

ANALYSIS OF INFORMATION SECURITY UNDER THE CONDITIONS OF HYBRID WAR IN UKRAINE: SOCIAL ASPECTS

Dariusz Krawczyk

Silesian University of Technology

Vitalina Babenko

Daugavpils University,

Kharkiv National Automobile and Highway University

Liudmyla Yemchuk

Khmelnytskyi National University

Serhii Lienkov

Research Center Military Institute of Taras Shevchenko National University of Kyiv

Volodymyr Dzhulii, Larysa Dzhulii, Ihor Muliar

Khmelnytskyi National University

Abstract:

The development of the post-industrial society requires the acceleration of the integration of the national economy into the globalized economic space. This stage is characterized by active informatization of all spheres of life in society, which requires information security and cyber protection for high-quality information provision of the country's population, intellectualization of economic processes and prevention of destructive informational influence on the social status of the individual. It is also necessary to consider that for Ukraine the specified stage is complicated by the hybrid war with Russia, which requires strengthening the protection of information from cyber-attacks and the formation of new approaches in preserving the quality of information on social networks. Therefore, the purpose of this article is the development of scientific and methodological approaches in information security management, strengthening its social significance. This requires solving a certain range of tasks of identifying and preventing socially dangerous information based on the use of economic and mathematical methods and models. The article highlights the main directions of socialization of modern technological development and theoretically substantiates its significant impact on human consciousness and behavior, puts a person in front of serious challenges and, under conditions of hybrid warfare, requires strengthening of information security in social networks. In the work, the components of information security are supplemented, its impact on social aspects of society's life is highlighted. As a result of the research, the authors proposed a scientific and methodical approach to the construction of a system for countering the spread of socially dangerous information in social networks. Besides, its functional elements are highlighted. A method of combating the spread of harmful information in social networks has been developed, which solves the problem of information support of the decision-making process and includes providing the chosen and alternative options to the person making the decision, with the justification of the choice. This creates prerequisites for information support for making a well-founded management decision.

Key words: *cyber security, social networks, harmful information, hybrid warfare, countermeasures*

INTRODUCTION

The dialectic of civilization of the 21st century is determined by globalization, the formation of the world economic space, with inherent hyper-competition, armed

conflicts and hybrid wars. As evidenced by the current complex situation in Ukraine, hybrid war covers fundamentally different types and ways of conducting it, which are used in a coordinated manner to realize the set

goal. The typical components of a hybrid war should primarily include socio-economic tools, the use of which contributes to the intensification of internal conflicts in the state chosen for aggression: the creation of socio-economic problems through socio-economic confrontation with the transition to socio-economic war and the strengthening of the relationships between the affected country and partner countries; dissemination of false information, organization of information war and information colonialism and terrorism; strengthening of internal public, political, economic and social contradictions, etc. The development of conflict in various spheres of social life is largely facilitated by the means of mass communication.

They are able to manipulate the opinions of the population of entire regions and the country in general, and by promoting certain ideals, lead to the aggravation of the situation and bloodshed over a long period of time.

Therefore, for Ukraine today, in the conditions of a hybrid war with Russia and the formation of a digital economy, one of the key problems is the creation and maintenance of information security of social networks as a component of cyber security, in which information becomes the most important resource capable of ensuring the victory of Ukraine.

REVIEW OF SOURCES, RESEARCH METHODS

Many scientists paid attention to the study of problematic aspects of information security and cyberspace. The relevance of the chosen direction of scientific research is due to the fact that confrontation in the information sphere is becoming a fundamentally new sphere of rivalry between states, and what is extremely important, between Ukraine and Russia in the conditions of a hybrid war [1, 2]. The development of information and communication technologies, the formation of a global information space has led to the emergence of many cyber threats in almost all spheres of financial, political, environmental, economic, social, cultural life of society [3, 4, 5, 6].

The conclusion of H. Sashchuk about the impact of information attacks on the social directions of the development of society is extremely important: "Taking into account the fact that under the influence of information attacks, the worldview and morality of both individuals and society in general can be purposefully changed, other people's interests, motives, lifestyles are imposed, the analysis of the essence and forms of the manifestations of modern methods of covert aggressive influence, the manifestation of actions (that have a purposeful aggressive nature and are contrary to the interests of national security) comes to the fore" [7].

This approach is shared by many other researchers in their works [7, 8, 9, 10, 11]. Also, in the writings of scientists, attention is focused on the need to ensure a reliable digital space through the improvement of legislation and policy in the field of cyber security [12, 13, 14], as cyber threats slow down the development of the digital economy [9] as the basis for the development of the modern global digital space.

The conducted comparative analysis of research in the field of countermeasures and detection of harmful information in social networks made it possible to determine the general requirements for the countermeasure system, the model-methodical apparatus is the basis of implementation [2, 15, 6, 16].

The lack of material form in the studied objects (cyber threats, cyber-attacks, software, databases, etc.) implies their evaluation using both qualitative and quantitative indicators, using the method of expert evaluations and tools of economic and mathematical modeling.

