Official translation
Last modification: 11.06.21 12:27:56

LAW OF UKRAINE

On the Basic Principles of Cybersecurity in Ukraine

(The Official Bulletin of the Verkhovna Rada (BVR), 2017, No. 45, Article 403)

{As amended by Laws
No. 2469-VIII of 21 June 2018, BVR, 2018, No. 31, Article 241
No. 720-IX of 17 June 2020, BVR, 2020, No. 47, Article 408
No. 912-IX of 17 September 2020}

This Law defines the legal and organisational basis for the protection of the vital interests of individuals and citizens, society and the state, national interests of Ukraine in cyberspace, the main objectives, directions and principles of public policy in the field of cybersecurity, the powers of state bodies, enterprises, institutions, organisations, individuals and citizens in this field, and the main basis for the co-ordination of their activities to ensure cybersecurity.

Article 1. Definitions

1. For the purposes of this Law, the following definitions shall apply:

1) cyber threat indicators – indicators (technical data) used to detect and respond to cyber threats;

2) information on a cybersecurity incident – information on the circumstances of a cyber incident, in particular, which objects of cyber defence were attacked and under which conditions, which were successfully detected, neutralised, which were prevented using which cyber defence means, including which cyber threat indicators were used;

3) cybersecurity incident (hereinafter referred to as cyber incident) – an event or series of adverse events of an unintentional nature (natural, technical, technological, erroneous, including due to human factor) and/or those that have signs of a possible (potential) cyberattack, which threaten the security of electronic communications systems, technological process control systems, create the possibility of disruption of the normal operation of such systems (including disruption and/or blockage of system work, and/or unauthorised management of its resources), endangering the security (safety) of electronic information resources;

4) cyberattack is a targeted (deliberate) act in cyberspace, which is carried out through electronic communications (including information and communication technologies, software, firmware, other technical and technological instrumentalities and equipment) and is aimed at achieving one or a combination of the following goals: violation of confidentiality, integrity, availability of electronic information resources processed (transmitted, stored) in communication and/or technological systems, obtaining unauthorised access to such resources; violation of security, stable, reliable and regular functioning of communication and/or technological systems; use of communication system, its resources and electronic communication means for cyberattacks on other objects of cyber defence;

5) cybersecurity is the protection of vital interests of individuals and citizens, society and the state in the use of cyberspace, which ensures the sustainable development of information society and the digital communication environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace;

6) cyber threat – existing and potentially possible phenomena and factors that pose a threat to vital national interests of Ukraine in cyberspace, have a negative impact on the state's cybersecurity, cybersecurity and cyber defence of its facilities;

7) cyber defence – a set of organisational, legal, engineering and technical measures, as well as measures of cryptographic and technical protection of information, aimed at preventing cyber incidents, detecting and protecting against cyberattacks, eliminating their consequences, restoring consistency and reliability of functioning of communication and technological systems;

8) cybercrime (computer crime) – a socially dangerous criminal act in cyberspace and/or with its use, the liability for which is provided by the law of Ukraine on criminal liability and/or which is recognised as a crime by the international treaties of Ukraine;

9) cybercrime – a set of cybercrimes;

10) cyber defence – a set of political, economic, social, military, scientific, scientific-technical, informational, legal, organisational and other activities carried out in cyberspace and aimed at

protecting the sovereignty and defence capabilities of a state, preventing armed conflict and repelling armed aggression;

11) cyberspace – an environment (virtual space) that provides opportunities for communication and/or the realisation of social relations, resulting from the operation of shared (interconnected) communication systems and the provision of electronic communications using the Internet and/or other global data transmission networks;

12) cyber intelligence – actions carried out by intelligence agencies in cyberspace or with its use;

13) cyberterrorism – terrorist activity carried out in cyberspace or with its use;

14) cyberespionage – espionage that takes place in cyberspace or with its use;

15) critical information infrastructure – a set of critical information infrastructure facilities;

16) critical infrastructure facilities (hereinafter referred to as critical infrastructure facilities) – enterprises, institutions and organisations, regardless of their form of ownership, whose activities are directly related to technological processes and/or the provision of services that are important for the economy and industry, the functioning of society and public safety, whose failure or malfunction could have a negative impact on the national security and defence of Ukraine, the environment, cause property damage and/or pose a threat to human life and health;

