

Russian Information-psychological Special Operations in Ukraine and Peculiarities of System Design for Their Countermeasures

Oleksandr Markovets, Mykola Buchyn, Anastasiia Kovalchuk and Taras Basyuk

Lviv Polytechnic National University, Bandery Str. 12, 79013 Lviv, Ukraine

Abstract

The article includes the analysis of the peculiarities of the using information technologies by Russian Federation in the context of conducting information-psychological special operations in Ukraine at the present stage. Russian information-psychological operations' in Ukraine essence, peculiarities, aims, subjects, objects and distribution channels are disclosed. The periodization of the transformation stages of Russian information-psychological operations against Ukraine is disclosed. The role of modern media in spreading key messages in the context of conducting information-psychological operations in Ukraine is shown. The design of the system for analyzing posts in social media using an object-oriented approach was carried out.

Keywords

Informational technologies, information-psychological operations, messengers, information warfare, information security, cybersecurity, social media, manipulations, propaganda, Russian Federation, Ukraine.

1. Introduction

The confrontation between states is an integral element of modern international system. Since the emergence of the first political entities its leaders sought to find new effective methods of neutralizing and subjugate opponents. The development of information technologies and increasing role of information in society caused the advent of new techniques of information flows manipulating, which allow changing the object's of influence mind, values and even the model of behavior.

Information-psychological special operations (next – IPOs) were an important part of states' foreign policy yet in the XX century. Over the time the role of IPOs as an instrument of achieving governments' hidden purpose has only been increasing. Information influence was mostly used in the USA and the USSR. After the collapse the Soviet Union became an active subject of conducting information-psychological operations. The state didn't only become the successor of the USSR, but also inherited and developed all the propaganda methods of waging information warfare against its geopolitical opponents.

One of the vivid examples of waging hybrid warfare is Russian information warfare against Ukraine, in the frames of which the government of the Russian Federation systematically exerts influence on Ukrainian political leadership and population. In this context the research of the essence and peculiarities of information-psychological operations conducted by Russia will allow to understand the official Moscow's key goals and objectives in Ukraine as well as highlight information

SCIA-2023: 2nd International Workshop on Social Communication and Information Activity in Digital Humanities, November 9, 2023, Lviv, Ukraine

EMAIL: oleksandr.v.markovets@lpnu.ua (O. Markovets); mykola.a.buchyn@lpnu.ua (M. Buchyn); kv.anasta.ev@gmail.com (A. Kovalchuk); Taras.M.Basyuk@lpnu.ua (T. Basyuk)

ORCID: 0000-0001-8737-5929 (O. Markovets); 0000-0001-9087-5123 (M. Buchyn); 0000-0002-8462-8705 (A. Kovalchuk); 0000-0003-0813-0785 (T. Basyuk)



© 2023 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

methods of its implementations for further development of techniques to counter Russian information aggression.

The purpose of the study – is to carry out a comprehensive analysis of the problem of Russian information and psychological special operations in Ukraine and the features of designing a system for countering them.

Research hypothesis – the Russian Federation is currently actively using information and psychological special operations against Ukraine, which pose a significant threat to national security and require the design of a system to counter them.

The following methods were used during the research: logical: analysis, synthesis, induction, deduction; general scientific: historical - to highlight the evolution of Russia's use of IPOs methods in Ukraine; systemic - for consideration of IPOs as a complete system of forms and methods of information influence; structural and functional - to clarify the structure of the IPOs and the peculiarities of the impact of their individual elements: comparative - to compare the goals and means of the IPOs of the Russian Federation in Ukraine from 2000 to today; modeling – for designing a system to counteract Russia's use of IPOs against Ukraine; empirical: the method of document analysis - to determine the regulatory and legal regulation of information influence in the Russian Federation; qualitative and quantitative content analysis - to identify the key messages of Russian propaganda and disinformation at the current stage.

The work includes an introduction, analysis of the source base, the main part, which includes 4 subsections and highlights the main results of the research, conclusions, a list of used literature.

2. Related Works

Despite the novelty, information-psychological special operations became the object of research for many scientists, experts and specialists in the field of information technologies. Taking into account the applied nature and the modernity of the described events, the source base of our research includes both scientific publications and analytical materials or news, which reveal certain facts about the use of information-psychological special operations by the Russian Federation.

Literature on the topic of the research can be divided into two groups. The first concerns the disclosure of general concepts, related to information-psychological operations or related categories. Thus group includes the researches of information-psychological special operations as one of the modern instruments of geopolitical confrontation [1]; information-psychological struggle and its peculiarities [2]; theoretical approaches to defining information-psychological special operations [3]; information-psychological influence, its exerting and methods of counteracting [4]; analysis and implementation of information-psychological operations in the context of waging hybrid warfare [5]; information-psychological special operations as a challenge to states' security and protection [6]; psychological operations, its techniques, tactics and procedures of realization [7], [8], [9], [10].

This group of sources should also include research on the specifics of information-psychological special operations and mechanisms of countering informational and psychological influence. In this context, it is worth mentioning the works devoted to the issue of information security in the frames of waging a hybrid war and the role of journalism in it [11]; research on information resistance as a mean of countering socio-psychological strategies of information warfare [12]; analysis of the information war on a global scale and its cognitive effects [13]; research of the mechanisms of countering fake information, which is the key to ensuring the information security of any state [14]; research of information as a modern geopolitical weapon [15]; analysis of behavior in social networks and manipulation of public opinion [16], etc.

Considering the fact, that the information-psychological special operations are most widely and effectively used to correct the results of the will of citizens during elections, a number of literary sources refer to the analysis of the impact of information-psychological special operations on the election process and democracy, and especially in the context of the security threats during the use of electronic voting [17], [18].

Another group of literary sources refer to the practice of information-psychological operations conducted by the Russian Federation. On the one side, this group includes the literature, which generally characterize the Russian Federation as the subject of information-psychological special

operations at the present [19], [20], [21]; reveals the anatomy of Russian disinformation [22]; examines Russian Internet policy as network authoritarianism and the mechanism of using information as a geopolitical tool [23]; reveals Russia's information war against the West through the Russian government's use of hacking, propaganda and election manipulation [24]. On the other side, this group also consists of researches of peculiarities of conducting information-psychological special operations against Ukraine. In particular, it goes about the general analysis of Russian information campaigns against Ukraine [25]; research of the reasons of an aggressive behavior and the full-scale invasion on the territory of Ukraine on the 24th of February 2022 [26]; disclosure of the features of disinformation in the media space during the war in Ukraine, aimed at forming the opinion that the culprit of Russia's invasion of Ukraine is the USA, NATO and Ukrainian society [27]; field studies of disinformation during the Russian-Ukrainian war through the prism of the perception and opinion of the Ukrainian population regarding the manipulation of information [28], etc.

The basis of the source base of the research are the works of Ukrainian and foreign researches, analytical reports of NATO, field manuals of the Armed Forces of the USA, legislation of the Russian Federation as well as publications of the online newspapers. At the same time, despite considerable attention to the problem of the information and psychological influence of the Russian Federation in foreign countries, the studying of the Russian IPO in Ukraine from the 2000s to now remains fragmented, and therefore requires deeper and more careful analysis.

3. Results and Discussion

3.1. Concepts and types of information-psychological operations

Information- psychological special operations is one of the examples of selective and purposeful use of information flows in order to influence the target audience. It should be mentioned, that in foreign sources (mostly English-language) the separate forms and abbreviations of the concept are used: «PSYOPS» - psychological operations and «IO» - information operations, as well as «IPO» - information-psychological operation.

The evolution of the means of information and psychological influence as well as differences in its exerting in different states caused the emergence of various approaches to definition of the concept “information-psychological special operations”. The origin of the term is associated with the creation of the propaganda division led by the military intelligence of the American Expeditionary Force in 1918, and its first used – with the surrender messages sent to the Japanese mainland in 1945. The term remained generic for decades, despite the fact its components were actively used by the countries of the world [7].

The official definition of “psychological operations” was firstly established in the field manual of the Armed Forces of the USA in 1979. It was mentioned, that the psychological operation encompasses political, military, economic and ideological actions, which are planned and conducted with the aim of creating in neutral, friendly and hostile foreign groups emotions, attitudes or behavior, favorable for the achievement of national goals [10].

