Organizational and Technical Model of National Cybersecurity and Cyber Protection

Roman Boyarchuk[a], Mykola Khudyntsev[a], Oleksiy Lebid[b], and Oleksandr Trofymchuk[b]

[a] *International Cybersecurity University, 171 Deputatska str., Kyiv, 03115, Ukraine*
[b] *Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, 13, Chokolivskyi ave., Kyiv, 03186, Ukraine*

Abstract

The work is devoted to topical issues of building an Organizational and Technical Model of Cybersecurity and Cyber Protection (OTM) and the National Cybersecurity System of Ukraine (NCS). For the first time, definitions of OTM are proposed in the paper. The role and place of OTM in the NCS and the Cybersecurity Ecosystem of Ukraine are studied, the composition and functions of the components of the OTM are analyzed, the ways of improvement of OTM and the NCS as a whole are offered.

Keywords

Cybersecurity, cyber protection, cybersecurity ecosystem of Ukraine, National Cybersecurity System of Ukraine, organizational and technical model.

1. Introduction

The Law of Ukraine "About the basic principles of ensuring the cybersecurity of Ukraine" [1] defined tasks for the main stakeholders to ensure cybersecurity, in particular, the State Service of Special Communications and Information Protection of Ukraine is tasked with implementing Organizational and Technical Cyber Protection Model (OTM CP) to ensure the functioning of the National Cybersecurity System (NCS). The implementation of the Organizational and Technical Cybersecurity Model (OTM CS) is carried out by the State Cyber Defense Center (SCDC), which ensures the creation and functioning of the main components of the system of secure access of state entities to the Internet, provides a system of antivirus protection of national information resources, inspection (audit) of information security and the status of cyber protection of the components of the critical informational infrastructure, vulnerability detection and response to cyber incidents and cyberattacks on cybersecurity facilities, system of interactions of computer emergencies response teams moreover it develops in cooperation with other entities providing cybersecurity scenarios to respond to cyber threats, measures to counter such threats, programs, and methods of cyber training.

Ensuring the functioning and development of the NCS is the most important task for the State in the field of cybersecurity [2–5]. Recently, the State Service of Special Communications and Information Protection of Ukraine presented the Concept of OTM CP and invited the entire community of experts to join the discussion concerning the elements of this model [11]. Despite the frequent use of the terms OTM CS and CP, they are not defined under the normative regulation. In English-language sources, close terms such as "cybersecurity framework" and "cybersecurity ecosystem" are used (see, for example, [6–8]).

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine
EMAIL: roman.boyarchuk@icu-ng.org (A.1); mykola.khudyntsev@icu-ng.org (A.2); o.g.lebid@gmail.com (B.3); itgis@nas.gov.ua (B.4)
ORCID: 0000-0003-4862-9724 (A.1); 0000-0002-9324-6901 (A.2); 0000-0002-4003-8068 (B.3); 0000-0003-3358-6274 (B.4)


The paper proposes the author's definitions and content of terms "Organizational and Technical Model" and "ecosystem" for cybersecurity and cyber protection systems (including NCS), analyzes the composition and functions of the components of OTM CS and CP, Cybersecurity Ecosystem of Ukraine (CEU), proposed ways of development and improvement of OTM CS and CP, as well as NCS in general.

2. Organizational and Technical Model and Ecosystem of Cybersecurity and Cyber Protection

In [8] the definition of the digital ecosystem is given: a digital ecosystem is an ICT-enabling infrastructure for economies, based on fluid, amorphous, and often transitory structures, alliances, partnerships, and collaborations among small and middle enterprises, that supports cooperation, knowledge sharing and the building of a community that shares business, knowledge, and infrastructure.

Cybersecurity Framework by the definition of the National Institute of Standards (USA) denotes [6]: a complex description of current status and target state, identification and prioritization of the opportunities for improvement in the context of an ongoing and recurring process, assessment of progress to the target state, communication between internal and external stakeholders on risks.

The terms OTM CS and CP are mentioned in [1], but any of the three terms haven't the legal (normative) definition in Ukraine.