17) National Telecommunication Network – a set of special telecommunication systems (networks), special communication systems, other communication systems that are used in the interests of government authorities and local governments, law enforcement agencies and military formations formed under the law, designed for the circulation (transmission, reception, creation, processing, storage) and protection of national information resources, and that are used to provide secure electronic communications, provision of a range of modern secure information and communication (multi-service) services in the interests of the administration of the state in peacetime, in a state of emergency and a special period, and which is a dual-use network (system) using part of its resource to provide services, in particular, cyber defence, to other consumers;

18) national electronic information resources (hereinafter referred to as national information resources) – systematised electronic information resources that contain information regardless of the type, content, form, time and place of its creation (including public information, state information resources and other information), designed to meet the vital public needs of a citizen, person, society and state. Electronic information resources are defined as any information created, recorded, processed or stored in digital or another intangible form by electronic, magnetic, electromagnetic, optical, technical, software or other means;

19) critical information infrastructure facility is communication or technological system of a critical infrastructure facility, a cyberattack on which would directly affect the sustainable operation of such critical infrastructure facility;

20) technological process control system (hereinafter referred to as technological system) – an automated or automatic system, which is a set of equipment, means, complexes and systems of processing, transmission and acceptance, designed for organisational management and/or control of technological processes (including industrial, electronic, communication equipment, other technical and technological means) regardless of the system access to the Internet and/or other global data transmission networks;

21) electronic communication systems (hereinafter – communication systems) – transmission, switching or routing systems, equipment and other resources (including passive network elements which enable the transmission of signals by wire, radio, optical or other electromagnetic means, mobile, satellite networks, electric cable networks as far as they are used for the transmission of signals), which ensure electronic communications (transmission of electronic information resources), including communication means and devices, computers, other computer equipment, information and telecommunication systems, which have access to the internet and/or other global data transmission networks.

The terms “national security”, “national interests”, “threats to national security” are used in this Law in the meaning defined by the Law of Ukraine “On the Fundamentals of National Security of Ukraine”.

Article 2. Principles of application of the Law

1. This Law does not apply to:

1) relations and services related to the content of information that is processed (transmitted, stored) in communication and/or technological systems;

2) actions related to the protection of information constituting a state secret, communication and technological systems intended for its processing;

3) social networks, private electronic information resources on the Internet (including blogging platforms, video hosting, other web resources), if such information resources do not contain information the need to protect which is established by law, relations and services related to the operation of such networks and resources;

4) communication systems that do not interact with public electronic communication networks

4) communication systems that do not interact with public electronic communication networks (electronic public networks), are not connected to the internet and/or other global data transmission networks (other than technological systems).

2. The application of cybersecurity legislation and decision-making by authorities pursuant to the norms of the Law shall be carried out in compliance with the principles of:

1) minimum necessary regulation, according to which the decisions (measures) of the subjects of power must be necessary and minimally sufficient to achieve the purpose and objectives defined in this Law;

2) objectivity and legal certainty, applying national and international law as much as possible to the powers and responsibilities of state bodies, enterprises, institutions, organisations and citizens in the field of cybersecurity;

3) ensuring protection of the rights of users of communications systems and/or consumers of electronic communications services and/or information protection services, cyber defence, including rights of non-interference in private life and protection of personal data;

4) transparency, according to which decisions (measures) of the subjects of power must be duly justified and notified to the subjects concerned before they come into force (their application);

5) balancing requirements and liability, according to which there should be a balance between imposing liability for failure to meet cybersecurity and cyber defence requirements and imposing excessive requirements and restrictions;

6) non-discrimination, according to which the decisions, actions and omissions of subjects of power cannot result in the legal or factual scope of the rights and obligations of the person who is:

different from the scope of the rights and obligations of others in similar situations, unless such a difference is necessary and minimally sufficient to satisfy the general public interest;

as well as the scope of rights and obligations of others in dissimilar situations, unless such equality is necessary and minimally sufficient to satisfy the general public interest;

7) equivalence of cybersecurity requirements for critical infrastructure facilities, according to which the application of legal provisions should be as equivalent as possible concerning the cyber defence of communications and technology systems of critical infrastructure facilities belonging to the same economic sector and/or performing similar functions.

The above principles shall apply without prejudice to any of them, taking into account the purpose and objectives of this Law.

Article 3. Legal basis for cybersecurity of Ukraine

1. The legal basis for cybersecurity of Ukraine is constituted by the Constitution of Ukraine, laws of Ukraine regarding the foundations of national security, the foundations of domestic and foreign policy, electronic communications, protection of state information resources and information whose protection is required by law, this and other laws of Ukraine, the Convention on Cybercrime, other international treaties ratified by the Verkhovna Rada of Ukraine, decrees of the President of Ukraine, acts of the Cabinet of Ministers of Ukraine, as well as other legal acts adopted according to the laws of Ukraine.

