I. J. Computer Network and Information Security, **2025, 5, 1-14**
Published Online on October 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2025.05.01

Fundamental Principles of the Information Confrontation Ontological Model Construction

Andrii Gizun*
Department of Software Engineering, National Aviation University, Kyiv, 03058, Ukraine
E-mail: andriy.gizun@npp.nau.edu.ua
ORCID iD: https://orcid.org/0000-0002-2974-6987
*Corresponding author

Vladyslav Hriha
Department of Software Engineering, National Aviation University, Kyiv, 03058, Ukraine
E-mail: gsmgrey1@gmail.com
ORCID iD: https://orcid.org/0000-0002-1408-5805

Ruslana Ziubina
Department of Computer Science and Automatics, University of Bielsko-Biala, 2 Willowa St., 43309 Bielsko-Biala, Poland
E-mail: rziubina@ath.bielsko.pl
ORCID iD: https://orcid.org/0000-0002-8654-6981

Received: 10 April 2025; Revised: 28 May 2025; Accepted: 12 July 2025; Published: 08 October 2025

Abstract: The information stage of human society development which began at the end of the last century results in the fact that the state of information security has become directly dependent not only on the information processing technical systems and features but also on the perception of information at the level of individual psychological qualities. The use of information aggression and special information operations including those performed in modern geopolitics at the international and domestic levels for population management, during electoral campaigns is gaining enormous scope. The tasks of early information impact detection, situation development modeling in the information space necessitate the development of specialized models reproducing information confrontation. The major contradiction in the development of such models is that the more relevant and adaptive these models are the more complex and resource-intensive they become. At the same time, oversimplifying the information confrontation process makes such models inconsistent with real risks. This article gives a brief overview of modern information confrontation models and concepts. It is described the basic principles of the construction of an information confrontation ontological model: such key elements as subjects, objects, actual impacts, and the basic characteristics of each element are identified. An attempt has been made to develop a universal information confrontation ontological model. It has been also proposed a multipart tuple of information confrontation representation. This article is the beginning of a separate research project on information confrontation modeling, which will be further developed in papers to follow.

Index Terms: Information Confrontation, Information Warfare, Model, Ontological Model, Subject, Object, Information Impact, System, Set, Subset, Interconnection.

1. Introduction

Historical experience has shown that information circulating in automated governance and communication systems, which are integral components of the state, economic, financial and defense management structure, is becoming a critical public resource, which has an increasing impact on national security.

However, the role of other information resources in the state and citizens` private and public life is increasing. Increased information scope, information infrastructure, and the level of digitalization in administrative and economic processes are clear and unstoppable trends of today. All this leads to the fact that the rivalry unfolding around the information resource, the struggle for its possession, the achievement and retention of information advantage today occupy a central position in the geopolitical competition among developed countries. The fighting ground for a battle (not necessarily between two countries, as information confrontation processes become multilateral) is the so-called

infospace or infosphere as a separate new geographical shell of the Earth - along with the noo- and technosphere.

The Infosphere is an international information space that covers information flows, information resources and all spheres of civilization`s life. The infosphere can also be defined as cyberspace with mass media [1].

Cyberspace is a virtual space formed by information, telecommunication and information-telecommunication systems (local computers, local and global networks), in which information production, storage, processing, exchange, and destruction are performed electronically [2].

Cyberspace is a virtual space formed by information. Mass media are a means of communicating information (verbal, audio, visual) based on the principle of a wide-ranging channel covering a large audience and operating on a continuous basis [3].

Due to the emergence and accelerated development of mass media and cyberspace, the role of public opinion has dramatically increased becoming extremely influential in political processes in society, especially in the operation of the social information environment. Thus, to gain information advantage, it is now possible to influence not only direct decision-making centers in a state but also wider public, large and small social groups, which will then independently exert public pressure on the country`s highest-level leaders. Therefore, it is necessary to study the peculiarities of information impacts aimed at obtaining information advantage based on what practical ways of ensuring the political elite and population`s security should be worked out. And the first stage should logically be information impact formalization in the conditions of information confrontation. It is ensured by ontological, functional and target models, or a single ontological model, which would include all of the above-listed.

That is why the urgent task is to develop an information confrontation ontological model, which, unlike the known models, will describe a wide class of information confrontation objects and subjects and the actual processes of a particular information impact realization. Ontological models typically serve as a basis for special expert systems, predictive methods and simulation facilities for various processes as well as for situation centers` operation. The choice of the ontological description of the information confrontation subject area is made based on the fact that this method allows combining relational, object-oriented, and mathematical models, thesauruses, etc. into a single whole.

Therefore, the aim of the article is to reflect and describe the information confrontation processes by developing a corresponding ontological model. However, to put it more exactly, the result of this work is not an actual ontological model but rather its frame or foundation. In fact, the fundamental features of such a model and a description of its basic elements will be offered. Therefore, it is not improbable that certain changes in the model presented here can be made – its deployment or reformatting, refinement, restructuring in the course of further scientific research.

The work consists of three sections and conclusions. The first of them is devoted to the object of research and analysis of the current state of development of the theory of information confrontation. The second section directly describes the ontological model of information confrontation. The third section contains the results of experimental research of the developed model.

2. Subject Area and Research Overview

To begin with, we should introduce the basic concepts that will be used in our study exactly as described here, unless otherwise stated.

Information impact is an organized deliberate use of special information media and technologies to make changes in the individual, social groups or population`s consciousness (behavioral correction), the information-technical infrastructure of the impacted object and (or) the person`s physical condition [3].

Information advantage is a situation that gives the opportunity to change the opponent's perception of the real situation and deprive them of their ability to predict and influence subsequent events. The vast majority of researchers consider this situation to be the primary purpose of conducting information confrontation.

Information confrontation (IC) is a form of information security provision that is a set of special methods (political, economic, diplomatic, technological, military and others), techniques and means of beneficial influence on the information sphere of the object of interest and on the opponent`s (a person, organization, state) vital information search, processing, dissemination and storage systems together with the protection of one`s own information sphere from an unauthorized and destructive influence in order to achieve the set goals [4].

The purpose of the information struggle is to provide the necessary degree of one`s own information security and to minimize the information security level of the opposing party. The achievement of information struggle goals is accomplished by carrying out a number of tasks, the main of which is the defeat of the confronting party`s information sphere objects and the protection of one`s own information [4].

The concepts of information impact, information confrontation, and information warfare are not new. Information warfare methods were used in ancient times in numerous wars. Misinformation, propaganda to disorient both the competitive country`s troops and population were used to formulate the necessary information model. Modern information warfare technologies, which are based on different methods of information manipulation, use the capabilities of modern information and cyberspace [5]

Therefore, today these processes are taking on new forms. The scope of confrontation in the information sphere has become so large that it necessitates the creation of a special conception called “information confrontation” or “information warfare”. It is implemented in all spheres of public administration becoming an effective tool for the

administration of both internal and, especially, external policy. This trend is most fully reflected in the concepts of information warfare developed by leading military countries. Information warfare is viewed from various perspectives as one of the main factors ensuring national security and national interests in the vital spheres of state and public activity, in particular in the military one [6].

