

INFORMATION PSYCHOLOGICAL IMPACT DETECTION AND IDENTIFICATION SYSTEM «FALCON»

Andii Gizun, Vladyslav Hriha

Abstract: *The article discusses the theory of information confrontation. Own classification of methods of information psychological impact were developed. The formalized and integrated models of information psychological impact that are used during its detection and identification are developed. The method and system of detection and identification of information psychological impact based on fuzzy logic were developed for the first time. The results of work can be used for the effective implementation of countermeasures against the negative informational impacts in the conditions of information warfare.*

Keywords: *Information psychological influence, Information warfare, Destructive influence, Expert evaluation, Quantification.*

DOI: <https://doi.org/10.54521/ijita30-02-p03>

Introduction

Information impact is becoming more and more important in the modern world. This process is facilitated by globalization and the transition to an information society. Exactly this factor affects on the wider use of the information tools for self-interest. The most widespread areas of their implementation are military, political and economic. During the military operations, important aspects are the popular support of the military actions, deterioration and disorganization of the enemy morally-psychological state, in the political sphere – the incensement of the government trust percentage, the imposition of ideology, and in the economic sphere – gaining an advantage over a competing company or over the whole state. One of the methods to achieve this is the information psychological impact.

The issue of providing information psychological security in Ukraine gained the particular importance due to Russia's aggression against Ukraine, when the question of formation of support by the population of the territorial integrity of Ukraine, and maintenance a high level of moral combat spirit of ATO troops was raised. The information psychological impact implementation and providing information psychological security is impossible without a detailed examination of its theory and methods of realization [1]. During this research were examined the scientific works of South African scientists B. Van Niekerk and M. Maharaj, in which studied the lifecycle of information and psychological warfare, Finns Yormakka I. and J. Mols, in which studied the information warfare from the perspective of game theory, Australians B. Hutchison M. Warren in which identified and described the tactics of information warfare, American S. Johnson with his information attack model, and US Council Scientific Research of monitoring [2- 4]. Also studied works of Ukrainian scientists: A. Shiyan, who presented method of detection information psychological influences and confrontation methods and R. Grischuk, who considered the technological aspects of information influences. Above-mentioned researchers have made a significant contribution in practical research of information psychological influences [5-6]. In this study developed a formalized informational psychological influence model, define basic characteristics and design the method, and based on it the detection system and the identification information psychological influences.

Information Psychological Impact Detection and Identification Method

First, The Information psychological impact I can be described via the tuple:

$$I = \{Id, Is, T, Q, R\}$$

The above parameters of the tuple form the target model and are determined by the signs of information psychological impact.

Id – set of methods methods of information psychological impact $Id = \{Idp\}$.

Is – the space on which the information psychological impact is carried out. It is important to limit the size of space, objects of information infrastructure and

social groups that are exposed to IPI (aggression does not affect the whole information psychological space of the victim state, but only part of it).

T – time of impact. The duration of the use of information psychological impact methods on a particular information space.

Q – purpose of impact. The purpose is a local or partial goal, as a rule, aggression ceases after the aggressor has achieved the full achievement of the specific goals and rarely takes a protracted nature.

R – a set of countermeasures aimed at resisting information psychological impact.

Also the functional model of information psychological impact I can be represented as:

$$I = \{Idp, IPI, OPI\}, \text{ where}$$

Idp – method of information psychological impact. During one information psychological impact action several methods can be used simultaneously. During the modern warfare, the following classification can be made:

1) methods aimed at people who perceive the information critically:

- change of opinion by persuasion;
- psychological isolation of the object;
- coercion;
- propaganda.

2) methods aimed at people who perceive the information uncritically:

- misinformation;
- propaganda;
- change of sights by suggestion;
- infection;
- manipulation;
- reframing.

As we can see, there is a certain imbalance among the methods, which are directed at people who perceive information uncritically in most cases. This situation is due to the fact that it is much easier to achieve a result, to carry out an attack, if the attacker's actions are aimed at noncritical thinking, since they will bypass a certain "psychological shield" of a person.

