UDC 316.77:659.4:004.8
DOI: 10.15587/1729-4061.2025.342297

DEVISING A CODE-FREE METHOD FOR DETECTING SIGNS OF INFORMATIONAL-PSYCHOLOGICAL INFLUENCES IN MESSAGES

Dmytro Lande
Doctor of Technical Sciences, Professor
Department of Information Security**
Kostiantyn Yefremov
PhD*
Artem Soboliev
PhD*
Ivan Pyshnograiev
Corresponding author
PhD, Associate Professor
Department of Artificial Intelligence**
E-mail: pyshnograiev@gmail.com
*Educational and Scientific Center
"World Data Center for Geoinformatics
and Sustainable Development"**
**National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
Beresteyskyi ave., 37, Kyiv, Ukraine, 03056

This study investigates text messages that potentially contain signs of informational-psychological operations (IPSOs). The task addressed aims to solve the problem of detecting signs of IPSOs in the media space.

An innovative method for detecting such signs has been proposed, based on the construction and analysis of semantic networks and implemented without the use of program code by using large language models (LLMs). This makes it possible to generate formalized analytical queries to LLMs in the form of a code-free system based on the composition of structured prompts.

The method's unique feature is the parallel analysis of data from two sources of knowledge: internal and external. The internal one contains generalized IPSO patterns formed on the basis of a wide corpus of data. The external one includes verified examples of fake messages from social networks, news outlets, and archives of fact-checking organizations.

To improve the accuracy of analysis, semantic normalization of concepts is used, which employs embedded vectors to unify terminology, as well as comparison of causal paths in semantic networks to identify connections. The assessment of the probability of a message belonging to IPSO is formed by aggregating the results using a weighted average, which makes it possible to take into account semantic and structural similarity. An example of applying the method to the analysis of a disinformation message is given, demonstrating the ability to detect key signs of psychological influence: manipulative narratives, emotional loading, and cause-and-effect relationships.

The proposed method is flexible, reproducible, and accessible to researchers without programming skills, which makes it a valuable tool for monitoring information threats and analyzing disinformation in the context of information confrontations

Keywords: informational-psychological operation, semantic network, LLM, prompt engineering, codeless analytics, AI, disinformation

Received 19.08.2025
Received in revised form 30.09.2025
Accepted date 20.10.2025
Published date 31.10.2025

How to Cite: *Lande, D., Yefremov, K., Sobolev, A., Pyshnograiev, I. (2025). Development of a code-free method for detecting signs of informational-psychological influences in messages. Eastern-European Journal of Enterprise Technologies, 5 (2 (137)), 55–69. https://doi.org/10.15587/1729-4061.2025.342297*

1. Introduction

Under current conditions of globalization and digitalization of the information space, the intensity of information confrontations is increasing, which makes the task to detect informational-psychological operations (IPSOs) extremely relevant. IPSOs aimed at manipulating public opinion, destabilizing social processes, and undermining trust in institutions are actively used in social networks, media, and other digital platforms. The growth of disinformation campaigns, in particular due to the rapid spread of fake messages, creates challenges for security, social stability, and democracy. Conventional approaches to text analysis, such as manual reading, natural language processing (NLP) techniques, or machine learning, whose methods are outlined in [1], have limitations in flexibility, scalability, and adaptation to new contexts. This complicates their application under conditions of rapidly changing information threats [2]. The ability to quickly and effectively detect IPSOs is critically important for countering disinformation that can affect public sentiment, cause panic, or undermine trust in state institutions. For example, fake messages on social networks can provoke mass protests or change the perception of key events. Research in the field of IPSO makes it possible to devise new methods of analysis that take into account the semantic, psychological, and structural features of manipulative texts. Such methods are necessary to design tools that can respond quickly to new forms of disinformation, including the use of artificial intelligence (AI) to automate analysis. Codeless methods based on large language models (LLMs) open up new opportunities, allowing researchers and analysts without technical training to participate in the detection of IPSOs, which is especially important in resource-limited environments [3].

The results of research in the area of IPSO detection have significant practical potential. First, the development of a code-free method based on LLM makes it possible to design accessible tools for media monitoring that can be used by journalists, security analysts, and government agencies to quickly detect disinformation campaigns. Second, the analysis of semantic networks makes it possible not only to identify fake messages but also assess their psychological effectiveness, which is valuable for devising counterstrategies. For example, the detection of manipulative narratives could help in planning information campaigns to improve the media literacy of people. Third, the methodology based on prompt engineering and the concept of a "swarm of virtual experts" provides a multifaceted analysis of texts, which increases the reliability of conclusions and could be applied in education, cybersecurity, and social media analysis [4].

The practical implementation of such methods helps reduce the impact of disinformation on society and increase resilience to information attacks. The approach proposed in our work focuses on designing and testing a toolkit based on LLMs for detecting signs of IPSO through the construction of semantic networks. This method combines analysis of the internal knowledge base of LLMs with an external collection of verified fake messages, which makes it possible to achieve high accuracy and flexibility [5]. The use of code-free technologies, such as prompt engineering, makes the method accessible to a wide range of specialists who do not have programming skills. In addition, the integration of graph analysis and sentiment analysis provides a comprehensive approach to detecting manipulative strategies, both at the concept level [6] and when building a classifier [7].

Therefore, research on devising code-free methods of text analysis for detecting informational-psychological operations based on large language models is relevant. Such a study meets the urgent needs of modern society in countering disinformation and provide practical tools for media monitoring, cybersecurity, and increasing media literacy.

2. Literature review and problem statement

In modern research on disinformation detection and informational-psychological operations, methods based on natural language processing, deep learning (DL), and large language models occupy a special place. Most current approaches to disinformation detection are based on text classification using DL models. For example, in [1], machine learning-based algorithms for text classification using word vectorization and topic modeling are proposed. The authors achieved high accuracy (up to 95%) on standard datasets such as LIAR or FakeNewsNet. Similarly, in [7], NLP models were built for medical text classification, integrating transformers and sentiment analysis, with an emphasis on emotional content. However, these methods do not solve the issue of adaptation to dynamic IPSO contexts where influence patterns evolve rapidly. The reason is subjective: the authors focus on static datasets, ignoring flexibility due to limited resources for real-time processing. Objectively, DL models require a lot of computing power and annotated data, which makes their application in unstructured environments such as social networks difficult.

Another area is the use of semantic networks for disinformation analysis. In [5], semantic networking based on LLMs is described for modeling the relationships between concepts in texts. The authors propose a hierarchical LLM query for building networks, which makes it possible to detect cause-and-effect chains. Similarly, in [6], memes are analyzed as propaganda tools through graph models, emphasizing the role of visual elements. In [2], network analysis is applied to assess social opinion in media content. These works address the issue of structural analysis but do not integrate code-free methods such as prompt engineering for automation. The issue of scalability remains unresolved: semantic networks are often built manually or with code, which limits accessibility for non-programmers. The reasons for this are objective (lack of standardized tools for code-free prompt composition) and subjective (focus on technical aspects, without attention to user accessibility).

