Draft

Ukraine Information Security Concept

Table of Contents

Introduction

This Information Security Concept (hereinafter – "the Concept) is aimed at setting the preconditions for developing Ukraine's information potential to ensure rapid growth with negative external effects brining no real risks to the national information security. The main objective of the information security system is to sustain such development preventing negative impacts of third party interference.

Such an approach may be put into practice only subject to the involvement of all internal parties to information relationships and the efficient cooperation among the Government, civil society, private sector and individuals for information development and its joint protection from external threats.

Part I. General Provisions

Article 1. Purpose of the Concept

The purpose of this Concept is to ensure information sovereignty and identify approaches to protecting the national information space in order to provide a comprehensive information support for Ukrainian people.

Article 2. Definition of Terms

1. Wherever the following words and phrases appear in this Concept, they will have the following meaning:

Information security means protection of vital interests of an individual, citizen, society and the state, such protection preventing the infliction of harm from the provision of incomplete, outdated and unreliable information, violation of information integrity and accessibility, unauthorised circulation of restricted data as well as negative information and psychological impact and wilful infliction of negative effects of the application of information technologies;

Information security threats means the existing and potential events and factors that pose a threat to vital information interests of an individual, citizen, society and the state;

Strategic content means the national information product aimed at maintaining political, cultural and spiritual integrity and developing a political nation;

National information product means audio visual, printed or other product designed to meet information and communication needs of Ukrainian citizens, society and the state, designed by citizens or legal entities of Ukraine in accordance with applicable law;

National information policy means the government action aimed at shaping and regulating the environment in which information and communication needs of Ukrainian citizens, society and the state are met;

Sustainable development of the national information space means a state of the national information space whereby basic information needs and vital information interests of the citizens, society and the state are satisfied to a sufficient degree;

National information space means information flows, national and foreign, available in Ukraine in their entirety;

Information field means information technologies, resources, products and services, information infrastructure facilities, subjects of information activity and systems for regulating social and information relationships;

Ukraine's information sovereignty means Ukraine's exclusive power under the Constitution of Ukraine, Ukrainian legislation and the rules of international law to individually and independently identify and implement, subject to balancing the interests of an individual, citizen, society and the state, national and geopolitical information interests, domestic and foreign information policy, dispose of own information resources, build an infrastructure of the national information space, pave the way for integrating it into a global information space and ensure the national information security;

Information infrastructure means organizational structures and systems in their entirety providing for the functioning and development of the information space, means of information exchange and user access to information resources;

Provision of information security means the activity aimed at prevention, timely identification, removal or neutralization of real and potential threats to Ukraine's information security;

Cyber security means security of vital interests of an individual, citizen, society and the state in the cyberspace;

Cyberspace means the environment, which emerges due to information (automated), telecommunication and information and telecommunication systems operating based on the unified principles and common rules;

Cyber crime means an act in the cyberspace, which is socially dangerous and punishable under applicable criminal laws of Ukraine;

Cyber terrorism means terrorist activities in or using the cyberspace.

2. Other terms not defined herein have the meanings set forth in Ukrainian law.

Article 3. Legal basis for information security

1. Constitution of Ukraine, Law of Ukraine On the Fundamentals of National Security of Ukraine and international treaties by which the Cabinet of Ministers of Ukraine has consented to be bound form the legal basis for information security.

2. This Concept serves as the basis for designing and approving strategies, programmes and plans that set out objectives, principles and lines of action of Ukraine's information security practitioners.

Article 4. Basic approach to providing information security

1. Activities of government agencies responsible for information security are focused on the two dimensions:

ensuring sustainable development of the information space of Ukraine so that such information space is capable of counteracting external and internal threats;

enabling establishment and functioning of the system for protection of the information space development process against threats.

2. Ukraine's information security is ensured through the protection of the national information space against information threats and the promotion of its sustainable development to satisfy vital information interests and needs of a citizen, society and the state.

