Draft

THE LAW OF UKRAINE
"CRITICAL INFRASTRUCTURE AND ITS PROTECTION"

This Law establishes the principles and directions of developing a state system for the protection of critical infrastructure, defines the legal and organizational framework for the provision of its activities and is an integral part of Ukraine's national security legislation.

SECTION I
TERMS

Article 1 Definition of terms and concepts

1. In this Law the following terms are used in the given meaning:

1) an act of unauthorized interference is an act that created a threat to the safe functioning of the critical infrastructure and led to one or more of the following consequences: violated its continuity and stability; has created real or potential threats to national security;

2) critical infrastructure security – the state of critical infrastructure protection, which provides functionality, continuity of operation, integrity and stability of the critical infrastructure;

3) state system of critical infrastructure protection – a system of entities ensuring the implementation of state policy in the field of critical infrastructure protection;

4) vital services – services provided by state institutions, enterprises and organizations of any form of ownership, crashes and interruptions which result in immediate negative consequences for national security;

5) vital functions – functions performed by bodies of state power, state institutions, enterprises and organizations of any form of ownership, violation of which leads to rapid negative consequences for national security;

6) protection of critical infrastructure – all activities aimed at timely detection, prevention and neutralization of threats to the security of critical infrastructure objects, as well as minimization and mitigation of consequences in case of their implementation;

7) category of criticalness of the infrastructure object – a relative measure of the importance of the critical infrastructure object, classified according to the degree of its impact on the implementation of vital functions and the provision of vital services;

8) categorization of infrastructure objects – classification of infrastructure objects into categories of criticalness.

9) crisis situation – violation or threat of violations of the standard mode of operation of critical infrastructure or individual object, the response to which the use of additional forces and resources is required;

10) critical infrastructure – objects that are strategically important for the economy and national security, whose malfunctioning may be detrimental to vital national interests;

11) the object of critical infrastructure – an integral element of the critical infrastructure determined in accordance with the procedure established by the legislation, functionality, continuity, integrity and stability of which ensure the implementation of vital national interests;

12) critical infrastructure operator – a state body, enterprise, institution, organization, legal and / or natural person to whom, under the ownership, lease or for other legitimate reasons, the objects of critical infrastructure belong and which is responsible for its current functioning ;

13) protection of objects of critical infrastructure – a complex of regime, engineering, technical and other measures that are organized and carried out by subjects of the state system of protection of critical infrastructure in order to prevent and / or non-admit or stop illegal actions on objects of critical infrastructure ;

14) security passport is a document of the defined form that contains structured data about the critical infrastructure object and defines a set of measures taken by the operator to protect this object from all types of threats (information contained in a security certificate may be attributed to the information constituting official information, state or commercial secret);

15) level of criticalness – a relative measure of the importance of critical infrastructure objects, which takes into account the impact of a sudden cessation of functioning or functional failure on the security of supply, providing society with important goods and services;

16) operating mode of critical infrastructure – defined conditions and requirements for the functioning of critical infrastructure, depending on the state and dynamics of the situation development (standard mode of operation, crisis prevention mode, crisis mode, rescue mode);

17) critical infrastructure sector – a set of critical infrastructure objects that belong to one sector of the economy and / or have a common functional orientation;

18) stability of critical infrastructure – the state of critical infrastructure, which ensures its ability to function in the standard mode, adapt to constantly changing conditions, resist and quickly recover from the impact of threats of any kind;

19) entities of the state system for the protection of critical infrastructure – bodies of state power, local self-government bodies, the Armed Forces of Ukraine and other military formations formed in accordance with the laws of Ukraine, law enforcement bodies, as well as enterprises, institutions and organizations, regardless of the form of ownership, which carry out activities related to security of objects of critical infrastructure;

20) critical technological information – data that is processed (received, transmitted, stored) in the control systems of technological processes of objects of critical infrastructure.

2. Other terms are used in the meanings set forth in the Code of Civil Protection of Ukraine, the Criminal Code of Ukraine, the Laws of Ukraine "On Fundamentals of National Security of Ukraine", "On Combating Terrorism", "On the

Physical Protection of Nuclear Installations, Nuclear Materials, Radioactive Waste, Other Ionizing Sources" , "On the objects of high danger", "On the main principles of ensuring the cyber security of Ukraine", "On information", "On state secrets", "On operative-search activity", "On counterintelligence activity "," On the Legal Status of Emergency Situations "," On the Legal Status of the Military Status ".

Article 2 The legal basis for critical infrastructure protection.

1. The legal basis for activities in the field of critical infrastructure protection is the Constitution of Ukraine, international treaties relating to the protection of critical infrastructure, the consent of which is binding on the Verkhovna Rada of Ukraine, this Law, other laws of Ukraine, acts of the President, the Cabinet of Ministers of Ukraine, as well as other regulatory framework adopted for the implementation of this Law.

Article 3 Scope of the Law

1. The law regulates activities in the field of critical infrastructure protection in peacetime and in a state of emergency. Activities in the field of protection of critical infrastructure in terms of a martial law are regulated by other laws of Ukraine.

CHAPTER II.
BASIC PRINCIPLES OF THE STATE POLICY IN THE PROTECTION OF CRITICAL INFRASTRUCTURE

Article 4. Principles of state policy in the field of critical infrastructure protection

1. Principles of state policy in the field of critical infrastructure protection.

2. State policy in the field of critical infrastructure protection is based on the following principles:

1) recognition of the need to ensure the continuity and sustainability of the functioning of the critical infrastructure;

2) definition of legislative requirements for the protection of critical infrastructure;

3) determining of the powers and responsibilities of the state system of critical infrastructure protection entities;

4) creation of conditions aimed at minimizing the realization of possible threats, elimination and/or minimization of the realized threats consequences, crisis situations and other types thereof;

5) creation of conditions for the rapid restoration of critical infrastructure functioning in the event of realized threats, crisis situations;

6) Creating threats management system for critical infrastructure;

7) introduction of interaction between the state, business entities, expert environment and population on issues of ensuring the protection and stability of critical infrastructure;

8) ensuring international cooperation in the field of critical infrastructure protection.

3. State policy in the field of critical infrastructure protection is aimed at forming a complex of organizational, regulatory, engineering, technical, operational,

scientific and other measures aimed at ensuring the security and stability of critical infrastructure.

4. State policy in the field of critical infrastructure protection in the temporarily occupied territories is carried out in accordance with the Laws of Ukraine "On the peculiarities of the state policy of ensuring state sovereignty of Ukraine in temporarily occupied territories in the Donetsk and Luhansk regions", "On ensuring the rights and freedoms of citizens and the legal regime in the temporarily occupied territory of Ukraine".

Article 5. Basic principles of state policy in the field of critical infrastructure protection

1. The basic principles of state policy in the field of critical infrastructure protection include:

1) co-ordination;

2) the unity of methodological foundations;

3) public-private interaction;

4) ensuring confidentiality;

5) international cooperation.

Article 6 Aim and tasks of the state policy in the field of critical infrastructure protection

1. The purpose of the state policy in the field of critical infrastructure protection is to ensure an uninterrupted and stable functioning of the critical infrastructure of Ukraine, prevent the acts of unauthorized interference, forecast and oppose crisis situations with a negative impact on the critical infrastructure objects, as well as increase the protection level, improve the security measures and sustainability of these objects from existing threats.

