Information & Security: An International Journal

Hryshchuk & Molodetska-Hrynhchuk
vol.41, 2018, 61-79

https://doi.org/10.11610/isij.4105

METHODOLOGICAL FOUNDATION OF STATE'S INFORMATION SECURITY IN SOCIAL NETWORKING SERVICES IN CONDITIONS OF HYBRID WAR

Ruslan HRYSHCHUK and Kateryna MOLODETSKA-HRYNHCHUK

Abstract: At the present stage of the development of information technologies, social networking services have become a leading means of mass communication with a significant impact on all spheres of public activity. Thanks to its popularity and communication benefits, social networking services are used by leading nations to achieve their own geopolitical goals. Through information operations in social networking services, one can spread manifestations of hostility on national, religious, or ethnic grounds, and thus increase the level of social tension, dissatisfaction with the existing system of governance, etc. That may have further consequences in real social and political life, with the subsequent transition to chaotic social dynamic. Therefore, the provision of state information security in social networking services in the conditions of globalization of the information space and hybridization of military conflicts remains one of the most pressing problems not only for Ukraine, but globally.

This article analyses the peculiarities of the use of social networking services during the hybrid war with the Russian Federation. It was established that the counterpart party carried out information operations using social bots, informational and information-psychological influence on the actors of virtual communities. In addition to these actions, operations involved actors with the task to enhance the impact of negatory material and destructive propaganda. The authors then elaborate methodological principles 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 methodological principles is achieved by developing timely measures to identify and assess threats, using the natural peculiarities of the interaction of actors in social networking services for the synthesis of controlling influence and artificially managed transition to a definite stable state of information security of the state.

Keywords: social networking service, hybrid war, information operations, information security of the state, cyber threats.

Introduction

At present, as a result of deepening the processes of informatization of all spheres of social activity, the system of strategic communication develops in an evolutionary manner. Users of advanced information technologies pose a variety of new requirements to mass media – ensuring timeliness, interactivity, coordination of the interaction, availability of tools for creating and sharing multimedia content, etc.[1,2] These requirements are most fully satisfied with social networking services (SNS); where users have the opportunity to turn into actors. In today's market of information technology, the SNS is distinguished by the peculiarities of its functioning and purpose, and one can distinguish social networks, blogs, media repositories, geoservices, etc.[3,4] In view of the constantly growing popularity among the citizens of the developed world countries, and of Ukraine in particular, the 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. 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., SNSs turn into a source of threats to national information security (NIS).[5] 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 SNSs have been used to organise long-lasting civil protests, change or overthrow governments in North Africa and the Middle East. SNSs 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.[6]

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.[7] 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 fo solutions not only in Ukraine but also in the world.

The analysis of known approaches to the solution of the problem of providing the ISS in the SNS [8 – 14] demonstrated that in the leading countries of the world there is a gradual improvement of the approaches to the creation of systems for the provision of the ISS. The primary task is to regulate the general principles of providing the ISS with a view to their further use in the guidance documents and the development of international agreements in the field of information security. Despite the difference in existing approaches to the formation of state policy in the information sphere and the directions of its implementation, the common awareness remains the need to protect the global information space on the background of continuous growth ISS threats, their hybridization and complex character.

With the hybrid war with the Russian Federation in the background, in 2017 the Doctrine of Ukraine’s Information Security was approved with the aim to counter targeted threats to national security in the information sphere. The Doctrine clarifies the principles of the formation and implementation of state information policy, primarily on counteracting the devastating informational influence of the Russian Federation in the conditions of its hybrid war.[12] Also, the Doctrine formulated the need to identify innovative approaches to the formation of a system of protection and development of information space in a globalized and free circulation of information. Therefore, the implementation of the Doctrine requires the development of methodological principles for ensuring the security of the national information space, in particular in the SNSs.

Critical analysis of published research works [6,10,13,14] 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. Consequently, the development of methodological foundations for the detection, evaluation and counteraction of threats to the ISS in the SNS is an actual scientific and applied problem in the path of creating a system of protection and ensuring the sustainable development of the state's information space.

Features of Information Operations against ISS in the SNS

Given the peculiarities of the use of information technologies to influence the individual and mass consciousness of actors in the SNS in conditions of conducting hybrid warfare it was established that such threats of ISS are complexly formalized entities and are manifested in various forms.[15 – 17] One of the most common forms of achieving unilateral advantages in the information space of the SNS is the conduct of information operations.[6,7,15,16] The peculiarities of their implementation in the virtual community of the SNS at the initial stages of the hybrid war in Ukraine in the form of patterns are given in Fig. 1.