One of the modern definitions, suggested by Ukrainian researchers V. Zhadko and Y. Kharytonenko explains IPOs as the planned use of technologies and means of spreading information for influencing the people’s mind in a broad sense; and as an instrument of influence, which is practically used during combat operations with the aim to demoralize opponent – in narrow sense [4]. According to the statements of Russian scientists A. Manoilo, A. Petrenko, D. Frolov, V. Veprintsev IPOs – the complex of measures to manipulate the information flows in order to achieve advantage over the enemy. Ukrainian researcher H. Pocheptsov explains such operations as communicative technologies, which change the behavior and the mind of people by influencing psychological state of the target audience [3].

Table 1.
Main definitions and the goals of IPOs

Definition of IPOs	Goal of the IPOs
Political, military, economic, ideological actions	Creation of emotions, attitudes or behavior,

Planned use of technologies and means of spreading information	which is favorable for the achievement of national goals
Instrument of influence during combat operations	Influencing the people's mind
Complex of measures of the information flows manipulations	Demoralization of the opponents
Communicative technologies	Achievement the advantage over the enemy
	Change of the people's behavior by influencing the target audience's psychological state

One more definition was suggested by NATO and the US Ministry of Defense. It separates the concepts “psychological” (PSYOP) and “information” (IO) operations. IO is explained as integral use of information possibilities during combat operations in order to influence, obstruct, corrupt and usurp decision-making of actual and potential adversaries with the simultaneous protection of the domestic one. IO is first of all military activities in information space, which has exactly defined goals, and also includes offensive and defensive measures aimed at influencing the opponents decisions and manipulating information and information systems. Instead psychological operations are the pre-planned activities, which involve the use of communication methods and the other resources on the target audience to influence their attitude, behavior, perception and interpretation of the reality. It is emphasized that PSO is build on a certain psychological theme (a prepared narrative or idea), and the greater the sensitivity of the target audience to the topic or tool of PSYOP, the greater the probability of success of the operation. In accordance to the mentioned above, PSYOPs are conducted in peacetime, and IO – during military operations [6].

Table 2.

The difference between information and psychological operations

Criteria	Information operations	Psychological operations
The essence of the concept	Integral use of information technologies	Pre-planned activity, which includes application of communicative methods
Goal	Influence, obstruction, corrupting, usurping the decision-making with the simultaneous protection of the domestic one.	Influence on the target audience's attitudes, behavior, perception and interpretation of the reality.
Methods of the use	Manipulation of information	Preparation and spreading the narratives and ideas
Context of application	During military operations	Peacetime

In our opinion, information-psychological special operations should be understood as the complex of particular actions, which has relevant information spreading and interpretation, involves manipulation, misrepresentation, and aims to shape the object's certain emotional and psychological state and reactions, needed by the subject.

It should be mentioned, the term IPOs is often used in the context together with the concept “information warfare”, which unlike IPOs is more strategic in nature. Thus, it can be argued that information warfare is a complex of information and psychological special operations.

Modern researchers distinguish offensive and defensive IPOs (although a significant part of such operations is mixed). By the goals and orientation, the operations aimed at making the decisions required by the customer, obtaining or demonstrating compromising material, disrupting the political system and/or society, as well as destabilizing the opponent are also identified. Short-term (up to 2 weeks), medium-term (up to a month) and long-term (more than 4 weeks) are distinguished by the criterion of duration [11].

In the Allied Doctrine on Psychological Operations, developed by NATO, the following categories of IPOs are defined: strategic (planned operations to gain support and strengthen cooperation with friendly and neutral audiences as well as weaken the capabilities and desire of enemy audiences to carry out aggressive actions); crisis (operations, which are the part of the settlement of crisis situations and are conducted to create a favorable atmosphere and desire for cooperation between the parties to the conflict and the civilian population); military (as part of combat operations against a defined target audience in order to defeat the enemy or eliminate his desire to continue aggression) [8].

Table 3.
Main types of IPOs

Criteria	Types of IPOs
Focus on the object	Defensive Offensive Mixed
Goals and orientation	Aimed at making the decisions needed by the object Aimed at obtaining or demonstrating compromising material
Duration	Aimed at destabilization of the opponent Short-term (up to 2 weeks) Medium-term (up to 1 month) Long-term (more than 1 month)
Context and purpose	Strategic Crisis Military

3.2. Goals, methods and forms of conducting information-psychological special operations

According to the statements of V. Horbulin, the main goal of IPOs is the manipulation of the target audience's consciousness. And the tasks can be the following: changing or fixing in the people's consciousness particular views and ideas, misinforming and intimidating the population, as well as weakening the existing beliefs, which form the basis of society. Another scientist V. Petryk distinguishes such goals as: inducement to make decision beneficial to the initiator, obtaining compromising material for its further use and destabilization of the social/political/economic order [4].

Considering the fact, that IPOs are conducted in both peace- and wartime, the following distribution of operation tasks can be made. *In peacetime*: destabilization of socio-political situation in the country; demoralization of the civilian population and the military; creating and aggravating contradiction between political forces, creating prerequisites for a social explosion. *In wartime*: undermining the psychological and morale of the opponent's army; creation and exacerbation of contradictions between the military, society and political forces; supporting the opposition and inciting it to confront the authorities [5].

Based on the analyzed approaches to defining IPOs, the following goals of the information-psychological special operations can be distinguished (see Figure 1).

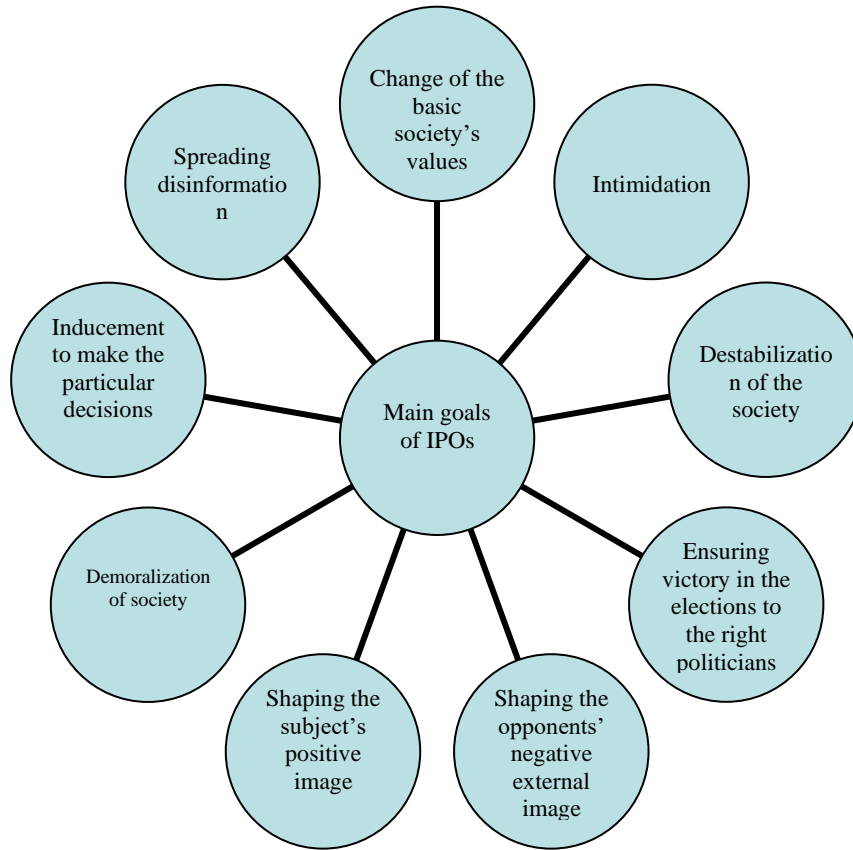


Figure 1: The main goals of IPOs

The subjects of IPOs are the people and sources, which are directly engaged in exerting information and psychological influence, in particular: political authorities and state special services, media, non-governmental organizations, Internet-platform etc. [1].

The objects of IPOs (or the target audience) are the people or groups of people, whom the specified influence is directed to. According to the US Field Statute “Psychological Operations, Tactics, Techniques and Procedures”, published in 2003 there exist several types of the objects of influence (see Table 4) [9].

Table 4.

Main objects of IPOs

Objects of IPOs	Characteristics of the objects of IPOs
Primary groups	Small social groups, families and companies
Secondary groups	Political or governmental structures, organizations and associations
Categories	Large groups of people who share certain demographic characteristics
Aggregates	A group of people identified only by a common geographic area
Centers of gravity	Individuals or small groups who may have significant power over others
Key communicators	Persons to whom members of the target audience address for the information or its interpretation

The choice of the target audience varies depending on the type and purpose of the IPOs. In general, the targets of IPOs are: military personnel (both authorities and soldiers), political leaders and representatives of governmental structures, civilians, religious, ethnic and cultural groups, business representatives, mass media, academic groups, public activists and non-governmental organizations. The subjects of IPOs can influence both the audience in a foreign state and their own.

