CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

National Cybersecurity Governance: UKRAINE

Andrii Davydiuk

NATO Cooperative Cyber Defence Centre of Excellence

Oleksandr Potii

State Service of Special Communications and Information Protection of Ukraine

National Cybersecurity Governance Series

Tallinn 2024

About the authors

Andrii Davydiuk is a PhD in Cybersecurity, a technology researcher at NATO CCDCOE, deputy branch chief in the State Cyber Protection Centre State Service of Special Communications and Information Protection of Ukraine, senior scientific research staff in the G.E. Pukhov Institute for Modelling in Energy Engineering National Academy of Sciences of Ukraine.

Oleksandr Potii deputy head of the State Service of Special Communications and Information Protection of Ukraine, Doctor of Technical Sciences, Professor.

About this study

This publication is part of a series of national reports offering a comprehensive overview of cybersecurity governance by country. The aim is to improve awareness of cybersecurity management across varied national settings, supporting nations in enhancing their domestic cybersecurity governance, encouraging the spread of best practices, and contributing to the development of inter-agency and international cooperation.

Primarily focusing on those NATO Members that are Sponsoring Nations of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), each country report outlines the division of cybersecurity roles and responsibilities between agencies, describes their respective mandate, tasks, and competences as well as any inter-agency coordination. In particular, it covers the mandates of political and strategic management; operational cybersecurity capabilities; cyber incident management; military cyber defence; and cyber aspects of crisis prevention. It offers an introduction to the broader digital ecosystem of the country and outlines national cybersecurity strategy objectives in order to clarify the context for the organisational approach in a particular nation.

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited knowledge hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. The heart of the CCDCOE is a diverse group of international experts from military, government, academia, and industry, currently representing 39 nations.

The CCDCOE maintains its position as an internationally recognised cyber defence hub, a premier source of subject-matter expertise and a fundamental resource in the strategic, legal, operational, and technical aspects of cyber defence. The Centre offers thought leadership on the cutting edge of all aspects of cyber defence and provides a 360-degree view of the sector. The Centre encourages and supports the process of mainstreaming cybersecurity into NATO and national governance and capability, within its closely connected focus areas of technology, strategy, operations, and law.

The Tallinn Manual, prepared at the invitation of the CCDCOE, is the most comprehensive guide for policy advisers and legal experts on how international law applies to cyber operations carried out between and against states and non-state actors. Since 2010, the Centre has organised Locked Shields, the biggest and most complex technical live-fire cyber defence challenge in the world. Each year, Locked Shields gives cybersecurity experts the opportunity to enhance their skills in defending national IT-systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies, and simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects.

The CCDCOE hosts the International Conference on Cyber Conflict, CyCon, a unique annual event in Tallinn, bringing together key experts and decision makers from the global cyber defence community. The conference, which has taken place in Tallinn since 2009, attracts more than 600 participants each spring.

The CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Table of Contents

1. Digital society and cybersecurity assessment

1.1 Digital infrastructure availability and take-up

Country indicators in Ukraine (2023)

Population	37,289,000[1] (2019)
Internet users (% of population)	83.47%[2] (2020)
Area (km2)	603,700[3]
GDP per capita (USD)	4,534[4] (2022)

International rankings

UN statistics[5]	
E-government Development Index 2022	0.80290 (2022) Rank 46 of 193 countries
Online Services Index (OSI)	0.8148 (2022)
Telecommunications Infrastructure Index (TII)	0.7270 (2022)
Human Capital Index (HCI)	0.8669 (2022)
EU statistics[6]	
Global Cybersecurity Index	66 % (2021)
National Cybersecurity Index	80.83 % (2024)

[1] "The Results of the Assessment of the Existing Population of Ukraine Have Been Published" (*www.kmu.gov.ua*) <www.kmu.gov.ua/news/oprilyudneno-rezultati-ocinki-chiselnosti-nayavnogo-naselennya-ukrayini>, accessed on 06.08.2023.

[2] "The Number of Internet Subscribers by Region as of January 1, 2020" (*ukrstat.gov.ua*) <https://ukrstat.gov.ua/operativ/operativ2019/zv/zv_reg/kal_reg/kal_reg0419_u.htm> accessed on 06.08.2023.

[3] "National Atlas of Ukraine" (*World Data Centre | WORLD DATA CENTRE*) <http://wdc.org.ua/atlas/1060000.html> accessed on 06.08.2023.

[4] "GDP Per Capita (Current US$) - Ukraine" (*data.worldbank.org*) <https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=UA> accessed on 06.08.2023.

[5] "E-Government Development Index" <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine> accessed on 06.08.2023.

[6] "NCSI :: Ukraine" (*Index*) <https://ncsi.ega.ee/country/ua/210/> accessed on 06.06.2024.

Ukraine global cyberindex's ranking (2023)

ICT Development Index (IDI) (2017)[7]	IDI Rank 79
National Cyber Power Index (NCPI) (2022)[8]	NCPI Rank 13
Network Readiness Index (NRI) (2022)[9]	NRI Rank 43
Nuclear Security Index (NSI) (2023)[10]	NSI Rank 24

1.2 Digital public services

In Ukraine, to digitise the state and implement digital services, the Ministry of Digital Transformation of Ukraine (MODT) was established.[11] MODT is a central executive body whose activities are directed and coordinated by the Cabinet of Ministers of Ukraine (CMU).

MODT is the main body within the system of central executive authorities that ensures the formation and implementation of state policy in the areas of:

digitisation, digital development, digital economy, digital innovations and technologies, e-governance and e-democracy, development of the information society, informatisation;

implementing electronic document management; in the area of developing digital skills and digital rights of citizens;

open data, public electronic registries, development of national electronic information resources and interoperability, development of broadband Internet access infrastructure, e-commerce and e-business;

providing electronic and administrative services;

electronic trust services and electronic identification;

IT industry development; in the area of development and operation of the Diia City legal regime.

In its activities, the MODT is guided by the Regulation the MODT.[12]

The MODT implements its powers by the Order. Cab. of Ministers of Ukraine dated February 17, 2021 No. 365-r [13] and Decree of the Cabinet of Ministers. of the Ministers of Ukraine dated January 30, 2019 No. 56.[14]

---

[7] "ITU | 2017 Global ICT Development Index" (*ITU: Committed to connecting the world*) <www.itu.int/net4/ITU-D/idi/2017/index.html> accessed on 06.06.2024.

[8] "National Cyber Power Index 2022" (*Belfer Centre for Science and International Affairs*) <www.belfercentre.org/publication/national-cyber-power-index-2022> accessed on 06.06.2024.

[9] "Ukraine – Network Readiness Index" (*Network Readiness Index – Benchmarking the Future of the Network Economy*) <https://networkreadinessindex.org/country/ukraine/> accessed on 06.06.2024.

[10] "The 2023 NTI Nuclear Security Index" (*The Nuclear Threat Initiative*) <www.nti.org/analysis/articles/the-2023-nti-nuclear-security-index/> accessed on 06.06.2024

[11] "About Us Ministry of Digital Transformation of Ukraine" (*Ministry of Digital Transformation of Ukraine*) <https://thedigital.gov.ua/ministry> accessed on 06.06.2024.

[12] Issues of the Ministry of Digital Transformation: Resolution of the Cab. of the Ministers of Ukraine dated September 18, 2019 No. 856: as of January 13 2024 <https://zakon.rada.gov.ua/laws/show/856-2019-п#Text> accessed on 06.06.2024

[13] Issues of digital transformation: Order. Kab. of Ministers of Ukraine dated February 17, 2021 No. 365-r: as of May 4 2023<https://zakon.rada.gov.ua/laws/show/365-2021-p#Text> accessed on 06.06.2024

[14] Issues of digital development: Resolution of the Cab. of the Ministers of Ukraine dated January 30, 2019 No. 56: as of June 30 2023<https://zakon.rada.gov.ua/laws/show/56-2019-п#Text> accessed on 06.06.2024

At the same time, the CMU approved the Strategy of Digital Transformation of the Social Sphere [15] and the Strategy for Implementation of Digital Development, Digital Transformations and Digitalisation of the State Finance Management System for the period until 2025.[16]

Given the above in Ukraine in ministries, other central bodies of executive power, and regional military administrations by the Resolution of the CMU dated 03.03.2020 No. 194[17] the position of deputy head of the relevant body for digital development, Chief Digital Transformation Officer (CDTO) was introduced.

To increase the pace and scope of digitalisation in Ukraine, the Ministry of Digital Affairs created the Unified State Web Portal of Electronic Services "Diia".**[18]**

The Regulation on the Unified State Web Portal of Electronic Services, as approved by the Resolution of the CMU of December 4, 2019 No. 1137,[19] determined that the Diia Portal is intended to implement the right of everyone to access electronic services and information about administrative and other public services, appeal to executive authorities, other state bodies, local self-government bodies, enterprises, institutions and organisations (including by the Law of Ukraine "On appeals of citizens"),[20] obtaining information from national electronic information resources, which is necessary for the provision of services, as well as for monitoring and assessing the quality of services in the cases specified by this Regulation."

In general, the Ministry of Digital has developed and supported such projects as "Diia", " Diia. Digital education", " Diia. Business", "Safety of Children on the Internet", "E-residency", " Diia. City", "European integration", "Laptop for every teacher", "Virtual assets", " Diia. Centre".[21]

Thanks to the "Diia" mobile application, citizens of Ukraine can use electronic documents from a smartphone.

The legal force of digital documents is determined by the following legal acts:

— e-passports and TIN: the Resolution of the CMU dated August 18, 2021 No. 911;[22]

— e-birth certificate: Resolution of the CMU dated September 23, 2020 No. 911;[23]

---

[15] On the approval of the Strategy of digital transformation of the social sphere: Order. Cab. of the Ministers of Ukraine dated October 28, 2020 No. 1353-r <https://zakon.rada.gov.ua/laws/show/1353-2020-p#Text> accessed on 06.06.2024.

[16] On the approval of the Strategy for implementation of digital development, digital transformations and digitalisation of the state finance management system for the period until 2025 and approval of the plan of measures for its implementation: Order. Cab. of the Ministers of Ukraine dated November 17, 2021 No. 1467-r: as of April 11 2023 <https://zakon.rada.gov.ua/laws/show/1467-2021-p#Text> accessed on 06.06.2024.

[17]Issues of the activities of units on issues of digital development, digital transformations and digitalisation of central and local executive bodies and deputy heads of central executive bodies, regional, Kyiv and Sevastopol city state administrations on issues of digital development, digital transformations and digitalisation: Decree of the Cabinet. of Ministers of Ukraine dated 03.03.2020 No. 194<https://zakon.rada.gov.ua/laws/show/194-2020-п#Text> accessed on 06.06.2024.

[18] "Unified state web portal of electronic services DIIA | State Enterprise "DIIA"" (State Enterprise "DIIA")<https://se.diia.gov.ua/unified-state-web-portal-of-electronic-services-diia> accessed on 06.06.2024.

[19] Issue of the Unified State Web Portal of Electronic Services and the Unified State Portal of Administrative Services: Resolution of the Cabinet of Ministers. of Ministers of Ukraine dated 04.12.2019 No. 1137: as of April 2 2024<https://zakon.rada.gov.ua/laws/show/1137-2019-п#Text> accessed on 06.06.2024.

[20] On citizens' appeals: Law of Ukraine dated October 2, 1996 No. 393/96-VR: as of December 31 2023<https://zakon.rada.gov.ua/laws/show/393/96-вр#Text> accessed on 06.06.2024.

[21] About Us Ministry of Digital Transformation of Ukraine (*Ministry of Digital Transformation of Ukraine*) <https://thedigital.gov.ua/ministry> accessed on 06.06.2024.

[22] On the approval of the Procedure for the formation and verification of e-passport and e-passport for traveling abroad, their electronic copies: Decree of the Cabinet of Ministers. of Ministers of Ukraine dated August 18, 2021 No. 911: as of November 17 2022 <https://zakon.rada.gov.ua/laws/show/911-2021-п#Text> accessed on 06.06.2024.

[23] On the implementation of an experimental project on the use of electronic display of information contained in the birth certificate and information about the registered place of residence, which is in the possession and at the disposal of the State. Migration Service: Decree of the Cab. of the Ministers of Ukraine dated September 23, 2020 No. 911: as of March 14. 2022 <https://zakon.rada.gov.ua/laws/show/911-2020-п#Text> accessed on 06.06.2024.

— e-certificate: Resolution of the CMU dated October 1, 2014 No. 509[24];

— e-student card: Resolution of the CMU dated December 18, 2019 No. 1051.[25]

The Committee of the Verkhovna Rada of Ukraine on Digital Transformation is also functioning in Ukraine — formed on August 29, 2019, in the Verkhovna Rada of Ukraine of the 9th convocation.[26]

The subject matter of the Committee is:

- legislative principles of digitisation and digital society in Ukraine;
- National and state informatisation programmes;
- EU programmes "Digital Single Market" (Digital Single Market, EU4Digital) and other digital cooperation programmes;
- innovations in the field of digital entrepreneurship, development of the start-up ecosystem;
- research centres in the field of digital technologies;
- digital industry and telecommunications;
- electronic governance and public electronic services;
- electronic democracy;
- electronic trust services and digital identification;
- state information and analytical systems, electronic document flow;
- state information resources, electronic registers and databases;
- e-commerce (e-commerce, e-business);
- virtual assets, blockchain and tokenisation;
- smart infrastructure (cities, communities, etc.);
- development of the field of "open data";
- radio frequency resources;
- development of orbital economy;
- legislative principles of administration, functioning and use of the Internet in Ukraine;
- cybersecurity and cyber protection, including in the field of critical infrastructure;
- technical and cryptographic protection of information;
- development of digital competencies and digital rights.

