Административное право и процесс

UDC 004.056

Tkachuk Nataliya
Research Institute of Informatics and Law of the National Academy of Legal Sciences of Ukraine

NATIONAL CYBER SECURITY SYSTEM OF UKRAINE: PERSPECTIVES OF POLICY DEVELOPMENT AND CAPACITY BUILDING

Summary. *Russian cyber aggression against Ukraine, which started in 2014, have caused an urgent need for building national cybersecurity system, enabling Ukraine to counter current cyber threats to its security, stability and well-being. In this research the legislative and institutional framework of the National Cyber Security System of Ukraine (NCSS) is studied, consistent steps of the State aimed at enhancing cybersecurity and its progress for the last five years are analyzed. This work focuses on defining main problems, which hamper further development of the NCSS, and offers comprehensive recommendations for enhancing Ukraine's cyber security policy, institutional framework and national capacities to address current multidimensional cyber domain challenges. The materials of practical activity of Ukrainian state authorities responsible for cybersecurity are used in the research as well as scientific works, open source publications, analytics, legislation of national and international level in the sphere of cyber security.*

Key words: *cybersecurity, Ukraine, cybersecurity strategy, cybersecurity policy, cyber threats.*

Introduction. In order to address multidimensional cyber domain challenges and to counteract current cyber threats of Russian hybrid aggression, the process of developing effective cyber security system has been started in Ukraine in 2014.

Over the past few years the legislative framework of such system has been created – the Cyber Security Strategy of Ukraine and the Law of Ukraine "On the Basic Principles of Cyber Security" have been adopted. The mechanisms of interdepartmental interaction and coordination as well as public-private partnership in cyber security domain have been established. A number of measures have been taken to increase capabilities of main state bodies, responsible for cyber security. International partnership in the sphere of cyber security has been reinvigorated, namely the NATO Trust Fund on Cyber Defence for Ukraine has been founded, aimed on helping Ukraine to develop capabilities to counter cyber threats.

However, the devastating impact of cyber-attacks on Ukraine's critical infrastructure and state information systems that have occurred over recent years, escalation of Russian cyber aggression and emergence of new global cyber threats have demonstrated urgent need to increase the state’s capacity to counter current cyber domain challenges and to review cyber security policy.

At present the main problematic issues that hamper further development of the National Cyber Security System of Ukraine (NCSS) are the lack of effective cybersecurity policy implementation, low level of cyber-risk awareness and insufficient human capacity of the main actors of the NCSS. Among other problems there are absence of legal and organizational framework for critical infrastructure protection, outdated standards for cybersecurity, weak national legislation on cybercrime and necessity to facilitate public-private partnership.

The development of strategic directions for enhancing Ukraine’s cybersecurity policy addressing current challenged is important for drafting the Cyber Security Strategy of Ukraine 2020-2025 as well as improving existent legislative framework in this sphere. In addition, the suggestions for enhancing of institutional framework of the National Cyber Security System (NCSS) can be applied in the ongoing process of reforming security and defense sector of Ukraine. Also the conclusions and recommendations of this research will contribute to defining further vectors of international cooperation, including development of further activities within the NATO Trust Fund for Ukraine aimed to help Ukraine develop technical capabilities to counter cyber threats.

The above confirms the importance and practical significance of this issues for the development of cyber security policy of Ukraine in accordance with the best practices of the EU and NATO countries, promotion of international cooperation and worldwide action to secure cyber space.

Purpose of this research is to develop well-grounded suggestions, based on comprehensive analysis and best international practices, for enhancing Ukraine's cyber security policy, institutional framework and national capacities to address current multidimensional cyber domain challenges.

Legal and Organizational Framework of the National Cyber Security System of Ukraine

Cyber Security Strategy and Law

The key impetus for building cybersecurity system in Ukraine came from power grid cyber-attacks which took place on 23 December 2015 and is considered to be the first known successful cyberattack on a power plant [1]. Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers [2].

The results of this attack made the government realize that there was a strong need to develop necessary capacities and create effective cyber security mechanisms, which primarily would be able to protect Ukraine from cyber threats of Hybrid Warfare. Due to the increasing level of threats to national security attributed to the active use of cyberspace by the aggressor country for destructive influence on Ukraine's information resources and critical infrastructure it was necessary to make radical and rapid decisions. The first step for building the cybersecurity capacities became the creation of appropriate legal framework.

In 2016, the Cybersecurity Strategy of Ukraine was approved, where it was first recognized at the legislative level the urgent need to create a national system of cyber security as a component of the system of ensuring national security of Ukraine, which, above all, had to ensure interaction on the issues of cybersecurity of major actors - state bodies, local authorities, military formations, law enforcement agencies, scientific institutions, educational institutions, non-governmental organizations and business [3].

The Strategy of Cyber Security of Ukraine provided the basis for the development of further regulations on cybersecurity issues. It defined main cyber threats to Ukraine, outlined the priorities and directions of state policy in this area and identified main state bodies responsible for cyber security and their functions. This legal document has become the basis for systematic action to build the National Cyber Security System.

The provisions of the Strategy have been further developed in the Law of Ukraine "On Basics of Providing Cyber Security of Ukraine" (Cyber Security Law), adopted by Ukraine’s Parliament (Verkhovna Rada of Ukraine) on 5 October 2017. This Law defined the conceptual apparatus, basic principles, objects and subjects of cyber security and cyber protection, main directions of public-private partnership in this sphere, outlined basics for critical infrastructure protection framework.

The law formalized the model of the National Cyber Security System, announced in the Cybersecurity Strategy of Ukraine, defining it as "a set of actors providing cybersecurity and interrelated measures of political, scientific, technical, informational, educational character, organizational, legal, operative, intelligence, counter-intelligence, defense, engineering and technical measures, as well as measures of cryptographic and technical protection of national information resources, cyber defense of critical infrastructure" [4].

The other legal documents that form the basis for cyber security legislation in Ukraine are the following:

- The Constitution of Ukraine
- National Security Strategy of Ukraine
- Law on National Security
- Law on Information
- Law on Information Protection in Information and Telecommunication Systems
- Law on Telecommunications
- Law on Protection of Personal Data
- Other laws, as well as statutory legal acts issued in accordance with these laws.

The Decision of the National Security and Defense Council of Ukraine (NSDC) which are to be approved by a presidential decree, the acts of the President of Ukraine and the Cabinet of Ministers of Ukraine aimed at solving complex problems in the field of cyber security, also play an important role in shaping the legal and regulatory framework of the cyber security system. Among them should be distinguished the following:

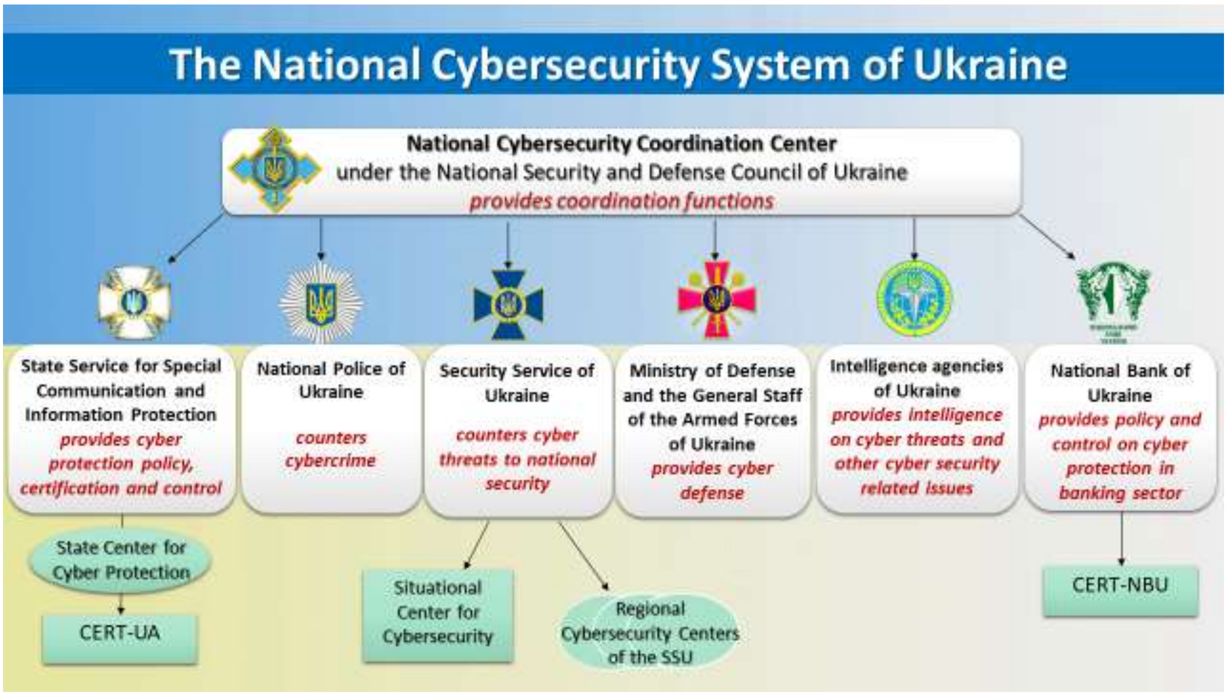
- Decision of the NSDC dated December 29, 2016 "On Threats to the Cyber Security of the State and Urgent Measures for their Neutralization" [5].
- Decision of the NSDC dated 10 July 2017 "On the State of Implementation of the Decision of the National Security and Defense Council of Ukraine dated December 29, 2016" [6].
- Resolution of the Cabinet of Ministers "On the Approval of the Procedure for the Establishment of the List of the Information and Telecommunication Systems of the State Critical Infrastructure Facilities" [7] etc.

