International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 28, No. 1, February, 2023, pp. 41-47
Journal homepage: http://iieta.org/journals/isi

An Intelligent Multi-Stage Model for Countering the Impact of Disinformation on the Cybersecurity System

Myroslav Kryshtanovych[1*], Nadiya Lyubomudrova[2], Hanna Bondar[3], Volodymyr Motornyy[4], Vitalii Kuchmenko[5]

[1] Department of Pedagogy and Innovative Education, Lviv Polytechnic National University, Lviv 79000, Ukraine
[2] Department of Human Resource Management and Administration, Lviv Polytechnic National University, Lviv 79000, Ukraine
[3] Department of Local Self-Government and Regional Development, Petro Mohyla Black Sea National University, Mykolaiv 54001, Ukraine
[4] Department of Units Daily Activities Management, Odesa Military Academy, Odesa 65125, Ukraine
[5] Department of National Security, Public Administration and Administration, Zhytomyr Polytechnic State University, Zhytomyr 10001, Ukraine

Corresponding Author Email: kryshtanovych.lpnu@gmail.com

https://doi.org/10.18280/isi.280105

Received: 20 October 2022
Accepted: 20 January 2023

Keywords:
disinformation, cybersecurity, model, information, digitalization

ABSTRACT

The main purpose of the paper is to form an intelligent multi-stage model for counteracting the negative impact of disinformation on the cybersecurity system. The research methodology involves the use of various modeling methods, including the construction of diagrams, intelligent models and matrices. The main results of the study are modeling the process of counteracting the negative impact of disinformation in the cybersecurity system for a particular region. Successful should be considered the application of a methodical approach to solving the tasks. All stages of the modeling technique were successfully completed. As a result of the study, the main intellectual multi-stage model for counteracting the negative impact of disinformation on the cybersecurity system was identified and presented. The study has a number of limitations related to the fact that it does not allow to cover all types of disinformation. Only those that, according to the authors, were of the greatest relevance today, were selected for modeling. Further research should be devoted to expanding the intellectual model, taking into account new factors of the negative impact of disinformation on the cybersecurity system.

1. INTRODUCTION

In modern society, the issue of cybersecurity is attracting more and more attention. The relevance of ensuring cybersecurity is determined by the modern development of the information society, which is moving from traditional public administration to management through electronic forms, the formation of new forms of information activity, which leads to a significant expansion of the volume of information, the penetration of its components into various areas of public activity. At the same time, the development of the information society and the established legal instruments ensure the implementation of the information rights and obligations of citizens, determine the degree of development of the information sphere, the state of the information law and order, the level of legal protection and the protection of social values.

One of the biggest threats to modern society is disinformation, which can have disastrous consequences for humanity. We don't have to look far for examples of the negative impact of disinformation. For example, 89-year-old propagandist from Rwanda Felicien Kabugu is already on trial in The Hague, who is accused of calling for genocide, financing armed groups and political organizations responsible for the 1994 genocide in Rwanda. And the Russian disinformation machine led to a full-scale war against Ukraine in 2022.

The globalization of social relations and the acceleration of technological progress determine a clear understanding that the modern information society covers all spheres of human and state life, and the cybersphere has become an important economic, political and social resource. The growing dependence of a person, society and national infrastructures (energy, transport, telecommunications) on the proper operation of information and telecommunication systems makes them vulnerable to cyber threats, which in turn increases the risk of emergencies, creates real threats to the life of a person, society, state.

Cyberspace is vast and covers every person. The cybersecurity system, by its very nature, is now a key component of national security. You don't even have to get up off the couch to get a piece of disinformation. In such conditions, the relevance and curiosity of this issue in the information space is gaining great attention.

The main purpose of the paper is to form an intelligent multi-stage model for counteracting the negative impact of disinformation on the cybersecurity system.

The structuring of the study is simple and most convenient for the reader: we analyze the literature, explain in detail the methods used, and present the main results of the study. Through the discussion section, we compare our results with similar ones in the scientific and practical community. We form the main conclusions from the study.

2. LITERATURE REVIEW

Now the level of cybercrime continues to grow at an extremely fast pace, so the concept of cybersecurity is increasingly seen as a strategic problem of the state, which causes significant harm to the economy not only of individual business entities, but also the economy of the state as a whole. This leads to the fact that cyberspace is turning into a separate sphere of hostilities, in which the armed forces of highly developed states, terrorist and criminal organizations operate. To date, the problem of ensuring security in cyberspace is being actively researched and discussed.