CYBER SECURITY AS THE BASIS OF INFORMATION PROVISION OF SOCIO-ECONOMIC SYSTEMS

Based on the research of scientific works, it should be concluded that in a generalized form, cyber security is understood as a set of special legal, organizational, and technical measures, the implementation of which allows to ensure the protection of information computer systems, networks, and various software applications from cybernetic attacks by intruders [5, 15]. Cyberattacks are aimed at disabling both national and global financial-economic, technical-technological, multimedia and energy systems, as well as causing damage to both enterprises and individual countries. And this trend is constantly growing with the spread of digitization and computerization.

This is confirmed by such information that today, according to expert estimates, there are about six thousand shadow markets in the world where 45 thousand products or services are sold for committing cybercrimes, and the fastest growing market in this area is the market for computer hacking services [5, 12, 13].

In essence, the modern struggle of Ukraine in the hybrid war with Russia for its own independence is also an information struggle, which is carried out in the following directions: information intelligence – search, collection, systematization and analysis of information about cyber attacks, cyber threats; information risks and threats; organization of cyber systems and planning of information activities at the tactical (local, intra-Ukrainian), operational (with neighboring countries) and strategic (together with countries that strongly influence the development of geopolitics) levels; conducting events of an informational nature (informational operations, actions, promotions) in order to implement the objectives of the state's internal and foreign policy; evaluation of the effectiveness of information measures – determination of the level of achievement of planned results.

Under such conditions, the correct organization of both macro- and micro-level information security as a component of cyber security becomes important, which involves its construction in compliance with the following requirements and characteristics (Figure 1).

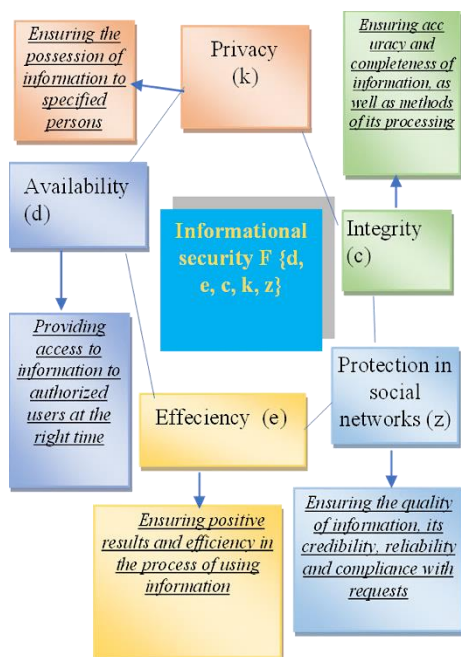


Fig. 1 Main characteristics of information security

Today, everyone's attention is focused on the information of social networks, which directly or subconsciously motivate a person to decisive actions, global thinking, business development, learning and intellectualization of everyday actions.

But if low-quality information is spread in social networks, the actions of a person will be the opposite, which will increase the moral impoverishment of the nation.

Therefore, the main tasks of information security should also include ensuring the quality of information, its value and truthfulness for all sections of the country's population.

INFORMATION SECURITY OF A SOCIAL NETWORK AS A GUARANTEE OF SOCIAL STABILITY OF SOCIETY

In today's conditions, when the world is moving to a new paradigm of technological development, based on ICT infrastructure and digital technologies, the social environment of the development of states needs adequate changes that will contribute to the implementation of social values in strategies, programs and projects adequate to global challenges.

Therefore, determining the trends of technological development of the world economy and society and forecasting the impact of the technological imperative on society should become a reference point for a wide range of alternatives for future human development and the development of approaches to the implementation of long-term projects, the implementation of appropriate management changes, which should be implemented in the network environment, including social networks. Accordingly, it is extremely important for Ukraine to use all the chances of the transition to social policy, which, based on the quality of human capital, should become the driver of socio-economic growth and the development of sustainable economic development.

The extremely negative dynamics of migration processes, which are currently turning into a threat not only to the

development of human capital, but also to the development of the economy and national security as a whole, as well as insufficient attention to the development of the country's human capital over a long period of time lead to significant public costs, cause damage to people's well-being, limit the possibilities of sustainable growth and management efficiency.

Without investment in the country's population, its social standards, it is impossible to ensure strong economic and sustainable development of the country.

During the hybrid war in Ukraine, there is a change in ideas, social and moral values, as well as the growth of global transformations, among which there is a significant lag in human knowledge from changes in the modern techno-economic sphere.

Despite the difficult socio-economic situation, Ukraine still has significant reserves for developing the potential of human capital. Accordingly, the main task is to focus political and economic instruments and implement transformative transformations in the socio-economic sphere to ensure further development of potential and its direction to build sustainable development and preserve and improve the social standards of the population.

The influence of information security on the social components of person's social life is presented in Figure 2.