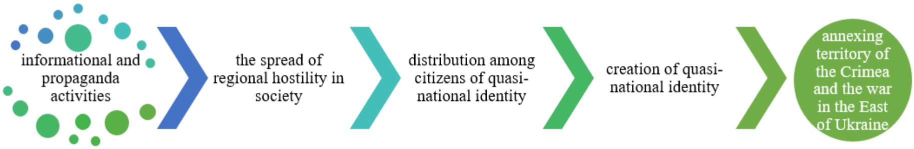
informational and propaganda activities
the spread of regional hostility in society
distribution among citizens of quasi-national identity
creation of quasi-national identity
annexing territory of the Crimea and the war in the East of Ukraine

Figure 1: Patterns of information operations in the SNS.

Thus, the SNS were an effective tool for destructive influence on the individual and mass consciousness of the citizens and the processes of making managerial in the state. Activities in SNSs augmented the military actions and, although they were of background character and artificially created, their wide spread was used to form the protest potential of the local population.

Summarizing the experience of information operations in SNS, Zhdanova and Orlova found that a key feature is the systematic use of information resources or special software such as social bots to achieve this goal.[16] The use of the mechanism of targeting for information impact on the target audience actors in virtual communities provides for selectivity and effectiveness. By means of social bots, warring parties resolve such issues as blocking profiles of known bloggers and opinion leaders in SNS, content distribution and its destructive content socialization, creating a given background information, etc. Social bots are used in SNS to shape public opinion on topical issues, organization of active discussion in virtual communities on minor events, creating a negative image of certain global developments, and so on.

Earlier research demonstrated that the content distributed by the subjects of the ISS in the SNS aims at destructive information influence on the actors.[6,18] The essence of such influence is the purposeful intervention in the functioning of the virtual community actor and by publishing content with signs of destructiveness. Such content of the directed content includes deviation from the generally accepted concept of using lexemes in a particular subject area of publication. The considered information influences on actors in the SNS [19] have a hidden character and manifest as a threat to the functioning of an object or in the form of a deviation from the safe profile of the behavior of this object.

During the interaction of actors in the SNS, there are a number of psychological phenomena, the use of which by the opposing side for information operations creates prerequisites for manipulating public opinion, the influence on the freedom of choice of actors, their emotional and mental state. Information-psychological impact is purposefully carried out on the virtual community of actors in order to motivate them for a given behavior in real life and bring changes in their moral and psychological state.[20,21] Various technologies, such as the spiral of silence, herd instinct, opinion leaders, anonymous authority, distraction, and others, are used to implement information and psychological influence in the SNS. Considered threats in the content of the SNS are manifested by emotional exaggeration, the presence of rhetorical questions, evaluative judgments, hidden content, etc. The determining requirement for the success of the implementation of information and psychological influence is its latent nature, when the object of influence is not suspected of manipulating and believes that events develop naturally and inevitably.

Considering the peculiarities of the processes of social communication of actors in the SNS, they are the leading source of content for virtual communities and at the same time are its users. Therefore, the opposing party uses the actor's profiles in the SNSs, who carry out provocative publications and comments to them, in order to disseminate materials of a destructive propaganda nature. Thus, in 2013 a set of specialized offices for organizing SNS activities was disclosed. Located in the Olgino neighbourhood of St. Petersburg, Russia, it was conducting an information war against Ukraine. Later, that group of actors was named "Olginsky trolls."[16]

Research results published by Pennacchiotti and Popescu have shown that the use of aggregated actor profiles in the SNS is a source of additional information about him, or her, as a possible participant in information operations.[22] Establishing the specifics of their activity in the SNS and the connections with other actors allows to identify the subjects of influence on the ISS in the SIS in a timely manner.

It is known that the actors and their virtual communities in SNS form a complex nonlinear dynamic system that is characterized as highly sensitive to any changes in the parameters of the information space,[23 – 26] in particular as a result of information operations against the ISS. In this case, the processes of communication among actors in the SNS can move into chaotic dynamics, the results of which may be the chaotization of society in real life, with subsequent control of the subjects of information operations.[25] Irreversible changes in the processes of interaction between actors in the SNS lead to disasters, the consequences of which for the ISS, its sovereignty and integrity are unpredictable.