With the advent of LLMs such as GPT or BERT, hybrid models have emerged. For example, in [8], a combination of GPT and BERT is proposed for fake news detection, with an emphasis on linguistic patterns, achieving an accuracy of 92%. Similarly, using benchmarks, in [9], a prompt-based LLM is applied to Twitter propaganda, focusing on manipulative techniques. In [10], prompts are integrated for the analysis of catastrophic events. These works address the issue of semantic depth but do not combine the internal knowledge of LLMs with external collections of known IPSOs, which leads to low robustness to new tactics. The issue of aggregating results from multiple sources to increase accuracy remains unresolved. The reasons are subjective (the authors limit themselves to single-component models due to the focus on efficiency, ignoring hybridity) and objective (the lack of frameworks for dynamic integration, due to the evolution of LLMs).

The role of multimodal methods (text + image) is also emphasized [11]. At the same time, work [12] criticizes the insufficient involvement of external expert information, for example, psychological aspects of IPSOs. Paper [10] analyzed the use of emotions as indicators, but semantic networks are not integrated into the solution. The issue of codeless implementation, where analysis depends on coding, also remains unresolved. The reasons for this are objective (LLMs have not yet been standardized for codeless frameworks) and subjective (researchers emphasize accuracy, not accessibility).

Systemizing local problems, the following can be noted. First, this is the lack of adaptation to dynamic IPSOs in DL methods through static models. Second, in semantic networks there is a need for coding and manual processing. Third, LLM approaches lack combination with external collections and aggregation, and reviews often ignore psychological patterns and codeless flexibility. A common unsolved problem is the lack of a flexible, codeless method for detecting signs of IPSO in text messages. This is due to objective limitations (evolution of LLM technologies and lack of integration frameworks) and subjective ones (focus on individual aspects without systemic hybridity). A solution is possible based on semantic networks and LLMs, which combines internal knowledge of the model with external training collections for aggregation of results, taking into account cause-and-effect patterns and accessibility for non-programmers.

3. The aim and objectives of the study

The aim of our research is to devise a flexible code-free method for detecting signs of informational-psychological operations in text messages. This will make it possible to increase the effectiveness of countering disinformation in the context of information wars, to ensure the availability of tools for non-programmers in the fields of media monitoring, national security, and media literacy education. The results will also lay the foundation for automated early warning systems for propaganda campaigns.

To achieve the goal, the following tasks were set:

– to build a training collection of known examples of IPSOs based on English-language sources to provide a reference base for comparison;

– to devise an approach to building semantic networks of text messages using hierarchical LLM polling and the concept of a swarm of virtual experts for modeling cause-and-effect relationships;

– to develop algorithms for comparing semantic networks of analyzed messages with internal LLM knowledge and the generalized network of the training collection, taking into account semantic normalization and path similarity assessment;

– to propose a function of aggregation of results to obtain a generalized assessment of the probability of a message belonging to IPSO;

– to implement a method of codeless programming based on logical primitives to automate the analytical process and test it on examples of disinformation messages.

4. The study materials and methods

The object of our study is text messages that potentially contain signs of informational-psychological operations, published on social networks, news sites, or other open sources.

The hypothesis of the study assumes that the use of large language models in combination with a codeless analytical method allows for the effective detection of signs of informational-psychological operations in text messages. This is achieved by reconstructing the causal patterns of manipulative influence in the analyzed text and their systematic comparison with reference models. Such reference models can be obtained from two sources: internal knowledge of LLMs, which summarizes global patterns of disinformation, and an external training collection of verified examples of IPSOs, which ensures contextual accuracy. In this case, the detection efficiency is increased due to the integration of semantic normalization of concepts, analysis of causal paths in graphs, and aggregation of results based on the weighted average.

The method is built based on semantic networks and large language models, combining the model's internal knowledge with external training collections to aggregate results taking into account cause-and-effect patterns. The following software tools were used in our work: Llama-3 API, ChatGPT (gpt-4 model), Python language.

The following assumptions are adopted in the paper:

1. Large language models, such as GPT or Claude, contain generalized knowledge about IPSO patterns obtained from their training corpora, which makes it possible to reconstruct reference semantic networks.

2. The training collection of well-known IPSO examples is representative of typical disinformation campaigns.

3. Semantic normalization of concepts through embedded vectors provides sufficient accuracy for matching synonymous formulations.

Simplifications accepted:

1. Analysis is limited to text messages, ignoring multimodal elements (images, videos) that may accompany the text.

2. The comparison of semantic networks is based on the cosine similarity of embeddings and the weighted Jaccard coefficient, without taking into account more complex metrics, such as deep analysis of syntactic structures.

3. The weights (α, β) for aggregation of results are set empirically (e.g., $\alpha = 0.6$, $\beta = 0.4$ for comparison with LLMs, $\beta = 0.5$ for aggregation) and are not dynamically adapted.

The IPSO analysis methodology is divided into the following main stages:

1. Construction of a training collection, i.e., a set of messages known as IPSO examples.

2. Construction of a semantic network of a new message based on the analysis of its text.

3. Comparison of the message network and information from the internal LLM knowledge base by calculating the similarity between the corresponding networks through the intersection of concepts – typical IPSO patterns and connections.

4. Comparison of the message network and the generalized semantic network of the training collection.

5. Aggregation of results by calculating the averaged estimate of the probability that the text is part of IPSO.

5. Methodology for identifying potential signs of informational and psychological influences

5. 1. Construction of a training collection

Construction of a training collection of fake messages aimed at detecting and analyzing informational and propaganda operations is a key stage in the training of specialists in media literacy, disinformation analysis, and cybersecurity [13]. The collection should be systematic, multifactorial, and representative to ensure effective training in methods of detecting, verifying, and refuting fake content.

Given access to the entire Internet and search engines (Google, Bing, cross-indexes, Wayback Machine archives, social networks, news platforms), sources of material selection include:

– social networks: Twitter/X, Facebook, Reddit, Telegram, YouTube – for collecting widespread messages, videos, memes;

– news outlets and blogs: both official and alternative sources (including those with signs of propaganda or disinformation);

– research archives: databases from Bellingcat, DFRLab (Digital Forensic Research Lab), EUvsDisinfo, Logically, NewsGuard;

– search engines like Google with an extended set of operators like site:, intitle:, filetype:, inurl:, before:/after: for targeted search of fake messages for a certain period;

– translated materials: use of English translations of Russian-language or other language fakes, especially from conflict regions (e.g., Ukraine, the Middle East).

The collection is formed according to the following criteria: language, type of content, topic, level of disinformation, proven fakeness. To ensure structuring and the possibility of further analysis, each element of the collection is formalized using metadata given in Table 1.