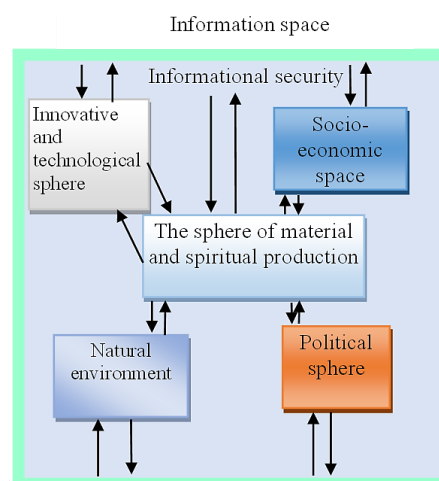


Fig. 2 Scheme of the impact of information security on social aspects of society's life

Therefore, information security, based on modern achievements in the techno-economic sphere, controlling the tools of their spread, strengthens the economic effects through the actualization of the intellectual component and affects the social aspects of the country's development, which are fundamental in ensuring sustainable development on a global scale. Therefore, the creation of a positive image based on the growth of social standards of self-education, intellectuality, professionalism, high qualification (which is extremely important in the conditions of obtaining a quick victory and modernization of society) requires special attention in Ukraine.

Solving the tasks of building a system to counteract the spread of socially and socially dangerous information in social networks

To build a system to counter and prevent the spread of socially dangerous (harmful) information in social networks, we will determine its fundamental elements of functionality (Figure 3). The countermeasure system (Figure 3) can be a central element in the process of detecting malicious messages in social networks. Processes in the system of combating and detecting malicious messages in a social (Internet) network can be automated using the proposed algorithms and appropriate software components.

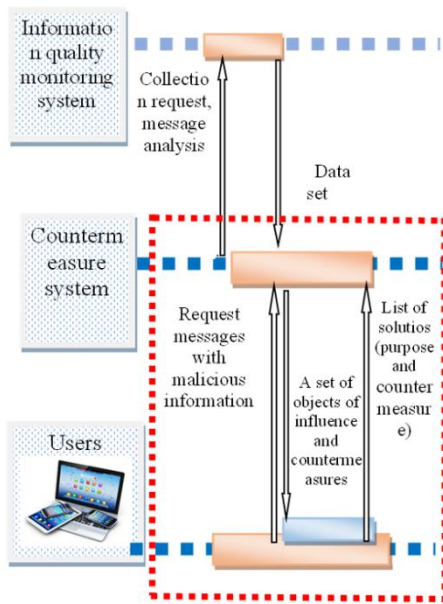


Fig. 3 Fundamental elements of the functionality of the system for preventing the spread of socially dangerous information in social networks

The requirements for the countermeasure system will be divided into two groups: functional and non-functional. Functional requirements can be implemented by designing and developing the architecture of components, software prototypes. Functional requirements – functions that the countermeasure system must perform. Non-functional requirements can be implemented by developing appropriate models and algorithms. Non-functional requirements describe the target characteristics of the system: responsiveness, requirements for reasonableness and resource consumption.

Functional requirements for the system of countering the spread and detection of harmful information in social networks include: formation of a message collection task; analysis of messages for the monitoring system; analysis of message sources in the received data set; adjustment of available measures for detecting and countering the spread of harmful information in the information and analytical system; sorting and ranking of objects of influence on the received data set; selection of means of influence for countermeasures; sorting and ranking the available countermeasures from the countermeasure database for the corresponding set of received data; generation of

reports on the operation of the system of detection and countermeasures in an adapted form, for the system administrator; generation of reports on the obtained results in an adapted form for an information security expert.

For the functioning of the system, it is necessary to solve many problems, which are in the development of: models of harmful information, sources of messages and social networks; algorithms for analyzing the sources of the spread of harmful information in social networks and ranking countermeasures; the method of detecting and countering the spread of harmful information in social networks, taking into account the requirements for reasonableness; development of the architecture of the components of the information and analytical system for combating the spread of harmful information in social networks.

Method of preventing the spread and detection of harmful information in social networks

Prevention of the spread of harmful information can be carried out on the basis of the conducted analysis and research of message sources [6, 15, 17]. Users of social networks are the object of the destructive influence of harmful information. Each user leaves a corresponding trace when viewing a message on the network and can leave a corresponding reaction. Thus, the algorithm for evaluating message sources must take into account feedback from users of harmful information in the social network, in the process of information exchange. The set *ACTIVITY* includes all signs of feedback from users of harmful information on a social network (1):

$$ACTIVITY \left\{ \begin{matrix} countrepost, countLike, \\ countComment, countView \end{matrix} \right\}, \quad (1)$$

where:

countrepost – the number of links to the source ("reposts"),

countLike – number of marks,

countComment – number of comments,

countView – number of views.

The *SOURCE*{*sourceID*,*messageURL*} set includes the source identifier, the address of messages in the social network.

Thus, it is necessary to find a tuple of attributes, based on the elements of the set and the relation *R*, which characterize *SOURCE* (2).

$$R(SOURCE, MESSAGE) - < index_{active}, index_{viewability}, index_{impact} >, \quad (2)$$

where:

index_{active} – activity index,

index_{viewability} – view index,

index_{impact} – index of influence of the message source.