In the modern conditions of the information world, a special place in scientific research, which is activated every year, is occupied by cybersecurity. Recently, cybersecurity and its particular aspects have become the subject of numerous research papers.

In general, scientists believe [1-3] that the latest information technologies contribute, on the one hand, to the development of democratic regimes in the world, and, on the other hand, become a means of destabilization. Given the pluralism of opinions common in a globalizing society, the use of problematic issues by other countries allows the formation of discontent among the population and, as a result, all the prerequisites are created for manipulation in order to satisfy certain political ambitions.

According to Singh et al. [4] and Weru et al. [5], it is necessary to form a powerful regulatory a legal framework that regulates the security of the information space and, on the basis of scientific institutions or think tanks, organize a system of counter-propaganda and combat disinformation, while not forgetting the basic democratic principles. At the same time, the state is obliged to stimulate the development of the IT sector, in particular in the security system, taking into account the latest challenges and foreign policy threats.

As most scientists note [6-8], the numerous problems of mankind, which, on the one hand, were the result of the processes of globalization of the modern world, and on the other hand, turned out to be a condition for accelerating the onset of the era of this globalization, intensified the effect of such a powerful and often unpredictable side effect, the definition of which "disinformation". This phenomenon, as a virus dangerous to the social organism, is capable of exponentially spreading in the information space in a short time, parasitizing primarily on the painful problems of the world as a whole, individual regions and countries. We agree with this collective scientific opinion.

As noted, at the present stage of the latest information technologies, cybersecurity, which contains an interdepartmental character in a globalized world, is becoming relevant [9]. After all, cybersecurity is a human rights manifestation of the modern virtual world against the background of the innovative development of information technologies in the system of legal capital.

In general, as some scientists note [10-12], disinformation (especially in the context of the existence of so-called unknown variables of a global nature) turns into a national security problem that can destabilize the world order. Since disinformation and its consequences can further increase the potential threat to social stability in general, as well as to the life and health of citizens, this phenomenon should be considered precisely in the context of measuring the modern world, considering it one of the most notable challenges that has recently accompanied the process of globalization existence of any subject of information relations.

As for multisimulation, its usefulness and effectiveness has been confirmed by more than one scientific literature. For example, the works [13-15] demonstrated real practical results of multisimulation.

The key results that scientists have brought in their work are of value in developing the problem of countering disinformation in the cybersecurity system.

One of the important conclusions that can be obtained as a result of the literature review is that the problem of countering disinformation is relevant and has a lot of attention among scientists and practitioners. Other conclusions are formed on the fact that disinformation has a strong negative impact on cybersecurity.

In general, it should be noted that disinformation has not disappeared anywhere and still remains relevant. That is why, knowing due to scientific and practical achievements, the search for new means of counteracting its negative impact on the cybersecurity system is relevant.

3. METHODOLOGY

Describing the research methodology, we will try to briefly and as concisely as possible clarify all the methods we use in the article.

Of course, simple modeling is only a superficial phenomenon. There must be a specific real-world entity or example of a cybersecurity system that is negatively impacted by disinformation. In this case, the real practical experience of the authors in a particular cybersecurity system is a good initial option. To do this, we can talk about the application of the scientific method of monitoring the cybersecurity system chosen as an example.

An intellectual model implies the use of a combination of methods of graphic and language symbols and rules, using the processes and information structure for a particular process to fix itself. This modeling method involves the use of a graphic language characterized by such properties as completeness and expressiveness, accuracy, conciseness, means of information communication, lightness and simplicity. Therefore, this method was chosen for modeling.

In general, thanks to the applied methodology, the intellectual model of counteracting the negative impact of disinformation in the cybersecurity system will provide the following structure: it consists of diagrams, text fragments and a glossary. Diagrams are presented as blocks and arcs, on which neither sequence nor time is explicitly indicated. This method is difficult to perceive and there are difficulties in linking several processes.

The construction of an intelligent model is associated with the improvement of its supporting tools - software products for process modeling (for example, BPWin, ProCap, IDEF0/EM Tool, etc.).

Helps to better understand the intellectual model, the black box method. Which better graphically can clarify the system of counteracting the negative impact of disinformation (Figure 1).

