Draft of the Cybersecurity Strategy of Ukraine (2021-2025) (Unofficial English translation)

SECURE CYBERSPACE - THE GUARANTEE OF SUCCESSFUL DEVELOPMENT OF THE STATE

Section 1. CYBERSECURITY: A GLOBAL CONTEXT

The Cybersecurity Strategy of Ukraine defines the priorities, goals and objectives of ensuring the cybersecurity of Ukraine with the purpose of forming the conditions for the safe operation of cyberspace, its use in the interests of the individual, society and the state.

Cybersecurity is one of the priorities of the National Security system of Ukraine. This priority will be implemented by strengthening the capacity of the National Cybersecurity System to counter cyber threats in today's security environment.

Forming the new Cybersecurity Strategy of Ukraine, we take into account world trends in the global cyber environment as factors influencing the development of the national cybersecurity ecosystem.

The XXI century is marked by the active formation of the sixth technological domain (bio-, nano-, info-, cognotechnologies, their convergence) and the risks faced by civilisation due to the introduction of new technologies, including their use in cyberspace.

The role of cyber threats in the spectrum of threats to national security is growing, and this trend will intensify as information technology develops and converges with artificial intelligence technologies in the next decade. The growth of such influence on the functioning of management structures, both national and transnational, forms a completely new security situation with the challenges of a new technological level. There is a division of spheres of influence in cyberspace between the world's centers of power, and their desire to ensure the realization of their own geopolitical interests is growing.

Cyberspace, along with other physical domains, is recognized as one of the possible military operating domains, so the state's ability to protect national interests in it is seen as an important component of cybersecurity. The trend of creating a new kind of forces - cyber forces, which aims not only to protect critical information infrastructure from cyber attacks, but also to conduct preventive offensive operations in cyberspace, aimed at destroying computer networks and information systems of the enemy forces, as well as withdrawal from system of critical enemy objects by destroying the information systems that control such objects.

At the same time, the combination of traditional and non-traditional strategies and tactics with the use of digital information technologies is increasingly used. In particular, the Russian Federation is actively implementing the concept of information confrontation, based on the symbiosis of hostilities in cyberspace and information operations, the

mechanisms of which are actively used in the process of hybrid war against Ukraine. EU countries, NATO, leading international companies and experts unanimously recognize the Russian Federation and its actions in cyberspace as a major threat to international cybersecurity. Its cyber-exploration activities are part of the hybrid war that is waging against Ukraine. Such destructive activity poses a real threat of acts of cyberterrorism and cyber diversion against the national information infrastructure.

The intensity of interstate confrontation and reconnaissance and subversive activities in cyberspace is projected to increase, which will be manifested primarily in expanding the range of states that will try to form their own cyber intelligence, master modern technologies of reconnaissance and subversive activities in cyberspace, and strengthen state control over the Internet. At the same time, the development of tools that are based on the accumulation of large amounts of data on human behavior, social groups and on the use of modern advances in artificial intelligence will become widespread.

A negative sign of technological development associated with the widespread spread of digital technologies, the expansion of the Internet environment, is the critically growing technical level of tools for the realization of cyber threats, and the landscape of such threats covers more and more areas of life as the result. Cyberattacks, their varieties are becoming more intelligent and dangerous, creating a real threat to critical infrastructures. Attackers focus on finding vulnerabilities in assets (management systems) and develop unique features: multifunctional malware, ransomware, botnets that perform distributed attacks (DDoS) on operating networks, production systems that use cloud services, attacks on supply chains. Given the development of artificial intelligence technologies in the next 5-10 years, the scale and consequences of such interventions will increase.

The use of cyberspace by terrorist organizations (cyberterrorism) is gaining global scale. This will be facilitated by the comprehensive digital transformation of management and livelihood systems, which is constantly expanding the target audience of cyberterrorism and the range of potential targets of cyber attacks. The priority objects of terrorist cyberattacks are nuclear energy facilities, power supply control systems, air and rail transport, powerful storage facilities for strategic raw materials, water supply systems, chemical and biological facilities.

New challenges bring the transition to 5G networks, the operation of which depends on the correct operation of the software, which due to the novelty of technology may have new, not fully anticipated threats. Technologies such as "Internet of Things", "augmented reality", "smart city" are actively supplemented by new ones - "hyperautomation", "smartly arranged business", "cybersecurity network", "distributed cloud", "Internet behavior", etc.