Figure 2 visualises a generalization of the peculiarities of conducting information operations in the SNS in conditions of Russian hybrid warfare.

Individual information operations may vary not only in terms of content, but also in the underlying technologies used, which further complicates the procedures for their detection in the information space of the SNS.

Methodological Foundation of Detection, Evaluation and Countering the threats to the ISS in the SNS

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,[17,19,27-35] the methodological foundations and principles and the provision of ISS in the ISS are examined in thr three consequent sub-sections, taking into account also the requirements of normative documents.[12]

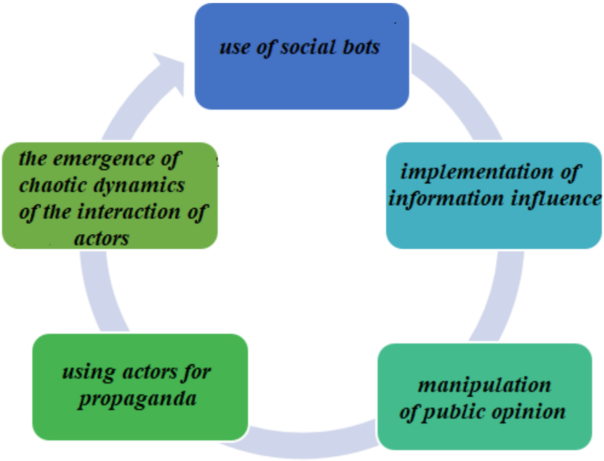
use of social bots
implementation of information influence
manipulation of public opinion
using actors for propaganda
the emergence of chaotic dynamics of the interaction of actors

Fig. 2: Ways to achieve one-sided advantages in the information space of the SNS.

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 [17]

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

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*) 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.[19] First, the preliminary processing of text content is performed: removal of stop words, stimming and lemmatization. Next, the words that are used only once are excluded and the construction of the frequency matrix M is realized. After that, a singular frequency matrix M is calculated to find the relevant semantic core of the text content in the SNS TC^* and the actors who distributed A^*

$$M = U \times S \times V^T ,$$

where U and V^T – orthogonal dimension matrices $i \times k$ and $k \times j$ in accordance; S – a diagonal dimension matrix $k \times k$, and k – the number of singular values of the matrix (the hidden content subjects), and its elements are sorted in descending order.

Collections of text content are determined by the largest singular numbers and their value corresponds to the degree of manifestation keywords publication in posts in the SIS. The collected data is stored in the data warehouse and is available for further research at the second stage (described below), in conjunction with the data on the actors that distributed it.

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

At this stage, an analysis of the pre-selected text content and the actors' data is performed. To do this, text content is analysed to establish the presence of the signs of information operations, the effect of information on the actors of virtual communities, cases of manipulation of public opinion, and to explore selected—based on the available data—actors' profiles.

2.1. *Detection of signs of information operations in the SNS* is based on the technology proposed by one of the authors,[27] 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. 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 $I_1 \in \{0;1\}$.

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.[19] 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 [18]

$$\exists r_t\left(p_t\right): p_t \in P_n \wedge r_t \in R_z\left(p_n\right),$$

where $r_t\left(p_t\right)$ – some relation between the concepts of the analyzed text content in SNS; $p_t \in P_n$ – explored concepts used by the virtual community; $r_t \in R_z\left(p_n\right)$ – set of relationships that indicate a danger to a certain concept p_n.

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, when a certain concept can not be used in relation to [18]

$$\exists r_t\left(p_t\right): p_t \in P_n \wedge r_t \in R_n \wedge p_t \notin P_{in}\left(r_n\right).$$

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: [18]

$$\forall p_n \in P_n \neg \exists r_n \in R_n : r_t = r_n .$$

If the text content being studied is highly relevant to the search query from the first stage, it is further studied by an ISS expert to identify new security threats and the formation of semantic patterns of the ontological knowledge base.

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.[21] Establishing such features in text content of the SNS provides procedures for identifying information and psychological effects on actors. Molodetska-Hrynchuk 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 .[28] 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 actors

$$H = -\sum_{\nu=1}^{k}\sum_{l=1}^{g} Q_l^\nu \log_2 Q_l^\nu ,$$

where H – the value of information entropy (uncertainty); Q_l^ν – the numerical value of the sign of manipulation of public opinion; $l = \overline{1, g}$ – indices of partial signs of second level manipulations; $\nu = \overline{1, k}$ – indices of partial signs of first-level manipulations.

