Approved by
Presidential Decree of Ukraine
No. 96/2016 dated 15 March 2016

CYBER SECURITY SRTATEGY OF UKRAINE

1 General Provisions

Rapid advances in information technology are gradually transforming the world. A free and open cyberspace increases the freedom and opportunities for people, enriches the society, creates a new global online interactive marketplace of ideas, researches and innovations, encourages responsible and effective work of a government, as well as the active citizens participation in state administration and resolving issues of local importance, provides publicity and transparency of a government, contributes to prevention of corruption.

However, the advantages of modern digital world and the information technologies development led to the emergence of new threats to national and international security. In addition to incidents of a natural origin (unintended) the number and capacity of cyber-attacks motivated by interests of individual States, groups and individuals are increasing.

The cases of illegal collection, storage, use, destruction and dissemination of personal data are increasingly presented along with illegal financial transactions, theft and fraud in the Internet. Cyber crime is becoming transnational and capable of harming the interests of individuals, society and the State.

The ongoing aggression of the Russian Federation, other fundamental changes in the external and internal security environment of Ukraine require immediate establishment of a national cyber security system as an integral part of the National security of Ukraine.

The objective of the Cyber Security Strategy of Ukraine (hereinafter – Strategy) is to create conditions for the safe functioning of cyberspace, application of cyberspace to benefit of individuals, society and the State.

To achieve this goal it is necessary to undertake the following measures:

- establishment of a national cyber security system;
- enhancing the capacity of entities of security and defence sector to the effective fight against military cyber threats, cyber espionage, cyber-terrorism and cyber crime, and also deepening international cooperation in this area;
- ensuring cyber protection of national electronic information resources, information, since the requirement of information protection was imposed by law, and also ensuring cyber protection of information infrastructure that is under jurisdiction of Ukraine and disruption of its sustained operation will

have a negative impact on the status of national security and defence of Ukraine (critical information infrastructure).

Ensuring cyber security of Ukraine as protection of vital interests of a man and citizen, society and the state in cyberspace, which is to be achieved through integrated application of a complex set of legal, institutional and information measures, should be based on the following principles of:

- the rule of law and respect for human and civil rights and freedoms;
- ensuring Ukraine's national interests;
- openness, accessibility, stability and security of cyberspace;
- public-private partnership, extensive cooperation with civil society for cyber security and cyber defence;
- adequacy and proportionality of cyber security measures to actual and potential risks;
- priority of proactive measures;
- inevitability of punishment for commission of cyber crimes;
- high priority development and support of national scientific, technological and productive capacity;
- international cooperation for building confidence and mutual trust in cyber security and for development of cooperative approaches to confront cyber threats, consolidation of efforts in the investigation and prevention of cyber crime, preventing the use of cyberspace for unlawful and military purposes;
- ensuring democratic civilian control over legally established military units and law enforcement agencies, that operate in the area of cyber security.

Security and development of cyberspace, introduction of e-governance, guarantee of security and sustainable functioning of electronic communications and national electronic information resources should be integral aspect of the State policy on information space development and evolution of the Information Society in Ukraine.

This Strategy is based on the provisions of:

- the Convention on Cyber crime, ratified by Act of Ukraine № 2824-IV of September 7, 2005,
- the legislation of Ukraine on the national security foundations, the principles of domestic and foreign policy, electronic communications, protection of state information resources and also information, since the requirement of information protection is imposed by law.

This Strategy aims at implementing up to 2020 the Ukraine’s National Security Strategy which was approved by a Presidential Decree of Ukraine No. 287 of May 26, 2015 "On the decision of the National Security and Defence Council of Ukraine on May 6, 2015 "On National Security Strategy of Ukraine".

2 Threats to cyber security

Alongside the traditional war domains such as "Land," "Air," "Sea" and "Space", cyberspace is gradually becoming a specific operation area, where relevant military units of leading nations of the world are increasingly active. The defence of our country is becoming more vulnerable to cyber threats owing to the broad application of modern information technology in defence and security sector, and establishment of a unified automated system for management of the Armed Forces of Ukraine.