2. If an international treaty of Ukraine ratified by the Verkhovna Rada of Ukraine, provides for rules other than those established by this Law, the provisions of the international treaty of Ukraine shall apply.

Article 4. Objects of cybersecurity and cyber defence

1. The objects of cybersecurity are:

1) constitutional human and citizen rights and freedoms;

2) society, the sustainable development of the information society and the digital communication environment;

3) the state, its constitutional order, sovereignty, territorial integrity and inviolability;

4) national interests in all spheres of life of the individual, society and state;

5) critical infrastructure facilities.

2. The objects of cyber defence are:

1) communication systems of all forms of ownership that process national information resources and/or are used in the interests of government authorities, local governments, law enforcement agencies and military formations formed under the law;

2) critical information infrastructure facilities;

3) communication systems that are used to meet public needs and/or implement legal relations in the areas of e-government, e-government services, e-commerce, e-document management.

3. The procedure for forming the list of facilities of critical information infrastructure, the list of such facilities and the procedure for including them in the state register of critical information

such facilities and the procedure for including them in the state register of critical information infrastructure facilities, as well as the procedure for forming and maintaining the state register of critical information infrastructure facilities shall be approved by the Cabinet of Ministers of Ukraine.

The National Bank of Ukraine is responsible for the formation and operation of the register of critical information infrastructure facilities in the banking system of Ukraine.

Article 5. Subjects of cybersecurity

1. Co-ordination of cybersecurity activities as part of Ukraine's national security is carried out by the President of Ukraine through the National Security and Defense Council of Ukraine headed by him.

2. The National Coordination Centre for Cybersecurity, as a working body of the National Security and Defense Council of Ukraine, co-ordinates and monitors the activities of security and defence sector subjects that provide cybersecurity, submits proposals to the President of Ukraine on the formation and refinement of the Cybersecurity Strategy of Ukraine.

3. The Cabinet of Ministers of Ukraine ensures the formation and implementation of public policy in the field of cybersecurity, the protection of human and civil rights and freedoms and national interests of Ukraine in cyberspace, and the fight against cybercrime; organises and ensures the necessary forces, means and resources for the functioning of the national cybersecurity system; forms requirements and ensures the functioning of the information security audit system at critical infrastructure facilities (except for critical infrastructure facilities in the banking system of Ukraine).

4. Subjects that directly implement cybersecurity measures within their competence are:

1) ministries and other central executive authorities;

2) local state administrations;

3) local governments;

4) law enforcement, intelligence and counter-intelligence agencies, subjects of operational and investigative activities;

5) the Armed Forces of Ukraine and other military formations formed in accordance with the law;

6) the National Bank of Ukraine;

7) enterprises, institutions and organisations classified as critical infrastructure facilities;

8) business entities, citizens of Ukraine and associations of citizens, other persons carrying out activities and/or providing services related to national information resources, electronic information services, electronic transactions, electronic communications, information protection and cybersecurity.

5. Subjects of cybersecurity within their competence shall:

1) implement measures to prevent the use of cyberspace for military, intelligence-subversive, terrorist and other illegal and criminal purposes;

2) detect and respond to cyber incidents and cyberattacks, eliminate their consequences;

3) carry out information exchange regarding actual and potential cyber threats;

4) develop and implement protective, organisational, educational and other measures in the field of cybersecurity and cyber defence;

5) ensure the conduct of information security audits, including at subordinate facilities and facilities belonging to the scope of their management;

6) carry out other activities to ensure the development and security of cyberspace.

Article 6. Critical infrastructure facilities

1. Critical infrastructure facilities may include enterprises, institutions and organisations, irrespective of their form of ownership, which:

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

2) provide services in the areas of essential services of the population, in particular, in the areas of centralised water supplies, water disposal, electricity and gas supplies, food production, agriculture and health care;

3) are utility, emergency and rescue services and emergency services for the public;

4) are included in the list of enterprises of strategic importance for the economy and security of the state;

5) are objects of potentially hazardous technologies and industries.

2. Criteria and procedure for classifying facilities as critical infrastructure facilities, a list of such facilities, general requirements for their cyber defence, including the application of cyber threat indicators, and requirements for independent audits of information security shall be approved by the

Cabinet of Ministers of Ukraine, and in the banking system of Ukraine – by the National Bank of Ukraine.