The concept of information warfare is a system of views on information warfare and ways of its conduct [4]. To date, there is no universally accepted conception of information warfare; moreover, the concepts used to define and study this phenomenon and its consequences have not yet been established and can change according to another classification in the future. Due to its multifaceted nature, various researchers studying information warfare concentrate on its different aspects. According to some researchers, under the influence of evolutionary changes, the information component of combat devices is rapidly increasing ensuring mission accomplishment on the battlefield. The proponents of this approach to the information warfare concept agree that victory will largely depend on the level of the latest information technology development and use in the military sector [7]. Information security issues are recognized internationally: in most industrialized countries, the research and development of new information weapons are underway, allowing direct control over the information resources of a potential adversary and, if necessary, directly influencing them. According to the US think tanks, such weapons are being developed in 120 countries [8]:

- Nuclear weapon developments are on the drawing board in 20 countries;
- In some countries, the development of information warfare (confrontation) tools against a possible adversary is completed, both in case of military conflicts of different intensity and in peacetime at strategic, operational, and tactical levels as well as in the field environment to protect the national infosphere from aggression and unauthorized intervention;
- In developed countries, the concept of information warfare is a military doctrine constituent element requiring personnel and individual units` special training for conducting information operations;
- The experience of international, regional and ethnic conflicts has revealed the uniqueness of the use of information weapons to influence the international community and to fight for geopolitical interests.

Analysts identify the following models of the global information security system [8, 9]:

Model A – the creation of an absolute protection system for a country that is an information leader against any type of an offensive information weapon resulting in an objective advantage in a potential information war. It forces other countries to seek an alliance in military information actions with a leading country. In this case, a system of strict control over the information weapons of an adversary may be used based on potential international information security documents.

Model B – the creation of a significant advantage for a country that is an information warfare-monger in offensive weapons, the neutralization of the hostile state`s defense systems by means of an information impact, the coordination of actions with allied states using certain information weapons to identify sources and types of information threats

Model C - the presence of several leading countries and potential information confrontation between them, the determination of a factor serving as a deterrent for information threats, the prospect of the domination of one of the countries in the field of international information security with the potential to significantly influence the global infosphere and the prevailing right to solve the problems of the global order.

Model D - all parties to the conflict use transparency of information to form situational alliances, to derive the benefits from local decisions that can block technological leadership, to use the informational infrastructure of individual territories in order to organize the internal conflict between opposing forces (political, separatist, ethnic conflicts) to conduct international counter-terrorism information operations.

Model E is a confrontation between the world community and international organized crime that is able to control the course of political, economic, social and, ultimately, civilization processes. The possibility of such a model is foreseen in a study by the US National Intelligence Council's “Mapping the Global Future– 2020” in “Cycle of Fear”, which is the most pessimistic scenario for the future global community.

Experts from leading European countries have proposed the information confrontation conceptual model for a better problem understanding (Fig. 1) [9].

The physical space is the material world where traditional combat operations take place. Here information and communication systems (infrastructure) play the supporting role.

The information space is the dimension where information is created, processed, distributed and stored. It links physical and cognitive dimensions and is used to obtain both input and output information. Information circulates in the so-called OODA "loop" – observation, orientation decision, and action. Decisions are made taking into account information coming from the physical environment (intelligence, reconnaissance and surveillance) and impact the real world through the information space (databases, remote servers and nodes of the specialized computer network).

The cognitive space exists in the human mind. Here the information received in accordance with different perception models is processed, decisions are made, ideas and intentions are formed.

Such a conceptual model can serve as a basis for determining the information confrontation scope for competing subjects and the goals of information dominance.

However, R. Hryshchuk, I. Kankin, and V. Okhrimchuk, Ukrainian researchers studying this issue, have presented their own conception expressed in the form of the scheme "Technological IC aspects at the present stage" (Fig. 2),

which describes each aspect and the relationship between them, the features of planning and implementation, methods, techniques, and tools for information impact realization [10].

