Risk assessment of cyberattacks in conditions of hybrid war based on analysis of cybersecurity basic capacity in the civil security sector in Ukraine

Oleksandr Korystin [1], Nataliia Svyrydiuk [1], Ganna Sobko [2], Olena Mitina [3] and Marek Aleksander [4]

[1] *State Scientifically Research Institute of the Ministry of Internal Affairs, Y. Gutsalo Lane 4a, Kyiv, 01011, Ukraine*
[2] *Odesa State University of Internal Affairs, 1, Uspenskaya, Odesa, 65000, Ukraine*
[3] *Odesa National Polytechnic University, Shevchenko Ave., 1, Odesa, 65044, Ukraine*
[4] *University of Applied Sciences in Nowy Sacz, Nowy Sacz, Poland*

Abstract

The article focuses on hybrid threats' study in the civil security sector in Ukraine. The main emphasis is on evaluative variations in the perception of the capacity or vulnerability of the law enforcement system. The analysis covers the whole range of activities of the Ministry of Internal Affairs of Ukraine, taking into account the activities of National Police, National Guard, State Border Service, State Emergency Service, State Migration Service and service centers. An empirical study of the relationship between cyberattacks and cyber-hygiene in the civil security sector is presented. Unique empirical materials are used - the results of a survey of specialists of the Ministry of Internal Affairs and these CEBs on the identification and assessment of hybrid threats in the civil security sector, as well as quantification of the ability of law enforcement agencies to combat these threats. The basic characteristics of cyber-hygiene are used to estimate the level and impact of internal and external factors of law enforcement. Based on the application of linear regression, the risk assessment of the spread of hybrid cyber threat "use of cyber operations" is assessed, priority risk reduction factors are identified and an appropriate forecast model is built.

Keywords

Hybrid threats, civil security sector, central bodies of executive power of the Ministry of Internal Affairs, capacity, vulnerability, correlation, risk assessment, regression analysis

1. Introduction

Building an independent state, an important area of security for Ukraine is countering hybrid threats which show the specifics of their distribution in the civil security sector. The adequacy of such activities objectively requires raising awareness of such threats' prevalence, understanding of their content and the ability to reduce the risk of their spread. The issue of combating hybrid threats covers the problems of national security quite broadly and comprehensively. This, above all, requires significant analysis of the situation, the study of those factors that cause the inability to effectively combat hybrid threats, in particular in the areas of public safety and civil protection [1].

CMiGIN 2022: 2nd International Conference on Conflict Management in Global Information Networks, November 30, 2022, Kyiv, Ukraine
EMAIL: alex@korystin.pro (O. Korystin); svyrydiuk@gmail.com (N. Svyrydiuk); gsobko@gmail.com (G. Sobko); omitina@gmail.com (O. Mitina); marek.aleksander@gmail.com (M. Aleksander)
ORCID: 0000-0001-9056-5475 (O. Korystin); 0000-0002-0983-2116 (N. Svyrydiuk); 0000-0002-5938-3400 (G. Sobko); 0000-0001-8732-2421 (O. Mitina); 0000-0003-2619-1063 (M. Aleksander)
© 2022 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-3530/paper10.pdf

2. Research analysis

Hybrid threats have been the subject of research by many scientists around the world. Therefore, it is the subject of discussion among politicians, problem international organizations are trying to solve. Development of certain ways of counteraction to hybrid threats is also a subject of research by scientists of the most various branches, in particular: the essence and structure of hybrid war (E. Magda [2]), reconceptualizing of hybrid threats (F. G. Hoffman [3, 4]), threat detection in web [5, 6], risk-assessment of cyber attacks [7-9], hybrid threats of economic security ([10], Z. Hbur [11]), experience of the EU [12], M. Malsky, V. Predborskyi [13], I. Rusnak [14] and others Davis, J. R. [15].