The value of the indices of viewing, activity, influence of the message source is in the range [0-2], normalization – comparative normalization is applied to the index values, the ideal value is the maximum.

Let's consider the algorithm for evaluating the sources of social network messages:

1. The input of the algorithm is a tuple:

$\langle sourceID, messageURL, repostCount, likesCount, commentCount, viewCount \rangle$.

2. Calculation of the activity index of social network message sources: hash tables are formed (key-value) – $\langle sourceID, urlCOUNTER \rangle$, $\langle messageURL, likesCount \rangle$, $\langle messageURL, commentCount \rangle$, $\langle messageURL, repostCount \rangle$; the following hash table summarizes the indicators $commentCount$, $repostCount$, $likesCount$ for $messageURL$, a tuple is formed, in this case $\langle message.SourceID, activityIndex \rangle$; values from the tuple are added $\langle message.SourceID, activityIndex \rangle$, the result is divided by the indicator $urlCOUNTER$ from the first hash table, thus forming a set of activity indices of message sources to which normalization is applied.

3. Calculation of the index of viewing sources of social network messages: hash tables are formed (key-value), $\{SourceID: urlCOUNTER, messageURL: viewCount\}$. Values $viewCount$ of all

$messageURL$ are added up and the result is divided by $urlCOUNTER$. As a result, a tuple $\langle SourceID, viewIndex \rangle$ is formed. Indexes of views are normalized.

4. Calculation of the index of influence of the source of messages of social networks: for each source of messages, the indexes of views and activity are multiplied, as a result we will get the value of the index of influence, we will also use comparative normalization for it. At the output of the algorithm for evaluating the sources of social network messages, a tuple is formed $\langle sourceID, activityIndex, viewIndex, impactIndex \rangle$.

The algorithm for evaluating the sources of social network messages in the process of information exchange considers feedback and turns its quantitative characteristics from the audience of the spread of harmful information into qualitative indices.

We will also analyze the algorithm for sorting objects of social network influence. The basis of existing solutions and methods of countering the spread of harmful information in social networks is the approaches of identifying information objects with harmful information [18, 19, 20]. The considered approaches are based on the concept – "detection-countermeasure" of information objects [6, 15]. There are millions of information objects that contain sources of harmful information in social networks. Information objects can be divided by activity indices and source potential, thus, a filter can be applied in the process of selecting a countermeasure information object and set a priority. The algorithm for sorting information objects of influence of the social network is related to algorithms for evaluating message sources and ranking by

potential, and receives input data from them, sorts information objects of influence by priority at the output. The

objective function of the objects of influence by priority is given by the following formula:

$$f(S) \rightarrow I_{pr}^S = I_p^S + I_i^S = [0, 4], \quad (3)$$

where:

S – message source,

I_{pr}^S – message source priority,

I_p^S – potential,

I_i^S – influence index.

Rules for choosing the object of influence $Target$:

$\{source \in TARGET \mid I_{pr}^S \equiv \max\}$;

$\{message \in TARGET \mid I_{pr}^S \equiv \min\}$,

where:

$TARGET$ – set of information objects of influence.

The algorithm for sorting objects of social network influence is shown in Figure 4.

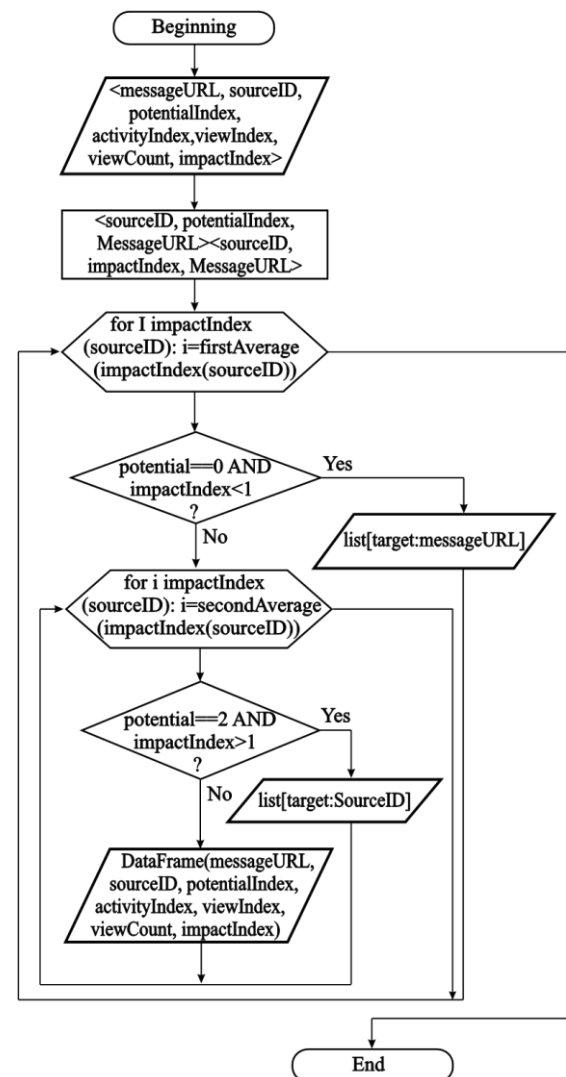


Fig. 4 Algorithm for sorting social network influence objects

A set of tuples is passed to the input of the object sorting algorithm (Figure 4):

$\langle \text{messageURL}, \text{sourceID}, \text{potentialIndex}, \text{activityIndex}, \text{viewIndex}, \text{impactIndex} \rangle$.