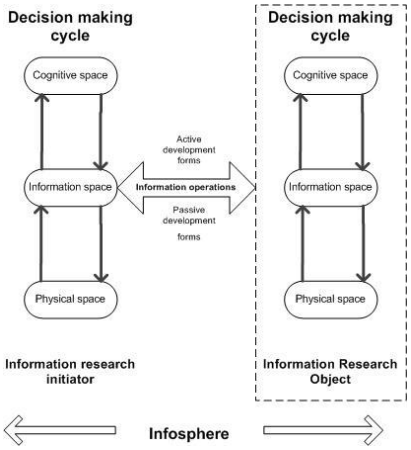

Fig.1. Information confrontation conceptual model

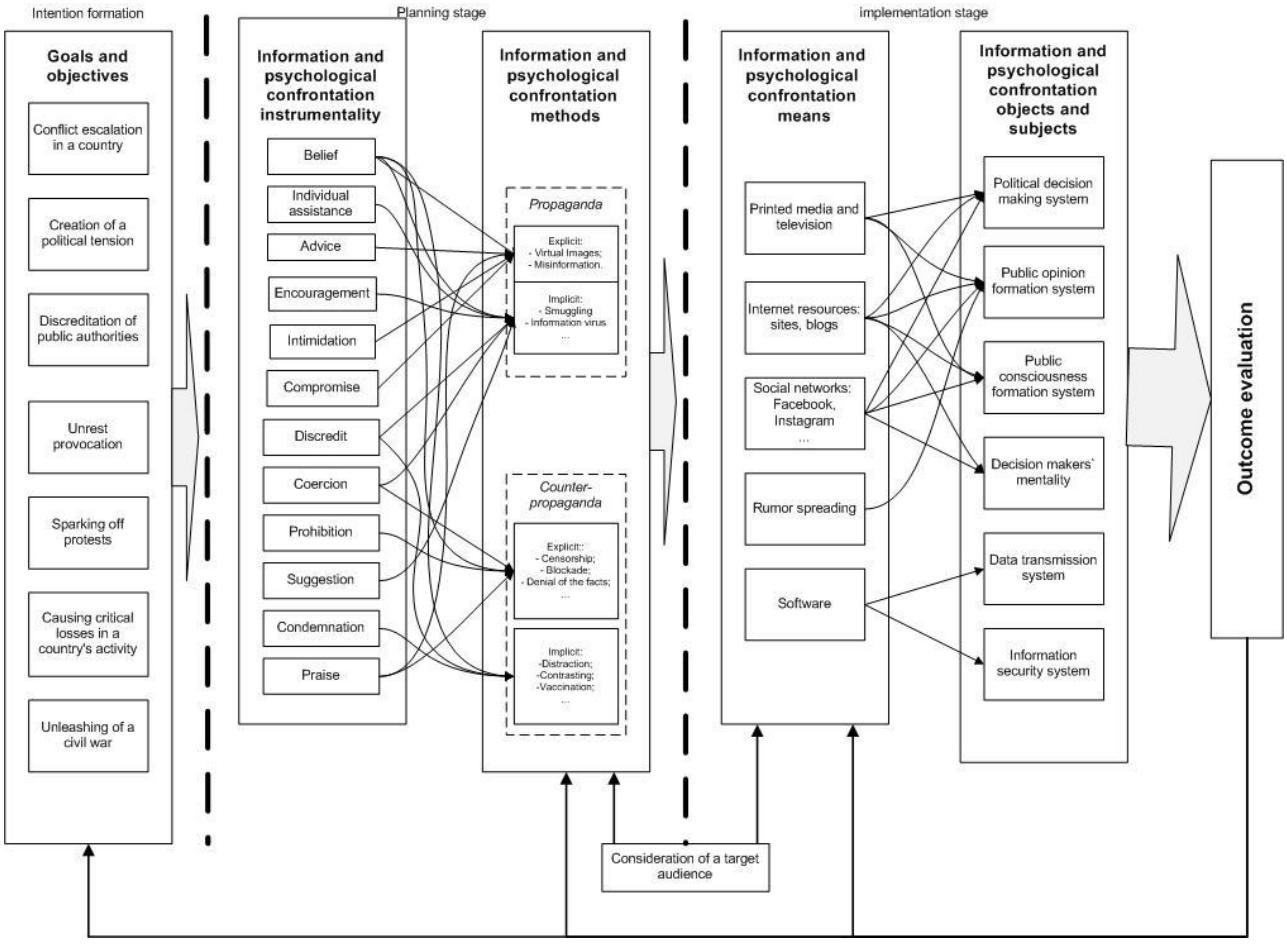

Fig.2. IC technological aspects at the present stage

The capabilities of modern information and cyberspace are determined, first of all, by the possibilities of creating a communication system between users and various objects that are included in the global information environment. Assessing the information security level is a complex problem, and its solution requires an appropriate scientific and methodological basis. In addition to the complexity of the use of information security methods, direct or indirect social dependence of each protection line should also be taken into account. This determines the importance of another IC model based on the consideration of the impacted object as a complex structured system changes in which led to a change in the object state [11,13].

In recent years, IC has been characterized by the elements of information warfare, that is, a set of special operations aimed at a particular object in order to change its state by changing its structure or changing the links

between the elements of that structure. Actions directed towards the object of influence are implemented through the certain categories of public members or through the use of mass media by artificially altering their consciousness and their personal attitude to the object. The subject that implements special operations is a center of impact. A necessary component is the prediction of competitors' behavior and the dynamics of changes in internal threats. This allows us to evaluate possible scenarios of competitors' behavior and to determine the mechanisms for conducting special information operations.

In most cases, typical object destabilization schemes are used, which are formalized in the form of influence on a person, bringing discredit on the object management, information-psychological influence on the public concerning the object of influence, as well as the systematic dissemination of specially selected information [6].

An important task is to create a so-called "friendly interface" through which the center of impact can accomplish its tasks. In this case, the impacted object can also be in two possible states: passive and active. The passive state of an object is characterized by the fact that it falls under the complete information dependence on the center of impact, due to the fact that the center of impact has a significant advantage in different resources: financial, information, ideological, etc. The active state of an object is characterized by the fact that the object carries out appropriate attacking or counterattacking actions [12].

Possible ways for the center of impact to realize its tasks are the mechanisms of propaganda, agitation and IC. For the passive state of the object, the most effective ways are agitation and propaganda, as they are aimed at changing employees` minds and corresponding information dissemination which will change the object state. The IC involves the interaction of competing structures in a struggle for leadership. Concerned parties can act as dual agents and accomplish both the tasks of the impacted object and the center of impact. Through a "friendly impact interface", the prepared information has some effect on a potential competitor. The management of the object of influence takes into account the prepared information that is input to it and makes managerial decisions to provide the required information security level [13].

The structural model of information confrontation implementation is presented in Fig. 3, where ICSS is the interaction center security service formalizing the interaction processes between two competing subjects, which can cause changes in information links between their elements and, consequently, change their structure and object transition to another state [11, 13].

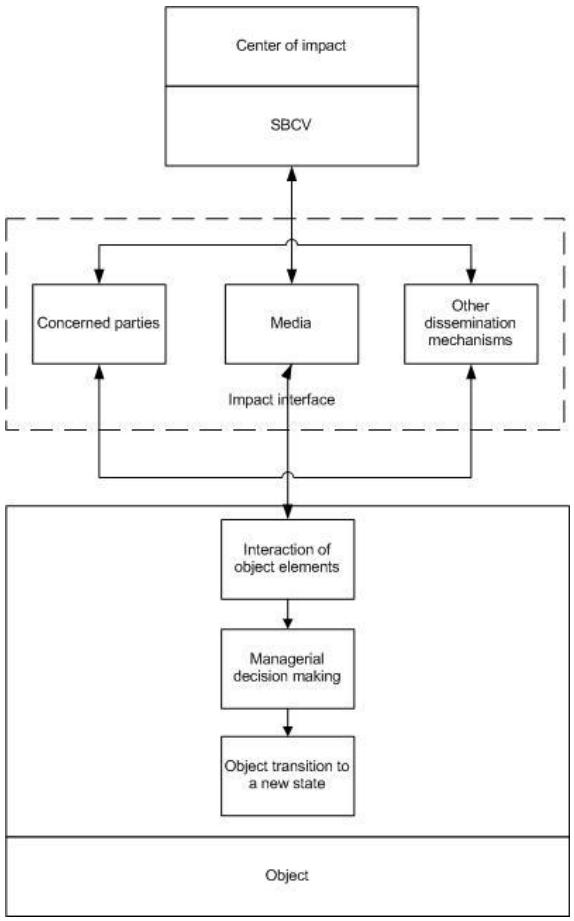

Fig.3. Structural model of the information confrontation

Changing the connections between the elements of an object or its transition to another state can, and in most cases, be accompanied by a decrease in the information security level. Information influence begins with a certain sequence of actions carried out by a competitor. Such actions are treated by any external observer as specially prepared information presented in news received from open information sources and obtained with the help of special technical means and technology, as well as in an agential way [11,13].

In addition, a detailed overview and analysis of these and other known IC conceptions and models are given in our previous article [14]. The summary of considered models is presented in Table 1, in which the following comparison criteria were singled out:

- The mathematical model underlying the conception;
- Ability to reflect subjects and objects;
- Ability to show connections (impact process);
- Functionality to show levels;

+ - Enabling the formalization and description of the model element to the full extent;
- Not applicable for the formalization and description of the model element;
+/- - partially enables the formalization and description of the model element.

Table 1. Generalization of analytical research results

Name	Developers	1	2	3	4
IC Contextual Model [15]	CEPA Project	Statistical characteristics	-	+/-	-
IC Life Cycle Model, L.Cox Model [16]	V. Nickerk, M. Maharaj, L. Cox	Functional and Descriptive	+	+	-
Shiyan Model [17]	A. Shiyan	Mathematical analysis, set theory	-	+/-	+/-
Technological model of information confrontation [10]	R. Hryshchuk, I. Kankin, V. Okhrimchuk	Functional and Descriptive	+	+/-	-
Information Attack Model (three-tier target IC model) [18]	Scott Johnson	Functional and Descriptive	-	+	+
Hybrid models [19]	R. Pev, E. Mevor	Mathematical analysis, social network model	+/-	+/-	-
Information Confrontation in terms of the Game Theory[20]	Jorma Jormack and Yarmo Mols	Game Theory	+/-	+	-
Information Confrontation Tactics [21]	Bill Hutchison, Matt Warren, Stafford Beer	Structural Algorithmic Modeling	+/-	+	+/-
Information Confrontation Lifecycle Model [22]	B. Van Nickerk, M. S. Maharaj	Functional and Descriptive, Graphic	+/-	+/-	+/-

Thus, IC research and development is quite widespread and substantive. However, there is a problem with the information impact and information confrontation formal model construction that would allow us to fully formalize IC processes based on all its components (participants, an implementation process, and level).