For the convenience of interpreting the calculated values, we introduce the normalized value of entropy

$$H_n = \frac{H_{\max} - H}{H_{\max}} ,$$

where $H_{\max}$ – the maximum value of entropy.

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.[22,29] 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. 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 essence of boosting is to build a composition of algorithms of machine learning, when each subsequent algorithm compensates for the disadvantages of the composition of all previous algorithms. The final classifier is calculated as

$$k(x) = \arg\min_{k\in[1,K]} \sum_{\bar{k}=1}^{K} c\left(k,\bar{k}\right) p_{\bar{k}M}\left(x\right),$$

where $p_{\bar{k}M}(x)$ – probability of membership of an actor of a class of threats k after carrying out the M boost cycle; $c(k,\bar{k})$ – the cost of an actor’s mistaken assignment to a class of threats k, when he belongs to a class $\bar{k}$.

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 Professor Voronin.[30, 31]

$$I^* = \arg\min_{I\in M} \sum_{j=1}^{4} \alpha_j \left(1-I_j\right)^{-1}.$$

To move to a qualitative assessment scale, the resulting indicator is normalized to a minimum

$$I = 1 - \frac{1}{I^*}.$$

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).[32]

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 [33] is in the following. In the first step, a content function is created $X^Q(t)$, that describes the change in the dynamics of the distribution of content and requests for it according to the content-analysis of messages in the SNS. The next step is to calculate the metric of self-similarity of the content function through the Hurst index

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; 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 Synergistic management of the interaction of actors in the SNS

$$H^Q = \frac{\lg(R/S)}{\lg(l/2)} ,$$

where H^Q – the Hurst index for the content function $X^Q(t)$; S – the mean square deviation of the content function $X^Q(t)$; R – spread of accumulated deviation of content function $X^Q(t)$; l – number of observations.

The third step is to establish the nature of the content function, depending on the value of the indicator H^Q: random, anti-persistent (ergodic), persistent. Prediction of the change of the content-function $X^Q(t)$ is carried out for the persistent number $H^Q > 0,5$, in particular using the least squares method

$$F = \sum_{t=1}^{l} (P^Q(t) - X^Q(t))^2 \to \min ,$$

where $P^Q(t)$ – the approximating polynomial.

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.[34, 35] According to the concept, in the first step formalization of the interaction of actors in the SNS as a system of nonlinear differential equations is performed. On thenext step, the order parameter that will determine the dynamics of virtual community actors interaction is calculated as

$$\psi_\upsilon = \psi_k(x_1, y_1, ..., x_\lambda, y_\mu) + \psi_d(x_1, y_1, ..., x_\lambda, y_\mu) ,$$

where $\psi_k(x_1, y_1, ..., x_\lambda, y_\mu)$ is the conservative component or managed aspect of the interaction of actors in the SNS, $k = 1, 2, \ldots$; $\psi_d(x_1, y_1, ..., x_\lambda, y_\mu)$ is the dissipative component that defines the type of attractor, which reflects the ordering of the virtual community at the macro level of the SNS $d = 1, 2, \ldots$.

The appearance of the order parameter is determined in accordance with the task set for changing the character of the interaction of actors in the SNS and achieving a given state of the ISS.[36,37] Due to the introduction into the system of nonlinear differential equations of the component $\psi_\upsilon(t)$, it is possible to start the process of self-organizing actors in a virtual environment. The synergetic control $u_\gamma(t)$ is synthesized from the modified system of nonlinear differential equations with allowance for controlled self-organization to achieve predefined points of a surge of synergistic effect, as described in a previous ublication of the authors.[34] Implementation of the counteraction to the threats to the ISS in the SNS is carried out with the involvement of certain executive bodies depending on the sphere of public activity, which is aimed at the identified threat D .[12, 32]

Experimental Study

Experiment 1. This experiement looks into the change in the number of publications of actors in the SNS using the developed method of forecasting the distribution of content aimed at discrediting the highest political leadership of Ukraine. In September 2015, Russian mass media disseminated information on the participation of Prime Minister of Ukraine A. Yatsenyuk in hostilities in Chechnya in late 1994 and early 1995. The Prime Minister was accused of supporting the Chechnya’s independence fighters from Russia Federation during an armed uprising in this republic.[38] The text content of SNS, which contained damaging information on “Yatseniuk fought in Chechnya” was analyzed. Based on the results of the generated queries to the content service *IQBuzz* in the period from December 26, 2015 to January 4, 2016 the value of the Hurst index was calculated. It is established that the dissemination of this content in the SNS has a persistent (non-random) nature, and a number has signs of a trend. By means of the MS Excel table processor for the least squares method, an approximating curve for the studied content function is constructed (Figure 3).