At the first stage of the algorithm, the arithmetic average of the impact index of all message sources is calculated, low and high priority objects are distinguished. Tuples with a priority index are formed $1 \leq I_{pr}^s \leq 3$

$\langle \text{messageURL}, \text{sourceID}, \text{potentialIndex}, \text{activityIndex}, \text{viewIndex}, \text{impactIndex} \rangle$.

The result of the algorithm is a set of tuples and two lists: a set of *Priority_Medium* tuples, which is passed to the operator for selection and additional evaluation of the information object of influence between the address of the page in the social network and the address of the message; *Priority_High* – the *Target, sourceID* are an informational object of influence, for the adoption of countermeasures, they have a high priority; *Priority_Low* – the *Target, messageURL* are an information object of influence, for taking countermeasures, they have a low priority. The algorithm for sorting information objects of social network influence forms priority lists to counter the spread of harmful information.

Our proposed method of countering the spread of harmful information in social networks solves the problem of information support for the decision-making process and includes: conducting an analysis of collected and processed information; development, based on the analysis of messages, decision options; evaluation of received options, selection of the best option; providing the chosen and alternative options to the decision-maker, with justification for the choice (Figure 5).

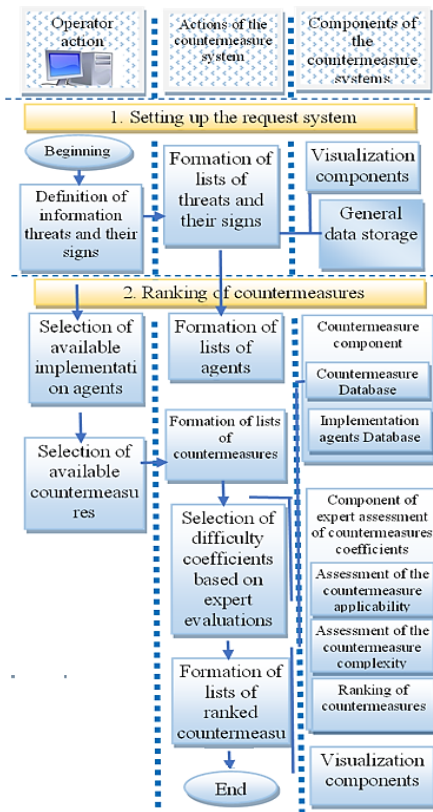


Fig. 5 Method of countering the spread and detection of harmful information in social networks

The countermeasure method, according to the life cycle of information systems, is divided into two stages: configuration and operation. The stage of forming input data and setting up the countermeasures system provides: lists of countermeasures available in the system, their coefficients; lists of informational threats; lists of available sales agents; a list of ranked countermeasures is formed.

The operation stage includes: analysis of objects of influence and their sorting; receiving information from the monitoring system; formation of "goal-countermeasure" matches; launching countermeasures.

The proposed algorithms and method are implemented within the framework of the system for countering and spreading harmful influence in social networks [22]. The architecture of the system for countering the spread of harmful information in social networks includes eight components and three levels (Figure 6) – management level: visualization component, management component; content assessment level: component of assessment and analysis of message sources, database, SQL server; level of implementation of countermeasures: component of selection of countermeasures, component of implementation of countermeasures.

The input data of the method of countering the spread of harmful information in social networks are: parameters of objects of influence, according to which the operator distributes the sequence of making a decision on countermeasures; established "target-countermeasure" matches to counter the spread of harmful information in social networks through available implementation agents; countermeasures and their coefficients, information threats, available agents for the implementation of countermeasures, signs [21].

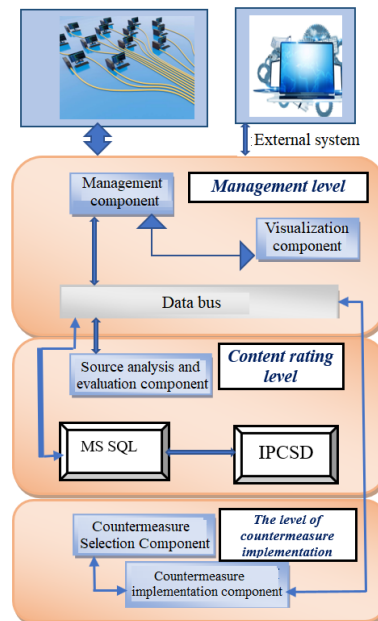


Fig. 6 Architecture of the anti-malicious information system in the social network

Management level – the functions of the manager component include tasks within the system and load management, the functions of the visualization component with the operator of the anti-malware system

provide communication, the data bus is intended for data transmission between the components of the anti-malware system; level of content evaluation – the component of evaluation and analysis of message sources includes the functions of evaluating the parameters of objects of influence, ranking by potential, prioritization, there is a component for database management (SQL Server), which manages the database of countermeasures and information threats; level of implementation of countermeasures – the component of the selection of countermeasures includes the tasks of the system of forming lists of countermeasures and the goals of supporting decision-making, the component of implementation of countermeasures maintains communication with implementation systems, external agents.