The effectiveness of IPOs mostly depends on the right choice of channels for the distribution of the narratives needed for the subjects. Among the main channels of spreading information for the IPOs are the following (see Figure 2) [5]:

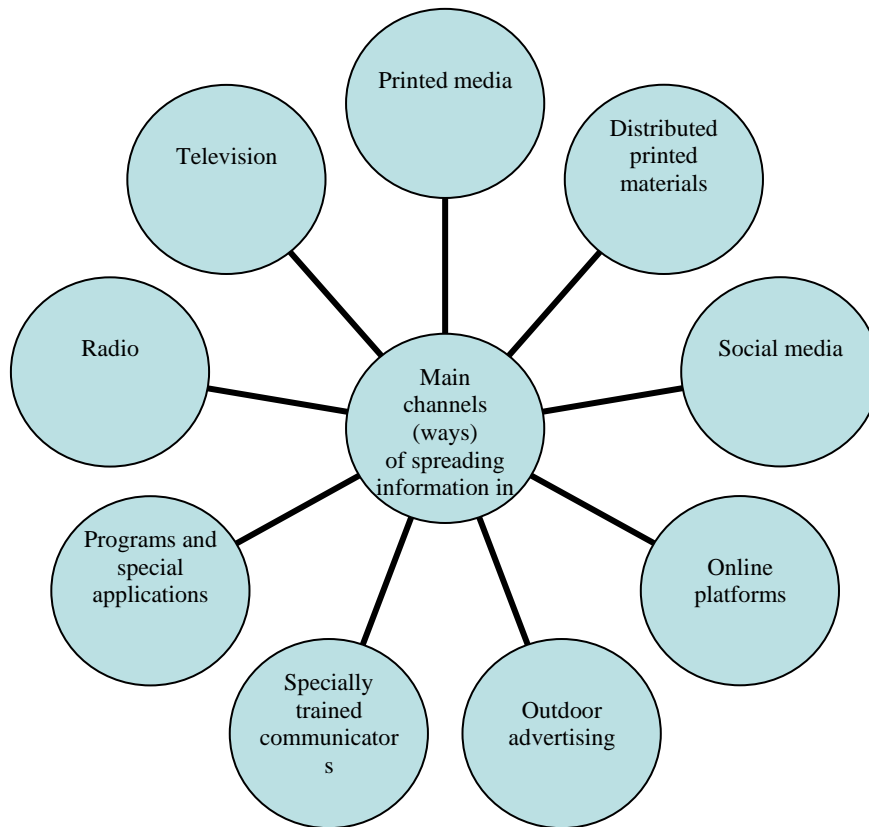


Figure 2: Main channels (ways) of spreading information in IPOs

Through these channels such methods of IPOs as *disinformation*, *propaganda*, *psychological pressure*, *spread of rumors*, *diversification of public opinion* are applied [4]. Each of the mentioned IPOs methods has its own characteristics and specific forms of practical application (see Table 5).

Table 5.

Methods of IPOs application

Methods of IPOs	Peculiarities	Forms of application
Disinformation	Deliberate dissemination of false information in order to hide the truth or to influence public opinion to induce the object to take certain actions.	Tendentious distortion of facts; Disinformation “from the reverse” ; Terminological “mining”; “Grey” disinformation; “Black” disinformation.
Propaganda	Dissemination of ideas for their consolidation in public opinion, as well as the practical application of these ideas in the	Simplification; Silencing; Displacement of fact.

Diversification of public opinion	mass activities of people. Purposeful distraction of the political authorities' attention of the state (by artificially drawing attention to a certain range of problems), which prevent it from concentrating on solving urgent and important issues for the state and society.	Destabilization of the country or region; Intensification of opposition movements; Publicity of scandalous court proceedings; Introduction of sanctions, etc.
Psychological pressure	Intimidation of the object and influence on his psyche forcing him to act accordingly to a certain pattern of behavior.	Dissemination of information about existing or false threats; Blackmailing Committing acts of terrorism and mass massacres; Taking hostages, etc.;
Spread of rumors	Dissemination of information (mostly disinformation) among the masses through unofficial channels to complicate the object's activities.	Dissemination of information to demoralize; Dissemination of information to intimidate; Dissemination of information to disintegrate

IPOs are often conducted during elections and are used as one of the forms of foreign interference in the election process. It can be explained by the important role, the elections play in the development of a democratic society, being the main attribute, indicator and catalyst of democracy [29]. On the other hand, the results of elections define the strategic direction of each state's development. Thus, external influence on the election process and its results allows the aggressor to achieve its global goals by conducting IPOs. It is especially common in terms of using information-communicative technologies and electronic voting in particular, which must be reliably protected from foreign information influence [17], [18].

Fighting IPOs is an important issue for each state. However, the difficulty of countering IPOs is in the actual absence of the possibility of prosecuting the object of informational-psychological operations as the characteristic features of information-psychological influence are its latency and the absence of direct proves of aggression, with the simultaneous infliction of significant damage to the target object without declaring war or terminating diplomatic relations. Another difficulty is an identification of the primary sources of influence and determining the true intentions, means and methods of the subjects' actions [5].

Legal regulation of the information sphere as a mechanism for countering IPOs is also difficult. This can be explained, in particular, by the low efficiency of such a mechanism. In addition, the high level of legal regulation of the information sphere has a negative impact on the level of democracy and freedom of speech, limiting, in this way, the possibilities for countering IPOs in democratic countries.

The implementation of countermeasures against informational and psychological influence at the state level can be carried out by the implementation of counteroperations aimed at the opponents or the implementation by specially developed state security policy. The negative impact can be neutralized by conducting information-explanatory campaigns for the population, using all available channels of information dissemination; delivering truthful information to citizens and the international community about the actions of country's political leaders and its military structures; monitoring the information space and immediate responding to the identified active and potential subjects of influence; the unification of society around national values and the integration of citizens for the joint fight against external threats; forming positive image of the state and its political authorities, etc. [4].

However, some of the most effective and universal mechanisms for counteracting informational and psychological influence are a high level of consciousness and culture of citizens, a high level of

awareness and intelligence of individuals, in particular, their information literacy, a high level of critical thinking. These make individuals significantly less vulnerable to IPSO, minimize the effectiveness of informational and psychological influence

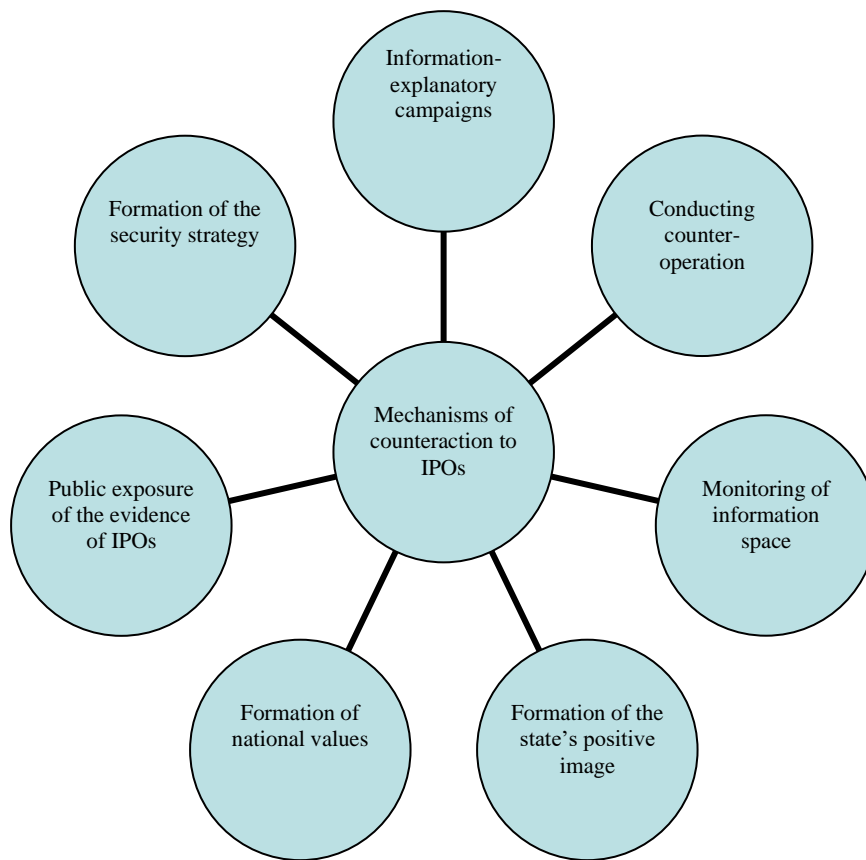


Figure 3: Mechanisms of counteraction to IPOs

3.3. The peculiarities of Russian information-psychological special operations in Ukraine

After the collapse of the USSR, despite the factual end of the confrontation between the Soviet Union and the USA, the competition in information sphere was increasing. At the times of B. Yeltsyn’s presidency several strategic documents were published, in which it was mentioned, that information and psychological operations became an integral element of the national security strategy.