We will call the OTM superposition (block diagram) of allied forces (resources), activities and facilities, and related people, data and processes with defined political, regulatory (contain rules of law adopted by the competent public authorities in the prescribed manner), technical regulatory (the same applies to technical regulations), informational, organizational, technical and technological, financial and economic, scientific-educational, social and household components (projections) of the superposition.

The OTM elements (forces, measures, means and people, data, processes) partially intersect. For the OTM CS or OTM CP, the affinity of elements means their relation to the sphere of cybersecurity or cyber protection, respectively. The affinity of elements can also be defined for national or personal security or NCS and other ones. The use of the term "superposition" emphasizes the non-additive nature of these elements and components, but in practice, the OTM is also understood as a list set or a set of tracks of elements without taking into account the impact of each element on the other. The time projection of the OTM characterizes the state of the OTM at a certain point in time.

The completeness of the description and the level of detail of the elements or components of any OTM are determined as needed. For example, the legislative definition of NCS contains only subjects (forces) and measures (National Cybersecurity System is a set of subjects of cybersecurity and interconnected measures of political, scientific and technical, informational, educational nature, organizational, legal, operational and investigative, intelligence, counterintelligence, defense, engineering, and technical measures, as well as cryptographic and of technical protection of national information resources, cyber protection of critical information infrastructure objects [1]), therefore the OTM of the NCS in case of normative use should contain only these two elements. Thus, the OTM of the NCS is a subsystem of the OTM of CS in terms of forces and measures, and the OTM of CS contains (except forces and measures) also means (assets, objects, data) whose owners (administrators) are cybersecurity subjects (entities, stakeholders). Cybersecurity tools (means) constitute the material basis of the cyber protection of any asset, i.e., are cyber protection tools (means) at the same time. Therefore, the OTM of CP is a subsystem of the OTM of CS in terms of means. The analysis shows that the OTM of CS is a complete structural scheme of cybersecurity, which consists of the OTM of the NCS (forces and

measures) and the OTM of CP (means). It should be noted that we propose to consider cyber protection means as a basic element of the OTM of CP, despite the normative definition of the term "cyber protection" as a set of measures (cyber protection, more correctly in the case—cyber defense, a set of organizational, legal, engineering and technical measures, as well as measures of cryptographic and technical protection of information aimed at preventing cyber incidents, detection, and protection against cyberattacks, elimination of their consequences, restoration and reliability of communication and technological systems [1]). In practice, OTM CP often is considered only as detailing (decomposition) of OTM CS technical and technological components (projection) yet. However, it is obvious that within the proposed approach the description of all OTM elements and components should be balanced depending on the conditions of consideration.

Table 1 contains information about the elements and components of the above organizational and technical models.

Table 1
Matrix of the elements and components (projections) of the OTM

OTM (Type)	Security Types	Forces/Means/ Measures	People/Data/ Processes	Main Components (Projections)
Personal security	Ecological, collective, personal, psychological, physical, civil	Forces	People	Social
National security	All basic types of security	Forces, means, measures	People, data, processes	Political, financial, and economic
Information security	Information	Means, measures	Data, processes	Informational, scientific-educational, normative-legal, organizational
Cybersecurity	Military-technical, computer, corporate, information, network	Forces, means, measures	People, data, processes	Informational, scientific-educational, normative-legal, organizational
Cyber Protection	Computer, corporate, information, network	Means	Data, processes	Informational, normative-technical, technical-technological, organizational
National Cybersecurity System	Military-technical, corporate, information	Forces, measures	People, processes	Informational, organizational

The level of detail of the elements and components of the OTM of CS and CP is determined primarily by the state of maturity of the processes in cybersecurity systems and the NCS as a whole [9, 10].

For a detailed schematic representation of the elements and components (projections) of the OTM, it would be appropriate to use the term "ecosystem." We propose to call an ecosystem a set (composition, linear scheme) of related forces (resources) or means separately without detailing the properties of elements or components of such set, and connections between them.