The proposed method of countering the spread and detection of harmful information in social networks, taking into account the requirements for reasonableness, at various stages of the life cycle allows: to determine the potential of the source of messages, the value of which depends on the number of messages on the page; to estimate the activity index of the source of network messages, the value of which is affected by the level of activity of users of messages containing malicious information; to evaluate network message viewing indices, as well as sources; to determine the influence index of the message source, the value of which depends on the activity and viewing of information in general.

EVALUATION OF THE METHOD OF COUNTERING THE SPREAD AND DETECTION OF HARMFUL INFORMATION IN SOCIAL NETWORKS

The main requirements for the method of countering the spread and detection of harmful information in social networks are divided into groups: efficiency; reasonableness; resource consumption.

Evaluation of efficiency corresponds to the following steps: at the stage of setting up the system for countering the spread of harmful information – ranking countermeasures, setting up the request system; at the stage of operation of the system for countering the spread of harmful information – a request for data collection, sorting and ranking of information objects of action, countering the spread of harmful information. The execution time of the process of countering the spread of harmful information in social networks will consist of the duration of the analysis operations of the following steps (4):

$$T^M = T_1^{HC} + T_2^{HC} + T_1^{EC} + T_2^{EC} + T_3^{EC}, \quad (4)$$

where:

T_i – the i -th step execution time.

The time of execution of the steps of the process of countering the spread of harmful information in social networks is considered as a random variable, the probability is subject to the law of normal distribution. The expected time of the process of countering the spread of harmful information in social networks and its variance are calculated using the two-valued method [1]. The probability

that the execution time of the i -th step will not exceed the permissible value $T^{additional}$, is calculated according to the following formula (5):

$$P_{op}(T \leq T^{additional}) = \Phi(Z), \quad (5)$$

where:

$\Phi(Z)$ – the Laplace function for (6):

$$Z = \frac{T^{additional} - \sum_{i=1}^n T_i}{\sqrt{\sum_{i=1}^n \sigma_i^2(T_i)}}, \quad (6)$$

The most time-consuming process of countering the spread of harmful information in social networks from the point of view of efficiency is the operator's working time, respectively, at the stage of setting up the system and at the stage of operation. The experts evaluated the following tasks: the time needed by the operator to identify information threats, their signs (the expert fills in a table with three threats and their signs); the time the operator spends on choosing the appropriate available implementation agents and countermeasures (the expert fills in the table with available implementation agents and countermeasures; time required by the operator to fulfill the request for collection, analysis of information; time spent by the operator on selecting informational objects of influence and adjusting relevant pairs, target-countermeasure [23]. Thus, on the basis of the conducted research, the time characteristics of the operator's work at the stage of setting up the system and at the stage of operation of the system of countering the spread and detection of harmful information in social networks were obtained. The obtained values are shown in Table 1.

Table 1
Time characteristics of the operator's work using the countermeasure system

Step	t_i^{min}	t_i^{max}	$T_i = \frac{3 \cdot T_i^{min}}{5} + \frac{2 \cdot T_i^{max}}{5}$	$\sigma^2(T_i) = 0.4 \times (T_i^{max} - T_i^{min})^2$
T_1^{HC}	46.00	64.10	52.44	102.685
T_2^{HC}	11.20	13.50	15.00	8.396
T_1^{EC}	1.08	1.26	1.24	2.046
T_3^{EC}	1.50	7.01	3.16	15.547
Total, min			71.84	128.674

The study was also conducted to compare the time characteristics of the proposed method with the process of countering the spread and detection of malicious information in social networks without using the proposed approach [24, 25]. The experts were asked to estimate the time to form a corresponding request to the monitoring system, the time to make a decision on the selection of an informational object of influence on the threat, the time to make an adequate decision on the selection of countermeasures. As a result, the following experimental values were obtained for $T^{additional} = 98$ min. Thus, the value of the Laplace function $\Phi(Z)$ for $T^{additional} = 98$ min. for the system of countering the spread and detection of harmful information in social networks, we get (7):

$$Z = \frac{T^{additional} - \sum_{i=1}^n T_i}{\sqrt{\sum_{i=1}^n \sigma_i^2(T_i)}} \approx 2.69 \quad (7)$$

According to the obtained values of the Laplace function given in the relevant tables, the probability of execution of the anti-spreading system in social networks and the detection of harmful information in a given time is $P_{op}(T_m \leq T^{additional}) = 0.9924$, which meets the requirements for the anti-spreading system for operational efficiency ($P_{op}^{additional} = 0.99$). At the same time, the total working time of the anti-spreading system operator has been reduced in the social network from 98 min. to 71.84.