The sources of international law, which form the basis of the regulatory framework for the National Cyber Security System of Ukraine, primarily include the Council of Europe Convention on Cybercrime, ratified by the Verkhovna Rada of Ukraine on 7 September 2005.

Creation of the National Cyber Security System is a prerequisite for ensuring the safe functioning of cyberspace, its use in the interests of individuals, society and the state. The NCSS is an integral part of the Ukraine's System of National Security.

The Structure of the National Cyber Security System of Ukraine

The main actors of the NCSS are the following: the State Service for Special Communications and Information Protection of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine, intelligence agencies, the National Bank of Ukraine. Coordination and control of the activities of the security and defense sector entities that provide cybersecurity of Ukraine is carried out by the National Security and Defense Council of Ukraine (NSDC) through the subsidiary body, the National Coordinational Cyber Security Center.



The National Cybersecurity System of Ukraine

National Cybersecurity Coordination Center
under the National Security and Defense Council of Ukraine
provides coordination functions

State Service for Special Communication and Information Protection
provides cyber protection policy, certification and control

State Center for Cyber Protection

CERT-UA

National Police of Ukraine
counters cybercrime

Security Service of Ukraine
counters cyber threats to national security

Situational Center for Cybersecurity

Regional Cybersecurity Centers of the SSU

Ministry of Defense and the General Staff of the Armed Forces of Ukraine
provides cyber defense

Intelligence agencies of Ukraine
provides intelligence on cyber threats and other cyber security related issues

National Bank of Ukraine
provides policy and control on cyber protection in banking sector

CERT-NBU

The State Service for Special Communications and Information Protection of Ukraine. This organization provides such functions:

- Development and implementation of state policy on the protection in cyberspace of governmental information resources and information, the requirement for protection of which is established by law, cyber protection of critical infrastructure.
- Coordinate the activities of other cybersecurity entities regarding cyber protection, exercise state control in this area;
- Ensure the creation and operation of the National Telecommunication Network, implementation of organizational and technical model of cyber protection.
- Carry out organizational and technical measures to prevent, detect and respond to cyber incidents and cyber-attacks and to eliminate their consequences.
- Inform about cyber threats and appropriate methods of protection against them.
- Coordinate, organize and conduct critical infrastructure vulnerability audit.
- Provide functioning of the State Center for Cyber Protection and the Government Response Team for Computer Emergencies in Ukraine (CERT-UA) [4].

An important role in cyber protection of the state information resources, detection and counteraction to cyber-attacks and cyber incidents is being played by *the State Center for Cyber Protection and Countering Cyber Threats (SCCPCC)* [8], created on July 1, 2015 as a structural unit of the State Service for Special Communications and Information Protection of Ukraine. Creation of the mentioned Center has become an important step towards the development of the National Cybersecurity System in Ukraine.

Among the main tasks are the following:

- Asses of the state of information protection in governmental authorities.
- Ensure the long-term functioning, security and development of the National Confidential Communication System.
- Ensure the functioning and development of the antivirus protection system for state authorities.
- Ensure the functioning and modernization of the System of Secured Internet Access for the state authorities of Ukraine and the Secured Internet Access Point of the State Service for Special Communications and Information Protection of Ukraine [4].

The SCCPCC is also engaged in the introduction of the latest and advanced technologies in information and telecommunication systems, carrying out expertise of Complex Systems of Information Protection (CSIPs) and other information protection means, software and hardware in the field of information security used in state authorities, administrating and upgrading the Register of Information Communication Systems of State Bodies.

In addition, the main task of the Center is to ensure the functioning of *the Emergency Response Team of Ukraine (CERT-UA)*, which is its structural subdivision. The unit was established in 2007. In 2009, it has been accredited to the Forum in Incident Response and Security Teams (FIRST) [9].

Functional tasks of CERT-UA involve accumulation and analysis of data on cyber incidents, maintenance of the state register of cyber incidents and providing state bodies and private owners of critical infrastructure with practical help in preventing, detecting and eliminating the effects of cyber incidents. Also CERT-UA organizes and conducts practical workshops on cyber protection as well as interacts with law enforcement agencies, foreign and international organizations on responding to cyber incidents.

The main types of cyber threats that CERT-UA counteracts include: malware, botnets, Internet fraud, DDoS attacks, exploitation of software and hardware vulnerabilities, unauthorized access to automated information systems, web resources and violation of the regular mode of their operation.

In addition, the Emergency Response Team of Ukraine provides the operation of a number of services available on its official website: accumulation and processing of information about the compromised IP-addresses, active monitoring of network threats, service for verifying vulnerabilities, functioning of on-line platform for reporting a cyber-incident [10].

The CERT-UA plays an important role in the National Cyber Security System as a practical unit that responds directly to a cyberattack, helps to restore network functioning and eliminate negative impacts of cyber incidents.

The most prominent examples of CERT-UA activity are the elimination of hacker attacks on the automated system Elections during the extraordinary Presidential elections in Ukraine in 2014, the localization and neutralization of the BlackEnergy virus on the objects of the energy and transport complex of Ukraine in 2015 and 2016. The CERT-UA team together with specialists from Cyber Policies, the Security Service of Ukraine, foreign partners, and private sector participated in counteracting and eliminating the consequences of large-scale hacker attacks against Ukraine in June 2017.

On February 2, 2018, a new unit – the Cyber Threat Response Center (CTRC), was established within the State Center of Cyber Protection and Countering Cyber Threats. This unit is engaged primarily in providing cyber protection of state authorities and critical information infrastructure of Ukraine [11].

The Security Service of Ukraine (SSU). This organization carries out following tasks:

- Prevent, detect, suppress and disclose crimes against peace and security of mankind committed in cyberspace.
- Carry out counter-intelligence, operational and investigative activities aimed at combating cyberterrorism and cyber-espionage.
- Secretly check readiness of critical infrastructure for possible cyber-attacks and cyber incidents.
- Counteract cybercrime, the consequences of which can create a threat to the vital interests of the state.
- Investigates cyber incidents and cyber-attacks concerning the state electronic information resources, the information, protection requirements of which are established by law, critical infrastructure.
- Provides response to cyber incidents in the field of national security [4].

The unit of the SSU responsible for conducting these functions is the Cyber Security Department, official name of which is the Department of Counterintelligence Protection of State Interests in the Sphere of Information Security. This counterintelligence body is the main actor of the National Cyber Security System which protects national security of Ukraine from cyber threats. At present it concentrates mostly on countering Russian cyber operations organized by Russian special services.

To achieve this aim, with the support of Ukraine's western partner states, serious work has been done to develop the SSU's technical and operative capabilities. Within framework of the NATO Trust Fund on Cyber Defense for Ukraine the Situational Center for Cybersecurity of the Security Service of Ukraine has been created in 2017 [12].

This is a unique structure as it combines functions and technical abilities of CERT/CSIRT with counterintelligence tools and instruments of special service and law enforcement body. It already proved to be very effective in countering cyber threats of hybrid warfare and greatly facilitated capacities of

Security Service of Ukraine in Cyber Security. During 2018-2019 three regional Cyber Security Centers of the SSU have been established in the cities Dnepr, Odessa and Sumy [13]. Their main task is to counter cyber threats at the regional level.

Another important direction of developing the SSU capabilities is promotion of public-private partnership, impossible to counter cyber threats effectively without cooperation with private sector. Firstly, because more than 80% of Ukrainian critical infrastructure is privately owned and secondly, the nature of cyber threats and cyber space makes no difference between character of threats to public sector or to national security [14].

Recognizing this importance, the Security Service of Ukraine has started a number of successful initiatives, directed on enhancing cooperation with private sector and building trust. Professionals of the Cyber Security Situational Awareness Center of the SSU on the basis of the NATO standards created the Malware Information Sharing Platform – Ukrainian Advantage (MISP-UA). This platform provides on-line automatic information exchange between Security Service of Ukraine and Critical Infrastructure about indicators of compromise and possible cyber threats. The MISP-UA is not yet being used for international information exchange but it might be considered as further step for its development.

Through this platform the SSU provides to private sector timely information which is important to protect their computer systems from cyber-attacks and greatly contributes to enhancing the security of critical infrastructure. At present there are more than 30 Critical Infrastructure Facilities in the sphere of energy, telecommunications, transport, finance connected to the MISP-UA. The legal basis for such cooperation is the Memorandum for Information Sharing [15].

