JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2020 December Volume 10 Number 2
http://doi.org/10.9770/jssi.2020.10.2(13)

ADMINISTRATIVE AND LEGAL SUPPORT OF CYBERSECURITY MANAGEMENT OF UKRAINE

Stanislav Zlyvko[1], Tetiana Pluhatar[2], Maksym Sykal[3], Olha Alieksieieva[4], Mykhailo Prokhorenko[5]

[1,3]Academy of the State Penitentiary Service, Honcha str. 34, Chernihiv, 14000, Ukraine*
[2,4]State Research Institute of the Ministry of Internal Affairs of Ukraine, Eugene Gutsal Lane, 4A, Kyiv, 01011, Ukraine
[5]National defence university of Ukraine named after Ivan Gherniakhovskyi,
Povitroflotskyy Avenue, 28, 03049, Kyiv, Ukraine

E-mail: [1]szlyvko@ukr.net (Corresponding author)*

Received 11 March 2020; accepted 25 October 2020; published 30 December 2020

Abstract. The essence of administrative and legal regulation of the activities of the subjects of the national cybersecurity system of Ukraine has been established, which consists in building an effective system for ensuring cybersecurity and requires from the state bodies of Ukraine a clear legal definition of the principles of state policy in this area and an advanced response to dynamic changes taking place in the world in the field of cybersecurity. The classifier of threats to the security of information resources has been improved, which, in contrast to the existing ones, is based on a synergetic model of threats, which allows to classify threats by security components, types of services, and hierarchy levels of the infrastructure of automated systems, to assess the synergy and hybridity of threats to information security, cybersecurity, information security, and the likelihood of their impact on the security of information resources. It has been proved that the choice of specific means and ways of ensuring the cybersecurity of Ukraine is conditioned by the need to take timely measures adequate to the nature and scale of real and potential cybernetic threats to the vital interests of a person and citizen, society and the state. The purpose of the cybersecurity system of Ukraine has been clarified. The task of the cybersecurity system is to create the necessary conditions in cyberspace, under which it is possible to achieve national goals and realize the interests, tasks, and goals of its elements.

Keywords: cybersecurity; information security; administrative and legal regulation; cyberspace; classifier

Reference to this paper should be made as follows: Zlyvko, S., Pluhatar, T., Sykal, M., Alieksieieva, O., Prokhorenko, M. 2020. Administrative and legal support of cybersecurity management of Ukraine. *Journal of Security and Sustainability Issues* 10(2): 533-546. http://doi.org/10.9770/jssi.2020.10.2(13)

JEL Classifications: F35; F42

1. Introduction

Ukraine's national security, its economic prosperity, and social and information well-being increasingly depend on the availability, integrity, and confidentiality of information resources, which are provided by information and communication technologies, or in a broader sense - cyberspace. At the same time, the growing dependence on information technologies makes modern Ukrainian society more vulnerable to the possible negative consequences of illegal use of cyberspace. Every year the number of cyber attacks and various cyber incidents grows in the most important spheres of life of our state.

Under these conditions, one of the main tasks of the state is to take proactive measures that will create guaranteed conditions for the realization of national interests in cyberspace. One of the directions of realization of this task consists in the formation of backup copies (backups) of information resources of the state and also the formation of the effective national system of cybersecurity, including the support of cybersecurity systems, which will fundamentally reduce (and sometimes completely prevent) the consequences of cyberattacks, as well as create conditions for timely forecasting of the implementation of certain cyber incidents.

In recent decades, the development of information and communication technologies (ICT), cybernetics, and the Internet has led to significant changes in society. The Internet has brought great social benefits to the world for many forms of activity. These profits have become significant for people, business, the state, and society as a whole. Today, information and communication technology systems are integrated into all aspects of society and are critical to its functioning. Cyberspace and technology have become the basis for interaction between different sectors, both public and private, and can be considered a fundamental social infrastructure.

However, along with many benefits, there are a significant number of threats associated with the functioning of modern technology. This phenomenon has led to a significant number of dangers that affect society both nationally and internationally. Thus, there is a need for mechanisms to protect cyberspace, which are described in the national strategies of world powers, which in turn are dedicated to ensuring its protection. Therefore, a very important topic is the study of implementation mechanisms to ensure a cybersecurity strategy, initially at the international level, as it will help in further understanding of this phenomenon. It will also be useful in gaining valuable experience for the formation and implementation of mechanisms to ensure cybersecurity in Ukraine.

Cyberspace has been the cause of social and economic growth due to its openness and accessibility for all actors. Excessive administration and regulation of cyberspace reduce its benefits and can hinder active growth in all areas of activity. Therefore, it is very important to ensure openness and interaction in the cyber network, as well as to maintain and develop the secure and reliable cyberspace to create a free flow of information. This will ensure freedom of expression and active economic activity in cyberspace, promote innovation, economic growth, and the solution of social problems, and provide positive benefits that will be available to the world community. Every country in the world, as well as business structures, enjoy the benefits of expanding cyberspace. As a result, cyber threats have become a reality, they are transcontinental in nature, and the consequences of their interventions in critical infrastructures have become more severe.

Cybersecurity expands the scope of traditional IT security to cover the entire cyberspace. The latter covers all information technologies that connect to the Internet or similar networks, including cyberspace communications, programs, processes, and processed information. Thus, for all intentions and purposes, modern information and communication technologies become part of cyberspace.

The purpose of the work is to determine the essence, features, and system of administrative and legal regulation of cybersecurity of Ukraine on the basis of the analysis of the current legislation of Ukraine, historical, modern scientific sources, as well as to formulate proposals and recommendations for improving its functioning.