By radically changing the world order, the COVID-19 coronavirus pandemic will have a long-term impact on the world order. Dependence on digital communications is growing, which makes the process of information exchange, protection of information and personal data vulnerable. Cybercriminals, making the most of the pandemic, have increasingly used new methods of cyberattacks since its inception, forcing national governments to implement additional countermeasures, maintain access to the necessary devices, and ensure the proper functioning of all electronic resources and systems.

The spread of the threat landscape and the complexity of the tools for their implementation encourage governments of leading countries to improve the architecture of national cybersecurity systems, change the strategy and tactics of combating cyber threats. Changes are being made to the model of countering cyber threats, which is related to the understanding of the insufficient ability to build completely invulnerable security systems. As practice shows, any information and communication systems can be affected by a cyber attack, regardless of their level of protection. Therefore, it is important to quickly identify vulnerabilities and cyberattacks, respond and disseminate information about them to minimize possible damage.

The rapidly changing digital world needs to form a more balanced and effective national cybersecurity system that can flexibly adapt to changes in the security environment, ensuring the safe functioning of the national segment of cyberspace, providing new opportunities for digitalization of all spheres of public life.

We create Ukraine capable of ensuring its social and economic development in the digital world, which requires the ability to effectively deter destructive actions in cyberspace, achieve cyber resilience at all levels and the interaction of all actors in cybersecurity through partnership and cooperation.

Section 2. IMPLEMENTATION OF THE CYBERSECURITY STRATEGY OF UKRAINE FOR 2016 - 2020

The adoption of the Cyber Security Strategy of Ukraine in 2016 was an important step in introducing long-term planning approaches in this area, and therefore, the very fact of its adoption were a positive result.

Over the years, efforts have been made to establish and develop a national cybersecurity system. An important stage in its institutionalization was the adoption of the Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine", which is the legal basis for creating a national cyber security system and its main actors in the field of cyber security.
Regulatory support for cyber security of critical information infrastructure has been improved, the procedure for its definition and general requirements for its cyber security have been adopted.

Centers (subdivisions) for cybersecurity or cyber defense have been established in the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Bank of Ukraine, the Ministry of Infrastructure of Ukraine, and the Ministry of Defense of Ukraine (Armed Forces of Ukraine).

The National Telecommunication Network is being developed, secure data processing centers (data centers) are functioning, the National Center for Reserving State Information Resources is being formed, and a system for identifying vulnerabilities and responding to cyber incidents and cyberattacks has been launched.

In order to improve the coordination of the activities of cybersecurity entities, a working body of the National Security and Defense Council of Ukraine was established - the National Cybersecurity Coordination Center, the solutions of which contribute to solving the most complex problems in this area.

Cooperation with foreign partners is actively developing, Ukraine's cooperation with the EU and NATO is deepening, and cyber exercises are being conducted with the participation of other states and international organizations.

An annual event, Cyber Security Month, has been launched.

At the same time, the activities of the subjects of the national cybersecurity system remain insufficiently coordinated and aimed at performing only current tasks. According to the results of expert assessments, the state of implementation of the Strategy according to certain indicators does not exceed 40%. The issues of operative exchange of information on cyber threats, effective training system and effective model of public-private partnership remain unresolved. The organization and conduct of research in the field of cybersecurity is defined by all experts as unsatisfactory.

The experience gained during the duration of the Strategy made it possible to identify a number of systemic problems that either complicated or prevented its effective implementation.

One of the identified problems was the lack of clarity in the identified priorities and areas of cybersecurity in Ukraine, much of which did not have a clear ultimate goal and was not specific. The level of planning of measures for the implementation of the Strategy was unsatisfactory, the planned measures were not always correlated with the objectives of the Strategy. The implementation of the Strategy was complicated by the lack of a holistic vision (program) of developing the capabilities of the main actors of the national cybersecurity system, limited resources to ensure the functioning of this system, lack of proper government support for its institutional support.

Indicators for the implementation of the Strategy have not been developed, which has complicated the process of evaluating its effectiveness and identifying unfinished tasks. Entities in the security and defense sector mainly took part in the implementation of the Strategy, other ministries and departments, scientific institutions, and the public were insufficiently involved. Educational and research institutions were insufficiently involved in the implementation of tasks related to the development of scientific potential and the spread of cyber literacy.

