Risk forecasting of information-content-security

Oleksandr Korystin[1,2,*,†], Serhii Demediuk[2,3,†], Nataliia Sviridyuk[2,4,†], Olena Mitina[5,†], Marek Aleksander[6,†] and Yuriy Kardashevskyy[4,†]

[1] State Scientifically Research Institute of the MIA of Ukraine, Evgena Gutsala Provulok, 4-A, Kyiv, 01011, Ukraine
[2] National Academy of the Security Service of Ukraine, Mykhaila Maksymovycha Str., 22, Kyiv, 03066, Ukraine
[3] National Security and Defense Council of Ukraine, Petro Bolbochan Str., 8, Kyiv, 01601, Ukraine
[4] Odesa State University of Internal Affairs, Uspenska Str., 1, Odesa, 65000, Ukraine
[5] Odesa Polytechnic National University, Shevchenko Ave., 1, Odesa, 65044, Ukraine
[6] Panstwowa Wyzsza Szkoła Zawodowa w Nowym Saczu, Stanislawa Staszica, 1, Nowy Sacz, 33300, Poland

Abstract

This paper elucidates the findings of an investigation into the cybersecurity status within Ukraine. This study utilizes a risk-oriented approach to develop a predictive model aimed at mitigating the potential dissemination of recognized cyber threats, specifically those related to information content security. Identified vulnerabilities play a crucial role in diminishing the risk associated with information content security.

Keywords

cybersecurity, cyber threats, risk assessment, linear regression, vulnerabilities, forecasting

1. Introduction

The occurrence of extensive cyberattacks and their resultant adverse effects can be attributed to the emergence of hybrid war in Ukraine. In order to effectively address cybersecurity concerns, it is imperative to employ a precise and robust methodology. Furthermore, it is necessary to adequately evaluate the indicators related to cyber threats and vulnerabilities in the national cybersecurity system, taking into account not only their probability but also their impact on cyberspace and the consequences they pose to cybersecurity. Under such circumstances, the adoption of a risk-oriented approach in the domain of cybersecurity holds significant importance in establishing a comprehensive understanding and consciousness of the capabilities inherent in cybersecurity system to effectively combat potential threats.

2. Related works

A great deal of research has been done in the area of cybersecurity. A wide range of scientists chose the research directions. Many research works have focused on clarifying the basic principles of creating a modern communication system and the requirements that go along with it [1]. These studies have also offered recommendations for assessing the reliability of particular communication technologies [2, 3]. To protect the cloud environment, various proposed "ontological techniques" are assessed and a comprehensive analysis of various models is conducted [4–7]. A great deal of work has gone into finding and analysing software vulnerabilities as well as creating methods for reporting

CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, January 24–27, 2024, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
alex@korystin.pro (O. Korystin); cyberdemediuk@protonmail.com (S. Demediuk); S_N_P_@ukr.net (N. Sviridyuk); olenamitina@ukr.net (O. Mitina); marek.aleksander@gmail.com (M. Aleksander); lvivtin@gmail.com (Y. Kardashevskyy)
0000-0001-9056-5475 (O. Korystin); 0009-0008-1359-5265 (S. Demediuk); 0000-0001-9772-1119 (N. Sviridyuk); 0000-0001-8732-2421 (O. Mitina); 0000-0003-2619-1063 (M. Aleksander); 0009-0009-8940-6384 (Y. Kardashevskyy)

and classifying them in software security [8–10]. In the domain of information protection, particular emphasis is placed on the prevailing techniques for identifying deviations and present threats in networks. Statistical approaches are regarded as potent means of identifying anomalies, while the chosen method is subject to empirical testing. Additionally, techniques for intercepting and scrutinizing network traffic during passive monitoring of a network segment are also taken into account [11–13]. The examination of diverse aspects of managing information security within organizations of varying sectors remains a significant aspect, encompassing the allocation and utilization of resources in the information security system of the organization [14–16]; information security threats and risk management [17, 18]; management of documentation and information support systems in an organization [19, 20]; management of information security audits [21, 22]; management analysis of the effectiveness of information security systems [23, 24]. Several references have been linked to the utilization of diverse predictive techniques through the development of suitable models [25, 26].