2. Literature Survey

Cybersecurity policy is emerging area of scientific research (e.g. Šišulák, S. (2017); Limba, T., Stankevičius, A. & Andrulevičius A. (2019); Plėta, T., Tvaronavičienė, M., & Della Casa, S. (2020); Plėta, T., Tvaronavičienė, M., Della Casa, S., & Agafonov, K. (2020); Tvaronavičienė, M., Plėta, T., Della Casa, S., & Latvys, J. (2020)).

In general, the essence of cybersecurity policy in the context of legal sciences can be viewed from the standpoint of three main aspects:

1) it acts as part of the state legal policy - the effective implementation by citizens of their rights and freedoms in the cyber sphere, effective norms, which govern public relations in the cyber sphere are an integral element (Sabillon, R., Cavaller, V., & Cano, J. (2016), Aliyeva, L. M., & Hwang, G. H. (2019));

2) it acts as a part of state security policy - the level of cybersecurity directly determines, under the current conditions of digitalization of society, the level of national, regional, international, and global security (Carr, M. (2016), Kolini, F., & Janczewski, L. (2017))

3) it acts as a part of the state information policy (SIP) (Pernik, P., Wojtkowiak, J., & Verschoor-Kirss, A. (2016), Herrera, A. V., Ron, M., & Rabadão, C. (2017)) aimed at the formation of an effective information society, ensuring information security, ensuring the implementation of information human rights and freedoms, forming mechanisms for the information balance of the interests of the individual, society, and the state; strengthening

ties and interaction between the managers and the managed; organization of effective information interaction between institutions of the state and civil society (Slipachuk, L., Toliupa, S., & Nakonechnyi, V. (2019)).

Consequently, today the Ukrainians face the danger of implementing destructive cyberwar scenarios regardless of whether this is perceived by the scientific community or not; whether this is reflected in the corresponding indicative excitement of scientific interest in this topic or not, or legitimized by the concept of cyberwar in national legislation or not.

It is such wars that give rise to the formation of a new cyber-supremacy with its inherent cyber culture, cyber-civilization, cyber-economy, cyber-economy, and artificial intelligence, etc, and in general - a new cyber world, a new cyber world order (Galinec, D., Moznik, D., & Guberina, B. (2017)). Therefore, when analyzing the state of scientific research, the author relied on the adequacy of response to these tendencies, and the descriptions were not made from the standpoint of slashing criticism, and not denial of the existing order, accepting and perceiving reality as it really is: whether someone likes it or not, whether it fits into the canons of information-legal and security science or not (Tiirmaa-Klaar, H. (2016), Shackelford, SJ (2016)).

3. Methods

General and specific scientific methods were used: systemic and structurally functional approaches, which made it possible to determine the essence, structure, functions, and special features of support of the cybersecurity and information security; comparison method – in order to identify common and distinctive features in ensuring the cybersecurity of world states, providing mechanisms for the implementation of various cybersecurity strategies, as well as cybersecurity of Ukraine. In order to assess the features of the functioning of the mechanisms, the following methods were used: the analytical method, which provided the identification of the existing situation for the implementation of cybersecurity strategies and mechanisms for their implementation. The research conducted is based on theoretically grounded and practically tested methods of set theory, probability theory and mathematical statistics, system analysis, and laws of synergy.

To construct threat metrics based on the synergetic approach proposed in the works (Reznik, O, et al. (2017)), the authors use the approach of constructing a threat classifier based on the information-analytical model of the double triplets method proposed by the authors in the works (Reznik, O, et al. (2020)). In contrast to what is known in the construction of the classifier, the content of each of the four platforms includes a number of components, respectively.

The normative basis of the work includes the Constitution of Ukraine, international legal acts ratified by Ukraine, laws of Ukraine, acts of the President of Ukraine and the Cabinet of Ministers of Ukraine, normative acts of central executive bodies, local self-government bodies that determine the content and features of administrative and legal regulation of cybersecurity in Ukraine.