In recent years, research has been conducted in the field of cybersecurity: the principles of building a modern communication system are formulated and the requirements for them are determined [2, 16], recommendations are given to assess the reliability of certain types of communication technology [17-19] and more. However, building a state based on key areas of national security, including cybersecurity, requires further understanding of hybrid warfare problems in Ukraine, its scale, and mastering current methodological approaches to the analysis of hybrid threats, risk assessment of their spread, as well as the vulnerability of the system to hybrid threats.

3. The purpose of the article

Analyze hybrid cyber threats in the civil security sector, factors capable of counteracting cyber operations and identify basic ones that ensure a certain level of cyber hygiene. Develop a process for assessing the risks of the spread of cyber operations in the civil security sector and build an appropriate model and forecast.

4. The main material

Developing theoretical and applied aspects, scientists of the Research Institute of the Ministry of Internal Affairs of Ukraine participated in several research projects to implement the general concept of strategic analysis based on risk assessment of modelling and forecasting, in particular - strategic analysis of hybrid threats in the civil security sector [1]. The study focuses on:

- Identification and rating of hybrid threats (matrix and analysis of variance in the environment of IBM SPSS Statistics);
- Risk analysis of the spread of hybrid threats (integration of two estimates of "probability" and "consequences" in the IBM SPSS Statistics environment);
- Rating and ranking of external and internal factors that contribute to (reduce) the effectiveness of actors in combating hybrid threats (IBM SPSS Statistics, matrix analysis);
- Assessment of the ability or vulnerability of the system of subjects of counteraction to hybrid threats (integration of two assessments "level" and "impact" in the IBM SPSS Statistics environment);
- Conducting SWOT and PESTL analysis;
- Risk assessment of the spread of hybrid threats (comparison of the threat level with the level of vulnerability (ability) of the system, the formation of a mathematical model of risk assessment based on correlation and regression analysis).

Based on the analysis of the risk of the spread of hybrid cyber threats in the civil security sector, the following are highlighted (Fig. 1):

Cyber-attacks against critical infrastructure facilities (52.25%) and central bodies of executive power (50.03%) have the highest risk of spreading. The risk of using cyber operations (49.29%) as a generalizing indicator of hybrid cyber threats was identified at the same high level.

Further analysis was conducted with an emphasis on the generalizing indicator "use of cyber operations". Based on the correlation analysis, internal and external factors that have a certain statistical relationship with this threat are identified. Internal factors are divided into two groups: the strengths and weaknesses of the subjects of the civil security system in combating hybrid threats. 28 correlates were identified from the list of strengths and 9 - weaknesses. Among the external factors (opportunities

to increase the effectiveness of countering hybrid threats) identified 27 correlates with the threat of using cyber operations.