Propaganda is attributed to both groups, because of the variety of means, it is evident that its use is equally effective for all people.

IPI - set of identifying parameters.

OPI - set of evaluation parameters.

Concepts and classifications regarding information psychological impact analysis has shown that today there is no single classification that would cover all aspects and characteristics of its implementation during the information warfare.

During the research, the following basic characteristics of the *Idp* were identified:

- «information psychological impact implementation duration» - *LT* ,
- «stage of manifestation» - *DM* ,
- «economic losses level» - *EL* ;
- «percentage of the population that watches foreign TV» - *PP* ;
- «percentage of the population that reads the foreign press» - *PN* ;
- «level of trust in government» - *CG* ;
- «the level of population protest attitudes» - *PM* ;
- «information infrastructure development degree» - *II* ;
- «external factors impact degree» - *IF* .

So, the set of identifying parameters for the number of investigated situations when $n = 8$ can be presented as follows:

$$IPI = \left\{ \bigcup_{i=1}^N IPI_i \right\} = \{IPI_1, IPI_2, IPI_3, IPI_4, IPI_5, IPI_6, IPI_7, IPI_8\} = \{LT, DM, EL, PP, CG, PM, II, IF\}$$

Reference values are formed in accordance with [7, 8].

The parameter EL is characterized by the following linguistic assessments: $\{\text{short}(S), \text{medium}(M), \text{long}(L)\}$. Intervals for reference values determination = $\{[0-25], [26-50], [51-100]\}$ days.

After making the transformation, obtain a set of parameter reference values $LT = \{\text{short}(S), \text{medium}(M), \text{long}(L)\}$ and the terms of the linguistic variables for this parameter:

$$S = \{0/0,25; 1/0,25; 0,3/0,5; 0,1/1; 0/1\}$$

$$M = \{0/0,25; 0,6/0,25; 1/0,5; 0,7/1; 0/1\}$$

$$L = \{0/0,25; 0,5/0,25; 0,7/0,5; 1/1; 0/1\}.$$

Similar operations were conducted for other methods. Let's represent the calculated reference values in the form of graphs [14].

Therefore, in order to predict the possibility of realizing information psychological impact or to define and identify it is necessary to develop a system that will monitor the basic characteristics and, basing on heuristic rules, to reveal information psychological impact.

Currently, there is a problem of identifying the methods of information psychological impact. For its solution it is expedient to use a mechanism of heuristic rules, which will help to conduct identification on the basic characteristics of the methods.

The construction of rules is usually carried out on the basis of an expert approach, and this is especially important in cases where one of the alternatives needs to be preferred. To select one solution from the set of alternatives, we use the methods of determining the coefficients of importance [7]. We will use the method of rank transformations, because it allows to attract several experts, tabular forms are used as input, the output function is linear, and the complexity is low.

Apply the apparatus of the logical-linguistic connection "method-parameter" and the interdependence between the rates of parameters and the possibility of

implementing an information attack, we will form heuristic rules for their detection and identification by analogy with [9].

Heuristic rules allow you to evaluate the possibility (degree) of the implementation of this or that attack, depending on the set of values of parameters at a certain point in time. During the research, the following basic characteristics of the IPI were identified: «stage of manifestation» - DM, «economic losses level» - EL; «percentage of the population that watches foreign TV» - PP; «percentage of the population that reads the foreign press» - PN; «the level of protest attitudes of the population» - PM; «information infrastructure development degree» - II; «level of trust in government» - CG; «the goal of IPI implementation» - RE; «external factors impact degree» - IF, by which the detection and identification process is carried out. Characteristics may acquire the values determined by the linguistic variables – «Low» (L), «Medium» (M), «High» (H) for IF, EL, PM, «Primary» (P), «Deployed» (D), «Final» (F) for DM, «Undeveloped» (U), «Moderately developed» (M), «Developed» (D) for II; «Distrust» (D), «Partial trust» (P), «Full confidence» (F) for CG; «Small» (S), «Medium» (M), «High» (H) for PP and PN.