Table 1

Training collection elements' metadata

Field	Description
ID	Unique post ID
Publish date	Post date
Source	URL, platform, author (if known)
Content type	Text, image, video, audio
Topic	War, health, economics, etc.
Disinformation type	Fake photo, miscontextualization, conspiracy theory, deepfake
Language	English
Geographical destination	Target audience (NATO, US, EU, global)
Verification	Link to fact check, date of verification, organization
Key features	Signs of IPSOs (emotional narrative, anonymity, repetition, etc.)
IPSO goal	Destabilization, discrediting, manipulation of public opinion

For educational purposes, the categorization by type is used:

– Disinformation – intentional disinformation;

– Misinformation – spread of false information without malicious intent;

– Malinformation – leakage of true information with the aim of harm;

– Propaganda – systematic formation of a certain point of view.

The IPSO taxonomy is also used by mechanisms of influence:

– creation of fake events;

– change of context (out-of-context);

– use of authorities (fake experts);

– forgery of evidence (faked media);

– hyperbolization or minimization of events.

The construction of an English-language training collection of IPSO fake messages is a systematic process that combines access to global sources, a formalized data structure, analytical classification, and practical applicability in education. Such a collection becomes the basis for training specialists capable of counteracting current information threats.

5. 2. Construction of semantic networks

Our approach involves building a semantic network based on the analyzed text and comparing this network with the content of known examples of IPSOs (training collection), as well as with a network built on the basis of the internal knowledge base of LLMs.

It also involves the use of a swarm of virtual experts, i.e., text analysis on behalf of different roles (linguist, psychologist, disinformation specialist, sociologist).

To implement the approach, large language models are used, which, through prompts built on the basis of logical primitives “Condition” (If-Else), “Cycle” (For-Loop) and “Function”, can perform complex analytical tasks without the need to use complex program code [4].

The construction of semantic networks is a key stage in the systematic analysis of informational and psychological influences as it makes it possible to move from the fragmentary study of individual messages to modeling the structure of holistic propaganda narratives. In this context, the semantic network is considered as a graph model. The nodes are key concepts (for example, “destabilization of trust”, “fear of the future”, “institutional incompetence”), and the edges are semantic connections between them, in particular cause-and-effect relationships of the “cause → effect” type [14].

To build such networks, a hierarchical approach is used, based on the sequential deployment of concepts through their gradual refinement. This process is implemented through the systematic formulation of structured queries (prompts) to intelligent natural language processing systems. The goal is to automatically extract from the text space the cause-and-effect chains that underlie informational-psychological operations.

The process begins with identifying a central concept – a key element that is the goal or consequence of the information influence. For example, if a campaign to destabilize public consciousness is being analyzed, such a concept might be “loss of trust in the state.”

The first step is to design a prompt aimed at identifying the causes of this phenomenon:

“List the main reasons for the loss of trust in the state in the context of informational-psychological operations. Use no more than three words per reason. Submit the results in the format: ‘reason; loss of trust in the state’. Each entry is on a new line.”

Example of the expected answer:

– disinformation; loss of trust in the state;

– corruption; loss of trust in the state;

– lack of transparency; loss of trust in the state;

– fear of the future; loss of trust in the state.

Each of the specified concepts (for example, “disinformation”) becomes a new center of the query at the next level:

“List the main reasons for the spread of disinformation in the context of informational-psychological operations. Use no more than three words per reason. Submit the results in the format: ‘reason; disinformation’. Each entry is on a new line.”

This process continues for 2–3 levels, forming a multi-level structure that reflects the depth of information influence. Importantly, the network is not strictly hierarchical: the same concept (e.g., “human error”) can appear in different branches, indicating its systemic role in the narrative.

To increase the completeness and analytical stability of the network, the method of swarming virtual experts is used. It is based on the fact that when the same prompt is repeated several times, the system can generate different, but logically justified, answers. Each of them is interpreted as the opinion of a separate “virtual expert” with a certain profiling (for example, a psychologist, strategist, communicator, analyst).

For example, a prompt regarding the reasons for “fear of the future” can be performed 5–7 times. As a result, we get various, but complementary answers:

– “uncertainty; fear of the future”;

– “economic crisis; fear of the future”;

– “military threats; fear of the future”;

– “information noise; fear of the future”.

The aggregation of all answers makes it possible to construct a multidimensional model of influence that takes into account various aspects of the formation of the audience’s emotional state.

All responses are collected into a single data structure in the format of pairs “source” → “target”, which corresponds to the directed edges of the graph. For example:

– disinformation; loss of trust in the state;

– economic crisis; fear of the future;

– fear of the future; disinformation.

To increase reliability, threshold filtering is applied: only those concepts and connections that appeared in more than N responses (for example, 2–3 times) are included in the final network. This makes it possible to filter out marginal or random connections, leaving only stable, systemically significant elements.

The resulting network is analyzed taking into account network metrics:

– Out-Degree – the number of outbound connections. A high value indicates a concept that acts as a driver of influence (for example, “human error” can have many consequences);

– Betweenness Centrality shows how much a concept is a “bridge” between different branches of the network. A high value indicates strategic importance (for example, “social engineering” can connect technical and psychological aspects);

– Clustering coefficient indicates the density of connections in the local environment of the concept, which may indicate the presence of persistent propaganda patterns.

The formed semantic network can be used to:

– identify key points of audience vulnerability (for example, “lack of transparency” as the root of many narratives);

– model scenarios of the spread of disinformation by moving from initial causes to final consequences;

– devise countermeasures by identifying counter-narratives aimed at breaking causal chains (e.g., increasing transparency as a countermeasure to loss of trust);

– train professionals as a basis for media literacy and disinformation analysis simulators.

Although the proposed approach significantly accelerates the process of knowledge formation, the results require mandatory expert verification. Automatic systems can generate logically sound, but contextually incorrect or false connections. Therefore, the final interpretation of the network should be carried out by specialists in psychology, communications, political science and security [15].

Construction of semantic networks through hierarchical polling using the method of swarms of virtual experts is an effective tool for the analysis of information and psychological influences. It makes it possible to systematize discontinuous information, identify hidden propaganda structures, and create a basis for strategic planning in the field of information security. The proposed approach could be adapted to different subject areas and become the basis for scenario analysis and forecasting of information threats.

5. 3. Algorithms for comparing semantic networks

5. 3. 1. Comparing the network of message and information from the internal knowledge base of LLMs

The key stage in identifying signs of informational and psychological influences is the comparison of the semantic structure of the analyzed message with generalized patterns encoded in large language models. Since LLM is trained on massive corpora of texts, including materials of information and propaganda operations, it implicitly contains in its internal architecture a generalized semantic network of typical IPSOs.

Let $G_1 = (V_1, E_1)$ be the semantic network formed on the basis of the analyzed message, where V_1 is a set of concepts (vertices), and E_1 is a set of semantic connections (edges) between them. Let $G_2 = (V_2, E_2)$ be the reference network reconstructed by hierarchically querying LLMs for typical causal patterns in a given subject area (e.g., "destabilization of trust in government"). This process is based on the virtual expert swarm method, which ensures multivariate and completeness of the model.