The time projection of an ecosystem characterizes the state of a set of forces (resources) or means at a certain point in time. The ecosystem differs from the OTM in the absence of measures, as well as the lack or low level of detail of forces (resources) and means.

The Cybersecurity Ecosystem of Ukraine in terms of forces (subjects) is a linear structural scheme of forces (subjects) of the NCS. The Cybersecurity Ecosystem in terms of means is a linear structural scheme of cyber protection (or Cyber Protection Ecosystem) of the country.

3. Cybersecurity Ecosystem of Ukraine

A set (composition, linear scheme) of forces (resources) or means of national cybersecurity is called the Cybersecurity Ecosystem of Ukraine (CEU). The elements and components of the CEU in a general case coincide with the elements and components of the OTM of CS. For the ecosystem, it is proposed to take into account an additional category of components (compared to the OTM of CS), namely the category: objects, subjects, connections.

In the CEU matrix elements proposed below, a list of items is described and elements are combined in groups for convenience.

The difference between CEU and NCS is, firstly, in the degree of detail of elements and components, secondly, in the inclusion of cybersecurity means in the CEU, and, thirdly, in the lack of cybersecurity measures in the CEU (compared to the NCS).

The study of the state of regulatory and legal support for the functioning of the NCS was made in [2-5], but from our point of view, it needs significant updating. The study of the state of regulatory and technical support for the functioning of individual elements of the CEU has not yet been studied by the authors, primarily due to the lack of relevant information in open sources.

The general list of groups of the elements of the CEU contains the next items:

- System of strategic planning and coordination.
- Cybersecurity Stakeholders.
- Main Cybersecurity Actors.
- Basic Cybersecurity Actors.
- Technological Core (Central Segment).
- Means of the State Center of Cyber Defense.
- Means of other divisions of the State Service of Special Communication and Information Protection.
- Means of other Cybersecurity Actors.
- Computer Emergency / Computer Security Incidents Response Teams.
- Local Segment (branched subsystems of the Technological Core (Central Segment)).
- Local Segment (Cybersecurity Actor's SOCs, ISMSs, CPSs).
- State Information Resources (SIR) on the Internet.
- Vital Services (VS) and Information Resources (IR) on the Internet.
- Other IR on the Internet.
- Air Gap SIR.

- Other Air Gap IR.
- Critical Infrastructure (CI).
- Critical Information Infrastructure (CII).
- System of Monitoring, Control, Management, Operational and Technical Interaction, Information and Analytical Support.
- System of Cyber Threats Indicators, Cybersecurity and Cyber Protection State of SIR and CII.
- Regulatory Framework.
- Regulatory and Technical Base.
- System of Standardization.
- System of Certification (Conformity Assessment).
- System of Accreditation.
- System of Threat Modeling, Risk Assessment, Technical-Technological and Financial-Economic Control, Examination and Expertise.
- System of Education, Training, Retraining, and Knowledge Exchange.
- System of Scientific and Scientific-Technical Research and Development.
- Material and Technical Base (non-Specialized Assets).
- Social Base.

A detailed description of the elements and their groups is beyond the scope of this study. The preparation of such a report may be a preparatory measure in conducting a review of the state of cyber protection of critical information infrastructure, public information resources, and information, the requirement for protection of which is established by law (see https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text).

Belonging an element (a group of elements) to the category "measures" means the need to take into account the measures stipulated by other categories for this element (a group of elements). It is proposed to study the composition of individual groups of elements of the CEU elements in further research (for example, the group of computer emergencies response teams as of 01.12.2020 includes the Government team CERT-UA, the NBU team CSIRT-NBU and with some reservations—the SBU, SSU, the team of the Department of Counterintelligence Protection of the State in the field of information security, teams of State University of Telecommunications, ISZZI Igor Sikorsky's KPI and Crytek Ukraine, https://www.first.org/members/liaisons/, all teams except the second are FIRST members).

The list of groups elements of the CEU includes groups whose elements exist as of 01.12.2020, as well as groups whose elements need to be created at the 2nd and 3rd stages of the OTM implementation.