3. Requirements and procedures for independent audits of information security at critical infrastructure facilities are established by relevant regulations on information security audits approved by the Cabinet of Ministers of Ukraine.

The development of regulations on independent audits of information security at critical infrastructure facilities is based on international, European Union and NATO standards with the mandatory involvement of representatives of the main subjects of the national cybersecurity system, scientific institutions, independent auditors and cybersecurity experts, public organisations.

4. Responsibility for ensuring the cyber defence of communication and technological systems of critical infrastructure facilities, protection of technological information under the requirements of the legislation, for the prompt reporting of cybersecurity incidents to the government's computer emergency response team of Ukraine CERT-UA, for arranging an independent information security audit at such facilities is entrusted to the owners and/or managers of enterprises, institutions and organisations classified as critical infrastructure.

5. The exchange of information on cybersecurity incidents containing personal data shall comply with the requirements of the Law of Ukraine "On Protection of Personal Data".

Article 7. Principles of ensuring cybersecurity

1. Ensuring cybersecurity in Ukraine is based on the principles of:

1) the rule of law, legality, respect for human rights and fundamental freedoms and their protection in the manner prescribed by law;

2) ensuring the national interests of Ukraine;

3) openness, accessibility, stability and security of cyberspace, development of the Internet and responsible action in cyberspace;

4) public-private co-operation, broad co-operation with civil society in the field of cybersecurity and cyber defence, in particular, through sharing information on cybersecurity incidents, implementing joint scientific and research projects, and training and professional development of personnel in this field;

5) proportionality and adequacy of cyber defence measures to actual and potential risks, realising the inherent right of a state to self-defence in accordance with international law in the event of aggressive actions in cyberspace;

6) priority of precautionary measures;

7) inevitability of punishment for committing cybercrimes;

8) priority development and support of domestic scientific, scientific-technical and production potential;

9) international co-operation in order to strengthen mutual trust in the field of cybersecurity and develop joint approaches to counter cyber threats, consolidate efforts to investigate and prevent cybercrime, and prevent the use of cyberspace for terrorist, military and other illegal purposes;

10) ensuring democratic civilian control over military formations and law enforcement agencies established under the laws of Ukraine, carrying out actions in the field of cybersecurity.

Article 8. National cybersecurity system

1. The national cybersecurity system is a set of cybersecurity subjects and interrelated measures of a political, scientific and technical, informational, educational, organisational, legal, intelligence, counterintelligence, defence, engineering and technical nature, as well as measures for the cryptographic and technical protection of national information resources and the cyber defence of critical information infrastructure facilities.

2. The main entities of the national cybersecurity system are the State Service for Special Communication and Information Protection of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine, intelligence agencies and the National Bank of Ukraine, which, under the Constitution and the laws of Ukraine, perform the following main tasks in the prescribed manner:

1) The State Service for Special Communication and Information Protection of Ukraine ensures the formation and implementation of public policy on the protection in cyberspace of state information resources and information whose protection is required by law, cyber defence of critical information infrastructure facilities, and exercises state control in these fields; co-ordinates the activities of other cybersecurity subjects with regard to cyber defence; ensures the establishment and operation of the National Telecommunications Network and the implementation of an organisational and technical model for cyber defence; implements organisational and technical measures to prevent, detect and respond to cyber incidents and cyberattacks and eliminate their consequences; informs about cyber threats and appropriate methods of protection against them; ensures implementation of information security audits at critical infrastructure facilities, establishes requirements for information security

auditors, determines the procedure for their attestation (recertification); co-ordinates, organises and conducts an audit of the security of communications and technological systems of critical infrastructure facilities; ensures the functioning of the State Centre for Cyber Defence, the government's computer emergency response team of Ukraine CERT-UA;

2) The National Police of Ukraine ensures the protection of human and civil rights and freedoms and the interests of society and the state from criminal encroachments in cyberspace; takes measures to prevent, detect, suppress and disclose cybercrimes and raise citizen awareness of security in cyberspace;

{Clause 2, part two of Article 8 as amended by Law No. 720-IX of 17 June 2020}

3) The Security Service of Ukraine prevents, detects, suppresses and solves criminal offences against peace and security of humanity that are committed in cyberspace; carries out counterintelligence and operational-search activities aimed at combating cyberterrorism and cyber espionage, and covertly checks the readiness of critical infrastructure facilities for possible cyberattacks and cyber incidents; counteracts cybercrime, the consequences of which may threaten the vital interests of the state; investigates cyber incidents and cyberattacks against state electronic information resources and information, the requirement for protection of which is established by law, and critical information infrastructure; provides a response to cyber incidents in the field of national security;