Article 5. National information security policy principles

1. Fundamental principles of Ukraine’s information security are as follows:

rule of law;

priority of protection of human rights and freedoms relating to information;

timely and adequate protection of vital national interests against real and potential information security threats;

protection of Ukraine’s information sovereignty;

freedom of thought, freedom of speech and free expression of opinions and convictions;

freedom to collect, store, use and disseminate information;

protection against interference with the private and family life of an individual;

access to information only by operation of law;

harmonisation of personal, public and national interests, responsibility of the entire Ukrainian nation for ensuring information security;

delineation of authority, interaction and responsibility of the state and non-state information security practitioners;

priority of development and expansion of information technologies, products and services, ongoing improvement of information transmission channels in terms of quantity and technical quality;

employment of international and collective security systems and arrangements to ensure Ukraine’s information security;

harmonisation of information legislation with the rules of international law and EU regulations;

protection of information sovereignty, national sovereignty, constitutional order and territorial integrity of Ukraine;

construction of Ukrainian identity in the information space, such identity being an integral part of politico-social discourse;

building a dual system of public service and commercial broadcasting;

promoting development of the content in the information space to safeguard and protect universal human values, as well as intellectual, spiritual and cultural potential of Ukrainian people.

Part II. Fundamental Principles of the National Information Security Policy

Article 6. Vital information interests and needs of a citizen, society and the state

1. The focus of the national information security policy is to meet and protect vital information interests and needs of an individual, citizen, society and the state in terms of:

production, consumption, dissemination and development of the national strategic content and information in the interests of a citizen, society and the state;

functioning and security of cybernetic, telecommunication and other automated computer systems forming the infrastructural backbone of the national information space.

Article 7. Focal points of the national information security policy

1. Focal points of the national information security policy are as follows:

striking a balance between strict observance of constitutional rights and freedoms of an individual in relation to information, in particular the freedom of speech, and performing public functions in terms of prevention, timely identification, removal or neutralization of threats to information security of an individual, citizen, society and the state;

putting a regulatory framework in place to orchestrate the development of information space and its protection against external threats and harmonising such regulatory framework with the rules of international law, international cooperation requirements and EU standards and regulations;

designing and implementing an effective national information policy aimed at development of the national information space and harmonisation of control and coordination system among national information policy practitioners and national information security policy practitioners;

establishing cooperation among the government, social sector and private sector, facilitating international cooperation with a view to implement the national information policy and provide information security, designing a high-quality national information product;

comprehensive assistance, government support and priority of designing and distributing the national information product, including beyond the boundaries of Ukraine;

using Ukraine's national information product for the promotion of universal human values in the international information environment and information development of humankind, in particular exchanging visions, approaches and mechanisms with Ukraine's foreign partners to address contemporary challenges instigated by destructive policies of other countries and targeted at undermining democratic values and freedom of expression in the information space.

Article 8. Ukraine's information security threats

1. National information security policy is implemented to prevent interference of internal and external information security threats with the pursuance of vital information interests and needs of an individual, citizen, society and the state, such prevention being a cornerstone of sustainable development of the national information space.

2. Threats to Ukraine's information security are as follows:

communications related threats in relation to the pursuance of the needs of an individual, citizen, society and the state in terms of production, consumption, dissemination and development of the national strategic content and information;

technology related threats in relation to the functioning and security of cybernetic, telecommunication and other automated computer systems forming the infrastructural (technical, instrumental) backbone of the national information space.

3. Communications related threats in relation to the pursuance of the needs of an individual, citizen, society and the state in terms of production, consumption, dissemination and development of the national strategic content and information are as follows:

a) external negative information influence on human and public consciousness through mass media and the Internet, exerted to the detriment of the state with the aim of:

attempting to alter an individual's mental or emotional state, their psychological and physiological characteristics;

influencing freedom of choice by cultivating a culture of violence and cruelty, insolence and contempt for human and national dignity, inciting religious, racial or ethnic hatred and discrimination based on any ground such as ethnic origin, language, religion, etc.;

calling for separatism, overthrow of the constitutional order or violation of the country's territorial integrity;

b) information influence upon Ukraine's population, including military personnel and mobilisation reinforcement pool, to impair defence readiness and undermine the image of service in the military;