Let's formulate a set of heuristic rules for detection and identifying the IPI method "Persuasion" and present it in the form of a table. It can be characterized by the following confidence indicators of its implementation: "Low" (L), "Average" (A), "High" (H), which is evaluated based on the value of the identifying parameters set for it (DM, EL, II, PN, PP). Taking into account all possible combinations of controlled parameters states, it is possible to form 243 corresponding heuristic rules. Here are some of them.

Similar operations were conducted for other methods. Detection and identification of information psychological impact will help to select and implement means of countermeasures more effectively, which will help minimize losses from its negative effects. The method of detection and identification of information psychological effects was developed exactly for this purpose. It allows to detect and identify impact on a population of more than 1,000 people. The method uses such methods of fuzzy logic as a method of linguistic terms using statistical data (MELS) – for constructing reference values

of parameters and evaluation benchmarks, linear approximation by local maximum (LALM), generalized Heming distance (HD) – to process fuzzy data and carry out fuzzy logic operations. In addition, expert methods of evaluation and ranking are used: the method of average grades (AG).

The method consists of the following steps:

Stage 1. Formation of sets of basic characteristics and information psychological impact methods.

Stage 2. Formation of bundles of basic characteristics with information psychological impact methods. A set of bundles of the basic characteristics with information psychological impact methods is formed, on the basis of which the identification of a specific type of IPI and the construction of reference values is carried out [10, 11].

Stage 3. Fuzzy parameters benchmarks formation. This stage is aimed at obtaining reference values, which compares to the current values of controlled parameters [12].

Stage 4. Formation of a set of heuristic rules. Creation of sets of heuristic rules that are used to detect information psychological impact on the basis of comparison of reference and current values of information space parameters using a set of identifiers of the current state, unique to each method of information psychological impact [9].

Stage 5. Pacification of parameters monitored for the purpose of revealing information psychological impact. At this stage, the transformation of a current values plurality of parameters that are fixed at each t intervals over a certain period of time T in one fuzzy number occurs and thus we obtain fuzzy numbers characterizing the current values of the identifying parameters [7, 10, 11].

Stage 6. Identifying parameters current values processing and result formation.

The issue of impact assessment and evaluation parameters OPI will be discussed in other works.

Experimental Study of Information Psychological Impact Detection and Identification System «Falcon»

Before the identification of information impact is not currently enough, considering the importance of protecting social groups, coupled with the rapid development of modern means and methods of violating information security. There is a need for its identification, since the choice of countermeasures is more effective for a particular and previously known impact. Therefore, the primary purpose of this system is to predict or detect and identify the IPI. Nowadays, there are no analogous systems. An example is a system for detecting information psychological impact, which is based on the theory of probability [13]. This approach does not allow to detect unknown methods of impact, to control a slightly formalized space. In addition, such systems require a long-term preparatory stage before they are put into operation. As part of such training, there is usually a sample of statistical data, system training, etc. Therefore, when developing this system, we will use approaches based on fuzzy logic and expert methods that devoid of such disadvantages. The purpose of Detection Identification Information Psychological Impact System “Falcon” (DIIPIS) is to detect and identify the IPI. The input data of the system are IPI identifiers, controlled parameters and their values. At the output of the system - information about IPI, its identifying data.

The architecture of DIIPIS includes such structural elements as (Fig. 1): sensor system (SS); the module of initial processing of input parameters, containing the identifying parameters registers (IPR), IPI registers (IPIR), impact parameter bundle formation block (IPBFB); module of secondary processing of identifying parameters, consisting of a phasification parameters identification block (PPIB) and the phased parameters sets formation block (PPSFB); module for fuzzy arithmetic operations execution, which includes the current state identifier formation block (CSIFB) and decision block (DB); a module of benchmarks and heuristic rules formation, which includes the corresponding blocks of the same name BFB and HRFD; a result representation module containing a logical conclusion block (LCB) and visualization block (VB); and mode control module (MCM) that puts the system in a benchmarks correction mode (BCM) or

heuristic rules correction mode (HRCM). The SS is located in a cybernetic environment that is fuzzy and slightly formalized. The composition of SS depends on the goals set. The SS monitors the context in the cybernetic space.