CONCLUSIONS

The armed conflict in Ukraine is taking on a planetary scale and is a powerful stimulus for finding new ways for humanity to transition to peaceful coexistence. The basis of such processes should be a new paradigm of technological development, which will determine new conditions for the transformation of socio-economic systems to achieve sustainable economic development.

As a result of the research carried out in this direction, the authors added the components of information security, with an emphasis on its effectiveness and ensuring the quality of information, its credibility, reliability and compliance with user requests in social networks. The impact of information security on the social aspects of society's life is substantiated and highlighted.

The research results obtained by us make it possible to form a complex algorithmic approach to high-quality information provision of society through the use of social networks, both under the conditions of hybrid war in Ukraine and during peacetime, based on modern scientific and mathematical methods and the conclusions of scientists and expert specialists. which allow the use of both quantitative and qualitative indicators.

The authors have developed a method of countering the spread of harmful information in social networks, which solves the problem of information support of the decision-making process. The countermeasure method allows: to determine the priority of the object of countermeasure influence, considering that the object of influence is affected by the index of influence and the potential of the source; to sort the countermeasure impact objects by priority to support operator decision-making; to form correspondences "target-countermeasure" to support the adoption of the appropriate decision on countering the spread of harmful information in the social network.

REFERENCES

- [1] S. Honchar, "Otsiniuvannia ryzykiv kiberbezpeky informatychnykh system ob'ektiv krytychnoi infrastruktury". *Alfa Reklama*, Kyiv, K, 2019.
- [2] V. Babenko, O. Nazarenko, I. Nazarenko, O. Mandych, and M. Krutko, "Aspects of program control over technological innovations with consideration of risks". *Eastern-European Journal of Enterprise Technologies*, Vol. 3/4 (93), 2018.
- [3] M.P. Voynarenko, V.M. Dzhulii, L.V. Dzhulii, L.V. Yemchuk, "Modeling of intangible assets development and improvement processes in the enterprise management", 2019. DOI: <http://dx.doi.org/10.21533/pen.v7i2.561>.
- [4] L. Buiak, V. Dzhulii, L. Yemchuk, L. Dzhulii, L. Skorobohata, L. Bilorusets, "Information and communication technologies as the main factor in the development of intellectual capital of the enterprise", 2022. DOI: 10.1109/ACIT54803.2022.9913192.
- [5] Yu. V. Kindzerskyi, "Kiberbezpeka ta stanovlennia tsyfrovoy ekonomiky: problemy vzaimozv'iazku", 2020 pp. 18-26. DOI: <https://doi.org/10.33271/ebdut/71.018>.
- [6] V.M. Dzhulii, Yu.V. Khmelnytskyi, N.S. Petliak, O.V. Pakhar, "Model potoku tekstovyykh povidomlen tematychnykh internet-resursiv systemy prohnovuvannia informatsiinoi bezpeky", 2022, pp. 294-300.
- [7] M.V. Hranovskyi, "Derzhavna polityka u sferi zapobihannia ta protydiv kibernetnychnym zahrozam – dosvid Respubliky Polshcha", 2019, pp. 212-220.
- [8] I.H. Hrabar, R.V. Hryshchuk, K.V. Molodetska, "Bezpekova synerhetyka: kibernetnychni ta informatsiyni aspekty". *ZhNAEU*, Zhytomyr, Zh, 2019.
- [9] V.B. Dudykevych, H.V. Myktyyn, A.I. Rebets, "Kvintesentsiia informatsiinoi bezpeky kiberfizychnoi systemy", 2018, pp. 58-68.
- [10] S. Lienkov, V. Podlipaiev, I. Tolok, I. Lisitsky, N. Lytvynenko, S. Kuznichenko. "The Information and Analytical Using of Non-Structured Information Resources", *CEUR*, Workshop, Proceedingsthis link is disabled, 2021, pp. 81-87.
- [11] P.P. Tkachuk, R.V. Hula, O.I. Syvak, O.M. Shchurko, V.V. Shemchuk, "Informatsiina viina i natsionalna bezpeka", *NASV*, Lviv, L, 2015.
- [12] S.O. Dovhyi, O.Ya. Savchenko, P.P. Vorobiienko, "Suchasni telekomunikatsii: merezhi, tekhnolohii, ekonomika, upravlinnia, rehliuvannia", *Ukrainskyi Vydatsnychi Tsent*. Kyiv, K, 2012.
- [13] S. Lenkov, M. Kubyavka, L. Kubiavka, Y. Lenkov, V. Shevchuk, "Reflex Intellectual text processing systems: Natural language text addressing", *CEUR*, Workshop Proceedings, 2019, pp. 85-95.
- [14] O. Tkachenko, K. Tkachenko, "Kiberprostir i kiberbezpeka: problemy, perspektyvy, tekhnolohii", 2018, pp. 75-86. DOI: <https://doi.org/10.31866/2617-96x.1.2018.147257>.
- [15] S.V. Lenkov, D.A. Perehudov, V.A. Khoroshko, "Metody y sredstva zashchyt ynfomatsyy", *Aryi*, Kyev, K, 2008.
- [16] "Cotsialni merezhi – realni zahrozy virtualnoho svitu", 2011. URL: <http://ogo.ua/articles/view/011-02-23/26490.htm>.
- [17] O. Zhylinska, A. Chorny, V. Dzhulii, L. Yemchuk. "Organizational Network Analysis as a Tool for Leadership Assessment in Software Development Team", 2020, DOI: 10.1109/ACIT49673.2020.9208827.
- [18] I. Gontareva, V. Babenko, B. Kuchmacz, S. Arefiev. "Valuation of Information Resources in the Analysis of Cybersecurity Entrepreneurship". *Estudios de Economía Aplicada*, Vol. 38-3(1), 2021, pp. 1-11. <http://dx.doi.org/10.25115/eea.v38i4.3984>.
- [19] Ye. Starychenko, A. Skrypnyk, V. Babenko, N. Klymenko, K. Tuzhyk. "Food Security Indices in Ukraine: Forecast Methods and Trends". *Estudios de Economía Aplicada*, Vol. 38-3(1), 2021, pp. 1-8. <http://dx.doi.org/10.25115/eea.v38i4.4000>.
- [20] O. Shumilo, V. Babenko, L. Liubokhynets, I. Volovelska, O. Arefieva, O. "Method of Enterprise Economic Security Evaluation". *Estudios de Economía Aplicada*, 39 (7), 2021. <https://doi.org/10.25115/eea.v39i7.4998>.
- [21] I. Voronenko, M. Nehrey, A. Laptieva, V. Babenko, K. Rohoza. "National cybersecurity: assessment, risks and trends". *International Journal of Embedded Systems*, Vol. 15, No. 3, 2022, pp. 226-238. DOI: <https://doi.org/10.1504/IJES.2022.124854>.
- [22] A. Kuzior, Y. Samusevych, S. Lyeonov, D. Krawczyk, D. Grytsyshen. "Applying Energy Taxes to Promote a Clean, Sustainable and Secure Energy System: Finding the