New groups of elements of the CEU elements have been introduced: cybersecurity actors (top, President of Ukraine, National Security and Defense Council of Ukraine, National Coordination Center for Cyber Security of the National Security and Defense Council of Ukraine, Cabinet of Ministers of Ukraine), cybersecurity actors (main, the same as the main actors in the NCS: State Service for Special Communications and Information Protection of Ukraine, National Police of Ukraine, Security Service of Ukraine, Ministry of Defense of Ukraine and General Staff of the Armed Forces of Ukraine, intelligence agencies, National Bank of Ukraine), cybersecurity actors (other subjects, entities, of cybersecurity in addition to the top and main subjects of cybersecurity).

4. OTM: Status and Implementation Plans

The stages of the implementation of the OTM have to be determined by normative and administrative documents of the National Security and Defense Council, the Office of the National Security and Defense Council of Ukraine, the National Coordination Cyber Security

Center, the State Service of Special Communications and Information Protection of Ukraine and the State Center for Cyber Defense. Some positions on the status and implementation plan of the OTM are offered below.

The 1st stage of implementation of the OTM during 2017–2019 consisted in creating the material and technical base of the central segment (technological core) of NCS (development of forces and means/processes).

The 2nd stage of implementation of the OTM during 2019–2021 should aim to improve and develop the material and technical base of the central segment (technological core) and local segments (sources or subsystems of telemetry information collection, including sectoral or industrial cyber threats response centers and SOCs) NCS (development of forces and means/processes and data).

The 3rd stage of implementation of the OTM, starting from 2020, should consist in the creation and development of a personnel base of the NCS (development of forces and means/people) in the directions of preparation and advanced training of users of computer systems and networks, experts of information security, cybersecurity, and cyber protection, effective improvement of the system of motivation, stimulation and encouragement of staff, the introduction of new (not involved in the previous stages) technologies and solutions (Video Streams, Social Networks, Expert Systems, Big Data, Industrial Control Systems, IoT, Machine Learning, Artificial Intelligence) to improve the quality of cybersecurity and cybersecurity services, as well as increase the capacity of sources of telemetry information about cyber threats, compromise indicators, and cyber incidents.

The 1st stage of implementation of the OTM ended with the deployment of the central segment (technological core) of the NCS, the operation of which is provided by the State Center for Cyber Defense [11–13]. A detailed analysis of the results of the1st stage of implementation of the OTM will be a subject of further research.

For each stage of the implementation of the OTM, measures are envisaged that belong to all the components (projections) of the OTM. Following the normatively defined tasks, the cybersecurity actors should provide details of all these components.

Parameters and indicators of the stage's implementation of the OTM should be taken into account in the following editions of the Cyber Security Strategy of Ukraine and the Doctrine of Information Security of Ukraine.

4.1. The Main Tasks of the 1st Stage of Implementation of the OTM

The elements of the CEU, which were created or are created separately from the plans for the implementation of the central segment (technological core) of the NCS and OTM include:

- Information systems of the National Coordination Cyber Security Center of the National Security and Defense Council of Ukraine (see https://www.president.gov.ua/documents/9232019-31465).
- National Telecommunication Network (NTN) [1].
- National Center for Operational and Technical Management of Telecommunications Networks (NCTN, see https://www.kmu.gov.ua/npas/pro-utvorennya-nacionalnogo-centru-operativno-tehnichnogo-upravlinnya-merezhami-telekomunikacij).
- Situation cybersecurity center of the Security Service of Ukraine (see https://ssu.gov.ua/ua/pages/330).
- The platform for the exchange of compromise indicators between critical infrastructure facilities and public authorities of the Security Service of Ukraine (see https://misp.dis.gov.ua/users/login).
- The web page of recommendations of the Cyber Police Department of the National Police of Ukraine on combating cybercrime (see https://cyberpolice.gov.ua/articles/).