The tasks of the Strategy, which are extremely important for the development of the national cybersecurity system, have not been fulfilled: the list of critical information infrastructure has not been formed, the model of public-private partnership has not been created. The development of digital literacy was carried out without a clear program, cyber learning was conducted sporadically.

The new Cyber Security Strategy of Ukraine takes into account this experience and problems and determines the mechanisms for implementing the Strategy for the next five-year period.

Section 3. NATIONAL CYBERSECURITY SYSTEM: BUILDING PRINCIPLES

Ukraine seeks to create the most open, free, stable and secure cyberspace, which takes into account human rights and freedoms, supports social, political and economic development.
Implementing the Cyber Security Strategy of Ukraine for 2016 - 2020, the state was able to form the core of the national cyber security system. Ukraine has increased the potential that allows for further development of the national cybersecurity system on the basis of deterrence, cyber resilience, and interaction.

To achieve that, Ukraine:

- will strengthen the capabilities 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);
- will ensure the development of communication, coordination and partnership between cybersecurity actors at the national level, the development of strategic relations in the field of cybersecurity 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, on which it relied at the initial stage of formation of the national cybersecurity system, in solving tasks related to cybersecurity on a national scale. public associations and individual citizens of Ukraine.

The National Cybersecurity 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 legislation in the field of cybersecurity and promptness of actions to update it in accordance with changing security conditions;
- focus on society, which will contribute to its economic and social growth;
- using 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 the needs of the state and the rights of citizens, observance of the rule of law, procedural guarantees and legal remedies, respect for fundamental values, human and individual rights to freedom of expression, the same protection of universally recognized fundamental rights online and 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 creation of conditions for active participation of all stakeholders, taking into account their needs and obligations in the conditions when cybersecurity of the digital environment has become of paramount importance for the state, society and citizens;
- defining clear roles, needs, responsibilities in solving cybersecurity tasks of varying complexity, the use of incentives and the exchange of unique knowledge and experience;
- risk-oriented approach in terms of cybersecurity and cybersecurity measures;
- cooperation and inclusive dialogue of all actors of cybersecurity, in particular in the framework of public-private partnership, 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 the state, business and society;
- balanced allocation of available material and financial resources, as well as optimal use to address each specific task in the field of cybersecurity such levers as legislation, standardization, educational programs, mechanisms to stimulate and strengthen trust, exchange of information and best practices;
- a proactive approach, involving precautionary measures, including the use of cyberattack prevention systems, shifting the organizational and technological focus from countermeasures to countering cyberattacks in the early stages;
- ensuring democratic civil control over the functioning of the national cybersecurity system, namely compliance with the Constitution and laws of Ukraine by cybersecurity entities, the state of implementation of strategic documents, concepts, state programs and plans in the field of cybersecurity, efficient use of resources, including budget funds.

Section 4. NATIONAL CYBERSPACE: CHALLENGES AND CYBER THREATS

CHALLENGES

Accelerated development and interpenetration of information technologies, along with powerful socially significant benefits, is accompanied by the scaling of cyber threats to all spheres of life, their evolution towards high-tech solutions and diversification of implementation tools.

Ukraine has the necessary potential 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, big data, Internet of Things, machine learning / artificial intelligence (AI), etc. ;
- the militarization of cyberspace and the growing technological capabilities of cyber weapons, which make it possible to carry out covert enemy 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 using the methods of social engineering, 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 the widespread 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 technologies and processes. Without a systematic approach to cybersecurity and risk assessment, there is a possibility to lose public confidence in the processes of digital transformation.

THREATS

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, defense and weapons control systems of the defense forces, as well as on 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 by the security and defense sector.

Extremely relevant threat today is intelligence and subversive activities in cyberspace against Ukraine, which is associated with 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, primarily government systems, livelihoods, electricity, transport, nuclear and chemical industries, banking (acts of cyber diversion).

In Ukraine, the threat of cyberterrorism has increased significantly 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. There is the use of cyberspace to finance terrorist groups. At the same time, Ukraine's cooperation with international partners on developing mutually beneficial mechanisms to combat cyberterrorism is insufficient.