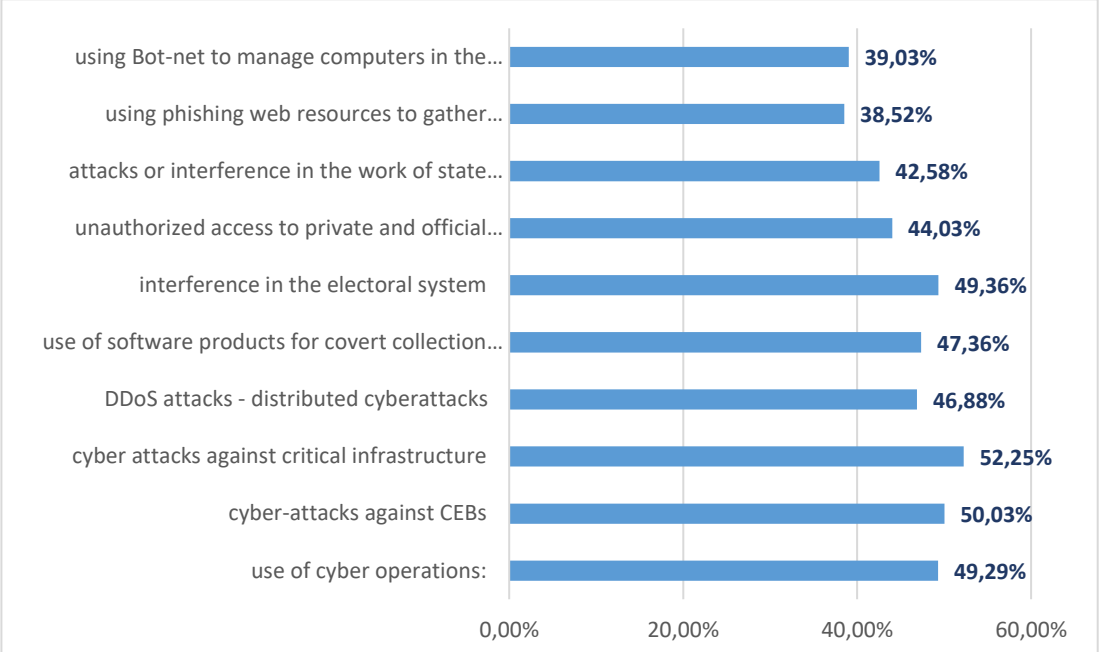

Figure 1: Rating of hybrid cyber threats to the civil security sector

Expertly from the general list of correlates, the internal and external factors forming basic bases of cyber-hygiene in the system of bodies of civil safety are defined (Table 1).

Table 1

Correlates of cyber hygiene

Performance indicators are strengths	Use of cyber operations	P value
8.7 According to international standards, the newly created services of detective services operate	-,138**	0,002
13 The procedure for selection for service has been improved (in the bodies of the Ministry of Internal Affairs system)	-,113*	0,013
16 Cybersecurity is provided in the units of the system of the Ministry of Internal Affairs	-,143**	0,002
24.1 Cybersecurity critical infrastructure is protected	-0,074	0,004
27 Level of use of licensed software and security systems	-,092*	0,044
31.1 Conformity of initial (basic) training	-,222**	0,000
31.2 Compliance of professional education in higher education institutions of the Ministry of Internal Affairs	-,115*	0,012
31.3 Conformity of advanced training	-,110*	0,016
36 The level of response of the organs of the Ministry of Internal Affairs to new challenges	-,113*	0,013
Performance indicators are weaknesses	Use of cyber operations	P value
7 Cases of appointment to positions of persons not according to professional competencies	-.163**	0,000
8 Insufficient level of professional training:	-.224**	0,000

Performance indicators are strengths	Use of cyber operations	P value
8.1 Insufficient level of professional training of managerial (superintendential) level	-.266**	0,000
8.2 Insufficient level of professional training of executive level (staff)	-.170**	0,000
Capacity indicators - opportunities	Use of cyber operations	P value
7 The EUMC has been deployed with a mandate to build capacity in the SGBC	.160**	0,000
18.6 Raising the intellectual level of employees of the Ministry of Internal Affairs	.216**	0,000
18.7 Improving the technical equipment of the organs of the Ministry of Internal Affairs	.129**	0,005
21 The involvement of international technical assistance to:	.191**	0,000
21.1 holding reforms in the organs of the Ministry of Internal Affairs	.169**	0,000
21.2 technical re-equipment of the system of the Ministry of Internal Affairs	.166**	0,000
21.3 training of personnel of the organs of the system of the Ministry of Internal Affairs	.200**	0,000
32 Network and information security platform for interaction with public and private players in cyberspace	.192**	0,000

Further analysis was performed using linear regression. The array of data obtained was analyzed by the method of step by step inclusion, step by step exclusion, and finding the best subsets. The conclusion about the adequacy of the model was inferred by the F-criterion at a given level and relatively high scores of the multiple (Fig. 2, Table 2):

```
REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT TA92
  /METHOD=STEPWISE Rs21 Rs28 Rs31 Rs40 Rs46 Rs51 Rs52
    Rs53 Rs58 Rs62 Rw7 Rw8 Rw9 Rw10
    Ro7 Ro24 Ro25 Ro34 Ro35 Ro36 Ro37 Ro48.
```

Figure 2: Syntax of linear regression of the threat "use of cyber operations" (TA92)

Taking into account the estimated values and applying the linear regression model, the risk of spreading the use of cyber operations in the presence of cyber hygiene in the civil security system is determined (Fig. 3) and a forecast of reducing the risk of cyber operations in the civil security sector is constructed (Fig. 4, 5):