c) dissemination of corrupted, unreliable and prejudicial information by subjects of information activity to discredit public authorities and destabilize social and political situation, significantly complicating political decision making, inflicting harm on national interests or creating a negative image of Ukraine;

d) threats to free speech are as follows:

mass media owners' interference with editorial policies;

lack of legal framework to strengthen the role of creative teams and editorial staff in the implementation of editorial policies by mass media, both public and private;

media monopolies allowing for a targeted influence over consumers of information;

administrative and regulatory prerequisites set to restrict free speech and manipulate public opinion, both under external influence and by domestic political organisations, businesses and particular persons;

e) creation, dissemination, transfer and storage of information to support or intensify criminal or terrorist activities.

4. Technology related threats in relation to the functioning and security of cybernetic, telecommunication and other automated computer systems forming the infrastructural (technical, instrumental) backbone of the national information space are as follows:

a) use of cyber forces, cyber units, new types of information weapons and cyber weapons by foreign states to the detriment of Ukraine;

b) acts of cyber crime, cyber terrorism or military cyber aggression posing a threat to the stable functioning of the national information and telecommunication systems, performed via interference with, unauthorised access to or disturbance of the functioning of telecommunication, cybernetic and automated computer systems, public or private, with the aim of:

performing acts of sabotage or terrorism;

supporting or intensifying criminal, extremist or terrorist activities;

exerting destructive information influence;

intercepting telecommunications;

electronic jamming or blocking of information systems, communication media and controls, using software and mathematical tools that disturb the functioning of information systems;

adding hidden malicious functions to software and hardware tools.

c) underdeveloped national information infrastructure, in particular:

dependence of the national information infrastructure on foreign manufacturers of high-technology products;

use of counterfeit and non-certified software and information processing equipment;

inconsistency of the rules governing liability for committed offences with contemporary information security challenges and threats;

insufficient protection of Ukraine's critical information infrastructure facilities.

d) violation of arrangements for access, handling, collection, processing, storage, dissemination or transfer of information protected by the state (state secrets, confidential information, personal data, copyrights and intellectual property) or operations with information resources containing such information;

e) lack of non-governmental monitoring of the activities of information security practitioners and of the security of the national information infrastructure and information space.

Part III. Ukraine's Information Security Practitioners and Mechanisms

Article 9. Ukraine's information security practitioners

1. Information security practitioners are as follows:

citizens of Ukraine, associations of citizens, non-governmental organisations and other civil society institutions;

President of Ukraine, Verkhovna Rada of Ukraine, Cabinet of Ministers of Ukraine, other central executive authorities and security and defence agencies;

mass media, public or private, enterprises, institutions and organisations, public or private, engaged in information activity;

scientific and educational institutions conducting research and training experts in the field of information and information security.

Article 10. Duties and powers of government authorities responsible for information security

1. National Security and Defence Council of Ukraine is a central competent authority designated to coordinate and control the provision of information security as part of the national security and defence within the limits of its competence and authority. According to its mandate, the National Security and Defence Council:

determines strategic national interests of Ukraine as well as conceptual approaches to ensuring national security and defence in the field of information;

drafts national programmes, doctrines, laws of Ukraine, decrees of the President of Ukraine, directives of the Supreme Commander-in-Chief of the Armed Forces of Ukraine, international treaties and other regulations and documents relating to information security of Ukraine;

coordinates and exercises control over other government authorities in the national security and defence sector in relation to the provision of information security of Ukraine;

ongoingly monitors the influence of processes occurring in the field of information on the national security;

specifies the state of information aggression and proposes to the Verkhovna Rada of Ukraine to introduce a special legal framework for the protection of the national information space.

2. Within the limits of their competence and authority, the principal national information security policy practitioners are:

Security Service of Ukraine;

Ministry of Internal Affairs of Ukraine;

Ministry of Defence of Ukraine;

Foreign Intelligence Service of Ukraine;

Designated central executive authority with special status, which provides for formation and implementation of the national policy in relation to the arrangement of special communication, information protection, telecommunications and use of Ukraine's radiofrequency resources.

