UDC 004.738.5:004.056.5(045)

*R. V. Hryshchuk, DSc (Zhytomyr Military Institute, Ukraine),*
*K. V. Molodetska, DSc (Zhytomyr National Agroecological University, Ukraine)*

**The theoretical basis of system construction of the state information security in social networking services**

*The authors elaborate theoretical basis of providing information security of the state in social networking services by implementing procedures for detection, assessment and countering threats in the information space. Effectiveness of the proposed theoretical basis is achieved by developing timely measures to identify threats, using the natural peculiarities of the interaction of actors for the synthesis the controlling influence and artificially managed transition to a definite stable state of information security of the state.*

In view of the constantly growing popularity among the citizens of the developed world countries, and of Ukraine in particular, the social networking services (SNS) became an integral part of the national information space and are being applied, inter alia, as platforms for sharing active civic positions and organising respective activities [1]. Hence, the SNS is not only an effective tool for social communication; it is also used by society to influence state-building and political processes. Thanks to the communication benefits of the SNS, they have become an effective tool for achieving the geopolitical goals of world's leading powers. When used for conducting information operations, manipulating the public opinion, spreading propaganda, etc., SNS turn into a source of threats to national information security (NIS) [1, 2]. The consequences of such actions can encompass the virtual communities of actors and can be used to spread or boost social tension, interethnic or inter-religious hatred, dissatisfaction with the system of state governance, the spread of protest sentiments, etc. Even when there is no state control over such phenomena, one still needs to consider their effects on the social and political life. During the so-called 'Arab Spring,' for the first time SNS have been used to organise long-lasting civil protests, change or overthrow governments in North Africa and the Middle East. SNS were also actively used by revolutionary movements in the former Soviet countries to organize what later became known as 'color revolutions' to overthrow governments and change the respective political regimes [2].

The events of the armed aggression of the Russian Federation in the east of Ukraine and the annexation of the Crimea outlined the next stage in the use of SNSs for a new form of confrontation – the hybrid war. It was established that the SNS played a leading role in informational support and organization of the annexation of the Crimea, incitement of social hatred and escalation of violence in the East of Ukraine. Therefore, the provision of information security of the state (ISS) in the SNS in the conditions of the globalization of the information space and the hybridization of military conflicts remains one of the urgent problems in need for solutions not only in Ukraine but also in the world [3].

Critical analysis of published research works [4-6] showed that the provision of ISS in the information space of virtual communities relies on the

system of providing the ISS in the SNS. It is a component of the system of ensuring national security of the state on the one hand and consists of departmental subsystems for solving individual tasks on the other. Given the insufficient availability of scientific tools, ISS support system in SNS counter threats in the information space service comes with a significant delay. Therefore, there is an objective contradiction between the problems of practices associated with the need to improve the ISS using SNS nationals in conditions of war and hybrid issues of science, which leads to a lack of methodological principles ensuring ISS in the SNS with the requirements of the regulations.

We formulate the basic assumption about the source of threats to the ISS in the SNS. Let the informational influence on virtual community actors in the SNS be carried out using text content. Then the provision of the ISS in the SNS is carried out in the following three phases:

- monitoring information space in virtual communities;
- detecting and evaluating ISS threats;
- deciding on measures to counter identified threats to the ISS in the SNS.

Building on the results of previous studies, the methodological foundations and principles and the provision of ISS in the ISS are examined in three consequent sub-sections, taking into account also the requirements of normative documents.

***I Implementation monitoring in information space of the SNS***

In the first stage, the ISS expert analyses significant for society subject to the national information space for further search of publications in the SNS. To do this, research on text content is conducted, which is the largest share of the information space of the virtual communities of the SNS. In this case, the expert performs the formalization of the set of possible threats to the ISS in the SNS as a tuple in accordance with the model [3]

$$D = \langle R, S, C, T, Sph, M, F, Sr, Pos, I \rangle,$$

where $R$ – relation between threat and actors of the SNS; $S$ – type of subject of threats; $C$ – nature of the threat to the SNS; $T$ – purpose of realizing the threat; $Sph$ – sphere of public activity, which is affected by the threat; $M$ – way of the threat; $F$ – frequency of repetition; $Sr$ – hidden manifestation; $Pos$ – possibility of implementing a threat to the SNS; $I$ – level of influence on actors in the SNS.