In the final results for the discussion section, a matrix method was applied, which can best represent the key elements achieved through modeling. The matrix method made it possible to better depict what results the process of forming an intellectual model of counteracting negative disinformation on the cybersecurity system allows achieving.

An interesting fact is that, taking into account scientific works in a similar research area [10-20], most of them actively apply their modeling method. This only confirms the fact that the formation of one or another model can be effective for solving the problem (Figure 2).

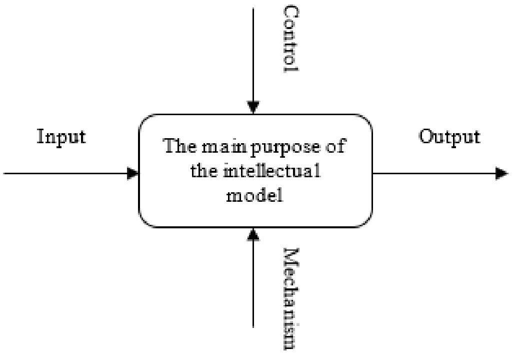

Figure 1. Black box application mechanism (formed by the authors)

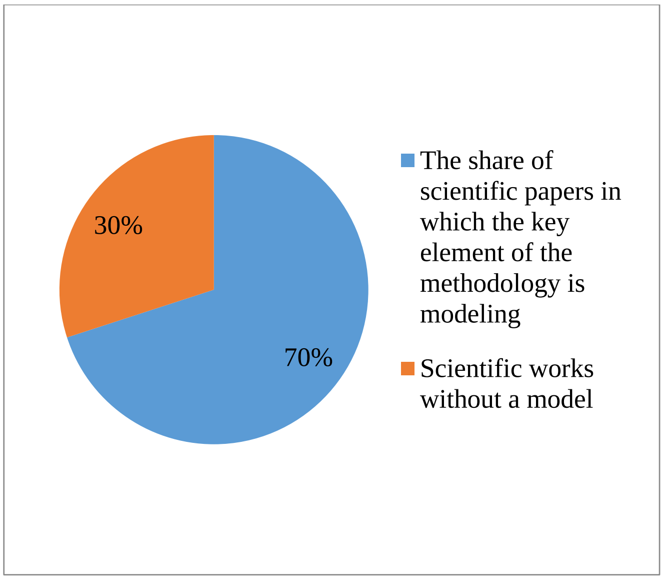

Figure 2. The share of scientific papers on this topic, applied by the modelling method [10-20]

In general, the methodology is not new and all are presented above in the text, the methods have already passed the time and practice of their effectiveness. Methods more than once [12-15] showed good efficiency in work. Various methods together will allow us to achieve our goals.

Reference were required to demonstrate the relevance and feasibility of modeling during the study. It was interesting to depict how often the modeling technique is used as the basis of any methodology. This allows us to confirm the thesis about the expediency of modeling in our article.

4. RESULTS OF RESEARCH

As a result, it was decided to choose a socio-economic system that has its own elements of cybersecurity. Such a socio-economic system, which will serve as a clear example for us to conduct modeling, will be the administrative region of Lazio in Italy. Almost 10% of the population of the region are immigrants. The capital of Italy is located in the region, and the issue of disinformation here is one of the most critical factors that can negatively affect the cybersecurity system. We will try to form our intellectual model for Lazio's cybersecurity system, based on the extensive experience of our authors living there. We have selected the most negative elements that have a significant negative impact on the cybersecurity system in the region and propose the following stages of counteraction (all stages received their own unique designation according to the method of language symbols) are presented in Table 1.

Table 1. Designation according to the method of language symbols of the stages of the intellectual model

The stages of the intellectual model	A(n)
Effective countering the negative impact of disinformation on the cybersecurity system	**A(0)**
Introduction of fact-checking technology in the information field of the region	**A(1)**
Maintaining a balance in the information field	**A(2)**
Control over the share of media others countries	**A(3)**
Implementation of media literacy strategy in cyberspace	**A(4)**

Thus, we have the main goal that the intellectual model should achieve - A(0). As a result, during simulation, it is achieved as follows (1):

$$A(1)\rightarrow A(2)\rightarrow A(3)\rightarrow A(4)=A(0) \qquad (1)$$

According to (1), each stage gradually passes into the next and thus, in the final case, we reach A(0).

It should be noted that according to the methodology, the result can be any number of A(n), but in our opinion, A(4) is enough for this intellectual model.