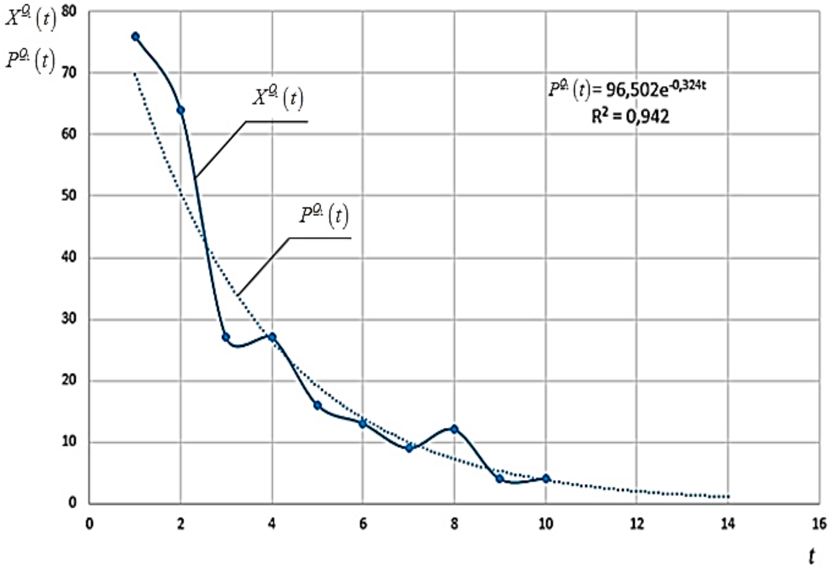

Figure 3: Dynamics of content distribution “Yatseniuk fought in Chechnya” in the SNS: extrapolation results.

The number of publications for the next four days also extrapolated. The results of the prediction of the approximating curve $P^{Q_1}(t)$ are consistent with the experimental data. Given the declining demand for such content, it is inappropriate to attract the resources of the ISS support system in the SNS for the organization of information countermeasures.

Experiment 2. The dynamics of SNS requests for the content of the “Yarosh’s business card” from October 2014 to September 2015, according to *Google AdWords* data, is related to the involvement of the public-political figure D. Yarosh in a shootout in Slavyansk through a business card, found, as it was supposed, in a burnt car [39] (see Figure 4). It is established that the Hurst index becomes meaningful $H^{Q_2} = 0{,}891$, which indicates the persistence of the series and the presence of a constant component. An approximating curve $P^{Q_2}(t) = 1605{,}3e^{-0{,}139t}$ is constructed. In view of the slow decline in the level of interest of SNS actors to such content under the exponential law, in order to reduce the length of transient processes, it is expedient to apply the developed concept of synergetic control.

We formalize the interaction of actors in the SNS as a system of nonlinear differential equations [34]

$$\begin{cases} \dfrac{dx(t)}{dt} = ax - xy - bx^2; \\ \dfrac{dy(t)}{dt} = -cy + xy, \end{cases}$$

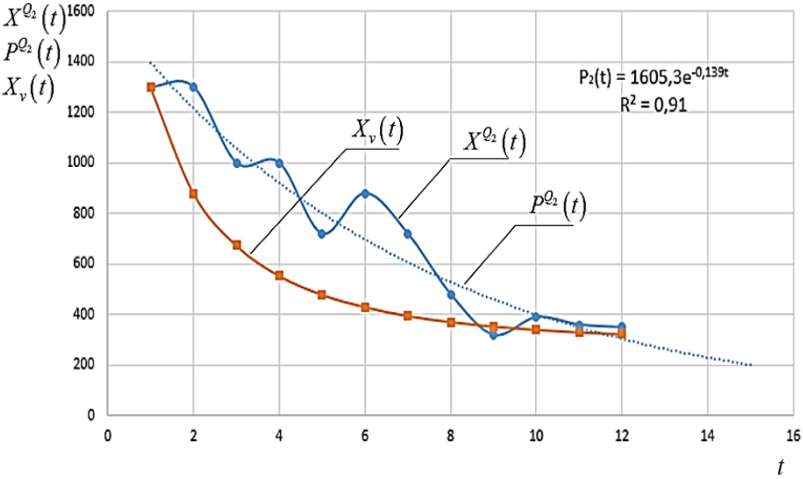

Figure 4: Dynamics of the distribution of requests for content “Yarosh’s business card” in the SNS: extrapolation results and synergistic control actions.