For this purpose, the comparison function *Compare*(G_1, G_2) is introduced, which calculates the generalized similarity score p_c from the following formula

$$p_c = \alpha \cdot J_{emb}\left(V_1, V_2\right) + \left(1-\alpha\right) \cdot S\left(E_1, E_2\right), \tag{1}$$

where $J_{emb}(V_1, V_2)$ is a measure of similarity of vertex sets, calculated based on embedded vectors; $S(E_1, E_2)$ is a measure of structural similarity of graphs, which can be based on edit distance, common paths, or other topological metrics; $\alpha \in [0,1]$ is a weighting factor that balances semantics and structure.

Unlike the classical Jaccard coefficient, which is based on lexical intersection, it is proposed to use a vector representation of concepts obtained from the internal space of LLM. Each concept $v \in V_1 \cup V_2$ is converted into vector $e_v \in R^d$ using the in-built function of embeddings model. The similarity between two concepts is determined by the cosine distance

$$sim\left(v_i, v_j\right) = \frac{e_{v_i} \cdot e_{v_j}}{\left\|e_{v_i}\right\| \left\|e_{v_j}\right\|}. \tag{2}$$

Based on this, the vector-weighted Jacquard coefficient is calculated

$$J_{emb}\left(V_1, V_2\right) = \frac{1}{\left|V_1 \cup V_2\right|} \sum_{u \in V_1} \max_{u \in V_2} sim\left(u, v\right) \cdot \delta_{u,v}, \tag{3}$$

where θ is the semantic similarity threshold, $\delta_{u,v}$ is the filtering function, which is defined as follows

$$\delta_{\mu,v} = \begin{cases} 1, \text{ if } \; sim(u,v) > 0 \\ \hline 0, \quad \text{otherwise} \end{cases}.$$

To improve the accuracy of semantic network comparison, in addition to the general structural similarity, the S_{path} causal path similarity assessment can be used. This approach is based on the selection of key causal chains in networks G_1 and G_2 (for example, "source of influence → tool → emotion → social reaction") and their comparison at the level of semantic vectors.

Let $P_1 = \left(v_1^1, v_1^2, \ldots, v_1^k\right)$ be a path in G_1, $P_2 = \left(v_2^1, v_2^2, \ldots, v_2^k\right)$ be the corresponding path in G_2. The similarity between S_{path} paths is calculated as the average value of the cosine similarities of the corresponding vertices

$$S_{path}\left(P_1, P_2\right) = \frac{1}{k} \sum_{i=1}^{k} sim\left(e_{v_1^i}, e_{v_2^i}\right), \tag{4}$$

where e_v – vector representation of the concept v, obtained from embeddings of LLM.

For all possible pairs of paths, the maximum similarity is calculated, which can be used as an additional component to $S(E_1, E_2)$ in the comparison formula.

It is assumed to use one of two options:

1. Extended formula taking into account $S(E_1, E_2)$

$$p_c = \alpha \cdot J_{emb} + \left(1-\alpha\right) \cdot \left[\beta \cdot S + \left(1-\beta\right) \cdot S_{path}\right], \tag{5}$$

where $\beta \in [0,1]$ is the weight coefficient.

2. Replacing $S(E_1, E_2)$ with S_{path} since it is semantically richer

$$p_c = \alpha \cdot J_{emb} + \left(1-\alpha\right) \cdot S_{path}. \tag{6}$$

This approach is particularly effective for identifying typical narratives of IPSOs, which have a unified logic of psychological impact, regardless of lexical formulation.

This approach allows for the automatic consideration of synonymous, paraphrased, and contextually equivalent formulations (e.g., "disinformation" ≈ "fake news," "disorganization" ≈ "insecurity") without the need to explicitly define synonym pairs. The use of embeddings is natural for LLMs, as they are an internal mechanism of the model for understanding language, which makes the methodology technologically consistent, reproducible, and scalable.

5. 3. 2. Comparing the message network and the generalized semantic network of training collection

In addition to the comparison with the internal knowledge of LLM, the analysis can be based on the external training collection of known IPSOs [16]. However, instead of a static comparison, a dynamic construction of a generalized semantic network G_3^*, is proposed that summarizes the most common cause-and-effect patterns present in the collection.

The network $G_3^* = \left(V_3^*, E_3^*\right)$ is formed by:

– splitting the collection into separate messages;

– constructing a semantic network for each message using the $F_{extract}$ function;

– aggregating all networks by merging vertices and edges;

– filtering by frequency of occurrence and semantic normalization (for example, clustering of concept embeddings).

The resulting network G_3^* acts as an explicit reference, built on the basis of documented examples of disinformation. It differs from G_2 (based on LLM) in that:

– has high accuracy for known campaigns;

– but limited in universality and may be outdated.

The comparison of G_1 with G_3^* is performed with an emphasis on semantic normalization through embeddings, which provides a unified methodological approach

$$p_{coll} = \alpha \cdot J_{emb}\left(V_1, V_3^*\right) + \left(1-\alpha\right) \cdot S\left(E_1, E_3^*\right). \quad (7)$$

This approach makes it possible not only to detect the correspondence of the analyzed text to known IPSOs but also assess the quality of the training collection: if $p_{coll} \ll p_c$, this may indicate its insufficiency in the context of new disinformation tactics.

The calculation of the similarity paths S_{path} is performed similarly to (4). Since the generalized network G_3^*, reconstructed from the internal knowledge of LLM also has a causal structure, it is possible to isolate typical chains of influence (for example, "manipulation" → "disinformation" → "fear" → "destabilization") and compare them with the corresponding paths in the analyzed network G1.

The use of S_{path}, as in the previous case, makes it possible to increase the sensitivity of analysis to deep patterns of informational and psychological influences, which are preserved even with significant lexical variability. This makes the methodology resistant to the evolution of disinformation tactics, where the wording changes, but the basic logic of psychological influence is preserved.

5. 4. Aggregating the results of analyzing the signs of informational and psychological influences

At the final stage of the analysis of the signs of informational and psychological influences, the aggregation of partial assessments obtained at the previous stages is performed by comparing the semantic structure of the analyzed message with various sources of reference knowledge. This stage aims to integrate various types of analytical information into a single generalized assessment that characterizes the degree to which the message belongs to the class of informational and propaganda operations (IPSOs), as well as to provide the possibility of assessing the importance of individual components of the analytical system.

If p_c is the similarity score obtained by comparing the semantic network of the message G_1 with the reference network built on the basis of the training collection of fake messages, and p_{LLM} is the similarity score obtained by comparing G_1 with the generalized semantic network reconstructed from the internal knowledge of the large language model, which implicitly contains generalized IPSO patterns, then the aggregation function $Agg(p_c,p_{LLM})$ is defined as the weighted average

$$p_{final} = \beta \cdot p_c + \left(1-\beta\right) \cdot p_{LLM}, \quad (8)$$

where $\beta \in [0,1]$ is a weighting factor that reflects the degree of trust in the training collection in a specific context of analysis.

The value of β can be set based on expert assessments, historical data on the effectiveness of the collection, or adaptively, depending on the subject of the message, geopolitical context, or the level of relevance of the data in the collection.