Also in Ukraine for the needs of state bodies by the Resolution of the CMU dated February 8, 2021 No. 94[27] the National Centre for Reservation of State Information Resources was implemented.

The National Centre for Reserving State Information Resources (hereinafter - the National Centre) is an organised set of objects created to ensure the reliability and uninterrupted operation of state information resources, cyber protection, storage of state electronic information resources, backup of information and information of state electronic information resources of state bodies, military formations (except the Armed Forces and the Main Intelligence Directorate of the Ministry of Defence) formed by laws, enterprises, institutions and organisations. Duties for ensuring the functioning of the National Centre are assigned to the State Service of Special Communications and Information Protection of Ukraine (SSSCIP). The mechanism of operation of the National Centre for Reservation of State Information Resources is determined by the Resolution of the CMU

---

[24] On the accounting of internally displaced persons: Decree of the Cabinet of Ministers. of the Ministers of Ukraine dated October 1, 2014 No. 509: as of November 24 2023 <https://zakon.rada.gov.ua/laws/show/509-2014-п#Text> accessed on 06.06.2024.

[25] On the implementation of an experimental project regarding the use of electronic student (pupil) tickets: Decree of the Cabinet of Ministers. of the Ministers of Ukraine dated 18.12.2019 No. 1051: as of February 1 2022 <https://zakon.rada.gov.ua/laws/show/1051-2019-п#Text> accessed on 06.06.2024.

[26] About the list, quantitative composition and subjects of the committees of the Verkhovna Rada of Ukraine of the ninth convocation: Resolution Verkhov. of the Council of Ukraine dated August 29, 2019 No. 19-IX: as of February 23 2023 <https://zakon.rada.gov.ua/laws/show/19-20#Text> accessed on 06.06.2024.

[27] On the implementation of an experimental project regarding the functioning of the National Centre for Reservation of State Information Resources: Decree of the Cabinet of Ministers. of Ministers of Ukraine dated February 8, 2021 No. 94: as of April 11 2023 <https://zakon.rada.gov.ua/laws/show/94-2021-п#Text> accessed on 06.06.2024.

dated 04/07/2023 No. 311.[28] Also, the Resolution of the CMU dated 03.03.2022 No. 522 defines the procedure for providing services to the National Centre for Reserving State Information Resources.[29] In particular, the following services are provided:

1. Placing the equipment in the electronic communication cabinet or its part in the common hall.
2. Placement of equipment in an electronic communication cabinet in a screened hall.
3. Placement of equipment in an electronic communication cabinet in a separate screened hall.
4. Providing the use of disk space for technical means of information storage, which is located in the common hall.
5. Providing the use of disk space for technical means of information storage, which is located in a screened hall.
6. Providing the use of disk space for technical means of information storage, which is located in a separate screened hall.
7. Provision of computing resources in the common hall.
8. Provision of use of computing resources in a screened hall.
9. Provision of computing resources in a separate screened hall.
10. Provision of a separate physical server for rent.
11. Providing a virtual server for use.
12. Providing use of dynamically allocated disk resources.
13. Backup of computing resources used for processing (saving) national electronic information resources.
14. Backup of national electronic information resources used for processing (saving) of national electronic information resources.
15. Provision of use of software using computing resources.
16. Placement of national electronic information resources.
17. Administration of national electronic information resources.
18. Storage of national electronic information resources.
19. Connection to protected nodes of access to the Internet of systems for the processing and preservation of national electronic information resources.
20. Provision of secure communication channels for organising access to national electronic information resources.
21. Provision of secure communication channels for the administration of national electronic information resources.
22. Provision of secure mobile access to national information resources.
23. Post-disaster restoration of national electronic information resources.

{Item 23 with changes as introduced by the Resolution of the Cabinet of Ministers No. 311 of 04/07/2023}.

24. Saving backup copies of national electronic information resources.
25. Preservation of data archives of national electronic information resources.
26. Detection and protection against cyber attacks (DDoS attacks and others).
27. Deploying simulation of computing resources of the cyber defence facility.
28. Protection of information in the user domain name system.
29. Detection of cyber incidents and cyber attacks on user equipment.
30. Detection and prevention of unauthorised access to the data transmission network.
31. Protection of information resources using the technical capabilities of the network screen.
32. Protection of e-mail from external cyber threats.
33. Managing access to the data transmission network by security policies.
34. Management of privileged user accounts.
35. Testing computer systems and networks for vulnerability to cyber attacks.

---

[28] Issues of the functioning of the National Centre for Reservation of State Information Resources: Resolution of the Cabinet of the Ministers of Ukraine dated 04/07/2023 No. 311<https://zakon.rada.gov.ua/laws/show/311-2023-п#Text> accessed on 06.06.2024.

[29] On the approval of the Procedure for the provision of services of the National Centre for Reservation of State Information Resources: Resolution of the Cabinet of the Ministers of Ukraine dated May 3, 2022 No. 522: as of April 11 2023<https://zakon.rada.gov.ua/laws/show/522-2022-п#Text> accessed on 06.06.2024.

36. Providing a secure, isolated virtual environment for computer program security research.

37. Protection of websites from cyber incidents and cyber attacks.

38. Provision of virtual secure data transmission networks.

In addition, the SSSCIP, for cyber protection of state bodies and critical infrastructure facilities, ensures the implementation of the National Telecommunications Network, which functions by the Resolution of the CMU dated 16.12.2020 No. 1358.[30]

The national telecommunications network is intended for:

circulation (transmission, reception, creation, processing, storage) and protection of national information resources;

provision of secure electronic communications;

provision of services of the National Telecommunication Network (NTN) in the interests of state management in peacetime, in emergency conditions and special periods;

providing users with cyber protection services.

The list of services of the NTN is determined by the order of the Administration of the State Service for Special Communications and Information Protection of Ukraine dated August 17, 2021 No. 502.[31] In particular, the following groups of services are available:

- transport electronic communication services of NTN;
- special communication services;
- multimedia services of NTN;
- services of access to information resources;
- cyber protection services.

Separately, it is worth highlighting the system of protected access of state bodies to the Internet of the State Cyber Protection Centre[32], which provides secure access to the Internet to government agencies.

The SSSCIP also ensures the functioning of the Computer Emergency Response Team of Ukraine of Ukraine CERT-UA[33] which processes information received from citizens about cyber incidents.

The main regulatory documents that regulate the protection of information in the state bodies of Ukraine in which capacity they provide digital services and their implementation are:

- Law of Ukraine "On information protection in information and communication systems";[34]
- Resolution of the CMU "On Approval of the Rules for Ensuring the Protection of Information in Information, Telecommunication and Information and Telecommunication Systems";[35]
- Resolution of the CMU "On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects";[36]

---

[30] Issues of the functioning of the National Telecommunication Network: Resolution of the Cabinet of the Ministers of Ukraine dated 16.12.2020 No. 1358 as of August 20 2022<https://zakon.rada.gov.ua/laws/show/1358-2020-п#Text> accessed on 06.06.2024.

[31] On the approval of the list of services of the National Telecommunications Network: Order of the Admin. Govt. Special Services Communication and of Information of Ukraine dated August 17, 2021 No. 502: as of April 12 2023. <https://zakon.rada.gov.ua/laws/show/z1288-21#Text> accessed on 06.06.2024.

[32] On the approval of general requirements for cyber protection of critical infrastructure objects: Resolution of the Cabinet of the Ministers of Ukraine dated June 19, 2019 No. 518: as of September 7. 2022. <https://zakon.rada.gov.ua/laws/show/518-2019-п#Text> accessed on 06.06.2024.

[33] "CERT-UA" (*cert.gov.ua*) <https://cert.gov.ua/about-us> accessed on 06.06.2024.

[34] On the protection of information in information and telecommunication systems: Law of Ukraine dated 07/05/1994 No. 80/94-VR: as of April 4 2024 <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text> accessed on 06.06.2024.

[35] On the approval of the rules for ensuring the protection of information in information, telecommunication and information-telecommunication systems: Resolution of the Cabinet of the Ministers of Ukraine dated March 29, 2006 No. 373: as of October 21 2022 <https://zakon.rada.gov.ua/laws/show/373-2006-п#Text> accessed on 06.06.2024.

[36] On the approval of general requirements for cyber protection of critical infrastructure objects: Resolution of the Cabinet of the Ministers of Ukraine dated June 19, 2019 No. 518: as of September 7. 2022. <https://zakon.rada.gov.ua/laws/show/518-2019-п#Text> accessed on 06.06.2024.

- Law of Ukraine "On Protection of Personal Data";[37]
- Law of Ukraine "On electronic identification and electronic trust services";"[38]
- Resolution of the CMU "On the approval of the procedure for the interaction of executive authorities on issues of protection of state information resources in information and electronic communication systems";[39]
- Regulation on the Register of Information, Electronic Communication and Information and Communication Systems of executive authorities, as well as enterprises, institutions and organisations belonging to the sphere of their management (from August 3, 2005 No. 688);[40]
- List of mandatory stages of work during the design, implementation and operation of Informatisation tools (from February 4, 1998 No. 121);[41]
- The procedure for the formation and use of the information fund of the Information and communication systems (ICS) Register (from April 24, 2007 No. 72).[42].

1.3 Digitalisation in business

To scale business and simplify bureaucratic procedures, the Ministry of Digital has developed the Diia.Business project.[43]

This is a large-scale national project for the development of entrepreneurship and exports, which was initiated by the MODT in February 2020. From May 2021, the project will be implemented by the MODT together with the Office for the Development of Entrepreneurship and Export, a state institution responsible for the development and support of Ukrainian entrepreneurship in domestic and foreign markets. The project web portal provides information to Ukrainians who are already engaged in entrepreneurship or are just planning to open their own business on:

- how to prepare for starting a business;
- where to study and receive consultations;
- where to get financial support for business from the state or international programmes;
- how to find investors and partners;

---

[37] On the protection of personal data: Law of Ukraine dated June 1, 2010 No. 2297-VI: as of April 27 2024. <https://zakon.rada.gov.ua/laws/show/2297-17#Text> accessed on 06.06.2024.

[38] On electronic trust services: Law of Ukraine dated October 5, 2017 No. 2155-VIII: as of January 1 2024. <https://zakon.rada.gov.ua/laws/show/2155-19#Text> accessed on 06.06.2024.

[39] On the approval of the procedure for the interaction of executive authorities on the protection of state information resources in information and telecommunication systems: Resolution of the Cabinet of Ministers of Ukraine dated November 16, 2002 No. 1772: as of September 7. 2022 <https://zakon.rada.gov.ua/laws/show/1772-2002-п#Text> accessed on 06.06.2024.

[40] On the approval of the regulations on the Register of Information, Telecommunications and Information and Telecommunications Systems of Executive Authorities, as well as enterprises, institutions and organisations belonging to the sphere of their management: Resolution of the Cabinet of the Ministers of Ukraine dated August 3, 2005 No. 688: as of September 7. 2022 <https://zakon.rada.gov.ua/laws/show/688-2005-п#Text> accessed on 06.06.2024.

[41] On the approval of the list of mandatory stages of work during the design, implementation and operation of informatisation facilities: Decree of the Cabinet of Ministers of Ukraine dated February 4, 1998 No. 121: as of September 3. 2011 <https://zakon.rada.gov.ua/laws/show/121-98-п#Text> accessed on 06.06.2024.

[42] On the approval of the procedure for the formation and use of the information fund of the Register of Information, Telecommunication and Information and Telecommunication Systems of Executive Authorities, as well as enterprises, institutions and organizations belonging to the sphere of their management: Order Admin. Govt. special services communication and of Information of Ukraine dated April 24, 2007 No. 72: as of January 10 2023. <https://zakon.rada.gov.ua/laws/show/z0500-07#Text> accessed on 06.06.2024.

[43]"National project Diia.business" (Diia.business - Main page) <https://business.diia.gov.ua/about-project> accessed on 06.06.2024.

- more about programmes for women's entrepreneurship;
- banking support programmes for various types of businesses;
- how to use state online services for doing business.

Diia.Business is a sub-brand of the Diya ecosystem.

Diia is a brand of the digital state and an ecosystem of projects: Diya portal, Diya mobile application, and Diia.Digital education, Diia.Business and Diia City national projects.

1.4 Cyber threat landscape and cybersecurity assessment

Ensuring cybersecurity is a necessary component of national security.[44] Challenges and cyber threats to the national cyberspace are described in Chapter 3 of the Cybersecurity Strategy of Ukraine Safe Cyberspace and constitute the key to the country's successful development.[45] These include:

- active use of cyber means in international competition;
- the competitive nature of the development of cybersecurity tools in the conditions of rapid progressive changes in information and communication technologies, in particular cloud and quantum computing, 5G networks, big data, the Internet of Things (IoT), artificial intelligence (AI), etc.;
- the militarisation of cyberspace and the development of cyberweapons, which makes it possible to covertly carry out cyber attacks to support hostilities and intelligence-subversive activities in cyberspace;
- the impact of the COVID-19 pandemic on economic activity and social behaviour, which caused a rapid transformation and reorganisation of a significant segment of social relations in remote mode with the wide use of electronic services and ICS;
- introduction of new technologies, digital services and mechanisms of electronic interaction between citizens and the state, which are carried out unsystematically in terms of cybersecurity measures and without proper risk assessment.