Table 2
Linear regression model of the use of cyber operations in the basic conditions of cyber hygiene

	Factor[a]			
Model	Unstandardized factors	Standardized factors	т	P value

Factor[a]					
	B	Std. Err.	Beta		
(Constant)	58,813	1,966		29,913	0,000
8.1 Insufficient level of professional training at the management level	-0,201	0,033	-0,266	-6,034	0,000
(Constant)	71,908	3,237		22,218	0,000
8.1 Insufficient level of professional training at the management level	-0,198	0,033	-0,261	-6,071	0,000
31.1 Compliance of primary preparation	-0,220	0,044	-0,216	-5,023	0,000

Taking into account the estimated values and applying the linear regression model, the risk of spreading the use of cyber operations in the presence of cyber hygiene in the civil security system is determined (Table 3) and a forecast of reducing the risk of cyber operations in the civil security sector is constructed (Table 4, 5).

Table 3

Risk assessment of the use of cyber operations in the presence of cyber hygiene

Model and forecast	Coefficient	P value	Rating	
(Constant)	71,908	0,000		
8.1 Insufficient level of professional training of managerial (superintendential) level	-0,198	0,000	47,14	-9,33
31.1 Conformity of initial (basic) training	-0,220	0,000	60,24	-13,25
Use of cyber operations			RA =	49,32 %

Table 4

Forecast of the risk of using cyber operations with an increase in capacity by 10%

Coefficient	P value	Rating	
71,908	0,000		
-0,198	0,000	57,14	-11,31372
-0,220	0,000	70,24	-15,4528
		RA =	45,14 %

Table 5

Forecast of the risk of using cyber operations if the capacity increases by 20%

Coefficient	P value	Rating	
71,908	0,000		
-0,198	0,000	67,14	-13,29372
-0,22	0,000	80,24	-17,6528
		RA =	40,96 %

Further analysis was continued, taking into account some differences of experts' opinion on the risk level of using cyber operations as a hybrid threat (Fig. 2). The frequency response of the generalized data indicates a significant divergence of experts' opinions. Less than 10 percent of experts report a low level of risk (1.71%; 6.29%; 12.0%). 13 percent of respondents determine the level of risk to 20%, and almost the same - 10 percent of respondents - about 100%. However, the vast majority of experts (about 70%) focus on the level of risk in the range of 37.14 - 68.57%. This discrepancy is also quite inaccurate, although the average value of the risk of using cyber operations is determined at 49.29%.

