- implement digital services for the population and develop the national information infrastructure, providing for the allocation of funds for cybersecurity and cybersecurity measures of at least 5% of the total cost of the relevant information infrastructure (information and communication system);
- develop new national standards in the field of cybersecurity, organizational and technical requirements for the security of applications, mobile devices, workstations, servers and networks, cloud computing models, taking into account European and international standards;
- establish bodies to assess the compliance of providers of electronic trust services with the requirements for qualified providers of qualified electronic trust services;
- introduce electronic trust services based on a qualified website authentication certificate;
- develop a system of conformity assessment bodies for information and communication technologies used to create such systems, security requirements, information security management of entities providing digital services; create the necessary prerequisites (regulatory, organizational, technological) for the authentication of users of digital services (where required) using electronic identification technologies and /
or electronic trust services; increase the effectiveness of the system of personal data protection of citizens, defining the basic requirements for their storage and processing and strengthening the responsibility for violating these requirements, harmonizes domestic legislation with relevant EU legislation.

The National Cyber Security Coordination Center will ensure the coordinated activities of all stakeholders in the development and operation of the national cybersecurity system (Objective B.1) by:
- development and approval of the procedure for conducting a review of the state of the national cybersecurity system, ensuring its implementation at least once a year during the implementation of the Strategy;
- introduction of mandatory real-time information on cyber-attacks and cyber incidents by all departmental and sectoral (sectoral) cybersecurity or cyber defense centers to the National Cyber Security Coordination Center; ensuring the consideration of the most important issues in the field of cyber security of Ukraine at the meetings of the National Coordination Center for Cyber Security, the decisions of which are binding on all subjects of cyber security;
- expansion of the network of information exchange on cyber-attacks, cyber incidents and indicators of cyber threats on the basis of the technological platform of the National Cyber Security Coordination Center, covering all government agencies and critical infrastructure, unification of information exchange formats; introduction, in the experience of EU member states, of coordinated detection and disclosure of vulnerabilities in information and communication systems under the auspices of the National Cyber Security Coordination Center;
- development and implementation of mechanisms to encourage the private sector, the scientific community, public organizations and individuals to participate in the formation and implementation of measures to ensure cybersecurity of the state; ensuring the annual publication by the main actors of the national cybersecurity system of public reports on the state of cybersecurity by areas of responsibility.

The state in cooperation with the private sector will form an effective model of relations in the field of cybersecurity, based on trust (goal B.2), implementing the following measures:
- regulate at the legislative level the issue of public-private partnership in the field of cybersecurity, defining the forms and methods of such partnership, strengthening mutual trust and providing for the possibility of implementing pilot projects in this area;
- introduce on a regular basis consultation of stakeholders and provide methodological assistance on the establishment of cyber security units, sectoral (sectoral) cybersecurity centers and cyber incident response teams, fully promote their development; will involve on a regular basis representative of scientific institutions, public organizations and independent experts in the field of cybersecurity in the development of regulations, normative documents and standards in this field;
- increase the effectiveness of public involvement in cybersecurity decision-making by conducting relevant surveys (questionnaires) and posting their results on the information resources of the National Cyber Security Coordination Center and the main actors of the national cybersecurity system; will stimulate the development of domestic software products, in particular open source software, which will be used as a priority for processing and protection of state information resources, as well as at critical information infrastructure facilities; implement a program for the development of the market of goods and services in the field of cybersecurity, which will include stimulating its development and international recognition;
- develop a system for assessing the latest technologies that directly affect the country's cyber resilience, create tools (standards, protocols, certificates, etc.) to assess the effectiveness of the use of new technologies to combat cyber-attacks; introduce pilot mentoring programs for specialists of public bodies that directly perform the functions of cyber security and cyber defense, by involving certified by international standards of private sector specialists;
- continue the practice of holding an annual Cyber Security Month in Ukraine with the involvement of a wide range of relevant specialists and experts from government agencies, academic and educational institutions, as well as the public and private sectors, confirming the need for relevant legislation; will promote, in particular by providing organizational and technical support, the functioning of permanent dialogue platforms (conferences, seminars, forums, etc.) in all regions of Ukraine, whose activities are aimed at building trust between cybersecurity actors;
- will promote the implementation of a culture of cybersecurity in enterprises, institutions and organizations, regardless of ownership, which is to constantly increase the cyber awareness of their managers and employees;
- promote mutual recognition of the results of cybersecurity conformity assessment and certification carried out by the relevant authorities both in Ukraine and abroad; introduce a mechanism for estimating the losses of economic entities due to cyber-attacks for the possibility of their compensation and as an element of further implementation of the cyber insurance system.

Ukraine will develop international cooperation in the field of cybersecurity, aimed primarily at ensuring independence and state sovereignty, restoring the territorial integrity of Ukraine (Goal B.3).

