Actual Threats of Defence of National Critical Informative Infrastructure, Ways of Decision

Dmytro Melnyk [1] * [0000-0002-1497-950X], Oleksandr Shamsutdinov [1] [0000-0002-9325-9227], Yevhen Yudenko [2] [0000-0002-5122-726X]

[1] *National Academy of the Security Service of Ukraine, Kyiv, Ukraine*
[2] *Krementchuk flying college of the Kharkiv national university internal affairs, Krementchuk, Ukraine*
* *ratel6969@meta.ua*

ABSTRACT

The actual state of the legal adjusting of defence of critical informative infrastructure of Ukraine is reflected in the article. The reference list of objects of domestic critical informative infrastructure is offered for the use in scientific researches and practice. Actual threats are marked to safety of critical informative infrastructure, certain in the documents of strategic level and додатово is specified on results the analysis of materials of practice of counteraction to such threats. Safety and security of objects of critical informative infrastructure from such threats are certain in Ukraine one of base elements of the national system of firmness. Modern problem aspects and necessities of defence of objects of critical informative infrastructure are outlined, offered ways of their decision taking into account Ukrainian and world experience, in thereby legislative, organizational, technical, regime, reconnaissance, оперативно-розшукові et al.

Keywords: *critical infrastructure, objects, defence, necessities, problems, decisions.*

1. INTRODUCTION

The actions of cybernetic influence in modern terms became the inalienable constituent of hybrid aggression of Russian Federation (RF) against Ukraine. Ukraine became a ground for the hacker experiments of the special services of Russian Federation, numerous diversions and acts of terrorism against the objects of critical infrastructure. The harmful viral programs ("Black Energy", "WannaCry", "Petya", "Locky", "Bad Rabbit" and others like that) at first were approved in Ukraine, and then used in the countries of the West [1, 2].

During 2014-2021 years Ukraine tested the unprecedented amount of cyberattack on the informative resources of objects of critical infrastructure (farther - OCI) - enterprises of life-support, power, transport sphere, public financial institutions, organs, which guarantee safety, defensive, defence against extraordinary situations and others like that. Direct harmful influence was tested by the informative systems and networks on such objects.

2. METHODOLOGY

Research of problem aspects and necessities of defence of objects of critical informative infrastructure (farther - OCII) it was realized in a few stages. The state of the normatively-legal adjusting of defence of objects of national critical informative infrastructure was analysed at first. Present threats and problem aspects to the safe functioning of national critical informative infrastructure are certain in future. In the end were drawn conclusion, and also the given recommendations in relation to the improvement of defence of critical informative infrastructure of Ukraine.

For implementation researches were drawn on different materials and applied row of methods. These methods were select taking into account a select purpose and tasks of research. In particular, in-process an author used the aggregate of scientific and specially-legal scientific methods: dialectical method, method system and to the analysis of content, method of induction and deduction, формально-юридичний method and other.

3. RESULTS

The processes of globalization and swift development of information technologies stipulated appearance of new threats to the national critical infrastructure, first of all terrorist and cybernetic.

Next to the traditional methods of assassinating on the objects of critical infrastructure (explosions, other damages fell), terrorists are widely use the newest of informatively-communication technologies for violation of the regular modes of operations of CASS of management technological processes. All greater distribution in a cyberspace is acquired by the politically explained activity in form attacks on state and corporate informative resources.

Also on the state of safety of OCI and them informative resources influence: imperfection of the national system of defence of critical infrastructure, absence of only public organ which carries out co-ordination of actions in this sphere; unclearness of tasks, plenary powers and responsibility of subjects of defence of critical infrastructure; absence of the ratified list, and also to the order of the passport system and categorizing of such objects and only methodology of estimation of threats to the critical infrastructure and others like that.

Such state of businesses creates obstacles for effective implementation of near-term safety tasks the authorized subjects, does not allow to organize effective defence of OCII, that substantially promotes the ununconcern of corresponding threats to national safety of Ukraine[1].

Taking into account possible negative consequences, certain Order of forming of list of the information-telecommunication systems of objects of critical infrastructure of the state [3], to the number of OCII of Ukraine it is expedient to take the information-telecommunication systems (farther - ITS) of public and management (Administration of President, NSDC of Ukraine and her working organ, is the National co-ordinating center of cybersecurity, the Cabinet of Ministers of Ukraine, NCRC, National Bank, State Service of Special Communication and Information Protection (SSSCIP) of Ukraine, National center of the technical operation management of telecommunications of Ukraine networks and others like that), forces of safety and defensive authorities (SSU, Ministry of defence, National Police of Ukraine (NPU), reconnaissance organs), and also enterprises, establishments and organizations regardless of pattern of ownership, which are the proprietors (by managers) of objects of critical informative infrastructure and / or carry out activity in the field of protection of data, electronic communications and provide their functioning.