So, due to the introduction of the dark box method, we eventually built a constructive diagram of the basis of an intellectual model for counteracting the negative impact of disinformation on the cybersecurity system (Figure 3).

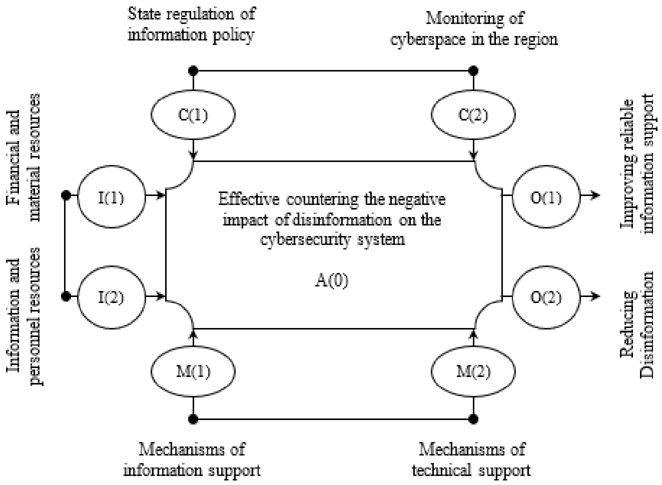
State regulation of information policy
Monitoring of cyberspace in the region
Financial and material resources
Information and personnel resources
C(1)
C(2)
I(1)
I(2)
Effective countering the negative impact of disinformation on the cybersecurity system
A(0)
O(1)
O(2)
M(1)
M(2)
Improving reliable information support
Reducing Disinformation
Mechanisms of information support
Mechanisms of technical support

Figure 3. Constructive diagram of the basis of the intellectual model of counteracting the negative impact of disinformation on the cybersecurity system (formed by the authors)

I(n) and O(n) according to the black box method are inputs and outputs. In our case, these are the resources that are directed to achieve the goal of the intellectual model and the desired result that can be obtained at the output (2):

$$I(1)+I(2)\rightarrow O(1)+O(2) \quad (2)$$

In total, all inputs should give a certain socio-economic effect and turn into outputs.

M(n) and C(n) are mechanisms and control according to the methodology presented in Figure 1. At the same time, according to the methodology, the achievement of the main goal of the intellectual model A(0) is also achieved through (3):

$$(M(1)+M(2))+(C(1)+C(2))=A(0) \quad (3)$$

It should be noted that in total, the mechanisms and elements of control together make it possible to achieve A(0).

Cyberspace is a new channel for the creation and dissemination of a variety of information, it has become a new engine of economic growth, a new platform for social management, a new way of international cooperation, and a completely new sphere of state sovereignty. In this context, it is extremely important to build an effective intellectual model to counteract the negative impact of disinformation in the cybersecurity system (Figure 4).

It should be noted that the intersection of lines should not be mandatory, this only happens when several arrows go into the same object. Arrow lines only where needed to concretize an action or influence.

A(1). Introduction of fact-checking technology in the information field of the region. Internet disinformation is a problem that crosses borders, both national and disciplinary. It is becoming increasingly clear that a solution to the problem cannot be found without significant international and interdisciplinary cooperation. Thus, in the conditions of information wars and manipulations, the need to verify the reliability of information and facts circulating in our information environment is growing. Fact-checking is fact-checking to provide accurate, unbiased analysis of public statements in order to correct public misperceptions and raise awareness of important issues. It should be noted that the verification of information is based on official documents. In cyberspace, there should be constant elements of fact-checking for the public as part of ensuring cybersecurity.

A(2). Maintaining a balance in the information field. Firstly, it is necessary not to allow propaganda, referring to liberalism and pluralism of opinions. Countering disinformation should not be confused with censorship, which is banned in most democracies. There may be different views in a society, but there cannot be two different truths. If the information distorts this or that event or fact, the source disseminating such news must be found. If it disseminates fake news systematically and purposefully, it should be banned.

A(3). Control over the share of media others countries. The region should pay attention to cases when the share of mass media of another state grows in its information space. This means when a society draws a certain, fairly significant percentage of information precisely from information sources belonging to a particular country.