The growth of cybercrime in the national segment of cyberspace is a large-scale threat that harms public information resources, social processes, personally citizens, which reduces public confidence in information technology and leads to significant material losses. The use of cyberspace for other crimes (against the foundations of national security, money laundering, trafficking in human beings, illicit trafficking in weapons, drugs and other objects and substances that threaten human life and health) is becoming more widespread. The situation is complicated by the low level of cyber literacy of the population, in particular ordinary users of electronic services.

Public information resources and critical information infrastructure, which are designed to meet the vital needs of citizens, individuals, society and the state, are insufficiently protected from cyberattacks.

Public authorities, when deciding on the automation of public administration processes, do not always assess the risks that arise in the cyber protection of public information resources. Protection of information and communication systems of state bodies and business entities, which process a large part of official information and personal data of citizens, does not meet the requirements of legislation, which increases the risks of interference in such systems, threatens confidentiality, integrity and availability of information (registers, databases).), which is designed to meet the needs and ensure the constitutionally guaranteed interests of citizens, society and the state.

Ukraine's high technological dependence on foreign manufacturers of ICT products and management software, lack of modern national standards on security requirements for the supply chain of relevant equipment, development of software and information and communication systems, certification or conformity assessment systems for safety of such products increase the degree of vulnerability. military, political, financial, economic and

industrial infrastructure of the state from harmful and undeclared functions in such equipment and narrow the domestic capacity to counter cyber threats.

Many enterprises, institutions and organizations of all forms of ownership do not provide cyber protection of electronic information resources at their disposal, which leads to violations of the rights of users of digital services and discredits the processes of digital transformation in the state.

The basic landscape of the tools for implementing the outlined cyber threats is characterized by the growth of a high-tech component and diversity.

The number of cyberattacks aimed at stealing personal and other confidential data of citizens and organizations using social engineering methods is constantly increasing.

There is a growing risk of phishing attacks, botnets, malware, including extortionate programs, both from financially motivated cybercrime groups and from hacker groups controlled by the aggressor country and other countries.

Increasing information in databases and information systems and increasing responsibility for the leakage of personal data of citizens in leading countries has created a global market for the development of extortionate programs that require funds to unblock access to information or not post stolen information on the Internet.

Increasingly, cyberattacks are not directed at governments and organizations. Developers and vendors of software and hardware are attacked in order to infect popular applications, make changes to source code, and update processes. In the future, it is used to penetrate a large number of their customers and cause large-scale damage.

Popular websites, social networks, registries collect a large amount of user identification and personal data. Leaks of information from databases that belong to them pose a threat to the use of this data to attack other resources and information systems.

Preconditions and factors that form the outlined threats:

- imperfect legal framework in the field of cybersecurity, as well as its obsolescence in the field of information protection, slow implementation of European law in domestic law, insufficient regulation of the digital component of criminal investigations, as well as low level of legal liability for violations of legislation in this area;
- the lack of relevant ministries and departments does not have the appropriate structural units, the necessary staffing and proper control over cybersecurity. Cybersecurity work is funded on a residual basis with technological errors;
- lack of an independent information security audit system and mechanisms for disclosing information about vulnerabilities in the context of dynamic digitalization of all spheres of public administration and life of the country, which requires strict compliance with relevant standards;

- non-compliance with modern requirements for the level of training and advanced training of specialists in cyber security and cyber defense, in particular ineffective mechanisms to encourage them to work in the public sector;
- lack of legislation on critical infrastructure of Ukraine and its protection, which significantly complicates the formation of a system of cyber protection of such infrastructure;
- incomplete measures to implement the organizational and technical model of cybersecurity, which will meet modern threats, challenges in cyberspace and global trends in the cybersecurity industry;
- lack of a system to increase digital literacy of citizens and a culture of safe behavior in cyberspace, raising public awareness of cyber threats and cyber defense.

Section 5. AIMS AND GOALS OF THE CYBERSECURITY STRATEGY.

The aims of cybersecurity in Ukraine are:

- secure cyberspace to protect the sovereignty with the development of state and society;
- protection of the rights, freedom and legitimate interests of Ukrainian citizens of in the 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 period of implementation of the Strategy.