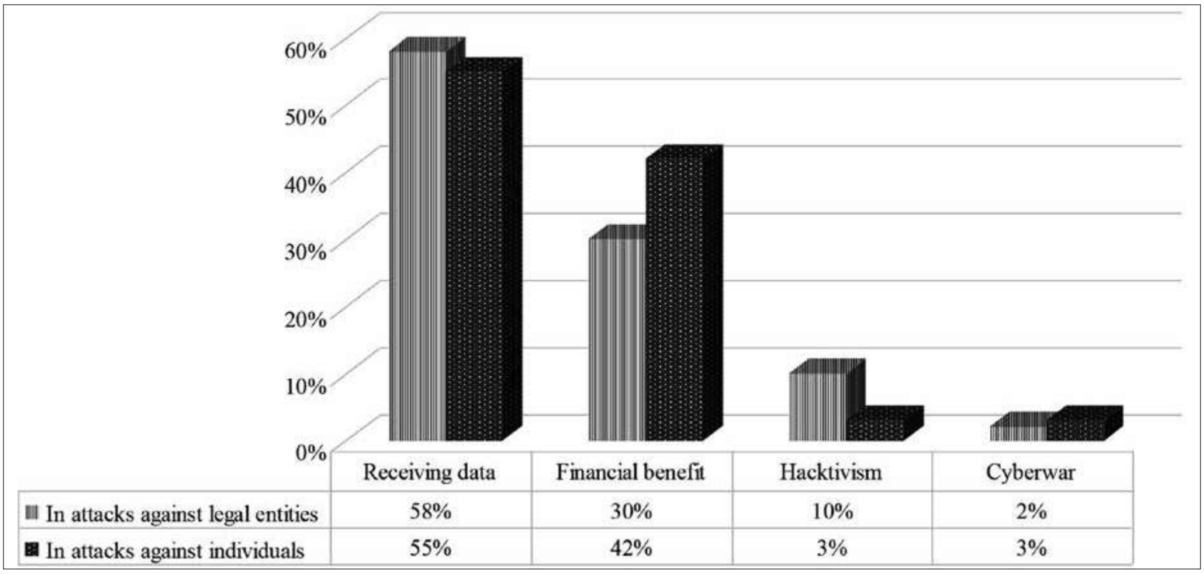
4. Results

The development of society at the beginning of the XXI century is characterized, first of all, by the transition from an information society to a society of high technologies, which provide oversaturation with the latest information and communication technologies, the further development of globalization processes in the modern economy, the dynamics of informatization of such areas of society as the communications sector, energy, transport, oil and gas production and storage system, financial and banking systems, defense and national security, structure for ensuring the stable operation of central executive authorities, widespread transition to electronic management and document management methods.

Secondly, the information processes taking place throughout the world highlight the most important task of ensuring the security of information. This is due to the special importance for the development of the state of its information resources, the growth in the cost of information in market conditions, its high vulnerability, and often significant losses as a result of its unauthorized use.

Thirdly, the rapid development of the Internet and other information and communication technologies forms a global information space that allows creating new threats and new forms of international conflicts, including information wars, network confrontations, hacker attacks, etc. The development of computer technologies and information and telecommunication networks provide great opportunities for society, while at the same time giving rise to a new type of crime - cybercrime.

Information theft remains a priority target for most cyber attacks in Ukraine (Figure 1). As for the financial gain, cybercriminals pursue it in 30% and 42% of attacks on legal entities and individuals, respectively. The high share of financially motivated attacks on individuals is explained by regular mass infections with malicious software with obtrusive advertising (including on mobile devices), infection by miners, and other software on dubious websites, as well as ransomware campaigns, during which criminals threaten to distribute compromising information about a person.

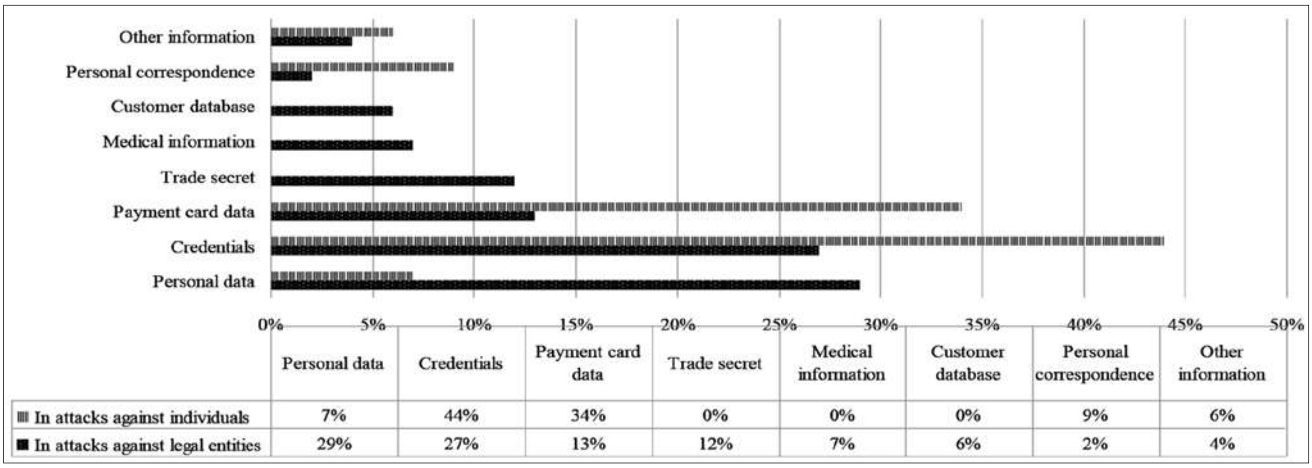


	Receiving data	Financial benefit	Hacktivism	Cyberwar
▥ In attacks against legal entities	58%	30%	10%	2%
■ In attacks against individuals	55%	42%	3%	3%

Figure 1. Motives of criminals in 2019 in Ukraine

Source: compiled on the basis https://cybersecurity.ciseventsgroup.com/

Cybercriminals are most often interested in personal and credentials when they attack legal entities (Figure 2). This is not surprising since companies can store large databases of both personal and customer credentials. In addition, attackers may be interested in the credentials of the employees of the victim company.



	Personal data	Credentials	Payment card data	Trade secret	Medical information	Customer database	Personal correspondence	Other information
▥ In attacks against individuals	7%	44%	34%	0%	0%	0%	9%	6%
■ In attacks against legal entities	29%	27%	13%	12%	7%	6%	2%	4%

Figure 2. Types of stolen data in 2019 in Ukraine

Source: compiled on the basis https://cybersecurity.ciseventsgroup.com/

Accounts on social networks are also under threat, especially if the account is well promoted, that is, it has many subscribers. Users, in turn, do not always care about the security of their accounts: they use unstable and identical passwords, enter credentials without making sure the resource is reliable, and give out information about themselves that can help to find a password. This explains the high proportion of stolen credentials (44%) in attacks on individuals. For example, the category of people entering the zone of increased risk of attacks from hackers includes fans of computer games. For example, in the second quarter of 2019, cybercriminals lured Steam users to web resources where supposedly they could get a new game for free by entering their Steam account credentials. In addition, gamers can fall for the bait of malefactors on specialized forums. So, under the guise of cheat codes packed in a ZIP archive, several web resources distributed a Trojan for mining the TurtleCoin cryptocurrency.