As the former Head of the SSU Vasyl Hrytsak has said, emphasizing the priority of such public-private partnership - "Any representative of a large, medium and even small business can turn to the Cyber Security Situational Awareness Center for consultation and assistance" [12].

Another direction of cooperation with private sector is the engagement of so-called "white hackers" to responsible disclosure of information about vulnerabilities of computer systems of critical infrastructure and governmental authorities as well as their penetration testing. In cooperation with private sector the draft of Public Memorandum for cooperation with the Security Service of Ukraine on Responsible Search and Disclosure of Information about Vulnerabilities of Computer Systems had been developed [16]. Work is continuing to create legal basis for involving young IT-professionals in conducting confident testing of readiness of critical infrastructure for possible cyber-attacks and cyber incidents, which is one of the functional tasks of the Security Service of Ukraine.

The National Police of Ukraine ensures the protection of human and civil rights and freedoms, the interests of society and the state from criminal encroachments in cyberspace. It carries out measures on prevention, detection, suppression and disclosure of cybercrime, raising awareness of citizens about security in cyberspace.

The direct execution of these tasks is entrusted to the Department of Cyber Police of the National Police of Ukraine, established on October 13, 2015, which replaced the Office for Combating Cybercrime of the Ministry of Internal Affairs of Ukraine [17].

As stated by the Minister of Internal Affairs of Ukraine Mr. Avakov [18], the purpose of creation the Cyber Police in Ukraine was to reform and develop the units of the Ministry of Internal Affairs of Ukraine, in order to ensure training and functioning of highly qualified specialists in the expert, operational and investigative units of the Police involved in the fight against cybercrime, who would be capable of applying at the highest professional level the latest technology in operative and investigatory activities.

The Department of Cyber Police consists of structural divisions, acting on the interregional basis and directly subordinated to the Head of the Department.

In accordance with the Law of Ukraine on Ratification of the Convention on cybercrime [19] in order to ensure the international cooperation of Ukraine on combating cybercrime, the National 24/7 point of contact for the immediate assistance in investigation of cybercrimes is functioning in the structure of the Department of Cyber Police.

The number of crimes in the field of cyber security is constantly growing – in Ukraine each year the number of detected cybercrime increases by an average of 2,500 [20]. Today, the former model of cyber police units is being transformed into the effective law enforcement body oriented first of all on human rights protection, which by its technical and professional capabilities, would be able to provide immediate response to cyber threats, as well as conduct international cooperation on neutralizing transnational criminal groups in accordance with the best European standards in this area.

Among the capabilities of the Cyber Police there are the following:

- Ability to receive information on crimes from cyber-units of foreign countries.
- Professionally analyze Internet resources and network systems.
- Carry out sophisticated digital forensics.
- Provide professional assistance to other police units.
- Conduct joint operations with the international organizations such as the Europol, the Interpol etc.

The Ministry of Defense and the General Staff of the Armed Forces of Ukraine. Among the main tasks of these authorities there are:

- Carry out measures to prepare the state for reflecting military aggression in cyberspace (cyber defense).

- Carry out military cooperation with NATO and other defense actors in the field of security of cyberspace and joint protection against cyber threats.
- Implement measures to ensure cyber defense of critical information infrastructure in conditions of emergency and martial law [4].

The division within the structure of the General Staff of the Armed Forces of Ukraine, which performs the functions in the field of cyber security is the Department of Communication and Information Systems of the General Staff of the Armed Forces, subordinated to the Deputy Minister of Defense - the Head of the Apparatus [21].

The important role of the Ministry of Defense in the National Cyber Security System is attributed to the progressing militarization of cyberspace and the actualization of the threat of cyber warfare as a new phenomenon in the world security environment [22-24].

According to the data of the National Intelligence of the USA, more than 30 countries are developing offensive cyber attack capabilities. So attacks against critical infrastructure and information networks will allow attackers a means of circumventing traditional defense measures [25] and can become an asymmetric measure in a military conflict [26].

With regards to the growing threat of Russian cyber warfare against Ukraine [27], cyber security issues are increasingly reflected in the strategic documents of the Ukrainian military sector.

The Strategic Defense Bulletin of Ukraine, approved by the Decree of the President of Ukraine No 240/2016 [28], defines the development of the system of cyber defense as a prerequisite for ensuring the state's defense capability. In turn, the inability to respond effectively to the growing number of cyber-attacks is defined as one of the main problems of the of the Defense Forces functioning in the context of existing and potential threats.

The document considers the improving of the information and cyber security system to be a separate operational goal, the implementation of which involves the creation in the Ukraine's defense sector of special units aiming at cyber defense, countering technical intelligence, implementing measures to protect information in accordance with the requirements of regulatory legal acts of Ukraine and NATO standards.

The Intelligence Agencies of Ukraine carry out intelligence activities regarding threats to the national security of Ukraine in cyberspace, other events and circumstances related to the sphere of cybersecutity.

According to the Law of Ukraine "On intelligence agencies" [29], the state bodies which provide intelligence activities are the following: The Foreign Intelligence Service of Ukraine, the Defence Intelligence of Ukraine and the Intelligence Agency of the Administration of the State Border Guard Service of Ukraine.

In order to increase the efficiency of the activity of the intelligence agencies of Ukraine, the Joint Intelligence Committee under the President of Ukraine was formed [30]. The Concept of Development of the Security and Defense Sector of Ukraine, approved by the Presidential Decree No 92/2016 [31], defines the main purpose of the development of intelligence agencies, which is to strengthen the intelligence capabilities of Ukraine on the basis of their concerted, precise functioning, coordination of their activities and enhancing cooperation with the partner special services of NATO member states.

Strengthening the capabilities of intelligence agencies in the field of cybersecurity through the creation of organizational, logistical and financial conditions for improving their operational capabilities is identified as one of the priority directions of the development of the Security and Defense Sector of Ukraine.

The National Bank of Ukraine (NBU). This organization executes following functions:

- Determine the order, requirements and measures for the provision of cyber protection and information security in the banking system of Ukraine.
- Provide functioning of the CERT-NBU.
- Ensure the functioning of the cyber protection system in the banking sector of Ukraine.
- Provide cyber and information security audit on critical infrastructure of the Ukraine's banking system [4].

Banks remain the main target of cybercriminals all over the world [32] and Ukraine is no exception. The overall assessment of the events of 27-29 June, 2017 showed that 70% of Ukrainian banks have been hit in one way or another by cyberattacks of the Petya virus [33], launching of which is attributed to the Russian special services [34]. The visible consequence of such attacks was stopping the work of terminals, payment systems, bank branches, as well as limiting access to Internet banking and international transfers.

The fact that banks did not survive a cyberattack had demonstrated that the problem was not only with the efficiency of IT department of each individual bank. Underestimation of potential threats, lack of proper software and neglect by proper budgeting of cybersecurity systems of banks – all this testified to insufficiency of systemic approach to providing cyber security in banking sphere.

These conclusions made the National Bank of Ukraine as a regulative body take comprehensive measures directed on enhancing cyber security in banking system of Ukraine: the Center for Cyber Protection of the National Bank of Ukraine was created, the Computer Security Incident Response Team of the banking system of Ukraine (CSIRT-NBU) has been organized, Regulation

No. 95 of the National Bank of Ukraine "On the organization of measures to ensure information security in the banking system of Ukraine" was put in force.

By this Regulation, the NBU has obliged banks to take immediate measures to strengthen their cyber security in accordance with the established requirements, based on international ISO standards [35]. Now the banking sphere of Ukraine has the highest level of resilience in comparison with governmental structures and other facilities of critical infrastructure.

The National Cybersecurity Coordination Center (NCCC), as the working body of the National Security and Defense Council of Ukraine, coordinates and monitors the activities of the security and defense sector providing cybersecurity, forecasts and identifies potential and actual cyber threats, generalizes international experience in the field of cyber security; provides operational, informational and analytical support of the National Security and Defense Council of Ukraine on cybersecurity issues.

The NCCC was created in June 2016 by the Decree of the President of Ukraine No. 242/2016 and according to the former Secretary of the National Security and Defense Council of Ukraine Mr. Turchinov, it were to become a system-forming element of the whole system of cyber security and cyber defense of Ukraine [36].

The Head of the Center is the Secretary of the National Security and Defense Council of Ukraine. The Secretary of the Center is the Head of the structural unit of the apparatus of the National Security and Defense Council of Ukraine, whose responsibilities include cybersecurity.

The members of the Center are: the Deputy Minister of Defense of Ukraine, the Chief of the General Staff of the Armed Forces of Ukraine, the Head of the Security Service of Ukraine, the Head of the Foreign Intelligence Service of Ukraine, the Head of the National Police of Ukraine, the Head of the National Bank of Ukraine (with consent), as well as the Head of the Main Directorate of Intelligence of the Ministry of Defense of Ukraine, the Head of the Office of Intelligence of the Administration of the State Border Guard Service of Ukraine, the Head of the State Service for Special Communications and Information Protection of Ukraine. The main form of the Center's work is sessions which are held as needed, but not less frequently than quarterly [37].