{Clause 3, part two of Article 8 as amended by Law No. 720-IX of 17 June 2020}

4) The Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine shall, with the respective competence, carry out measures to prepare the state to repulse military aggression in cyberspace (cyber defence); carry out military co-operation with NATO and other defence subjects to ensure the security of cyberspace and joint protection against cyber threats; implement measures to ensure cyber protection of critical information infrastructure in conditions of emergency and martial law;

5) intelligence agencies of Ukraine carry out intelligence activities on threats to the national security of Ukraine in cyberspace, other events and circumstances related to the field of cybersecurity;

6) The National Bank of Ukraine determines the procedure, requirements and measures to ensure cyber defence and information security in the banking system of Ukraine and for the subjects of funds transfer, monitors their implementation; establishes a cyber defence centre of the National Bank of Ukraine and ensures the functioning of the cyber defence system in the banking system of Ukraine; provides an assessment of the state of cybersecurity and audit of information security at critical infrastructure facilities in the banking system of Ukraine.

3. The functioning of the national cybersecurity system is ensured by:

1) development and operational adaptation of the public policy in the field of cybersecurity, aimed at the development of cyberspace, achieving compatibility with the relevant standards of the European Union and NATO;

2) creation of a legal and terminological base in the field of cybersecurity, harmonisation of normative documents in the field of electronic communications, information protection, information security and cybersecurity in line with international standards, in particular, those of the European Union and NATO;

3) establishment of mandatory information security requirements for critical information infrastructure facilities, including during their creation, commissioning, operation and upgrading, taking into account international standards and the specifics of the industry to which the relevant critical information infrastructure facilities belong;

4) formation of a competitive environment in the field of electronic communications, provision of information protection and cyber defence services;

5) involving the expertise of scientific institutions, professional and public associations in the preparation of draft conceptual documents in the field of cybersecurity;

6) conducting exercises on actions in case of emergencies and incidents in cyberspace;

7) functioning of the information security audit system, implementation of global best practices and international standards on cybersecurity and cyber defence;

8) development of a network of computer emergency response teams;

9) development and improvement of the system of technical and cryptographic protection of information;

10) ensuring compliance with the requirements of the legislation on the protection of state information resources and information;

11) creation and ensuring the functioning of the National Telecommunication Network;

12) exchange of information on cybersecurity incidents between cybersecurity subjects in the manner prescribed by law;

13) implementation of a unified (universal) system of cyber threat indicators, taking into account

international standards on cybersecurity and cyber defence;

14) training specialists at bachelor's and master's levels of education and qualification under the state order in the amount necessary to meet the needs of the public sector of the economy, as well as for non-budgetary funds, including for recurrent training and mandatory periodic certification (recertification) of personnel responsible for ensuring the cybersecurity of critical infrastructure facilities, taking into account international standards;

15) implementation of the organisational and technical model of the national cybersecurity system as a set of measures, forces and means of cyber defence aimed at a rapid (crisis) response to cyberattacks and cyber incidents, the introduction of countermeasures aimed at minimizing the vulnerability of communication systems;

16) establishment of requirements (rules, guidelines) for the safe use of the Internet and the provision of electronic services by government authorities;

17) public-private co-operation in preventing cyber threats to critical infrastructure facilities, responding to cyberattacks and cyber incidents, and dealing with their consequences, in particular, in crisis, state of emergency, martial law and special periods;

18) conducting periodic reviews of the national cybersecurity system, developing cybersecurity indicators;

19) strategic planning and software targeted support in the development of electronic communications, information technology, information protection and cyber defence;

20) development of international co-operation in the field of cybersecurity, support of international initiatives in the field of cybersecurity that meet the national interests of Ukraine, deepening co-operation of Ukraine with the European Union and NATO to strengthen Ukraine's capacity in the field of cybersecurity, participation in confidence-building measures in the use of cyberspace, conducted under the auspices of the Organisation for Security and Co-operation in Europe;

21) carrying out investigative, intelligence, counter-intelligence and other activities aimed at preventing, detecting, suppressing and solving criminal offences against the peace and security of mankind, committed using cyberspace, investigating, prosecuting, promptly responding to and countering cybercrime, intelligence-subversive, terrorist and other activities in cyberspace that are detrimental to Ukraine's interests, and the use of the Internet for military purposes;