Customers' bank card details and payment information are usually protected by cryptographic methods, so it is easier for attackers to learn it using social engineering methods directly from the customer. As a result, 34% of data stolen as a result of attacks on individuals is their bank card details.

In the second quarter of 2019, the share of targeted attacks increased significantly compared to the first quarter and amounted to 59% (in the first quarter - 47%). The share of cyber incidents, as a result of which individuals suffered, was 24%. Among legal entities (Figure 3), cybercriminals most often attacked government organizations, industrial companies, medical organizations, banks, and other organizations in the financial sector. In the second quarter, there are supply chain attacks on large IT companies with a large number of clients from various industries, so some attacks are considered in more detail below.

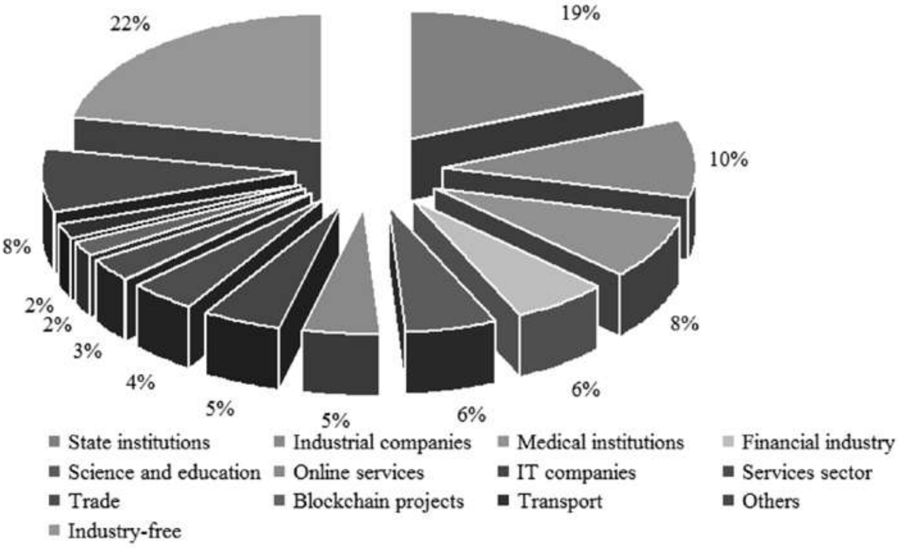


Figure 3. Categories of victims among legal entities in 2019 in Ukraine

Source: compiled on the basis https://cybersecurity.ciseventsgroup.com/

Security models play an important role in the development and research of secure computer systems, including automated systems (AS). The models provide a system-technical approach that includes the solution of the most important tasks: the choice and justification of the basic principles of the architecture of the AS, which determine the mechanisms of implementation of means and methods of information protection; confirmation of the properties (security) of the developed systems by formally proving compliance with the security policy (requirements, conditions, criteria); drawing up a formal specification of the security policy as the most important part of the organizational and documentation support of the developed secure computer systems. The principles of constructing a classifier of threats of the components of information resource security are formalized at the national level: information security (IS), cybersecurity (CS), information security (IS).

Formation of metric coefficients of threats by experts on security services. I-services of information resources security (IRS). The main security services of IRS are K - confidentiality; S - integrity; D - availability; A - authenticity. Then the classifier for the four security services is described by the expression of the form $i=\{K,S,D,A\}$. The classifier contains M threats. K experts took part in compiling the weights of manifestation of each threat to IRS security services.

Denote by j the current number of the threat $(\{j\}_i^M)$, by n - the current number of the expert who performed the assessment $(\{n\}_i^N)$. The average value of the expert assessment of all threats to a particular security service can be recorded:

$$v^i = \frac{1}{N}\sum_{j=1}^{M}\sum_{n=1}^{N} v_{jn}^i \tag{1}$$

where v_{jn}^i - the value of the metric coefficient set by the n-th expert for the j-th threat of the i-th security service; M-number of threats; N - number of experts.

Formation of threat identifiers according to the components of the classifier. In this step, the experts generate a digital value (code) of the threat identifier for the relevant components of the classifier.

The choice of weights w_j that determine the conditions of the manifestation of the j-th threat (Table 1).

Table 1. Table of choice of weights of manifestation of the j-th threat depending on the condition of its manifestation

Weights w_j	Conditions of the manifestation of the threat
0,067	the threat manifests no more than once every 5 years
0,133	the threat manifests no more than once a year
0,2	the threat manifests no more than once a month
0,267	the threat manifests no more than once a week
0,333	the threat manifests daily

Source: author’s development

Determining the implementation of each j-th threat, taking into account the probability of an attack (its occurrence) (P_j^i) is carried out by the expression:

$$v_j^i P_j^i = \frac{1}{N} P_j^i \sum_{n\sphericalangle=1}^{M} v_{jn}^i \infty \tag{2}$$

For each security service and j-th threat, it is calculated according to formula (2).