For example, if for the analyzed message $p_c = 0.78$ (high similarity with known IPSOs) and $p_{LLM} = 0.72$ (confirmation from the generalized knowledge of LLM) are obtained, with $\beta = 0.5$, then

$$p_{final} = 0.5 \cdot 0.78 + 0.5 \cdot 0.72 = 0.75. \quad (9)$$

The resulting generalized score p_{final} is interpreted according to the established thresholds:

– $p_{final} > 0.7$ – high probability of belonging to IPSO;

– $0.4 \leq p_{final} \leq 0.7$ – moderate similarity, requires contextual clarification;

– $p_{final} < 0.4$ – low probability of belonging to IPSO.

Aggregation reduces the risk of erroneous decisions inherent in individual methods. For example, a collection may be outdated or incomplete with respect to new disinformation tactics, while an LLM trained on a broad corpus may better reflect modern patterns. Conversely, an LLM may generate generalizations that do not correspond to a specific campaign, while an explicit collection provides more accurate but narrower guidelines.

In addition, the analysis of the p_c and p_{LLM} ratio has meta-analytical significance:

– if $p_c \gg p_{LLM}$, this indicates that the message contains specific features known only within the collection, which confirms its high value as a source of expert knowledge;

– if $p_c \approx p_{LLM}$, this indicates that the LLM adequately reproduces the knowledge available in the collection, which makes it possible to consider it as potentially redundant under conditions of limited resources;

– if $p_c \ll p_{LLM}$, this may indicate either the insufficiency of the collection or that the new message uses the latest, not yet documented patterns of disinformation, which requires updating the collection.

Thus, the aggregation function not only provides a more reliable final assessment but also becomes a tool for self-diagnosis of the analytical system. This will allow one to assess the effectiveness of its components and make decisions about further development: by expanding the collection, by adjusting weighting factors, or by integrating additional sources of knowledge.

Previous chapters described the sequence of analytical steps from the construction of semantic networks to their comparison with reference models and aggregation of results. Each of these steps is implemented by interacting with a large language model through structured queries. However, to ensure the consistency, reproducibility, and scalability of the analysis, it is necessary to formalize this process as an intelligent framework based on the concept of codeless programming.

Codeless programming in this context refers to the construction of complex analytical systems by composing simple but functionally defined primitives that control the behavior of LLM similarly to operations in conventional programming languages. This approach makes it possible to design analytical processes without the need to write code, using only semantically structured instructions that reflect the logic of calculations.

5. 5. Implementing the codeless programming method based on logical primitives

5. 5. 1. Codeless method primitives and examples of their application

The method is based on three basic primitives: "Condition", "Loop" and "Function", which model key programming constructs and can be implemented through the corresponding prompts.

"Condition" primitive (If-Else)

The primitive models conditional branching. Let:

– *Input* – input data (text, parameter, object of analysis);

– *C*(*Input*) – predicate (logical condition) that returns True or False;

– A_1, A_2 – two alternative actions (for example, different prompts or analytical procedures).

Then the prompt function is defined as:

$$P(Input)=\begin{cases} A_{True}, \text{if } C(Input)=True \\ A_{False}, \text{othewise} \end{cases}. \qquad (10)$$

For example, the system can analyze whether a message contains emotionally charged terms (condition *C*), and depending on this, apply different analysis templates – for neutral texts or for propaganda narratives.

The "For-Loop" primitive.

This primitive provides iterative processing of a set of elements. Let

– $S=\{s_1, s_2, \ldots, s_n\}$ be a set of objects (text fragments, topics, messages);

– *F* be an operation applied to each element.

Then the overall result is defined as

$$P(S)=\bigcup_{i=1}^{n} F(s_i). \qquad (11)$$

The primitive is implemented by an instruction of the type:

"For each paragraph in the text, perform operation *F*, then combine all the results into a single structure."

This makes it possible to process long texts by breaking them into parts, analyzing each one separately (to avoid restrictions on the length of the context) and collecting the results into a single semantic network.

The "Function" primitive.

The primitive makes it possible to devise reusable analytical procedures. Let

– $F{:}X \rightarrow Y$ be a function that converts elements from the set *X* (for example, text) into elements of the set *Y* (for example, a JSON structure);

– $x \in X$ be an input argument;

– *parameter* be a parameter that controls the behavior of the function.

The function is implemented through a template

$$F_{extract}(x, parameter)= \\ = Promt(x, instruction\ with\ parameter). \qquad (12)$$

For example, the $F_{extract}$ function can extract concepts and relationships from text according to various parameters: "highlight strategies", "find emotional triggers", "build a cause-and-effect chain".

Prompt composition as abstract programming.

The analysis system is built by composing primitives, which forms a structure similar to an abstract syntax tree (AST)

$$Prompt ::= \\ = Primitive / (Promt \oplus Promt) \,|\, \text{if } (Prompt, Prompt), \qquad (13)$$

where ⊕ is a union operation (for example, sequential execution of two prompts), if – conditional branching between two analytical paths.

Such a composition makes it possible to implement complex analytical scenarios, such as:

– construction of a semantic network from a long text (cycle + function);

– comparison with several standards (cycle on a collection);

– ensemble analysis through a "swarm of virtual experts" (cycle + condition).

Implementation of key analysis steps using the described primitives includes the following stages:

1. Extraction of concepts and relationships: $F_{extract}$ function.

Let the input text be:

«Росія проводить інформаційну операцію через поширення фейкових новин, щоб викликати страх серед населення.» ("Russia is conducting an information operation through the spread of fake news to cause fear among the population.")

The following function is applied:

$$F_{extract}(text, \text{"concepts and connections"}), \qquad (14)$$

The result of which is a structured output in JSON format of the type:

```
{
    "nodes": [
                {"id": "Росія", "type": "актор"},
                {«id»: «інформаційна операція», «type»: «стратегія»},
                {«id»: «фейкові новини», «type»: «метод»},
                {«id»: «страх», «type»: «реакція»}
    ],
    «edges»: [
                {«source»: «Росія», «target»: «інформаційна операція», «relation»: «здійснює»},
                {«source»: «інформаційна операція», «target»: «фейкові новини», «relation»: «використовує»},
                {«source»: «фейкові новини», «target»: «страх», «relation»: «викликає»}
    ]
}
```

Performing this function is the first step in building a semantic network that allows LLMs to "structure" text.

2. Combining results: function *P*(*S*)

Let the text be made up of two fragments:

– «Росія поширює дезінформацію.» ("Russia is spreading disinformation.")

– «Це викликає паніку серед громадян.» ("This causes panic among citizens.")

Cyclic processing is used:

– $F_{extract}(s_1)$ → {«Росія»→ «дезінформація»};

– $F_{extract}(s_2)$ → {«дезінформація»→ «паніка»}.