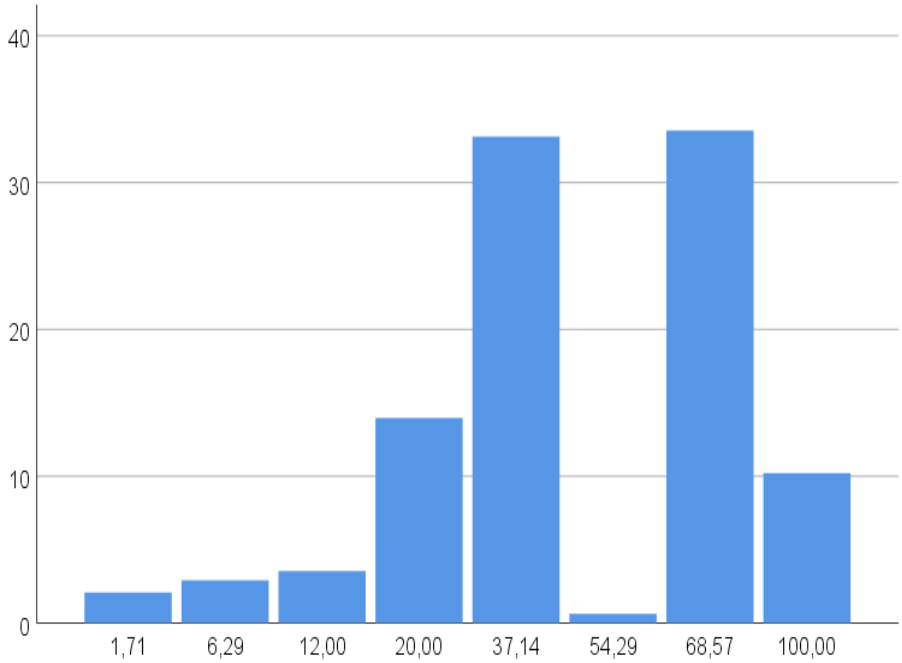

Figure 2: Frequency response to assess the risk level of using cyber operations in hybrid warfare.

That is, hypothetically, there is a possibility of different risk assessments of cyber operations' using different samples, in particular, in relation to the scope of activities for the specifics of law enforcement. In this regard, the risk level of using cyber operations as a hybrid threat was calculated taking into account the area of professional activity of the expert, i.e. by type of law enforcement agency (Table 6). Indeed, the hypothesis of a discrepancy in the assessment of the risk level of the use of cyber operations in hybrid warfare is confirmed. There are significant differences in the samples of experts from different law enforcement agencies. The highest level of risk is 60.51%, according to the experts of the Ministry of Internal Affairs of Ukraine. At the same time, experts working in the SESU (45.08%) and the SBGS (46.66%) focus on slightly lower than average values (49.29%).

Given these differences, it is logical to make statements about possible discrepancies in the samples and to assess the ability of some law enforcement agencies to counter cyber operations, in particular, taking into account the basic requirements of cyber hygiene. Appropriate linear regression models were developed for verification (Table 6, 7, 8, 9, 10).

Table 6

The risk level of using cyber operations in a hybrid war based on a sample by type of law enforcement agency

Law enforcement agency	Risk level, %
Ministry of Internal Affairs of Ukraine (MIA)	60,51

Law enforcement agency	Risk level, %
Ministry of Internal Affairs of Ukraine (MIA)	60,51
National Police of Ukraine (NPU)	47,49
National Guard of Ukraine (NGU)	47,34
State Emergency Service of Ukraine (SESU)	45,08
State Border Guard Service of Ukraine (SBGS)	46,66
State Migration Service of Ukraine (SMSU)	54,04
Main Service Center of the Ministry of Internal Affairs (HSC of the Ministry of Internal Affairs)	51,47
Average	49,29

The developed model of linear regression of the use of cyber operations, according to experts of the Ministry of Internal Affairs, emphasizes the importance of the following predictors of cyberhygiene: a significant vulnerability of cyber hygiene is the appointment of persons outside professional competencies (-0.433); as well as capacity building requires access to the best foreign practices of practical activities (0.113) and the formation of a professional core of work teams (0.123).

Table 7

Linear regression model of the use of cyber operations in the basic conditions of cyber hygiene (sample of the Ministry of Internal Affairs of Ukraine)

Factor[a]					
Model	Unstandardized factors		Standardized factors	т	P value
	B	Std. Err.	Beta		
(Constant)	47,424	10,405		4,558	0,000
7. Cases of appointment to positions not according to professional competencies, but on the basis of interpersonal communications	-0,433	0,125	-0,550	-3,462	0,002
19.2. Access to best foreign practice practices	0,326	0,113	0,409	2,881	0,007
9. Blurred professional core of work teams (loss of communication between generations)	0,274	0,360	0,360	2,220	0,034

The developed model of linear regression of the use of cyber operations, according to experts of the Ministry of Internal Affairs, emphasizes the importance of the following predictors of cyberhygiene: a significant vulnerability of cyber hygiene is the appointment of persons outside professional competencies (-0.433); as well as capacity building requires access to the best foreign practices of practical activities (0.113) and the formation of a professional core of work teams (0.123).