Another form of developing the interagency cooperation is conducting national and international cyber security trainings with the engagement of main actors of the National Cyber Security System. For example, in the beginning of March, 2019 such trainings aimed on working out joint mechanisms of response and crisis management concerning possible cyber threats to the election process in Ukraine were held. It was conducted on the technical base of the SSU Cyber Security Situational Awareness Center using simulated virtual infrastructure of the Central Election Commission of Ukraine [38]. This had provided development of effective cooperation mechanisms which were implied during further response to mass and advanced cyber-attacks on elections infrastructure, which took place in March – May 2019 during the process of elections of the President of Ukraine. Due to coordinated common efforts of state subjects of the National Cyber Security System the timely countermeasures were taken and the necessary level of resilience and stable functioning of election systems was ensured [39].

Consequently, due to comprehensive national efforts supported by assistance from international partners, Ukraine actually managed to build from scratch effective Cybersecurity System capable of countering cyber threats to national security that intensified with the onset of Russian hybrid aggression.

The proper legislation framework was developed, main state actors responsible for cybersecurity and their functions were defined, the coordination body was established, network of CERTs and Situational Centers for Cybersecurity was created, operative and technical capabilities of main state actors of the NCSS were raised by building in its structure new operational units, public-private partnership was initiated, international cooperation on cybersecurity was facilitated.

Main Challenges of Ukraine’s Cyber Security System Further Development.

Ineffective Cybersecurity Strategy Implementation.

Though Ukraine has made a substantial step forward in cyber security domain, the main obstacle that hampers its further development is the lack of the effective mechanisms of implementing cybersecurity policies, in particular the provisions of the Cybersecurity Strategy of Ukraine and the formal approach to this issue by responsible state authorities.

The Cyber Security Strategy of Ukraine is a document of long-term strategic planning that defines the priorities of Ukraine's national interests in the field of cybersecurity, main directions, conceptual approaches to the formation and implementation of state policy in this field. The Strategy is a basis for further policy planning, developing of state programs and regulations on cyber security [40]. At the same time, in Ukraine, there is currently no effective system of state control providing objective assessment and guaranteeing its implementation.

According to the legal regulations the implementation of the Strategy provisions takes place within the framework of annual Implementation Plans, formed at the beginning of each year by the State Service for Special Communications and Information Protection of Ukraine and approved by relevant Orders of the Cabinet of Ministers of Ukraine. However, the comprehensive analysis of their fulfillment by responsible state authorities has shown that these documents are mainly of a declarative character [41].

Most of the activities envisaged by Plans for Implementing the Cybersecurity Strategy of Ukraine for 2016-2018 [42-44] are currently not executed or partially executed. There are only a few plans provisions fulfilled with expected results. Among such there are adoption of the Cyber Security Law of Ukraine, creation of the Cyber Security Situational Awareness Center of the Security Service of Ukraine, and improving the requirements for the cyber protection in the banking sector by adopting the relevant Regulation of the NBU.

Many other important issues still are not resolved:

- The Register of Critical Infrastructure Information Systems as well as the legal framework for it protection is not created.
- The Budapest Convention on Cybercrime in not fully implemented.
- The secure data center for governmental bodies isn't built.
- Any effective measures to stimulate the development of domestic software are not being taken.
- The EU directives and standards for the protection of critical infrastructure is not implemented.
- No system of cyber security auditing of such objects or main indicators of cybersecurity and risk assessment are formed.
- A unified system of cyber threats detection and information exchange between the main state actors of cyber security is not created.
- Many gaps in cyber security legislation are still not closed etc.

Although all these measures and many others were envisaged by the Cybersecurity Strategy Implementation Plans providing specific deadlines for their fulfilment and a responsible state authority. For example, the responsible authority for executing 15 provisions from the existing 18, provided by the Plan of Implementation of the Strategy of Cybersecurity of Ukraine for 2018 (approved by the Governmental Order on July 11, 2018, No. 481-p), is defined to be the State Service for Special Communications and Information Protection of Ukraine.

Moreover, timely and effective fulfilment of the Implementation Plans is hampered by untimely adoption of such plans on governmental level with the delay up to six months. For example, as at June 2019 the draft of Implementation Plan on 2019 is still not approved although it has been half a year since it should have come into force to ensure its relevant execution.

Reports on the implementation of the Cybersecurity Strategy, which are to be submitted by the responsible state bodies to the Cabinet of Ministers and the National Security and Defense Council of Ukraine every six months are also perfunctory. No disciplinary or management measures are taken as a consequence of under-performance of planned activities. The unfulfilled plan items are simply being transferred to another year or ignored without any governmental control or public scrutiny over this process.

The NCCC on its plenary sessions once a year revises the state of Cyber Security Strategy implementation, but as it's only a collective coordinating body and its members are the heads of main government authorities responsible for cybersecurity in Ukraine, it has neither powers nor will to make state actors accountable for insufficient performance of provided tasks.

Therefore, while the comprehensive organizational measures to address the issue of implementation of cyber-security policy are not taken, it is difficult to talk about solving any other tasks of the development of the National Cybersecurity System of Ukraine in general.

Addressing the problem

To address the problem of low effectiveness of cyber security policy implementation there are necessity to take a number of organizational and legal measures.

At the same time, the main priority should be focused on building strong political will and understanding on the highest state level of the importance of Cybersecurity for Ukraine's national interests, as well as commitment to take comprehensive measures to deal with existent problems of cybersecurity policy implementation even if it requires tough and unpopular initiatives.

Therefore, taking into consideration recent political changes in Ukraine in short-term perspective it is recommended for the Head of the National Cybersecurity Coordination Center:

- Prepare a comprehensive assessment of the current state of Cyber Security Strategy implementation on the basis of submitted reports of main state actors, statistics and analytics (including international expertise such as MITRA) highlighting existent problems and recommendations, providing further submission of this assessment to the President of Ukraine.
- Establish a number of high-level meeting and consultations with newly appointed top-officials of key state bodies, responsible for cybersecurity with the involvement of the main international partners of Ukraine (such as NATO experts) to identify and prioritize important issues of cybersecurity policy and cooperation in this sphere and to make further recommendations for its implementation.
- In order to provide comprehensive approach to cybersecurity policy (from the National Security Strategy to the Cyber Security Strategy and finally to the direct steps provided by the annual Cyber Security Strategy Implementation Plans) to initiate including into the National Security Strategy of Ukraine for 2020-2025 (which is now being drafted by the National Security and Defense Council of Ukraine) provisions on following cybersecurity priorities:
    - Increasing the efficiency of developing and implementation of the national cybersecurity policy, implementation of the Cybersecurity Strategy of Ukraine.
    - Enhancing capacities of main state actors of the National Cyber Security System of Ukraine.
    - Rising cybersecurity awareness and cyber hygiene.

- Developing the system of strategic communications in the sphere of cyber security.

- Widen participation format of the NCCC sessions in order to provide more broad and effective dialog on cyber security issues and policy implementation. For example, providing the participation of Ministry of Information Policy and Ministry of Education of Ukraine is important within framework of cyber awareness and strategic communications issues, the role of the Head of Parliamentary Committee on Informatization and Communications could be important to facilitate cybersecurity legislation initiatives, the dialog with private sector representatives is essential for public-private partnership development as well as critical infrastructure protection issues.

In long-term perspective it is recommended:

- Create the governmental executive body under the Cabinet of Ministers of Ukraine responsible for the cyber security policy forming and implementing which would deal with cyber security issues and provide state control in this sphere on national level. As in present, this functions aren't vested to any actor of cyber security of Ukraine and in the structure of the Ukrainian Government there is no any unit responsible for cyber security. For example, this could be the Ministry of Innovations and Cybersecurity.
- Deprive the State Service for Special Communications and Information Protection of Ukraine of its function to prepare the annual Plans for the Cyber Security Strategy Implementation. This state body according to the law is responsible only for the sphere of information protection (cyber protection) which is far narrower than the whole national cyber security sphere. Furthermore, it has already proved its ineffectiveness in timely establishing comprehensive plans of action (Implementation Plans) for all

the actors of the NCSS. This function should instead be transferred to the National Cybersecurity Coordination Center as the body representing all the main stakeholders of the National Cyber Security System.

- Increase the role of the NCCC by adding to its functions preparing annual plans for the Cyber Security Strategy Implementation, Assessments on the Current State of Cybersecurity in Ukraine and Effectiveness of Cyber Security Strategy Implementation and providing strategic coordination and control on the intergovernmental joint cyber operations in the sphere of national security. This in its turn implies providing organizational changes aimed on increasing stuffing and resourcing of the Information Security Department in the Secretariat of the National Security and Defense Council of Ukraine – the unit which provides functioning of the National Cybersecurity Coordination Center.
- Launch governmental campaign under the initiative of the NCCC aiming on encouraging authorized state bodies taking concrete measures of disciplinary character up to and including dismissal and conducting criminal prosecution (in case of criminal negligence) to those responsible state officials who didn’t provide timely execution of tasks provided by the Cyber Security Strategy Implementation Plans. If there are objective obstacles hampering its timely execution the clear mechanism of reporting and postponing are to be followed.