A(4). Implementation of media literacy strategy in cyberspace. Media literacy appears as a result of the process of media education and plays a significant role in the activities of the region, because it is necessary to inform people about the phenomenon of disinformation, about how it can interfere in various political processes and make adjustments to the course of events, so it is necessary to teach the public to respond correctly to these threats. Media literacy is one of the key forms of protection against the destructive influence of disinformation and fake news spread through digital media. Critical thinking and education play a major role for citizens, because it is thanks to these skills that the further effective use of social networks is possible.

A characteristic feature of the intellectual model is that each stage can be detailed and analyzed. For an illustrative example, we take stage A(4), which is the final one, and it determines what the output will be (Figure 5).

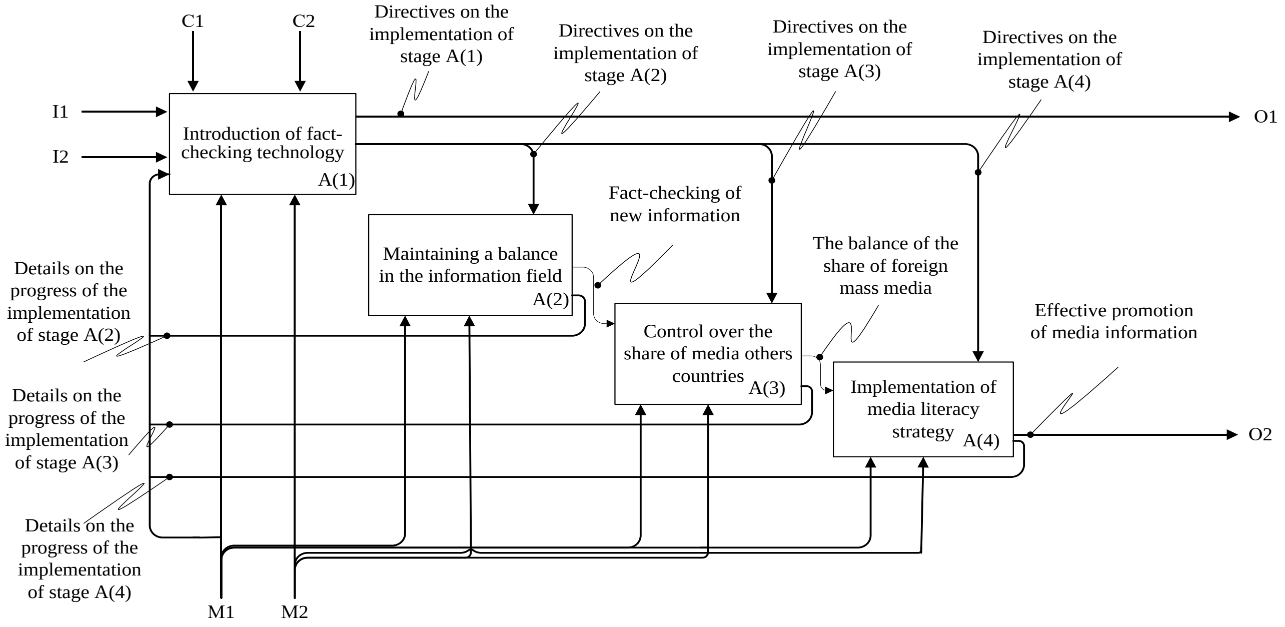
C1
C2
Directives on the implementation of stage A(1)
Directives on the implementation of stage A(2)
Directives on the implementation of stage A(3)
Directives on the implementation of stage A(4)
I1
I2
O1
Introduction of fact-checking technology
A(1)
Fact-checking of new information
Maintaining a balance in the information field
A(2)
The balance of the share of foreign mass media
Details on the progress of the implementation of stage A(2)
Effective promotion of media information
Control over the share of media others countries
A(3)
Implementation of media literacy strategy
A(4)
Details on the progress of the implementation of stage A(3)
O2
Details on the progress of the implementation of stage A(4)
M1
M2

Figure 4. An intellectual multi-stage model for countering disinformation in the cybersecurity system in the region (formed by the authors)