Table 8

Linear regression model of the use of cyber operations in the basic conditions of cyber hygiene (NGU sample)

Factor[a]					
Model	Unstandardized factors		Standardized factors	τ	P value
	B	Std. Err.	Beta		
(Constant)	4,131	9,383		0,440	0,465
32. Level of financial support for the development of educational, scientific and research activities in the field of National Security	1,533	0,336	1,328	4,557	0,001
33 The level of capabilities of educational and research institutions for strategic research in the field of National Security	-0,672	0,291	-0,672	-2,306	0,044

Therefore, the model of linear regression of cyber operations, according to NGU experts, emphasizes the importance of increasing the level of financial support for the development of educational, scientific and research activities in the NB and significant vulnerability of educational and scientific institutions to strategic research in the NB.

Table 9

Linear regression model of the use of cyber operations in the basic conditions of cyber hygiene (NPU sample)

Factor[a]					
Model	Unstandardized factors		Standardized factors	τ	P value
	B	Std. Err.	Beta		
(Constant)	57,460	2,501		22,978	0,000
8.1 Insufficient level of professional training at the managerial level	-0,213	0,043	-0,289	-4,988	0,000

The model of linear regression of cyber operations' using, according to NPU experts, highlights only significant vulnerabilities in the training of management level. This in some way corresponds to the general trend based on average values. This is also the case in the constructed model of linear regression (Table 10) of the sample, taking into account the opinion of SBGS experts.

Table 10
Linear regression model of the use of cyber operations in the basic conditions of cyber hygiene (SBGS sample)

Factor[a]					
Model	Unstandardized factors		Standardized factors	т	P value
	B	Std. Err.	Beta		
(Constant)	69,313	7,443		9,312	0,000
8.1 Insufficient level of professional training at the managerial level	-0,498	0,134	-0,548	-3,707	0,001

Therefore, the linear regression model (Table 11) of the use of cyber operations in hybrid warfare, according to SESU's experts on vulnerability, emphasizes the lack of training of both managers and staff and the inability of educational and research institutions to strategic research in national security; and also needs to increase the capacity to attract international technical assistance for the training of staff of the Ministry of Internal Affairs of Ukraine.

Table 11
Linear regression model of the use of cyber operations in the basic conditions of cyber hygiene (SESU sample)

Factor[a]					
Model	Unstandardized factors		Standardized factors	т	P value
	B	Std. Err.	Beta		
(Constant)	63,798	7,682		8,305	0,000
8. Insufficient level of professional training	-0,310	0,080	-0,466	-3,875	0,000
33 The level of capabilities of educational and research institutions for strategic research in the field of National Security	-0,431	0,113	-0,478	-3,821	0,001
21.3 Involvement of international technical assistance for training of personnel of the Ministry of Internal Affairs	0,261	0,080	0,409	3,260	0,002

5. Conclusions

Thus, hybrid cyber threats in the civil security sector have been identified, among which cyber-attacks against critical infrastructure facilities (52.25%) and central bodies of executive power (50.03%)

have the highest risk of spreading. The risk of using cyber operations (49.29%) as a generalizing indicator of hybrid cyber threats was identified at the same high level.

Using correlation analysis and linear regression model: the risk assessment of the use of cyber operations in the civil security sector was conducted - 49.32%; priority risk reduction factors have been identified and the level of capacity for them has been determined - an insufficient level of professional training at the management level (47.14%) and compliance with initial training (60.24%); the forecast is based on an increase in capacity by 10 and 20 percent and a reduction in the risk of using cyber operations, respectively 45.14% and 40.96%. At the same time, the level of risk of using cyber operations in a hybrid war is assessed rather ambiguously by sample experts on the basis of a professional body in the system of the Ministry of Internal Affairs. The highest level of risk is 60.51%, according to experts of the Ministry of Internal Affairs of Ukraine, and lower than the average (49.29%) is determined by experts of the State Emergency Service of Ukraine (45.08%) and the State Border Guard Service of Ukraine (46.66%).

The developed models of linear regression on the basis of sampling by the body of the system of the Ministry of Internal Affairs have formed an opportunity to identify key predictors that form the basic principles of cyber hygiene in law enforcement agencies.