Another important instrument necessary to provide effectiveness of cyber security policy implementation is the appropriate public scrutiny of this subject. At present there isn’t any open publicly available information on the state of the Cyber Security Strategy Implementation Plans fulfillment by the responsible state authorities. The annual and semi-annual reports on this matter which all the state actors of the National Cyber Security System are to submit to the government stay closed to the public, though according to the Law of Ukraine

“On National Security”, content and state of implementation of strategies, doctrines, concepts, state programs and plans in the areas of national security are the subject of public control [40].

Solution to this problem may lie in regular and transparent informing the public about current state and results of the Cyber Security Strategy implementation through publishing the reports mentioned above on the official web-site of the National Cybersecurity Coordination Center and the Government of Ukraine.

Moreover, in Ukraine there isn’t any mechanisms of parliamentary oversight of the implementation of cybersecurity legislation. Sole adoption of a law cannot be enough to ensure that it works effectively and that the state budget for its implementation is not spent in vain. Therefore, to provide transparency of such procedures it is recommender to vest the Parliamentary Committee on Informatization and Communications dealing with cybersecurity legislation with new function of parliamentary oversight in the sphere of cybersecurity.

Ensuring high level of international cooperation is a very important element of cyber security policy in any country. In order to raise its effectiveness in Ukraine it’s recommended to include the Ministry of Foreign Affairs of Ukraine in the structure of the National Cyber Security System through the amendments to the Cyber Security Law, providing it with appropriate responsibilities concerning organization of effective international cooperation in cyber security domain.

Rising awareness, cyber hygiene and compliance

Cybersecurity awareness and hygiene play a critical role in protecting national interests, critical information infrastructure, businesses and personal data against cyber threats [45]. At present cyber hygiene among state officials and operators of critical infrastructure of private and public sector stays insufficient in Ukraine. This facilitates illegal activities of malicious actors aiming on cyber espionage and cyberattacks on critical infrastructure.

Along with constant breaking of basic principles of cyber security and absence of adequate motivation for cyber hygiene another factor that greatly influences resilience of systems is extensive use of pirated software. According to the MITRE assessment "even if cyber security awareness was higher in Ukraine, it might have negligible impact on minimizing risk because of ubiquitous use of unlicensed software in the public and private sector" [46].

The systematic inspections of state of compliance with the information and cyber protection requirements in governmental bodies show little progress in this sphere during the last few years, thought the results of resent cyber-attacks on Ukrainian critical infrastructure should have changed common understanding of cyber threats and importance of cyber hygiene. The attempts of state bodies on raising cybersecurity awareness and hygiene are sporadic, have no centralized authority or any coordination. Occasionally, some actors of the National Cyber Security System launches separate initiatives in this sphere within their competence through publishing on their web-resources some warning information and guidance [47-49] but with no substantial effect.

However, there is an example of a very successful cyber awareness campaign in Ukraine on stop using Russian software and information services which has supported the state initiative of banning Russian software and social media. In 2015 the National Security and Defense Council of Ukraine by its Decision from August 23, 2015 has imposed sanctions to Russian antivirus software products – Dr. Web and Kaspersky, prohibiting its usage in governmental bodies [50]. In 2017 the sanction list was widened with other Russian software products as well as popular Internet platforms and social media (Odnoklassniki, VKontakte, Yandex, Mail.ru) [51]. Though in the beginning this idea seemed to be unpopular among the population of Ukraine, due to active information campaign on behalf of the state the existent risks of using these products by Russia as an instrument of cyber espionage, sabotage and propaganda were effectively communicated to the public, which provided understanding and public support to this state initiative. Moreover, it gave new opportunities to Ukrainian business to develop national product.

The framework for cybersecurity awareness consists of three main elements that should provide any state within its comprehensive initiatives:

- *Develop understanding and motivation.* The primary task of Ukrainian government is to form understanding between necessity to follow cybersecurity requirements and promoting national security, prosperity of the nation as well as personal interests and well-being. People should clearly understand all the possible risks and consequences of their breaking the rules or ignoring basic cyber hygiene (especially if we are talking about the state and military servants or critical information operators) such as leakage of classified information, blocking of critical infrastructure activity, substantial financial losses, cyberterrorism, hazardous events etc. Ukraine's advantage is already formed motivation to protect the State and national security against external aggressor – the Russian Federation. Therefore, the main task is to ccommunicate to public the role and the place of cybersecurity and cyber hygiene in this process.
- *Provide education and training.* The platform for cyber hygiene is creation of educational basis which would provide some theoretical knowledge about cyber threats and basics of cybersecurity combined with trainings for obtaining practical skills. Such education should be built considering on target groups including school education, educational programs in higher education institutions, professional education, common cyber awareness initiatives, training for certain categories (e.g. state servants, military personnel, critical information operators etc).
- *Ensure monitoring and control.* Without proper control it is impossible to provide sufficient level of compliance with cyber security rules even with a clear understanding of risks and having enough practical knowledge to

do it. The most important element of control is possibility of implying sanctions in case of incompliance. Such monitoring and control should be organized on the national level by the State Service for Special Communications and Information Protection of Ukraine, on ministerial level by each responsible state authority within its structure and among critical infrastructure taking into consideration national requirements for cyber protection.

In order to raise awareness, cyber hygiene and compliance, its's advisable to take following steps:

- Launch the National Cybersecurity Awareness Campaign under the coordination of the National Cybersecurity Coordination Center with involvement of all state authorities, private sector and international donors. Along with the stakeholders of the NCSC the Ministry of Education and the Ministry of Information Policy of Ukraine also should play main role in this initiative.
- Develop mechanisms of strategic communications in case of a serious cyber incident of national character.
- Provide a compulsory annual computer-based training and following exams on cyber hygiene to all public and military servants as a part of their appraisal process.
- Apply disciplinary and administrative sanctions to those public servants and operators of critical infrastructure who systematically breaks the requirements of cyber security regulations. The State Service for Special Communications and Information Protection of Ukraine according to its competence must provide effective monitoring and control on an ongoing basis over cyber protection and cyber hygiene in state sector and critical infrastructure.

- Make comprehensive quantitative and qualitative assessment of unlicensed products used in state bodies of Ukraine along with mapping of all state networks, hardware and software in order to determine current needs in licensed products for gradual replacement. It seems hardly possible for Ukrainian government to solve the problem with pirated software on its own taking to consideration high prices of licensed software in comparison with an average income of Ukrainians and existent state budgets for cyber protection of governmental authorities. So it is important to involve international donors for providing necessary software to state bodies of Ukraine and engaging worldwide IT-companies to provide its products under more favorable conditions in the framework of international cooperation and public-private partnership.

Developing Capacities of Main Actors of the National Cyber Security System.

Supported by strong political will and high level of awareness all the comprehensive cybersecurity policy initiatives will led to nowhere if there are no skilled IT-professionals able to provide technical aspect of State's cybersecurity.

One of the main keys to the effectiveness of the National Cyber Security System is providing its actors with necessary human sources – skilled cybersecurity professionals able to detect, investigate and prevent advanced cyber threats. Unfortunately, today Ukraine cannot provide sufficient maintenance for such employees in government agencies and it's almost impossible to compete with salaries and compensations offered by private industry.

Within the framework of the National Cybersecurity Coordination Center activity all state cybersecurity actors have taken coordinated measures to resolve this problem or at least to make it not so acute. As a result of these efforts, changes were made to the legislation that regulates the payroll of civil servants and military personnel, providing for the establishment of a special allowance for performing tasks in the field of cyber security by approving the Governmental Decree No. 336/2018 [52]. But despite the fact that this allowance provides for additional payments in the amount up to 100 percent of the salary, due to insufficient budget financing for current fiscal year in many government agencies the actual wages were increased by only 10 percent. However now in Ukraine there is at least transparent legal mechanism of financial rewards for cybersecurity professionals of public sector.

Another sufficient problem of stuffing is rather low level of IT and cybersecurity capacities of educational institutions which prepare cybersecurity specialists for the need of state authorities. For example, the National Academy of the Security Service of Ukraine, which has Bachelor and Master Programs in Cyber and Information Security and prepare specialists for the needs of security and defense sector of Ukraine, does not have sufficient training equipment (hardware and software) to provide practical trainings on countering cyber threats because of its high cost and absence of teachers with appropriate experience.

Never the less, it must be noted that the technical capabilities of the main state actors of the NCSS have been greatly developed as well as the professional level of their cybersecurity specialists. This became possible first of all due to the international assistance to Ukraine (supply of modern software/hardware, sharing best practices and organizing systematic trainings on countering cyber threats) and common understanding on the national level of importance of cyber security issues.