3. Ontological Model of Information Confrontation

The contemporary and appropriate ontological model, as shown above, should include all key IC elements and accurately show the interaction between them together with the specifics of their changes. Of course, the key elements of any process are its initiators and managers (subjects) and objectively existing physical systems or objects of a social or technical nature, the features of which are subject to a certain procedural influence adapting accordingly to the conditions of reality which are determined by the course of the process. The ontological model of the process should reflect these features. Therefore, the construction of such an IC model should start with the identification of key objects and subjects of an information conflict (confrontation).

IC Levels, Objects and Subjects. But first, it should be noted that both the IC implementation process and accordingly its subjects and objects depend on the main goals and direction of the information impact and its initiator`s interests. These criteria can serve as a basis for the division of the whole process into sub-processes according to their implementation level (planning, realization). So, it is generally accepted that the information struggle is conducted at three levels: strategic, operational and tactical. At the strategic level, information confrontation is planned and coordinated by the highest bodies of state power. At the operational and tactical levels, this activity is carried out using the resources of the armed forces, national security environment, as well as state socio-political institutions [23].

However, in our opinion, this does not make it possible to clearly classify ICs by their level, since some subjects and objects may be assigned to different levels at the same time. In the determination of the IC level, we stick to the principle of a subjective attribute (identification of a subject). Therefore, we propose to distinguish the following 3 levels: state that includes IC processes initiated, coordinated and implemented by public authorities, or special services, international alliances or international organizations; public describing IC processes initiated, coordinated and implemented by non-governmental organizations, political or social groups, mass media and media corporations;

personal – IC processes that are initiated, coordinated and carried out by individual citizens or small social groups.

It is worth noting that the IC object can also be classified according to levels, but if the IC process involves multi-level subjects and objects, its overall level is determined by the subject level.

The IC subject is a person, a group of people or an organization, irrespective of the form of organization and ownership, which may carry out hostile acts or special information operations, plan or initiate them.

The features of information confrontation subjects according to [11] are as follows:

- the subject has its own interests in the information and psychological space;
- the presence in the subject` structure of special forces (departments), functionally intended for conducting information confrontation or authorized to conduct information confrontation;
- ownership and / or development of information weapons, their delivery and disguise means;
- under control of the subject there is a segment of the information space, within which it has the priority right to set rules for the regulation of information-psychological relations (on the ownership rights codified by the national and international law) or state sovereignty (the national segment of the information space as a part of the state territory);
- the existence in the official ideology of provisions allowing the subject's participation in information confrontation.

Subjects of information confrontation according to [11] can be:

- states, their unions and coalitions;
- international organizations;
- non-state illegal (including illegal international) armed formations and organizations with a terrorist, extremist, radical political, and radical religious orientation;
- religious organizations, sects and neo-cult groups
- transnational corporations;
- virtual social communities;
- media corporations and mass media;
- bodies of special services;
- enterprises and organizations (subject to certain characteristics);
- non-governmental public associations and movements;
- individual citizens, their groups (under certain conditions and if there are interests in the IC area).

Similar to the approach proposed in [11, 13], subjects in our model may be in several states – active when they can fully exert their own informational influence offsetting the enemy`s impact, and actively act in this direction; and passive when a subject is capable of influencing hostile objects, but for some reason does not take active actions; in a lock state, when under the influence of hostile subjects it loses wholly or partly their ability to realize any form of information impact according to their goals and objectives. Initially, the subject is in a passive state.

The information confrontation object is any object exposed to information impact (including the use of information weapons) or other influence (power, political, economic, etc.) resulting in the modification of its properties as an information system. The information confrontation object can be any component or segment of the information and psychological space [11].

A common feature of an information confrontation object is any form of information used in its functioning [11].

Based on the above, we can distinguish information confrontation generic objects:

- system of social relations in the information society (citizens` mass consciousness, a system of social values, value system psychological tolerance);
- system of political relations in the information society (socio-political systems and processes, state institutions);
- system of psychological relations in the information society (citizens` individual consciousness, psychological tolerance (stability) of citizens` consciousness, citizens` mental health);
- technical systems in the information society (information infrastructure, management, communication, information security, and weapon systems).

Given that all objects can be both technical and physical in nature, which is consistent with the conventional division of IC into 2 groups – information-psychological (IPC) and information-technical (ITC) confrontation, they should be classified by this feature.

The following subgroups may then be protected (or impacted) under IPC [24]:

- political decision-making systems (public authorities and their individual representatives, political parties and associations, etc.);
- public opinion formation systems (public associations, trade unions, public media);

- systems of public consciousness formation (book-printing organizations, cinematographers, TV-program producers, private printed media, individual citizens and small social associations).

The following subgroups are subject to protection under ITC [24]:

- data transmission systems;
- information management and protection systems;
- electronic warfare systems

The purpose of IC subjects` influence is to change the object operation, to disable them or to make them work incorrectly. If an IC object ceases to perform its direct functions, it may indicate that information impact is exercised. For this purpose, the initial functions of IC objects should be defined (Table 2). The following reference designations are used:

- Classification of IC objects by type
- IC object
- Initial functions of IC objects F

Table 2. Features of IC objects

1	2	3
IPC	Political decision-making systems	– articulation of interests and public opinion preparation; – problem analysis and draft decision development; – political decision making; – execution of a decision.
	Public opinion formation systems	– Promoting the transition from verbal to real behavior; – The influence of public opinion on the power structures and the adoption process of socially significant decisions.
	Public consciousness formation systems	– Informational – Cultural and educational – Integrative – Socio-pedagogical or managerial – Organizational – Educational
ITC	Data transmission systems	– Provision of an open secure communication channel for subscribers; – Signal conversion; – Transmission of information between two or more users via a data channel.
	Electronic warfare systems	– Obtaining information on the location of radio-electronic means, troop command systems and the enemy's weapons, their destruction by all kinds of weapons or seizure (bringing out of operation) and radio-electronic suppression; – Radio-electronic protection of their radio-electronic means, troop command systems and weapons against radio-electronic reconnaissance and counteraction organized by the enemy (counter- electronic countermeasures).
	Information management and security systems	– Recording the cases of security policy violation, dangerous and unforeseen events, and analysis of the reasons leading to them as well as the database support of such events. – Taking measures in case of unauthorized access attempt detection to the resources of complex systems, the violation of information security facility operation rules or other destabilizing factors. – Ensuring the integrity of information security tools and responding quickly to their failure or malfunction – Access management of system resources – distribution among the users of the necessary information security details: passwords; privileges; keys. – Information security database support and activation: access matrices; classification tags of objects; user IDs. – Monitoring, logging and audit of system events, their components. – Archiving, backing up software components, storing and testing them. – Analytical assessment of the current information security condition in complex systems.