Economic, information, scientific and technological spheres, the sector of public administration, military-industrial complex and transportation system, electronic communication infrastructure, defence and security sector of Ukraine are increasingly becoming vulnerable to intelligence-subversive activities of foreign intelligence agencies in cyberspace. The extensive presence of some organizations, groups and individuals directly or indirectly linked to the Russian Federation, sometimes even their dominant presence in Ukraine’s information infrastructure contributes to this vulnerability.

Modern information and communication technologies can be used to execute terrorist acts, in particular by malfunction of automatic control systems for technological processes of critical infrastructure. A politically motivated activity in cyberspace, especially in the form of attacks on government and private Web sites on the Internet, is becoming more widespread.

Information resources of financial institutions, transport companies and energy suppliers, state agencies, that guarantee the security, defence and protection from emergencies, are increasingly becoming targets for cyber-attacks and cyber crimes. The newest technologies are not only applied to committing conventional types of crimes, but also for perpetrating fundamentally new types of crimes in society with a high level of informatization.

Threats to cyber security are actualized through the following factors, in particular:

- discrepancy of national electronic communications infrastructure, its development and protection level to modern requirements;
- insufficient level of protection of critical infrastructure, public electronic information resources and information, since the requirement of information protection was imposed by law, from cyber threats;
- unsystematic cyber protection measures of critical infrastructure;
- lack of development of the organizational and technical infrastructure for cyber security and cyber protection of critical infrastructure and national electronic information resources;
- ineffective activities of the security and defence sector of Ukraine in combating cyber-threats of military, criminal, terrorist and other nature;
- inadequate level of coordination, cooperation and information exchange among the cyber security entities.

3 The national cyber security system, key entities of cyber security

National cyber security system is to ensure, above all, cooperation on cyber security issues among the state agencies, local governments, military units, law enforcement agencies, research institutions, educational institutions, non-governmental organizations, institutions and organizations regardless of their ownership and operating in electronic communications, information security sectors and / or are the owners (disponent owner) of critical information infrastructure.

According to the Constitution of Ukraine and under the procedure established by law the National Security and Defence Council of Ukraine is to coordinate and control activities of the entities of security and defence sector, ensuring cyber security of Ukraine.

The national system of cyber security will be based on the Ministry of Defence of Ukraine, the State Service of Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Police of Ukraine, the National Bank of Ukraine, the intelligence agencies. In accordance with the established procedure an implementation of the following key responsibilities and tasks should be assigned to:

the Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine in accordance with their competences are to be responsible for :

- implementation of the activities relating to preparation of the State for repelling military aggression in cyberspace (cyber defence);
- development of military cooperation with NATO on issues of secure cyberspace and joint protection against cyber threats;
- providing cyber protection of their own information infrastructure in cooperation with the State Service of Special Communications and Information Protection of Ukraine and the Security Service of Ukraine;

the State Service of Special Communications and Information Protection of Ukraine is to be responsible for:

- formation and implementation of the national policy on protection of state information resources in cyberspace, information security, since the requirement of information protection was imposed by law, cyber protection of critical information infrastructure, state control in these spheres;
- coordination of cyber defence activities of other cyber security entities;
- implementation of organizational and technical measures to prevent, detect and respond to cyber attacks and cyber incidents, mitigate any effects of them, inform about cyber threats and relevant methods of protection against them;
- support of State Cyber Centre;
- security audit for identifying vulnerability of critical information infrastructure;

the Security Service of Ukraine is to be responsible for:

- prevention, detection, suppression and exposure of crimes against the peace and security of mankind committed in cyberspace;
- implementation of counterintelligence and operational-investigative measures to combat cyber-terrorism and cyber espionage, as well as assure readiness of critical infrastructure to deal with possible cyber attacks and cyber incidents;
- cyber crime prevention, the potential impacts of which directly pose a threat to the vital interests of Ukraine;
- investigation of cyber incidents and cyber attacks on national electronic information resources, critical information infrastructure, information, since the requirement of information protection is imposed by law;
- computer emergency response for the national security;

the National Police of Ukraine are to be responsible for:

- protection of the human and civil rights and freedoms, defence of society and state interests from criminal attacks in cyberspace;
- prevention, detection, suppression and exposure of cyber crime;
- raising public awareness about security in cyberspace;

the National Bank of Ukraine is to be responsible for:

- establishing requirements for cyber protection of critical information infrastructure in the banking sector;

intelligence agencies of Ukraine are to be responsible for:

- conducting intelligence activities to identify threats to Ukraine's national security in cyberspace, intelligence-gathering operations aimed at other events and circumstances relating to the cyber security matters.