However, further development of capacities of main actors of the National Cyber Security System demands following steps:

- Insert additional separate budget line for cyber security in the State Budget for the Security and Defense Sector of Ukraine, including expenses for maintenance of cybersecurity personnel. This step will provide full implementation of the Cabinet of Ministers Decree No. 336/2018 and contribute to settling the problem with underfunding of cybersecurity professionals in state sector.
- Use outsourcing for providing some of the cybersecurity functions of the State. For example, outsourcing services for providing cyber protection for many governmental structures will be much more effective and cheaper then training and maintaining in-house specialists. This also could be an impetus for bringing public-private partnership on cybersecurity in Ukraine to a higher level.
- Establish a short-term working group including main actors of the NCSS, private sector (cybersecurity companies and academia) and Ministry of Education of Ukraine for developing and implementing into educational process common standards and requirements for training cybersecurity specialists taking into consideration best EU practices and standards in this sphere.
- Create the National Cybersecurity Training Center aimed at preparing cybersecurity specialists for law enforcement, intelligence and counterintelligence services under the National Academy of the Security Service of Ukraine as the higher educational establishment with the most expertise, resources and experience in this sphere. This will give an ability to bring together efforts of all the national stakeholders as well as international partners (e.g. NATO Trust Fund) to create educational capabilities with necessary technical facilities, teaching personnel and based on best international practices. The regular universities also should be involved into this initiative.

Enhancing Public-Private Partnership

The importance of efficient public-private cooperation in cyber security domain is reflected in Ukrainian cyber legislation and recognized by all state stakeholders of the National Cyber Security System. Though the substantial work in this direction had already been done there still is a necessity to create an appropriate organizational platform aiming at providing and developing public-private partnership mechanisms.

In this prospective a reasonable idea was put forward by Konstantin Korsun [53], Ukrainian cyber security expert, for the government of Ukraine along with international donors and the biggest players in Ukrainian IT-business to establish a non-governmental organization with different stakeholders' shares (for example, government - 40%, business - 30%, international donors - 30%). The share of state shouldn't be controlling in order not to create another state body, but, at the same time, it still should be significant to ensure the stability of the project. All three stakeholders may be able to delegate to the Supervisory Board 3-5 or more representatives, but they all have only one vote together.

According to K. Korsun, the main purpose of its creation will be to build or renew public trust. This Multi-Stakeholder Cybersecurity Platform will carry out the following tasks:

- Providing free of charge qualified consultations on all aspects of cybersecurity, available to every resident of Ukraine, private companies, state institutions, law enforcement agencies, organizations of any form of ownership with the possibility to go to the place of cyber incident (in exceptional cases).
- Comprehensive raising of cyber-hygiene and cyber-awareness level among all strata of the population.
- Development of recommendations on primary measures to improve cybersecurity, including the regulatory framework.

- Hosting and providing organizational support to cyber conferences, local or international Capture the Flag (CTF) competitions and cyber training.
- Daily publication of newsletters on current cybersecurity news, publication of analyzes, researches and studies on cybersecurity.

This organization must have extensive practical experience in cybersecurity, management, jurisprudence, public administration, experience in international co-operation on cyber security issues, be free to navigate in contemporary world trends and latest approaches, international standards, practices, achievements.

This initiative will not only build trust but also will create shared responsibilities for the state and businesses in cyber security while the international stakeholders will play an important role of mediators providing safeguards to avoid misuses.

Building Legal Framework for Critical Information Infrastructure Protection and Resilience

The protection of Critical Information Infrastructure still remains to be unsettled in Ukrainian legislation. There isn’t a specific law on this issue, though a number of bills are being drafted by Ukrainian state bodies during last couple years. But the main gap of legislation in this sphere is absence of the National Register of Critical Information Objects. This means that there is no legal basis to apply to any Ukrainian facility of private sector of vital importance (such as energy production and electricity generation, financial services, telecommunication and transportation infrastructure, and so on) any requirements of cyber protection or providing immediate information to state authorities about cyber incidents and cyber-attacks because none of it has an official status of “Critical Infrastructure Object”.

The formation of such Register was entrusted by the Cabinet of Ministers of Ukraine to the State Service for Special Communications and Information

Protection of Ukraine. According to the Governmental Decree from August 23, 2016, N 563 [7] this task should have been done till February, 2017 (in six months' time). Despite the colossal work that have been done in this direction by responsible state authority, the draft of the Register wasn't finished and approved by the Government. The main reason is unwillingness of private sector to participate in this process even sabotaging in order not to obtain the status of Critical Infrastructure Object as for them it would mean more financial costs and additional responsibilities [54].

In this contest it's difficult not to agree with conclusion of Madeline Carr [55] that successful public–private partnerships in cyber are either characterized by shared interests or, if the interests of the partners are not well aligned, governed by rules.

To settle this problem in Ukraine the state should demonstrate strong political will and finish the process of establishing strict and clear regulations for critical infrastructure protection. Moreover, it is necessary to provide in legislation clear sanctions of a financial character to owners of critical infrastructure facilities for breaking the requirements of its cyber protection imposed by the state.

Of course, the state authorities should and will provide all kinds of assistance on cyber security issues to critical infrastructure of private sector, including not only methodology and information sharing but practical actions of response to cyber-incidents and cyber-attacks. However, positive motivation in providing critical infrastructure protection has proved insufficient if it's not supported by effective governmental requirements and control.

Taking into consideration European vector of Ukraine's further development the implementation of the EU Network and Information Security directive (NIS Directive) [56] should be the primary step for building comprehensive framework of critical infrastructure protection in Ukraine.

Updating Cyber Security Standards

According to the Law of Ukraine "On Protection of Information in Information and Telecommunication Systems" all state information resources must be processed only in systems secured with the Integrated Information Protection System (IIPS) with verified compliance [57]. But existent standards which are the basis for building such IIPS are outdated and do not take into account present cyber threats (e.g. APT-attacks).

According to the Analytical Report to the Annual Address of the President of Ukraine to the Verkhovna Rada of Ukraine "On the Internal and External Situation of Ukraine in 2018" [58] the issue of upgrading the IIPS or its change to another protection system remains unresolved. The very idea, internal structure and model of the implementation of IIPS in most cases does not meet the requirements of modern cyber protection (especially in the non-state sector, in particular in business). This is the cause of persistent acute criticism among domestic expert and business circles, which focuses on the static nature of this system, its bulkiness, and the scarcity of scalability. In addition, the Law of Ukraine "On Basics of Providing Cyber Security of Ukraine" requires an independent audit of information security of critical infrastructure objects, carried out on the basis of international standards, European Union and NATO standards.

Therefore, in order to strengthen cyber resilience of critical information infrastructure of private and public sector (including state electronic resources) it is a must to update existent national cyber security standards taking into account existent cyber threats or to implement requirements for cyber protection on the basis of international or European cyber security standards.

Enhancing Cybercrime Prevention

The constant rise of cybercrime is a worldwide tendency [59]. Losses from cybercrime are predicted to cost the world $6 trillion annually by 2021 [60]. According to the Head of the Cyber Police of Ukraine, a steady increase in cybercrime is recorded in Ukraine [61]. Thus, the development of efficient capabilities to counter cybercrime is an essential challenge for the Ukraine’s National Cyber Security System.

One of the main obstacles preventing Ukrainian cyber police from protecting the rights and freedoms of citizens of Ukraine from encroachments by cybercriminals remains the imperfection of domestic criminal and procedural law. The rapid growth of cybercrime in Ukraine is facilitated by the fact that domestic legislation in the field of criminal prosecution of computer crimes is one of the most liberal in the world. There were cases when international cybercriminals were arrested in Ukraine in a result of an international law enforcement joint operation but pursuant to a court order based on national criminal code they were released after paying a fine or receiving a suspended sentence. For today, no hacker has been imprisoned in Ukraine yet [62].

As the Head of the Department of Cyberpolice of the National Police of Ukraine Sergey Demedyuk noted, "The country is turning into Mecca for cybercriminals. They move to Ukraine and use it, also as a platform for money laundering" [63].

Cybercrime migrates towards those territories where there aren’t appropriate laws or it is not possible to effectively apply these laws. So the main issue to promote cybercrime prevention in Ukraine is to increase the penalties for cyber-crimes according to EU and NATO practices.

Another important measure to take is the implementation of the Convention on Cybercrime, to which Ukraine is signatory since 2005. Though Ukraine takes an active part in international initiatives on its implementation within the framework of the Cybercrime Convention Committee (T-CY) of the Council of Europe and has developed draft law harmonized with the Convention, many important provisions are still not implemented to the domestic legislation. In particular, it’s important to provide norms that would oblige service-providers to store, preserve and partially disclose computer data including traffic data by a request of competent authorities, and also would address the problem of collection of evidence in electronic form.

Failure to settle this issues not only hampers cybercrime prevention in Ukraine but also complicates international cooperation within contact point 24/7, as the Ukrainian law enforcement bodies don't have necessary authority to obtain from service-providers information requested by foreign partners and necessary to prevent and investigate international cybercrime.

Conclusions. Over the past few years, Ukraine has managed to create from the scratch the National Cyber Security System developing necessary capacity to address emerging cyber-threats, primarily those coming from Russian hybrid aggression. Of course, not all the tasks have been solved so far and there are still many problematic issues that need to be addressed for further development of Ukraine's cyber capabilities in the face of new challenges coming from cyber space.