where $x(t)$ describes the demand of actors in the SNS for content of interest to actors of virtual communities; $y(t)$ describes the offer to provide such content; a – indicator, the value of which describes the change in the speed of demand for actors in the SNS on the content being studied; b is an indicator, the meaning of which describes the change in the process of competition actors in the SNS to publish content similar in nature and content; c is an indicator, the value of which describes the change in the rate of the proposal to provide actors' interaction in the SNS of such content.

It is established that the working parameters of the system of nonlinear differential equations take the following values: change in the speed of demand for content $a=0,7$; change of the competition process $b=0,45$ and the rate of the offer for the provision of content $c=0,3.$ To regulate the demand for actors for the content of the SNS, the order of the form is chosen [37]

$$\psi\left(x,y\right)=\varphi_1 x+\varphi_2\left(1-\frac{y}{N}\right),$$

where φ_1, φ_2 are coefficients of demand regularization and supply of content that is of interest to interaction actors in the SNS; N is the level of the content proposal, which is of interest based on its value.

The essence of this order parameter is to manage the interaction of actors in the SNS, taking into account the time value change of the content of interest. Parameters of synergetic control $u(x,y)$ are the level of supply of content $N=0,35;$ content indicators of regularization $\varphi_1=0,6$ and $\varphi_2=0,3$; the duration of transitions in the system $T_2=1$ month. As a result of the information counteraction organization, the synergistically driven actors demand $X_v\left(t\right)$ for content containing destructive information will change as shown in Figure 4. That is, the demand for content actors in the SNS with destructive signs will be reduced by 3 times, and the duration of transitions in the virtual communities as a result of response to such content will be reduced by 30 %. As a result of the self-organization of actors in the SNS, inhibition of chaotic dynamics of interaction in virtual communities is provided with the subsequent transition to a given state of the ISS.

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 methodological grounds 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.

Notes

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

[2] Jonathan A. Obar and Steven Wildman, "Social media definition and the governance challenge: An introduction to the special issue," *Telecommunications policy* 39 (2015): 745–750.

[3] Danah M. Boyd and Nicole B. Ellison, "Social Network Sites: Definition, History, and Scholarship," *Journal of computer-mediated communication* 13, no. 1 (2007): 210–230.

[4] Juriy Danyk, Ruslan V. Hryshchuk, and Oleksiy Samchyshyn, "Mobilni socialni Internet-servisy jak odyn iz riznovydiv masovoi komunikacii na suchasnomu etapi," *Bezpeka informacii* 21, no. 1 (2015): 16–20.

[5] Kateryna Molodetska, "Socialni internet-servisy jak subjekt informacijnoi bezpeky derzhavy," *Information Technology and Security* 1, no. 6 (2016): 13–20.

[6] Ruslan V. Hryshchuk and Juriy H. Danyk, *Osnovy kibernetychnoi bezpeky. Monografija* (Zhytomyr: ZhNAEU, 2016).

[7] Michael Holloway, "How Russia Weaponized Social Media in Crimea," *Realclear-defense.com*, May 10, 2017, https://www.realcleardefense.com/articles/2017/05/10/how_russia_weaponized_social_media_in_crimea_111352.html (accessed November 10, 2017).

[8] Ruslan V. Hryshchuk, *Teoretychni osnovy modeljuvannja procesiv napadu na informaciju metodamy teorij dyferencialnyh igor ta dyferencialnyh peretvoren* (Zhytomyr: Ruta, 2010).

[9] Volodymyr L. Burjachok, Ruslan V. Hryshchuk, and Volodymyr O. Horoshko, *Polityka informacijnoi bezpeky* (Kuiv: PVP "Zadruga," 2015).

[10] Volodymyr M. Petryk, Mykola M. Prysjazhnjuk, and Dmytro S. Melnyk, *Zabezpechennja informacijnoi bezpeky derzhavy* (Kiyv: DPU "Knyzhkova palata Ukrainy," 2015).