Confidentiality service:

$$v_j^K w_j^K = \frac{1}{N} w_j^K \sum_{n=1}^{M} v_{jn}^K \tag{3}$$

Integrity service:

$$v_j^S w_j^S = \frac{1}{N} w_j^S \sum_{n=1}^{M} v_{jn}^S \tag{4}$$

Availability service:

$$v_j^D w_j^D = \frac{1}{N} w_j^D \sum_{n=1}^{M} v_{jn}^D \qquad (5)$$

Authenticity service:

$$v_j^A w_j^A = \frac{1}{N} w_j^A \sum_{n=1}^{M} v_{jn}^A \qquad (6)$$

where $v_{jn}^K, v_{jn}^S, v_{jn}^D, v_{jn}^A$ - expert weights of security services: confidentiality, integrity, accessibility, authenticity;

$v_j^K, v_j^S, v_j^D, w_j^A$ - weighting factor of security service: confidentiality, integrity, accessibility, authenticity of the j-th threat attack.

Determining the implementation of several threats to the selected service is calculated taking into account the expression (3-6):

Confidentiality service:

$$V_{synerg}^K = \sum_{i=1}^{L} v_j^K w_j^K \qquad (7)$$

Integrity service:

$$V_{synerg}^S = \sum_{i=1}^{L} v_j^S w_j^S \qquad (8)$$

Availability service:

$$V_{synerg}^D = \sum_{i=1}^{L} v_j^D w_j^D \qquad (9)$$

Authenticity service:

$$V_{synerg}^A = \sum_{i=1}^{L} v_j^A w_j^A \qquad (10)$$

where L is the number of several threats that are selected by the expert from the set $(\{j\}_i^L)$ that is a subset of the whole set of threats of the classifier, ie $L \leq M$.

When forming metric coefficients, it is assumed that the results obtained belong to independent threats. In case of their dependence (coincidence of the threat classifier), it is necessary to use the expression to determine the full probability of dependent events: P(HB) = P(H) + P(B)-P(AB).

Statistical processing of the results of the assessment of the possibility of the impact of the j-th threat on security services at the national level is carried out according to the following analytical algorithm:

$$y_i = \frac{\sum_{n=1}^{N} y_n \times n_n}{N} \qquad (11)$$

where y_n - the assessment of the n-th expert of the impact of the j-th threat; n_n - the level of competence of the expert; N - number of experts.

The degree of consistency of experts' opinions is the variance calculated by the expression:

$$z_y^2 = \frac{1}{N}\sum_{n=1}^{N} n_n (y_k - y_j)^2 \tag{12}$$

The statistical significance with $1-w_j$ probability is: $[y_j - \Delta, y_j + \Delta]$, where the value y_j is distributed according to the normal law with the center in y_j and variance z_y^2. Then Δ is determined by the expression:

$$\Delta = t\sqrt{z_y^2 / M} \tag{13}$$

where t is the value that follows the Student's distribution for M-1 degrees of freedom, M is the number of experts.

$$\Delta = t\sqrt{z_y^2 / M} \tag{14}$$

Determination of the total threat on the security components, taking into account the expression (7-10) is calculated:

$$\begin{cases} V_{\sin erg}^{IB} = \sum_{j=1}^{M} (v_j^K \cap v_j^S \cap v_j^D \cap v_j^A) w_j \\ V_{\sin erg}^{KB} = \sum_{j=1}^{M} (v_j^K \cap v_j^S \cap v_j^D \cap v_j^A) w_j \\ V_{\sin erg}^{BI} = \sum_{j=1}^{M} (v_j^K \cap v_j^S \cap v_j^D \cap v_j^A) w_j \end{cases} \tag{15}$$

Identification of the generalized synergistic threat to the IRS:

$$V_{\sin erg}^{IB,KB,BI} = V_{\sin erg}^{IB} \cup V_{\sin erg}^{KB} \cup V_{\sin erg}^{BI} \tag{16}$$

Determination of the generalized synergetic threat taking into account its hybridity is calculated:

$$V_{\sin erg}^{hybrid\ K,S,D,A} = V_{\sin erg}^{K} \cap V_{\sin erg}^{S} \cap V_{\sin erg}^{D} \cap V_{\sin erg}^{A} \tag{17}$$

The results of studies of threats with the maximum frequency of their manifestation on the IRS are shown in Table 2.

Table 2. Results of the threat assessment based on a synergetic approach

Components of the security	Security services				
	K, V_{synerg}^{K}	S, V_{synerg}^{S}	D, V_{synerg}^{D}	A, V_{synerg}^{A}	Result
IB, $V_{\sin erg}^{IB}$	0,023	0,223	0,193	0,207	0,0002
KB, $V_{\sin erg}^{KB}$	0,222	0,234	0,197	0,134	0,0014
BI, $V_{\sin erg}^{BI}$	0,226	0,109	0,152	0,189	0,0007
Result	0,471	0,566	0,542	0,53	X
$V_{\sin\ erg}^{IB,KB,BI} = V_{\sin\ erg}^{IB} \cup V_{\sin\ erg}^{KB} \cup V_{\sin\ erg}^{BI} = = 0.0002 + 0.0014 + 0.0007 = 0.0223$					$V_{\sin\ erg}^{hybrid\ K,S,D,A} = V_{\sin\ erg}^{K} \cap V_{\sin\ erg}^{S} \cap V_{\sin\ erg}^{D} \cap V_{\sin\ erg}^{A} = = 0{,}471 \times 0{,}556 \times 0{,}542 \times 0{,}53 = 0{,}0766$

Source: author's research

Practical implementation makes it possible to form an on-line expert assessment of IRS threats, analyze their synergy and hybridity, assess the likelihood of the impact of these threats on IRS security without significant investment and human resources costs.