Threats to cybersecurity in Ukraine include:

Hybrid aggression of the Russian Federation against Ukraine in cyberspace. The aggressor state is constantly expanding its arsenal of offensive cyber weapons, the use of which can have irreparable and irreversible destructive consequences. Cyberattacks of the Russian Federation are aimed, first and foremost, at the ICS of the state bodies of Ukraine and objects of critical information infrastructure to disable them (cyber sabotage), obtain covert access and control, and conduct intelligence and intelligence-subversive activities. Cyber attacks are also actively used by the aggressor state as an element of special information operations to achieve manipulative influence on the population, interfere in election processes and discredit Ukrainian statehood;

Cybercrime, which damages information resources, social processes, and individual citizens, reduces public trust in information technologies and leads to significant material losses. The use of cyberspace to commit crimes against the foundations of the national security of Ukraine, as well as criminal offences related to the legalisation of the proceeds of crime; human trafficking; the illegal handling of weapons, ammunition or explosives; the illegal circulation of narcotic drugs, psychotropic substances and their analogues or precursors (which are becoming widespread), as well as other objects and substances that threaten the life and health of people, as organised and sponsored by the governments of other states; cyberattacks related to the theft of sensitive information for political, economic or military purposes (i.e., cyber espionage); and the implementation of intelligence and subversive activities. The features of such cyber attacks are their duration, complexity and hidden nature, which makes them difficult to prevent, detect and neutralise, and the use of cyberspace by terrorist organisations to commit acts of cyber terrorism, financial crime and other illicit acts in support of terrorist activities.

Taking into account the challenges and threats that Ukraine faces in cyberspace, the role of cybersecurity in the processes of digital transformation of the state is becoming critical.

---

[44] On the national security of Ukraine: Law of Ukraine dated June 21, 2018 No. 2469-VIII: as of March 31. 2023 <https://zakon.rada.gov.ua/laws/show/2469-19#Text> accessed on 06.06.2024.

[45] On the decision of the National Security and Defence Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine dated August 26, 2021 No. 447/2021. <https://zakon.rada.gov.ua/laws/show/447/2021#Text> accessed on 06.06.2024.

Prerequisites and factors that form the outlined threats:

Ukraine's high technological dependence on foreign manufacturers of information and communication technology products and the lack of a system for assessing the compliance of such products with security requirements increases the degree of vulnerability of the information infrastructure from undeclared functions and narrows the ability to counter cyber threats;

the imperfection of the regulatory and legal framework in the field of cybersecurity, as well as its obsolescence in the field of information protection, slow implementation of the provisions of European legislation, insufficient regulation of the digital component of the investigation of criminal offences, as well as a low level of legal responsibility for violating the requirements of legislation in this area;

lack of relevant structural subdivisions, necessary staffing and proper control over cyber protection in a significant part of state bodies, as well as the inadequate financing of cyber protection works on a residual basis;

lack of a system of an independent audit of information security and mechanisms for disclosing information about vulnerabilities in the conditions of dynamic digitalisation of all spheres of public administration and life activities of the state;

non-compliance with modern requirements of the level of training and advanced training of specialists in cybersecurity and cyber protection, in particular, the ineffective mechanisms of their motivation to work in the public sector;

the absence of a legislative act on the critical infrastructure of Ukraine and its protection, which significantly complicates the formation of a cyber protection system for such infrastructure;

the incompleteness of measures to implement the organisational and technical model of cyber protection (OTM) which will correspond to modern threats, challenges in cyberspace and global trends in the development of the cybersecurity industry;

lack of a system for improving the digital literacy of citizens and a culture of safe behaviour in cyberspace, compounded by a low level of public awareness of cyber threats and cyber protection;

lack of an effective system of information and analytical support for cybersecurity;

insufficient protection against cyber attacks on state information resources and objects of critical information infrastructure;

non-compliance with the requirements of the legislation on the state of protection of ICS of state bodies and economic entities, in which a significant part of information with limited access is processed.

In a separate act, the National Security and Defence Council of Ukraine (NSDC)[46] determined urgent measures to neutralise threats to the state's cybersecurity.

The state has procedures for identifying vulnerabilities and deficiencies in the configuration of information, electronic communication, and ICS in which state information resources are processed;[47] the detection of vulnerabilities and response to such cyber incidents and cyber attacks;[48] search and detection of the open vulnerability of information (automated); electronic communication, ICS, electronic communication networks[49] ; the assessment of the state of security of state information resources in information, electronic

[46] On threats to the cybersecurity of the state and urgent measures to neutralise them: Decision of the National Council of Security and Defence of Ukraine dated December 29, 2016: as of February 16 2017. <https://zakon.rada.gov.ua/laws/show/n0015525-16#Text> accessed on 06.06.2024.

[47] On the implementation of an experimental project on the introduction of a set of organisational and technical measures to identify vulnerabilities and deficiencies in the configuration of information, telecommunication and information and telecommunication systems in which state information resources are processed: Resolution of the Cabinet of Ministers of the Ukraine dated 12/23/2020 No. 1363: as of September 7. 2022 <https://zakon.rada.gov.ua/laws/show/1363-2020-п#Text> accessed on 06.06.2024.

[48] Issues in ensuring the functioning of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks: Resolution of the Cabinet of the Ministers of Ukraine dated December 23, 2020 No. 1295: as of September 7. 2022 <https://zakon.rada.gov.ua/laws/show/1295-2020-п#Text> accessed on 06.06.2024.

[49] On the approval of the Procedure for searching and identifying potential vulnerabilities of information (automated), electronic communication, information and communication systems, electronic communication networks: Decree of the

communication and ICS; [50] scanning for vulnerabilities in government information resources posted on the Internet;[51] a review of the state of cyber protection of critical information infrastructure, state information resources and information, and the requirement for the protection of that which is established by law.[52] [53] In particular, to ensure the operation of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks, equipment sets of the telemetry collection subsystem of ICS (active sensors).[54]

Comprehensive reviews of the state of cyber protection are available in the relevant periodic reports of the SSSCIP, in particular the "Report on the review of the state of cyber protection of critical information infrastructure, state information resources and information, the requirement for the protection of which is established by law",[55] "Information and analytical materials on the state of protection of state electronic information resources in the ICS",[56] "Analytical report on the implementation of the cybersecurity strategy plan of Ukraine for the first half of 2023",[57] "Report on the implementation by the State Service of Special Communications and Information Protection of Ukraine of tasks related to ensuring the cybersecurity of the state in 2022",[58] "Analytical report of the SSSCIP based on the results of the threat research",[59] «Report on the System of Vulnerability Detection and Response to Cyber Incidents and Cyber Attacks»,[60] Committee of the Verkhovna Rada of Ukraine on Digital Transformation and, in particular, the "Report on the submission and further evaluation of the annual report on the results of an independent audit of the activities of the main subjects of

---

Cabinet of the Ministers of Ukraine dated May 16, 2023 No. 497 <https://zakon.rada.gov.ua/laws/show/497-2023-п#Text> accessed on 06.06.2024.

[50] On the approval of the Procedure for assessing the state of security of state information resources in information, telecommunication and information-telecommunication systems: Order of the Admin. Govt. Special Services Communication and of Information of Ukraine dated 02.12.2014 No. 660: as of January 10 2023. <https://zakon.rada.gov.ua/laws/show/z0090-15#Text> accessed on 06.06.2024.

[51] On the approval of the Procedure for scanning for vulnerabilities of state information resources posted on the Internet: Order of the Admin. Govt. special services communication and of Information of Ukraine dated January 15, 2016 No. 20: as of January 10 2023 <https://zakon.rada.gov.ua/laws/show/z0196-16#Text> accessed on 06.06.2024.

[52] On the approval of the Procedure for conducting a review of the state of cyber protection of critical information infrastructure, state information resources and information, the requirement for the protection of which is established by law: Resolution of the Cabinet. of Ministers of Ukraine dated 11.11.2020 No. 1176. <https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text> accessed on 06.06.2024.

[53] On the formation of the Interdepartmental Working Group on the Review of the State of Cyber Protection of Critical Information Infrastructure, State Information Resources and Information whose protection is required by law: Order of Admin. Govt. Special Services Communication and of Information of Ukraine dated September 10, 2021 No. 550: as of November 2 2023 <https://zakon.rada.gov.ua/laws/show/z1264-21#Text> accessed on 06.06.2024.

[54] On the approval of the Procedure for the transfer of equipment sets of the telemetry collection subsystem of information and communication systems (active sensors), the system of detecting vulnerabilities and responding to cyber incidents and cyber attacks to cyber protection objects: Order of Admin. State Service of Special Communication and Information Protection of Ukraine dated June 24, 2022 No. 284 <https://zakon.rada.gov.ua/laws/show/z0758-22#Text> accessed on 06.06.2024.

[55] *Report on the review of the state of cyber protection of critical information infrastructure, state information resources and information, the requirement for the protection of which is established by law* (SSSCIP 2023).

[56] *Informational and analytical materials on the state of protection of state electronic information resources in ICS* (SSSCIP 2023).

[57] *Analytical report on the implementation of the cybersecurity strategy plan of Ukraine for the first half of 2023* (SSSCIP 2023).

[58] *Report on the implementation by the State Service of Special Communications and Information Protection of Ukraine of tasks related to ensuring the cybersecurity of the state in 2022* (SSSCIP 2023).

[59] *Analytical report of the SSSCIP based on the results of the threat research* (SSSCIP 2023). <https://cip.gov.ua/services/cm/api/attachment/download?id=60201>.

[60] *Report on the System of Vulnerability Detection and Response to Cyber Incidents and Cyber Attacks* <https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf>.

national cybersecurity",[61] "Preliminary analytical report on monitoring the implementation of the Law of Ukraine "On the main principles of cybersecurity in Ukraine",[62] "Analytical report of the norms of the legislation of the European Union, which must be implemented in the projects of laws on cybersecurity and on objects of critical infrastructure in Ukraine", and "Best practices of cybersecurity management".[63]

Publications of analytical and statistical data on cyber attacks and threats in cyberspace are carried out by the government response team, the CERT-UA and the National Cybersecurity Coordination Centre of the NSDC.[64]

[61] *Report on the submission and further evaluation of the annual report on the results of an independent audit of the activities of the main subjects of national cybersecurity (Committee on Digital Transformation)* <www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_01.pdf>.

[62] *Preliminary report on monitoring the implementation of the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity in Ukraine" (Committee on Digital Transformation).* <www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_02.pdf>.

[63] *Cybersecurity Management Best Practices (Committee on Digital Transformation)* <www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf>.

[64] "National Cybersecurity Centre" (*National cybersecurity centre*) <www.ncscc.gov.ua/> accessed on 06.06.2024.

2. National cybersecurity strategy and legal framework

2.1 National cybersecurity strategy documents

The first Cybersecurity Strategy of Ukraine was approved by the Decree of the President of Ukraine No. 96 of March 15, 2016. During the years of its implementation, efforts were made to establish and develop the national cybersecurity system. An important stage of its institutionalisation was the adoption of the Law of Ukraine "On the Basic Principles of Ensuring the Cybersecurity of Ukraine", which defined the legal and organisational foundations for the protection of the vital interests of man and citizen, society and the state, the national interests of Ukraine in cyberspace, the main goals, directions and principles of state policy in the field of cybersecurity, the powers of state bodies, enterprises, institutions, organisations, individuals and citizens in this area, and the main principles of coordination of their activities to ensure cybersecurity.

Regulatory support for the cyber protection of critical information infrastructure objects has been improved, and the procedure for its definition and general requirements for its cyber protection have been adopted.

Centres (units) for ensuring cybersecurity or cyber protection have been established in the State Service of Special Communications and Information Protection of Ukraine, the Security Service of Ukraine (SSU), the National Bank of Ukraine, the Ministry of Infrastructure of Ukraine, the Ministry of Defence of Ukraine, and the Armed Forces of Ukraine.

The NTN is being developed, the National Centre for Reserving State Information Resources is being formed, the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks is functioning, and the government response team for computer emergency events of Ukraine CERT-UA is operational. To improve the coordination of the activities of the subjects of the security and defence sector, which provide cybersecurity, a working body of the NSDC – the National Cyber Security Coordination Center (NCSCC), whose solutions contribute to solving the most complex problems in this area, was formed.

Cooperation in the field of cybersecurity with foreign partners is actively developing (the United States of America, the United Kingdom of Great Britain and Northern Ireland, the Federal Republic of Germany, the Kingdom of the Netherlands, Japan, etc.), cooperation with the EU and NATO is deepening, and cyber training is being conducted with the participation of other states and international organisations.

The annual Cybersecurity Month event has been launched.

Decree of the President of Ukraine No. 447/2021, On the decision of the National Security and Defence Council of Ukraine, dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine" a new Cybersecurity Strategy of Ukraine was adopted as a safe cyberspace is the key to the country's successful development.[65]

Ukraine, in addition to the main subjects of the national cybersecurity system, involves a wider range of participants, including business entities, public associations and individual citizens of Ukraine, in solving tasks in the field of cybersecurity. The National Cyber Security Coordination Centre will play a key unifying and coordinating role in this process.

The interaction of cybersecurity entities is regulated by the Law of Ukraine "On the Basic Principles of Cybersecurity".[66]

Subjects that directly implement measures to ensure cybersecurity within their competence are:

1) ministries and other central bodies of executive power;
2) local and state administrations;
3) local self-governing bodies;

[65] On the decision of the National Security and Defence Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine dated August 26, 2021 No. 447/2021. <https://zakon.rada.gov.ua/laws/show/447/2021#Text> accessed on 06.06.2024.

[66] On the main principles of ensuring the cybersecurity of Ukraine: Law of Ukraine dated October 5, 2017 No. 2163-VIII: as of April 4 2024 <https://zakon.rada.gov.ua/laws/show/2163-19#Text> accessed on 06.06.2024.