Thus, it can be argued that in the normal state, each object has a set of functions $\mathbf{F}$, depending on its type. The very ability to perform these functions determines the conditions of transition of the object from the normal state to others: the state of getting impaired, in which the object impacted by the hostile IC subject loses a number of its functions but is able to perform some of the standard functions to a limited extent, that is, a set of its functions $\mathbf{F}' \neq \mathbf{F}$, and the state of death when $\mathbf{F}^{x} = \mathbf{0}$. The change in a set of performed functions is due to the presence of information impact caused by the subject. These impacts are one of the key IC processes that require a separate mathematical apparatus to describe them, and can be categorized as being carried out under IPC, ITC, and II as the most aggressive IC form. It is worth stressing that the level of influence is determined by the IC subject.

Information impact is expressed in the form of specific actions, special information operations or their elements with the use of information weapons, so the existing classifications of information weapons are important and connected with their description.

Table 3 summarizes the results of the study of information impacts. The following in the table is referred to as:

- Impact category;
- Objects that can be influenced;
- Name of impact;
- Impact means;
- IC levels (state / public / individual) (S / P / I).

Table 3. Formal description of information impacts

1	2	3	4	5
IPC	Consciousness and mentality of the population, the enemy`s members of the armed forces, special services, the public opinion formation system as well as strategic managerial decision-making	Information and psychological impact	Word, information	P, I
		Neurolinguistic impact	Penetration into the human consciousness of special linguistic programs	P, I
		Psychoanalytic impact	Therapeutic agents (especially in the state of hypnosis or deep sleep)	I
		Psychotronic impact	Information transmission through extrasensory (unconscious) perception	P, I
		Psychogenic impact	Physical impact on the individual`s brain, the shock effect of environmental conditions or events	I
		Psychotropic impact	Psychotropic drugs	P, I
ITC	Automated information systems Electronic information resources and databases	Information and Computer Impact	Specially written programs and hardware-software complexes (information weapons), destructive influence software (Trojans, logic bombs, etc.); an effective and common way to block such resources is to deploy denial-of-service cyber attacks	S, P
	Telecommunication and communication systems	Hardware and technical impact	Violation of the normal telecommunication system operation, the creation of electromagnetic interference	S, P
	Automated information and communication systems, information dissemination process	Electronic warfare	Using physical methods (creating interference)	S, P
II	Consciousness and subconscious of a society or a certain group of people,	Information Impact Campaigns	Bogus stories, misinformation, rumor spreading	P
	The consciousness and subconscious mind of the "decision-maker", the country`s population.	Special information operation	Propaganda, public opinion diversification, psychological pressure.	P, I

Mathematical description of the ontological model. In this paper, we will try to mathematically describe the key elements of the ontological model which include subjects, objects and actual IC processes.

Each individual subject is an element of a subset of subjects of a certain level, which taken together form a common set of subjects. Thus, we define a set of IC subjects $\mathbf{S}$:

$$\mathbf{S} = \{\bigcup_{\mathbf{r=1}}^{\mathbf{R}} \mathbf{S_r}\} = \{\bigcup_{r=1}^{R}\bigcup_{i=1}^{I_r} S_{ri}\} = \{\{\mathbf{S_1}\},\{\mathbf{S_2}\},..,\{\mathbf{S_R}\}\} = \{\{S_{11},S_{12},..,S_{1I_1}\},\{S_{21},S_{22},..,S_{2I_2}\},..,\{S_{R1},S_{R2},..,S_{RI_R}\}\} \quad (1)$$

Where $\mathbf{S_r} \subseteq \mathbf{S}$ is a subset of the r level subjects, R is the total number of subject levels (the level of the IC process realized by them) and I_r is the number of subjects of the same IC level, and it is not strictly defined and can change allowing the easy expansion of both the model itself and its scope of application.

Since we have already identified the 3 basic states of a subject, we will use the following designations: S_{ri} is the subject in a passive state, S_{ri}^{+} is the subject in an active state, S_{ri}^{-} shows that the subject in a lock state. It should be noted that the subject not only exercises attacking information impact, but also performs protective functions in relation to its own objects.

In the active state, subjects influence objects by changing their structure and a set of functions. Therefore, to begin with, we define a set of IC objects $\mathbf{O}$ that will contain subsets of the objects of defined groups (IPCs and ITCs), which in turn contain the subsets of subgroups:

$$\mathbf{O} = \{\bigcup_{\mathbf{g=1}}^{\mathbf{G}} \mathbf{O_g}\} = \{\bigcup_{\mathbf{g=1}}^{\mathbf{G}} \bigcup_{\mathbf{p=1}}^{\mathbf{P_g}} \mathbf{O_{gp}}\} = \{\bigcup_{g=1}^{G} \bigcup_{p=1}^{P_g} \bigcup_{j=1}^{J_{pg}} O_{gpj}\} = \{\{\mathbf{O_1}\},\{\mathbf{O_2}\},..,\{\mathbf{O_G}\}\} =$$
$$=\{\{\{\mathbf{O_{11}}\},\{\mathbf{O_{12}}\},..,\{\mathbf{O_{1P_1}}\}\},\{\{\mathbf{O_{21}}\},\{\mathbf{O_{22}}\},..,\{\mathbf{O_{2P_2}}\}\},..,\{\{\mathbf{O_{G1}}\},\{\mathbf{O_{G2}}\},..,\{\mathbf{O_{GP_G}}\}\}\} =$$
$$= \{\{\{O_{111},O_{112},..,O_{11J_{11}}\},\{O_{121},O_{122},..,O_{12J_{12}}\},..,\{O_{1P_1 1},O_{1P_1 2},..,O_{1P_1 J_{1P_1}}\}\},$$
$$\{\{O_{211},O_{212},..,O_{21J_{21}}\},\{O_{221},O_{222},..,O_{22J_{22}}\},..,\{O_{2P_2 1},O_{2P_2 2},..,O_{2P_2 J_{2P_2}}\}\},..,$$
$$\{\{O_{G11},O_{G12},..,O_{G1J_{G1}}\},\{O_{G21},O_{G22},..,O_{G2J_{G2}}\},..,\{O_{GP_G 1},O_{GP_G 2},..,O_{GP_G J_{GP_G}}\}\}\} \quad (2)$$

where $\mathbf{O_{gp}} \subseteq \mathbf{O_g} \subseteq \mathbf{O}$ is the subset of objects of the g group of the p subgroup, G is the total number of object groups, P_g is the total number of the object subgroups in the g group, and J_{pg} is the number of objects in subgroup p of group g, and these numbers can be varied allowing the easy expansion of both the model itself and its scope of application.

Since we have already identified the 3 basic states of an object depending on the number of functions they perform, we will use the following designations: O_{gpj} is the object in a normal state, O'_{gpj} is the impaired object, O^x_{gpj} is a dead object.