Monitoring of text content in the SNS is carried out according to the semantic core $W = \langle w_i \rangle$, $i = \overline{1,n}$. For the information retrieval, the method of latent-semantic indexing (*LSI*) [7] is used to index content based on its text and hidden semantic dependencies, the essence of which is provided by one of theauthors in an earlier publication.

***II Detection and evaluation of threats of the ISS in the SNS***

*2.1. Detection of signs of information operations in the SNS* is based on the technology proposed by one of the authors, used to find duplicate content $TC^*$. In this case, the search for duplicate publications of actors and comments on them is based on the method of shingle [8]. After that, the readability $I_{ARI}$ of text messages is calculated, which characterizes the complexity of understanding the text content. The

expression for determining the readability index differs for different languages. Conducting a "request-response" dialogue with an actor who distributes such content allows you to determine whether the actor is a social bot or not. Then a decision is made on the presence of signs of information operations based on the rules developed. As a result, a generalized indicator of the threat of conducting an information operation in the information space of the SNS is defined as $I_1 \in \{0;1\}$ [8].

2.2. *Detection of information influence on actors in the SNS* is carried out in accordance with the method presented in a recent publication by Molodetska-Hrynchuk [8]. The basic idea is to semantically analyze the text content of SNS using the ontologies. The first step is to construct a semantic description of such content. After that, we search for signs of threats to the ISS in the SNS by using the signature method. The next step is to find the threats of the ISS in the SNS on the basis of the anomaly method by establishing inconsistencies of the facts in the text content of the SNS. Also found in the text content are contradictions between the relations, the essence of which is the use of the relationship between concepts, which is not defined ontology. The resulting assessment of the threat of the ISS in the SNS in the context of the implementation of information influence on the actors acquires the respective values $I_2 \in \{0;1\}$.

*2.3. The establishment of information and psychological influence on actors in the* SNS is based on methods of content analysis, thematic modeling and methods of machine learning. Several studies have shown that methods of manipulating the public opinion of actors in the SNS, which took place in the information space of virtual communities, are characterized by common features. Molodetska-Hrynchuk [9] proposed to include among such signs the doubtfulness of the facts $Q_1$; emotional content $Q_2$; tone $Q_3$; sensationalism $Q_4$; presence of a hidden topic $Q_5$. At the same time, $Q_1$, $Q_2$ and $Q_4$ are determined using the signs of the lower level of the hierarchy. Then we calculate information entropy, which characterizes the level of uncertainty about the presence of hidden informational and psychological impact on actor. For the convenience of interpreting the calculated values, we introduce the normalized value of entropy $H_n$. Thus, evaluation of information-psychological influence on actors in the SNS is calculated as $I_3 = 1 - H_n$ and it acquires values in the range $I_3 \in [0;1]$.

*2.4. The detection of actors involved in information operations in the* SNS is based on the methodology for assessing the profiles of information security actors. Towards this purpose, data from personal pages of actors in the SNS is used, and the aggregation of such data provides for the construction of the actor's information security profile as a threat to the ISS [10]. Given the differences in the amount of actor data in the accounts of different SNS, to build an information security profile, the following main characteristics are studied: attributes of the actor profile in the ISS $S_1$; performance indicators for content publishing $S_2$; characteristic features of the text content of the actor profile $S_3$; connections with other actors and virtual communities in the SNS $S_4$. To do this, we use the methods of machine learning

with the teacher, which allows us to perform the classification of the actors in the predefined classes. The methods that are based on the boosting procedures of binary classifiers are effective for solving the problem of classifying actors by the level of threats. The general evaluation of the profiles of information security actors in the SNS $I_4$ acquires values on the interval $[0;1]$.

*2.5. The assessment of the level of threats to the ISS in the SNS* is to calculate the generalized indicator of their manifestations in the information space of virtual communities. A multicriterial assessment of the threats of the ISS $I_j$, $j=\overline{1,4}$ with various weighting factors based on the nonlinear compromise scheme of Prof. Voronin [3]. The resulting evaluation of the symptoms of the threats of the ISS in the SNS is defined as $I \in [0;1]$.

***III Decision-making on measures to counter identified threats to the ISS in the SNS***

Depending on the magnitude of the threat assessment of the ISS in the SNS obtained in the previous stage, decisions are made to counteract the threat and protect the information space (Table 1).