To build the **deterrence potential (D)** by 2026, we must achieve the following strategic goals:

- **Goal D.1. Effective cyber defense.** Ukraine must not only create and develop effective (including personnel and technology) forces 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 D.2. Capacity building 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 the conditions that contribute to them and their causes to protect the interests of the state, society and individuals.

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

- **Goal D.4. Development of asymmetric deterrence 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 (R)** for the national cybersecurity system, we must achieve the following strategic goals by 2025:

- **Goal R.1. Strengthening national cyber readiness and cyber defense.** Introduce and implement clear and understandable for all stakeholders measures to strengthen

national cyber preparedness in the interests of economic well-being and protection of the rights and freedoms of every Ukrainian citizen. Cyber preparedness is the ability of all stakeholders, especially the subjects of the security and defense sector, to respond to cyber attacks in a timely and effective manner, to ensure a regime of constant readiness for real and potential cyber threats, detection and elimination of preconditions for their occurrence, thus ensuring cyber resilience. critical information infrastructure.

- **Goal R.2. Professional development, cyber-aware 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 primarily be involved in solving the problems of cybersecurity of the state. Cyberhygiene, digital skills, cyber awareness of modern cyber threats and countering them should become an integral part of the education of every Ukrainian citizen.
- **Goal R.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.

Cooperation (C) will be improved by achieving the following strategic goals by 2026:

- **Goal C.1. Strengthening the cooperation system.** The state will create conditions for effective interaction 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 C.2. Formation of a new model of relations in the field of cybersecurity**. We will introduce a service model of state participation in cyber security 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 C.3. Pragmatic international cooperation.** We focus our relations with international partners both on the development of mutual trust for joint response to cyberattacks and overcoming crisis situations in cybersecurity, and on purely practical cooperation: exchange of information on cyberattacks and cyber incidents, joint cyber operations and investigation of international cybercrimes, regular cybercrimes, regular cybercrimes experience and best practices.

Section 6. STRATEGIC GOALS

Strengthening the capacity of the national cybersecurity system is carried out by fulfilling strategic objectives aimed at achieving certain prices.

On the basis of deterrence:

Ukraine will form a system of effective cyber defense through (goal D.1):

- formation of a separate type of forces within the Armed Forces of Ukraine - cyber defense forces, provisioning them with appropriate financial, personnel and technical resources to deter armed aggression in cyberspace and provide repulse to aggressors;
- 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 the goals of cyber defense;
- ensuring constant monitoring of electronic communication networks and information resources of the "ua" domain, analysis of the intrusion to these networks and resources, as well as real-time identification of anomalies in their functioning;
- development and implementation of a 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 of the Armed Forces of Ukraine, establishing a permanent base of cooperation with the European military network CERT (military network CERT);
- providing assessments of the capabilities of security and defense sector actors in terms of joint implementation of the cyber defense set, in particular during defense and cyber security reviews;
- introduction in the system of military-patriotic education and the system of territorial defense of training programs for the preparation and conduct of practical training in the field of cybersecurity.

Ukraine will provide effective counteraction to intelligence activities in cyberspace and cyberterrorism for the purpose of D.2:

- creation in accordance with the approved conceptual foundations of the national system for detecting cyberattacks, combating acts of cyberterrorism and cyber espionage on objects of critical information infrastructure, defined for monitoring of cyberspace by own publication, prevention of cyber threats and their neutralization, operational rehabilitation.
- improvement of analytical and forensic support of counterintelligence protection of cybersecurity of the state due to introduction of innovative methods of processing and estimation of digital data, formation of electronic data;

- ensuring maximum coverage of critical infrastructure facilities in accordance with checking the state of their readiness for possible cyber attacks and cyber incidents by eliminating the 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 committing acts of cyberterrorism in Ukraine;
- strengthening counterintelligence protection in the field of electronic communications, IT industry, the official environment of them, targeted detection, pre-assignment and assignment by intelligence-contracting to achieve the foreign intelligence service of Ukraine in the field of cybersecurity;
- creation of technological capabilities for automatic detection of cyberattacks in real time in the data flows of national information and communication systems and individual critical infrastructure, their blocking and prioritization;
- improvement of normative-legal, organizational and personnel support of the national system of fight against terrorism in parts, which is connected with involvement of law enforcement bodies in measures on preliminary prevention, establishment and registration of acts of cyberterrorism.