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

5) Armed Forces of Ukraine and other military formations formed by the law;

6) National Bank of Ukraine;

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

8) business entities, citizens of Ukraine and their associations, and other persons who conduct activities and/or provide services related to national information resources, electronic information services, execution of electronic transactions, electronic communications, information protection and cyber protection.

The main subjects of the national cybersecurity system are the SSSCIP, the National Police of Ukraine, the SSU, the Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine, intelligence agencies, and the National Bank of Ukraine, through which the Constitution and laws of Ukraine perform the following main tasks in the prescribed manner:

1) The SSSCIP ensures the formation and implementation of the state policy on the protection of state information resources and information in cyberspace; the requirement for the protection as enshrined by law; active countermeasures against aggression in cyberspace; cyber protection of critical information infrastructure objects; the conducting of state control in these areas; and the coordination of the activities of other cybersecurity entities concerning cyber protection;

ensures the creation and functioning of the National Telecommunications Network, implementation of the OTM;

conducts organisational and technical measures to prevent, detect and respond to cyber incidents and cyber attacks and eliminate their consequences;

informs about cyber threats and appropriate methods of protection against them; ensures the implementation of information security audits at critical infrastructure facilities; establishes requirements for information security auditors; determines the procedure for their attestation (re-attestation); coordinates, organises and conducts vulnerability audits of the communication and technological systems of critical infrastructure facilities; ensures the functioning of the State Centre for Cyber Protection, the Centre for Active Countering Aggression in Cyberspace, and the government response team for computer emergency events of Ukraine CERT-UA.

2) The National Police of Ukraine ensures the protection of human and citizen rights and freedoms, the interests of society and the state against illegal encroachments in cyberspace; implements measures to prevent, detect, stop and solve cybercrimes, and increase citizens' awareness of cybersecurity.

3) The SSU carries out the prevention, detection, termination and disclosure of criminal offences against the peace and security of humanity, which are committed in cyberspace; carries out counter-intelligence and operational research measures aimed at combating cyber terrorism and cyber espionage; secretly checks the readiness of critical infrastructure facilities for possible cyber attacks and cyber incidents; combats cybercrime, the consequences of which may pose a threat to the vital interests of the state; investigates cyber incidents and cyber attacks regarding state electronic information resources, information whose protection is required by law, as well as critical information infrastructure; and responds to cyber incidents in the sphere of state security.

4) The Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine, by their competence, execute measures to prepare the state to repel military aggression in cyberspace (cyber defence); carry out military cooperation with NATO and other subjects of the defence sphere to ensure the security of cyberspace and joint protection against cyber threats; and implement measures to ensure adequate cyber protection of critical information infrastructure in conditions of emergency and martial law.

5) Intelligence agencies of Ukraine conduct intelligence activities regarding threats to the national security of Ukraine in cyberspace and other events and circumstances related to the field of cybersecurity.

6) The National Bank of Ukraine determines the procedure, requirements and measures for ensuring cyber protection and information security by banks, other persons operating in financial services markets, state regulation and the supervision of those whose activities are carried out by the National Bank of Ukraine, operators of payment systems and/or participants of payment systems, and technological operators of payment services; supervises their implementation; creates a cyber protection centre within the National Bank of Ukraine; ensures the functioning of the cyber protection system for banks; other persons operating in financial services markets whose activities are regulated and supervised by the National Bank of Ukraine; operators of payment systems and/or participants of payment systems; technological operators of payment services; and provides an assessment of the state of cyber protection and audit of information security of critical infrastructure facilities in banks, other persons operating in financial services markets, and state regulation and supervision, whose activities are carried out by the National Bank of Ukraine, operators of payment systems and/or participants of payment systems, as well as technological operators of payment services.

1. Coordination of activities in the field of cybersecurity as a component of the national security of Ukraine is carried out by the President of Ukraine through the NSDC.

2. The National Cybersecurity Coordination Centre, as a working body of the NSDC, coordinates and controls the activities of security and defence sector entities that ensure cybersecurity, and makes proposals to the President of Ukraine regarding the formation and clarification of the Cybersecurity Strategy of Ukraine.

3. The CMU ensures the formation and implementation of state policy in the field of cybersecurity, the protection of human and citizens' rights and freedoms, the national interests of Ukraine in cyberspace, and the fight against cybercrime. Moreover, it organises and provides the necessary forces, means and resources for the functioning of the national cybersecurity system; formulates 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).

The development of the cybersecurity system of Ukraine is carried out based on the OTM.[67] The OTM was developed by specialists of the State Special Communications Service, based on the five-year practice of applying the norms and provisions of the current legislation; the experience of building the national cybersecurity system; the analysis of the strengths and weaknesses of the cybersecurity models of other countries; the practice of organising work in this area and interaction with other subjects of cybersecurity. The OTM is a set of measures, forces and means of cyber protection aimed at prompt (crisis) response to cyber attacks and other cyber incidents, and the implementation of countermeasures aimed at minimising the vulnerability of communication systems.

The Regulation on OTM defines the model itself, its mission, composition and structure, functioning mechanism and goals. For the first time, the definitions of the forces and means of cyber protection, response teams to computer emergency events, and cyber hygiene have been defined. OTM envisages a multi-level architecture, which is a structured system comprising three infrastructures, each of which covers relevant sectors, levels and elements.

The upper level – organisational and management infrastructure – a set of cybersecurity entities that form and/or implement state policy in the field of cybersecurity; the middle level – technological infrastructure – a set of forces and means of cyber protection and their provision; and basic level – basic infrastructure – a set of critical information infrastructure objects and their critical assets, economic entities, the citizens of Ukraine and their various associations, and other persons who conduct activities and/or provide relevant services.

The Regulation on OTM specifies that its implementation is aimed at prompt (crisis) response to cyber attacks and cyber incidents, the implementation of countermeasures and a minimisation of the vulnerability of communication systems.

The regulation on OTM outlines a coherent, non-contradictory, structured system unified by a single idea; the positioning of each subject of the national cybersecurity system within it; the nature of connections with other subjects; forms of interaction between various subjects of one or other levels of the model; directions of information exchange; the main stages of cyber incident management; basic mechanisms of prevention, detection, and identification; as well as responses to cyber incidents and cyber attacks and recovery from them. The Regulation on OTM clearly formulated the cybersecurity ecosystem, in which all participants are closely related to each other and complement each other's activities, while the nature of the relationship is mostly in the form of a partnership rather than an administrative command.

The OTM consists of the organisational and management, technological and basic infrastructure of cyber protection and is implemented to ensure the functioning of the national cybersecurity system.

The organisational and management infrastructure of cyber defence consists of the following sectors:

nationwide, which includes the main subjects of the national cybersecurity system, security and defence forces, and the National Cyber Security Coordination Centre as a working body of the NSDC;

sectoral, which includes central bodies of executive power, other state bodies that ensure the formation and/or implementation of state policy in one or more areas, or directly carry out measures to ensure cybersecurity by their competence, and objects of critical infrastructure regardless of the form of ownership ;

regional (local), which includes local executive bodies, local self-governing bodies, enterprises, institutions and organisations, regardless of the form of ownership, that are engaged in activities in the field of information protection and cyber protection;

---

[67] On the approval of the Regulation on the organisational and technical model of cyber protection: Resolution of the Cabinet of Ministers of Ukraine dated 12/29/2021 No. 1426 <https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text> accessed on 06.06.2024.

of education and science, which includes research institutions, institutions of higher education in the field of information protection and cybersecurity, and those participating in the training, upgrading and retraining of professional personnel;

private, which includes enterprises of non-state ownership, organisations and institutions engaged in information protection and cyber protection (except for critical infrastructure facilities);

public, which includes public organisations, unions, associations, unions and experts in the field of cybersecurity, as well as international and intergovernmental organisations conducting their activities in the field of cybersecurity.

The basic infrastructure of cyber defence functions to ensure the protection of the vital interests of the person and citizenry, society and the state, as well as national interests in cyberspace.

Improving the effectiveness of the national cybersecurity system is currently the main task for ensuring the stable and safe functioning of the national critical information infrastructure in cyberspace, to which OTM provides the solution being implemented. Its normative definition is to create conditions for unifying the efforts of cybersecurity entities in solving the task of increasing the level of cyber resilience of the state's critical information infrastructure, which includes both critical infrastructure objects and communication and information and other systems, the stability and reliability of whose functions are critically important for the functioning of state bodies, enterprises, institutions and organisations of all forms of ownership, associations of citizens.[68]

The implementation of the strategy is carried out by the decision of the National Security and Defence Council of Ukraine dated December 30, 2021 "On the Plan for the Implementation of the Cybersecurity Strategy of Ukraine" as put into effect by the Decree of the President of Ukraine No. 37 dated February 1, 2022, approved at the meeting of the CMU on February 23, 2022 (protocol No. 17).[69] By this document, the State Special Communications Administration is tasked with developing and submitting to the government draft acts necessary for the implementation of the Implementation Plan of the Cybersecurity Strategy of Ukraine, as well as the task of providing the CMU and the NSDC Apparatus with information on the status of implementation of the Implementation Plan of the Cybersecurity Strategy of Ukraine every six months.

As part of the Implementation Plan of the Cybersecurity Strategy of Ukraine, 90 of 94 tasks are actively being carried out, of which 5% were at the stage of "very limited progress" in the first half of 2023 (5% less than in 2022); 13% were at the stage of "initial progress" (2% less than in 2022); 36% at the stage of "accelerating progress" – (2% less than in 2022); and 42% at the stage of "gradual achievement of planned results" – (12% more than in 2022). For the entire year of 2023, the implementation of the tasks of the strategy, in general, increased by 17%.

2.2 National cybersecurity strategy

Priorities of ensuring the cybersecurity of Ukraine and strategic goals. The priorities of ensuring cybersecurity in Ukraine are:

ensuring cyberspace for the protection of state sovereignty and the development of society;

protection of the rights, freedoms and legitimate interests of Ukrainian citizens in cyberspace; and,

European and Euro-Atlantic integration in the field of cybersecurity.

The formation of a new quality of the national cybersecurity system requires a clear and understandable definition of those strategic goals that must be achieved during the period of implementation of this strategy.

For the formation of deterrence potential (C), it is necessary to achieve the following strategic goals:

---

[68] Scientific and practical commentary on the provision on the organisational and technical model of cyber protection, as approved by the resolution of the Cabinet of Ministers of Ukraine dated 12.29.2021 No. 1426" (*https://cip.gov.ua*, 11 Feb. 2022) <https://cip.gov.ua/ua/news/naukovo-praktichnii-komentar-do-polozhennya-pro-organizaciino-tekhnichnu-model-kiberzakhistu-zatverdzhenogo-postanovoyu-kabinetu-ministriv-ukrayini-vid-29-grudnya-2021-r-1426> accessed on 06.06.2024.

[69] On the decision of the National Security and Defence Council of Ukraine dated December 30, 2021 "On the Implementation Plan of the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine dated February 1, 2022 No. 37/2022 <https://zakon.rada.gov.ua/laws/show/37/2022#Text> accessed on 06.06.2024.

Goal C.1. Effective cyber defence - Ukraine will create and ensure the development (including personnel and technology) of units with the authority to conduct armed conflict in cyberspace, will form an appropriate legal, organisational, and technological model of their functioning and application; will ensure effective interaction of the main subjects of the national cybersecurity system and forces of defence during cyber defence activities, proper training and financial support of such structures; systematic cyber training; the evaluation of the capabilities and effectiveness of units; and the development and implementation of indicators for evaluating their activities.

Goal C.2. Effective countering intelligence and subversive activities in cyberspace and cyber terrorism – Ukraine will ensure the continuous implementation of counter-intelligence measures to detect, prevent and stop intelligence and subversive activities of foreign states, acts of cyberespionage and cyberterrorism, eliminate the conditions that contribute to them, and the causes of their occurrence to ensure the interests of the state, society and individual citizens.

Goal C.3. Effective countermeasures against cybercrime – Ukraine will ensure that law enforcement agencies and special state bodies with law enforcement functions acquire capabilities to minimise threats of cybercrime, strengthen their technological and human resources to carry out preventive measures and investigate cybercrimes.

Goal C.4. Development of asymmetric deterrence tools – Ukraine will create the necessary conditions to ensure the deterrence of aggressive actions in cyberspace against Ukraine through the use of economic, diplomatic, and intelligence measures, as well as the involvement of the potential of the private sector.

To acquire cyber resilience (K), it is necessary to achieve the following strategic goals:

Goal K.1. National cyber readiness and reliable cyber defence – Ukraine will introduce and implement clear and understandable measures for national cyber readiness for all interested parties in the interests of ensuring economic well-being and protecting the rights and freedoms of every citizen of Ukraine. Ukraine will strengthen cyber readiness, which will consist of the ability of all interested parties, primarily subjects of the security and defence sector, to respond in a timely and effective manner to cyber attacks, to ensure a regime of constant readiness for real and potential cyber threats, to identify and eliminate prerequisites for their occurrence, thereby ensuring cyber resilience, primarily objects of critical information infrastructure. To this end, Ukraine will create a national incident management system.

Goal K.2. Professional improvement, a cyber-aware society and scientific and technical support of cybersecurity – Ukraine will carry out a fundamental reform of the system of training and advanced training of specialists in the field of cybersecurity, as well as implement measures to preserve the existing qualified personnel potential of cybersecurity subjects; stimulate research and development in the field of cybersecurity, taking into account emergence of new cyber threats and challenges; and establish the creation of national information systems, platforms and products. The domestic scientific and technical potential will primarily be involved in solving the tasks of ensuring the cybersecurity of the state. Digital skills, cyber awareness of modern cyber threats and their countermeasures will become integral elements of the education of every citizen of Ukraine.