An appropriate environment should be created for involvement in cyber security activities of Ukraine for some enterprises, institutions and organizations irrespective of the form of ownership and which operate in the field of electronic communications, information security and/or are owners (disponent owners) of critical infrastructure. In accordance with the law, the issues of mandatory measures for information protection and cyber defence should be settled along with assistance to state agencies in their cyber security and cyber defence tasks implementation.

The State will encourage involvement of research institutions, educational institutions, organizations, non-governmental organizations and citizens into development and implementation of measures on cyber security and cyber defence.

4 Priorities and ways for ensuring of cyber security in Ukraine

4.1. The primary concerns of development of secure, stable and reliable cyberspace are to be as follows:

- formation and operational adaptation of state cyber security policy on the cyberspace development, achieving compatibility with the relevant EU and NATO standards;
- creating a national regulatory framework and term base in this area, harmonization of regulatory documents for electronic communications, information protection, information security and cyber security in accordance with international standards and standards of the EU and NATO;
- development of competitive environment in electronic communications sector, delivery of information security and cyber defence services;
- cyber technology development of mobile communications facilities; maintenance of hardware security, content security, application security and security of communication services;
- expertise inputs of scientific institutions, professional and public organizations to prepare drafts of conceptual cyber security documents;
- enhancing digital literacy of citizens and promoting security culture of safe behaviour in cyberspace, improving comprehensive knowledge, skills and abilities required to support cyber security objectives;
- implementation of state and community projects in order to raise public digital awareness of cyber threats and cyber defence;
- delivery of the training for emergency situations and incidents in cyberspace;
- development and improvement of the State control system over information security situation and also advancing the independent audit system of information security; implementation of global best practices and international standards for cyber security and cyber defence;
- development of electronic communications infrastructure, including broadband Internet access, digital and interactive television;
- development of network of computer emergency response teams;
- establishment of the system of timely detection, prevention and neutralization of cyber threats, including involvement of volunteer organization;
- development and improvement of the system for technical and cryptographic protection of information;
- enhancing international cooperation and support of international cyber security initiatives served the national interests of Ukraine;
- deepening cooperation with the EU and NATO to strengthen cyber security capacity of Ukraine;
- participation in activities on trust building in cyberspace, held under the guidance of the OSCE ;
- creating conditions for introduction of modern cyber defence technologies in Ukraine.

4.2. Cyber protection of information infrastructure intended for processing of information, since the requirement of information protection was imposed by law,

as well as cyber protection of national electronic information resources should principally focus on:

- establishment and operations support of the national telecommunications network as the single secure electronic communications platform of agencies of the State power;
- implementation of organizational and technological model of the national cyber security system; rapid response to cyber attacks and cyber incidents;
- deployment of integrated network of situation centres for the relevant government authorities in security and defence sector on the basis of protected information infrastructure (within the scope of competence);
- development of secure integrated system of electronic state registries, databases, data centres, including a single data centre for backup data storage of national electronic information resources;
- system development for storage, transmission and processing of state registers data and databases using modern information and communication technologies (including technologies of online access);
- development of new methods for preventing cyber attacks, cyber incidents and dissemination of information on them;
- requirements elaboration (regulations, instructions) for the safe Internet usage and for providing electronic services by state agencies;
- raising cyber security awareness of state agencies personnel, delivery of the relevant training.

4.3. The primary concern of cyber protection of critical infrastructure is to consist of:

- integrated improvement of legal framework for cyber protection of critical infrastructure;
- definition of criteria for classification of automated information systems, telecommunications systems, information and telecommunication systems as critical information infrastructure;
- establishment and operations support of the public register of the critical information infrastructure;
- regulation of requirements to cyber protection of critical infrastructure;
- establishment and operations support of cyber defence units by the owners (disponent owners) of critical infrastructure;
- determination of qualification criteria for certain categories of employees of critical infrastructure with account of current trends in cyber security and urgent cyber threats; introduction of mandatory periodic performance appraisal of employees for compliance with specified criteria;
- establishing cooperation among cyber security entities which provide cyber protection of critical infrastructure; development of public-private partnership on cyber threats prevention; response to cyber attacks and cyber incidents, elimination of their negative effects, particularly in the cases of crisis situations, special contingency period, state of emergency and martial law;

- development and application of the scheme for information exchange among the state agencies, private sector and citizens regarding the threats to critical information infrastructure.