Ukraine will strengthen its capacity to combat cybercrime (goal D.3), this requires:

- to conduct an audit of the implementation in Ukrainian legislation of the provisions of the Convention on Cybercrime and to complete this process by making the necessary changes to the laws of Ukraine;
- to regulate the issue of electronic indicators at the legislative level, using best practices and suitable EU member states on these issues;
- to improve the legislation of Ukraine, providing for the introduction of necessary changes taking into account current challenges and trends in the field of cybersecurity;
- Introduce a nationwide awareness-raising campaign against real citizens when they encounter cyberspace, the distribution of malicious software or pornographic content, along with cybercrime, as well as clarification of procedures for appealing to law enforcement agencies;
- develop a methodology for collecting cyber statistics and annually publish statistical information on cyber attacks, cybersecurity and countermeasures for the areas of responsibility of the main actors of the national cybersecurity 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 counteracting them and to ensure the conduct of such surveys;
- to develop a method of communication between the state and society to counter large-scale cyberattacks and cyber incidents, to create all the necessary conditions for its practical implementation;
- introduce mechanisms for identification of e-commerce entities in cyberspace, ensuring appropriate amendments to the legislation of Ukraine;

- to regulate at the legislative level the legal status of cryptocurrencies, to determine the legal mechanisms for operations with cryptocurrencies and the creation of markets;
- conduct joint activities with the EU under the EU's External Cyber Capacity 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 equipment and software products, communication systems and means;
- 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 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 cybercrimes.

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

- a permanent working group on cyber intelligence has been established, its effective cooperation with the EU Intelligence and Situation Center (INTCEN) has been established in order to promote Ukraine's strategic cooperation in the field of cyber threat intelligence and cybersecurity activities;
- improved the system of intelligence support for cybersecurity of the state in terms of creating, developing 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;
- technological possibilities of connection by suppliers of electronic communication networks and / or services of technical means for realization of operatively-search, counterintelligence and reconnaissance actions are created;
- introduced 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 actions 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 using internationally available tools to counter malicious cyberspace activities 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;

- regulated at the legislative level the issue of full involvement of the private sector and civil society in the implementation of measures to curb destructive activities in cyberspace;
- effective mechanisms have been developed to involve private sector cybersecurity professionals in deterring and countering aggression against Ukraine in cyberspace.

<u>On the basis of cyber resilience</u>

The state, in cooperation with the private sector, academia and the public, will ensure the achievement of national cyber preparedness and cyber defense (goal R.1). This requires:

- develop a National Cyber Contingency Plan, which will identify mechanisms for responding, with subsequent recovery, to large-scale cyber attacks and cyber incidents on critical information infrastructure, and define the roles and responsibilities of all actors in cybersecurity and security. critical infrastructure projects during an emergency situation, key processes and measures to overcome the emergency situation, criteria for classifying the situation as an emergency situation, mechanisms for informing citizens, conducting exercises to check the state of emergency preparedness;
- develop baseline requirements and recommendations for cybersecurity;
- deploy a system for exchanging information on cyber incidents between all cybersecurity actors;
- introduce a risk-oriented approach in terms of cybersecurity and protection measures for critical infrastructure and government agencies, in particular to 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 the obligation to conduct periodic risk assessments. on the basis of the developed techniques;
- 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, to introduce mechanisms for timely identification of threats, tools for detecting cyberattacks for rapid response to them and rapid restoration of 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 protection, taking into account modern international standards on cyber security;
- to introduce a national program to identify vulnerabilities of information and communication systems, to conduct on a regular basis an audit 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 critical infrastructure facilities, define mechanisms and basic methods for conducting independent audits, set requirements for information security auditors, their certification, certification (re-certification), training and retraining, as well as the mandatory and frequency of audits, providing generalized information on the results of audits to the National Cybersecurity 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 information of domestic production 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;
- conduct annual tabletop cyber exercises at the strategic level with the participation of representatives of the public and private sectors;
- to ensure the development of a network of sectoral (sectoral) response centers to cyberattacks 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, 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 R.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 in cybersecurity ;
- an 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 a National Cyberhygiene Program aimed at raising 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 have been 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 cyber defense with the introduction of short- and long-term courses and programs on these issues;
- provided 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 for

government professionals who directly perform the functions of cybersecurity and cybersecurity, as well as employees of educational institutions that directly carry out training of cybersecurity specialists;