The value of critical information infrastructure as a strategic resource more grows, that requires permanent attention and guard. In accordance with binding overs to the century of 4 Laws OCII are the objects of cybersecurity and cybersafety. On OCI protecting of ITS is provided from cyberattacks, and also realise the independent audit of informative safety, requirement and order of realization of which are set by normatively-legal acts, worked out on the basis of international standards, standards of EU and NATO and ratified by the Cabinet of Minister's of Ukraine.

From cyberattacks' objects, included to List of ITS of objects of critical infrastructure of the state, are subject the priority protecting. Criteria and order of taking to OCI, the list of such objects, general requirements, in relation to their cybersafety become firmly established Cabinet of Ministers and national Bank of Ukraine (in the banking system) [3].

The necessity of defence of OCII for modern terms is predetermined row of serious threats to national safety, the list of which was specified in Strategy of national safety of Ukraine, ratified by Decree of President of Ukraine from 14.09.2020 № 392/2020.

Among them: modern model of globalization, which did possible distribution of international terrorism, religious and ideological fundamentalism and extremism; continuation of RF of hybrid war is against Ukraine by system application of political, economic, informatively-psychological, cybernetic and soldiery facilities; continuation of the foreign states the special services, first of all Russian Federation, reconnaissance-blasting activity against Ukraine; strengthening of threats for a critical infrastructure, related to worsening of her the technical state, by absence of investments in her updating and development, by unauthorized interference with her functioning, continious by battle actions, temporal occupation of part of territory of Ukraine; use of resources of OCI for financing of terrorism, separatism and distribution of massive weapon and others like that.

The indicated list of threats to national safety is specified and complemented by positions of Strategy of cybersecurity of Ukraine, ratified by Decree of President of Ukraine from 26.08.2021 № 447/2021: hybrid aggression of Russian Federation against Ukraine in a cyberspace; cyberattacks of the RF, sent to the of

[1] Critical informative infrastructure - aggregate of objects of critical informative infrastructure - of communication or technological systems of objects of critical infrastructure, cyberattack on which directly will influence on their permanent functioning (ч. 1 century of a 1 Law of Ukraine is "About basic principles of providing of cybersecurity of Ukraine").

informatively-communication systems of public organs of Ukraine and other OCII with the purpose of leadingout of them from a line-up, receipt of the hidden access and control; the use of cyberspace is for the feasance of acts of cyberterrorism, grant of financial and other support of terrorist activity; cybercrime which harms to the informative resources and results in considerable material losses; the use of cyberspace is for committing crime, related to the illegal conduct with decimators and other objects and matters, dangerous for life and health of people; a theft of sensible information is in political, economic or soldiery aims; reconnaissance-blasting activity is in a cyberspace by the feasance of difficult and hidden cyberattacks protracted, organised by other states.

Taking into account existence of the indicated threats, the first steps from the improvement of defence of critical infrastructure of Ukraine were done yet on implementation of row of decisions of NSDC of Ukraine, declared in 2016 - 2017 years. It mainly taken measures by domestic law enforcement authorities in relation to providing of safety, improvement of defence of critical infrastructure of Ukraine, neutralization of attempts to complicate functioning of OCI, doing of attempts of public nuisance impossible on her objects [4].

At the same time first in the days of independence accepted, Laws of Ukraine "On basic principles of providing of cybersecurity of Ukraine", "About a critical infrastructure", Conceptions of providing of the national system of firmness[2], Conception of creation of the state system of defence of critical infrastructure [5] but Order of forming of list of ITS of objects of critical infrastructure of the state [3], renewed Strategy of cybersecurity of Ukraine[3] accelerated the processes of forming of the national system of cybersecurity[4].

The law of Ukraine "On basic principles of providing of cybersecurity of Ukraine" (century 5) determines the wide list of subjects of providing of cybersecurity is President, Cabinet of Ministers, NSDC of Ukraine, that through the working organ the National co-ordinating center of cybersecurity[5] carries out co-ordination and control after activity of other subjects, and also row of state and non-state subjects which carry out providing of cybersecurity directly. In accordance with the century of a 8 Law and Strategy of cybersecurity of Ukraine, basis of the national system of cybersecurity is presented by SSSCIP, SSU, NPU, Ministry of defence and General Staff of AFU, National Bank of Ukraine, reconnaissance organs, on what fixed corresponding tasks.

At the same time taken measures system character was not yet purchased and did not provide complex counteraction to the threats, their neutralization and removal.

During a few last years the informative systems and resources of OCI of Ukraine constantly test cyberattacks from the side of controlled by the special services RF of hacker groupments and individuals [6]. A most danger was carried by cyberattacks on the automatic systems of remote-control of power and transport infrastructure of Ukraine [7, 8].