One of the most important tasks for the optimal construction of an integrated information protection system is to choose from a variety of tools such a set, which will ensure the neutralization of all possible information threats with the best quality and the lowest possible resource consumption. Information protection (IP) tasks are most effectively solved within the framework of a preventive protection strategy when at the design stage potential threats are assessed and protection mechanisms against them are implemented. At the same time, when designing IP systems, the developer, not having statistical data on the results of the functioning of the system being created, is forced to make a decision on the composition of the IP complex, being in conditions of significant uncertainty.

The construction of models while designing or modernizing the information security system is carried out in a natural way by solving problems of analysis and design with minimal costs and high efficiency. Thus, at the analysis stage, the information security system model is used to study each function (operation) performed in order to discover, for example, what information and what resources each employee should have access to while on duty.

Thus, as a result of the study, we can see that the state policy of cybersecurity is determined taking into account the priority of national interests and threats to the cybersecurity of Ukraine and is carried out through the implementation of relevant concepts, doctrines, strategies, and programs in various spheres of life in accordance with current legislation.

The state cybersecurity policy consists of two main interrelated blocks:

1) the activity of exclusively state bodies;

2) the activity of non-state institutions, civil society institutions, information society in the information sphere.

It is proposed to legitimize the “cybernetic society” category in legislative acts, that is, a society in which activity is based on the use of services using the achievements of cybernetics.

The main goal of the state cybersecurity policy of cybersecurity is to manage real and potential cyberthreats and dangers in order to create the necessary conditions to meet the cybernetic needs of a person and citizen, as well as to realize national interests in the cybernetic sphere.

The directions of the state policy of cybersecurity should be determined as: ensuring the cybernetic sovereignty of Ukraine; systematization of information (cybersecurity) legislation of Ukraine, creation of the necessary prerequisites for the development of the cyber sphere in general, as well as ensuring cybersecurity in particular; engaging the mass media to counter cyber threats; ensuring the existence of the rule of law; taking comprehensive measures to protect the national cyberspace and counter the monopolization of the cyber sphere of Ukraine. It should be emphasized that the list of directions of state cybersecurity policy cannot be static since there are constant changes in cyberspace.

Therefore there is a need for a quick response and the possibility of taking appropriate measures. Thus, in the Annual Address of the President of Ukraine to the Verkhovna Rada of Ukraine “On the Internal and External Situation of Ukraine in 2016”, the following most relevant steps for this perspective were identified:

1) development of a list of critical infrastructure facilities and the formation of clear and understandable rules for the protection of such facilities based on consensus in the business sector;

2) not just the willingness to cooperate with civil society on the development of cybersecurity but the institutionalization of such cooperation;

3) increased attention to cybersecurity issues in the Armed Forces. This is one of the priorities for the develop-

ment of the security and defense sector, which must be fully ensured both at the operational-tactical level and at the national level;

4) further strengthening of the capabilities of the security and defense sector to ensure comprehensive cybersecurity of the state, expressed in stimulating the training of professional personnel, increasing the material interest for cybersecurity specialists in working for state structures, optimizing the organizational model for managing the cybersecurity sector.

However, in 2017, in the Annual Address of the President of Ukraine to the Verkhovna Rada of Ukraine "On the Internal and External Situation of Ukraine in 2017", other priorities were highlighted:

solving the problem of limited access information exchange between Ukraine and NATO (Administrative Arrangements On The Protection Of Restricted Information Between The Government Of Ukraine And The Organization Of The North Atlantic Agreement (2016)): a legal basis has been created and detailed procedures for the mutual protection of information with limited access, which will be transmitted or created in the course of cooperation, are determined (On termination of the Agreement between the Cabinet of Ministers of Ukraine and the Government of the Russian Federation on cooperation in the field of television and radio broadcasting and the Agreement between the Cabinet of Ministers of Ukraine and the Government of the Russian Federation on cooperation in the field of information (2016)). Ensuring the equal and partner-like nature of relations in the process of information exchange will help to increase the effectiveness of mutually beneficial cooperation between Ukraine and NATO;

termination of intergovernmental agreements with the Russian Federation on cooperation in the field of television, radio broadcasting and information, is due to the fact that their further action does not correspond to the state of interstate relations and is not consistent with the measures, which Ukraine uses to ensure the protection of its information field from negative information and psychological influences (On termination of the Agreement between the Cabinet of Ministers of Ukraine and the Government of the Russian Federation on cooperation in the field of television and radio broadcasting and the Agreement between the Cabinet of Ministers of Ukraine and the Government of the Russian Federation on cooperation in the field of information (2016));

improving the procedure for the application of sanctions by the National Council of Ukraine on television and radio broadcasting and expanding the list of grounds for reissuing a license (Law Of Ukraine On Amendments to the Law of Ukraine "On Television and Radio Broadcasting" (2016)), which is aimed at ensuring an effective mechanism for exercising supervision in the field of television and radio broadcasting. The ultimate goal of the adopted changes is the protection of the information space of the state, the possibility of timely response to identified threats and counteraction to them;

depriving the Russian special services of the opportunity to track out the citizens of Ukraine by blocking the corresponding sites (VKontakte attendance in 5 days fell by 3 million visits (2017)) (sanctions against legal entities Yandex, Mail.ru Ukraine, VKontakte, Odnoklassniki, etc.) (On the decision of the National Security and Defense Council of Ukraine of April 28, 2017 "On the application of personal special economic and other restrictive measures (sanctions)").