The new era of understanding the advantages of waging “information wars” started with the coming to power in Russia of V. Putin in early 2000s. In the following years, a number of strategic security documents, which highlighted the presence of information threats to Russia from other states, seeking to dominate in the global information space in influence the government and the population was noted. These documents also declared the need for countering the other states’ use of technologies to achieve aggressive military and political goals as well as the key role of information activities in Russian security strategy.

The main reason for Russia's active use of IPOs at the current stage lies in the geopolitical interests and imperial ambitions of the current Russian political elite. The effort to be one of the poles of influence and to increase its dominance on the planet is realized, including, due to the spread of informational and psychological influence both on its own audience and on the population of other countries of the world.

Since the restoration of Ukrainian independence, the country has also been informationally influenced by the Russian Federation. Having studied the peculiarities of Russian IPOs in Ukraine (including conducting content-analysis of Russian media), we consider it appropriate to define 4 main periods: 2000-2007; 2008-2013; 2014-2021; from 2022 – till now.

The beginning of the mentioned periodization from 2000, and not from 1991 (the period of the collapse of the USSR), in our opinion, can be explained by the fact that during the presidency of B. Yeltsin, the Russian political elite paid less attention to foreign policy interests due to the numerous internal political problems. However, with V. Putin coming to power in Russia in 2000, imperial foreign policy ambitions began to dominate. This led to the active use of IPOs. Therefore, the period from 1991 to 2000, in the context of the issues we are investigating, can be considered a preparatory stage for Russia's future use of IPOs in general, and against Ukraine, in particular.

2000-2007 years can be characterized as the stage of conceptual understanding and strategic planning of the Russian further actions. V. Putin set the goal of “restoring the former great power”. Since the early XX century the Russian Federation has been introducing hard “vertical” power and making long-term investments in controlled media and non-governmental organizations, which could be used as the instruments of soft power. In 2000s a significant part of Ukrainian heads of media holdings had close ties with the Russian Federation. For example, New Channel and STB were owned by the Russian Alfa Group and Lukoil, and in 2006 the UA. Inter Media Group Limited company was sold to the Russian billionaire A. Abramov. In 2000-2005 the director of the ICTV Channel's information service was Russian journalist D. Kiselyov, who was the host of political talk-show “National Interest” at the same time. A significant part of the TV programs and films broadcast by Ukrainian channels was created together with Russian media groups or even borrowed: for a certain time the Inter Channel aired the new programs of the First Channel, and Ukrainian TET was filled with the content of Russian STS. Print mass media wasn't left out the attention of the Russian Federation: such newspapers as “Kommersant”, “Arguments and Facts”, “Komsomolsk Truth” were actively published in Ukraine [2].

During 2004-2007 years in the rhetoric of the Russian political elite, theses, saying that Ukraine and Russian are parts of the same Orthodox civilization appear. Numerous public organizations, including: Russian Movement of Ukraine, Russian Movement of the Crimes, Slavic Committee of Ukraine, Russian Community, Ukrainian branch of the Institute of CIS Countries as well as International Eurasian Movement (headed by A. Dugin) promoted such ideas. The aims of these organizations were to impose pro-Russian views, spread dissatisfaction with Ukrainian policies among Russian-speaking population, form a negative attitude of Ukrainians towards the integration into the EU and NATO, conduct public actions and create the Russian image as the guarantor of the protection of the Russian-speaking population, etc.

The ideas of historic, cultural and religious unity of Ukraine and Russia were supported by the representatives of the Russian Orthodox Church, the Ukrainian Orthodox Church of the Moscow Patriarchate, “Black Hundred”, “United Fatherland”, the “Union of Orthodox Peoples”, etc. The latter's members actively spread the information, discrediting Ukraine in the Internet and participated in mass protests [2].

The coverage of the event of the Orange Revolution of 2004-2005 by the Russian media deserves special attention. In October-December 2004, print and online publications accused the USA of financing actions on the Independence Square and “interfering in the country's foreign affairs”. In addition, it was noted that the revolution was organized by Western supporters of V. Yushchenko and did not reflect the interest of Russian-speaking part of the population [30].

Until 2008-2009 it was possible to notice only some of the elements of Russian IPOs, which were mostly aimed at maintaining the citizens' loyalty to the Russian Federation, and so-called “reflexive control” over the Ukrainian political elite, conducted by economic blackmailing (the Russian-Ukrainian gas conflicts can be considered a vivid example of it).

The intensification of Ukraine-EU interaction during the presidency of V. Yushchenko also contributed to the increase in tension between the parties. In 2008 the Russian media criticized Ukraine, claiming that “there is no basic order” there, and “the country's acceptance into NATO and the EU will mean the destabilization of the entire West”. Russian mass media began to broadcast narratives about the destructiveness of European values and the threat of potential economic collapse

in Ukraine after the signing of the Association Agreement, simultaneously raising the issue of the status of Russian language [25].

Similar thesis actively circulated in the Ukrainian information space during the presidency term of V. Yanukoych in 2010-2013. In the articles of Russian edition “Arguments and Facts in Ukraine” there were phrases that “the integration of Ukraine into the EU will have serious negative impact on the relations between Ukraine and Russia”, “Kyiv’s desire to “sit on two chairs” is vile”, “after signing the Agreement, Ukraine will lose the right to vote and decide what laws to adopt, what tariffs to set and how to interact with other unions – everything will be decided by the European Commission”, “Russian-speaking population will not only suffer from great economic problems, but also will become a victim of assimilation – a large piece is being separated from our common civilizational space”, “in case of Ukraine’s accession to the EU, the Customs Union will take protective measure, which will increase the deficit of Kyiv’s balance of payments to 15-16 billion dollars. In 6 months, the state will become a bankrupt”. In 2012-2013 so-called “Internet-trolls” were added to the list of means of Russian information influence, acting to create a positive coverage of Russian government’s activities and suppress the opposition and discredit Western countries [19].

The new era of Russian IPOs started in the beginning of 2014. Taking advantage of the moment of internal tension in the country, Russian incited the population of the Crimea to revolt against the “Kyiv regime” and lobbied for its interests in the governmental structures of the autonomous republic. Since mid-January 2014, with the support of the Russian community of Crimea and the political party “Russian Unity” self-defense units were formed on the territory of the peninsula as a force of popular resistance. These units were financed by Russian political structures and supposed to oppose the “banderians” and advocate the creation of Ruthenia in case of a coup d’état. On February 20, 2014 the operation to seize Crimea by the “little green men” began and was actually completed by March 1st. On the same day the self-proclaimed Head of the Council of Ministers of Crimea S. Aksyonov appealed to the President of the Russian Federation with a request to contribute to the establishment of “peace and tranquility”, and the Parliament of Russia adopted a decision on sending troops to the territory of Ukraine. According to the version of Russian media, the seizure of administrative buildings was carried out by “groups of people without identification marks” and the protests took place between the “supporters” and the “opponents” of the new government in Ukraine. What is more important, the latter demanded the extension of the powers of the autonomous republic and the repeal of the law introducing the Ukrainian language as the only state language on its territory [21].

In the frames of its informational operation Russian also limited the access of the Crimean population to Ukrainian media: on March 6, 5th Channel, 1+1, Crima-24 were disconnected. Instead of them Russia broadcast Russia-1. On March 9, all the Ukrainian television stations were switched off. The President of the Russian Federation argued the feasibility of holding referendum and the subsequent accession of Crimea to Russia in the following way: “Crimea has the same right to leave Ukraine as Ukraine had – to leave the USSR”, “the Ukrainian authorities violate the rights of people who speak Russian and Crimean Tatar”, “there is no legitimate executive power in Ukraine as the current government is controlled by nationalists, Russophobes and anti-Semites” [31].