- Cyber defense center of the National Bank of Ukraine (see https://www.rbc.ua/ukr/news/nbu-sozdast-tsentr-kiberzashchity-bankov-1499335025.html).
- Cyber incident response team in the banking system (CSIRT-NBU, see https://bank.gov.ua/ua/news/all/natsionalniy-bank-ta-derjavniy-tsentr-kiberzahistu-spivpratsyuvatimut-u-sferi-kiberbezpeki).
- Secure Internet Access Nodes (SIAN) of the telecommunication operators (providers, see https://cip.gov.ua/ua/news/zakhisheni-vuzli-dostupu-do-merezhi-internet).
- Global Center for Interaction in Cyberspace of the National Joint-Stock Company Naftogaz (see https://www.naftogaz.com/www/3/nakweb.nsf/0/0BEDE357B60EBACBC22585EE003A329E?OpenDocument&Highlight=0,%D0%93%D0%BB%D0%BE%D0%B1%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D1%86%D0%B5%D0%BD%D1%82%D1%80).
- I-Cyber branch cyber defense center of the State enterprise "Branch Center of Digitalization and Cybersecurity" of the Ministry of Infrastructure of Ukraine (see https://icdc.gov.ua/).
- Center for Research of Information Asset Protection Technologies (educational cyber range) of Borys Grinchenko Kyiv University (see https://kubg.edu.ua/prouniversitet/news/podiji/5698-vprovadzhennia-innovatsiinykh-tekhnolohii-kiberbezpeky-v-universyteti.html).
- Cyber range of the State University of Telecommunications (see http://www.dut.edu.ua/ru/news-1-574-8195-naraschivanie-moschnostey-kiberpoligona--vnedrenie-v-uchebnyy-process-luchshih-resheniy-kiberbezopasnosti_kafedra-informacionnoy-i-kiberneticheskoy-bezopasnosti).
- Cyber range of the Zhytomyr Military Sergiy Korolyov Institute (see https://www.zvir.zt.ua/1029-ofitsijne-vidkrittya-unikalnogo-kiberpoligonu-u-zhitomirskomu-vijskovomu-instituti).
- Information and telecommunication systems of the responsible units of other subjects of cybersecurity (information security, cybersecurity, information protection, and cybersecurity).

The main tasks of the 1st stage of implementation of the OTM include the creation or modernization and deployment of elements of the central segment (technological core) of the NCS and OTM:

- The State Service of Special Communications and Information Protection Cyber Threat Response Center (CRC, see https://www.rnbo.gov.ua/ua/Diialnist/2978.html?PRINT).
- Cyber protection systems of state information resources and critical infrastructure facilities (see https://cip.gov.ua/ua/news/operativna-informaciya-derzhspeczv-yazku-shodo-zakhistu-derzhavnikh-informaciinikh-resursiv-za-period-z-16-po-22-grudnya-2020-roku).
- Public resources of the government's CERT-UA computer emergency response team (see https://cert.gov.ua/).
- State Register of Cyber Incidents (Unified Interactive Database on Cyber Incidents) (SR UID CI, see https://cip.gov.ua/ua/news/golova-derzhspeczv-yazku-valentin-petrov-dopoviv-pro-pidsumki-roboti-sluzhbi-za-2019-rik-ta-vikonannya-pokladenikh-na-neyi-zavdan).
- Internet Access Single Point for state bodies (IASP, see https://cip.gov.ua/ua/news/zakhisheni-vuzli-dostupu-do-merezhi-internet).
- Secure Internet Access System for state bodies (SIAS, see https://zakon.rada.gov.ua/laws/show/481-2018-%D1%80#Text).

- Single main and backup protected data centers for information storage of state electronic information resources (SPDC, see https://zakon.rada.gov.ua/laws/show/n0015525-16#Text).
- Secure data center (data processing center) for the needs of government agencies, security and defense sector, financial, energy, transport sectors (see https://zakon.rada.gov.ua/laws/show/481-2018-%D1%80#Text).
- Center for Anti-Virus Information Protection (CAIP, see http://cazi.gov.ua/).
- State Software and Updates Repository (SSUR, see https://zakon.rada.gov.ua/laws/show/455-2019-%D1%80#Text).
- Malware laboratory (MW-Lab, see https://prozorro.gov.ua/tender/UA-2019-08-16-001174-a).
- The State Service of Special Communications and Information Protection cyber range and test site for modeling cyber threats and conducting cyber exercises (see https://mbr.com.ua/uk/news/technology/628-derzhspeczvyazok).