[11] Olga Zernecka, "UA Foreign Affairs: Evoljucija strategij kiberbezpeky SShA", *Uaforeignaffairs.com*, Jun 30, 2015, http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/evoljucija-strategii-kiberbezpeki-ssha-1/ (accessed: 22 May 2018).

[12] Oficijne predstavnyctvo Prezydenta Ukrainy, "Ukaz Prezydenta Ukrainy № 47/2017. Doktryna informacijnoi bezpeky Ukrainy," (February 25, 2017), http://www.president.gov.ua/documents/472017-21374 (accessed: 22 May 2018).

[13] Juriy Radkovec, Oleksandr Levchenko, and Oleksiy Kosogov, "Pogljady na stvorennja systemy informacijnoi bezpeky Ukrainy ta ii Zbrojnyh Syl," *Nauka i oborona* 1 (2014): 38–42.

[14] Jaroslav Malyk, "Informacijna bezpeka Ukrainy: stan ta perspektyvy rozvytku," *Efektyvnist derzhavnogo upravlinnja* 44 (2015): 13–20.

[15] Bret 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 (accessed: Nov. 10, 2017).

[16] Mariia Zhdanova and Dariya Orlova, *Computational Propaganda in Ukraine: Caught between external threats and internal challenges*, Working Paper 2017.9 (Oxford, UK: Project on Computational Propaganda, 2017).

[17] Kateryna Molodetska, "Uzagalnena klasyfikacija zagroz informacijnij bezpeci derzhavy v socialnyh internet-servisah," *Zashhyta ynformacyy: sb. nauch. trud. NAU* 23 (2016): 75–87.

[18] Sergiy V. Chernyshuk, "Metodyka vyjavlennja kibernetychnyh zagroz u pryrodnomovnyh tekstah," *Problemy stvorennja, vyprobuvannja, zastosuvannja ta ekspluatacii skladnyh informacijnyh system* 8 (2013): 112–121.

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

[20] Yannis Theocharis, Will Lowe, Jan W. van Deth, and Gema García-Albacete, "Using Twitter to Mobilize Protest Action: Online Mobilization Patterns and Action Repertoires in the Occupy Wall Street, Indignados, and Aganaktismenoi Movements," *Information, Communication & Society* 18, no. 2 (2015): 202–220.

[21] Jaroslav M. Zharkov, Volodymyr M. Petryk, Mykola M. Prysjazhnjuk, Jevhen D. Skulysh, and Larysa F. Kompanceva, *Informacijno-psyhologichne protyborstvo (evoljucija ta suchasnist)* (Kiev: Vipol, 2013).

[22] Marco Pennacchiotti and Ana-Maria Popescu, "Democrats, Republicans and Starbucks Afficionados: User Classification in Twitter," in Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining, 2011, p. 430–438.

[23] Hryhoriy A. Ostapenko, Lyudmyla V. Parynova, Volodymyr Y. Belonozhkyn, Yuriy L. Bataronov, and Kyryl V. Symonov, *Informacyonnye ryski v socyalnyh setjah* (Voronezh, Chair of NIB, 2013).

[24] Dmitriy A. Gubanov, Dmitriy A. Novykov, Aleksandr G. Chhartyshvyly, *Socyalnye sety: modely ynformacyonnogo vlyjanyja, upravlenyja y protyvoborstva* (Moscow: Izdatel'stvo fyzyko-matematycheskoj lyteraturyi, 2010).

[25] Volodymyr P. Horbulin, Oleksandr H. Dodonov, and Dmytro V. Lande, *Informacijni operacii ta bezpeka suspilstva: zagrozy, protydija, modeljuvannja* (Kyiv: Intertehnologija, 2009).

[26] Chris Barrett, Stephen Eubank, and Madhav Marathe, "Modeling and simulation of large biological, information and socio-technical systems: an interaction based approach," in *Interactive Computation* (Berlin: Springer Berlin Heidelberg, 2006).

[27] Kateryna Molodetska, "Tehnologija vyjavlennja organizacijnyh oznak informacijnyh operacij u socialnyh internet-servisah," *Problemy informacijnyh tehnologij* 20 (2016): 84-93.