For DIIPIS input parameters are IPI; output parameters – the degree of expert confidence in the decision to identify the fact of IPI realization. The maximum parameters values are determined by the expert depending on the field of application and type of impact, which is the reason of the current situation. In addition, identifying parameters can be described as linguistic variables, such as "low" (H), "medium" (C), "big" (B), etc.

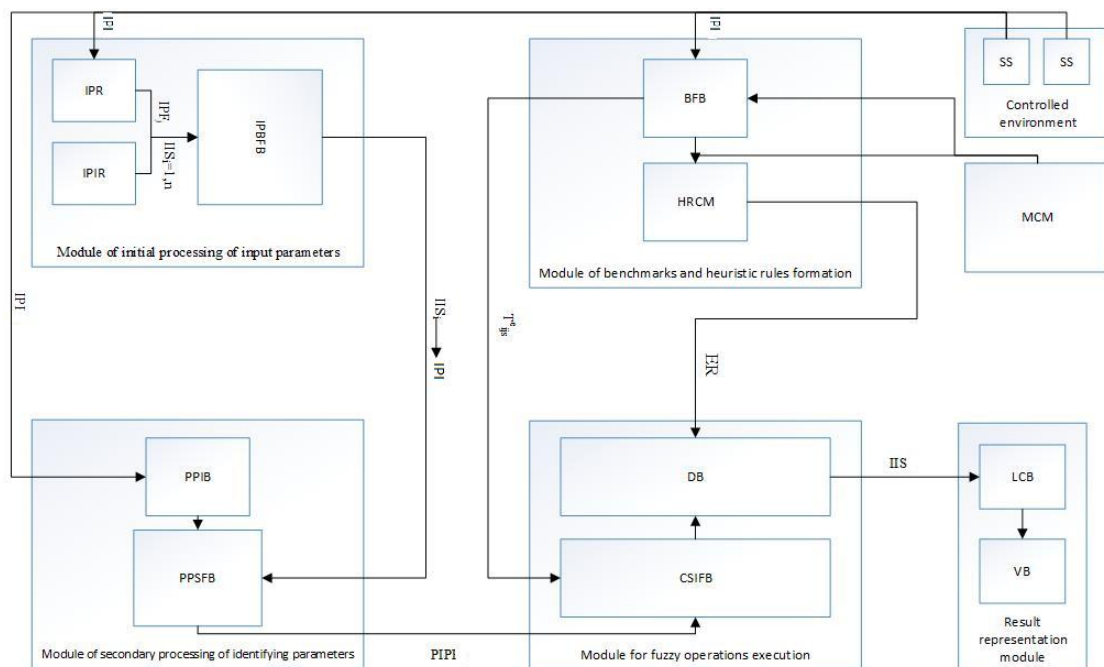


Figure 1. The architecture of DIIPIS

DIIPIS research is performed in a full accordance with the stages of the IPI detection method - a set of identifying parameters is given; their current values are measured and phasified, which are then compared with the benchmarks; the identifiers of the current situation are checked for compliance with the given rules from the set of HR, the result is formed (decision on the possibility of implementation of the IPI is taken).

The experiment was conducted within 10 days (01.05.2023 - 08.05.2023). The participants of the experiment were competent representatives of state authorities, employees of special services of Ukraine, scientists in the field of information warfare. The purpose of the experiment is to detect and identify the information psychological impact on Ukrainian citizens in 2023. During the examination, a number of information psychological impact methods were detected and identified (Table 1):

Table 1. Experiments result

The name of the method	Number of detections
Manipulation	14
Psychological isolation	0
Suggestion	19
Persuasion	12
Propaganda	12
Misinformation	5
Reframing	1
Coercion	0
Poisoning	10

Conclusion

After the results of the work are solving the actual scientific and practical task of developing the method and the system for detection and identification of information and psychological impact.