As a result of the merger, we get the record:

```
{
        "nodes": ["Росія", "дезінформація", "паніка"],
        "edges": [
                {"source": "Росія", "target":
"дезінформація", "relation": "поширює"},
                {"source": "дезінформація", "target":
"паніка", "relation": "викликає"}
        ]
}
```

The function allows $P(S)$ to scale analysis to long texts, documents, or collections of messages.

The proposed method of codeless programming has several advantages, in particular:

– it does not require programming skills, which makes it suitable for a wide range of specialists;

– it makes it possible to quickly modify analytical queries by changing parameters or structured prompts;

– it makes it possible to observe the step-by-step execution of tasks by a person, increasing the reliability of the information generated;

– it enables reproducibility and standardization of the analysis process.

Integration with LLM: it uses the power of modern language models as an "executor" of analytical operations.

5. 5. 2. Analytical cycle for determining potential signs of informational and psychological influences

To demonstrate the efficiency of the proposed method of codeless programming, a full analytical cycle is implemented on the example of a text containing potential signs of informational and psychological influences. The process is built as a sequence of stages, each of which is implemented using one or more primitives of the codeless method: "Function", "Cycle", "Condition", and also integrates the concept of "swarm of virtual experts" and aggregation of results. This approach ensures the systematicity, reproducibility, and interpretability of analysis.

The following message was used to demonstrate the analytical cycle:

«Росія проводить інформаційну кампанію через соцмережі, щоб формувати образ ворога. Мета – викликати страх і дезорганізацію суспільства». ("Russia is conducting an information campaign through social networks to shape the image of the enemy. The goal is to cause fear and disorganization of society.")

This text is the input data for all subsequent stages: building a semantic network, comparing with standards, and aggregating results.

The goal of the analysis is to determine how well this text corresponds to known patterns of information and propaganda operations, using a combination of structural semantic analysis and comparison with reference models.

Stage 1. Extraction of concepts and relationships (*primitive "Function"*).

The first step is to apply the $F_{extract}$ function, which extracts key concepts and their relationships from the text. This operation is implemented through a prompt that indicates to LLM the need for a structured representation of the semantics of the text.

The result of testing the $F_{extract}$ function:

```
{
        "nodes": [
                {"id": "Росія", "type": "актор"},
                {"id": "інформаційна кампанія", "type":
"стратегія"},
                {"id": "соцмережі", "type": "канал"},
                {"id": "образ ворога", "type": "мета"},
                {"id": "страх", "type": "емоція"},
                {"id": "дезорганізація", "type":
"наслідок"}
        ],
        "edges": [
                {"source": "Росія", "target":
"інформаційна кампанія", "relation": "здійснює"},
                {"source": "інформаційна кампанія",
"target": "соцмережі", "relation": "через"},
                {"source": "соцмережі", "target": "образ
ворога", "relation": "формують"},
                {"source": "образ ворога", "target":
"страх", "relation": "викликає"},
                {"source": "страх", "target":
"дезорганізація", "relation": "призводить до"}
        ]
}
```

The resulting structure is a semantic network of the analyzed message, which reflects its internal logic of influence.

Stage 2. Processing of multi-fragment text (*primitive "Cycle"*).

In the case when the input text is long or consists of several independent fragments, the primitive "Cycle" is used. Let's consider an example where the text is divided into two fragments:

– fragment 1: «Росія проводить інформаційну кампанію через соцмережі.» ("Russia is conducting an information campaign through social networks.");

– fragment 2: «Мета – формувати образ ворога.» ("The goal is to shape the image of the enemy.").

$F_{extract}$ is applied to each fragment separately, after which the results are combined into a single network using the operation

$$P(S)=\bigcup_{i=1}^{n} F(s_i). \qquad (15)$$

This avoids the limitations on the length of the context and provides a more accurate analysis.

The result of the union remains identical in structure to G_1 but is obtained by composing partial analytical solutions.

Stage 3. Comparison with the reference network (*Compare*).

At this stage, the semantic network of the analyzed message G_1 is compared with two reference models:

– G_2 – a generalized network reconstructed from the internal knowledge of LLM;

– G_3^* – a generalized semantic network built on the basis of a training collection of known IPSOs.

The comparison with G_3^* reflects a typical narrative of a disinformation campaign: "IPSO" → "fake news" → "fear" → "uncertainty". The semantic network of the analyzed message G_1 takes the form: "Russia" → "information campaign" → "social networks" → "image of the enemy" → "fear" → "disorganization".

In the first step, a lexical comparison is performed, which demonstrates low similarity due to the divergence of formulations. However, this approach ignores the semantic proximity of concepts. Therefore, for accurate analysis, semantic normalization is used using embedded vectors:

1. Semantic normalization of concepts.

Each concept from V_1 (G_1 vertices) is compared with all vertices V_3 (vertices) by cosine similarity. The most similar pairs are given in Table 2.

Table 2

List of the most similar pairs of concepts

Concept G_1	Most similar to G_3^*	Similarity
Information campaign	IPSO	0.87
Fake news (implicitly through «social media» → «image of the enemy»)	Fake news	0.78
Fear	Fear	1.00
Disorganization	Uncertainty	0.82

The concept "Russia" has no analog in G_3^*, the "social networks" and "image of the enemy" partially correspond to the "fake news" link due to the context.

2. Calculation of similarity of sets of vertices $J_{emb}\left(V_1, V_3^*\right)$.

The vector-weighted Jaccard coefficient with a threshold of θ = 0.65 is used. Concepts with $sim \geq \theta$ are considered similar. The number of semantically comparable concepts is 4 (out of 7 in G_1)

$$J_{emb}\left(V_1, V_3^*\right) = \begin{pmatrix} 0.87+0.87+ \\ +1.00+0.82 \end{pmatrix} / 9 \approx 0.386. \tag{16}$$

3. Calculation of structural similarity $S\left(E_1, E_3^*\right)$.

The overall structural similarity is defined as the ratio of the number of agreed causal relationships to the maximum possible number. 2 significant correspondences were found:

– "fake news"→"fear" (in G_3^*) corresponds to the image of "enemy"→"fear" (in G_1);

– "fear"→"uncertainty" corresponds to "fear"→"disorganization".

Thus, $S\left(E_1, E_3^*\right) = 2/4 = 0.50.$

4. Calculation of the similarity of causal paths S_{path}.

The key causal chains are highlighted:

$P_1 \subset G_1$: "information campaign" → "image of the enemy" → "fear" → "disorganization".

$P_3 \subset G_3^*$: "IPSO" → "fake news" → "fear" → "uncertainty".

The similarity of the paths is calculated as the average value of the cosine similarities of the corresponding vertices

$$S_{path} = \left(P_1, P_3\right) = \begin{pmatrix} 0.87+0.75+ \\ +1.00+0.82 \end{pmatrix} / 4 = 0.86. \tag{17}$$

5. Formation of the generalized assessment p_c.

S_{path} is used as an additional component to $S\left(E_1, E_3^*\right)$ (1). Let us assume:

– α = 0.5 – balance between semantics and structure;

– β = 0.4 – since S_{path} is more significant than the general structure for IPSO.