- Preferable Approaches". *Energies*, 16 (10), 4203, 2023. <https://doi.org/10.3390/en16104203>.
- [23] A. Kuzior, O. Arefieva, O. Vovk, P. Brożek. "Innovative Development of Circular Systems While Ensuring Economic Security in the Industry". *Journal of Open Innovation: Technology, Market, and Complexity*, 8(3), 2022 139. <https://doi.org/10.3390/joitmc8030139>.
- [24] A. Kuzior, T. Vasylieva, O. Kuzmenko, V. Koibichuk, P. Brożek. "Global Digital Convergence: Impact of Cybersecurity, Business Transparency, Economic Transformation, and AML Efficiency". *Journal of Open Innovation: Technology, Market, and Complexity*, 8(4), 2022, 195. <https://doi.org/10.3390/joitmc8040195>.
- [25] A. Kuzior, H. Yarovenko, P. Brożek, N. Sidelnik, A. Boyko, T. Vasilyeva. "Company cybersecurity system: assessment, risks and expectations" *Production Engineering Archives*, vol. 29, nr 4, 2023, pp.379-392. DOI:10.30657/pea.2023.29.43.

Dariusz Krawczyk (correspondence author)

ORCID ID: 0000-0003-1823-0309

Silesian University of Technology

Roosevelta 26-28, 41-800 Zabrze, Poland

e-mail: dariusz.krawczyk@polsl.pl**Vitalina Babenko**

ORCID ID: 0000-0002-4816-4579

Daugavpils University

Vienības iela 13, Daugavpils, 5401, Latvia

Kharkiv National Automobile and Highway University

Kharkiv, Ukraine

e-mail: vita.babenko@gmail.com**Liudmyla Yemchuk**

ORCID ID: 0000-0003-4931-8004

Department of Accounting, Audit and Taxation

Khmelnitskyi National University

Khmelnitsky, Ukraine

e-mail: fortuna777@ukr.net**Serhii Lienkov**

ORCID ID: 0000-0001-7689-239X

Research Center Military

Institute of Taras Shevchenko

National University of Kyiv

Kyiv, Ukraine

e-mail: lenkov_s@ukr.net**Volodymyr Dzhulii**

ORCID ID: 0000-0003-1878-4301

Department of Cyber Security

Khmelnitskyi National University

Khmelnitsky, Ukraine

e-mail: dzhuliivm@khnmu.edu.ua**Larysa Dzhulii**

ORCID ID: 0000-0001-9475-7175

Department of Accounting, Audit and Taxation

Khmelnitskyi National University

Khmelnitsky, Ukraine

e-mail: olimpd505@ukr.net**Ihor Muliari**

ORCID ID: 0000-0002-6659-605X

Department of Cyber Security

Khmelnitskyi National University

Khmelnitsky, Ukraine

e-mail: muliariiv@khnmu.edu.ua