In the process of implementation, we obtained such significant results:

1. An analysis of modern theories of information confrontation was conducted. It is determined that the subject of information confrontation is widespread in scientific research, but there are no developments in establishing the fact of detection and identifying information psychological impact.
2. Benchmarks of identifying parameters and heuristic rules for identification of information psychological impact have been developed. The method was

developed for the first time, and on its basis a system of information psychological impact. The results obtained in the work can be used to develop countermeasures against the negative informational impacts in the context of information warfare in order to increase the information psychological safety of citizens, society and the state, as well as the preliminary and current assessment of the congestion level of specific IPIs.

3. The method and system of detection and identification of information psychological impact have been experimentally investigated. The result was the detection and identification of IPI methods in the Ukrainian information space during 2023. Thus, the adequacy of the developed methods and models, the possibility of using the developed system in real conditions was confirmed. In the future it is necessary to continue the IPI study in terms of assessing the criticality of their impact and choosing specific effective countermeasures.

Bibliography

- [1] G. Gizun A., Griga V., Analysis of modern information psychological impact theories in aspect of information confrontation, Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 3, p. 272-282. (in Ukrainian).
- [2] Van Niekerk, Brett, Manoj S. Maharaj, The information warfare life cycle model, South African Journal of Information Management, vol. 13, issue 1, 2011, p. 1-9.
- [3] Jormakka, Jorma, J. V. E. Molsa, Modelling information warfare as a game, Journal of information warfare, vol. 4, issue 2, 2005, p. 12-25.
- [4] Hutchinson, B., Warren M, Information Warfare: using the viable system model as a framework to attack organizations, Australasian Journal of Information Systems, vol. 9, issue 2, 2002.
- [5] Shiyan A., Methodology of complex security for the person and social groups against the negative informationpsychological influence, Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 1, p. 94-98. (in Ukrainian).
- [6] Hryschuk R., Fundamentals of cybernetic security: Monograph, Zhytomyr, ZNAEU, 2016, 636 P. (in Ukrainian).

- [7] Korchenko A.G., Development of the security systems on fuzzy sets. Theory and practical solutions, Kyiv, MK-Press, 2006, 320 P. (in Ukrainian).
- [8] Akhmetov B., Korchenko A., Zhumangalieva N., Kultan, J., Model decision rules to detect anomalies in Information Systems, Information Technology Application, 2016, №. 1, p. 126-136.
- [9] Gizun A., Gnatyuk V., Balyk N., Falat P., Approaches to improve the activity of computer incident response teams, Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2015, p. 442-447.
- [10] Karpiński M., Korchenko A., Vikulov P., Kochan R., Balyk A., Kozak R., The etalon models of linguistic variables for sniffing-attack detection, Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2017 9th IEEE International Conference, 2017, p. 258-264.
- [11] Shell J., Coupland S., Fuzzy transfer learning: methodology and application, Information Sciences, 2015, vol. 293, p. 59-79.
- [12] Gizun A., Computer complex for detection and evaluation of crisis situations in information sphere, Ukrainian Information Security Research Journal, 2016, Vol. 18, issue 1, p. 66-73.
- [13] Hriha V., Gizun A., Shchudluck I. Information psychological impact detection and identification system, Project interdyscyplinarny projektem XXI wieku, Tom 2, Bielsko-biala, 2017, p. 131-149.

Authors' Information

Andrii Gizun – Academic department of software engineering National aviation university Kyiv, Ukraine, e-mail: andrii.gizun@npp.nau.edu.ua.

Vladyslav Hriha – Academic department of software engineering National aviation university Kyiv, Ukraine, e-mail: vladyslav.griga@npp.nau.edu.ua.