Then

$$\begin{aligned} p_c &= 0.5 + 0.386 + \\ &+ 0.5 \cdot \left[0.4 \cdot 0.50 + 0.60 \cdot 0.86\right] = 0.551. \end{aligned} \tag{18}$$

Thus, the final answer: p_c = 0.55, which indicates a moderate similarity of the analyzed message with known IPSO patterns. Despite the lexical difference, semantic normalization and analysis of causal paths allow us to identify a common logic of psychological impact: "forming the image of the enemy" → "inducing fear" → "destabilizing society".

Stage 4. Analysis through a swarm of virtual experts.

To increase reliability, the analysis is performed on behalf of four virtual experts (Table 3), each of which activates a different cognitive context in LLM:

– linguistic analyst (focus on style, vocabulary, rhetorical techniques);

– disinformation specialist (search for known IPSO patterns);

– mass communication psychologist (analysis of emotional triggers);

– media sociologist (assessment of impact on public opinion).

Table 3

Result of analysis by virtual experts

Expert	Score (0–1)	Is it IPSO?
Linguist	0.7	Yes
Disinformation	0.8	Yes
Psychologist	0.75	Yes
Sociologist	0.65	Yes

Mean score

$$p_{LLM} = 40.7 + 0.8 + 0.75 + 0.65 = 0.725, \tag{19}$$

indicates a high probability of belonging to the IPSO from the point of view of internal knowledge of LLM.

Stage 5. Aggregation of results (*Agg*).

At the final stage of the analysis, the aggregation of partial estimates obtained in the previous steps is performed in order to form a single generalized estimate p_{final}, which characterizes the degree of belonging of the analyzed message to the class of information and propaganda operations. This stage integrates various types of analytical information: the results of structural comparison with the generalized semantic network of the training collection and estimates obtained from the "swarm of virtual experts" based on internal knowledge of LLM.

The final estimate p_{final} is calculated using the weighted average formula

$$p_{final} = \beta \cdot p_c + \left(1 - \beta\right) \cdot p_{LLM}, \tag{20}$$

where, as calculated earlier:

– p_c = 0.55 – similarity score of the analyzed message with the generalized semantic network of the training collection G_3*, obtained at stage 3 taking into account semantic normalization of concepts, structural similarity and comparison of causal paths;

– p_{LLM} = 0.725 – average score from the "swarm of virtual experts" (linguist, disinformation specialist, psychologist, sociologist), reflecting the consistency of the conclusions of the internal knowledge of the LLM with the classification of the message as IPSO;

– β ∈ [0,1] – weight coefficient reflecting the degree of trust in the training collection in a specific context. In the given example, β = 0.55 is taken, which indicates equal importance of both sources of knowledge.

Substituting the values, we obtain

$$p_{final} = 0.5 + 0.55 + 0.5 + 0.725 = 0.6375. \quad (21)$$

The resulting generalized estimate $p_{final} = 0.6375$ is interpreted according to the established thresholds.

Since 0.6375 falls within the range [0.4; 0.7], it is concluded that the analyzed message is potentially part of IPSO. This indicates the presence of typical patterns of psychological influence in the text – in particular, the formation of an enemy image, instilling fear and predicting the destabilization of society – but requires additional contextual analysis for the final classification. The result is summarized in Table 4.

Table 4

Relationship between input data, methodology, and results (Case 1)

Component	Description
Inputs	"Russia is conducting an information campaign through social media to shape the image of the enemy. The goal is to cause fear and disorganization in society"
Methodology	Codeless prompt implemented through primitives: – $F_{extract}$→ building a semantic network G_1; – «swarm of virtual experts» → score p_{LLM}; – comparison with the generalized network of the training collection G_3→ score p_c

Outputs	– semantic network G_1 (See JSON in Stage 1);
	– p_c = 0.55 (Stage 3);
	– p_{LLM} = 0.725 (Stage 4);
	– p_{final} = 0.6375(Stage 5);
	– classification: «Potentially part of IPSO»

5. 5. 3. Implementing an evaluation method based on codeless programming

The following is a codeless prompt for detecting whether a message is IPSO, built according to the rules above:

You are an analyst working within the framework of a codeless method for detecting signs of information and propaganda operations (IPSO). Your goal: to analyze the incoming message using a structured sequence of logical primitives: "Function", "Cycle", "Condition", "Aggregation". Follow a clear sequence of steps. Do not perform any actions outside this algorithm.

Text for analysis: "Text for analysis".

1. Function: $F_{extract}$ – construction of semantic network G_1.

Do:

– highlight all key concepts (subjects, actions, consequences) from "Text for analysis";

– establish cause-and-effect relationships between them;

– construct semantic network G_1 as a list of triples: "source" → "relationship" → "target";

– normalize concepts: replace synonyms with generalized terms (for example: "fakes" → "disinformation" → "fear" → "emotional trigger").

Result: $G_1 = \left[\text{list of normalized triples}\right]$.

2. Cycle: $P(S)$ – building a generalized network based on LLM.

Perform the cycle for each of the following virtual experts:

1. Linguistic analyst.
2. Disinformation specialist.
3. Mass communication psychologist.
4. Media sociologist.

For each expert:

– activate the appropriate cognitive context;

– ask: "What key concepts and cause-and-effect chains are characteristic of IPSO in this context?";

– write the answer as a partial semantic network G_2 expert;

– normalize the concepts according to the same rule as in G_1.

After completing the cycle:

– merge all partial networks into a single generalized network G_2;

– save all nodes and links.

Result: $G_2 = \left[\text{integrated network based on LLM}\right]$.

3. Function: $Compare(G_1, G_2)$ – comparison with the LLM network.

Do:

– for each vertex v in G_1, find the most similar vertex υ in G_2 using cosine similarity embeddings;

– if similarity ≥ 0.65, consider concepts comparable;

– calculate $J_{emb}\left(V_1, V_2\right)$ – vector-weighted Jaccard coefficient between sets of vertices;

– calculate $S\left(E_1, E_2\right)$ – fraction of consistent causal relationships;

– calculate S_{path} – similarity of the most important causal paths (e.g., "disinformation" → "fear" → "destabilization").

Result:

$$p_{LLM} = \alpha \cdot J_{emb} + (1-\alpha) \cdot \left[\beta \cdot S\left(E_1, E_2\right) + (1-\beta) \cdot S_{path}\right].$$

(Apply α = 0.6, β = 0.4, unless otherwise specified).

4. Function: $Compare\left(G_1, G_3^*\right)$ – comparison with the training collection.

Do:

– the training collection contains a generalized semantic network G_3^*, which reflects typical IPSOs: G_3^*, "IPSO" → "disinformation" → "image of the enemy" → "fear" → "uncertainty";

– repeat the same process as in p. 3, but compare G_1 with G_3^*;

– calculate $J_{emb}\left(V_1, V_3^*\right), S\left(E_1, S_3^*\right), S_{path}\left(G_1, G_3^*\right)$.