- mechanisms for training cybersecurity specialists have been created both at the level of higher education and at the levels of secondary and vocational education;
- periodic carrying out taking into account departmental specifics of attestation (re-attestation) of the experts responsible for maintenance of cybersecurity and cyberprotection of the state bodies and objects of critical infrastructure is provided;
- provides material incentives for cybersecurity professionals who serve in the military, civil service (including the civil service of a special nature), serve in law enforcement agencies or work under an employment contract in the public sector and directly perform cybersecurity and cybersecurity functions, taking into account pay levels the work of such specialists in the private sector;
- launched an annual national cyber competition 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 cyber hygiene, digital skills, cyber awareness of modern cyber threats and counteraction to secondary, vocational and higher education programs;
- coordination of the scientific community during the scientific developments 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) of strategically important for cybersecurity research institutions and organizations, research on cybersecurity and cyber defense for national security and defense;
- key actors in the national cybersecurity system have been 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 R.3):

- strengthen the confidence of the private sector and individuals in digital services provided by the state, unconditionally fulfilling the requirements for cybersecurity and cybersecurity during their provision and informing the public about their security and reliability;
- implement digital services for the citizens and develop the national information infrastructure, providing for the allocation of funds for cybersecurity and cyber security measures in the amount of not less than 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 related to the security of applications, mobile devices,

workstations, servers and networks, cloud computing models, taking into account European and international standards;

- create bodies for assessing 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 efficiency 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 the relevant EU legislation.

On the basis of cooperation

The National Cybersecurity Coordination Center will ensure the coordinated activities of all stakeholders in the process of building and operating a national cybersecurity system (Objective C.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 provision of real-time information on cyber attacks and cyber incidents by all departmental and sectoral (sectoral) cybersecurity or cyber defense centers to the National Cybersecurity Coordination Center;
- ensuring the consideration of the most important issues in the field of cyber security of Ukraine at the meetings of the National Cybersecurity Coordination Center, 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 Cybersecurity 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 Cybersecurity 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 C.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;
- will introduce on a regular basis consultations of interested parties and provide methodological assistance on the establishment of cyber defense units, sectoral (sectoral) cybersecurity centers and cyber incident response teams, will fully promote their development;
- will involve on a regular basis representatives of scientific institutions, public organizations and independent experts in the field of cybersecurity in the development of regulations, regulations and standards in this area;
- increase the effectiveness of public involvement in decision-making in the field of cybersecurity by conducting appropriate surveys (questionnaires) and posting their results on the information resources of the National Cybersecurity 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 evaluating 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 the latest technologies to combat cyberattacks;
- will introduce pilot mentoring programs for professional development of specialists of state bodies that directly perform the functions of cyber security and cyber defense, by involving international sector specialists certified according to international standards;
- continue the practice of holding an annual month of cybersecurity 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 its 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, the activities of which are aimed at building trust between the subjects of cybersecurity;
- will promote the introduction of cybersecurity culture in enterprises, institutions and organizations, regardless of the form of ownership, which is to constantly increase the cyber awareness of their managers and employees;
- promote the 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 business 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 C.3). For this:

- ensure Ukraine's participation in the work of the international platform of the Program of Action for the Promotion of Responsible Behavior of States in the Cyberspace of 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 guarantees 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 Directive 2016/1148 of the European Parliament and of the Council 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 issues of standardization in these areas;
- establish cooperation with the Internet Corporation for Assigned Names and Numbers (ICANN) to develop public policy on the Internet;
- expand cooperation on cybersecurity within the Organization for Democracy and Economic Development of GUAM;
- explore the possibility of Ukraine's accession to the EU strategy to diversify DNS name recognition, support the DNS4EU 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 IPv4 Restriction of Market Management, which will accelerate the introduction of IPv6 in Ukraine, as well as other established Internet security standards, 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 the national interests of Ukraine, deepening Ukraine's dialogue with the European Union, the North Atlantic Treaty Organization, the Organization for Security and Co-operation 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;
- define and approve a list of priority areas for attracting international technical assistance in the field of cyber security of Ukraine.