Adopted methodology involves analysing scientific sources, researching cybersecurity threats, identifying and evaluating vulnerabilities, and developing predictive models for assessing the impact of cyber threats. This approach is aimed at further analysing and assessing the risks associated with cyber threats, as well as evaluating the data's cybersecurity capabilities within the cybersecurity system of Ukraine [27].

3. Proposed methods

The data set utilized in this research was acquired through identification of cyber threats, indicators of cybersecurity capabilities and conducting a survey among cybersecurity experts in Ukraine [28]. As a result, the data set appropriately captures the expertise and professional knowledge of the survey participants. Respondents ensured their privacy and anonymity by electronically completing the questionnaires online. Information gleaned from respondents is increasingly being extracted using data obtained via online platforms. This approach makes it possible to effectively gather a wide range of opinions on a multitude of subjects from a sizable number of experts, spread out geographically. In order to guarantee the evaluation of potential risks, an assessment was conducted for every indicator based on two fundamental attributes: "Likelihood" and "Consequences".

To ensure the extraction of the most trustworthy information from the acquired data, only experts whose responses demonstrated logical coherence were chosen. The statistical justification for implementing a sample restriction procedure is rooted in the idea that the extensive nature of the questionnaire could potentially lead experts to provide erroneous responses. This is because the intricate nature of the questions coupled with the limited time available for comprehension can cause attention instability [29]. Moreover, when analysing the online mode data, it is imperative to recognize that the proficiency of specialists, lack of incentive to provide logical answers, and exhaustion or inattention due to the volume of questions could significantly reduce the quality of collected data [30].

3.1. Risk assessment

The general methodology employed in this study adheres to the guidelines outlined in ISO 31000 [31]. This pertains to the system of indicators in Ukraine's cybersecurity, which are categorized into three groups (threats, capabilities, and vulnerabilities). It encompasses the structure of data, assessment scoring, and the formation of an overall expert base. Additionally, it includes the application of specific methods, tools, data processing, analysis, and the interpretation of outcomes [32].

3.2. Linear Regression Algorithm Forecasting

Regression analysis comprises techniques for developing mathematical models of the examined systems, techniques for ascertaining the parameters of these models, and techniques for assessing

their sufficiency. Considering multicollinearity is crucial as it introduces computational instability through a substantial increase in computation errors. Consequently, it becomes unfeasible to interpret the outcomes, and the values of specific coefficients lose statistical significance. In certain scenarios, a method adopted to address the issue of multicollinearity involves repeatedly excluding related variables and subsequently comparing the outcomes. The stepwise regression procedure [33–35] is one of the approaches utilized to choose the most crucial variables.

4. Results

The adopted approach entails evaluating the potential risks posed by various threats, ranging from 0% to 100%, and it incorporates distinct threshold levels as follows [36]: when the risk level exceeds 60%, it falls into the red risk zone (indicating substantive threats); in the range of 50% to 60%, it belongs to the orange risk zone (representing significant threats); within the 40% to 50% range, it pertains to the yellow risk zone, alerting to threats that require attention; when the risk level is at 40%, it falls under the green risk zone.

The evaluation of risk associated with the identified threats presents a wide range of outcomes, indicating differing degrees of appropriateness in terms of accurately representing the results (Figure 1).