4.2.The Main Tasks of the 2nd Stage of Implementation of the OTM

The main tasks of the 2nd stage of implementation of the OTM include:

- Commissioning in full and ensuring the functioning of the elements (means) of the central segment (technological core) of the NCS and OTM.
- Ensuring the development and modernization of elements (means) of the NCS and OTM.
- Regulatory, and organizational, and technical support for the interaction of the main subjects of cybersecurity, cybersecurity entities, and owners (managers) of critical and critical information infrastructure.
- Practical implementation of automated processes of information exchange on cyber threats and cyber incidents with cybersecurity entities and response to cyber threats, cyberattacks, and cyber incidents.
- Optimization of configurations of technological and technical solutions and focus on organizational and technical solutions of national production.
- Creation and functioning of the system of detection of vulnerabilities and response to cyber incidents and cyberattacks on cyber defense objects by ensuring the functioning, development, and modernization of elements of the central segment (technological core) of the NCS and OTM.
- Creation and operation of the anti-virus protection system of national information resources through modernization, integration, operation, and development of the Center for Anti-Virus Information Protection, malware laboratory of the State Center for Cyber Defense, creation and implementation of the State Software and Updates Repository.
- Ensuring the audit of information security and the state of cyber protection of critical information infrastructure by creating an information security audit system (mandatory and voluntary) for cybersecurity entities and critical information infrastructure.
- Creation and functioning of the system of interaction of computer emergency response teams by ensuring the functioning and development of the Government Computer Emergency Response Team CERT-UA, situational centers, cyber threat centers, operational security centers, cybersecurity, and cyber defense centers, services response to cyber incidents of cybersecurity entities and critical and critical information infrastructure facilities, as well as implementation and improvement of the Protocol of joint actions of major cybersecurity entities, cyber protection entities and owners (managers) of critical information infrastructure facilities during prevention, detection, cessation of cyberattacks and cyber incidents, as well as in the elimination of their

consequences, bilateral protocols of actions of cybersecurity entities and cybersecurity actors.

- Development of scenarios for responding to cyber threats, measures to combat such threats, programs, and methods of cyber training by ensuring the functioning of the cyber range for modeling cyber threats and conducting cyber exercises of the State Service of Special Communications and Information Protection and implementation on its basis qualifications) of specialists in relevant fields of activity, conducting cyber competitions and cyber exercises.

4.3. The Main Tasks of the 3rd Stage of Implementation of the OTM

The main tasks of the 3rd stage of implementation of the OTM include:

- Control over the implementation of the tasks of the 1st and 2nd stages.
- Continuing to optimize the configurations of technological and technical solutions and focus on organizational and technical solutions of domestic production.
- Training and advanced training of users of computer systems and networks, specialists in the field of information security, cybersecurity, and cyber protection of basic and expert levels.
- Creation and implementation of a system for the dissemination of basic, common and specialized knowledge on information security, cybersecurity, and cyber protection within the existing system of educational, secondary, higher, and vocational education.
- Priority development of human resources and the system of training, motivation, stimulation, and encouragement of personnel.
- Development of interaction between the subjects (entities) of information security and cybersecurity.
- Creation and implementation of a system of monitoring, control, management, operational and technical interaction, and information and analytical support.
- Optimization of cyber threat indicator systems, cybersecurity status, SIR, and CII cyber protection status.
- Updating and maintaining the regulatory framework in an adequate state of potential challenges.
- Creation of a workable system of standardization, certification (conformity assessment), and accreditation.
- Creation and implementation of a system of threat modeling, risk assessment, technical-technological, and financial-economic control and expertise, automated exchange of knowledge and experience.
- Organization of scientific and scientific-technical research and development of the latest technologies and solutions in the field of information technology and security and cybersecurity.
- Introduction of a system of strategic planning and coordination.