Although this step has caused mixed assessments of experts and the general public, the main reason for the disagreement over the sanctions was the lack of prior communication by the state of the steps being taken. However, it is necessary to understand that blocking sites and services belongs to the field of security but not freedom of speech and was recognized by Ukrainian partners from the EU and international organizations (NATO). This thesis acquires particular significance in the context of recent examples of the use of BigData in the electoral process.

5. Discussion

The exceptionally challenging tasks facing the state on the way to protect its institutions, society, and citizens from criminal encroachments on their rights and freedoms in the information and communication space require an integrated approach to working with specialists who, in their professional activity, are called upon to ensure cybersecurity. This approach must have a comprehensive scientific basis.

Unlike traditional education, the formation processes take place not only in the educational environment of the higher education institution but also in teams where the applicant for higher education undergo practical training and internships, communicating with experienced specialists in the field of cybersecurity, while perceiving, analyzing, and interpreting information, which is obtained by a future professional in informal communities, in the media space, and in the mass media.

Based on the foregoing, we come to the conclusion that with the state approach, it would be necessary to introduce a practice in which the formation of a cybersecurity specialist did not begin at the student hood but through the search and support of talented children and youth by universities, future employers, even during their studies in a secondary school, a specialized lyceum, and in children's art houses.

Thus, we are faced with the task of establishing how the legal and organizational principles determine the process of formation and development of a future cybersecurity specialist.

Of course, we understand that the legal regulation process of the formation of the cybersecurity specialist is indirect since the laws and by-laws of Ukraine are aimed at the activities of all higher educational institutions and not only those that train these specialists. This means that, on the one hand, the general legal basis for the training of the cybersecurity specialist, like any other applicant for higher education, is the laws of Ukraine "On Education", "On Higher Education", and on the other hand, a number of normative legal acts including international, which regulate the activity of authorized entities in the field of transnational, national, information, and cybersecurity.

The training of highly qualified personnel was and remains a key element of the full-fledged life of the state. This process is characterized by a combination of the needs of society with technologies of didactic design, followed by consolidation at the level of regulatory legal acts. Since the training and advanced training of cybersecurity specialists is a relatively new type of activity, there is a need for a scientific substantiation of these areas from the standpoint of a systematic approach.

The directions of improvement of legal regulation of professional activity of subjects of cybersecurity policy are determined: improvement according to the established procedures and in accordance with theoretical achievements, taking into account the above-stated Law of Ukraine "On the basic principles of ensuring cybersecurity of Ukraine"; creation of a thesaurus of cybersecurity terminology and its legitimization in the text of relevant laws; harmonization of legislation on a single vision of the range of subjects who are entrusted with the responsibilities of ensuring national, including cybersecurity, defining, and implementing national and international cybersecurity policies; introduction of provisions on the role and place of scientific institutions, higher educational institutions in the study of cybersecurity problems, the formation of cybersecurity policy based on scientifically grounded principles into the existing normative legal acts.

Conclusions

The essence of administrative and legal regulation of the activities of the subjects of the national cybersecurity system of Ukraine has been established, which consists in building an effective system for ensuring cybersecurity and requires from the state bodies of Ukraine a clear legal definition of the principles of state policy in this area and a proactive response to dynamic changes, which occurr in the world in the field of cybersecurity. Choice of specific means and ways of ensuring the cybersecurity of Ukraine is conditioned by the need for timely adoption of measures, which are adequate to the nature and scale of real and potential cybernetic threats to the vital interests of individuals and citizens, society, and the state.

The concept for constructing a synergistic model of threats to the security of information resources has been developed, the basis of which is a three-level model of strategic management of information technology security. The concept covers all the main directions of development of the country's activity for the security of information resources, is based on a synergetic approach to the selection of the most effective directions for achieving the goals of information resources security at each level of the management model of strategic management of information technology security, taking into account the magnitude of risk at each level and ensuring effective control over the implementation of the functions of the information security management system.

Through a consistent analysis of the state and directions, educational standards of training and advanced training of specialists in the field of cybersecurity, as well as qualification requirements for them, the directions of administrative and legal regulation of cyber education in Ukraine are determined. It is established that the concept of assessment of specialists is interdisciplinary and has a complex character. Only under condition of the implementation of a systematic approach, the correct choice of methods and technologies of assessment, the most optimal use of assessment as a means of forming and improving the professional activity of a cybersecurity specialist is possible. It is emphasized that at present the issues of the professional activity of subjects of cybersecurity policy are outside the sphere of state regulation.

References

Administrative Arrangements On The Protection Of Restricted Information Between The Government Of Ukraine And The Organization Of The North Atlantic Agreement (2016). Available at: https://zakon.rada.gov.ua/laws/show/950_035-16?lang=en#Text

Aliyeva, L. M., & Hwang, G. H. (2019). The Model to Implement the Cyber Security Policy and Strategy for Azerbaijan Information System. Journal of digital convergence, 17(5), 23-31. Available at: https://www.koreascience.or.kr/article/JAKO201915561988838.page

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 2016". Kyiv: NISD, 2016. 688 p. Available at: https://niss.gov.ua/sites/default/files/2016-10/poslanya_new-cc2e3.pdf

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43-62. Available at: https://academic.oup.com/ia/article-abstract/92/1/43/2199930

Cyber Security Ukraine 2019. Available at: https://cybersecurity.ciseventsgroup.com/

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije, 58(3), 273-286. Available at: https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=299324