The next period of Russian IPOs followed the beginning of hostilities in the east of Ukraine. The scenario of the events was similar to the one used before in Crimea: Russia created and financed the organizations and people’s militias, which opposed the current Ukrainian government. The absence of identification marks, both in Crimea and in the east of Ukraine, gave Russia the opportunity to defend the thesis, that the hostilities are internal civil conflict in Ukraine. The Russian government spread propaganda accusing Ukrainian forces of shelling peaceful cities in Donbas. Therefore, Russian disinformation channels increased their influence first of all among the population of Lughansk and Donetsks People’s Republics and it continued to accuse the Ukrainian government in aggression. The information campaigns of the Russian Federation were also used against the representatives of the Armed Forces of Ukraine. The soldiers and military authorities received text messages, which encouraged them to surrender, saying Ukrainian government does not need them.

At the same time Russian sought to legitimize its actions in front of international community and domestic audience. Thus, the annexation of Crimea and the proclamation of the so-called Lughansk and Donetsks People’s Republics was positioned by the Russian government as “the right to self-determination of peoples”. The President and the Russian representatives in international

organizations appealed to the provisions of the UN Charter and the Kosovo case, responding to accusation with the thesis, that Western states apply double standards [25].

In addition to militaries, international community and the population of the occupied territories, Russian continued to put pressure on the residents of the rest of Ukrainian territory by launching a cyber war. Since November 2013 (in addition to the active operations of the “bot farms”) Russian hackers have systematically carried out attacks on state institutions, enterprises, energy companies, and even ordinary websites and TV channels to obtain state information, destabilize the work of structures and exert psychological influence on the population [30].

On January 12, 2022 the Russian Federation made a number of demands to NATO. One of them concerned the Alliance’s refusal of expansion and, in particular, the provision of guarantees that Ukraine would not become a member of the organization. NATO’s refusal prompted the Russian Federation to aggressive rhetoric. The state accused the bloc in threatening its national security [31]. In the media, Russia-NATO relations were described in the following way: “The relations between Moscow and the Alliance are at critically low level on the background of terrorist threats, the unfolding of arms race and the complete degradation of the security architecture in Europe... NATO’s repeated disregard of Russian side’s initiatives regarding de-escalation creates the preconditions for the emergence of conflicts and undermines the basics of security”. On February 21, V. Putin recognized the independence of the Lughansk and Donetsk Republics, and in the morning of February 24, 2022 he announced the beginning of a special military operation in Ukraine. The “Special military operation” was justified by the need to protect the residents of the Lughansk and Donetsk Republics from the “genocide by the Kyiv regime” and its goals were defined as “demilitarization” and “denazification” of Ukraine [26].

Table 6.
Historical peculiarities of Russian IPOs in Ukraine

Criteria	2000-2007	2008-2013	2014-2021	2022 – till now
IPOs’ goal	Make Ukraine remain in Russian sphere of influence.	Increase the economic and political influence on Ukraine by its integration into the Customs Union.	Seizure of power and recognition of the DPR and LPR as autonomous republics within Ukraine.	Discredit the image of Ukrainian government, demoralize the society and the military to end the war on the terms of Russia.
IPOs’ tasks	Influence on Ukrainian authorities to strengthen cooperation with Russia; Convictions of citizens in the historical and cultural unity of Ukraine and Russia.	Maintaining influence on political elite; Convincing people, that joining the Customs Union is more positive than integration with the EU; Discrediting Euromaidan participants; .	Forcing Ukraine to recognize the L/DPR and the annexation of Crimea; Discrediting Ukrainian authorities; Aggravation of contradictions in society and destabilization of the political situation; Encouraging regions neighboring the Russian Federation to become autonomous;	Discrediting the image of Ukrainian authorities; Demoralization of Ukrainian military and civilians; Legitimization of Russian actions in Ukraine;
Target audience	Ukrainian political authorities and population; Public activists and cultural	Ukrainian political authorities and population; Public activists and cultural actors;	Ukrainian political authorities and population; Residents of L/DPR and Crimea;	Ukrainian political authorities and population; Ukrainian military personnel;

	actors;		Ukrainian military personnel; International community;	Residents of the occupied territories; International community;
Subjects and channels of influence	Russian authorities; Cultural and religious organizations; Pro-Russian structures in Ukraine; Media (print media, television, radio, Internet); Russian cultural heritage;	Russian authorities; Cultural and religious organizations; Pro-Russian structures in Ukraine; Law enforcement structures of Ukraine; Media (print media, television, radio, Internet); Special Internet “trolls” and “bots”.	Russian authorities; Cultural and religious organizations; Pro-Russian structures in Ukraine; Media (print media, television, radio, Internet); Special Internet “trolls” and “bots”; Russian special military division; Representatives of foreign countries loyal to Russia.	Russian authorities; Cultural and religious organizations; Media (print media, television, radio, Internet); Special Internet “trolls” and “bots”; Russian special military division; Representatives of foreign countries loyal to Russia. Saboteurs;
Methods	Political and economic blackmail; Activities of non-governmental organizations; Propaganda in the media; Impact through soft power.	Political and economic blackmail; Activities of non-governmental organizations; Propaganda in the media (including social media); Suppression of groups disloyal to the Russian Federation; Aggravation of contradictions in Ukrainian society regarding the vector of foreign policy	Political blackmail; Activities of non-governmental organizations; Propaganda and disinformation in media; Suppression of groups disloyal to the Russian Federation; False flag operations: Provocations; Activities of agents of influence and internet trolls; Cyber attacks; Psychological pressure on military personnel and civilians; Propaganda and disinformation on international platforms;	Threats of using nuclear weapons; Psychological pressure on military personnel and civilians; Intimidation; Propaganda and disinformation in media; Provocations; Activities of agents on influence and internet trolls; Propaganda and disinformation on international platforms; Cyber-attacks; Persecution of pro-Ukrainian activists; Diversions.
Key messages	Russia and Ukraine are brotherly nations with a common history and culture; Ukraine is the “younger brother” of Russia;	EU policies and values are immoral; Ukrainian economy will not withstand European integration; Joining the Customs Union is a guarantee of stability and	The annexation of Crimea is completely legal and complies with the norms of international law; ATO is nothing but a civil war in Ukraine; Ukraine is waging a war against the civilian	Ukraine is an aggressor country, that posed threat to Russia; Ukraine must be de-Nazified and demilitarized; Russia is fighting against NATO; Ukrainian political

Ukraine and Russia are united by strong economic connections; Economic collapse awaits Ukraine without the support of Russia.	development; Euromaidan is organized by Nazis and Bandera people;	population of the L/DPR; Ukrainian political authorities are corrupt and ineffective;	authorities are exacerbating the conflict and do not want to sit down at the negotiating table.
---	---	---	---

The strategy of Russian IPOs in Ukraine (including the ones, which were used after the February 24, 2022) was based on 4 main information technologies (so-called “4 Ds”): demoralization, discreditation, destabilization, disinformation [20]. Demoralization of the army was achieved by conducting cyber-attacks on the information networks of the Armed Forces, state structures, and Ukrainian mass media. Through damaged communication channels Russian propaganda broadcast “classic” messages, discrediting the image of the Ukrainian authorities as well as encouraging military to lay down the arms and surrender. The influence on the civilian population of Ukraine was carried out by the use of manipulative techniques in the mass media, in particular, through social media, in which the Internet trolls and bots actively continued their activities. The new tasks of the latter were discrediting the Ukrainian government and its ability to counter aggression, positioning the power of the Russian Federation and inciting internal conflicts in the country. One more element of the demoralization of Ukrainian civilians was the direct use of psychological pressure, which prompted them to consider the possibility of ending the war at any cost. The examples of the pressure are dropping bombs on the theater in Mariupol and the Kramatorsk railway station, the actions of the occupying forces in the captured territories, shelling the colony in Olenivka and residential buildings in the cities, causing damage to critical infrastructure, etc.

Among the information technologies, used by Russian in its IPOs in Ukraine, the following should be highlighted [20].

Table 7.

Key information technologies of Russian IPOs in Ukraine after the full-scale invasion according to the result of content analysis of main channels of distribution of IPOS.

Information technologies of IPOs	The essence of information technologies	The examples of application of the information technologies
Substitution of concepts	Replacing general terms with a negative meaning with those that are perceived positively or neutrally.	hostilities in the East of Ukraine = civil war; foreigners fighting in Ukraine = mercenaries.
Mirroring	Accusing the enemy of what they are accused of.	Description of the crimes of the Russians in Buch as a production.
“Pass it on”	Creating a message that evokes a strong emotion and calls for its distribution.	The intentions of the Russian Federation regarding mass shelling.
Appealing to authority	Quoting famous people to support arguments.	Report of the French TV channel TF1.
Intimidation	Dissemination of information in order to create negative and panicky moods among the population.	The announcement that Ukraine plans to create a squad of "punishers" who will kill citizens loyal to the Russian Federation.
Stereotyping	The formation of a certain stereotype in public consciousness	Creating an image of Ukrainian servicemen as "militants" and "neo-

The primacy effect	Priority distribution of the version that will reach a large audience and have a better chance of dominating public opinion.	Nazis". Russia is at war with NATO.
Rationalization	Denying one's guilt and striving to prove one's right with logical arguments	The Russian Federation started a war in Ukraine because of a threat from NATO.