Each individual subject can exert an information impact on the object in various forms, in particular by forming and transmitting a dynamically variable dense flow of information messages, and it is advisable to classify this influence at the level of realization (determined by the subject) and realization categories (within IPC, ITC and II). Thus, we define a set of many information impacts in the IC process $\mathbf{I}$:

$$\mathbf{I} = \{\bigcup_{\mathbf{k=1}}^{\mathbf{K}} \mathbf{I_k}\} = \{\bigcup_{k=1}^{K} \bigcup_{n=1}^{N_k} I_{kn}\} = \{\{\mathbf{I_1}\},\{\mathbf{I_2}\},..,\{\mathbf{I_K}\}\} =$$
$$\{\{I_{11},I_{12},..,I_{1I_1}\},\{I_{21},I_{22},..,I_{2I_2}\},..,\{I_{K1},I_{K2},..,I_{KI_K}\}\} \quad (3)$$

where $\mathbf{I_k} \subseteq \mathbf{I}$ is a subset of information impacts of the k category, K is the total number of information impact categories and N_k is the number of information impacts of one category, and it is also not strictly defined and can change allowing the easy expansion of both the model itself and its scope of application.

The intensity and accordingly the estimation of information impact destructiveness which under certain conditions can provoke the transition of the object from the normal state to the state of impairment or death is calculated according to the approach described in [25, 26]

Another essential element of the ontological model is the channel of influence – the environment or technical system that connects the subject and the object and through which the transmission and distribution of impact takes place. Mathematically, it can be defined by a set $\mathbf{Ch} = \{\bigcup_{l=1}^{L} Ch_l\}$ where L is the total number of channels available, and its main elements will be different types of impact channels: oral, print, written, audio, visual, of a psychic and telepathic nature (focused on human subconsciousness), electronic, electromagnetic, low-and high-frequency, the Internet link and social networks as its variation, virtual and more

Each channel is characterized by information capacity, transmission speed, noise immunity, range and other technical characteristics.

Summarizing the described fundamental principles for the construction of the information confrontation ontological model and having identified its main elements, the IC process can be represented as a multi-component tuple by analogy to [27]

$$\mathbf{IW} =< \mathbf{S,O,I.Ch} > \quad (4)$$

4. Experimental Research

The practical application of the developed ontological model may consist in the modeling of information confrontation processes and the formalization of such processes. The latter can be merely based on the model framework described here.

The information confrontation formalization process involves the opportunity to describe its key components and their relationships, without the description of the essence of their formation and existence, the specific elements of a general situation and changes in the states of each object or subject.

First, we define a set of subjects. Provided that $R = 3$ and with the unlimited number of subjects, expression (1) describes a set of subjects $\mathbf{S}$ as follows:

$$\mathbf{S} = \{\bigcup_{\mathbf{r=1}}^{\mathbf{3}} \mathbf{S_r}\} = \{\bigcup_{r=1}^{3}\bigcup_{i=1}^{I_r} S_{ri}\} = \{\{\mathbf{S_1}\},\{\mathbf{S_2}\},\{\mathbf{S_3}\}\} =$$
$$\{\{S_{11},S_{12},..,S_{1I_1}\},\{S_{21},S_{22},..,S_{2I_2}\},\{S_{31},S_{32},..,S_{3I_3}\}\}$$

where $\mathbf{S_1}$ is a subset of state-level subjects, for example, S_{11} is a parliament, S_{12} is intelligence service, etc. (this and the following subsets are finite, but we are not aiming at its full definition);

$\mathbf{S_2}$ is a subset of public-level subjects, such as S_{21} referring to a terrorist group, S_{22} as a multinational corporation, and so on;

$\mathbf{S_3}$ is a subset of individual-level subjects, such as S_{31} referring to a citizen N, S_{32} as a small enterprise, etc.

Then, under the conditions when $G = 2$, $P_1 = P_2 = 3$ and not strictly specified number of objects, expression (2) will describe the set of objects $\mathbf{O}$ as follows:

$$\mathbf{O} = \{\bigcup_{\mathbf{g=1}}^{\mathbf{2}} \mathbf{O_g}\} = \{\bigcup_{\mathbf{g=1}}^{\mathbf{2}}\bigcup_{\mathbf{p=1}}^{\mathbf{3}} \mathbf{O_{gp}}\} = \{\bigcup_{g=1}^{2}\bigcup_{p=1}^{3}\bigcup_{j=1}^{J_{pg}} O_{gpj}\} = \{\{\mathbf{O_1}\},\{\mathbf{O_2}\}\} =$$
$$=\{\{\{\mathbf{O_{11}}\},\{\mathbf{O_{12}}\},\{\mathbf{O_{13}}\}\},\{\{\mathbf{O_{21}}\},\{\mathbf{O_{22}}\},\{\mathbf{O_{23}}\}\}\} =$$
$$= \{\{\{O_{111},O_{112},..,O_{11J_{11}}\},\{O_{121},O_{122},..,O_{12J_{12}}\},\{O_{131},O_{132},..,O_{1P_1J_{13}}\}\},$$
$$\{\{O_{211},O_{212},..,O_{21J_{21}}\},\{O_{221},O_{222},..,O_{22J_{22}}\},..,\{O_{231},O_{232},..,O_{23J_{23}}\}\}\}$$

where $\mathbf{O_1}$ is a subset of the objects of the IPC group, which includes subsets $\mathbf{O_{11}} \subseteq \mathbf{O_1}, \mathbf{O_{12}} \subseteq \mathbf{O_1}, \mathbf{O_{13}} \subseteq \mathbf{O_1}$. Referring to such subgroups of objects as political decision-making systems, public opinion formation systems, and public consciousness formation systems. Then, for example, O_{111} is a parliament, O_{112} is a president, O_{121} is a union of aviation workers, O_{122} is a public firearm owners` association, O_{131} is an editorial office of a newspaper, O_{132} is an owner of the TV channel, etc. (the subset is finite, but now we do not aim to fully define it);

$\mathbf{O_2}$ is a subset of the ITC group objects, which includes the subsets $\mathbf{O_{21}} \subseteq \mathbf{O_2}, \mathbf{O_{22}} \subseteq \mathbf{O_2}, \mathbf{O_{23}} \subseteq \mathbf{O_2}$ indicating such subgroups of objects as data transmission systems, information security systems, and electronic warfare systems. Then, for example, O_{211} is ATS, O_{222} is a government communication system, O_{221} is ACS, O_{222} is an antivirus computer system, O_{331} is a radar, O_{132} is a radio suppression system, etc. (a subset is finite, but now we do not aim to fully define it).

Finally, for example, under the conditions when $K = 3$ and given an unlimited number of information impacts within one category, expression (3) will define a set of information impacts $\mathbf{I}$ as follows:

$$\mathbf{I} = \{\bigcup_{\mathbf{k=1}}^{\mathbf{3}} \mathbf{I_k}\} = \{\bigcup_{k=1}^{3}\bigcup_{n=1}^{N_k} I_{kn}\} = \{\{\mathbf{I_1}\},\{\mathbf{I_2}\},\{\mathbf{I_3}\}\} =\{\{I_{11},I_{12},..,I_{1I_1}\},\{I_{21},I_{22},..,I_{2I_2}\},..,\{I_{31},I_{32},..,I_{3I_3}\}\}$$

where $\mathbf{I_1}$ is a subset of information impacts of the IPC category, for example, I_{11} is hypnosis, I_{12} is psychodysleptics (hallucinogens), etc. (this and the following subsets are finite, but now we do not aim at its full definition);

$\mathbf{I_2}$ is a subset of information impacts of the ITC category, for example, I_{21} is computer viruses, I_{22} is a violation of the established routing order, etc.