Herrera, A. V., Ron, M., & Rabadão, C. (2017, June). National cyber-security policies oriented to BYOD (bring your own device): Systematic review. In 2017 12th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-4). IEEE. Available at: https://ieeexplore.ieee.org/abstract/document/7975953

Kim, K., Kim, I., & Lim, J. (2017). National cyber security enhancement scheme for intelligent surveillance capacity with public IoT environment. The Journal of Supercomputing, 73(3), 1140-1151. Available at: https://link.springer.com/article/10.1007/s11227-016-1855-z

Kolini, F., & Janczewski, L. (2017). Clustering and topic modelling: A new approach for analysis of national cyber security strategies. In Pacific Asia Conference on Information Systems (PACIS). Association For Information Systems. Available at: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1160&context=pacis2017

Law Of Ukraine On Amendments to the Law of Ukraine "On Television and Radio Broadcasting" (2016). Available at: https://zakon.rada.gov.ua/laws/show/1715-19?lang=en#Text

Limba, T., Stankevičius, A. & Andrulevičius A. (2019). Cryptocurrency as disruptive technology: theoretical insights, Entrepreneurship and Sustainability Issues 6(4): 2068-2080. http://doi.org/10.9770/jesi.2019.6.4(36)

On termination of the Agreement between the Cabinet of Ministers of Ukraine and the Government of the Russian Federation on cooperation in the field of television and radio broadcasting and the Agreement between the Cabinet of Ministers of Ukraine and the Government of the Russian Federation on cooperation in the field of information (2016). Available at: https://zakon.rada.gov.ua/laws/show/1053-2016-п#Text

On the decision of the National Security and Defense Council of Ukraine of April 28, 2017 "On the application of personal special economic and other restrictive measures (sanctions)". Available at: https://www.president.gov.ua/documents/1332017-21850

Pernik, P., Wojtkowiak, J., & Verschoor-Kirss, A. (2016). National cyber security organisation: United States. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. Available at: https://afyonluoglu.org/PublicWebFiles/NATO/USA-National%20CyberSecurity%20Organization-2015%20Dec.pdf

Plėta, T., Tvaronavičienė, M., & Della Casa, S. (2020). Cyber effect and security management aspects in critical energy infrastructures. Insights into Regional Development, 2(2), 538-548. https://doi.org/10.9770/IRD.2020.2.2(3)

Plėta, T., Tvaronavičienė, M., Della Casa, S., & Agafonov, K. (2020). Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases. Insights into Regional Development, 2(3), 703-715. https://doi.org/10.9770/IRD.2020.2.3(7)

Reznik, O., Getmanets, O., Kovalchuk, A., Nastyuk, V., Andriichenko, N. (2020). Financial security of the state. Journal of Security and Sustainability Issues, 9(3), 843-852. https://doi.org/10.9770/jssi.2020.9.3(10)

Reznik, O.M., Klochko, A.M., Pakhomov, V.V., Kosytsia, O.O. (2017) International aspect of legal regulation of corruption offences commission on the example of law enforcement agencies and banking system of Ukraine. Journal of Advanced Research in Law and Economics. 8(1), 169-177.

Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: global trends in cyberspace. International Journal of Computer Science and Software Engineering, 5(5), 67.

Shackelford, S. J. (2016). Protecting intellectual property and privacy in the digital age: the use of national cybersecurity strategies to mitigate cyber risk. Chap. L. Rev., 19, 445. Available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/chlr19&div=26&id=&page=

Šišulák, S. (2017). Userfocus - tool for criminality control of social networks at both the local and international level, Entrepreneurship and Sustainability Issues 5(2): 297-314. http://doi.org/10.9770/jesi.2017.5.2(10)

Slipachuk, L., Toliupa, S., & Nakonechnyi, V. (2019, July). The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine. In 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT) (pp. 451-454). IEEE. Available at: https://ieeexplore.ieee.org/abstract/document/8847877

Tiirmaa-Klaar, H. (2016). Building national cyber resilience and protecting critical information infrastructure. Journal of Cyber Policy, 1(1), 94-106. Available at: https://www.tandfonline.com/doi/abs/10.1080/23738871.2016.1165716

Tvaronavičienė, M., Plėta, T., Della Casa, S., & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania. Insights into Regional Development, 2(4), 802-813. http://doi.org/10.9770/IRD.2020.2.4(6)

Vkontakte attendance in 5 days fell by 3 million visits (2017). Available at: https://www.epravda.com.ua/rus/news/2017/05/23/625156/

Short biographical note about the contributors at the end of the article:

Stanislav ZLYVKO, Doctor of Sciences (Law), Professor, Academy of the State Penitentiary Service, Ukraine
ORCID ID: orcid.org/0000-0003-2732-3144

Tetiana PLUHATAR, Candidate of Science of Law, Senior researcher, State Research Institute of the Ministry of Internal Affairs of Ukraine
ORCID ID: orcid.org/0000-0003-2082-5790

Maksym SYKAL, PhD in Law, Associate Professor, Academy of the State Penitentiary Service
ORCID ID: orcid.org/0000-0003-0334-4047

Olha ALIEKSIEIEVA, Candidate of Science of Law, State Research Institute of the Ministry of Internal Affairs of Ukraine
ORCID ID: orcid.org/0000-0003-3390-536X

Mykhailo PROKHORENKO, Candidate of Juridical Sciences, National defence University of Ukraine named after Ivan Gherniakhovskyi
ORCID ID: orcid.org/0000-0002-1471-9134