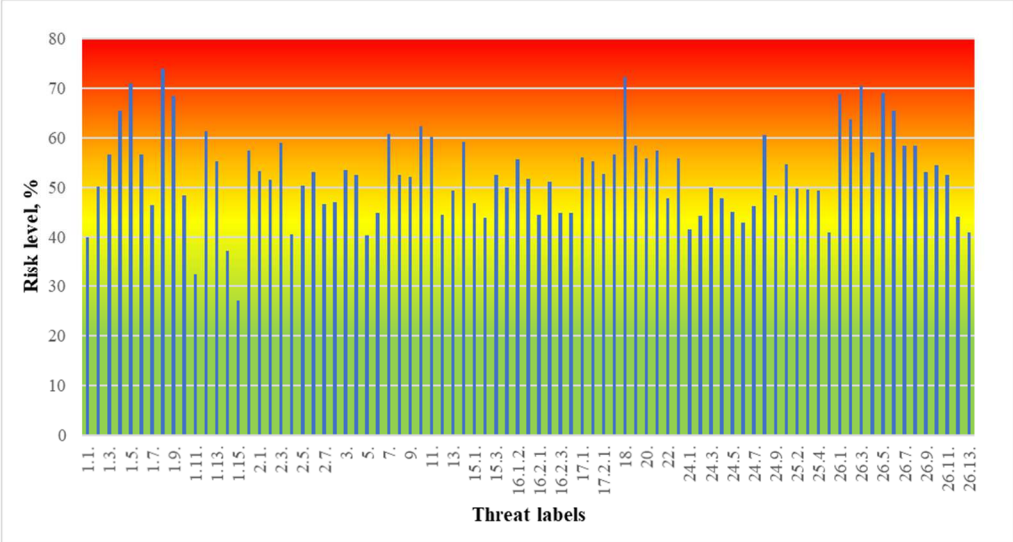

Figure 1: Overall ranking of cybersecurity threats.

From the whole list of cyber threats, further analysis focuses on Information-content-security: Unauthorised-information-access – 56,01 % (level of risk) and Unauthorised-information-modification – 55,20 % (Figure 2).

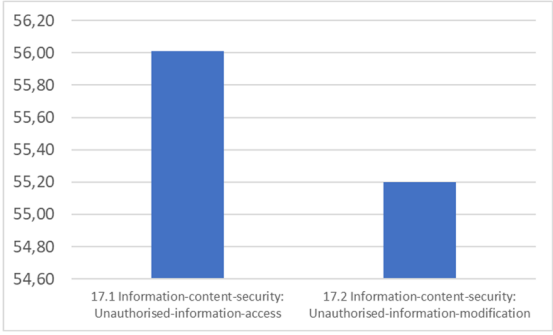

Figure 2: Cyber threat rating - Information-content-security.

It should also be noted that our analysis is based on a comparison of the mean value in assessing the level of risk. Expert assessments, despite the reliability of the sample, still have some differences (Figure 3.) But we perceive this as the variability of expert assessment, which once again emphasizes the representativeness of the empirical basis. Along with this, the use of the average value of expert evaluation is a common approach in our interpretation and is used by us mainly to analyse the trend, compare the risk of other indicators, as well as to build a forecast model.

The assessment of cybersecurity vulnerabilities will be the focus of further investigation. Twenty-one indicators of vulnerability have been identified and evaluated (Figure 4).

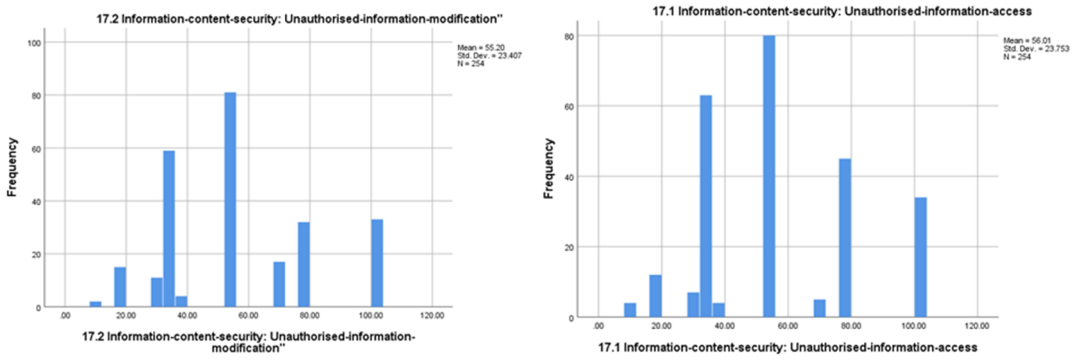

Figure 3: Variability of cyber threat assessment by experts – information-content-security.