$\mathbf{I_3}$ a subset of information impacts of the II category, such as misinformation, propaganda, etc.

The channel via which information and psychological impact is exercised at this stage of the research is not important to us, so we will not define it yet.

Table 4. The state of information confrontation

Subjects	Activity	Impact	Chanel	Object	State of the object before impact	State of the object after impact	Level
Intelligence service	Active	Propaganda	Social networks	Union of aviation workers	normal state	state of getting impaired	S, P
Intelligence service	Pasive	Hypnosis	Comntact	Presiden	normal state	normal state	S, I
…	…	…	…	…	…	…	…
Terrorist group	Active	Rocket attack	Physic	Radar	normal state	state of death	P, S

So, we have mathematically described the main elements of the information confrontation process within an ontological model and we can represent it in the form of an ontological model framework.

The framework of the ontological model in general is presented in Figure 4 and table 4.

The information space of each interacting party consists of objects and subjects that are interconnected by different formal and informal connections represented by dotted lines. It (model) reflects the information impact of 3 levels: state, public, and individual. The figure shows the three parties to the interaction and their subjects and objects, although, as noted above, IC is a multilateral process (i.e., the total number of parties may be more than two and in fact is unlimited). Each of the parties can be in an active and passive state, and attacking actions can be carried out against both one and many parties. The model is open. Its flexibility allows us to expand the database of the main model components, to change the number of existing elements and add new categories, levels, states of subjects and objects. Counterparts interact through open environment or special channels. Connecting lines reflect the influence of IC subjects through information channels, and line color determines the IC level. As can be seen from the model, the influence of subjects can be exerted on objects and subjects of other levels.

5. Conclusions and Prospects for Further Research

Having analyzed modern information confrontation models and concepts, the article identifies the fundamental principles of the IC ontological model construction and the main elements of the information confrontation process: subjects, objects, information impacts. The states, levels and groups of these elements are described as well as the peculiarities of their interaction with each other.

The framework of the information confrontation ontological model has been developed, which makes it possible to illustrate the process of information confrontation, to formalize and further model it, as well as to describe the IC process itself with a multi-component tuple. The advantage of the proposed model is its relative simplicity, moderately low resource consumption, the description of all IC elements, adaptability, expansibility and scalability.

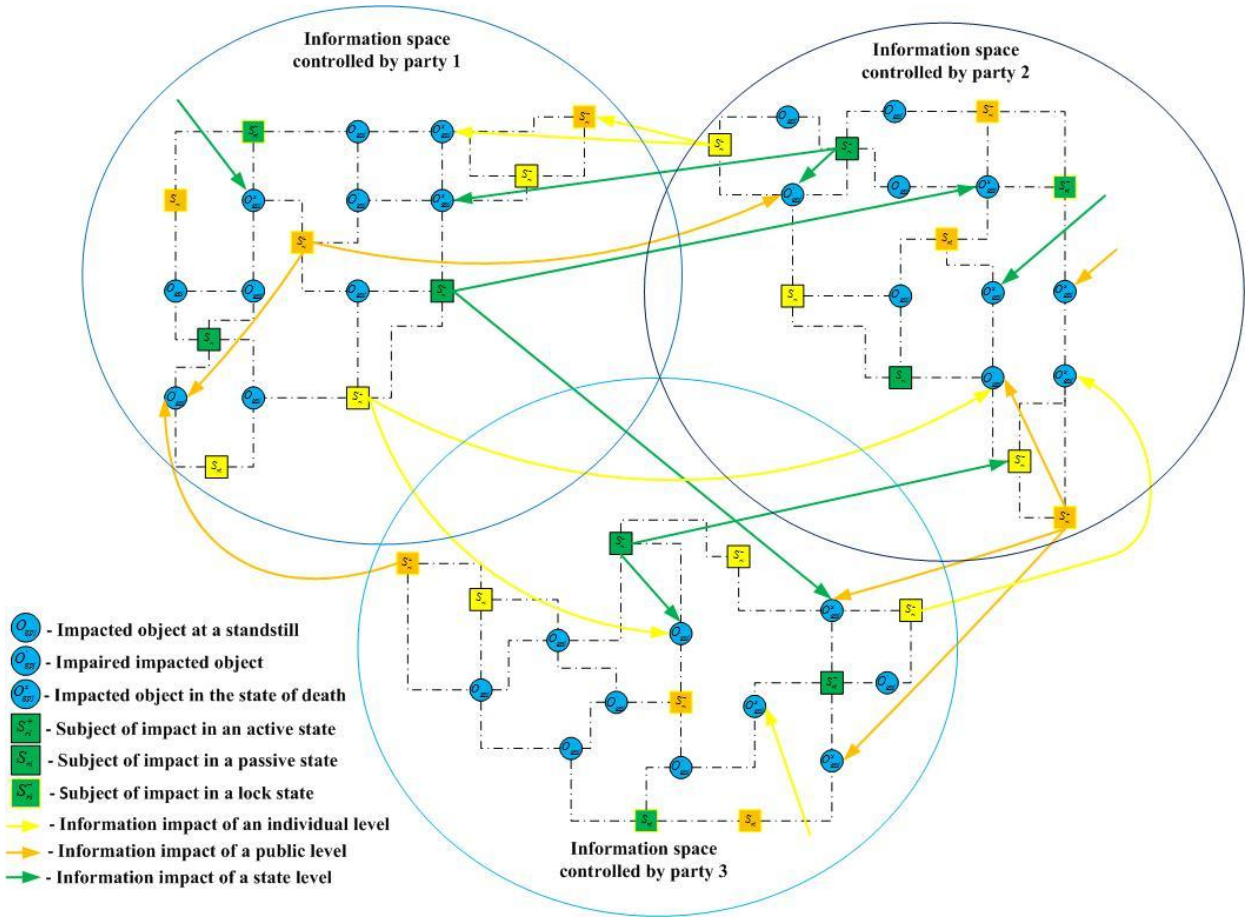

Fig.4. The framework of the ontological model

The proposed model, unlike the existing ones (see Table 1), fully meets the criteria of formalization completeness. Its compliance with these criteria is shown in table 5.

Table 5 uses the following reference designations:

- The mathematical model underlying the conception;
- Functionality to reflect subjects and objects;
- Functionality to show connections (impact process);
- Functionality to show levels;

+ - Enabling the formalization and description of the model element to the full extent;
- Not applicable for the formalization and description of the model element;
+/- - partially enables the formalization and description of the model element.