Within May-July, 2017 computer systems of some state financial institutions and many commercial structures in Ukraine have suffered the massed attack of the virus «WannaCry» and the net worm «Petya», which inventors demanded the considerable sum of means for restoration of access to information. In October, 2017 computer systems and networks have been attacked again with use of the viruses «Locky» and «Bad Rabbit» [4]. In January, 2018 hackers have cracked the server of the Head territorial administration of justice in Odessa region, and in April - a site of the Minenergovugleprom of Ukraine and state enterprise «Antonov».

In April - May, 2019 the state law enforcement agencies fixed cyberattacks from RF on the server of Central Election Commission of Ukraine. In November, 2019 by a command "CERT-UA" were blocked 11 DDoS-attacks on the web resources of the Office of President of Ukraine.

At the beginning of May, 2020 the CERT-UA team has blocked 9 DDoS-attacks to web resources of Office of the President of Ukraine. In August of this year the National coordination centre of cybersafety (NCCCS) at NSDC of Ukraine reported about preparation by hacker group «Armagedon» of the co-ordinated attack to information resources of the Ukrainian authorities and objects of critical information infrastructure on the eve of Independence Day of Ukraine. In September, 2020 hackers have cracked a site of NPU.

Anonymity and remoteness of access of cyberattacks promote them to wide application against Ukraine. The technical level of realization of cyberattacks on OCI grows constantly, new instruments and mechanisms of their feasance are perfected and developed. Acquires the global scale of the use of cyberspace terrorist organizations. International hacker groupments more

[2] Conception of providing of the national system of firmness, ratified by Decree of President of Ukraine from 27.09.2021 № 479/2021. URL: https://www.rnbo.gov.ua/ua/Ukazy/5017.html?PRINT.

[3] Strategy of cybersecurity of Ukraine, ratified by Decree of President of Ukraine from 26.08.2021 № 447/2021. URL: https://www.rnbo.gov.ua/ua/Ukazy/4974.html.

[4] The national system of cybersecurity is an aggregate of subjects of her providing and connected measures of defence of national informative resources, cyberdefence of objects of critical informative infrastructure (part 1 art. 8 Law of Ukraine is "About basic principles of providing of cybersecurity of Ukraine").

[5] Position about the National co-ordinating center of cybersecurity, ratified by Decree of President of Ukraine from 07.06.2016 № 242/2016 http://zakon2.rada.gov.ua/laws/show/242/2016.

frequent get the foreign special services for the sale of stocks of cyberinfluence[6].

4. DISCUSSION

Distribution of cyberathreats on all spheres of vital functions, related to functioning of OCI, and perfection of tool of their realization predetermines the necessity of change of strategy and tactic of counteraction in the conditions of sequel of hybrid war of Russian Federation against Ukraine [9, 10]. Principles of providing of safety of critical informative infrastructure of Ukraine require a revision.

Safety and security of OCI are certain in Ukraine one of base elements of the national system of firmness, the stable functioning of which must be provided: cybersecurity; security and trouble-free functioning of informative and of communication services; trouble-free energy-, water-, heat providing, supply of food; proof functioning of transport systems[7].

Therefore for the improvement of defence of critical informative infrastructure of Ukraine is considered expedient to accept such measures [11, p. 114; 12, p. 118]:

1) legislative is development and acceptance of normatively-legal acts in relation to determination of legal and organizational principles of introduction and functioning of the national system of firmness, in thereby. Strategies of defence of critical infrastructure of Ukraine; perfection of the normatively-legal adjusting of order of bringing in of law enforcement authorities is to work from warning, exposure and stopping of acts of cyberterrorism; strengthening of criminal responsibility is for illegal interference with work of objects of critical informative infrastructure;

2) organizational is creation of the effective national system of defence of critical informative infrastructure of Ukraine, co-ordination and management forces and backer-ups of her safety, in thereby: creation of national control system, introduction of standard operating procedures of кіберінцидентами for reacting on them for the estimation of criticism of events and priority of reacting; development of the National plan of reacting is on extraordinary (crisis) situations on OCI; introduction of risk-orientative approach is in relation to providing of кібербезпеки of OCI, development of methods of authentication and estimation of кіберризиків for the critical infrastructure of the state; creation of state register of OCI; an input is on permanent basis of estimation of the state of security of OCI and state informative resources on vulnerability; introduction of the system of obligatory audit of informative safety is on OCI, determination of mechanisms and base methods of realization of audits; deepening of international cooperation is in relation to providing of firmness of critical infrastructure;

3) technical is introduction of new algorithms of increase of level of cyberstability of the of communication and technological systems of OCI; creation of the system of certification of products, necessary for functioning and кіберзахисту of the of informatively-communication systems of OCI; providing of development of organizationally-technical model of cybersafety, systems of technical and cryptographic priv, introduction of domestic decisions is in relation to such types of priv; confession of priority of the use of facilities of such types of priv of domestic production is for кіберзахисту of state informative resources and OCII;