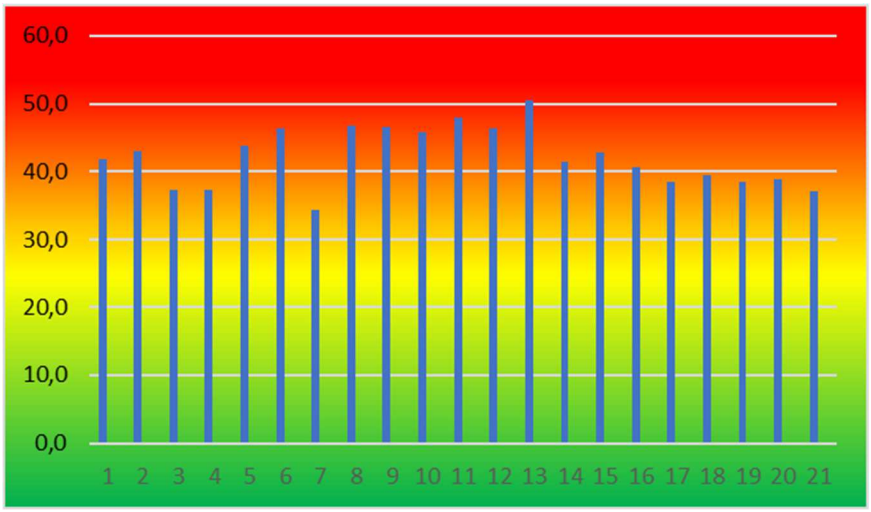

Figure 4: Overall rating of cybersecurity vulnerabilities.

Those that are the most pertinent and possibly at risk have been identified:

– technological vulnerabilities: the upcoming generation of mobile communications known as 5G (62.71%); Internet of Things (IoT) (62.57%); quantum technologies (65.56%);

– technical vulnerabilities, specifically information and telecommunication systems (54.27%). Software vulnerabilities, including the drawbacks of software code (53.65%).

– concerns about legal and organizational vulnerabilities: legal aspect includes complying with government regulations and industry standards (61.55%) and ensuring sufficient accountability for breaches of cybersecurity laws (60.43%); organizational aspect involves monitoring cybersecurity at departmental level (60.99%) and promoting cooperation between public and private sectors in the cybersecurity field (62.95%).

The examination of vulnerabilities is not limited to just analysing their descriptive statistics. In the realm of cybersecurity, it holds great significance to evaluate every potential threat identified and evaluated by the expert community in conjunction with the system of susceptibilities,

represented by various indicators [37, 38]. The resolution of this issue is achieved through the construction of a suitable predictive model.

By employing the linear regression model, we can determine the most efficient correlation between specific cybersecurity threats in Ukraine and the variables that describe the vulnerabilities of the national cybersecurity system (Figure 5). We utilized IBM SPSS Statistics software to analyse the data due to the vast array of potential combinations of independent variables in multiple linear regression.

The initial regression model utilises predictors that define vulnerabilities in the field of cybersecurity in Ukraine to analyse the relationship with the variable "Unauthorised-information-access" (Figure 6).

The appropriateness of the acquired outcomes of the linear regression model can be determined by evaluating the statistical significance of said outcomes (Significance ≤ 0.05).

```
REGRESSION
  /DESCRIPTIVES MEAN STDDEV CORR SIG N
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT TA47
  /METHOD=STEPWISE Va1 Va2 Va3 Va4 Va5 Va6 Va7 Va8 Va9 Va10 Va11 Va12 Va13 Va14 Va15 Va16 Va17 Va18 Va19 Va20 Va21.
```

Figure 5: Syntax of the linear regression model "TA47 - Unauthorised-information-access" (IBM SPSS Statistics).