The methods of Russian IPOs after the beginning of the full-scale invasion have remained unchanged since 2014: disinformation, cyber-attacks, provocations, activities of agents of influence, spreading rumors, psychological pressure, etc.

Social media and communication platforms became an important tool for spreading IPOs by Russia. In this context, the authors conducted a content analysis of several pro-Russian Telegram channels regarding the level and characteristics of the spread of IPOs in Ukraine after the beginning of the full-scale invasion. The content analysis was carried out during the first half of 2023.

Table 8.

Peculiarities of the spread of IPSO in Russia in Telegram channels according to the results of content analysis of pro-Russian Telegram channels.

Channel's name	Украина.ру	АГС_Z_Донб acca	UKR LEAKS	Open Ukraine Открытая Украина	Легитимны й
Characteristics	News channel of the Russia Today media group project.	The open channel for messages about "life of the people of L/DPR during war"	Telegram channel of the Investigation Center of V. Prozorov	There is no information	There is no information
Number of followers	252 432	206 186	128 518	189 590	903 944
Date of creation	June 11, 2017	July 11, 2019	April 20, 2019	April 11, 2019	December 20, 2018
Disinformation	+	+	+	+	+
	Mostly "grey"		Mostly "grey"		
Propaganda	+	+	+	+	+
Psychological pressure	negligible	+	negligible	+	+
Substitution of concepts	+	+	+	+	+
Mirroring	+	+	+	+	+
"Pass it on"	-	+	-	-	-
Stereotyping	+	+	+	+	+
Rationalization	+	+	+	+	+

3.4. Designing a system for analyzing posts in social media

The conducted analysis shows, that the number of users of social media and Telegram channels is about 5 billion today, and this number continues to grow. These statistics clearly show that virtual platforms for communication of interaction are very popular and have a huge audience. This means that extremely large volumes of public information are created in such places, which can and should be monitored. Carrying out such processed manually is extremely difficult. For this, you need to hire

whole departments that would select the necessary messages, so this process is very expensive and inefficient. In this case, it is proposed to create a system of analysis of posts in social media for effective monitoring of possible illegal actions.

In order to effectively design software, it is necessary to design it using an object-oriented approach and deep neural networks [32]. Therefore, we will start specifying that functioning by constructing a diagram of use cases [33]. This diagram is used to represent a system as a set of actors that interact with each other through use cases. The diagram of options for using the designed system is presented in Figure 4.

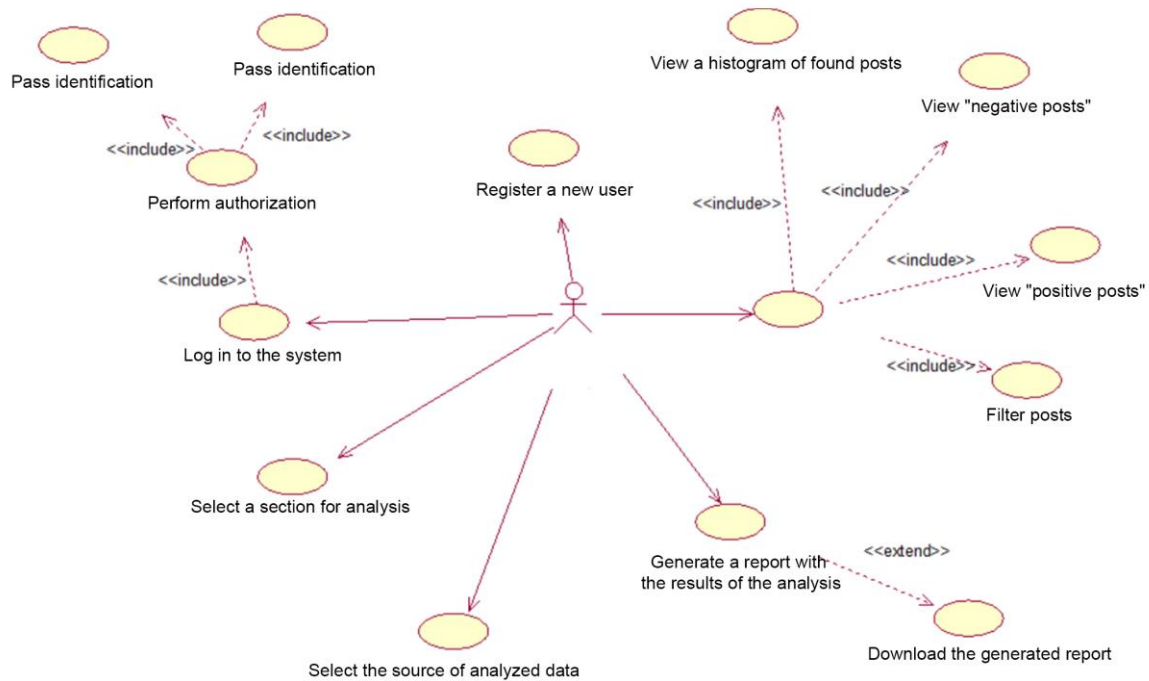


Figure 4: Diagram of use option

Since the system is planned to be developed using an object-oriented paradigm, the next step is to create a class diagram. Figure 5 shows the class diagram of the designed system.

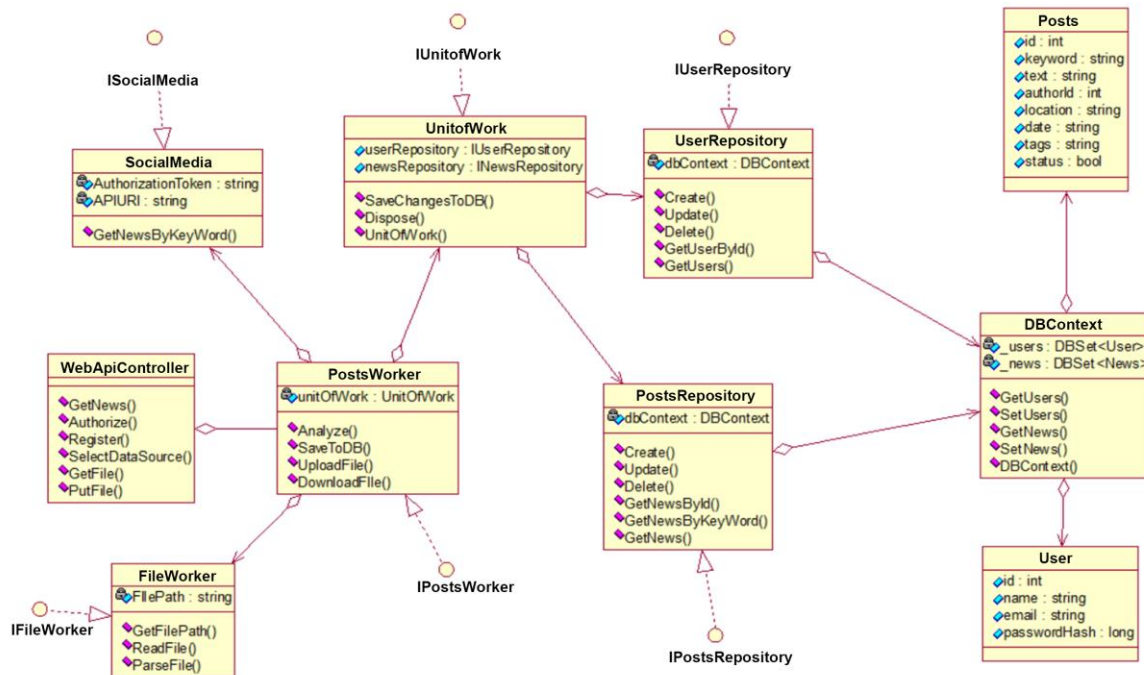


Figure 5: Class diagram

As we can see in Figure 5, the system consists of the following main classes:

- Posts – an entity class that stores post data;
- User – an entity class that stores information about the user;
- DbContext – a class needed to create and work with a database based on the Entity Framework;
- UserRepository – a class designed to provide methods for basic operations with the user table in the database;
- PostsRepository - a class that is designed to provide methods for basic operations with the table of posts in the database;
- UnitOfWork – the main task of this class is to ensure the display of changes in the database in the form of a transaction;
- PostsWorker – responsible for working with posts from social media and their further presentation in the form of an ontology [34];
- FileWorker – required for reading, saving and parsing data;
- WebApiController – provides web controllers that process client http requests;
- SocialMedia – needed to organize access to social media.