{Clause 21, part two of Article 8 as amended by Law No. 720-IX of 17 June 2020}

22) implementation of politico-military, military-technical and other activities to enhance the capabilities of the State Military Organisation, security and defence sector, using cyberspace, to create and develop forces, means and instruments of possible response to aggression in cyberspace, which can be used as a deterrent to military conflicts and threats using cyberspace;

23) restrictions on participation in information security and cybersecurity activities of any economic entities that are under the control of the state recognized by the Verkhovna Rada of Ukraine as the aggressor state, or states and individuals subject to special economic and other restrictive measures (sanctions) taken at the national or international level as a result of aggression against Ukraine, as well as limiting the use of products, technologies and services of such entities to ensure the technical and cryptographic protection of state information resources, and strengthening state control in this area;

24) development of a cybersecurity counter-intelligence system designed to prevent, timely detect and counteract external and internal threats to Ukraine's security using cyberspace; elimination of conditions contributing to them and the reasons for their occurrence;

25) conducting intelligence activities to identify and counteract threats to Ukraine's national security in cyberspace, identifying other events and circumstances related to cybersecurity.

4. The procedure of functioning of the National Telecommunication Network, criteria, rules and requirements for the provision of services, their tariffication for users of the budgetary sphere, reimbursement of state budget expenses for maintenance of the National Telecommunication Network shall be approved by the Cabinet of Ministers of Ukraine.

5. The implementation of the organisational and technical model of cybersecurity as a component of the national cybersecurity system is carried out by the State Centre for Cybersecurity, which ensures the creation and operation of the main components of the system of secure access to the Internet for government authorities, the system of anti-virus protection of national information resources, information security audits and cyber defence of critical information infrastructure facilities, the system for identifying vulnerabilities and responding to cyber incidents and cyberattacks against cyber defence facilities, the system for interaction of computer emergency response teams, and, in co-operation with other cybersecurity subjects, develops cyber threat response scenarios, measures to counter such threats, and cyber training programmes and methodologies.

Article 9. Government Computer Emergency Response Team of Ukraine CERT-UA

1. The tasks of CERT-UA are:

1) accumulation and analysis of data on cyber incidents, maintenance of the state register of cyber

1) accumulation and analysis of data on cyber incidents, maintenance of the state register of cyber incidents;

2) providing practical assistance to the owners of cyber defence facilities on the prevention, detection and elimination of the consequences of cyber incidents on these facilities;

3) organisation and holding of practical workshops on cyber defence for the subjects of the national cybersecurity system and owners of cybersecurity facilities;

4) preparing and posting on its official website recommendations on counteracting modern types of cyberattacks and cyber threats;

5) co-ordination with law enforcement agencies, ensuring they are informed on time about cyberattacks;

6) co-ordination with foreign and international organisations on cyber incident response, in particular, through participation in the Forum of Incident Response and Security Teams FIRST with annual membership fees;

7) co-ordination with Ukrainian computer emergency response teams, as well as other enterprises, institutions and organisations, regardless of their form of ownership, that carry out actions related to the security of cyberspace;

8) processing of information received from citizens on cyber incidents concerning cybersecurity objects;

9) assistance to government authorities, local governments, military formations formed under the law, enterprises, institutions and organisations regardless of their form of ownership, as well as citizens of Ukraine in addressing cyber defence and countering cyber threats.

The State Service for Special Communication and Information Protection of Ukraine is responsible for the operation of CERT-UA, within the limits of its staffing and funding.

Article 10. Public-private co-ordination in the field of cybersecurity

1. Public-private co-ordination in cybersecurity is carried out by:

1) establishing a system for the timely detection, prevention and neutralisation of cyber threats, including the involvement of volunteer organisations;

2) increasing digital literacy of citizens and a culture of safe behaviour in cyberspace, comprehensive knowledge, skills and abilities to support cybersecurity goals, government and public projects to raise public awareness of cyber threats and cyber defence;

3) exchange of information between government authorities, the private sector and citizens on cyber threats to critical infrastructure facilities, other cyber threats, cyberattacks and cyber incidents;

4) partnerships and co-ordination of computer emergency response teams;

5) involvement of expert potential, scientific institutions, professional associations and public organisations in the preparation of key industry projects and regulations in the field of cybersecurity;

6) providing advisory and practical assistance in responding to cyberattacks;

7) formation of initiatives and establishing authoritative advice points for citizens, industry and business to ensure safety on the Internet;

8) implementing of a mechanism of public control over the effectiveness of cybersecurity measures;

9) holding a national summit periodically with professional business service providers, including insurers, auditors, lawyers, to determine their role in promoting better risk management in the field of cybersecurity;

10) creation of a system of training and increasing the competence of specialists in various fields of activity on cybersecurity;

11) close co-operation with individuals, public and volunteer organisations, IT companies in order to implement cyber defence measures in cyberspace.