*Table 1*

Rules of decision making

| Interval Values Scale | Threat level | Recommendations |
|---|---|---|
| 0.00 – 0.30 | absent | Absent |
| 0.31 – 0.50 | below average | Monitoring the threat in the SNS information environment |
| 0.51 – 0.70 | higher than average | Monitoring of the threat in the information environment of the SNS;<br>Predict the distribution of text content and requests for it |
| 0.71 – 1.00 | threat exists | Monitoring of the threat in the information environment of the SNS<br>Synergistic management of the interaction of actors in the SNS |

In the case the threat of ISS in the SNS is identified as ‘absent,’ no information counteraction is made. If there is a threat at ‘below average’ level, then the procedure for monitoring the information space of the SNS in accordance with the first stage continues. In the case of a threat to the ISS in the SNS at ‘higher than average’ level, in addition to monitoring the information space, the prediction of the distribution of text content and requests by actors on it will be provided, which will save the resources of the system for providing ISS in the SNS. The essence of the forecasting method is in the following [11]. If the level of threat of the ISS in the SNS is defined as ‘threat exists,’ in addition to monitoring the information space for implementing the virtualized community’s controlled transition to the given state of the ISS, the concept of synergistic management of interaction between actors is used [3].

## Conclusion

The methodological principles of providing the ISS in the SNS under hybrid warfare have been developed taking into account the requirements of normative documents based on new methods and technologies for detecting, evaluating and counteracting threats to the ISS in the information space. The application of the developed theoretical foundations allows us to form an integral system of information space protection in the conditions of globalization and free circulation of information, which ensures the effective transition of the virtual community to a given stable state of the ISS. The obtained results promote the further development of modern information technologies both in Ukraine and abroad, which, along with the main tasks assigned to them, implement security functions.

## References


1. O. S. Onyshhenko, V. M. Gorovyj, and V. I. Popyk, *Socialni merezhi jak instrument vzajemovplyvu vlady ta gromadjanskogo suspilstva* (Kyiv: Natsionalna biblioteka Ukrainy im. V. I. Vernadskoho, 2014).

2. R. V. Hryshchuk and J. H. Danyk, *Osnovy kibernetychnoi bezpeky. Monografija* (Zhytomyr: ZhNAEU, 2016).

3. K. V. Molodetska-Hrynchuk, *Methodology of support system construction of the state information security in social networking services*, State Univ. of Telecom., Kyiv, 2018.

4. M. Holloway, "How Russia Weaponized Social Media in Crimea," *Realcleardefense.com*, May 10, 2017, https://www.realcleardefense.com/articles/2017/05/10/how_russia_weaponized_social_media_in_crimea_111352.html.

5. B. Perry, "Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations," *Small Wars Journal* 11, no. 1 (2017), http://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera.

6. M. Zhdanova and D. Orlova, *Computational Propaganda in Ukraine: Caught between external threats and internal challenges*, Working Paper 2017.9 (Oxford, UK: Project on Computational Propaganda, 2017).

7. K. Molodetska-Hrynchuk, "Metod vyjavlennja oznak informacijnyh vplyviv u socialnyh internet-servisah za zmistovnymy oznakamy," *Radioelektronika, informatyka, upravlinnja* 2, no. 41 (2017): 117–126.

8. K. Molodetska, "Tehnologija vyjavlennja organizacijnyh oznak informacijnyh operacij u socialnyh internet-servisah," *Problemy informacijnyh tehnologij* 20 (2016): 84–93.

9. K. Molodetska-Hrynchuk, "Metodyka vyjavlennja manipuljacij suspilnoju dumkoju u socialnyh internet-servisah," *Informacijna bezpeka* 3, no. 23 (2016): 80–92.

10. K. Molodetska-Hrynchuk, "Metod pobudovy profiliv informacijnoi bezpeky aktoriv socialnyh internet-servisiv," *Informacijna bezpeka* 1, no. 25 (2017):104–110.

11. R. Hryshchuk and K. Molodetska, "Metod prognozuvannja dynamiky poshyrennja kontentu j zapytiv na nogo za danymy kontent-analizu povidomlen u socialnyh internet-servisah," *Systemy upravlinnja, navigacii ta zv'jazku* 4, no. 36 (2015): 60–65.