2. The tasks of the formation and implementation of state policy in the field of protection of critical infrastructure in Ukraine include:

1) ensuring the security, stability and integrity of Ukraine's critical infrastructure;

2) prevention of crisis situations which violate the stable functioning of critical infrastructure;

3) creation and organization of a state system of critical infrastructure protection, including designation an Authorized Body for the Protection of Critical Infrastructure of Ukraine and defining the competence and authority in the field of critical infrastructure protection of other entities of the state critical infrastructure protection system;

4) development of a legal framework for juridical regulation of security at the critical infrastructure objects;

5) development and implementation of the state target programs for the protection of critical infrastructure;

6) development of a set of measures for the detection, prevention and elimination of the consequences of incidents on objects of critical infrastructure of Ukraine;

7) establishment of mandatory requirements of enhancing security of the critical infrastructure objects, their safety at all the stages of the life cycle, including at the time of creation, bringing into service, modernization;

8) analysis of the challenges and threats that affect the stability of the critical infrastructure, assessment of its security;

9) establishment of scientifically grounded approaches to the analysis of the effectiveness of state policy in the field of critical infrastructure protection.

Article 7 Management levels of the state system of critical infrastructure protection

1. The state critical infrastructure protection system includes the following levels of governance:

1) the state level, which is carried out by the Cabinet of Ministers of Ukraine, the Authorized body for the protection of critical infrastructure of Ukraine, state authorities in conformity with the distribution of powers, in accordance with this law;

2) the regional and sectoral level, which is carried out by state authorities, which, in accordance with the procedure established by the legislation, are designated responsible for the relevant sectors of critical infrastructure and their protection;

3) the local level, carried out by the local executive authorities within the powers entrusted to them by this law;

4) the object level, carried out by the operator of the critical infrastructure on the basis of legal and regulatory acts in the field of critical infrastructure protection.

CHAPTER II.
CRITICAL INFRASTRUCTURE OF UKRAINE

Article 8 Objects of critical infrastructure

1. Critical infrastructure objects can include enterprises, institutions, organizations regardless of ownership, which:

1) carry out activities and provide services in the sectors of energy, chemical industry, transport, information and communication technologies, electronic communications, banking and financial sectors;

2) provide services in the areas of life support of the population, in particular in the areas of centralized water supply, centralized drainage, heat energy, hot water, electric energy and gas supply, food production, nutrition, health care;

3) are included in the list of enterprises with strategic importance for the economy and security of the country;

4) are subject to protection and defense during emergency state and special period;

5) are the objects of high danger;

6) are the objects of national importance, have branched links and significant influence on another infrastructure;

7) are the objects, malfunction of which will lead to a crisis situation of regional significance.

Article 9 Criteria for assigning objects to critical infrastructure

1. Attribution of the objects to critical infrastructure is determined by a set of criteria that evaluates their importance for the fulfillment of vital functions and the provision of vital services, indicates the existence of threats to it, the possibility of emergency situations due to interference in their functioning, the cessation of functioning, the human factor or natural disasters, the duration of work to eliminate such effects until the full restoration of the regular regime, namely:

1) the existence of challenges and threats that may arise in relation to the objects of critical infrastructure ;

2) the infliction of significant damage to the normal life conditions of the population;

3) the vulnerability of these objects, severity of the occurrence of possible negative consequences, resulting in significant harm: to the public health (is determined by the number of victims, the deaths and persons who got significant injuries, as well as the number of evacuated population); to the social sphere (destruction of systems of social protection of the population and provision of social services, the loss of state's ability to meet the critical needs of society); to the economy (impact on GDP, the size of economic losses, both direct and indirect); to the natural resources of national importance; to the defense capability; to the image of the country;

4) the scale of negative consequences for the state, which: will affect the activity of strategically important objects for several sectors of life support or will lead to the loss of unique nationally significant assets, systems and resources, will have long-term consequences for the state and affect the activities of several other sectors;

5) the duration of elimination of such consequences and the effect of further negative impact on other sectors of the state;

6) the impact on functioning of related sectors of critical infrastructure.

Article 10 Categorization of objects of critical infrastructure

1. In order to determine the level of requirements for ensuring the protection of critical infrastructure, powers and responsibilities of entities, within the sectors, the categorization of critical infrastructure objects covered by the state protection system of critical infrastructure is carried out:

1) The first category of criticality – critical objects – objects of national importance, branched links and significant impact on another infrastructure. These objects are included in the National list of objects of critical infrastructure, requirements for ensuring their protection are formed;

2) The second category of criticality – vital objects, the malfunction of which will lead to a emergency situation of regional significance. These objects are included in the National List of Critical Infrastructure objects, requirements are created for differentiating the tasks and powers of public authorities and critical infrastructure operators, aimed at ensuring its protection and restoration of functioning;

3) The third category of criticality – important objects. The priority of protecting such objects is to ensure the rapid restoration of functions due to diversification and reserves. Responsibility for the stability of the functioning of the objects is carried

out by operators in accordance with the requirements established by law for interaction with public authorities;

4) The forth category of criticality – the necessary objects. The objects of infrastructure, the direct protection of which is the responsibility of the operator, who has to have a plan for reaction during an emergency situation.

2. The categorization of objects of critical infrastructure within certain sectors of critical infrastructure is carried out by the sectors responsible for the state system of critical infrastructure protection.

3. The entities of the state critical infrastructure protection system designated by the critical infrastructure sectors are compiling and conducting Lists of the critical infrastructure objects.

4. Mandatory requirements for the providing of critical infrastructure protection infrastructure are set to the objects of the 1st and 2nd category of criticality .

5. Recommendation requirements concerning the level of providing the protection and infrastructure sustainability are set to the infrastructure objects of the III category of criticality.

Article 11. Compilation and maintenance of the National List of Critical Infrastructure Facilities

1. The National List of critical infrastructure objects is being formed for the purposes of coordinating the actions of the entities of the state protection system of critical infrastructure on the organization of the protection of the most important infrastructure.

2. The collection, generalization, preliminary analysis of data concerning the objects of critical infrastructure and proposals for the inclusion of such objects in the National List of critical infrastructure objects within certain sectors is carried out by the sectors responsible for the state system of critical infrastructure protection.

3. The National List of critical infrastructure objects is formed and maintained by the Agency for the Protection of Critical Infrastructure on the basis of proposals provided by the entities of the state system for the protection of critical infrastructure, which were addressed to the Agency for the Protection of Critical Infrastructure.

4. After enlisting an object in the National List of Critical Infrastructure objects, the entity responsible for the state critical infrastructure protection system informs the operator of the critical infrastructure object for the certification of the critical infrastructure object.

5. The procedure for keeping the National List, enlisting objects in the National List of Critical Infrastructure objects, and providing information from the National List shall be established by the Cabinet of Ministers of Ukraine upon submission of the Agency for the Protection of Critical Infrastructure of Ukraine.

6. The Cabinet of Ministers of Ukraine approves a list of critical infrastructure sectors and establishes the subjects of the state critical infrastructure protection system that are responsible for the sectors, in order to distribute functions for the protection of critical infrastructure objects among the entities of the state critical infrastructure protection system.

7. In order to ensure a proper level of critical infrastructure protection, the entities responsible for the state critical infrastructure protection system may engage other entities of the state system of critical infrastructure protection, including on a contractual basis, in accordance with their authority, established by this Law and other regulatory frameworks controlling the activity of such subjects of the state system of protection of critical infrastructure.

8. Involvement of subjects of the state system of protection of critical infrastructure to protect critical infrastructure objects is carried out after the development, compilation and adjusting with designated authorities and service passports of safety on objects of critical infrastructure.