2. Public-private co-ordination in the field of cybersecurity is applied taking into account the peculiarities of the legal regime established by law for certain objects and certain types of activity.

Article 11. Assistance to the subjects of cybersecurity of Ukraine

Government authorities and local governments, their officials, enterprises, institutions and organisations, regardless of their form of ownership, persons, citizens and citizen associations are obliged to assist cybersecurity subjects, report data is known to them regarding national security threats using cyberspace or any other cyber threats to cybersecurity objects, cyberattacks and/or circumstances, information about which may contribute to preventing, detecting and deterring such threats, countering cybercrime, cyberattacks and minimising their consequences.

Article 12. Liability for breach of cybersecurity legislation

Persons guilty of breach of legislation in the fields of national security, electronic communications

and information protection, if cyberspace is the place and/or method of committing a criminal offence, other culpable act for which liability is provided by civil, administrative, criminal law, shall be held liable under the law.

{Article 12 as amended by Law No. 720-IX of 17 June 2020}

Article 13. Financial support for cybersecurity measures

Sources of funding for cybersecurity and cyber defence work and activities are state and local budgets, business entities' own funds, bank loans, international technical assistance funds and other sources not prohibited by law.

Article 14. International co-operation in the field of cybersecurity

1. Ukraine, in accordance with the international treaties it has concluded, co-operates in the field of cybersecurity with foreign states, their law enforcement agencies and special services, as well as with international organisations that combat international cybercrime.

2. Ukraine, under international treaties ratified by the Verkhovna Rada of Ukraine, may take part in joint cybersecurity measures, in particular, in conducting joint exercises of security and defence sector entities in the framework of collective defence measures in compliance with the laws of Ukraine "On the Procedure of Sending Units of the Armed Forces of Ukraine to the Other States" and "On the Admission Procedure and Conditions of Stay of Units of the Armed Forces of Other States on the Territory of Ukraine".

3. According to Ukrainian legislation in the field of external relations, cybersecurity subjects, within the limits of their authority, may bring about international co-operation in the field of cybersecurity directly on a bilateral or multilateral basis.

4. Information on issues related to combating international cybercrime is provided by Ukraine to foreign states on the basis of a request, in compliance with Ukrainian legislation and its international legal obligations. Such information may be provided without prior request by the foreign state, if it does not interfere with the pre-trial investigation or judicial review of the case and may assist the competent authorities of the foreign state in stopping the cyberattack, timely detection and termination of the criminal offence involving the use of cyberspace.

Article 15. Control over the legality of measures to ensure cybersecurity in Ukraine

1. The Verkhovna Rada of Ukraine shall exercise control over the observance of the legislation in the implementation of cybersecurity measures under the procedure established by the Constitution of Ukraine.

Parliamentary control of compliance with personal data protection legislation and access to public information in the field of cybersecurity is carried out by the Ukrainian Parliament Commissioner for Human Rights.

2. The President of Ukraine and the Cabinet of Ministers of Ukraine shall exercise control over cybersecurity activities of entities of the security and defence sector and other government authorities under the procedure established by the Constitution and laws of Ukraine.

3. An independent audit of the activities of the main subjects of national cybersecurity, defined in part two, Article 8 of this Law on the effectiveness of the state cybersecurity system shall be conducted annually in accordance with international auditing standards.

Reports on the results of the independent audit of the activities of the main national cybersecurity entities defined in part two Article 8 of this Law on the effectiveness of the state cybersecurity system for the previous year shall be submitted to the President of Ukraine, Verkhovna Rada of Ukraine and the Cabinet of Ministers of Ukraine within forty-five days after the end of the calendar year.

The Committee of the Verkhovna Rada of Ukraine, whose competence includes national security and defence issues, and the Committee of the Verkhovna Rada of Ukraine, whose competence includes information and communications issues, shall at their meetings consider reports by the main national cybersecurity subjects defined in part two, Article 8 of this Law on the results of an independent audit of their activities on the effectiveness of the state cybersecurity system.

The main subjects of national cybersecurity defined in part two, Article 8 of this Law shall submit once a year reports on the status of their implementation of measures to ensure the cybersecurity of the state, referred to their competence, which should include, in particular, information on the results of an independent audit of their activities.

Based on the results of a review of reports by the main national cybersecurity subjects, the Committee of the Verkhovna Rada of Ukraine, whose purview includes issues of information and communication, may raise the issue of consideration of these issues by the Verkhovna Rada of Ukraine.