In order to understand the features of the display of objects involved in the system and the order of message transmission between them, a sequence diagram was developed. For the designed system, the sequence diagram is shown in Figure 6.

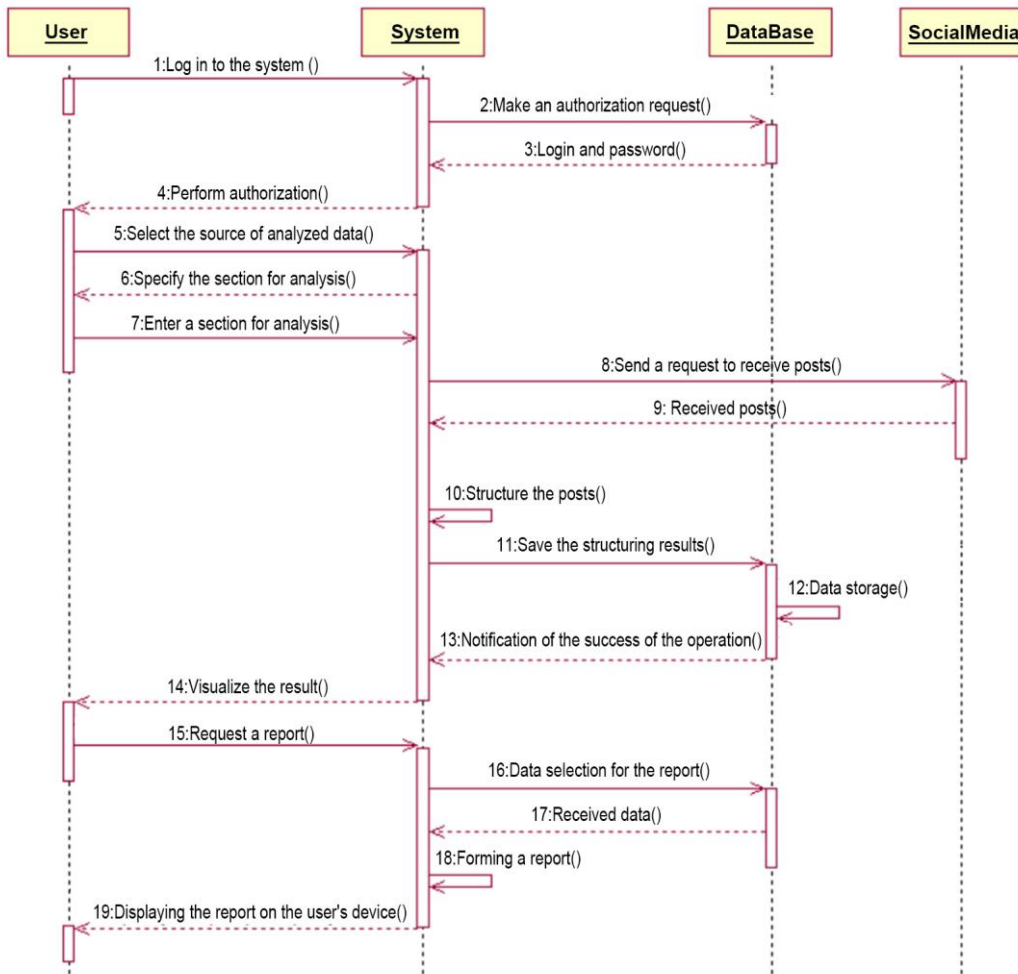


Figure 6: Sequence diagram

As you can see from Figure 6, we have four main objects that interact, in particular:

- User – a person who uses the system.
- System is a software tool that implements the basic business logic.
- DataBase – a place where all data necessary for functioning is stored.
- SocialMedia - is not an internal object of the system, but the system interacts with it as it sends a request to receive the necessary posts.

The next stage in the design process is the creation of the system architecture. In general, the following options can be chosen:

- Monolithic application - all processes take place on the user's device. The advantage of this approach is a smaller number of requests, so the disadvantage is that all calculations take place on the user's device, which leads to an additional load on the client side. This can lead to undesirable delays related to the performance of the platform.
- Client-server application - the system is divided into two main components - this is the server side, where all business logic and data storage is implemented; the server itself can be represented by several machines that will share the load among themselves; the client side is an application that is installed on the user's device and provides him with an interface for interacting with the system. This approach requires a greater number of requests. But it also has significant advantages, which are the possibility of easy scaling, since all calculations and requests are processed by a separate physical component. If necessary, their number and as the result performance can be increased. The specified architecture also allows reducing the load on the user's personal device, which will only visualize the received data from the server.

In view of the conducted analysis, it was decided to use the client-server method of building the system architecture, which will give it flexibility, scalability and reduce the load on the client side. An example of such an architecture is presented in Figure 7.

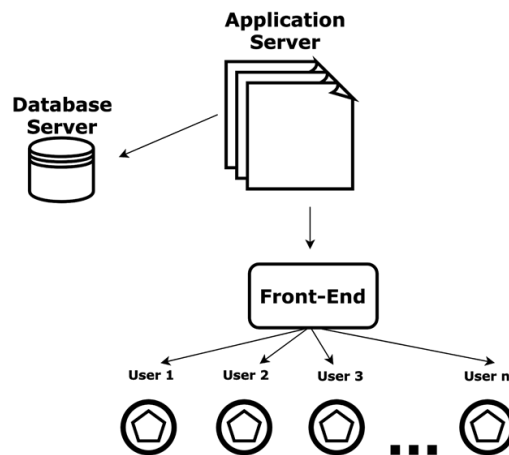


Figure 7: An example of the applied client-server architecture [35].

The next stage of the research will be the construction of a system for analyzing posts in social media using modern software tools.

4. Conclusions

The development of information technologies and increasing of role of information contributed to the emergence of ways for states to use information flows in order to achieve certain political goals. Therefore, IPOs have become an important tool for influencing the domestic and foreign audiences. In Ukrainian studies the concept “IPOs” is defined as a planned use of technologies and means of information dissemination and as a tool of influence on society. Western terminology separates informational and psychological operations, which are carried out during military operations and peacetime, respectively.

The purpose of IPOs is to manipulate the consciousness of the target object in order to change its beliefs, impose a certain model of behavior or make a decision beneficial to the object. Subjects in such operations are any people and sources, that directly exert influence (e. g. political authorities, mass media, non-governmental organizations, special services, etc.). Instead, the object is those at who this influence is aimed (e. g. military or political authorities, civilian population, religious or ethnic groups, mass media, public activities, etc.). Disinformation, propaganda, diversification of public opinion, psychological pressure, rumors, etc., are among the methods of influence.

Russia’s intensive use of information and psychological influence practices began in the 2000s. Since then, the Russian Federation has enshrined the need to conduct information campaigns abroad in the legislature, explaining it by a threat from Western countries and the need for protection of the Russian information space in the states of the post-Soviet space. Modern Russian information and psychological operations are directed both inside the state and at the audience of foreign countries. Russian citizens are forced to be loyal to the authorities, limiting their access to foreign sources of information at the legislative level, suppressing any manifestations of opposition and broadcasting propaganda through mass media. Instead, foreign audience is exposed through a wide range of “active measure” that include disinformation, sabotage, underground and intelligence activities, etc.

Russian IPOs in Ukraine are a vivid example of Russian information technologies in the post-Soviet space, which, according to the statements of Russian authorities, should remain Moscow’s sphere of influence. Prior to the intensification of the state’s cooperation with the EU and NATO, the Russian government mainly used soft power, emphasizing the unity of historical and cultural heritage. In 2008, after the invasion of Georgia, the Russian government intensively worked to increase its influence over the Ukrainian community and prevent its European integration, broadcasting

propaganda about the "economic consequences of joining the Union." The Revolution of Dignity and the destabilization of the political situation in the country were used by Russia to carry out a number of foreign flag operations, the annexation of Crimea and the declaration of L/DPR. The beginning of the anti-terrorist operation and the continuation of Ukraine's course to join the EU was characterized by the use of new methods of pressure on the country, in particular cyber-attacks, psychological pressure on the military and the civilian population, and disinformation through the media and diplomacy. After the start of the full-scale invasion, the IPSO focused on disinformation and demoralization of Ukrainian society, pushing it to end the war on Moscow's terms.

