



CYBERSECURITY STRATEGY OF UKRAINE



THE STRATEGY'S GOAL IS creating conditions that ensure safe cyberspace and its use in the interests of individual, society and government. The main focus is on:

1

Developing national cybersecurity system

2

Enhancing capabilities across security and defense sector

3

Ensuring cybersecurity of critical information infrastructure and of government information resources

GUIDING PRINCIPLES

- Respect for human and civil rights and freedoms
- Ensuring national interests of Ukraine
- Open, accessible, sustainable and secure cyberspace
- Cooperation with private sector, civil society and international community
- Adequate risk-based cybersecurity measures
- Priority given to preventative measures
- Inevitable punishment for cybercrimes
- Priority focus on the development of domestic scientific and technical industrial capacity
- Ensuring democratic civil control in the area of cybersecurity

NATIONAL CYBERSECURITY SYSTEM

Ensures collaboration in the area of cybersecurity between all government agencies, local authorities, military units, law enforcement agencies, research institutions, educational institutions, civil groups, businesses, and organizations, irrespective of their form of ownership, that deal with electronic communications and information security or are owners (managers) of critical information infrastructure.



SECURITY SERVICE OF UKRAINE

Fighting cyberterrorism, cyberespionage and countering cybercrimes which pose direct threat to vital interests of Ukraine



NATIONAL SECURITY AND DEFENSE COUNCIL

Coordination and control of defense sector actors responsible for cybersecurity in Ukraine



STATE SERVICE FOR SPECIAL COMMUNICATIONS AND INFORMATION SECURITY

Development and implementation of the government policy to protect the government information resources and critical information infrastructure



MINISTRY OF DEFENSE AND GENERAL STAFF OF THE ARMED FORCES OF UKRAINE

Preparing the state to respond to military aggression in cyberspace



NATIONAL POLICE OF UKRAINE

Countering cybercrimes




INTELLIGENCE AGENCIES OF UKRAINE

Intelligence operations to address the threats to national security in the cyberspace



CYBERSECURITY STRATEGY OF UKRAINE

THREATS TO CYBERSECURITY OF UKRAINE

 Cyberthreats of military nature

 Cyberespionage

 Cyberterrorism

 Cybercrime

KEY AREAS OF ENSURING CYBERSECURITY IN UKRAINE



DEVELOPMENT OF SAFE, SUSTAINABLE AND RELIABLE CYBERSPACE

-  Implement the relevant EU and NATO standards
-  Develop a CERT network
-  Improve legislation
-  Raise public awareness in terms of cybersecurity
-  Establish a system to identify, prevent and neutralize cyberthreats
-  Develop an up-to-date infrastructure of electronic communications, technical and cryptographic protection systems



CYBERSECURITY OF THE GOVERNMENT ELECTRONIC INFORMATION RESOURCES

-  Create an integrated platform of secure electronic communications for government authorities
-  Introduce an organizational and technical model of national cybersecurity system
-  Build up secure system of electronic government registers, databases and data centers



CRITICAL INFRASTRUCTURE CYBERSECURITY

-  Improve legislation
-  Regulate the requirements to cybersecurity of critical infrastructure
-  Develop public-private partnerships to prevent cyberthreats



DEVELOPMENT OF CYBERSECURITY CAPACITY IN DEFENSE SECTOR

-  Develop indicators to evaluate the status of cybersecurity in different spheres
-  Develop joint protocols for cybersecurity actors to respond to cyberattacks
-  Establish cybersecurity and cyberprotection components across the defense forces
-  Facilitate development of CERT network
-  Improve training systems for personnel



FIGHTING CYBERCRIMES

-  Establish a contact center for reporting cybercrimes and fraud in the cyberspace
-  Improve procedural tools for digital forensics
-  Train judges, detectives and prosecutors with regard to handling digital evidence
-  Train law enforcement personnel