For this:
- ensure Ukraine's participation in the work of the international platform of the Program of Action to Promote Responsible Behavior of States in Cyberspace.
- the UN General Assembly and the UN Group of Governmental Experts on Information Security (UNGGE);
- ensure Ukraine's participation in the revision of the Second Additional Protocol to the Budapest Convention of the Council of Europe on Cybercrime to develop measures and safeguards to improve international cooperation between law enforcement and judicial authorities, as well as between authorities and service providers in other countries;
- expand through dialogue with international partners the access of Ukrainian law enforcement agencies to the resources of the European Center for Combating Cybercrime (EC3), to the telecommunication system of Interpol I-24/7 (using FIND technology); continue cooperation with the EU Cybersecurity Agency (ENISA), in particular on coordinated vulnerability detection and implementation of the European Parliament and Council of Europe (EU) Directive 2016/1148 of 6 July 2016 on measures for a high common level of security of network and information systems in the Union (NIS Directive) as an element of Ukraine's European integration;
- deepen cooperation with the International Telecommunication Union (ITU) in the fields of cybersecurity and electronic communications, in particular on standardization in these areas;
- establish cooperation with the Internet Corporation for Assigned Names and Numbers (ICANN) to develop public policy on the Internet; expand cybersecurity cooperation within the GUAM Organization for Democracy and Economic Development;
- explore the possibility of Ukraine's accession to the EU strategy to diversify DNS name recognition, support the DNS initiative in order to avoid extreme scenarios of cyber-attacks on the global root DNS system, its hierarchical and delegated zone system;
- ensure that Ukraine implements the EU Regulation on the limitation of IP for market management, which will accelerate the introduction of IP in Ukraine, as well as other established standards of Internet security, best practices for DNS name recognition, routing and e-mail security;
- we will develop international cooperation in the field of cybersecurity by supporting international initiatives in the field of cybersecurity that meet Ukraine's national interests, deepening Ukraine's dialogue with the European Union, the North Atlantic Treaty Organization, the Organization for Security and Cooperation in Europe. improving the mechanisms of such cooperation;
- create a permanent working group on cooperation with leading IT companies, global digital service providers, social networks to combat hybrid threats, dissemination of misinformation, the possibility of sanctions in accordance with the laws of Ukraine;
- identify and approve a list of priority areas for attracting international technical assistance in the field of cybersecurity in Ukraine.

The strategy is valid for the period 2021 - 2025. Implementation coordinator. The Strategy is a working body of the National Security and Defense Council of Ukraine - National Cyber Security Coordination Center. The main criterion for the effectiveness of the Strategy is to achieve the goal and strategic goals by performing certain strategic objectives.

National Cyber Security Coordination Center legislation forms (for the entire period of the Strategy) planning measures for the implementation of the Strategy, coordinates their implementation and monitors the state performance and efficiency.

General plan developed by the National Coordination Center cybersecurity and approved by the National Security and Defense Council of Ukraine, is the basis for the formation of annual plans by the Cabinet of Ministers of Ukraine measures to implement the Strategy, as well as to exercise effective control over implementation of planned tasks and relevant activities.

The effectiveness of the Strategy is determined in the conducted and established order of reviews of a condition: national cybersecurity system; cyber protection of critical information infrastructure, state information resources and information required to be protected by law. The results of the reviews may be the
basis for changes to general plan and / or annual action plans for the implementation of the Strategy, which due to the need to adapt to changes in the security environment, elimination and minimization of negative trends in the field of cybersecurity.

**Conclusions and perspectives of further research.** The strategy is the basis for the development of other regulations acts in the field of cyber security of Ukraine, as well as to justify the distribution necessary material, human and other resources. Funding for the implementation of the Strategy will be provided within expenditures provided by the State Budget of Ukraine for the security sector and defense, which will be considered by the National Security and Defense Council of Ukraine in the manner prescribed by the Budget Code of Ukraine. In accordance to the legislation state bodies, enterprises, institutions and organizations will include in their plans the financial costs of cybersecurity. Within public-private partnership, international technical assistance investments will be attracted, which will be directed to development national cybersecurity system. The process of implementing the Strategy should be as transparent and open as possible and accompanied by democratic civilian control. From this purpose of the main actors of the national cybersecurity system within additional information will be provided annually the public through their own official websites on the status of their implementation of the Strategy and the state of funding for relevant activities.

**ЛІТЕРАТУРА**


8. Почепцов Г. Гібридна війна: інформаційна составляюча / Г.Почепцов. URL: http://psyfactor.org/ psyops/hybridwar5.htm


18. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року «Про Стратегічний оборонний бюлетень України» : указ Президента України від 06.06.2016 р. № 240. URL : https://zakon.rada.gov.ua/laws/show/440-2016-%D1%80,


REFERENCES


18. Pro rishennya Rady natsional'noyi bezpeky i oborony Ukrayiny vid 20 travnya 2016 roku «Pro Stratehichnyy oboronny byuletin' Ukrayiny » : ukaz Prezydenta Ukrayiny vid 06.06.2016 r. № 240. URL: https://zakon.rada.gov.ua/laws/show/440-2016-%D1%80.