3. Designated central executive authority shapes, implements and coordinates the national information policy as well as ensures Ukraine's information sovereignty according to its mandate.

The tasks of the designated central executive authority responsible for the national information policy are as follows:

drafting concept papers on sustainable development of the information space and monitoring their implementation within the system of executive authorities;

coordinating central executive authorities actions aimed at ensuring sustainable development of Ukraine's information space;

participating in drafting and implementing strategies, programmes and plans that determine objectives, principles and directions for the implementation of this Concept;

drafting regulations governing the procedure for communication of the government authorities with the public and disclosure of information about their activities, as well as coordinating and controlling actions of the central executive authorities that communicate with the public.

4. Principal national information security policy practitioners are central executive authorities, which shape and implement the national policy in the fields of:

1) education and science, intellectual property, scientific, scientific and technological, and innovation activities, informatisation, provision and use of national electronic information resources, creating preconditions for information-oriented society development, state supervision (control) of educational establishments, public and private;

2) culture and arts, protection of cultural heritage, import, export and return of cultural valuables, national language policy, formation and implementation of the national cinematography policy (with Ukrainian State Film Agency being responsible for the latter);

3) informatisation, e-governance, provision and use of national electronic information resources, information-oriented society development;

4) television and radio broadcasting, information and publishing.

5. Designated central executive authority responsible for shaping, implementing and coordinating the national information policy and the principal national information security policy practitioners act in cooperation with:

1) National Television and Radio Broadcasting Council of Ukraine, a standing collective authority responsible for the supervision of compliance with Ukrainian laws relating to television and radio broadcasting and exercise of the regulatory powers;

2) regulatory authority for telecommunications, informatisation, use of radiofrequency resources and provision of postal services;

3) self-regulatory authorities in Ukraine's media sector.

Article 11. Concept implementation mechanisms

1. Ukraine Information Security Concept, its main provisions and objectives are implemented via the body of regulations. Responsibility for the development and implementation of such regulations is born by the practitioners involved in ensuring information security and sustainable information development as defined in this Concept.

2. Designated central executive authority responsible for the implementation of the national information policy takes action to ensure integrity and coherence of the policy for the provision of information security and protection of information sovereignty of Ukraine.

3. Designated central executive authority responsible for the implementation of the national information policy drafts and submits for consideration in the Cabinet of Ministers of Ukraine proposals for development, approval and implementation of regulations guiding and coordinating information activities of the Cabinet of Ministers of Ukraine, Prime Minister of Ukraine, members of the Cabinet of Ministers of Ukraine, ministries and other central executive authorities and their officials as well as Antimonopoly Committee of Ukraine, State Property Fund of Ukraine and their officials.

4. Designated central executive authority responsible for the implementation of the national information policy drafts and submits for consideration in the National Security and Defence Council of Ukraine proposals for development, approval and implementation of regulations guiding and coordinating information activities of the President of Ukraine, National Security and Defence Council of Ukraine, Ministry of Defence of Ukraine, High Command of the Armed Forces of Ukraine, Ministry of Foreign Affairs of Ukraine, Security Service of Ukraine, National Anti-Corruption Bureau of Ukraine, State Border Guard Service of Ukraine, intelligence and foreign intelligence agencies, and local state administrations.

5. Designated central executive authority responsible for the implementation of the national information policy drafts and submits for consideration in the National Bank of Ukraine and the Prosecutor General's Office of Ukraine proposals for development, approval and implementation of regulations governing their information activities.

6. Cabinet of Ministers of Ukraine, National Security and Defence Council of Ukraine, National Bank of Ukraine and Prosecutor General's Office of Ukraine consider proposals of the designated central executive authority responsible for the implementation of the national information policy and make appropriate decisions within the limits of their competence and authority.

7. Executive authorities acting as national information security policy practitioners provide for the implementation of this Concept in pursuance of the orders of the Cabinet of Ministers of Ukraine and the National Security and Defence Council of Ukraine made based on the proposals of the designated central executive authority responsible for the implementation of the national information policy.

8. Designated central executive authority responsible for the implementation of the national information policy accepts and handles applications from other government authorities, citizens of Ukraine and non-governmental organisations to have them considered in the course of drafting proposals to the Cabinet of Ministers of Ukraine and other executive authorities.