Taking into consideration current problems that hamper further enhancing of the NCSS described in this research, primary steps of Ukraine in this direction should be first of all aimed on establishing effective mechanisms of cybersecurity policy implementation guaranteed by due governmental control in conjunction with public scrutiny, parliamentary oversight and foreseeing disciplinary measures in case of inappropriate fulfillment provisions of annual Plans for Cyber Security Strategy Implementation by responsible state officials.

But primary focus should be oriented towards building strong political will and understanding by highest state authorities the importance of effective implementation of cybersecurity policy for the good of the national security of Ukraine and necessity to take unpopular measures as well (such as strict control and disciplinary sanctions) to provide proper executions of cybersecurity policy and requirements by all responsible state actors.

Next steps should be directed at rising awareness and cyber hygiene first of all among state servants, military personnel and operators of critical information infrastructure within the framework of National Cybersecurity Awareness Campaign launched under the coordination of the NCCC. Also it is necessary to provide a compulsory computer-based training and following exams to the above-mentioned categories of personal as well as applying sanctions in case of systematic violations of cyber security requirements.

Supported by strong political will and high level of awareness all the comprehensive cybersecurity policy initiatives will led to nowhere if there are no skilled IT-professionals able to provide technical aspect of State's cybersecurity.

Taking into account that one of the main keys to the effectiveness of the National Cyber Security System is providing its actors with necessary human sources, developing capacities of the NCSS stakeholders should be primarily based on addressing the problem of low maintenance of cybersecurity personnel and improving existent system of cybersecurity specialists training.

To facilitate public-private partnership it is recommended to create Multi-Stakeholder Cybersecurity Platform with the state, business and international donors as stakeholders aiming at building trust and providing to population, state bodies and private companies free services in cyber security such as qualified consultations, campaigns on cyber-hygiene, recommendations on cybersecurity policy and legislation, organizing cyber conferences, publishing cyber analytics etc.

Other efforts should be directed at building legal framework for critical information infrastructure protection by adopting the National Register of Critical Information Objects and framework law establishing main requirements and responsibilities of their owners in the sphere of cyber protection. Furthermore, providing high level of critical infrastructure resilience is impossible without updating domestic standards of cyber security on the basis of international and European standards in this sphere.

To enhance cybercrime prevention and investigation as well as international cooperation in this area the cybersecurity policy of Ukraine should include measures on increasing penalties for cybercrimes and implementing the Budapest Convention in terms of obliging service-providers to store, preserve, and partially disclose computer data by a request of competent authorities as well as addressing the problem of collection of evidence in electronic form.

All the steps taken by Ukraine to enhance cybersecurity should be based on whole of government approach, broader involvement of private sector, transparent and comprehensive national cybersecurity policy.

Following European vector of Ukraine's national strategy, it is important to consider best European practices in cyber security (such as EU framework on Critical Infrastructure protection, comprehensive cybersecurity standards, approaches to cybersecurity education etc.) while developing the National Cyber Security System of Ukraine.

References

1. E-ISAC. 2016. Analysis of the Cyber Attack on the Ukrainian Power Grid. URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
2. Park D., Summers J, Michel W. Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks, 2017. URL: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks.
3. Cyber Security Strategy of Ukraine, 2016. URL: https://zakon5.rada.gov.ua/laws/show/96/2016.
4. Law of Ukraine on Basics of Providing Cyber Security of Ukraine 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
5. Decision of NSDC of Ukraine (December 29, 2016). URL: https://www.president.gov.ua/documents/322017-21282.

6. Decision of NSDC of Ukraine (July, 10, 2017). URL: https://www.president.gov.ua/documents/2542017-22502.
7. Resolution of Cabinet of Ministers of Ukraine № 563 (August 23, 2016). URL: https://www.kmu.gov.ua/ua/npas/249267402.
8. State Service for Special Communications and Information Protection of Ukraine. 2015. "У Держспецзв'язку створено Державний центр кіберзахисту та протидії кіберзагрозам" [State Center of Cyber Protection and Countering Cyber Threats was created in SSSCIP]. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=156473 &cat_id=119123.
9. "CERT-UA: скорая киберпомощь" [CERT-UA – Cybersecyrity Emergency] 2014. PCWeek/UE, №4. URL: https://www.pcweek.ua/themes/detail.php?ID=147850.
10. Emergency Response Team of Ukraine. "Скористайтеся нашою допомогою в ліквідації кіберзагроз" [Use Our Help to Liquidate Cyber Threats]. URL: https://cert.gov.ua/ (accessed June 9, 2019).
11. Emergency Response Team of Ukraine. "Відкриття Центру реагування на кіберзагрози" [Opening of Cyber Threat Response Center]. URL: https://cert.gov.ua/news/25 (accessed June 9, 2019).
12. Security Service of Ukraine "Голова СБУ відкрив Ситуаційний центр забезпечення кібернетичної безпеки" [Head of SSU Opens Cyber Security Situational Awareness Center]. URL: https://ssu.gov.ua/ua/news/1/category/21/view/4318#.7sucy46n.dpbs (accessed June 10, 2019).
13. Radio of Freedom "В Одесі відкрили центр запобігання кібератакам при СБУ" [In Odessa the Cyber Security Situational Awareness Center is opened]. URL: https://www.radiosvoboda.org/a/news-odesa-sbu/29919180.html (accessed June 10, 2019).

14. Tkachuk, Nataliya. 2018. "Правове регулювання взаємодії Служби безпеки України з приватним сектором у сфері забезпечення кібербезпеки" [Legal Regulations of Cooperation between Security Service of Ukraine and Private Sector in Sphere of Cybersecurity]. Information and Law, № 4 (December): 104-111. URL: http://ippi.org.ua/sites/default/files/12_10.pdf.
15. Security Service of Ukraine "СБУ посилює захист інформаційної безпеки підприємств енергетичної галузі України" [SSU Strengthens Protection of Information Security of Ukraine's Energy Sector]. URL: https://ssu.gov.ua/ua/news/1/category/21/view/5213#.ARNTdGPL.dpbs (accessed June 26, 2019).
16. Security Service of Ukraine "Публічний меморандум про взаємодію зі Службою безпеки України у сфері відповідального пошуку та розкриття інформації про вразливості інформаційно-телекомунікаційних систем та/або телекомунікаційних мереж" [Public Memorandum on Cooperation with the Security Service of Ukraine on Responsible Search and Disclosure of Information on Vulnerabilities of Information and Telecommunication Systems and/or Telecommunication Networks]. URL: https://ssu.gov.ua/ua/pages/330.
17. Decree of Cabinet of Ministers of Ukraine № 831 (October 13, 2015), https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF.
18. Avacov, Arsen. 2015. "Cyberpolice – Step to Reform" Facebook, October 11, 2015. URL: https://www.facebook.com/arsen.avakov.1/posts/916452195111554.
19. Law of Ukraine On the Ratification of the Convention on Cybercrime 2005. URL: https://zakon.rada.gov.ua/laws/show/2824-15.
20. Nekrasov, Vsevolod. 2018. "Глава Киберполиции: "Ваш сын в полиции" приносит мошенникам на "зоне" миллион гривен в сутки" [Chief of Cyberpolice – "Your Son in Prison Scheme Brings Crooks in

prison Million of Hryvnas a Day"] The Economic Truth, January 15, 2018. URL: https://www.epravda.com.ua/rus/publications/2018/01/15/633003/.

21. Ministry of Defense of Ukraine. 2013. "Головне управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України" [Department of Communication and Information Systems of the General Staff of the Armed Forces of Ukraine]. URL: http://www.mil.gov.ua/ministry/struktura-generalnogo-shtabu/golovne-upravlinnya-zvyazku-ta-informaczijnih-sistem-gsh-zsu.html (accessed June 11, 2019).
22. Cornish P., Livingstone D., Clemente D., Yorke C. 2010. "On Cyber Warfare" Chatham House (November 2010). URL: https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf.
23. Ismail, Nick. 2019. "Cyber war is here, according to 87% of security professionals". Information Age (March 19, 2019). URL: https://www.information-age.com/cyber-war-security-professionals-123480950/.
24. Dombrowski, Peter and Demchak, Chris C. 2014. "Cyber War, Cybered Conflict, and the Maritime Domain," Naval War College Review: Vol. 67, № 2, Article 7. URL: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1321&context=nwc-review.
25. United States Senate Committee on Armed Services. 2017. "Joint statement for the Record to the Senate Armed Services Committee on Foreign Cyber Threats to the United States" (January 5, 2017). URL: https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.
26. Gorbulin, Volodymyr. 2015. "В поисках асимметричных ответов: киберпространство в гибридной войне" [Searching for Asymmetric Response: Cyberspace in Hybrid Warfare]. The Mirror of the Week: Vol.

6, February 20, 2015. URL: https://zn.ua/internal/v-poiskah-asimmetrichnyh-otvetov-kiberprostranstvo-v-gibridnoy-voyne-_.html.