Article 12 Certification of objects of critical infrastructure

1. In order to analyze the main possible threats and potential negative consequences for critical infrastructure objects, prevent such threats to critical infrastructure, operators of critical infrastructure facilities prepare and submit to the responsible for critical infrastructure protection sectors, The Security Service of Ukraine and the entity of the provision of physical security, a security passport for each critical infrastructure object.

2. A security passport for a critical infrastructure object includes: procedures for identifying an object and measures for its protection and safety, and also defines a list of responsible persons whose tasks include communication and exchange of information with the entities of the state system of critical infrastructure protection.

3. A form of a security passport, a procedure for its development, content and terms of submission, shall be established by the Cabinet of Ministers of Ukraine.

4. The Critical Infrastructure Operator is responsible for the accuracy of the data contained in the security passport and the timeliness of its changes.

CHAPTER III.
STATE SYSTEM OF PROTECTION OF CRITICAL INFRASTRUCTURE

Article 13. Coordination of the activity of executive authorities in the field of critical infrastructure protection

1. The Cabinet of Ministers of Ukraine ensures the implementation of state policy in the field of critical infrastructure protection of Ukraine, organizes and provides the necessary forces, means and resources for functioning of the state system of protection of critical infrastructure.

2. A national network of situational crisis centers (information-analytical, dispatching), functioning by structural subdivisions of the entities of the state system for the protection of critical infrastructure, is created and functioning to create a system of informational and analytical support of the decision-making process on ensuring the protection and stability of critical infrastructure.

The Cabinet of Ministers of Ukraine approved Regulation of information exchange to ensure information exchange and collaboration of entities of the critical infrastructure protection

Article 14. Subjects of the state system of protection of critical infrastructure

1. The entities of the state system of critical infrastructure protection are:

1) Authorized Body for the Protection of Critical Infrastructure of Ukraine;

2) ministries and other central executive bodies;

3) law enforcement and intelligence agencies;

4) the Security Service of Ukraine;

5) the Armed Forces of Ukraine, other military formations, formed in accordance with the laws of Ukraine;

6) local state administrations;

7) critical infrastructure operators;

8) public organizations, population.

Article 15. Operating modes of the state critical infrastructure protection system

1. Ensuring protection and stability of critical infrastructure is carried out in the following operating modes:

1) standard mode – entities of the state system of protection of critical infrastructure concerning the assessment of possible threats and information about them;

2) the state of preparedness and prevention of the realization of threats – entities of the state system of protection of critical infrastructure verify and transfer the security system to the readiness to provide protection and response in case of a threat;

3) crisis response mode – entities of the state system of protection of critical infrastructure use crisis response measures. Infrastructure functioning is carried out in a crisis situation, restrictions are imposed on the operating modes of infrastructure objects, economic conditions of management, access to facilities.

4) resumption of regular operation mode – entities of the state system of protection of critical infrastructure take measures to return the parameters of the functioning of critical infrastructure to the standard mode. Infrastructure operation is carried out with restrictions in accordance with the specified deadlines for the liquidation of the consequences of the crisis.

For each operating mode of critical infrastructure responsible for critical infrastructure sectors, is developed a plan for interaction with other entities of the state defense system, which must be agreed with the procedure established by law.

The decision to declare the critical infrastructure operating modes and the introduction of certain legal statuses is accepted by the entity responsible for the sector of critical infrastructure.

Article 16. Authorized Body for Critical Infrastructure Protection

1. In order to form and implement the state policy in the field of critical infrastructure protection, the Authorized Agency for the Protection of Critical Infrastructure is established and functioning.

2. Authorized Body for the Protection of Critical Infrastructure of Ukraine:

1) coordinates the activity of ministries and other central executive authorities in the sphere of protection and safety of objects of critical infrastructure of Ukraine;

2) interacts with operators of critical infrastructure of Ukraine on issues of ensuring the protection of objects of critical infrastructure;

3) assesses the security of critical infrastructure objects included in the National List of Critical Infrastructure objects;

4) performs checks on the accuracy of assigning objects to the critical infrastructure;

5) carries out an assessment of threats to critical infrastructure at the national level with the involvement of the entities of the state critical infrastructure protection system, identified as responsible for critical infrastructure sectors;

6) maintains the National List of critical infrastructure objects of Ukraine;

7) develops and submits for approval by the Cabinet of Ministers of Ukraine:

National plan for protection and stability of critical infrastructure;

a list of critical infrastructure sectors and critical infrastructure entities responsible for these sectors;

the procedure for the development, form and content of the safety passport of the critical infrastructure object;

the procedure for the development, form and content of the plans for critical infrastructure protection are adopted at the national level;

proposals for the announcement of changing the operating modes of the state system of critical infrastructure protection;

typical requirements for ensuring the protection and stability of critical infrastructure objects according to critical categories;

8) applies to the National Academy of Sciences of Ukraine, the National Institute for Strategic Studies, other scientific institutions, institutions of higher education, for carrying out scientific, scientific and technical activities on issues of ensuring the protection and stability of critical infrastructure objects;

9) exercises other authorities provided by this Law and the Regulation on the Authorized Body for the Protection of Critical Infrastructure of Ukraine.

3. The Regulation on the Authorized Body for the Protection of Critical Infrastructure of Ukraine is approved by the Cabinet of Ministers of Ukraine.

Article 17. Security Service of Ukraine

1. Security Service of Ukraine:

1) participates in the formation and implementation of state policy in the field of critical infrastructure protection;

2) carries out counter-intelligence, counter-terrorism and counter-protection protection of critical infrastructure objects, protection of its economic and scientific and technical potential, exchange of information on threat assessment and response to threats and crisis situations, as well as liquidation of their consequences in cooperation with other entities of the state system of protection of critical infrastructure related to the illegal activities of special services of foreign states, the negative impact of certain organizations, groups and individuals, and develops and respond to them;

3) takes measures to prevent, detect, prevent and stop the manifestations of terrorist financing, extremism, separatism with the use of objects of critical infrastructure;

4) participates in the verification of investments and the origin of the funds aimed at financing critical infrastructure, for the purpose of following their interests of national security of the state;

5) take measures to prevent and counteract acts of unauthorized interference with the operation of critical infrastructure objects, financing of critical infrastructure out of the interests of national security,

6) receives in the manner prescribed by law access to automated information and reference systems, registers and data banks, the holder (administrator) of which are state authorities, operators of objects of critical infrastructure;

7) controls, within the scope of competence, the implementation of measures on the prevention, detection, prevention and suspending of leakage of information with restricted access, loss of its material resources, the localization of possible consequences, as well as the identification and elimination of the existing preconditions for this, within the framework of the critical infrastructure objects;

8) participates in the restriction and blocking of access to the objects and resources used for the organization, preparation, execution, financing, promotion or concealment of an act of unauthorized interference with the activity of critical infrastructure, as well as in other cases stipulated by the laws of Ukraine in accordance with the procedure established legislation;

9) carries out the verification of agreements for the supply of goods, works and services to objects of critical infrastructure and personnel of contractors for the purpose of damaging the national security of Ukraine;

10) participates in the development of categorization, determination of criteria and procedure for assessing the state of safety and security of critical infrastructure objects;

11) carries out a special inspection of persons for admission to objects of critical infrastructure;

12) submits to the bodies of state authority, local self-government bodies, enterprises, institutions, organizations of all forms of ownership mandatory proposals for the protection of critical infrastructure, and mandatory for execution of requests for activities of critical infrastructure objects, requirements for observance of legislation;