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	26,185	4,857		5,391	0,000
	Technology: On modern information and communication technologies	0,484	0,093	0,371	5,222	0,000
	Legal: Ensuring cybersecurity at the level of bylaws and regulations	0,248	0,081	0,218	3,062	0,003

a. Dependent Variable: Information-content-security: Unauthorised-information-access

Figure 6: Linear regression model "Unauthorised-information-access" taking into account existing vulnerabilities (IBM SPSS Statistics).

From a comprehensive range of indicators (Va1 - Va21) that depict the susceptibility to cybersecurity threats in Ukraine, through the utilization of linear regression analysis, two significant predictors were identified as means to mitigate the risk of the specific cybersecurity threat "Unauthorised-information-access". These essential predictors are categorized as follows: "Technology: On modern information and communication technologies" and "Legal: Ensuring cybersecurity at the level of bylaws and regulations."

Using the same syntax in SPSS for the threat "Unauthorised-information-modification", we also identified the best predictors from the list of cyber system vulnerabilities: "Technology: On modern information and communication technologies" and "Legal: Compliance with government and industry standards".

Based on the information provided, it is feasible to foresee a gradual decrease ranging from 10% to 30%. The forecast model is based on the example of a threat "Unauthorised-information-access" (Figure 7).

THREAT	RISK LEVEL					
	Basic level	Simulated level	Changing predictors			
			10 %		30 %	
			Technology: On modern information and communication technologies	*Legal: Ensuring cybersecurity at the level of bylaws and regulations*	*Technology: On modern information and communication technologies*	*Legal: Ensuring cybersecurity at the level of bylaws and regulations*
Information-content-security: Unauthorised-information-access	**56,01 %**	**56,59 %**	49,27 %		34,62 %	

Figure 7: Forecast of the threat level under the condition of changing the level of simulated predictors.

5. Conclusions

To address the matching of every identified and evaluated cybersecurity threat with the vulnerabilities in a system, the solution involves constructing a suitable predictive model.
Using the linear regression model, we aim to determine the ideal relationship between the specific cyber threat in Ukraine's domain of cybersecurity and the variables representing the vulnerabilities of the national cybersecurity system.

Among the various indicators that assess cybersecurity vulnerability in Ukraine, the primary factors that can help decrease the risk of threat propagation Unauthorised-information-access – "Technology: On modern information and communication technologies" and "Legal: Ensuring cybersecurity at the level of bylaws and regulations".

By inputting into the prediction model and progressively adjusting the estimated level and key predictors by 10% and 30% respectively, a decrease in the cyber threat of "Unauthorised-information-access" is anticipated.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] A. Tikhomirov, et al., Network society: aggregate topological models, Communications in Computer and Information Science 487 (2014) 415-421.

[2] 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.

[3] 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.

[4] J. S. Al-Azzeh, M. Al Hadidi, R. S. Odarchenko, S. Gnatyuk, Z. Shevchuk, Z. Hu, Analysis of self-similar traffic models in computer networks, International Review on Modelling and Simulations 10(5) (2017) 328–336. doi: 10.15866/iremos.v10i5.12009.

[5] P. Bhandari, M. S. Gujral, Ontology based approach for perception of network security state, in: Proceedings of Recent Advances in Engineering and Computational Sciences (RAECS), IEEE, Chandigarh, India, 2014, pp. 1–6, doi: 10.1109/RAECS.2014.6799584.

[6] K. Bernsmed, A. Undheim, P. Hakon Meland, M. G. Jaatun, Towards an ontology for cloud security obligations, in: Proceedings of International Conference on Availability, Reliability and Security, IEEE, Regensburg, Germany, 2013, pp. 577–581, doi: 10.1109/ARES.2013.76.