27. Ukrainian Multimedia Platform for Broadcasting. 2018. “Кремль націлений на гібридні, а не військові операції проти України – Вершбоу” [Kremlin Aims at Hybrid not Military Operations against Ukraine – Vershbow]. December 20, 2018. URL: https://www.ukrinform.ua/rubric-polytics/2604674-kreml-nacilenij-na-gibridni-a-ne-vijskovi-operacii-proti-ukraini-versbou.html.
28. Presidential Decree On Strategic Defense Bulletin of Ukraine. June 6, 2016, №240. URL: https://zakon.rada.gov.ua/laws/show/240/2016.
29. Law of Ukraine On Intelligence Agencies of Ukraine 2001. Consolidated, May 9, 2018. URL: https://zakon.rada.gov.ua/laws/show/2331-14.
30. Presidential Decree On enhancing of guidance, coordination and control over the activity of the intelligence agencies of Ukraine. January 30, 2015 № 42. URL: https://zakon.rada.gov.ua/laws/show/42/2015.
31. Presidential Decree On the Concept of Development of the Security and Defense Sector of Ukraine. March 14, 2016, №92. URL: https://www.president.gov.ua/documents/922016-19832.
32. Lewis, James. 2018. “Economic Impact of Cybercrime – No Slowing Down”. McAfee Report: February, 2018. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf.
33. Pavlovska, Anastasiya and Halimon Zarina. 2018. “Кібербезпека у банківському секторі: чи допоможе IT-outsourcing?” [Cyber Security in Banking Sector – Will IT-Outsourcing Help?]. Juridical Newspaper: Vol. 10, March 6, 2018. URL: https://www.sk.ua/sites/default/files/kiberbezpeka_u_bankivskomu_sektori.pdf.

34. The Washington Post. 2018. “Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes”, January 13, 2018. URL: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.
35. Decree of the National Bank of Ukraine, September 28, № 95. URL: https://bank.gov.ua/document/download?docId=56426049.
36. National Security and Defense Council of Ukraine. 2016. “О.Турчинов: Національний координаційний центр кібербезпеки повинен мобілізувати весь наявний потенціал для забезпечення надійного кіберзахисту країни” [O. Turchinov – National Cybersecurity Coordination Center Should Mobilize All Capacities for Cyber Protection of State]. July 11, 2016. URL: http://www.rnbo.gov.ua/news/2528.html (accessed June 12, 2019).
37. Presidential Decree on the National Cybersecurity Coordination Center, June 7, 2016, № 242. URL: https://www.president.gov.ua/documents/2422016-20141.
38. Security Service of Ukraine. 2019. “На базі СБУ проходять міжнародні навчання із забезпечення кібербезпеки систем ЦВК” [On the basis of the SSU International Training Is Going On to Ensure Cyber Security of the CEC systems]. ssu.gov.ua, March 6, 2019. URL: https://ssu.gov.ua/ua/news/1/category/2/view/5806#.qMpgxOgK.dpbs (accessed June 12, 2019).
39. RBK-Ukraine. 2019. “Аваков рассказал о кибератаках на сервера ЦИК в день выборов” [Avakov Told about Cyber-Attacks on CEC Servers on the Day of Elections]. April 2, 2019. URL: https://www.rbc.ua/rus/news/avakov-rasskazal-kiberatakah-servera-tsik-1554164761.html.

40. Law of Ukraine On National Security 2018. URL: https://zakon.rada.gov.ua/laws/show/2469-19.
41. Tkachuk, Nataliya. 2019. "Стан та проблемні питання реалізації Стратегії кібербезпеки України" [State and Problematic Issues of Cybersecurity Strategy Implementation]. Information and Law: Vol. 1 (April, 2019). URL: http://ippi.org.ua/tkachuk-na-stan-ta-problemni-pitannya-realizatsii-strategii-kiberbezpeki-ukraini-st-129-134.
42. Order of Cabinet of Ministers of Ukraine "On Approval of Cybersecurity Strategy Implementation Plan for 2016", June 24, 2016, № 140-р. URL: https://zakon.rada.gov.ua/laws/show/440-2016-%D1%80.
43. Order of Cabinet of Ministers of Ukraine "On Approval of Cybersecurity Strategy Implementation Plan for 2017", March 10, 2017, № 155-р. URL: http://zakon2.rada.gov.ua/laws/show/155-2017-%D1%80.
44. Order of Cabinet of Ministers of Ukraine "On Approval of Cybersecurity Strategy Implementation Plan for 2018", July 11, 2018, № 481-р. URL: https://zakon.rada.gov.ua/laws/show/481-2018-%D1%80.
45. European Union Agency for Network and Information Security. 2016. "Review of Cyber Hygiene Practices". enisa.europa.eu (December, 2016). URL: https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport.
46. MITRE. 2018. "Ukraine National Cybersecurity Strategy Assessment and Recommendations, prepared for the Government of Ukraine", January 20, 2018.
47. Security Service of Ukraine. 2017. "Recommendations on Protection Against Virus Petya" Facebook, October 27, 2017. URL: https://www.facebook.com/SecurSerUkraine/posts/1958917667671562.
48. CERT-UA. 2018. "Recommendations". Cert.gov.ua, January 13, 2018. https://cert.gov.ua/recommendations/21 (accessed June 13, 2019).

49. Cyberpolice of Ukraine. 2019. "Cyberpolice Gave Recommendations on Protection of Bank Acounts". cyberpolice.gov.ua, June 7, 2019. URL: https://cyberpolice.gov.ua/article/kiberpoliczziya-nadala-rekomendacziyi-po-zaxystu-zaoshhadzhen-na-bankivskyx-raxunkax-557/ (accessed June 13, 2019).
50. Decision of the National Security and Defense Council of Ukraine, August 23, 2016. URL: https://zakon.rada.gov.ua/laws/show/549/2015.
51. Decision of the National Security and Defense Council of Ukraine, April 28, 2017. URL: https://zakon.rada.gov.ua/laws/show/ru/n0004525-17/paran2#n2.
52. Decree of Cabinet of Ministers of Ukraine, February 21, 2018, № 336. URL: https://zakon.rada.gov.ua/laws/show/336-2018-%D0%BF.
53. Korsun, Konstyantyn. 2018. "Пропоную загальну концепцію побудови альтернативної системи кібербезпеки України" [Suggestions on Common Concept for Building Alternative Cyber Security System of Ukraine] Ukrainian multimedia platform for broadcasting. November 12, 2018. URL: https://www.ukrinform.ua/rubric-polytics/2578090-proponuu-zagalnu-koncepciu-pobudovi-alternativnoi-sistemi-kiberbezpeki-ukraini.html.
54. Tkachuk, Nataliya. 2018. "Організаційно-правові засади формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави" [Organizational and Legal Framework for Formation of the List of Information and Telecommunication Systems of the Critical Infrastructure of the State]. Information and Law: Vol. 24, December, 2018. URL: http://ippi.org.ua/sites/default/files/16_4.pdf.
55. Carr, Madeline. 2016. "Public–Private Partnerships in National Cyber-Security Strategies". International Affairs 92: Vol. 1 (2016) 43-62. URL: https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf.

56. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.
57. Law of Ukraine on Protection of Information in Information and Telecommunication Systems 1994. Consolidated, April 19, 2014. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
58. National Institute for Strategic Studies. 2018. “Analytical Report to the Annual Address of the President of Ukraine to the Verkhovna Rada of Ukraine “On the Internal and External Situation of Ukraine in 2018”. niss.gov.ua, 2018. URL: http://www.niss.gov.ua/sites/default/files/2019-02/Analit_Dopovid_Poslannia_2018.pdf.
59. Ismail, Nick. 2017. “The Rise of Cybercrime Continues to Accelerate”. Information Age: July 28, 2017. URL: https://www.information-age.com/rise-cyber-crime-continues-accelerate-123467629/.
60. Morgan, Steve. 2018. “Cybercrime Damages $6 Trillion By 2021”. Cybersecurity Ventures: December 7, 2018. URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
61. Lashchenko, Olesya. 2018. “Ми фіксуємо постійні кібератаки з території Росії – керівник кіберполіції України” [We fix constant Cyberattacks from the Territory of Russia – the Head of Cyberpolice]. Radio of Freedom, September 11, 2018. URL: https://www.radiosvoboda.org/a/29426438.html.
62. Interfax Ukraine. 2018. “Демедюк: Штрафовать простых людей за VPN мы не собираемся” [Demedyuk: We Are Not Going to Fine Common People for Using VPN]. interfax.com.ua, May 18, 2018. URL: https://interfax.com.ua/news/interview/506220.html.

63. Nekrasov, Vsevolod. 2016. “Легкі гроші: Україна перетворюється на Мекку для кіберзлочинців” [Easy Money – Ukraine is Turning into Mecca for Cybercriminals]. The Economic Truth, March 28, 2016. URL: https://www.epravda.com.ua/publications/2016/03/28/587004/.