13) participates in the verification and assessment of the security of critical infrastructure objects, the approval of security passports for each facility;

14) participates in the procedure established by legislation, in response to crisis situations related to the security, protection, stability and integrity of critical infrastructure;

15) uses for its activities information on critical infrastructure received from the Authorized Agency for the Protection of Critical Infrastructure of Ukraine and other entities for the protection of critical infrastructure;

16) acquaints public authorities, local government bodies, operators of critical infrastructure objects with documents and other physical storage media necessary for the prevention, detection and prevention of acts of unauthorized interference with the operation of critical infrastructure objects, including those, containing restricted information;

17) directs the servicemen of the Security Service of Ukraine for work in the positions of the Authorized Body for the Protection of Critical Infrastructure of Ukraine, objects of critical infrastructure irrespective of the forms of ownership in the interests of their protection;

18) initiates the use and prosecution of officials of operators of critical infrastructure objects, for failure to take measures for the safe operation of critical infrastructure objects and for committing (or not) their actions that lead to a decrease in their regime of protection, stability, integrity and do not provide for their recovery in case of refusals, attacks and other crises;

19) creates databases on the threats and vulnerabilities of critical infrastructure objects;

20) takes measures to ensure the fulfillment of Ukraine's international obligations in the framework of the protection of critical infrastructure;

21) carries out international cooperation and interacts with foreign state and special law-enforcement bodies in the framework of providing international legal assistance in the field of critical infrastructure protection;

22) carries out analytical processing of information, conducts counterintelligence, operative-search, search, regime, administrative, legal and other measures aimed at combating cyberterrorism and cyber-espionage in relation to objects of critical information infrastructure;

23) participates in the investigation of cyber incidents and cyber attacks on state electronic information resources, information required by law for protection, critical information infrastructure, and provides responses to cyber incidents in the field of state security;

24) carries out other activities for the protection of critical infrastructure within the limits of the powers determined by the laws regulating activities of critical infrastructure protection actors.

2. The Security Service of Ukraine carries out activities in the field of critical infrastructure protection through its structural bodies (departments, divisions, units, services), which are delegated the respective powers.

Article 18. Ministry of Internal Affairs of Ukraine

1. Ministry of Internal Affairs of Ukraine:

1) participates in the formation and implementation of the state policy for the protection of critical infrastructure;

2) ensure coordination in the sphere of critical infrastructure protection of central executive authorities whose activities are directed and coordinated by the Cabinet of Ministers of Ukraine through the agency of the Minister of Internal Affairs of Ukraine and cooperation with other entities of the state system of critical infrastructure protection;

3) participates in measures to ensure the stability of critical infrastructure facilities, to re-enforce their protection against criminal acts, terrorist acts and cyber attacks, to develop public-private interaction with regard to threats to critical infrastructure and to create an effective system for managing its security.

Article 19. Central body of executive power, which implements state policy in the field of civil protection

1. Central body of executive power, which implements state policy in the field of civil protection:

1) participates in the implementation of state policy in the field of critical infrastructure protection by protecting people and territories from emergency situations, preventing them from occurring, rectification of the consequences of emergencies, extinguishing fires, exercising state supervision (control) for observance and compliance with the requirements of civil protection legislation , fire and technotronic security;

2) implements state policy for civil defence engineering measures on critical infrastructure facilities;

3) takes part in the evaluation of the safety of critical infrastructure facilities within the competence;

4) carries out measures on operating of emergency of objects of critical infrastructure by emergency rescue services;

5) in cooperation with the Ministry of Internal Affairs of Ukraine, the Security Service of Ukraine provides for the organization of protection against terrorist attacks of the objects of emergency rescue services, which are involved and perform their functions on critical infrastructure facilities in the event of emergencies;

6) takes part in the development of legislative and other acts in the field of critical infrastructure protection within the limits of its competence.

Article 20. National Guard of Ukraine

1. The National Guard of Ukraine in the field of critical infrastructure protection provides:

1) protection of critical infrastructure facilities, lists of which are determined by the Cabinet of Ministers of Ukraine;

2) participation in the elimination of the consequences of crisis situations on the facilities.

Article 21. National Police of Ukraine

1. The National Police of Ukraine in the field of critical infrastructure protection provides:

1) counteracting criminal encroachments on critical infrastructure facilities or important state facilities that threaten the safety of citizens and violate the functioning of life support systems;

2) implementation on a contractual basis of the protection of critical infrastructure facilities, the lists of which are determined by the Cabinet of Ministers of Ukraine;

3) protection of critical infrastructure, interests of society and the state from criminal encroachment in cyberspace, takes measures for prevention, detection, termination and disclosure of cyber crime against critical infrastructure facilities;

4) conducting, in conjunction with the Security Service of Ukraine, the verification and assessment of the security of the critical infrastructure facilities of categories II, III and IV, the protection of which is entrusted to the National Police of Ukraine, and the approval of security passports for each such facility.

Article 22. Ministry of Defence of Ukraine

1. The Ministry of Defense of Ukraine in the field of critical infrastructure protection provides:

1) the organization of protection against terrorist attacks of the Armed Forces facilities, armaments, military equipment, facilities located in military units or stored at definite places, the preparation and use of the Armed Forces (forces) of the Armed Forces in the event of a terrorist act in the airspace or territorial waters of Ukraine;

2) participation in the conduct of anti-terrorist operations on military facilities;

3) implementation of measures to improve the survivability and fire and explosion safety of arsenals, bases and depots of the Armed Forces of Ukraine;

4) fulfillment of the tasks of air-covering of important state facilities, the list of which is determined by the Cabinet of Ministers of Ukraine.

Article 23. State Special Transport Service

1. The State Special Service for Transport provides, in the sphere of protection of critical infrastructure, in the peaceful and special period:

1) organization, planning and realization of works on technical protection and reconstruction of objects of the national transport system of Ukraine;

2) protection of state objects of the national transport system of Ukraine, the list of which is determined by the Cabinet of Ministers of Ukraine.

Article 24. The central executive body, which ensures the formation and implementation of state policy in such complexes as electrical energy, nuclear industry, coal industry, peat extraction, petroleum, oil and gas processing, and also provides the formation of state policy in the field of supervision (control) over the sectors of electrical energy and heat supply.

1. Within the competence of the central executive body, which ensures the formation and implementation of state policy in such complexes as electrical energy, nuclear industry, coal industry, peat extraction, petroleum, oil and gas processing, and also provides the formation of state policy in the field of supervision (control) over the sectors of electrical energy and heat supply in the area of protection of critical infrastructure, it:

1) participates in the formation and implementation of state policy in the field of critical infrastructure protection;

2) exchanges information on the threat assessment, threat and crisis situations response issues, as well as eliminates their consequences in cooperation with other subjects of the state system of critical infrastructure protection;

3) ensure the implementation of measures for the prevention, detection and suppression of terrorist acts and crimes of terrorist nature on objects belonging to its sphere of management;

4) takes part in the international cooperation on the critical infrastructure protection issues;

5) creates in its economy a structural subdivision for the protection of critical infrastructure;

6) prepares proposals for the inclusion of infrastructural objects in the critical infrastructure;

7) collects, summarizes and performs preliminary analysis of the data about the objects of critical infrastructure and their functioning in the energy sector;

8) ensures the functioning of the relevant systems of information exchange, monitoring of security conditions at critical infrastructure objects in the energy sector;

9) participates in the procedure established by law, in response to crisis situations related to the security, protection and resilience of critical infrastructure in the energy sector;

10) provides early warning (threat warning) to critical infrastructure operators and provides informational, advisory, expert and technological assistance to critical infrastructure operators in the energy sector, users of their services (the population) in order to prevent, respond and minimize the possible impact of the threats;

11) develops and implements standards, norms and regulations for the protection of critical infrastructure in the energy sector of critical infrastructure;

12) carries out inspections and assessments of the security of critical infrastructure objects in the energy sector;

13) provides critical infrastructure operators with the proposals for critical infrastructure protection in the energy sector and mandatory requirements for eliminating the causes and conditions that violate the integrity and stability of the critical infrastructure;

14) introduces sectoral programs to counter the threats of internal perpetrators, in particular through the measures aimed at achieving a high level of security culture (physical and technical);

15) takes part in approval and registration of safety passports for critical infrastructure objects in the energy sector, as well as in identifying risks for the administrative units.