9. Regulations to support the Concept implementation are as follows:

Ukrainian National Information Space Development Programme;

National Internet Access Programme;

National Domestic IT Production Support Programme;

National Programme for International Broadcasting and Ukraine's Representation in the Global Information Space;

National Programme on Common Official Communications Policy;

National Programme for Development of Public-Private Partnership in the Field of Information;

National Programme for Protection of Cultural and Information Needs of Ukrainian Citizens;

National Cyber Security Programme;

National Information Security Specialist Training and Retraining Programme;

National Programme for Scientific and Monitoring Support in the Field of Information.

10. Development and implementation of the above programmes is integral to the duties of practitioners involved in ensuring Ukraine's information security and sustainable information development.

11. Control over compliance with the implementation of said documents and their consistency among one another in terms of objectives and courses of action rests with authorities responsible for coordinating and monitoring Ukraine's sustainable information development and information security in line with this Concept.

Part IV. Non-Governmental Monitoring of and Public-Private Partnership for Implementation of the National Information Policy and Information Security

Article 12. Non-governmental monitoring of implementation of the national information policy and information security

1. Forms of non-governmental monitoring of the implementation of the national information policy are set forth in Ukrainian regulations on community councils and provisions of this Concept.

2. Non-governmental monitoring of the provision of information security is carried out in the forms prescribed by the National Security and Defence Council of Ukraine, such forms being not at variance with applicable laws of Ukraine concerning non-governmental monitoring.

Article 13. Expert Councils as part of non-governmental monitoring of the national information policy implementation

1. The focal point of non-governmental monitoring of the information policy implementation is the formation of designated Expert Councils under the designated central executive authority responsible for the implementation of the national information policy. Expert Councils are established with the aim of non-governmental monitoring of formation, execution and efficiency of the regulations set forth in this Concept and securing its implementation.

2. Regulation on Expert Council is developed and approved by the designated central executive authority responsible for the implementation of the national information policy. Experts Councils are composed of researchers, educators and representatives of community associations and civil society organisations (under a particular national programme). Additional (nonvoting) members may include representatives of government agencies including those responsible for the implementation of specific programmes. By his or her resolution, head of the designated central executive authority responsible for the implementation of the national information policy may appoint Chairpersons of Expert Councils elected by and from among their membership as his or her advisors acting on a pro bono basis.

3. Designated Expert Councils for monitoring the execution of regulations securing implementation of this Concept are primarily tasked with:

preparing proposals at the stage of drafting of the regulations securing implementation of this Concept;

processing interim reports and conducting an independent assessment of the implementation of said programmes in addition to the assessment by the designated central executive authority responsible for the implementation of the national information policy;

drafting targeted proposals to raise the efficiency of the programmes implementation;

inviting representatives of the agencies responsible for implementation of the programmes to participate in the Expert Councils' meetings;

drafting final reports on the efficiency of the national programmes implementation.

Part V. Final Provisions

1. This Concept takes effect on the day of its publication.

2. Applicable laws, i.e. Law of Ukraine On Information, Law of Ukraine On the Cabinet of Ministers of Ukraine (Clause 4, Article 3 and Clause 1, Article 47) and other regulations are to be respectively amended and brought into line with this Concept.

3. The Cabinet of Ministers of Ukraine is to:

bring regulations thereunder into line with this Concept;

submit for consideration in the Verkhovna Rada of Ukraine draft laws concerning the following national programmes:

- Ukrainian National Information Space Development Programme;
- National Internet Access Programme;
- National Domestic IT Production Support Programme;
- National Programme for International Broadcasting and Ukraine's Representation in the Global Information Space;
- National Programme on Common Official Communications Policy;
- National Programme for Development of Public-Private Partnership in the Field of Information;
- National Programme for Protection of Cultural and Information Needs of Ukrainian Citizens;
- National Cyber Security Programme;
- National Information Security Specialist Training and Retraining Programme;
- National Programme for Scientific and Monitoring Support in the Field of Information.