4.4 Cyber security capacity building of security and defence sector will include in due order the realization of the following measures, in particular:

- protection of technological processes from unauthorized tampering at the critical infrastructure, where control or monitoring is carried out by using information and communication technologies;
- periodical review of the national cyber security system, development of the industry-specific indicators for cyber security;
- development and implementation of joint actions protocols (including real-time information exchange) of cyber security entities during the time of detecting cyber-attacks and cyber incidents;
- training delivery for the entities of security and defence sector to respond to cyber-attacks and cyber incidents, including cyber training for the Armed Forces of Ukraine and other entities of defence and security sector of Ukraine, participation in trainings of this kind within the framework of the collective defence activity;
- state strategic planning practice and target programmes implementation in development of electronic communications, IT, information protection and cyber defence;
- implementation of politico-military, military-technical and other efforts for cyber capacity enhancement of the National Military Establishment, security and defence sector;
- establishment and development of tools, means and instruments for potential response to aggression in cyberspace, which can be used as an instrument of military conflict deterrence and military threats prevention in cyberspace (proactive cyber defence);
- establishment of a single unit to ensure cyber security and cyber defence of Armed Forces of Ukraine at the strategic, operational and tactical levels;
- development of cyber security and cyber defence subdivisions as part of Armed Forces of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Police of Ukraine, intelligence agencies;
- achievement of compatibility with the relevant cyber security and cyber defence subdivisions of NATO member states;
- assistance in development of system of rapid response to computer emergency;
- development of counter-intelligence and operational investigation systems to ensure national cyber security;
- promotion and coordination of research and development in cyber security and cyber defence for the needs of national security and defence;
- capacity enhancement of entities of counterterrorism to prevent from cyber attacks on national electronic information resources, critical infrastructure, and also to counteract intelligence and subversive activities of foreign special services, organizations, groups and individuals against Ukraine in cyberspace;

- restrictions on participation in cyber security and information protection activities for some economic entities that are controlled by the aggressor-nation (recognized as aggressor by the Verkhovna Rada of Ukraine), or countries and individuals, that are under special economic sanctions and other restrictive measures accepted nationally or globally as a consequence of aggression against Ukraine; setting of limits on the use of products, technologies and services provided by such business entities to ensure technical and cryptographic protection of national information resources; increase of state control in this area;
- division of criminal liability for computer-related offences (such as criminal use of electronic computing machines (computers), computer systems, computer networks and telecommunications) committed against the national resources, other information resources, critical information infrastructures and other critical assets; appropriate demarcation of investigative jurisdiction;
- development of staff training system for the needs of the security and defence sectors of Ukraine; increase of scientific and production potential of the system.

4.5. Combating cyber crime will include, as established by law, such measures, among others:

- establishment of effective and convenient contact-centre for reporting the cases of cyber crimes and fraud in cyberspace; improving rapid law enforcement response to cyber crime, especially operational capabilities upgrade of regional law enforcement units;
- improvement of procedural mechanisms for gathering of digital (electronic) criminal evidence; improving classification, techniques, means and technologies of cyber crime identification, cyber crime documentation and expert studies;
- court-ordered locking the identified information resource (information service) by operators and providers of telecommunications;
- norm setting procedure to issue instructions, binding upon the operators and providers of telecommunications with respect to emergency recording and subsequent storage of electronic data, traffic data retention;
- regulation of issue about urgent implementation of procedural actions in real-time environments by applying electronic documents and digital signature;
- implementation of the scheme (protocol) for law enforcement coordination in the area of combating cyber crime;
- training of judges (investigative judges), investigators and prosecutors for operation with electronic criminal evidence, giving full consideration to cyber crimes features;
- introduction of special procedure for information interception in case of cyber crime investigations;
- improving skills training of law enforcement staff.

5. Final Provisions

Strategy Provisions are taken into account during the development of other strategic planning documents on cyber security issues for entities of the security and defence sector of Ukraine.

Head, Administration of the President of Ukraine **B. Lozhkin**