Article 25. Central body of executive power, which ensures the formation and implementation of state policy in the areas of automobile, rail, sea and river transport, provision of postal services

1. Central body of executive power, which ensures the formation and implementation of state policy in the areas of automobile, rail, sea and river transport, provision of postal services:

1) ensures the formation of a state policy on the protection of objects of critical infrastructure of the transport industry on the basis of constant analysis of the state of their security;

2) ensures the legal regulation of state policy in the areas that fall within its competence, develops and implements sectoral standards and norms concerning the protection of objects and/or elements of the critical infrastructure of the objects of the national transport system;

3) provides preparation of proposals for the inclusion of objects (elements) of the national transport system in the list of objects (elements) of the critical infrastructure in the transport sector;

4) coordinates training of the critical infrastructure objects' employees in the transport sphere;

5) carries out monitoring, constant analysis of the state of affairs and assessment of the results of the implementation of the state policy on the protection of objects (elements) of critical infrastructure in the transport sector, develops

proposals for its improvement and options for solving the identified problems, assesses their benefits and risks;

6) develops proposals for the formulation of state policy based on the results of the analysis, coordination of interests, goals and ways of solving problems;

7) participates in public awareness campaigns on the protection of critical infrastructure;

8) carries out measures to adapt Ukrainian legislation to the legislation of the European Union in accordance with the obligations of Ukraine within the framework of the Association Agreement, explores European experience on the protection of critical infrastructure in the transport sector;

9) participates in the international cooperation on the protection of critical infrastructure, coordinates the attraction, provision and the use of international financial assistance for the protection of critical infrastructure in the transport sector;

10) in the established procedure, participates in responding to crisis situations aligned with the commission of acts of unauthorized interference;

11) provides consulting and expert assistance to critical infrastructure operators in the field of critical infrastructure protection in the transport sector;

12) participates in the approval and registration of security passports of critical infrastructure objects in the transport sector.

Article 26. State Service of Special Communication and Information Protection of Ukraine

1. State Service of Special Communication and Information Protection of Ukraine in the field of critical infrastructure protection:

1) ensures the formation and implementation of state policy on cyber defense of objects of critical information infrastructure, exercises state control in this area;

2) ensures the implementation of the informational security audit on critical infrastructure objects, establishes the requirements for information security auditors, and determines the procedure for their certification (re-certification);

3) coordinates, organizes and conducts audit of the security of communications and technological systems of objects of critical infrastructure for vulnerability;

4) ensures the formation and functioning of the state register of communication systems, control systems for technological processes, which operates on objects of critical infrastructure;

5) establishes general requirements for cyber defense of objects of critical infrastructure, maintains a list of objects of critical information infrastructure and carries out measures for its updating and actualization;

6) coordinates the activities of entities which provide cyber security regarding cyber defense of critical infrastructure objects;

7) informs about cyber threats and appropriate methods of protection against them;

8) provides critical infrastructure operators with advisory and practical assistance in preventing, detecting and eliminating the effects of cyber incidents on their objects;

9) exchanges information between public authorities and the private sector regarding cyber threats to the critical infrastructure objects;

10) carries out international cooperation on the issues of cyber security of critical infrastructure objects, ensures the implementation of international initiatives in the field of cyber security of critical infrastructure objects, corresponding with the national interests of Ukraine.

Article 27. Central executive body, which realises national policy on implementation of state supervision (control) in the field of environmental protection, rational use, reproduction and conserving of natural resources

1. The Central executive body, which realises national policy on implementation of state supervision (control) in the field of environmental protection, rational use, reproduction and conserving of natural resources, ensures:

realisation of national policy on implementation of state supervision (control) in the field of environmental protection, rational use, reproduction and conserving of natural resources;

within the limits of powers envisaged by the law, implementation of state supervision (control) over the compliance with the requirements of environmental legislation, in particular, on the objects of critical infrastructure for assessing their protection state against the possible occurrence of accidents, emergency, technogenic and ecological situations and natural phenomena that may cause significant extent of damage aligned with pollution, damage or destruction of its natural resources;

in accordance with the procedure established by law, participation in responding to crisis situations, by means of crisis monitoring of objects of the environment from the onset of their accidental pollution to the restoration of indicators of their natural state;

within the limits of authority, usage of information concerning critical infrastructure received from the Authorized Body for the Protection of Critical Infrastructure of Ukraine and other entities for the protection of critical infrastructure;

provision of critical infrastructure operators with mandatory requirements for critical infrastructure protection and mandatory requirements on critical infrastructure activity and instructions on eliminating the causes and conditions that violate the critical infrastructure sustainability;

providing suggestions within the limits of competence, prior to establishing the categories of critical infrastructure objects, defining criteria and procedures for assessing the state of safety and security of critical infrastructure objects;

access to automated information and reference systems, registers and data banks, the holder (administrator) of which are state authorities, operators of objects of critical infrastructure;

preparation of proposals for the inclusion of infrastructure objects in the critical infrastructure.

Article 28 Other central executive bodies

1. Other central executive bodies in the field of critical infrastructure protection:

1) take part, in accordance with the procedure established by law, in responding to crisis situations related to the security, protection and stability of the critical infrastructure;

2) prepare proposals for the inclusion of infrastructure objects in the critical infrastructure;

3) form a list of objects of critical infrastructure that belong to the sphere of their management and require priority protection in the case of complication of the situation, the emergence of a threat, including ones caused by the terrorist threats;

4) carry out other activities for the protection of critical infrastructure within the limits of the authority specified by the laws which regulate the activities of the critical infrastructure protection actors.

2. Other central executive bodies carry out activities in the field of critical infrastructure protection through their territorial bodies and/or enterprises, institutions and organizations that are in the sphere of their management.

Article 29 Executive bodies identified as responsible for relevant sectors of critical infrastructure

1. State executive bodies identified as responsible for the relevant critical infrastructure sectors:

1) establish structural units for the protection of critical infrastructure;

2) prepare proposals for the inclusion of infrastructure objects into critical infrastructure;

3) collect, summarize and carry out preliminary analysis of data on objects of critical infrastructure and their functioning;

4) develop and confirm requirements for ensuring the protection and stability of the critical infrastructure sectors; threats to critical infrastructure in the relevant sectors; plans for interaction of subjects of the state system for protection of critical infrastructure in the relevant sectors for all functioning modes of critical infrastructure;

5) ensure the functioning of the relevant information exchange systems, monitoring of security conditions at the objects of critical infrastructure;

6) in accordance with the procedure established by law, participate in responding to crisis situations related to the security, protection and stability of critical infrastructure;

7) carry out early warning (threat warning) of critical infrastructure operators and provide information, advisory, expert, technological assistance to critical infrastructure operators, users of their services (to the population) in order to prevent, respond, minimize the possible impact of the threats;

8) develop and implement standards, norms and regulations for the protection of critical infrastructure in relevant sectors of critical infrastructure;

9) carry out inspections and assessments of the security of critical infrastructure objects;

10) provide critical infrastructure operators with the proposals for critical infrastructure protection in the energy sector and mandatory requirements for eliminating the causes and conditions that violate the integrity and stability of the critical infrastructure;

11) implement sectoral programs to counter the threats of internal perpetrators, including due to measures aimed at achieving a high level of safety culture (physical

and technical);

12) take part in the approval and registration of security passports of critical infrastructure objects, as well as in determining the risks for administrative-territorial units;

13) organize a system of personnel training, education and practice on ensuring the stability and protection of the critical infrastructure sectors, etc.