Goal K.3. Secure digital services – Ukraine will ensure the achievement of a balance between the needs of society, the domestic market, the state's economy and the necessary cybersecurity measures, as well as the reliability and security of digital services throughout their entire life cycle.

To improve interaction (B), it is necessary to achieve the following strategic goals:

Goal B.1. Strengthening the coordination system – Ukraine will create conditions for the effective interaction of cybersecurity entities in the process of building and functioning of the national cybersecurity system, as well as for effective joint actions during the prevention, repulsion and neutralisation of the consequences of cyber attacks and cyber incidents, and will coordinate the activities of all interested parties to overcome emergencies (crisis) situations in cyberspace.

Goal B.2. Formation of a new model of relations in the field of cybersecurity – Ukraine will introduce a service model of state participation in cyber protection measures, under which the state will be perceived not as a source of requirements, but rather as a partner in the development of the national cybersecurity system.

Goal B.3. Pragmatic international cooperation – Ukraine will direct relations with international partners both to the development of mutual trust for a joint response to cyber attacks and overcoming crises in cybersecurity as well as to purely practical cooperation such as the exchange of information about cyber attacks and cyber incidents, joint cyber operations, and the investigation of international cyber crimes, regular e-learning and training, and the exchange of experience and best practices. Ukraine will ensure active participation in the dialogue within the framework of international organisations regarding the joint development of norms of behaviour in cyberspace and the improvement of the relevant regulatory and legal framework. Ensuring coordination with international partners will be carried out by the Ministry of Foreign Affairs of Ukraine.

2.3 Cybersecurity legislation

The legal basis for ensuring cybersecurity in Ukraine is embedded in the Constitution of Ukraine, the laws of Ukraine on the foundations of national security, the principles of internal and external policy, electronic communications, and the protection of state information resources and information, the requirement for the protection of which is established by law. This and the other laws of Ukraine, the Convention on Cybercrime, and other international treaties whose binding consent has been given by the Verkhovna Rada of Ukraine, decrees by the President of Ukraine, acts of the CMU, as well as other normative legal acts adopted to implement the laws of Ukraine.

The basic laws in the field are the Law of Ukraine "On Information"[70], the Law of Ukraine "On State Secrets"[71], and the Law of Ukraine "On the Basic Principles of Ensuring the Cybersecurity of Ukraine". This Law defines both the legal and organisational bases for ensuring the protection of the vital interests of person and citizen, society and the state, the national interests of Ukraine in cyberspace, as well as the main goals, directions and principles of state policy in the field of cybersecurity, the powers of state bodies, enterprises, institutions, organisations, individuals and citizens in this area, and the main principles of coordinating their activities to ensure cybersecurity.

This law defines the objects of cybersecurity and cyber protection, and the subjects of cybersecurity, and describes the principles underlying the cybersecurity of critical infrastructure objects, the principles of cybersecurity, the national cybersecurity system, and the tasks of the government team in responding to computer emergency events of Ukraine CERT-UA. The foundations of public-private cooperation in the field of cybersecurity and the provision of assistance to entities providing cybersecurity in Ukraine have also been laid. The law provides for responsibility for violations of legislation in the field of cybersecurity, takes into account the issue of financial support for cybersecurity measures, international cooperation within the field of cybersecurity, and control over the legality of measures to ensure cybersecurity in Ukraine.

The requirements for ensuring information and cybersecurity are as established by the Law of Ukraine "On the Protection of Information in Information and Communication Systems". This Law regulates relations in the field of the protection of information and electronic communication systems. This law defines important objects of protection in the system, subjects of relations, describes issues of access to information in the system, relations between the owner of the information and the owner of the system, relations between the owner of the system and the user, relations between owners of systems, conditions of information in the system, the process of ensuring information protection in the system, and the powers of state bodies in the field of information protection in such systems. In addition, responsibility for violation of legislation on information protection in systems and international cooperation is provided.

By this law, state information resources or information with limited access, the requirement for the protection of which is established by law, must be processed in a system using a comprehensive system of information protection with confirmed compliance. Confirmation of the compliance of the comprehensive information protection system is conducted based on the results of the state examination which is in turn carried out taking into account industry requirements and information security norms in the manner established by law.

Confirmation of compliance and state examination of means of the technical and cryptographic protection of information is conducted by the procedure established by legislation. To create a complex system for the protection of state information resources or information with limited access, the requirement for the protection of which is established by law, the cryptographic protection of information (which has a positive expert opinion based on the results of state expertise in the field of cryptographic protection of information) is effected. This affords a technical means of information protection that has a positive expert opinion based on the results of a state examination in the field of technical information protection or a certificate of conformity issued by a conformity assessment body accredited by the national accreditation body of Ukraine, or the national accreditation body of another state, if both the national accreditation body of Ukraine and the national accreditation body such a state is a member of an international or regional accreditation organisation and/or has concluded a mutual recognition agreement with such an organisation regarding conformity assessment.

---

[70] About information: Law of Ukraine dated October 2, 1992 No. 2657-XII: as of July 27 2023 <https://zakon.rada.gov.ua/laws/show/2657-12#Text> accessed on 06.06.2024.

[71] On state secrets: Law of Ukraine dated January 21, 1994 No. 3855-XII: as of January 1 2024 <https://zakon.rada.gov.ua/laws/show/3855-12#Text> accessed on 06.06.2024.

State information resources and information with limited access, except for state secrets, official information and state and unified registers, the creation and operation of which are defined by laws, can be processed in the system without the use of a comprehensive information protection system if all the following conditions are met:

confirmation of the compliance of the information security management system based on the results of the procedure for assessing compliance with the national standards of Ukraine regarding information security management systems which was carried out by a conformity assessment body, an accredited national accreditation body of Ukraine, or a national accreditation body of another state, if it is also a national accreditation body of Ukraine, and the national accreditation body of such a state are members of an international or regional accreditation organisation and/or have entered into a mutual recognition agreement with such organisation regarding conformity assessment;

use for information protection in the system by means of cryptographic information protection, which has a positive expert opinion based on the results of state expertise in the field of cryptographic information protection;

none of the elements of the system can be located, and the owner of such a system or its official representative cannot be a legal entity (its representative) registered in the territories of Ukraine, in which the state authorities of Ukraine temporarily do not exercise their powers, in the territories of states recognised by the Supreme by the Council of Ukraine by the aggressor states, on the territories of states to which sanctions have been applied by the Law of Ukraine "On Sanctions", and on the territories of states that are part of customs unions with such states;

the owner of the system or his representative who provides services using the system, the elements of which are located outside Ukraine, must be a legal entity registered in Ukraine or have its official representative in Ukraine;

fulfilment of special requirements established by the CMU to ensure the protection of information in systems depending on the category of state information resources or information with limited access, the requirement for the protection of which is established by law.

System owners must ensure the proper functioning of systems and the protection of information processed in them by:

creating backup copies of state information resources and systems in compliance with the requirements for their protection, integrity and confidentiality as established for such resources and systems;

ensuring the creation of backup copies of state information resources and systems on individual physical media in an encrypted form and their subsequent transfer (movement) for storage by the procedure established by law, including outside the borders of Ukraine (in particular, in foreign diplomatic institutions of Ukraine), during the period of validity of the legal regime martial law in Ukraine, and six months after its termination or cancellation;

ensuring the transfer (movement) of state information resources and their backup copies for placement on cloud resources and/or data processing centres located outside Ukraine during the period of the legal regime of martial law in Ukraine and six months after its termination or abolition.

Access to the Internet of state bodies must be carried out using secure Internet access nodes, while the state provides services to the system to ensure secure access of state bodies to the Internet.[72]

The use of computer programmes in executive bodies is regulated by Resolution No. 1433 of the CMU dated September 10, 2003.[73]

---

[72] On the approval of the Regulation on the system of protected access of state bodies to the Internet: Order of the Admin. State Service of Special Communication and Information Protection of Ukraine dated August 30, 2023 No. 771 <https://zakon.rada.gov.ua/laws/show/z1624-23#Text> accessed on 06.06.2024.

[73] On the approval of the 'Procedure for the use of computer programs in executive authorities': Resolution of the Cabinet of Ministers of Ukraine dated September 10, 2003 No. 1433: as of April 12 2024. <https://zakon.rada.gov.ua/laws/show/1433-2003-п#Text> accessed on 06.06.2024.

Methodological recommendations for increasing the level of cyber protection of electronic document management systems have been developed.[74]

Placement of systems and storage of backup copies of state information resources and systems in the territories of Ukraine, in which the state authorities of Ukraine temporarily do not exercise their powers, and in those territories of states recognised by the Verkhovna Rada of Ukraine as aggressor states, in the territories of states in respect of which sanctions have been applied by the Law of Ukraine on Sanctions, and the territories of states that are part of customs and military unions with such states, is prohibited.

According to the Decree of the President of Ukraine No. 447/2021, on the decision of the National Security and Defence Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine" provides for the National Response Plan to Emergency (crisis) situations in cyberspace. Also by the Decree of the President of Ukraine dated February 1, 2022 "On the decision of the National Security and Defence Council of Ukraine" dated December 30, 2021, and "On the Implementation Plan of the Cybersecurity Strategy of Ukraine" [75] the development of the National Plan for responding to emergency (crisis) situations in cyberspace is planned for the second half of 2023.

By the Law of Ukraine "On the Basic Principles of Ensuring the Cybersecurity of Ukraine", the Ministry of Defence of Ukraine, the General Staff of the Armed Forces of Ukraine, by their competence, carry out measures to prepare the state to repel military aggression in cyberspace (cyber defence).

At the same time, the Law of Ukraine "On the State Service of Special Communications and Information Protection of Ukraine"[76] is envisaged to create and ensure the functioning of a system of active countermeasures against aggression in cyberspace and to create and ensure the functioning of the Centre for active countermeasures against aggression in cyberspace.

The Law of Ukraine "On Cyber Forces of the Armed Forces of Ukraine" is also being developed in Ukraine.

The Convention of the Council of Europe "Convention on Cybercrime" and the Additional Protocol to the Convention on Cybercrime concerning the criminalisation of racist and xenophobic acts committed through computer systems dated January 28, 2003, were ratified in Ukraine.

The term cybercrime is defined in the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine". Cybercrime is a socially dangerous criminal act, for which criminal responsibility is provided by law, committed in cyberspace with the help of electronic computing machines (computers), automated systems, computer networks or telecommunication networks, which consists in the illegal, unauthorised creation, storage, processing, forgery, blocking, and/or destruction of information infrastructure objects.

- The Criminal Code of Ukraine defines criminal liability for crimes in cyberspace. It provides for the following types of crimes:
- Unauthorised interference in the operation of information (automated), electronic communication, ICS, electronic communication networks (Article 361 of the Criminal Code of Ukraine);
- creation for illegal use, distribution or sale of malicious software or technical means of its dissemination, as well as their distribution or sale (Article 361 of the Criminal Code of Ukraine);
- unauthorised sale or distribution of information with limited access, which is stored in electronic computing machines (computers), automated systems, computer networks or on the carriers of such information (Article 361 of the Criminal Code of Ukraine);
- unauthorised actions with information that is processed in electronic computing machines (computers), automated systems, computer networks or stored on the media of such information, committed by a person who has the right to access it (Article 362 of the Criminal Code of Ukraine);

---

[74] On the approval of 'Methodological recommendations for increasing the level of cyber protection of electronic document management systems': Order of Admin. SSSCIP of Ukraine dated August 30, 2023 No. 773. <https://zakon.rada.gov.ua/rada/show/v0773519-23#Text> accessed on 06.06.2024..

[75] On the decision of the National Security and Defence Council of Ukraine dated December 30, 2021 "On the Implementation Plan of the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine dated February 1, 2022. No. 37/2022<https://zakon.rada.gov.ua/laws/show/37/2022#Text> accessed on 06.06.2024.

[76] On the State Service for Special Communications and Information Protection of Ukraine: Law of Ukraine dated 23.02.2006 No. 3475-IV: as of December 31 2023.

<https://zakon.rada.gov.ua/laws/show/3475-15#Text> accessed on 06.06.2024.

• violation of the rules for the operation of electronic computing machines (computers), automated systems, computer networks or telecommunications networks or the order or rules for the protection of information processed in them (Article 363 of the Criminal Code of Ukraine);

• obstructing the operation of electronic computing machines (computers), automated systems, computer networks or telecommunication networks designed for the mass distribution of telecommunication messages (Article 363 of the Criminal Code of Ukraine).

In addition, the activities of cybercriminals are qualified under Article 200 of the Criminal Code of Ukraine – illegal actions with transfer documents, payment cards and other means of access to bank accounts, electronic money, equipment for their production and Part 3 190 of the Criminal Code of Ukraine "Fraud committed by illegal operations using electronic computing equipment", Art. 231 of the Criminal Code of Ukraine pertaining to the "Illegal collection for use or use of information constituting a commercial or banking secret."

Carding – fraudulent transactions with credit cards (credit card details) that are not approved by the cardholder. This can be theft or illegal acquisition of a credit card, or copying of card data for further forgery, or copying of card details for making purchases over the Internet without the participation of the cardholder. In any case, the main goal of criminals is to gain access to other people's money. To achieve this goal, criminals invent various ways of obtaining the necessary information from inattentive and gullible citizens. One such method is phishing.

Phishing – fraudulent actions aimed at luring card details from its owner. Usually, the owner of the credit card himself voluntarily informs the fraudsters of the necessary information.