5. References

- [1] Ya. Derkachenko, Information-psychological operations as a modern tool of geopolitics [Informatsiino-psykholohichni operatsii yak suchasnyi instrument heopolytyky], GOAL, 2016. URL: <https://goal-int.org/informacijno-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki/>. [in Ukrainian]
- [2] V. M. Petryk, V. V. Bed, M. M. Prysiashniuk, Information and psychological confrontation [Informatsiino-psykholohichne protyborstvo], 2nd ed., PAT «VIPOL», Kyiv. [in Ukrainian]
- [3] Yu. Tverdokhlib, Theoretical approach to the research of information and psychological operations [Teoretychni pidkhody do doslidzhennia informatsiino-psykholohichnykh operatsii], Epistemological studies in Philosophy, Social and Political Sciences, 2(2) (2019) 122–131. URL: <https://visnukpfs.dp.ua/index.php/PFS/article/view/983/1404>. [in Ukrainian]
- [4] A. O. Umanets, Information-psychological influence: concepts, peculiarities of implementation and countermeasures [Informatsiino-psykholohichni vplyvy: poniattia, osoblyvosti realizatsii ta sposoby protydii], TNU Vernadskoho 33(2) (2022) 106–112. URL: http://psych.vernadskyjournals.in.ua/journal/3_2022/18.pdf. [in Ukrainian]
- [5] I. Yu. Yuzova, Analysis of organization and conducting information-psychological operations during hybrid warfare [Analiz orhanizatsii ta vedennia informatsiino-psykholohichnykh operatsii pry vedenni hibrydnoi viiny], KhNU im. I. Kozheduba 2 (64) (2020) 40–44. [in Ukrainian]
- [6] P. Vejvodova, Information and Psychological Operations as a Challenge to a Security and Defence, *Vojenske rozhledy* 3 (2019) 83–96.
- [7] An overview of psychological operations (PSYOP), Federal Research Division, Library of Congress, Washington DC, 1989. URL: <https://apps.dtic.mil/sti/pdfs/ADA302389.pdf>.
- [8] AJP-3.10.1 (A) Allied Joint Doctrine for Psychological Operations. NATO/PfP Unclassified publication, 2007. URL: <https://info.publicintelligence.net/NATO-PSYOPS.pdf>.
- [9] FM 3-05.301/MCRP 3-40.6A Psychological Operations, Tactics, Techniques and Procedures. Headquarters. Department of the Army, Washington DC, 2003. URL: <https://irp.fas.org/doddir/army/fm3-05-301.pdf>.
- [10] FM 33-1 Psychological Operations. Headquarters. Department of the Army, Washington DC, 1979. URL: <https://irp.fas.org/doddir/army/fm33-1.pdf>.
- [11] V. Zhadko, O. Klymenko, P. Kuliias, O. Markiv, Hybrid warfare and journalism. Issues of information security [Hibrydna viina i zhurnalistyka. Problemy informatsiinoi bezpeky], Kyiv, NPU im. M. P. Drahomanova, 2018. [in Ukrainian]
- [12] A. Lebid, K. Vashyst, M. Nazarov, Information Resilience as a Means of Countering the Socio-Psychological Strategies of Information Wars, *International Journal of Media & Information Literacy* 7(1) (2022) 157-166.
- [13] T. Clack, R. Johnson, *The World Information War. Western Resilience, Campaigning, and Cognitive Effects*, Routledge, London, 2021. doi: <https://doi.org/10.4324/9781003046905>.
- [14] A. Svintsytskyi, O. Semeniuk, O. Ufimtseva, Y. Irkha, S. Suslin, Countering fake information as a guarantee of state information security, *Security Journal* 36 (2023) 427–442.
- [15] J. Olchowski, *How to Weaponise Information*, in *Disinformation, Narratives and Memory Politics in Russia and Belarus*, Routledge, NY, 2022.
- [16] L. Chen, J. Chen, C. Xia, Social network behavior and public opinion manipulation, *Journal of Information Security and Applications*, 64 (2022). doi: <https://doi.org/10.1016/j.jisa.2021.103060>.

- [17] O. Markovets, M. Buchyn, Threats of the implementation of e-voting and methods of their neutralization, CEUR Workshop Proceedings 3296 (2022) 29-39. URL: <https://ceur-ws.org/Vol-3296/paper3.pdf>.
- [18] M. Buchyn, A. Helesh, B. Shubyn, Information Security During Electronic Voting: Threats and Mechanisms for Ensuring, in: 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT), Lviv, Ukraine, 2021, pp. 266-269. doi: 10.1109/AICT52120.2021.9628971.
- [19] C. Paul, M. Matthews The Russian “Firehose of Falsehood” Propaganda Model', RAND Corporation, 2016. URL: <https://www.rand.org/pubs/perspectives/PE198.html>.
- [20] PSYOPS Are Russia’s Way to Save On Conventional Weapons – DI. Instytut masovoi informatsii, 2023. URL: <https://imi.org.ua/en/news/psyops-are-russia-s-way-to-save-on-conventional-weapons-di-i50384>.
- [21] Units of psychological operations of the Russian army [Pidrozdily psikhologichnykh operatsii rosiiskoi armii], Military, 2020. URL: <https://mil.in.ua/uk/articles/pidrozdily-psyhologichnyh-operatsij-rosijskoyi-armiyi/>. [in Ukrainian]
- [22] G. Colom-Piella, The anatomy of Russian disinformation, *Historia y Comunicación Social* 25(2) (2020). doi: <https://doi.org/10.5209/hics.63373>.
- [23] N. Maréchal, Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy, *Media and Communication* 5(1) (2017). doi: <https://doi.org/10.17645/mac.v5i1.808>.
- [24] M. Wehner, Hacking, propaganda and electoral manipulation. Moscow’s information war on the West, *EUROZINE*, 2017. URL: <https://www.eurozine.com/hacking-propaganda-and-electoral-manipulation-2/>.
- [25] Analysis of Russia’s Information Campaign Against Ukraine, The NATO StratCom Centre of Excellence, 2015. URL: https://stratcomcoe.org/cuploads/pfiles/russian_information_campaign_public_12012016fin.pdf.
- [26] E. Lazareva, Why Putin started military operation against Ukraine, 2022. URL: <https://ura.news/articles/1036284030>. [in Ukrainian]
- [27] M. Musiał-Karg, A. Łukasik-Turecka, Disinformation in the media space during the war in Ukraine. How did Kremlin’s fake news blame Ukraine, the USA and NATO for the invasion, in: *The War in Ukraine. (Dis)information – Perception – Attitudes*, 2023, pp.13-38.
- [28] L. Martín-Romo, M. Oliveros-Mediavilla, E. Vaquerizo-Domínguez, Perception and opinion of the Ukrainian population regarding information manipulation: A field study on disinformation in the Ukrainian war, *Profesional de la informacion* 32(4) (2023). URL: <https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/87245/63445>.
- [29] M. Buchyn, Peculiarities and problems of measuring the level of democratic elections, *Balkan Social Science Review* 21 (2023) 105–125. doi: 10.46763/BSSR2321105b.
- [30] S. Ctetsenko, Russia and cyber attacks. Ukraine shared cyber defense experience with Czech colleagues [Rosii i kiberatomy. Ukraina podilylasia dosvidom kiberzakhystu z cheskyim kolehamy], *Radio Svoboda*, 2018. URL: <https://www.radiosvoboda.org/a/29656549.html>. [in Ukrainian]
- [31] Russia formulated the response to the US and NATO regarding “security guarantees” [Rosiiia sformuluivala vidpovid SShA i NATO shchodo “harantii bezpeky”], *Ukrainska pravda*, 2022. URL: <https://www.pravda.com.ua/news/2022/02/14/7323955/>. [in Ukrainian]
- [32] O. Mediakov T.Basyuk, Specifics of Designing and Construction of the System for Deep Neural Networks Generation, CEUR Workshop Proceedings 3171 (2022) 1282–1296. URL: <https://ceur-ws.org/Vol-3171/paper94.pdf>.
- [33] P. Mrzyglocki, UML Summarized: Key Concepts and Diagrams for Software Engineers, Architects and Designers, Independently published, 2023.
- [34] T. Basyuk, A.Vasyliuk, Approach to a subject area ontology visualization system creating, CEUR Workshop Proceedings 2870 (2022) 528–540. URL: <https://ceur-ws.org/Vol-2870/paper39.pdf>.
- [35] J. Esterkin, Client-server architecture. URL: <https://openclassrooms.com/en/courses/6397806-design-your-software-architecture-using-industry-standard-patterns/6896156-client-server-architecture>.