Article 30. Local executive bodies

1. Local executive bodies in the field of critical infrastructure protection provide:

1) the development of local programs for the protection and sustainability of critical infrastructure, programs to increase community resilience to crises caused by the cessation or deterioration of the provision of essential services for their lives or access to vital resources;

2) development and agreement with interested bodies of local plans of interaction between involved actors, plans for restoration of the operation of critical infrastructure.

Article 31. Critical Infrastructure Operators

1. The main tasks of critical infrastructure operators are:

1) providing security of critical infrastructure facilities, in particular, creation, establishment and maintenance of functioning of an effective system of physical security, security of operating systems and cyber security;

2) development and updating of object plans of actions on protection and safety of critical infrastructure, as well as cyber defense measures;

3) providing risk assessments at critical infrastructure facilities and exchanging information about risks and threats with other entities of the state system of critical infrastructure protection of the state, local and private sectors;

4) taking operational measures in case of receiving information about the threat of penetration into the territory of facility;

5) operational cease of unlawful acts, physical attacks aimed at disconnecting or damaging the functioning of operating systems or systems providing physical security of the critical infrastructure facility;

6) organization of measures for responding to incidents, crisis situations, as well as rectification of their consequences on the critical infrastructure facilities in cooperation with other entities of the state system of critical infrastructure protection;

7) ensuring the restoration of the functioning of critical infrastructure facilities in the event of accidents / failures, committing unlawful actions or the impact of natural phenomena;

8) participation in airspace protection measures over definite critical infrastructure facilities;

9) to inform immediately the bodies of the National Police of Ukraine, the Security Service of Ukraine, the units of the National Guard of Ukraine and other state bodies on incidents related to any violations of the systems of physical security and cyber security;

10) ensuring constant communication with the responding authorities and with other authorized organizations and institutions;

11) ensuring constant interaction with the enterprises providing centralized water supply, centralized drainage, heat supply, power supply, telecommunication networks, transport, medical care, security and many other services, on which depends the process of crisis response and rehabilitation of critical infrastructure;

12) creation of the indispensable reserves of financial and material resources for responding to crisis situations and rectification of their consequences;

13) the appointment of responsible for protection, physical and cybernetic security at facilities, conducting education, training and checking personnel responsible for the protection and safety of critical infrastructure facilities;

14) protection of information on management system, communications, physical and cybernetic security, and ensuring, in accordance with the legislation requirements, the confidentiality of information during the processing of data on critical infrastructure facilities.

2. Critical Infrastructure Operators Have the Right:

1) to receive, in accordance with the established procedure, from the authorized bodies of state power, information lodged to them on the right of ownership or other legal basis related to the security of critical infrastructure facilities;

2) independently develop measures to ensure the security of critical infrastructure facilities, which do not contradict the requirements of this Law and the legislative acts adopted in accordance with it.

3. Critical Infrastructure Operators are bound to:

1) to provide protection, including physical and cyber defense, of the critical infrastructure facilities lodged to them on a property right or on another legal basis;

2) to send, within the prescribed time limits, to the controlling entities of the protection of critical infrastructure information on the implementation of measures contained in the statement on the results of the control and evaluation of the safety of critical infrastructure facilities;

3) promptly inform responsible for the critical infrastructure protection sectors about the incidents occurring on facilities of critical infrastructure lodged to them on a property right or other lawful basis;

4) to fulfill within the prescribed time limit the requests (requirements) concerning the provision of information on critical infrastructure facilities;

5) provide unimpeded access of controlling entities for the protection of critical infrastructure to the facilities of critical infrastructure, in the exercise of their powers created by this Law and other legislative acts;

6) to assist other entities of protection of critical infrastructure in identifying, preventing and stopping acts of unauthorized interference, as well as in eliminating their consequences, establishing the causes and conditions for their commitment;

7) ensure the integrity and constant operation of critical infrastructure facilities with the minimum possible risk;

8) ensure the implementation of the technical conditions (regulations), the procedure for the establishment and operation, as well as the maintenance of technical means for detecting, preventing and eliminating the consequences of cyber attacks on the information resources of critical infrastructure facilities;

9) comply the requirements of this Law and other legislative acts regulating activities of critical infrastructure facilities.

CHAPTER IV.
ORGANISATIONAL BASES OF THE STATE CRITICAL INFRASTRUCTURE PROTECTION SYSTEM

Article 32. Organisational frameworks of critical infrastructure protection

1. The protection of critical infrastructure includes:

1) determination of sectors of critical infrastructure, establishment of responsible of critical infrastructure protection for specified sectors;

2) compartmenting of objects of critical infrastructure for determining the level of requirements for ensuring the protection of critical infrastructure, powers and responsibilities of entities;

3) compilation and maintenance of the National List of Critical Infrastructure Facilities;

4) certification of critical infrastructure facilities;

5) the determination of critical infrastructure functioning and drafting of the crisis response plans;

6) the interaction and exchange of information between the entities of the state system for the protection of critical infrastructure and the setting of access level to such information for third parties;

7) control over the level of security of the critical infrastructure facilities and its' stability;

8) the establishment of interaction between public authorities and the private sector in the field of critical infrastructure protection;

9) the introduction of criteria and methodology for attribution infrastructure facilities to critical infrastructure;

10) the introduction of the methodology for assessment the threats to the critical infrastructure facilities and response plans to it, in particular accidents and technical failures, dangerous natural phenomena, malicious actions, etc.;

11) the implementation of measures aimed at preventing cyber incidents, the detection and protection against cyber attacks, the elimination of its' consequences, the restoration of sustainability and reliability of the functioning of communication and technological systems , and the protection of technological information circulating on critical infrastructure facilities.

Article 33. Planning of measures to ensure the stability and protection of critical infrastructure facilities

1. For the organization of the state system of critical infrastructure protection, the relevant plans and programs for responding to emergency situations are developed and approved by the Cabinet of Ministers of Ukraine, central executive authorities, local state administrations, local self-governments, and operators.

2. At the national level:

1) The National Plan for Protection and Stability of Critical Infrastructure is being developed, which must be approved by the Cabinet of Ministers of Ukraine;

2) the requirements are set for the planning of critical infrastructure protection measures, including emergency plans, crisis response plans, cooperation plans, critical infrastructure recovery plans, training plans.

3. Sectoral plans and programs to counter critical infrastructure threats are developed and approved by public athorities at the sectoral and regional levels.

4. The National Police of Ukraine, the National Guard of Ukraine, the Security Service of Ukraine, the Armed Forces of Ukraine and other bodies of security and defense sectors within their competence plan the appropriate measures to protect critical infrastructure.