There are several types of phishing:

• SMS phishing, when a potential victim of fraudsters receives a message that their credit card has been blocked by the bank and they need to provide details to unlock it, or that the cardholder has won a prize but needs to pay for its delivery. There are many options for SMS messages, so you need to be extra careful if you receive such a message.

• Internet phishing, when fraudsters create phishing (fake) pages that imitate official pages of banks, payment services, online stores, etc.

Vishing is a type of cybercrime in which the messages contain a request to call a certain city number and, during the conversation, the confidential data of the cardholder is requested.

Skimming – copying payment card data using a special device (skimmer). Usually occurs during card transactions with ATMs. To obtain data, criminals use mini-cameras or replaceable keyboards.

Point-of-Sale Skimming is a modernised type of skimming. In this case, fraudsters use an almost invisible device that is placed inside the card reader. In this way, credit card data is copied imperceptibly.

Online fraud – including fake online auctions, online stores, websites and telecommunications.

Piracy – illegal distribution of intellectual property objects on the Internet.

Malware – the creation and distribution of viruses and malicious software.

Illegal content – content that promotes extremism, terrorism, drug addiction, pornography, or the cult of cruelty and violence.

Refiling is an illegal substitution for telephone traffic.

By combating crime in cyberspace by the Resolution of the CMU "On the Formation of a Territorial Body of the National Police"[77] the Cyber Police Department was established.

[77] On the formation of a territorial body of the National Police: Resolution of the Cabinet. of the Ministers of Ukraine dated 13.10.2015 No. 831 <https://zakon.rada.gov.ua/laws/show/831-2015-п#Text> accessed on 06.06.2024

Critical infrastructure

The issue of the cyber protection of critical infrastructure is regulated by the Law of Ukraine "On Critical Infrastructure",[78]Resolution of the CMU "On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects" dated June 19, 2019 No. 518[79], Resolution of the CMU "Some issues of critical infrastructure facilities" dated October 9, 2020 No. 1109[80], Resolution of the CMU "Some issues of critical information infrastructure facilities" dated October 9, 2020 No. 943, Resolution of the CMU "Some issues of certification of critical infrastructure objects" dated August 4, 2023 No. 818[81], By Order of the SSSCIP Administration No. 23, On Approval of Methodological Recommendations for the Categorisation of Critical Infrastructure Object,[82] Order of the State Special Communications Administration No. 601, On Approval of Methodological Recommendations on Increasing the Level of Cyber Protection of Critical Information Infrastructure (with amendments),[83] Order of the SSSCIP Administration No. 463 On Approval of Methodological Recommendations for Ensuring Cyber Protection of Automated Process Management Systems. [84] Recommendations for the development of a plan for the protection of a critical infrastructure object based on the project threat of a national-level "cyber attack/cyber incident" and the corresponding form of a plan for the protection of a critical infrastructure object have been developed. Acquisition of the legal status of a critical infrastructure object is carried out after confirmation of the entry of information about such an object into the state register of critical infrastructure.[85]

Cloud services

The activities of cloud service providers in Ukraine are regulated by the Law of Ukraine "On Cloud Services".[86] This Law defines the legal relations that arise in the provision of cloud services and establishes the specifics of the use of cloud services by state authorities, authorities of the Autonomous Republic of Crimea, local self-government bodies, military formations formed by the laws of Ukraine, state enterprises, institutions and organisations by subjects of power and other subjects to whom such powers have been delegated.

According to the second part of Article 8 of the law, to provide cloud services and/or data centre services to public users and/or critical infrastructure facilities, information about providers of cloud services and/or data centre services must be included in the list.

By the first part of Article 12 of the Law, the CMU establishes the procedure for providing cloud services and/or data processing centre services related to the processing of state information resources or information

---

[78] On critical infrastructure: Law of Ukraine dated November 16, 2021 No. 1882-IX: as of January 1 2024. <https://zakon.rada.gov.ua/laws/show/1882-20#Text> accessed on 06.06.2024.

[79] On the approval of the General requirements for cyber protection of critical infrastructure objects: Resolution of the Cabinet of the Ministers of Ukraine dated June 19, 2019 No. 518: as of September 7. 2022. <https://zakon.rada.gov.ua/laws/show/518-2019-п#Text> accessed on 06.06.2024.

[80] Issues of critical infrastructure objects: Resolution of the Cabinet of the Ministers of Ukraine dated October 9, 2020 No. 1109: as of January 20 2024. <https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text> accessed on 06.06.2024.

[81] Issues of certification of critical infrastructure objects: Decree of the Cabinet of Ministers of Ukraine dated August 4, 2023 No. 818. <https://zakon.rada.gov.ua/laws/show/818-2023-п#Text> accessed on 06.06.2024.

[82] Order of the SSSCIP Administration No. 23, On Approval of Methodological Recommendations for the Categorisation of Critical Infrastructure Objects. <https://zakon.rada.gov.ua/rada/show/v0023519-21#Text> accessed on 06.06.2024.

[83] Order of the SSSCIP Administration No. 601, On the approval of Methodological recommendations for increasing the level of cyber protection of critical information infrastructure (with changes). <https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601> accessed on 06.06.2024.

[84] Order of the SSSCIP Administration No. 463, On Approval of Methodological Recommendations for Ensuring Cyber Protection of Automated Systems for Controlling Technological Processes. <https://zakon.rada.gov.ua/rada/show/v0463519-23#Text> accessed on 06.06.2024.

[85] Order of the SSSCIP Administration No. 793 On the approval of forms for submitting information to the state register of objects of critical information infrastructure. <https://zakon.rada.gov.ua/rada/show/v0793519-23#Text> accessed on 06.06.2024.

[86] On cloud services: Law of Ukraine dated February 17, 2022 No. 2075-IX: as of April 4 2024. <https://zakon.rada.gov.ua/laws/show/2075-20#Text> accessed on 06.06.2024.

with limited access, the requirement for the protection of which is established by law, based on the principles of interoperability and preservation of competition, and determines the order of:

mandatory backup and storage of backup copies in independent systems;

data transfers from the user of cloud services to the provider of cloud services and/or data centre services to ensure the provision of cloud services, as well as from the provider of cloud services to the user of cloud services;

data transfer from one provider of cloud services and/or data centre services to another;

provision of information necessary for assessing the security of network and information systems of providers of cloud services and/or data centre services, including documented security policies.

Part two of Article 12 of the Law establishes requirements for the provisions that must be contained in the procedure for providing cloud services and/or data centre services. Such an order should include:

- requirements for data transmission in a structured form, commonly used and machine-readable formats;
- a requirement for the volume of information regarding processes, technical requirements, terms and payments applicable in case of switching to another provider of cloud services and/or data centre services or refusal of cloud services, which must be provided to the user of cloud services in a clear and accessible form to determine the winner of the procurement procedure (simplified procurement procedure);
- approaches that facilitate the comparison of cloud services and/or data centre services and cloud infrastructure, including, in particular, information on quality management, information security management, service continuity management, and environmental impact assessment.

Article 8 of the Law of Ukraine "On Cloud Services" (dated February 17, 2022 No. 2075-IX) requires the provider of cloud services and/or data centre services to fulfil several requirements. The provider of cloud services and/or data centre services must take appropriate, proportionate technical and organisational measures to manage the risks arising for the security of the electronic communication network and those electronic communication service and information systems used to provide cloud services.

Such measures must ensure the level of security of the electronic communication network, electronic communication service and information systems used to provide cloud services, which corresponds to the risk that has arisen, and take into account the following elements: the security of systems and equipment; settlement of incidents; business continuity management; monitoring, auditing and testing; and compliance with international standards.

The provider of cloud services and/or data centre services must notify the regulator of communication services and CERT-UA without unreasonable delay about any incident that has a significant negative impact on the provision of the cloud service and/or data centre services, in the manner approved by the regulator communication services.

The provider of cloud services and/or data centre services must:

- provide the state body designated for the formation and implementation of state policy in the field of cyber protection with the information necessary to assess the security of the electronic communication network and electronic communication service and information systems, including the documented security policy;
- eliminate any non-compliance with the requirements approved by the communications services regulator.

Resolution of the CMU dated March 12, 2022 No. 263 "Some issues of ensuring the functioning of ICS, electronic communication systems, and public electronic registers under martial law" stipulates that, during the period of martial law, ministries, other central and local bodies of executive power, state and communal enterprises, institutions, and organisations belonging to the sphere of their management, must ensure the proper functioning of information, information and communication and electronic communication systems, and public electronic registers as the owners (holders) and/or administrators, as well as the protection of any information that is processed within them. To this end, they may take the following additional measures:

- place state information resources and public electronic registers on cloud resources and/or in data processing centres located outside of Ukraine, and register domain names in the gov.ua domain for each such placement;
- create additional backup copies of state information resources and public electronic registers in compliance with the requirements for integrity, confidentiality and availability established for such resources;
- stop and limit the operation of information, information and communication and electronic communication systems, as well as public electronic registers.

Ministries, other central and local bodies of executive power, state and communal enterprises, institutions, and organisations belonging to the sphere of their management can use cloud resources and/or data processing centres located outside the state border of Ukraine free of charge or for a fee.

Ministries and other central and local bodies of executive power are instructed, within six months after the termination or abolition of martial law, to stop implementing the above-mentioned measures, and to immediately notify the Administration of the SSSCIP and the Ministry of Digital Transformation of the termination of the above-mentioned measures.

3. National cybersecurity governance

3.1 Strategic leadership and policy coordination

At the strategic level, coordination on cybersecurity issues is carried out by the National Cybersecurity Coordination Centre of the NSDC, which is a working body of the NSDC, formed by the decision of the National Security and Defence Council of Ukraine dated January 27, 2016 "On the Cyber Security Strategy of Ukraine " and which was put into effect by the Decree of the President of Ukraine dated March 15, 2016 No. 96.

The NCSCC functions by the Regulation on the National Cybersecurity Coordination Center, approved by the Decree of the President of Ukraine dated June 7, 2016 No. 242/2016.[87] The NCCS coordinates only the main subjects of cybersecurity and its decisions are mandatory for consideration but not for implementation by all state bodies. The NCCS approved the procedure for the interaction of cybersecurity entities during any response to cyber incidents/cyber attacks.[88]

The NCSCC interacts with the NATO CCDCOE through the Technical Agreement, which includes interaction with NATO countries and partner countries represented in the NATO CCDCOE.

3.2 Cybersecurity authority and cyber incident response

The SSSCIP is a state body that is appointed to ensure the functioning and development of the state system of government communication, the National System of Confidential Communication, the formation and implementation of state policy in the fields of cryptographic and technical information protection, cyber protection, special purpose postal communication, government field service communication, active countermeasures against aggression in cyberspace, as well as other tasks mandated by the law.

The implementation of the OTM as a component of the National Cybersecurity System is carried out by the State Centre for Cyber Protection, which ensures the creation and operation of the main components of the system of protected access of state bodies to the Internet; the system of antivirus protection of national information resources; the audit of information security and the state of cyber protection of critical information objects infrastructure; systems for detecting vulnerabilities and responding to cyber incidents and cyber attacks regarding cyber protection objects; systems for the interaction of teams responding to computer emergencies, as well as in cooperation with other subjects of cybersecurity, developing scenarios for responding to cyber threats, measures to counter such threats, and programmes and methods of cyber training.

The tasks of CERT-UA are the:

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

2) provision of practical assistance to the owners of cyber protection objects in matters of prevention, detection and elimination of the consequences of cyber incidents in relation to these objects;

3) organisation and holding of practical seminars on cyber protection issues for subjects of the national cybersecurity system and owners of cyber protection objects;

4) preparation and placement on its official website of recommendations on combating modern types of cyber attacks and cyber threats;

5) interaction with law enforcement agencies, providing them with timely information about cyber attacks;

---

[87] About the National Cyber Security Coordination Center: Decree of the President of Ukraine dated 07.06.2016 No. 242/2016: as of July 17 2021. <https://zakon.rada.gov.ua/laws/show/242/2016#Text> accessed on 06.06.2024.

[88] "National Security and Defence Council of Ukraine" (National Security and Defence Council of Ukraine) <www.rnbo.gov.ua/ua/Diialnist/5765.html> accessed on 06.06.2024.

6) interaction with foreign and international organisations on cyber incident response issues, in particular within the framework of participation in the FIRST Security Incident Response Teams Forum with payment of annual membership fees;

7) interaction with Ukrainian computer emergency response teams, as well as other enterprises, institutions and organisations, regardless of the form of ownership, that conduct activities related to ensuring the security of cyberspace;

8) processing of information received from citizens about cyber incidents regarding cyber protection objects;

9) assistance to state bodies, local self-government bodies, military formations formed by the law, enterprises, institutions and organisations, regardless of the form of ownership, as well as citizens of Ukraine in solving issues of cyber protection and countering cyber threats.

Also important international interaction is the participation of the CERT-UA in the Forum of Computer Security Incident Response Teams FIRST and Trusted Introducer (TF-CSIRT).[89]

The exchange of information on cyber incidents is carried out by the General Rules for the Exchange of Information on Cyber Incidents (TLP Protocol) as approved at the meeting of the NCSCC of the NSDC.

The response of cybersecurity entities to various types of events in cyberspace is carried out by the Resolution of the CMU dated April 4, 2023 No. 299 "Some issues of the response of cybersecurity entities to various types of events in cyberspace"[90] taking into account the relevant methodological recommendations approved by the order of the State Special Communications Administration dated July 3, 2023 No. 570.[91] At the same time, this issue is also regulated by the Resolution of the CMU "On approval of the procedure for the interaction of executive authorities on the protection of state information resources in information and electronic communication systems".[92]

3.3 Cyber crisis management

To manage crises in cyberspace, a modern information and analytical system within the Main Situation Centre of the country "SOTA" has been developed and put into operation as part of the Apparatus of the NSDC of Ukraine.[93] The Cyber Security Situation Centre of the SSU was created and one of the decisions of the NCSCC envisages the construction of a cybersecurity situation centre, specifically in the field of energy.