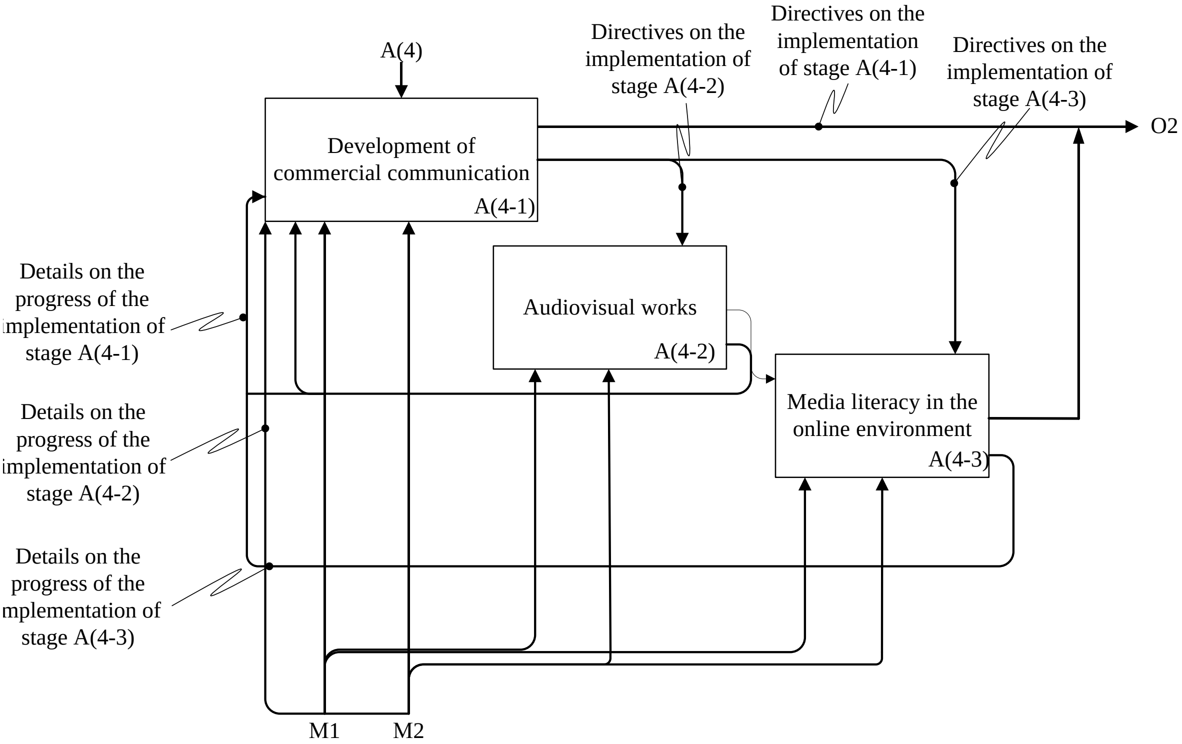
A(4)
Directives on the implementation of stage A(4-2)
Directives on the implementation of stage A(4-1)
Directives on the implementation of stage A(4-3)
O2
Development of commercial communication
A(4-1)
Audiovisual works
A(4-2)
Media literacy in the online environment
A(4-3)
Details on the progress of the implementation of stage A(4-1)
Details on the progress of the implementation of stage A(4-2)
Details on the progress of the mplementation of stage A(4-3)
M1
M2

Figure 5. Auxiliary intellectual model for achieving stage A(4) "Implementation of media literacy strategy in cyberspace" (formed by the authors)

A(4-1). Development of commercial communication. Since advertising plays a leading role in our lives today, it is important to raise audience awareness about commercial communication. In this area, media literacy focuses on two aspects: providing young audiences with the tools to develop a critical approach to commercial communication that allows them to make informed choices; encouraging public or private funding with due transparency in this area.

A(4-2). Audiovisual works. In this context, media literacy involves: providing European audiences with a better awareness of the heritage of the film industry and increasing interest in European films, as well as understanding the importance of copyright on the part of both consumers and content creators.

A(4-3). Media literacy in the online environment. For the online environment, media literacy should include: providing tools to critically evaluate online content; ensuring that the full benefits of the information society can be enjoyed by all, including people with disabilities and those at a disadvantage due to limited resources, education or ethnicity.

In general, making intermediate conclusions on the results of the study, we can say that, unlike other scientists [10-20], we made an attempt to clarify in detail the process and operation of our intellectual model and all its elements. Taking as an example the cybersecurity system of a particular region, we tried to adapt the methodological approach to the conditions of this socio-economic system.

5. DISCUSSIONS

A certain group of scientists [13-15] focuses on the problems of the legal field regarding misinformation in the cybersecurity system. Issues of legal regulation of public relations that arise in the course of informing the population should be considered in the context of ensuring cybersecurity. In legal regulation, a significant amount of information is implemented by the function of the state, which is determined by the needs of national security. The inevitability of the spread of disinformation is obvious, and the lack of legal regulation of its circulation weakens the national security system. But, in our opinion, the problem is not only this, and that is why we do not focus much attention on legal regulation during the simulation.