5. Conclusions

The paper proposes definitions of some terms for cybersecurity and cyber protection systems in Ukraine that can be used in general. The composition and list of elements, components (projections), and other categories of the organizational and technical model of cybersecurity and cyber protection and cybersecurity ecosystem of Ukraine are also offered. An analysis of the state of the cybersecurity ecosystem of Ukraine, a possible plan for the implementation of the organizational and technical model for future periods, and areas of future research are also given.

6. Acknowledgments

The authors are grateful for the support of research and consultation in the field of cybersecurity with colleagues from the Office of the National Security and Defense Council of Ukraine, the State Service of Special Communications and Information Protection, National Institute for Strategic Studies, and the Institute of Telecommunications and Global Information Space.

7. References

[1] Law of Ukraine on Basics of Providing Cyber Security of Ukraine, Law number 2163-VIII, Legislation of Ukraine, 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

[2] L. Streltsov, The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments, European Journal for Security Research (Springer) 2 (2017) 147–184. doi:10.1007/s41125-017-0020-x.

[3] Z. Zhyvko, T. Rudyi, V. Senyk, L. Kucharska, Legal Basis of Ensuring Cybersecurity of Ukraine: Problems and Ways of Eliminating, Economics, Finance and Management Review 2 (2020) 82–90. doi:10.36690/2674-5208-2020-2-82.

[4] V. Savchenko, S. Kononenko, V. Bobylov, L. Drok, Modern Information Technologies in the Sphere of Security and Defence 28 (2017) 41–46. URL: http://nbuv.gov.ua/UJRN/sitsbo_2017_1_9.

[5] N. Tkachuk, National cyber security system of Ukraine: perspectives of policy development and capacity building, International scientific journal Internauka. Series: Juridical Sciences, 21 (2019) 15–32. doi:10.25313/2520-2308-2019-7-5340.

[6] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, 2018. doi:10.6028/NIST.CSWP.04162018.

[7] CYBER: Global Cyber Security Ecosystem, ETSI TR 03 306 V1.2.1 (2017-03). URL: https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.02.01_60/tr_103306v010201p.pdf

[8] A. Corallo, The Digital Business Ecosystem, Edward Elgar Publishing Limited, Cheltenham, UK – Northampton, USA, 2007.

[9] CMMI V2.0 Performance Report Summary How Early-Adopters Leveraged CMMI V2.0 to Consistently Improve Their Performance, ISACA, 2020. URL: https://cmmiinstitute.com/getattachment/738104c0-a6f0-4e1c-8bbe-35076b75f36e/attachment.aspx

[10] A. Zhilin, M. Khudintsev, M. Litvinov, Functional model of the situational center of cyber defense, Network and Application Security (Information Technology and Security) 6 (2018) 51–67. doi:10.20535/2411-1031.2018.6.2.153490.

[11] O. Potiy, Organizational and Technical Model of Cyber Defense of Ukraine, in: Digitalization and Security, Kharkiv, 2020. URL: https://uaeuxperts.org/konferenciya-didzhitalizaciya-i-bezopasnost; in: Application of units, complexes, means of communication, automation and cybersecurity in the Joint Forces operation, Priority directions of development of telecommunication systems and special purpose networks. Application of units, complexes, means of communication, automation and cybersecurity in the Joint Forces operation, Kyiv, 2020.

[12] M. Khudyntsev, Main Directions of State Center of Cyber Defense Activity, Cybersecurity challenges, ITU Regional Seminar for Europe and CIS on Digital Future Powered by 4G/5G, Kyiv, Ukraine, 2018. URL: https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2018/05_Kiev/ITU%20Seminar%2015.05.18%20-%20Mykola%20Khudyntsev.pdf

[13] M. Khudintsev, A. Davydyuk, Establishing operational interaction of cybersecurity and cybersecurity as the main task of implementing the organizational and technical model of cybersecurity/cybersecurity within the national cybersecurity system, Information and telecommunication systems and technologies, and cybersecurity: new challenges, new task, Kyiv, 2019. URL: https://iszzi.kpi.ua/2019/4184