5. At the local level:

Local governments provide the development, approval and implementation of local programs of increasing community resilience to crises situations caused by the cessation of the provision or deterioration of the quality of vital services or the termination of access to vital resources. These programs include the measures to provide the protection and resilience of critical infrastructure, the interaction of the subjects related to system of critical infrastructure protection , as well as the restoration of the functioning of critical infrastructure facilities.

6. At the facility level:

Operators on each critical infrastructure facility develop and enforce an object plan for measures to protect and sustain the critical infrastructure, including physical protection measures, countering threats, providing informational and cyber security on critical infrastructure facilities.

7. Measures on cyber security of critical infrastructure facilities at all levels, as well as protection of technological information circulating in automated systems of critical infrastructure facilities, are carried out in accordance with legislation in the field of information security and cyber security.

The powers of the subjects of the state system of protection of critical infrastructure regarding the provision of cyber security and cyber defense of critical infrastructure objects are determined by legislation in the field of information security and cyber security.

Article 34. Control over the security level of critical infrastructure facilities and their stability

1. The control over the security level of critical infrastructure facilities is carried out by assessing the protection of critical infrastructure facilities.

2. The purpose of control is to establish the compliance of the security status of critical infrastructure facility with the parameters declared by the operator of the critical infrastructure facility in the security passport to the relevant facility, providing methodological assistance to operators of critical infrastructure facilities in improving the critical infrastructure protection system.

3. The assessment of the security of critical infrastructure facilities is carried out by the subjects of the state protection system of critical infrastructure facilities settled in this Law.

4. The control procedure is determined by the Cabinet of Ministers of Ukraine.

Article 35. Interaction of the state protection system of critical infrastructure with other protection systems in the national security sector

1. In order to ensure the critical infrastructure resistance to the threats of all kinds, the realization of national interests, the functioning of society and the provision of social and economic development, the state protection system of critical infrastructure interacts with other systems of protection in the sector of national security:

1) with a unified state system for the prevention, response, and termination of terrorist attacks and minimization of their consequences, with territorial and functional subsystems, structural subdivisions of the fight against terrorism, and the SBU Interdepartmental Coordination Commission of the Antiterrorist Center on counter-terrorism and response to threat of committing or committing terrorist attacks;

2) with the national cyber security system, the Situational Center for providing cyber security of the Security Service of Ukraine on cyber attacks and cyber incidents, which threaten the sustainable functioning of the facilities of critical information infrastructure;

3) with law enforcement agencies in the field of counteracting crime;

4) with the combined civil-military air traffic control system of Ukraine, the Ukrainian Center for Airspace Use Planning and Air Traffic Control, Command of the Air Forces, the Armed Forces of Ukraine on:

protection of airspace, air defense of important state facilities and certain critical infrastructure objects;

interaction regarding the termination of aircraft illegal acts that can be used to carry out terrorist attacks in the Ukrainian airspace against critical infrastructure facilities and important state facilities;

5) with a unified state civil defense system, with permanent functional and territorial subsystems and their links, with the State Commission for Technogenic and Environmental Safety and Emergency Situations and the Commissions for Technogenic and Environmental Safety and Emergency Situations in the Autonomous Republic of Crimea, regions, Kyiv and Sevastopol, on issues of prevention, response and liquidation of crisis situations on critical infrastructure facilities;

6) with the state system of physical security on issues of protection of nuclear installations, nuclear materials, prevention of sabotage, theft or any other illegal extraction of radioactive materials.

2. Interaction between state security systems is carried out during the threat of occurrence or occurrence:

1) illegal actions, seizure of critical infrastructure facilities or important state facilities that threaten the safety of citizens and violate the functioning of life support systems;

2) sabotage, terrorist attacks, theft, deliberate destruction, damage to property and other activities on objects of critical infrastructure and important state facilities, resulting in death of people or significant material damage;

3) large-scale cyber attacks, acts of cyber-terrorism against control systems, operational and other systems of critical infrastructure facilities;

4) anthropogenic or natural disasters and accidents at the critical infrastructure facilities and important state facilities;

5) accidents and technical failures, emergency situations at the critical infrastructure facilities that endanger the life and health of personnel of these facilities and local population;

6) other threats to national security, stability and security of critical infrastructure.

3. Organization of interaction between subjects of the state protection system of critical infrastructure is carried out by:

1) the operational exchange of information regarding the performing of tasks for the protection of critical infrastructure;

2) carrying out of joint operational meetings of the authority from central and territorial offices of the National Police of Ukraine, the Security Service of Ukraine, the National Guard of Ukraine, the Armed Forces of Ukraine, and other involved state bodies;

3) implementation of joint measures to protect critical infrastructure in accordance with plans developed at the national, sectoral, regional, local and object levels;

4) joint command-and-staff, tactical-special exercises, joint trainings and training courses regarding protection, security, defense, termination of criminal activity and cyber attacks against critical infrastructure systems and facilities;

5) regular clarification of the calculations of the forces and means involved in the joint performing of tasks for the protection of critical infrastructure facilities and important state facilities;

6) joint measures to stop illegal actions aligned to critical infrastructure facilities or important state facilities that threatens the safety of citizens and violates their functioning;

7) participation in the response and liquidation of the consequences of incidents, emergency situations at the critical infrastructure facilities;

8) coordination of actions to maintain or restore law and order at the critical infrastructure facilities during emergency situations;

9) implementation of other measures stipulated by the legislation.

Article 36. Public-private interaction in the field of critical infrastructure protection

1. Public-private interaction in the field of critical infrastructure protection is carried out by:

1) creation of a system for seasonable detection, prevention and neutralization of threats to critical infrastructure, including involving volunteer organizations;

2) improvement of complex knowledge, skills and abilities of citizens necessary for realization of state and public projects for raising public awareness about the protection of critical infrastructure;

3) the exchange of information between public authorities, the private sector and citizens on threats to critical infrastructure facilities and crisis situations at these sites;

4) involvement of expert potential, scientific institutions, professional

associations and public organizations in the preparation of key sectoral projects and legislative documents in the field of critical infrastructure protection;

5) provision of advisory and practical assistance on crisis response to critical infrastructure facilities;

6) formation of initiatives and creation of authoritative advisory centers for citizens, representatives of industry and business in order to ensure the security of critical infrastructure;

7) introduction of the mechanism of public control over the effectiveness of measures to protect critical infrastructure;

8) periodic joint arrangements with business service providers, identification of their role in promoting better risk management in critical infrastructure protection;

9) creation of a system of stuff training and stuff improvement in various areas of critical infrastructure protection;

10) ensuring constant interaction with individuals, non-governmental and volunteer organisations, other enterprises in order to implement measures to protect critical infrastructure;

11) ensuring the stable operation of critical infrastructure facilities in different working conditions by solving a body of tasks to support the relevant technological process and its trouble-free stop;

12) providing personnel protection against possible threats;

13) provision of the reserve of the main resources for functioning of the critical infrastructure facility in different working conditions;

14) alerting the local population about the incidents and crisis situations at critical infrastructure facilities.

2. Public-private interaction in the field of critical infrastructure protection is applied considering the specific legal regime established by the legislation regarding certain facilities and certain activity types.

3. The bodies of state power and local government bodies, their officials, enterprises, institutions and organisations, despite the form of ownership, individuals, citizens and public associations are bound to assist the entities, to inform them about the threats to national security or any other cyber threats to critical infrastructure, cyber attacks and / or circumstances that may help prevent, detect and eliminate actorssuch threats, counteract criminal acts, terrorist attacks and minimize their consequences.