Some researchers in their scientific papers [16-18] note that sustainability in the field of cybersecurity is formed based on the understanding of cyberspace as having fundamental uncertainties regarding the nature and forms of manifestation of hybrid cyberthreats, the time of their manifestation and distribution, and therefore acquires the content of the target setting based on normative implementation of an effective mechanism of administrative and legal regulation and subject to the implementation as measures of a system for assessing the risks of manifestation of hybrid threats and determining the vulnerability of society. However, our novelty lies not in the revealed essences of ensuring cybersecurity, but in a specific focus on the intellectual model of counteracting the negative impact of disinformation on the cybersecurity system itself as a whole.

The issue of modeling to counteract the negative impact of a particular phenomenon on the security system is not new. For example, Sylkin et al. [19] also used similar modeling methods in their work. However, our scientific direction of research and its results are fundamentally different.

For clarity, let's present a matrix of tasks solved as a result of the formation of an intellectual model to counteract the negative impact of disinformation in the cybersecurity system (Table 2).

It should be noted that, as can be seen from Table 2, not all tasks were completed as a result of the simulation, but only those that were outlined and set by us. We do not seek in one study to form such an intellectual model that would solve all the problems of disinformation in cyberspace. It takes time, but the first steps have already been taken.

Table 2. Information matrix of solved problems as a result of the existing intellectual model

A(n)	The problem of reliability of information	The problem of balancing in cyberspace	High proportion of foreign media	Lack of media literacy
A(1)	+	-	-	-
A(2)	-	+	-	-
A(3)	-	-	+	-
A(4)	-	-	-	+

6. CONCLUSIONS

Summing up, it should be noted that the development of the information society, made possible by the integration of new technologies in every sphere of life and all types of infrastructures, increases the dependence of individuals, organizations and countries on information systems and networks. Safety is the main component of any activity. It should be considered as a service that contributes to the formation of the possibility of creating other services and added value, in particular, the digitalization of the country, e-government, e-learning, e-health services. Security is not just a matter of technology. Along with this, until now, the main communication tools available have not had the resources necessary and sufficient to provide and maintain a minimum level of security. Networked information technology systems can be accessed at a distance and thus be a potential target for cyberattack and disinformation. Systems are at increased risk of intrusion and the possibility of attacks and offenses is increased. Along with the fact that the target of attacks is systems, the actions of offenders are aimed at disinformation of everything processed, transmitted or stored.

The scientific novelty of the results obtained lies in the fact that this study is one of the first in the field of building an intellectual model to counteract the negative impact of disinformation on the cybersecurity system. The practical significance of the results obtained lies in the fact that they are of scientific, theoretical and practical interest. The generated results can be used in the research field to form the theoretical basis for further scientific research in the relevant areas.

The study has a number of limitations related to the fact that it does not allow to cover all types of disinformation. Only those that, according to the authors, were of the greatest relevance today, were selected for modeling. Further research should be devoted to expanding the intellectual model, taking into account new factors of the negative impact of disinformation on the cybersecurity system.

It should be noted that at this stage of the study, the proposed model and the implemented methodological approach have no real practical application, however, in further studies, we plan to test for the convenience of its use.

REFERENCES

[1] Vieane, A., Funke, G., Gutzwiller, R., Mancuso, V., Sawyer, B., Wickens, C. (2016). Addressing human factors gaps in cyber defense. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 60(1): 770-773. https://doi.org/10.1177/1541931213601176

[2] Prause, G., Atari, S. (2017). On sustainable production networks for Industry 4.0. Entrepreneurship and Sustainability Issues, 4(4): 421-431. https://doi.org/10.9770/jesi.2017.4.4(2)

[3] Žižlavský, O. (2013). Past, present and future of the innovation process. International Journal of Engineering Business Management, 5(47): 1-8. https://doi.org/10.5772/56920

[4] Singh, M., Iyengar, S., Kaur, R. (2022) Mining social networks for dissemination of fake news using continuous opinion-based hybrid model. Advanced Data Mining and Applications. https://doi.org/10.1007/978-3-030-95405-5_16