Currently, specialists of the NSDC Apparatus of Ukraine, together with interested ministries and departments, are working on the implementation of the decision of the National Security and Defence Council of Ukraine dated June 4, 2021 "Regarding the improvement of the network of situational centres and digital transformation of the sphere of national security and defence", put into effect by the Decree of the President of

---

[89] "Trusted Introducer : Directory : CERT-UA" (*Trusted Introducer : Home*) <www.trusted-introducer.org/directory/teams/cert-ua.html> accessed on 06.06.2024.

[90] Some issues of response by cybersecurity entities to various types of events in cyberspace: Resolution of the Cabinet of Ministers of Ukraine dated 04.04.2023 No. 299 <https://zakon.rada.gov.ua/laws/show/299-2023-п#Text> accessed on 06.06.2024.

[91] Order of the SSSCIP Administration No. 570 On the approval of Methodological recommendations on the response of cybersecurity entities to various types of events in cyberspace <https://zakon.rada.gov.ua/rada/show/v0570519-23#Text> accessed on 06.06.2024.

[92] On the approval of the Procedure for the interaction of executive authorities on the protection of state information resources in information and telecommunication systems: Resolution of the Cabinet of Ministers of Ukraine dated November 16, 2002 No. 1772: as of September 7. 2022 <https://zakon.rada.gov.ua/laws/show/1772-2002-п#Text> accessed on 06.06.2024.

[93] "National Security and Defense Council of Ukraine" (National Security and Defense Council of Ukraine). <www.rnbo.gov.ua/ua/Diialnist/5011.html> accessed on 06.06.2024.

Ukraine dated 18 June 2021 No. 260,[94] in terms of software implementation of IAS "SOTA" into a unified network of state situational centres.

3.4 Military cyber defence

Communications and cybersecurity forces of the Armed Forces of Ukraine are special forces of the Armed Forces of Ukraine which are assigned the task of ensuring the functionality of communication and information systems in addition to combat control and alert systems, as well as their expansion in peacetime. During this special period, under which conditions of emergency and martial law prevail, they must solve the tasks of ensuring the management of the troops (forces) of the Armed Forces of Ukraine, as well as the implementation of measures for the functioning of the national cybersecurity system of Ukraine.

The main communication and cybersecurity department of the General Staff of the Armed Forces of Ukraine (hereinafter – J6) is a structural unit of the General Staff of the Armed Forces of Ukraine (hereinafter – the General Staff of the Armed Forces of Ukraine), and is responsible for the communication systems of the Armed Forces of Ukraine, which are designed to manage the communication systems of the Armed Forces of Ukraine, the organisation of their functioning, planning measures for their expansion and scaling, organisation, management of cybersecurity in the Armed Forces of Ukraine, protection of information in the communication systems of the Armed Forces of Ukraine (ICS of the Armed Forces of Ukraine) and cyber protection of the ICS of the Armed Forces of Ukraine, both in peacetime and during any special period of martial law, planning communications and defence cyber operations of the Armed Forces of Ukraine (participation of the Armed Forces of Ukraine in defensive cyber operations of the defence forces) during the course of strategic planning of the use of the Armed Forces of Ukraine, other components of the defence forces, the development of the communication system of the Armed Forces of Ukraine, planning to provide the Armed Forces of Ukraine with equipment and communications property.

J-6 is the central body of the classified communication of the Armed Forces of Ukraine and the main body for the organisation of providing field and postal communications of the Armed Forces of Ukraine.J6 підпорядковується начальнику Генерального штабу Збройних Сил України.

The activities of J6 are directly directed, coordinated and controlled by the Deputy Chief of the General Staff of the Armed Forces of Ukraine by the division of powers.

The main tasks of J6 are the:

- planning, organisation of operation, and implementation of the management of the electronic communication network of the Armed Forces of Ukraine, the organisation of its expansion and scaling;
- planning, organising and ensuring the functioning of special communication systems of the Armed Forces of Ukraine, including monitoring the state of the organisation and ensuring the security of special (classified) communication and cryptographic protection of service information;
- planning, organisation and management of the ICS of the Armed Forces of Ukraine, the organisation of basic and functional services to the leadership of the Armed Forces of Ukraine, military management bodies and other military organisational structures of the Armed Forces of Ukraine;
- organisation and management of cybersecurity of the Armed Forces of Ukraine, the protection of information in the ICS of the Armed Forces of Ukraine, and the cyber protection of the ICS of the Armed Forces of Ukraine, the organisation and preparation of defensive cyber operations of the Armed Forces of Ukraine, and the participation of the Armed Forces of Ukraine in defensive cyber operations of the defence forces;
- planning, organisation of operation and implementation of management of the operation of the field service and postal communication systems within the Armed Forces of Ukraine;
- communication planning during the strategic planning of the use of the Armed Forces of Ukraine and other components of the defence forces;
- planning of provision of military administration bodies, military units and units of the Armed Forces of Ukraine with equipment and communication property (services), as well as field and postal communication property;

[94] Україна, Рада національної безпеки і оборони України. (2021, 4 черв.). Рішення Ради національної безпеки і оборони України, Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони. Дата звернення: 13 серп. 2023. [Онлайн]. Доступно: https://zakon.rada.gov.ua/laws/show/n0039525-21#Text

• planning and direct implementation of measures to develop the communication system of the Armed Forces of Ukraine.

The Main Directorate of Radio-Electronic and Cyber Warfare of the General Staff of the Armed Forces of Ukraine (hereinafter – the Main Directorate) is designed to organise the implementation of tasks related to the planning of the cyber defence of Ukraine; the planning and conducting of radio-electronic warfare and cyber warfare; radio frequency spectrum management, and the development of relevant capabilities. The main tasks of the Main Department are the:

• planning, organising, preparation and conducting of cyber warfare in the interests of the strategic use of the Defence Forces of Ukraine and other components of the defence forces;

• planning and coordination of actions of cyber defence of Ukraine, state authorities, and components of the security and defence sector;

• planning, organisation of preparation and conduct of electronic warfare in the interests of strategic use of the Armed Forces of Ukraine and other components of the defence forces;

• implementation of the powers of the General Staff regarding management in the sphere of use of the radio frequency spectrum by special users by the Law of Ukraine "On Electronic Communications".

J-6 is also responsible for the organisation of cyber defence of the Armed Forces networks.

3.5 Engagement with the private sector

Public-private interaction in the field of cybersecurity is carried out by the Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine".

1. Public-private cooperation in the field of cybersecurity is carried out by:

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

2) increasing the digital literacy of citizens and the culture of safe behaviour in cyberspace, complex knowledge, skills and abilities necessary to support the goals of cybersecurity, the implementation of state and public projects to increase the level of public awareness of cyber threats and cyber protection;

3) exchange of information between state bodies, the private sector and citizens regarding cyber threats to critical infrastructure objects as well as other cyber threats, cyber attacks and cyber incidents;

4) partnerships and coordination 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 normative documents in the field of cybersecurity;

6) providing advisory and practical assistance in responding to cyber attacks;

7) formation of initiatives and the creation of authoritative consultation points for citizens, representatives of industry and business to ensure security on the Internet;

8) introduction of a mechanism for public control of the effectiveness of measures to ensure cybersecurity;

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

10) creation of a personnel training system and improvement of competence of specialists in various spheres of activity on cybersecurity issues;

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

2. Public-private interaction in the field of cybersecurity is applied, taking into account the specifics of the legal regime established by the law regarding certain objects and types of activities.

4. References

4.1 Policy

On the approval of the Strategy of digital transformation of the social sphere: Order. Kab. of the Ministers of Ukraine dated October 28, 2020 No. 1353-r <https://zakon.rada.gov.ua/laws/show/1353-2020-p#Text> accessed on 06.06.2024

On the approval of the Strategy for Implementation of Digital Development, digital transformations and digitalization of the state finance management system for the period until 2025 and approval of the plan of measures for its implementation: Order. Kab. of the Ministers of Ukraine dated November 17, 2021 No. 1467-r: as of April 11 2023 <https://zakon.rada.gov.ua/laws/show/1467-2021-p#Text> accessed on 06.06.2024.

On the decision of the National Security and Defence Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine dated August 26, 2021 No. 447/2021 <https://zakon.rada.gov.ua/laws/show/447/2021#Text> accessed on 06.06.2024.

4.2 Law

Issues of the Ministry of Digital Transformation: Resolution of the Kab. of the Ministers of Ukraine dated September 18, 2019 No. 856: as of January 13 2024 <https://zakon.rada.gov.ua/laws/show/856-2019-п#Text> accessed on 06.06.2024.

Issues of digital transformation: Order. Kab. of Ministers of Ukraine dated February 17, 2021 No. 365-r: as of May 4 2023 <https://zakon.rada.gov.ua/laws/show/365-2021-p#Text> accessed on 06.06.2024.

Issues of digital development: Resolution of the Kab. of the Ministers of Ukraine dated January 30, 2019 No. 56: as of June 30 2023 <https://zakon.rada.gov.ua/laws/show/56-2019-п#Text> accessed on 06.06.2024.

Issues of the activities of units on issues of digital development, digital transformations and digitalization of central and local executive bodies and deputy heads of central executive bodies, regional, Kyiv and Sevastopol city state administrations on issues of digital development, digital transformations and digitalization: Decree of the Cabinet of Ministers of Ukraine dated 03.03.2020 No. 194 <https://zakon.rada.gov.ua/laws/show/194-2020-п#Text> accessed on 06.06.2024.

Issue of the Unified State Web Portal of Electronic Services and the Unified State Portal of Administrative Services: Resolution of the Cabinet of Ministers of Ukraine dated 04.12.2019 No. 1137: as of April 2 2024 <https://zakon.rada.gov.ua/laws/show/1137-2019-п#Text> accessed on 06.06.2024.

On citizens' appeals: Law of Ukraine dated October 2, 1996 No. 393/96-VR: as of December 31 2023 <https://zakon.rada.gov.ua/laws/show/393/96-вр#Text> accessed on 06.06.2024.

On the approval of the Procedure for the formation and verification of e-passport and e-passport for traveling abroad, their electronic copies: Decree of the CMU dated August 18, 2021 No. 911: as of November 17 2022 <https://zakon.rada.gov.ua/laws/show/911-2021-п#Text> accessed on 06.06.2024.

On the implementation of an experimental project on the use of electronic display of information contained in the birth certificate and information about the registered place of residence, which is in the possession and at the disposal of the State Migration Service: Decree of the Kab. of the Ministers of Ukraine dated September 23, 2020 No. 911: as of March 14. 2022 <https://zakon.rada.gov.ua/laws/show/911-2020-п#Text> accessed on 06.06.2024.

On the accounting of internally displaced persons: Decree of the Cabinet of Ministers of Ukraine dated October 1, 2014 No. 509: as of November 24 2023 <https://zakon.rada.gov.ua/laws/show/509-2014-п#Text> accessed on 06.06.2024.
On the implementation of an experimental project regarding the use of electronic student (pupil) tickets: Decree of the Cabinet of Ministers. of the Ministers of Ukraine dated 18.12.2019 No. 1051: as of February 1 2022 <https://zakon.rada.gov.ua/laws/show/1051-2019-п#Text> accessed on 06.06.2024.
About the list, quantitative composition and subjects of the committees of the Verkhovna Rada of Ukraine of the ninth convocation: Resolution Verkhov. of the Council of Ukraine dated August 29, 2019 No. 19-IX: as of February 23 2023 <https://zakon.rada.gov.ua/laws/show/19-20#Text> accessed on 06.06.2024.
On the implementation of an experimental project regarding the functioning of the National Centre for Reservation of State Information Resources: Decree of the Cabinet of Ministers. of Ministers of Ukraine dated February 8, 2021 No. 94: as of April 11 2023 <https://zakon.rada.gov.ua/laws/show/94-2021-п#Text> accessed on 06.06.2024.
Issues of the functioning of the National Centre for Reservation of State Information Resources: Resolution of the Cabinet of Ministers. of Ministers of Ukraine dated 04/07/2023 No. 311 <https://zakon.rada.gov.ua/laws/show/311-2023-п#Text> accessed on 06.06.2024.
On the approval of the Procedure for the provision of services of the National Centre for Reservation of State Information Resources: Resolution of the Kab. of the Ministers of Ukraine dated May 3, 2022 No. 522: as of April 11 2023 <https://zakon.rada.gov.ua/laws/show/522-2022-п#Text> accessed on 06.06.2024.
Issues of the functioning of the National Telecommunication Network: Resolution of the Kab. of the Ministers of Ukraine dated 16.12.2020 No. 1358: as of August 20 2022 <https://zakon.rada.gov.ua/laws/show/1358-2020-п#Text> accessed on 06.06.2024.
On the approval of the list of services of the National Telecommunications Network: Order of the Admin. Govt. special services communication and of Information of Ukraine dated August 17, 2021 No. 502: as of April 12 2023 <https://zakon.rada.gov.ua/laws/show/z1288-21#Text> accessed on 06.06.2024.
On the approval of General requirements for cyber protection of critical infrastructure objects: Resolution of the Cabinet. of the Ministers of Ukraine dated June 19, 2019 No. 518: as of September 7. 2022 <https://zakon.rada.gov.ua/laws/show/518-2019-п#Text> > accessed on 06.06.2024.
On the protection of information in information and telecommunication systems: Law of Ukraine dated 07/05/1994 No. 80/94-VR: as of April 4 2024 <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text> accessed on 06.06.2024.
On the approval of the rules for ensuring the protection of information in information, telecommunication and information-telecommunication systems: Resolution of the Kab. of the Ministers of Ukraine dated March 29, 2006 No. 373: as of October 21 2022 <https://zakon.rada.gov.ua/laws/show/373-2006-п#Text> accessed on 06.06.2024.
On the protection of personal data: Law of Ukraine dated June 1, 2010 No. 2297-VI: as of April 27 2024 <https://zakon.rada.gov.ua/laws/show/2297-17#Text> accessed on 06.06.2024.
On electronic trust services: Law of Ukraine dated October 5, 2017 No. 2155-VIII: as of January 1 2024 <https://zakon.rada.gov.ua/laws/show/2155-19#Text> accessed on 06.06.2024.
On the approval of the procedure for the interaction of executive authorities on the protection of state information resources in information and telecommunication systems: Resolution of the Kab. of Ministers of Ukraine dated November 16, 2002 No. 1772: as of September 7. 2022 <https://zakon.rada.gov.ua/laws/show/1772-2002-п#Text> accessed on 06.06.2024.
On the approval of the Regulation on the register of information, telecommunications and information and telecommunications systems of executive authorities, as well as enterprises, institutions and organizations belonging to the sphere of their management: Resolution of the Kab. of the Ministers of Ukraine dated August