[7] N. F. Noy, D. L. McGuinness, Ontology Development 101: A Guide to Creating Your First Ontology, Stanford University, Stanford, CA, 2001.
[8] H. Kekül, B. Ergen, H. Arslan, Estimating missing security vectors in NVD database security reports, International Journal of Engineering and Manufacturing (IJEM) 12(3) (2022) 1–13. doi: 10.5815/ijem.2022.03.01.
[9] P. Mell, K. Scarfone, S. Romanosky, A complete guide to the common vulnerability scoring system version 2.0, in: Proceedings of FIRSTForum of Incident Response and Security Teams, 2007. URL: https://www.first.org/cvss/cvss-v2-guide.
[10] G. Spanos, A. Sioziou, L. Angelis, WIVSS: A new methodology for scoring information systems vulnerabilities, in: Proceedings of the 17th Panhellenic Conference on Informatics, 2013, pp. 83–90. doi: 10.1145/2491845.2491871.
[11] H. Kekül, B. Ergen, H. Arslan, A New vulnerability reporting framework for software vulnerability databases, International Journal of Education and Management Engineering (IJEME) 11(3) (2021) 11–19. doi: 10.5815/ijeme.2021.03.02.
[12] Z. Hu, R. Odarchenko, S. Gnatyuk, M. Zaliskyi, A. Chaplits, S. Bondar, V. Borovik, Statistical techniques for detecting cyberattacks on computer networks based on an analysis of abnormal traffic behavior, International Journal of Computer Network and Information Security (IJCNIS), 12(6) (2020) 1–13. doi: 10.5815/ijcnis.2020.06.01.
[13] R. Ranjan, G. Sahoo, A new clustering approach for anomaly intrusion detection, International Journal of Data Mining & Knowledge Management Process (IJDKP) 4(2) (2014) 29–38.
[14] I. Parkhomey, S. Gnatyuk, R. Odarchenko, T. Zhmurkoб et al, Method for UAV trajectory parameters estimation using additional radar data, in: Proceedings of the 2016 4th International Conference on Methods and Systems of Navigation and Motion Control, IEEE, Kyiv, Ukraine, 2016, pp. 39–42.
[15] F. Adeyinka, E. S. Oluyemi, A. N. Victor, U. C. Uchenna, O. Ogedengbe, S. Ale, Parametric equation for capturing dynamics of cyber attack malware transmission with mitigation on computer network, International Journal of Mathematical Sciences and Computing (IJMSC) 3(4) (2017) 37–51. doi: 10.5815/ijmsc.2017.04.04.
[16] M. Zaliskyi, R. Odarchenko, S. Gnatyuk, Y. Petrova, A. Chaplits, Method of traffic monitoring for DDoS attacks detection in e-health systems and networks, CEUR Workshop Proceedings 2255 (2018) 193–204. URL: https://ceur-ws.org/Vol-2255/paper18.pdf.
[17] T. P. Layton, Information Security: Design, implementation, measurement, and compliance. Auerbach Publications, 2016.
[18] J. Stuart. Engineering information security: The application of systems engineering concepts to achieve information assurance, John Wiley & Sons, NY, 2015.
[19] Ł. Grudzień, A. Hamrol. Information quality in design process documenta tion of quality management systems, International Journal of Information Management 36.4 (2016) 599–606.
[20] Y. Junseob, K. Lee, Advanced assessment model for improving effective ness of information security measurement, International Journal of Advanced Media and Communication 6.1 (2016), 4–19.
[21] E. Lavrov, A. Tolbatov, N. Pasko, V. Tolbatov, Cybersecurity of distributed information systems. The minimization of damage caused by errors of operators during group activity, штЖ Proceedings of 2017 2nd International Conference on Advanced Information and Commu nication Technologies (AICT 2017), IEEE, Lviv, Ukraine, 2017, pp. 83–87.
[22] S. Kasliono, M. Faizal, Point based forecasting model of vehicle queue with extreme learning machine method and correlation analysis, International Journal of Intelligent Systems and Applications (IJISA), 13(3) (2021) 11–22. doi: 10.5815/ijisa.2021.03.02.
[23] A. Anbarasa Pandian, R. Balasubramanian, Analysis on shape image retrieval using DNN and ELM classifiers for MRI brain tumor images, International Journal of Information Engineering and Electronic Business(IJIEEB) 8(4) (2016) 63–72. doi: 10.5815/ijieeb.2016.04.08.
[24] V. Lytvynenko, O. Kryvoruchko, I. Lurie, N. Savina, O. Naumov, M. Voronenko, Comparative studies of self-organizing algorithms for forecasting economic parameters, International Journal