4) regime, reconnaissance, counterespionage and operative-investigation, sent to the decline of level of vulnerability of OKII to cyberthreats of military, criminal, terrorist and other character, in thereby: creation of the national system of exposure of cyberattacks, counteraction of terrorism and cyberespionage in relation to such objects; providing of permanent realization of measures is on an exposure, warning and stopping of reconnaissance-blasting activity of the foreign states, acts of cyberespionage and cyberterrorism, removal of their reasons and terms; an improvement of the analytical and criminalistics providing of counterespionage defence of cybersecurity of the state is by introduction of innovative methods of treatment and estimation of digital data, forming of electronic proofs; strengthening of possibilities of public organs in realization of secret verifications of ready of OKI condition to possible cyberattacks and cyberincidents for minimization of cyberthreats.

5. CONCLUSIONS

Thus, for Ukraine characteristic are lacks of the legal adjusting of functioning and defence of national critical informative infrastructure, imperfection of public policy in the sphere of her defence in the conditions of high risk of feasance of diversions and terrorist and cyberattacks on her objects. Therefore for organization of effective defence of OCII of Ukraine it is necessary to complete the process of forming of legislative ground of this activity, form the national system of defence of such objects, enter only methodology of providing of them stable functioning. It is also expedient to provide introduction of international standards of activity, adjusting of state-private partnership and development of international cooperation.

[6] Strategy of cybersecurity of Ukraine, ratified by Decree of President of Ukraine from 26.08.2021 № 447/2021. URL: https://www.rnbo.gov.ua/ua/Ukazy/4974.html.

[7] Conception of providing of the national system of firmness, ratified by Decree of President of Ukraine from 27.09.2021 № 479/2021. URL: https://www.rnbo.gov.ua/ua/Ukazy/5017.html?PRINT.

REFERENSES

[1] Ukraine became a ground for the hacker experiments of the special services of Russian Federation. Interview of Chairman of SSU V. Gricak to information agency of "Ukrinform", available at: http://ukrinform.ua/rubric-politics/ 2144501 - vasil - gricak - golova - sluzbi - bezpeki - ukraini.htm

[2] In Lithuania on governmental computers educed Russian spy software, available at: http://www.rbc.ua

[3] Order of forming of list of the information-telecommunication systems of objects of critical infrastructure of the state: decision of the Cabinet of Ministers of Ukraine from 23.08.2016 №563, available at: http://zakon 2.rada.gov.ua/laws/show/563-2016-p

[4] Another front. As Ukraine answers on calls which appeared in virtual space, available at: http://tyzhden.ua/publication/ 183407

[5] Conception of creation of the state system of defence of critical infrastructure, approved by the order of the Cabinet of Ministers of Ukraine from 06.12.2017 №1009-р, available at: http://zakon3.rada.gov.ua/laws/show/1009-2017-p

[6] In Ukraine disrobed the hackers of FSB, which carried out over 5 thousand cyberattacks on state organs, available at: https://ord - ua.com/2021/11/04/v - ukraini - vikrili - hakeriv - fsb - jaki - zdijsnili - ponad - 5 - tisjach - kiberatak - na - derzhorgani/

[7] Minenergougleprom promulgated a report on Russian cyberattack on oblenergo, available at: http://mpe.kmu.gov.ua/minugol/control/uk/publish /article?art_id=245086886&cat_id=35109.

[8] In Ukrenergo explained a scale failure in a grid under Kyiv of cyberattacks, available at: http://economics.unian.ua/energetics/ 1689781 - v - ukrenergo - poyasnili - masshtabniyzbiy - v - energosistemi - pid - kievom - kiber - atakami.html.

[9] Korystin, Oleksandr and Svyrydiuk, Nataliia (2020), “Methodological principles of risk assessment in law enforcement activity”, Nauka i Pravookhorona, vol. 3 (49), pp. 191-198, DOI: 10.36486/np.2020.3(49).19

[10] Kovalchuk, T.I. Korystin, O.Y. and Sviridyuk, N.P. (2019), “Hybrid threats in the civil security sector in Ukraine”, Problems of Legality, vol. 147, pp. 163-175, DOI: 10.21564/2414-990x.147.180550

[11] Melnyk, D.S. (2018), “In relation to the actual necessities of defence of national critical informative infrastructure of Ukraine”, *Issues of the day of management of the state informative safety: coll. theses of sciences. rep. scien.-practic. conf.* (Kyiv, 30.03.2018) [Electronic edition], NA SSU, Kyiv, Ukraina, p. 112 - 115.

[12] Melnyk, D.S. (2019), “National critical informative infrastructure of Ukraine: modern necessities of defence of her objects”, *Collection of scientific labours ON SSU*, no. 70, p. 111-119.