[5] Weru, T., Sevilla, J., Olukuru, J., Mutegi, L., Mberi, T. (2017). Cyber-smart children, cyber-safe teenagers: Enhancing internet safety for children. 2017 IST-Africa Week Conference (IST-Africa), Windhoek, Namibia, pp. 1-8. https://doi.org/10.23919/ISTAFRICA.2017.8102292

[6] Gordieiev, O., Kharchenko, V., Illiashenko, O., Morozova, O., Gasanov, M. (2021). Concept of using eye tracking technology to assess and ensure cybersecurity, functional safety and usability. International Journal of Safety and Security Engineering, 11(4): 361-367. https://doi.org/10.18280/ijsse.110409

[7] Ismail, A., Saad, M., Abbas, R. (2018). Cyber security in internet of things. Review of Computer Engineering Studies, 5(1): 17-22. https://doi.org/10.18280/rces.050104

[8] Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. Wireless Networks, 20: 2481-2501. https://doi.org/10.1007/s11276-014-0761-7

[9] Mohelska, H., Sokolova, M. (2018). Management approaches for Industry 4.0 – the organizational culture perspective. Technological and Economic Development of Economy, 24(6): 2225-2240. https://doi.org/10.3846/tede.2018.6397

[10] Giannarakis, G., Zafeiriou, E., Sariannidis, N., Efthalitsidou, K. (2016). Determinants of dissemination of environmental information: an empirical survey. Journal of Business Economics and Management, 17(5): 749-764. https://doi.org/10.3846/16111699.2016.1195771

[11] Chowdhury, N., Nystad, E., Reegård, K., Gkioulos, V. (2022). Cybersecurity training in Norwegian critical infrastructure companies. International Journal of Safety and Security Engineering, 12(3): 299-310. https://doi.org/10.18280/ijsse.120304

[12] Pastor, V., Diaz, G., Castro, M. (2010). State-of-the-art simulation systems for information security education, training and awareness. IEEE EDUCON 2010 Conference, pp. 1907-1916. https://doi.org/10.1109/EDUCON.2010.5492435

[13] Kryshtanovych, M., Filippova, V., Huba, M., Kartashova, O., Molnar, O. (2020). Evaluation of the implementation of the circular economy in EU countries in the context of sustainable development. Business: Theory and Practice, 21(2): 704-712. https://doi.org/10.3846/btp.2020.12482

[14] Kryshtanovych, M., Antonova, L., Filippova, V., Dombrovska, S., Pidlisna, T. (2022). Influence of COVID-19 on the functional device of state governance of economic growth of countries in the context of

ensuring security. International Journal of Safety and Security Engineering, 12(2): 193-199. https://doi.org/10.18280/ijsse.120207

[15] Kryshtanovych, M., Ortynskyi, V., Zakharyash, O., Maziy, N., Krasivskyy, O. (2011). The impact of threats on the cybersecurity system of public administration in the context of the development of financial technologies. 2021 11th International Conference on Advanced Computer Information Technologies (ACIT), 2021, pp. 510-513. https://doi.org/10.1109/ACIT52158.2021.9548603

[16] Fakiha, B. (2021). Business organization security strategies to cyber security threats. International Journal of Safety and Security Engineering, 11(1): 101-104. https://doi.org/10.18280/ijsse.110111

[17] Satish Babu, J., Krishna Mohan, G. (2022). An intelligent multi-objective evolutionary model for establishing security in cyber-physical systems. Ingénierie des Systèmes d'Information, 27(2): 213-221. https://doi.org/10.18280/isi.270205

[18] Petroye, O., Lyulyov, O., Lytvynchuk, I., Paida, Y., Pakhomov, V. (2020). Effects of information security and innovations on country's image: Governance aspect. International Journal of Safety and Security Engineering, 10(4): 459-466. https://doi.org/10.18280/ijsse.100404

[19] Sylkin, O., Kryshtanovych, M., Zachepa, A., Bilous, S., Krasko, A. (2019). Modeling the process of applying anti-crisis management in the system of ensuring financial security of the enterprise. Business: Theory and Practice, 20: 446-455. https://doi.org/10.3846/btp.2019.41

[20] Zollo, F., Novak, P.K., Del Vicario, M., Bessi, A., Mozetič, I., Scala, A., Caldarelli, G., Quattrociocchi, W. (2015). Emotional dynamics in the age of misinformation. PloS One, 10(9): e0138740. https://doi.org/10.1371/journal.pone.0138740