of Modern Education and Computer Science (IJMECS) 12(6) (2020) 1–15. doi: 10.5815/ijmecs.2020.06.01
[25] N. H. Zulkifley, S. A. Rahman, N. H. Ubaidullah, I.l Ibrahim, House price prediction using a machine learning model: A survey of literature, International Journal of Modern Education and Computer Science (IJMECS) 12(6) (2020) 46–54. doi: 10.5815/ijmecs.2020.06.04.
[26] G. Babatunde, A. A. Emmanuel, O. R. Oluwaseun, O. B. Bunmi, A. E. Precious, Impact of climatic change on agricultural product yield using k-means and multiple linear regressions, International Journal of Education and Management Engineering (IJEME) 9(3) (2019) 16–26. doi: 10.5815/ijeme.2019.03.02.
[27] O.Ye. Korystin, O.O. Korystin, Threats in the sphere of cyber security in Ukraine, Nauka i pravookhoronna 1 (2022) 127–131. doi: 10.36486/np.2022.1(55)12.
[28] P. Goldammer, H. Annen, P. L. Stöckli, K. Jonas, Careless responding in questionnaire measures: Detection, impact, and remedies, The Leadership Quarterly 31(4) (2020) 101384.
[29] O. Korystin, N. Svyrydiuk, A. Vinogradov, The use of sociological methods in criminological research, in: Proceedings of the International Conference on Social Science, Psychology and Legal Regulation (SPL 2021). Series: Advances in Social Science, Education and Humanities Research, vol. 617, 2021, pp.1–6. doi: 10.2991/assehr.k.211218.001.
[30] ISO 31000:2018 - Risk Management. URL: https://www.iso.org/ru/publication/PUB100464.html.
[31] O. Korystin, N. Svyrydiuk, Methodological principles of risk assessment in law enforcement activity, Nauka i pravooxoronna 3 (2020) 191–197. doi: 10.36486/np.2020349.
[32] H.-G. Yu, G.-M. Huang, J. Gao, Nonlinear blind source separation using kernel multi-set canonical correlation analysis, International Journal of Computer Network and Information Security 2(1) (2010) 1–8. doi: 10.5815/ijcnis.2010.01.01.
[33] M. Z. Shahrel, S. Mutalib, S. Abdul-Rahman PriceCop–Price monitor and prediction using linear regression and LSVM-ABC methods for e-commerce platform, International Journal of Information Engineering and Electronic Business 13(1) (2021) 1–14. doi: 10.5815/ijieeb.2021.01.01.
[34] O. Korystin, N. Svyrydiuk, Activities of illegal weapons criminal component of hybrid threats, in: Proceedings of the International Conference on Economics, Law and Education Research (ELER 2021), Series: Advances in Economics, Business and Management Research, vol. 170, 2021, pp. 86–91. doi: 10.2991/aebmr.k.210320.016.
[35] O. Korystin, N. Svyrydiuk, V. Tkachenko, Fiscal security of the state considering threats of macroeconomic nature, in: Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL2021), Series: Advances in Economics, Business and Management Research, vol. 188, 2021, pp. 65–69. doi: 10.2991/AEBMR.K.210826.012.
[36] Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats a European Union response, 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.
[37] Joint Report to The European Parliament and the Council on the Implementation of the Joint Framework on countering hybrid threats - a European Union response, 2017. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017JC0030.
[38] Joint Report to the European Parliament, the European Council and the Council on the Implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018, 2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2018:014:FIN.