Table 5. Compliance of the proposed model with the requirements of the IC process formalization

Name	Developers	1	2	3	4
Proposed Model	A. Hizun, V. Hriha, K. Zanizdra	Functional-descriptive, mathematical analysis, structural-algorithmic modeling, graph theory	+	+	+

The obtained results can be used to develop situation centers for simulating the course of negative information impacts in the context of information warfare with the aim of researching them, enhancing the state, society and citizens` information security as well as the state of readiness for hostilities in the info- and cyberspace. The developed ontological model can be used to build systems for detecting, identifying and assessing information and psychological influence. We also see the application of the model in the development and modeling of tactics of both information attack and defense. The model can be used by private intelligence agencies, government institutions, competitive intelligence companies, and, with adaptation, marketing agencies.

Further research studies will describe in detail subjects and objects, their states and conditions for the transition from one state to another presented as a Markov process, their internal structure and the relationships between them as they form an interconnected system with a dynamic structure that can change under the influence of the hostile party. Markov processes allow modeling the sequence of information influences as a system with states, where the probability of transition depends only on the current state. This is especially useful for analyzing audience behavior in information confrontation, when there is a dynamic change of views. They are used to predict the consequences of information attacks, identify vulnerabilities in communication systems and optimize appropriate countermeasures. This approach contributes to real-time decision-making based on statistical information processing. The description of this dynamic system (by its nature, it is the IC party) will also be given in one of the following articles.

Accordingly, in the future we plan to develop an expert system for managing information-psychological influence. We assume that it will dynamically detect, identify and evaluate specific types of information attacks, as well as help counteract them. A software complex will be built on this basis. Using artificial intelligence technologies, we want to achieve operational management of information-psychological influence in a large information segment.

References

[1] S.N. Hriniaiev, RAND Corporation Experts on an Information Strategy. http://attend.to/commi
[2] Terms and definitions. http://lektsii.com/2-119431.html.
[3] Ye.D. Skulysh, History of information and psychological confrontation: textbook. *Scientific-ed. Department of National Academy of the Security Service of Ukraine*, 2012, 212 p.
[4] A.V. Dudatiev, Information Security of Sociotechnical Systems in the Conditions of Information War, *Information Technology and Computer Engineering*.3 (22), 2011, pp. 75-79.
[5] V.A. Lipkan, Yu.Ye. Maksymenko and V.M. Zhelikhovskyi, Information Security of Ukraine in the Conditions of European Integration. *KNT*, 2006, 280 p.
[6] M.M. Prysiazhniuk, I.V. Pampukha and V.M. Petryk, Basic concepts and features of conducting special information operations, http://nbuv.gov.ua/UJRN/Znpviknu_2014_46_19
[7] Information-analytical activity. http://megalib.com/content/2014_51_Ponyattya_i_sytnist_informaciinih_viin.html
[8] Ye.A. Makarenko, M.M. Ryzhkov, M.A. Ozhevan, International Information Security: Contemporary Challenges and Threats. *Tsentr vilnoi presy*, 2006, 916 p.
[9] International information security as an actual problem of modern times. https://naub.oa.edu.ua/2010/mizhnarodna-informatsijna-bezpeka-yak-aktualna-problema-suchasnosti/
[10] R.V. Hryshchuk, I.O. Kankin & V.V. Okhrimchuk, Technological Aspects of Information Confrontation at the Current Stage. *Protection of Information*. 17(1), 2015, pp. 80-86.
[11] A.V. Manoilo, Objects and subjects of information confrontation. http://www.cryptography.ru/
[12] V.V. Tsyganov, S.N. Bukharin, V.V. Vasin, Intellectual mechanisms of information warfare. *Problems of management*. part 1. pp. 25-30.
[13] A.V. Dudatiev, Complex Information Security of Sociotechnical Systems: Impact and Protection Models. *VNTU*, 2017, 128 p.
[14] A.I. Gizun, V.S. Hriha, Analysis of modern information and psychological impact theories in terms of information confrontation. *Security of information*. 22(3), 2016, pp. 272-282.
[15] CEPA. http://infowar.cepa.org/
[16] L. Cox, Planning for psychological operations: a proposal..*Air Command and Staff College, Maxwell Air Force Base*, 1997, 89 p.

[17] V.L. Buriachok, Possibility of security assurance against information-psychological influence based on the universal ontology method. *Modern information security* №4, 2013, pp. 57-67.
[18] L.S. Johnson, Toward a Functional Model of Information Warfare. *Center for the Study of Intelligence, 1997,* 8 p.
[19] R.W. Pew, Modeling Human and Organizational Behavior: Application to Military Simulations. *National Academy Press*, 1998, 418 p.
[20] J. Jormakka, Modelling Information Warfare as a Game. *Journal of Information Warfare*. 4(12), 2005, 25 p.
[21] B. Hutchinson, Information Warfare: Using the Viable System Model as a framework to attack organizations. *Australasian Journal of Information Systems*. 9(2). 2002. pp. 1-10.
[22] B. Van Niekerk, The Information Warfare Life Cycle Model. *SA Journal of Information Management.* 13, 2011, pp. 1-9.
[23] V. Ostroukhov, To the problem of Ukraine`s information security assurance. *National security, political management*, №4, 2008, pp. 135-141.
[24] T.M. Dziuba, The state`s information security in the military sphere: scientific method. edition *NUOU, 2012,* 264 p.
[25] A. Gizun, V. Hriha, M. Roshchuk, Y. Yevchenko and Z. Hu, Method of informational and psychological influence evaluation in social networks based on fuzzy logic. *CEUR Workshop Proceedings*, 2019, http://ceur-ws.org/Vol-2392/paper1.pdf.
[26] B. Zahran, J. AL-Azzeh, A. Gizun, V. Hriha and B. Bystrova, Developing an expert system for assessment of information psychological influence, *Indonesian Journal of Electrical Engineering and Computer Science,* 15(3), 2019, pp. 1571-1577.
[27] M.P. Karpinskyi, A.O. Korchenko and A.I. Gizun, An integrated model for crisis presentation and a formalized procedure for building standards for identifying parameters.*Legal, regulatory and metrological support for the information security system in Ukraine*, №1 (29), 2015, pp. 76-85.

Authors' Profiles

Andrii Gizun: PhD (Engineering, Cybersecurity), Associated Professor, an Associated Professor of the Department of Software Engineering, National Aviation University, Ukraine. Areas of scientific interests: information security, information security incident management, artificial immune systems, information and psychological security, psychological operations, information war.

Vladyslav Hriha: PhD (Computer Science), an Associated Professor of the Department of Software Engineering, National Aviation University, Ukraine. Areas of scientific interests: information security, information and psychological security, psychological operations, information war.

Ruslana Ziubina: PhD (Engineering, Cybersecurity), an Associated Professor of the Department of Computer Science and Automatics, University of Bielsko-Biala, Poland. Areas of scientific interests: information security, information security incident management, network intrusion detection.

How to cite this paper: Andrii Gizun, Vladyslav Hriha, Ruslana Ziubina, "Fundamental Principles of the Information Confrontation Ontological Model Construction", International Journal of Computer Network and Information Security(IJCNIS), Vol.17, No.5, pp.1-14, 2025. DOI:10.5815/ijcnis.2025.05.01