Article 37. Responsibility for violating legislation in the area of critical infrastructure protection

1. Bodies of state executive power, bodies of local government bodies, their officials, operators of critical infrastructure facilities, are guilty of violating legislation in the field of critical infrastructure protection, bear responsibility as set forth by law.

Article 38. Provision of finance in the field of critical infrastructure protection

1. Sources of financing of activities and measures to secure critical infrastructure protection are the funds of the state and local budgets, own funds of

business entities, bank loans, international technical assistance funds and other sources not prohibited by law.

Article 39. International cooperation in the field of critical infrastructure protection

1. Ukraine, in accordance with its international treaties, cooperates in the sphere of critical infrastructure protection with foreign states, their law enforcement agencies and special services, as well as with international organisations engaged in struggle against international crime and terrorism.

2. Ukraine, in accordance with international treaties approved by the Verkhovna Rada of Ukraine, may participate in common arrangements to ensure the protection of critical infrastructure, in particular, in conducting joint exercises of security and defense sector entities within the framework of collective defense measures in compliance with the requirements of laws Of Ukraine "On the order of sending units of the Armed Forces of Ukraine to other states" and "On the procedure of admission and conditions of stay of units of the armed forces of other states on the territory of Ukraine".

3. In accordance with the legislation of Ukraine in the field of external relations, the entities of the state system of protection of critical infrastructure, within the framework of their powers, can engage in international cooperation directly on a bilateral or multilateral basis.

CONCLUDING AND TRANSITIONAL PROVISIONS

1. This Law comes into force six months after its publication.

2. Amend the following laws of Ukraine:

1) In the Law of Ukraine "On the Cabinet of Ministers of Ukraine" (Bulletin of the Verkhovna Rada of Ukraine (VVR), 2014, No. 13, p.222), paragraph five of the first part of Article 20 after the sub-paragraph seven to propose an amendment specifying:

"Provides for state policy in the field of critical infrastructure protection in Ukraine";

2) The Law of Ukraine "On the Security Service of Ukraine" (Bulletin of the Verkhovna Rada of Ukraine, 1992, No. 27, Article 382, 2004, No. 32, Article 394, 2006, No. 14, Article 116, No. 30, Article 258, 2011, No. 10, Article 63, 2012, No. 29, Article 333):

a) the first part of Article 2 after the words "defense potential of Ukraine", amend by the words "critical infrastructure,";

b) the first part of Article 10 and part one of Article 15 after the words "protection of national statehood" amend with the words "counter-intelligence protection of critical infrastructure";

c) Part one of Article 24 amend with clause 6-1 specifying:

"6-1) carry out counter-intelligence protection of critical infrastructure;"

3)Sub-paragraph four of part one of Article 5 of the Law of Ukraine "On Operational and Investigative Activity" (Bulletin of the Verkhovna Rada of Ukraine, 1992, No. 22, Article 303, No. 39, Article 572; 1993, No. 11, Art. 83, 1998, No. 26, Article 149, 1999, No. 4, Article 35, 2001, No. 10, Article 44, No. 14, Article 72,

2002, No. 33, Art. 237, 2003, No. 27, Article 209, No. 30, Article 247, No. 45, Article 357, 2004, No. 8, Article 66, 2005, No. 10, Article 187, No. 25, Article 335, 2006, No. 14, Article 116) after the words "protection of national statehood," amend with the words "counter-intelligence protection of the state's interests in the field of information security, counter-intelligence protection of critical infrastructure,".

4) Paragraph 2 of part one of Article 6 of the Law of Ukraine "On counter-intelligence activities" (Bulletin of the Verkhovna Rada of Ukraine, 2003, No. 12, Article 89, No. 27, Article 209; 2006, No. 14, Article 116; 2011, No. 32, Article 314, 2013, No. 21, Article 208, 2014, No. 12, Article 178, 2016, No. 19, Article 214), amend by a new sub-paragraph four specifying: "counter-intelligence protection of critical infrastructure;".

In this regard, the sub-paragraphs fourth – seventh are considered sub-paragraphs five – eight, respectively.

5) Sub-paragraph four of the second paragraph of Article 1 of the Law of Ukraine "On the General Structure and Number of the Security Service of Ukraine" (Vidomosti Verkhovnoyi Rady Ukrainy, 2006, No. 4, Article 53, No. 30, Article 258, 2009, No. 24, Article 296, 2012, No. 29, Article 333), the words "counter-intelligence protection of the state's economy" shall be replaced by the words "counter-intelligence protection of critical infrastructure".

6) In the Law of Ukraine “On National Security Information”:

Paragraph 4 of part one of Article 8 after the third sub-paragraph amend specifying:

"Information on the organisation, content, status and plans for the protection of objects of critical infrastructure".

In this regard, the sub-paragraphs fourth – twelfth count as sub-paragraphs five – thirteenth, respectively.

6) In the Law of Ukraine "On Access to Public Information":

Part one of Article 9 after the first sub-paragraph amend with the following sub-paragraph:

"2) regarding the critical infrastructure facilities and measures taken to protect them, which are not classified as state secrets";

the third part of Article 9 after the words “other power entities" amend by the words "and critical infrastructure facilities".

7) The Law of Ukraine "On Access to Public Information":

Part one of Article 9 after the first sub-paragraph amend with the following sub-paragraph:

"2) regarding the critical infrastructure facilities and measures taken to protect them, which are not classified as state secrets";

the third part of Article 9 after the words “other power entities" amend by the words "and critical infrastructure facilities".

8) The Law of Ukraine "On the Legal Regime of the Military Situation" (Bulletin of the Verkhovna Rada (VVR), 2015, No. 28, p.250):

a) in the first part of Article 1, after the words "ensuring national security",

amend with punctuation marks and words: "protection of critical infrastructure":

b) in the first part of Article 15, after the words "On mobilization training and mobilization", amend with the punctuation marks and words: "'On critical infrastructure and its protection'".

9) The Law of Ukraine "On Information" (Bulletin of the Verkhovna Rada of Ukraine, 2011, No. 32, Article 313):

a) To amend Article 10 after the tenth paragraph with a new paragraph, with the following content:

"Technological Information".

In this regard, the paragraph eleventh is to be considered as paragraph twelve;

b) to amend Article 191 with the following content:

"Article 19-1. Technological information

1. 'Technological information' means the data processed (received, transmitted, stored) in the control systems of technological processes of critical infrastructure facilities.

2. The legal regime of technological information is determined by the laws and international treaties of Ukraine, which are binding after receiving the consent of the Verkhovna Rada of Ukraine.

3. By its access mode, technological information to is restricted information and is subject to protection under the law. It is prohibited to include in the technological information the data about cases of faults or improper functioning of the critical infrastructure facility that may have a negative impact on national security and defense of Ukraine, the environment, may cause property damage and/or are dangerous to life and health of the people."

в) Paragraph one of the second part of Article 21 should be worded as follows:

"2. 'Confidential' means information about an individual, the technological information, as well as information with restricted access for an individual or legal person, except the authorities. Confidential information may be distributed at the request (consent) of the relevant person in the order specified by them in accordance with the conditions set by them, as well as in other cases specified by law."

3. The Cabinet of Ministers of Ukraine within three months from the date this Law enters into force:

must ensure the adoption of regulatory framework necessary for the implementation of this Law;

bring its regulatory framework in compliance with this Law;

ensure that ministries and other central and local executive authorities bring their regulatory framework into compliance with this Law.