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

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

[30] Albert Voronyn and Juriy Zyatdynov, "Nelynejnaja shema kompromyssov v mnogokryteryalnyh zadachah," *Information Science & Computing. Artificial Intelligence and Decision Making* (2008).

[31] Kateryna Molodetska-Hrynchuk, "Metod ocinjuvannja oznak zagroz informacijnij bezpeci derzhavy u socialnyh internet-servisah," *Avtomatyzacija tehnologichnyh i biznes-procesiv* 9 (2017): 36–42.

[32] Kateryna Molodetska-Hrynchuk, "Model systemy pidtrymky pryjnjattja rishen dlja vyjavlennja oznak zagroz informacijnij bezpeci derzhavy u socialnyh internet-servisah ta ocinjuvannja ih rivnja," *Bezpeka informacii* 23, no. 2 (2017): 136–144.

[33] Ruslan V. Hryshchuk and Kateryna 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.

[34] Ruslan Hryshchuk and Kateryna Molodetska, "Synergetic Control of Social Networking Services Actors' Interactions," in *Recent Advances in Systems, Control and Information Technology,* ed. Roman Szewczyk and Małgorzata Kaliczyńska, *Advances in Intelligent Systems and Computing* 543 (Cham: Springer, 2017).

[35] Aleksandr A. Kolesnykov, *Synergetycheskoe metody upravlenyja slozhnymy systemamy: teoryja systemnogo synteza* (Moscov: Edytoral URSS, 2005).

[36] Kateryna Molodetska, "Sposib pidtrymannja zadanogo rivnja popytu aktoriv socialnyh internet-servisiv na content," *Radioelektronika, informatyka, upravlinnja* 4, no. 35 (2015): 113–117.

[37] Kateryna Molodetska, "Syntez synergetychnogo upravlinnja popytom agentiv na kontent u socialnyh internet-servisah," *Informatyka ta matematychni metody v modeljuvanni* 5, no. 4 (2015): 330–338.

[38] "Jacenjuk ne vojuvav u Chechni, istorija Bastrykina ne shodytsja – uchasnyk pershoi chechenskoi vijny". *Radio Svoboda*, 09 September 2015, https://www.radiosvoboda.org/a/news/27235507.html (accessed May 22, 2018).

[39] "'Vyzytka Jarosha,' yly pjat punktov TV-propagandyi," *BBC Russisan Service*, 22 April 2014, https://www.bbc.com/russian/international/2014/04/140422_russia_ukraine_propaganda_5points (accessed December 30, 2017).

About the Authors

Ruslan Hryshchuk, Doctor of Technical Sciences, Senior Researcher, Head of the Research Department of Information and Cybernetic Security at the Scientific Center of the Zhytomyr Military Institute named after S.P. Korolyov, Ukraine. He received an educational degree in electronics (2003) and a Ph.D. degree in engineering sciences in armament and military equipment (2007) at the Zhytomyr Military Institute of Radio Electronics named after S.P. Korolev. In 2012, he was awarded the title of the specialty of the information security system. He received a doctorate in science from the specialty of State Information Security (cybersecurity) at the National Aviation University (2013). Dr. Hryshchuk studies in the National Defence University of Ukraine named after Ivan Chernyakhovsky since 2017. Winner of the Diploma of the Cabinet of Ministers of Ukraine (2011), laureate of the Cabinet of Ministers of Ukraine Award for special achievements of youth in the development of Ukraine in 2013 in the nomination “For Scientific Achievements,” laureate of diplomas of the Presidium of the National Academy of Sciences of Ukraine (2010), winner of the All-Martial Competition “Best Invention of the Year” (2014).
E-mail: Dr.Hry@i.ua.

Kateryna Molodetska-Hrynchuk, Ph.D., is an associate professor (2013) in the department of computer technologies and modeling systems of Zhytomyr National Agroecological University, Ukraine. She received an educational degree in control systems and automation in the Zhytomyr Military Institute of Radio Electronics named after SP Korolev (2007) and a Ph.D. degree in mathematical modeling and computational methods at the Division of Hybrid Control and Modeling Systems in the Power Engineering Institute of Modeling Problems in Power Engineering named after G. E. Pukhov of the National Academy of Sciences of Ukraine (2011). Based on her research results aimed at developing a methodology for building a system for ensuring information security of the state in social networking services, she was awarded the scholarship of the Cabinet of Ministers of Ukraine for young scientists for 2016-2018. E-mail: kmolodetska@gmail.com.