3, 2005 No. 688: as of September 7. 2022 <https://zakon.rada.gov.ua/laws/show/688-2005-п#Text> accessed on 06.06.2024.
On the approval of the list of mandatory stages of work during the design, implementation and operation of informatization facilities: Decree of the Cabinet of Ministers of Ukraine dated February 4, 1998 No. 121: as of September 3. 2011 <https://zakon.rada.gov.ua/laws/show/121-98-п#Text> accessed on 06.06.2024.
On the national security of Ukraine: Law of Ukraine dated June 21, 2018 No. 2469-VIII: as of March 31. 2023 <https://zakon.rada.gov.ua/laws/show/2469-19#Text> accessed on 06.06.2024.
On threats to cybersecurity of the state and urgent measures to neutralize them: Decision of the National Council. of Security and Defence of Ukraine dated December 29, 2016: as of February 16 2017 <https://zakon.rada.gov.ua/laws/show/n0015525-16#Text> accessed on 06.06.2024.
On the implementation of an experimental project on the introduction of a set of organizational and technical measures to identify vulnerabilities and deficiencies in the configuration of information, telecommunication and information and telecommunication systems in which state information resources are processed: Resolution of the Cabinet of Ministers. of the Ministers of Ukraine dated 12/23/2020 No. 1363: as of September 7. 2022 <https://zakon.rada.gov.ua/laws/show/1363-2020-п#Text> accessed on 06.06.2024.
Issues of ensuring the functioning of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks: Resolution of the Kab. of the Ministers of Ukraine dated December 23, 2020 No. 1295: as of September 7. 2022 <https://zakon.rada.gov.ua/laws/show/1295-2020-п#Text> accessed on 06.06.2024.
On the approval of the procedure for searching and identifying potential vulnerabilities of information (automated), electronic communication, information and communication systems, electronic communication networks: Decree of the Kab. of the Ministers of Ukraine dated May 16, 2023 No. 497 <https://zakon.rada.gov.ua/laws/show/497-2023-п#Text> accessed on 06.06.2024.
On the approval of the procedure for assessing the state of security of state information resources in information, telecommunication and information-telecommunication systems: Order of the Admin. Govt. special services communication and of Information of Ukraine dated 02.12.2014 No. 660: as of January 10 2023 <https://zakon.rada.gov.ua/laws/show/z0090-15#Text> accessed on 06.06.2024.
On the approval of the procedure for scanning for vulnerabilities of state information resources posted on the Internet: Order of the Admin. Govt. special services communication and of Information of Ukraine dated January 15, 2016 No. 20: as of January 10 2023 <https://zakon.rada.gov.ua/laws/show/z0196-16#Text> accessed on 06.06.2024.
On the approval of the procedure for conducting a review of the state of cyber protection of critical information infrastructure, state information resources and information, the requirement for the protection of which is established by law: Resolution of the Cabinet of Ministers of Ukraine dated 11.11.2020 No. 1176 <https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text> accessed on 06.06.2024.
On the approval of the procedure for the transfer of equipment sets of the telemetry collection subsystem of information and communication systems (active sensors), the system of detecting vulnerabilities and responding to cyber incidents and cyber attacks to cyber protection objects: Order of Admin. State Service of Special Communication and Information Protection of Ukraine dated June 24, 2022 No. 284 <https://zakon.rada.gov.ua/laws/show/z0758-22#Text> accessed on 06.06.2024.
On the decision of the National Security and Defence Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine dated August 26, 2021 No. 447/2021 <https://zakon.rada.gov.ua/laws/show/447/2021#Text> accessed on 06.06.2024.
On the approval of the Regulation on the organizational and technical model of cyber protection: Resolution of the Kab. of Ministers of Ukraine dated 12/29/2021 No. 1426 <https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text> accessed on 06.06.2024.

On the decision of the National Security and Defence Council of Ukraine dated December 30, 2021 "On the Implementation Plan of the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine dated February 1, 2022 No. 37/2022 <https://zakon.rada.gov.ua/laws/show/37/2022#Text> accessed on 06.06.2024.
About information: Law of Ukraine dated October 2, 1992 No. 2657-XII: as of July 27 2023 <https://zakon.rada.gov.ua/laws/show/2657-12#Text> accessed on 06.06.2024.

On state secrets: Law of Ukraine dated January 21, 1994 No. 3855-XII: as of January 1 2024 <https://zakon.rada.gov.ua/laws/show/3855-12#Text> accessed on 06.06.2024.
On the approval of the Regulation on the system of protected access of state bodies to the Internet: Order of the Admin. State Service of Special Communication and Information Protection of Ukraine dated August 30, 2023 No. 771 <https://zakon.rada.gov.ua/laws/show/z1624-23#Text> accessed on 06.06.2024.
On the approval of the Procedure for the use of computer programs in executive authorities: Resolution of the Kab. of Ministers of Ukraine dated September 10, 2003 No. 1433: as of April 12 2024 <https://zakon.rada.gov.ua/laws/show/1433-2003-n#Text> accessed on 06.06.2024.
On the approval of methodological recommendations for increasing the level of cyber protection of electronic document management systems: Order of Admin. SSSCIP of Ukraine dated August 30, 2023 No. 773 <https://zakon.rada.gov.ua/rada/show/v0773519-23#Text> accessed on 06.06.2024.

On the State Service for Special Communications and Information Protection of Ukraine: Law of Ukraine dated 23.02.2006 No. 3475-IV: as of December 31 2023<https://zakon.rada.gov.ua/laws/show/3475-15#Text> accessed on 06.06.2024.
About the National Cyber Security Coordination Center: Decree of the President of Ukraine dated 07.06.2016 No. 242/2016: as of July 17 2021 <https://zakon.rada.gov.ua/laws/show/242/2016#Text> accessed on 06.06.2024.
Order of the SSSCIP Administration No. 570 On the approval of Methodological recommendations on the response of cyber security entities to various types of events in cyberspace <https://zakon.rada.gov.ua/rada/show/v0570519-23#Text> accessed on 06.06.2024.

Some issues of response by cyber security entities to various types of events in cyberspace: Resolution of the Cabinet of Ministers. of Ministers of Ukraine dated 04.04.2023 No. 299 <https://zakon.rada.gov.ua/laws/show/299-2023-n#Text> accessed on 06.06.2024.

4.3 Other

"The Results of the Assessment of the Existing Population of Ukraine Have Been Published" (*www.kmu.gov.ua*) <www.kmu.gov.ua/news/oprilyudneno-rezultati-ocinki-chiselnosti-nayavnogo-naselennya-ukrayini> Date accessed 5 Aug 2024.
The Number of Internet Subscribers by Region as of January 1, 2020" (ukrstat.gov.ua) <https://ukrstat.gov.ua/operativ/operativ2019/zv/zv_reg/kal_reg/kal_reg0419_u.htm> accessed on 06.08.2023.
"National Atlas of Ukraine" (World Data Centre | WORLD DATA CENTRE) <http://wdc.org.ua/atlas/1060000.html> accessed on 06.08.2023.
"GDP Per Capita (Current US$) - Ukraine" (*data.worldbank.org*).<https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=UA> accessed on 06.08.2023.
"NCSI :: Ukraine" (*Index*) <https://ncsi.ega.ee/country/ua/210/> accessed on 06.06.2024.

"ITU | 2017 Global ICT Development Index" (*ITU: Committed to connecting the world*). <www.itu.int/net4/ITU-D/idi/2017/index.html> accessed on 06.06.2024.
"National Cyber Power Index 2022" (*Belfer Centre for Science and International Affairs*) <www.belfercentre.org/publication/national-cyber-power-index-2022> accessed on 06.06.2024.
"Ukraine – Network Readiness Index" (*Network Readiness Index – Benchmarking the Future of the Network Economy*) <https://networkreadinessindex.org/country/ukraine/> accessed on 06.06.2024.
"The 2023 NTI Nuclear Security Index" (*The Nuclear Threat Initiative*) <www.nti.org/analysis/articles/the-2023-nti-nuclear-security-index/> accessed on 06.06.2024.
About Us Ministry of Digital Transformation of Ukraine" (*Ministry of Digital Transformation of Ukraine*) <https://thedigital.gov.ua/ministry> accessed on 06.06.2024.
"Unified state web portal of electronic services DIIA | State Enterprise "DIIA" (State Enterprise "DIIA") <https://se.diia.gov.ua/unified-state-web-portal-of-electronic-services-diia> accessed on 06.06.2024.
"CERT-UA" (*cert.gov.ua*) <https://cert.gov.ua/about-us> accessed on 06.06.2024.
"National project Diia.business" (Diia.business - Main page) <https://business.diia.gov.ua/about-project> accessed on 06.06.2024.
Report on the review of the state of cyber protection of critical information infrastructure, state information resources and information, the requirement for the protection of which is established by law (SSSCIP 2023).
Informational and analytical materials on the state of protection of state electronic information resources in ICS (SSSCIP 2023).
Analytical report on the implementation of the cyber security strategy plan of Ukraine for the first half of 2023 (SSSCIP 2023).
Report on the implementation by the State Service of Special Communications and Information Protection of Ukraine of tasks related to ensuring the cyber security of the state in 2022 (SSSCIP 2023).
Analytical report of the SSSCIP based on the results of the threat research (SSSCIP 2023) <https://cip.gov.ua/services/cm/api/attachment/download?id=60201>.
Report on the System of Vulnerability Detection and Response to Cyber Incidents and Cyber Attacks <https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf>.
Report on the submission and further evaluation of the annual report on the results of an independent audit of the activities of the main subjects of national cyber security (Committee on Digital Transformation) <www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_01.pdf>.
Preliminary report on monitoring the implementation of the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity in Ukraine" (Committee on Digital Transformation) <www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_02.pdf>.
Cyber Security Management Best Practices (Committee on Digital Transformation) <www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf>.
"National Cybersecurity Centre" (*National Cybersecurity Centre*) <www.ncscc.gov.ua/> accessed on 06.06.2024.
"Scientific and practical commentary on the provision on the organizational and technical model of cyber protection, approved by the resolution of the Cabinet of Ministers of Ukraine dated 12.29.2021 No. 1426" (*https://cip.gov.ua*, 11 Feb. 2022) <https://cip.gov.ua/ua/news/naukovo-praktichnii-komentar-do-polozhennya-pro-organizaciino-tekhnichnu-model-kiberzakhistu-zatverdzhenogo-postanovoyu-kabinetu-ministriv-ukrayini-vid-29-grudnya-2021-r-1426> accessed on 06.06.2024.
"National Security and Defence Council of Ukraine" (National Security and Defence Council of Ukraine) <www.rnbo.gov.ua/ua/Diialnist/5765.html> accessed on 06.06.2024
"Trusted Introducer: Directory: CERT-UA" (*Trusted Introducer: Home*) <www.trusted-introducer.org/directory/teams/cert-ua.html> accessed on 06.06.2024.

"E-Government Development Index" <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine> accessed on 06.08.2023.
National Security and Defense Council of Ukraine" (National Security and Defense Council of Ukraine)<www.rnbo.gov.ua/ua/Diialnist/5011.html> accessed on 06.06.2024.

5. ABBREVIATIONS

CCDCOE	Cooperative Cyber Defence Centre of Excellence
CDTO	Chief Digital Transformation Officer
CERT-UA	The Computer Emergency Response Team of Ukraine
CMU	Cabinet of Ministers of Ukraine
CSIRT	Computer Security Incident Response Team
EU	European Union
GDP	Gross Domestic Product
IAS	Information and Analytical System
ICS	Information and Communication Systems
ICT	Information and Communication Technology
IT	Information Technology
ITU	International Telecommunication Union
MODT	Ministry of Digital Transformation of Ukraine
NATO	North Atlantic Treaty Organisation
NCSCC	The National Cyber Security Coordination Centre
NCSI	National Cyber Security Index
NSDC	The National Security and Defence Council of Ukraine
NTI	Nuclear Threat Initiative
NTN	National Telecommunication Network
OTM	The Organisational and Technical Model of Cyber Protection
SMS	Short Message Service
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
SSU	Security Service of Ukraine
TIN	Tax Identification Number
TLP	Traffic Light Protocol
US	United States