Section 7. DIRECTIONS OF UKRAINE'S FOREIGN POLICY ACTIVITY IN THE FIELD OF CYBER SECURITY

Ukraine's main foreign policy priority 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 develop national capabilities. 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 with NATO partner services. mutually beneficial exchange of information and experience on national security in cyberspace, will use the best world practices, will actively implement other joint activities that will 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.

Based on the fact 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, scientific and educational circles, civil society. Attempts by some authoritarian states to sovereign the Internet run counter to the long-term interests of Ukraine and its model of socio-economic development.

Ukraine will promote further compliance with international law and human rights 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 terms of 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, ensure its basic freedoms. , guarantee non-

interference in her private life, 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 discussions in the UN and other international forums to promote, coordinate and consolidate its position in cyberspace, reducing the dangers of cyber warfare.

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 activity, 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.

Section 8. MECHANISMS FOR IMPLEMENTING THE STRATEGY AND ENSURING OPENNESS

The strategy is established for the period 2021 - 2025. The coordinator of the Strategy implementation is the working body of the National Security and Defense Council of Ukraine - the National Cybersecurity Coordination Center.

The main criteria for the effectiveness of the Strategy is the achievement of goals and strategic goals by fulfilling certain strategic objectives.

The National Cybersecurity Coordination Center in the forms prescribed by law provides (for the entire period of the Strategy) planning activities for the implementation of the Strategy, coordinates their implementation and monitors the status of implementation and effectiveness.

The general plan, developed by the National Cybersecurity Coordination Center and approved by the National Security and Defense Council of Ukraine, is the basis for the Cabinet of Ministers of Ukraine to formulate annual action plans to implement the Strategy, as well as to effectively monitor planned tasks and activities.

The effectiveness of the Strategy implementation is determined in the duly conducted state reviews:

- national cybersecurity system;
- cyber protection of critical information infrastructure, state information resources and information, the requirement for protection of which is established by law.

The results of the reviews can be the basis for making changes to the general plan and / or annual action plans for the implementation of the Strategy, due to the need to adapt to changes in the security environment, eliminate and minimize negative trends in cybersecurity.

The strategy is the basis for the development of other regulations in the field of cyber security of Ukraine, as well as to justify the distribution of the necessary material, human and other resources.

Funding for the implementation of the Strategy will be provided within the expenditures provided by the State Budget of Ukraine for the security and defense sector, which will be considered by the National Security and Defense Council of Ukraine in the manner prescribed by the Budget Code of Ukraine. According to the law, government agencies, enterprises, institutions and organizations will include in their plans financial costs for cybersecurity. Within the framework of public-private partnership, international technical assistance, investments will be attracted, which will be aimed at building a national cybersecurity system.

Every year, the National Cybersecurity Coordination Center publishes a public report on the implementation of the Strategy according to general assessments.

The process of implementing the Strategy should be as transparent, open and accompanied by democratic civilian control as possible. To this end, the main actors of the national cybersecurity system within the competence will additionally provide annual information to the public through their own official websites about the status of their implementation of the Strategy and the status of funding for relevant activities.

Section 9. METRICS

The priority task 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 of the functioning of the cybersecurity system.

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

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

The indicators should measure the progress made by cybersecurity actors in implementing the Strategy on issues such as:

- implementation of strategic tasks within the goals set by the Strategy (for each task);
- achievement of strategic goals defined by the Strategy (for each goal);
- the degree of impact of the measures implemented within the Strategy on the national cybersecurity system and the digital transformation of the state.

The introduction of indicators of the state of cybersecurity will ensure the improvement of 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 on social development will be determined by the following criteria:

- increasing the level of public confidence in the state regarding the security of cyberspace;
- formation of a secure information society, in which, in addition to state institutions, private entities and citizens are involved in cybersecurity measures;
- 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 the aggression of the Russian Federation against Ukraine).

With the help of an extensive system of indicators will determine the state of achievement of conditions for the safe operation of cyberspace, its use in the interests of the individual, society and the state.

The system of indicators will include basic indicators of the state of cybersecurity, indicators of the national cybersecurity system and indicators of the state of cyber protection of critical information infrastructure, state information resources and information required by law, which will allow comprehensive assessment of effectiveness and efficiency of the Strategy.