FINAL AND TRANSITIONAL PROVISIONS

1. This Law shall enter into force six months after its publication.

2. The following laws of Ukraine shall be amended:

1) Article 7 of the Law of Ukraine "On the National Bank of Ukraine" (The Official Bulletin of

the Verkhovna Rada of Ukraine, 1999, No. 29, Article 38 as amended) shall be supplemented with clause 32 and 33 to read as follows:

"32) determines the procedures, requirements and measures for cyber defence and information security in the banking system of Ukraine and for the subjects of funds transfer, and monitors their implementation; establishes the Cyber Defence Centre of the National Bank of Ukraine and ensures the functioning of the cyber defence system in the banking system of Ukraine;

33) ensures formation and maintenance of the list of critical infrastructure facilities, as well as the register of critical information infrastructure facilities in the banking system of Ukraine, determines the criteria and procedure for attributing facilities in the banking system of Ukraine to critical infrastructure facilities and critical information infrastructure facilities, ensures assessment of cyber defence and audit of information security in the banking system of Ukraine";

2) in the Law of Ukraine "On Defence of Ukraine" (The Official Bulletin of the Verkhovna Rada of Ukraine, 2000, No. 49, Article 420; 2011, No. 4, Article 27; 2015, No. 16, Article 110; 2016, No. 33, Article 564):

a) Article 3 after the nineteenth paragraph shall be supplemented by a new paragraph to read as follows:

"implementation of cyber defence (active cyber defence) measures to protect state sovereignty and ensure its defence capability, prevent armed conflict and repulse armed aggression".

In this connection, the twentieth paragraph shall be regarded as the twenty-first paragraph;

b) the second sentence, part two of Article 4 shall be supplemented with the words "including the conduct of special operations (intelligence, information and psychological, etc.) in cyberspace";

{Subclause 3, clause 2 of the section has been repealed under Law No. 912-IX of 17 September 2020}

{Subclause 4, clause 2 of the section has been repealed under Law No. 2469-VIII of 21 June 2018}

5) paragraph 6, Article 3 of the Law of Ukraine "On the Foreign Intelligence Service of Ukraine" (The Official Bulletin of the Verkhovna Rada of Ukraine, 2006, No. 8, Article 94) after the words "to the national security of Ukraine" add the words "including in cyberspace";

6) in the Law of Ukraine "On the State Service for Special Communication and Information Protection of Ukraine" (The Official Bulletin of the Verkhovna Rada of Ukraine, 2014, No. 25, Article 890, No. 29, Article 946):

a) part one, Article 2 and paragraph 2, part one of Article 3 after the words "cryptographic and technical protection of information" add the word "cybersecurity";

b) in part one of Article 14:

paragraph 39 after the words "ensuring the functioning" add the word "government";

add paragraphs 85–92 to read as follows:

"85) formation and implementation of public policy on the protection in cyberspace of state information resources and information whose protection is required by law, cyber defence of critical information infrastructure, implementation of state control in these fields;

86) co-ordination of cyber defence activities of cybersecurity subjects;

87) ensuring the establishment and operation of the National Telecommunication Network;

88) implementation of an organisational and technical model for cyber defence, implementation of organisational and technical measures to prevent, detect and respond to cyber incidents and cyberattacks and eliminate their consequences;

89) informing about cyber threats and appropriate methods of protection against them;

90) ensuring the implementation of the information security audit system at critical infrastructure facilities, establishing requirements for information security auditors, their certification (re-certification);

91) co-ordination, organisation and conducting of communication and technological systems of critical infrastructure facilities on vulnerability;

92) ensuring the functioning of the State Centre for Cyber Defence".

3. Within three months after the enactment of this Law, the Cabinet of Ministers of Ukraine shall:

ensure the adoption of regulatory acts required for the implementation of this Law;

bring its regulatory acts in line with this Law;

ensure that ministries and other central executive authorities review and cancel their regulatory acts contrary to this Law.

President of Ukraine **P. POROSHENKO**

City of Kyiv
5 October 2017
No. 2163-VIII

Publications of document

- **Голос України** on November 9, 2017 — N° 208
- **Відомості Верховної Ради України** on November 10, 2017 — 2017, N° 45, page 42, article 403
- **Урядовий кур'єр** on November 15, 2017 — N° 215
- **Офіційний вісник України** on November 21, 2017 — 2017, N° 91, page 31, article 2765, код акта 87903/2017