References

[1] T. I. Kovalchuk, O. Y. Korystin, N. P. Sviridyuk, Hybrid threats in the civil security sector in Ukraine, Problems of Legality (147) (2019) 163–175. doi: 10.21564/2414-990x.147.180550.

[2] E. Magda, Hybrid war: the essence and structure of the phenomenon, International Relations, Part 'Political Sciences' 4 (2014). URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/2489.

[3] F. G. Hoffman, Hybrid threats: Neither omnipotent nor unbeatable, Orbis 54(3) (2010) 441–455.

[4] F. G. Hoffman, Hybrid threats: Reconceptualizing the evolving character of modern conflict. Strategic Forum, Washington, 2009.

[5] E. Bashir, M. Bouguessa, Data Mining for Cyberbullying and Harassment Detection in Arabic Texts, International Journal of Information Technology and Computer Science 13(5) (2021) 41–50. doi: 10.5815/ijitcs.2021.05.04.

[6] S. Fedushko, E. Benova, Semantic analysis for information and communication threats detection of online service users, Procedia Computer Science 160 (2019) 254–259. doi: https://doi.org/10.1016/j.procs.2019.09.465.

[7] A. Süzen, Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem, International Journal of Computer Network and Information Security 12(1) (2020) 1–12. doi: 10.5815/ijcnis.2020.01.01.

[8] K. Umamaheswari, N. Subramanian, M. Subramaniyan, Distributed Denial of Service Attack Detection Using Hyper Calls Analysis in Cloud, International Journal of Computer Network and Information Security 15(4) (2023) 61–71. doi:10.5815/ijcnis.2023.04.06.

[9] A. Zimba, A Bayesian Attack-Network Modeling Approach to Mitigating Malware-Based Banking Cyberattacks, International Journal of Computer Network and Information Security 14(1) (2022) 25–39. doi: 10.5815/ijcnis.2022.01.03.

[10] A. Aliyev, R. Shahverdiyeva, Scientific and Methodological bases of Complex Assessment of Threats and Damage to Information Systems of the Digital Economy, International Journal of Information Engineering and Electronic Business 14(2) (2022) 23–38. doi: 10.5815/ijieeb.2022.02.02ю

[11] Z. Hbur, Actual hybrid threats of economic security of Ukraine, Investments: practice and experience 7 (2018) 97–99.

[12] Hybrid threats to Ukraine and public security, The experience of the European Union and the Eastern Partnership, 2018. URL: www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-end_0202.pdf.

[13] V. A. Predborskyi, "Hybrid" war as a reflection of the laws of the development of a society of incomplete modernization, Formation of market relations in Ukraine 10 (2004) 13–18.

[14] I. S. Rusnak, Military security of Ukraine in the light of reforming the security and defense sector, Science and defense 2 (2015) 9–14.

[15] A. Cederberg, P. Eronen, How can societies be defended against hybrid threats, Strategic Security Analysis 9(1) (2015) 1–10.
[16] N. Svyrydiuk, Y. Likhovitskyy, P. Polián, Information Threats in the Context of Hybrid War, Advances in Economics, Business and Management Research 188 (2021) 114–119.
[17] A. Tikhomirov, N. Kinash, S. Gnatyuk, A. Trufanov, O. Berestneva, A. Rossodivita, S. Gnatyuk, R. Umerov, Network Society: Aggregate Topological Models, in: A. Dudin, A. Nazarov, R. Yakupov, A., Gortsev (Eds.), Information Technologies and Mathematical Modelling, Communications in Computer and Information Science, volume 487, Springer, Cham, 2014. https://doi.org/10.1007/978-3-319-13671-4_47.
[18] A. V. Kharybin, O. N. Odaryshchenko, About the approach to the decision of questions of a choice of methodology of an estimation of system reliability and survivability of information systems of critical application, Radiotechnical and computer systems 6(18) (2006) 61–70.
[19] Z. Hu, V. Gnatyuk, V. Sydorenko, R. Odarchenko, S. Gnatyuk, Method for Cyberincidents Network-Centric Monitoring in Critical Information Infrastructure, International Journal of Computer Network and Information Security 9(6) (2017) 30–43.