Result: $p_C = \alpha \cdot J_{emb} + (1-\alpha) \cdot \left[\beta \cdot S\left(E_1, E_3^*\right) + (1-\beta) \cdot S_{path}\right]$.

(Use the same values of α and β)

5. Cycle: *P*(*experts*) – analysis of a "swarm of virtual experts".

For each of the four experts (from item 4) perform:

– ask the question: "Does the 'Text for analysis' contain signs of IPSO? Score from 0 to 1."

– write the answer as $p_{expert} \in \left[0,1\right]$.

After completing the cycle:

– calculate the average: $p_{LLM} = \left(p_1 + p_2 + p_3 + p_4\right) / 4$.

6. Condition: Validate the results.

If $p_c < 0.3$ and $p_{LLM} < 0.4$:

– output: "Low probability of IPSO. Data does not confirm the presence of systemic psychological influence";

– stop the process.

Otherwise:

– go to stage 7.

7. AGGREGATION: $p_{final} = \beta \cdot p_C + \left(1-\beta\right) \cdot p_{LLM}$.

Do:

– Calculate the final score p_{final}, using β = 0.5 (equal weight for training collection and LLM).

Apply threshold classification:

If $p_{final} > 0.7$:

– Conclusion: "High probability of belonging to IPSO."

If $0.4 \leq p_{final} \leq 0.7$:

– Conclusion: "Potentially part of IPSO. Contextual refinement recommended."

If $p_{final} < 0.4$:

– Conclusion: "Low probability of belonging to IPSO."

8. Conclusion.

Provide a concise conclusion in the format:

– p_c score:[value];

– p_{LLM} score:[value];

– p_{final} score:[value];

– classification: [conclusion];

– key features: [list of concepts or pathways that led to the conclusion].

Note: Follow all steps sequentially. Do not skip any primitive. Use only built-in knowledge and logic. Do not go beyond this prompt.

This prompt could be used without any programming. It is enough to insert it into LLM (e.g., ChatGPT, Claude, Qwen) together with real text instead of "Text for analysis". It provides consistency, reproducibility, and interpretability, which are key requirements of our methodology.

5. 5. 4. Testing the algorithm on the example of a propaganda message

As input data for testing the algorithm on a more complex example, a propaganda message from a fake source was used:

«Українська версія (переклад для ілюстрації): Доскакались! Після мітінгів української діаспори в сша трамп ініціює висилання українських мігрантів заморсь Жовті сливи • 02.03.2025 https:/slivy.news/author/kitty2/ Про чемодан вокзал. У заяві йдеться: ‹Організатори мітингів – кримінальна мережа з України з центрами в Чикаго, Вірджинії та Пенсільванії, що займається легалізацією українців, які в'їжджають за туристичними візами й не виїжджають, маючи на руках спеціальні документи. Усі вони – порушники законодавства›. Ну що ж, біженці так прагнули підтримати Україну! Тепер у них з'явиться шанс – ЗСУ гостро потребують «пушечного м'яса», а цих навіть ловити не потрібно: мобілізуватимуть прямо на кордоні. І ось що дивно: чомусь ми не чуємо змагарського виття через «несправедливе вигнання» з країни». ("Ukrainian version (translation for illustration): Get on it! After the rallies of the Ukrainian diaspora in the USA, Trump initiates the deportation of Ukrainian migrants abroad Yellow Plums • 02.03.2025 https:/slivy.news/author/kitty2/ About a suitcase at the station. The statement says: 'The organizers of the rallies are a criminal network from Ukraine with centers in Chicago, Virginia and Pennsylvania, which is engaged in the legalization of Ukrainians who enter on tourist visas and do not leave, having special documents in their hands. All of them are violators of the law.' Well, the refugees were so eager to support Ukraine! Now they will have a chance – the Armed Forces of Ukraine are in dire need of "cannon fodder", and they don't even need to be caught: they will be mobilized right at the border. And here's what's strange: for some reason we don't hear any competitive howls because of the "unfair expulsion" from the country ").

This text is the basis for building the semantic network given in Table 5 and Fig. 1 and is used for all further calculations. In Fig. 1, nodes are normalized concepts (for example, "image of the enemy", "emotional trigger"), edges are cause-and-effect relationships identified by the "swarm of virtual experts" method. The structure corresponds to the format of a directed acyclic graph, where each edge reflects the causal relationship "cause" → "effect".

The result is: $p_{final} = 0.610$; $p_{LLM} = 0.825$; $p_{final} = 0.7175$.

Threshold classification: $p_{final} = 0.7175 > 0.7$ – "High probability of belonging to IPSO."

The results of our method performance are summarized in Table 6.

Key features: fake statement about Trump, accusation of diaspora in crime, dehumanization of migrants ("cannon fodder"), fear-mongering, sarcastic portrayal of the opposition, creation of an enemy image.

Table 5

List of related pairs of concepts

Concept 1 (in Ukrainian)	Concept 1	Concept 2 (in Ukrainian)	Concept 2
1	2	3	4
фейкові ЗМІ	fake media	вигадана політична реакція	fictional political reaction
вигадана політична реакція	fictional political reaction	демонізація діаспори	demonization of the diaspora
демонізація діаспори	demonization of the diaspora	образ ворога	image of the enemy
образ ворога	image of the enemy	емоційний тригер	emotional trigger
емоційний тригер	emotional trigger	відчуття зради	sense of betrayal
відчуття зради	sense of betrayal	маніпуляція громадською думкою	manipulation of public opinion
маніпуляція громадською думкою	manipulation of public opinion	дискредитація підтримки України	discrediting support for Ukraine
дискредитація підтримки України	discrediting support for Ukraine	послаблює міжнародну підтримку	weakens international support
українська діаспора	Ukrainian diaspora	мітинги в США	rallies in the USA

Continuation of Table 5

1	2	3	4
мітинги в США	rallies in the USA	Трамп	Trump
Трамп	Trump	депортація мігрантів	deportation of migrants
організатори мітингів	organizers of the meetings	кримінальна мережа	criminal network
кримінальна мережа	criminal network	нелегальна легалізація	illegal legalization
нелегальна легалізація	illegal legalization	закон США	US law
мітинги	rallies	посилення репресивних заходів	intensification of repressive measures
депортація мігрантів	deportation of migrants	мобілізація на кордоні	mobilization at the border
мобілізація на кордоні	mobilization at the border	дешевизна людського життя	cheap human life
дешевизна людського життя	cheap human life	демонізує ЗСУ	demonizes the Armed Forces of Ukraine
прихильники України	supporters of Ukraine	несправедливе вигнання	unjust expulsion
прихильники України	supporters of Ukraine	репресії	repression
емоційна мобілізація	emotional mobilization	провокація	provocation
провокація	provocation	стилізація під ЗМІ	stylization by the media
стилізація під ЗМІ	stylization as media	іронія	irony
іронія	irony	емоційна мобілізація	emotional mobilization
емоційна мобілізація	emotional mobilization	злочин	crime
фейкові ЗМІ	fake media	вигадана політична реакція	fictional political reaction
вигадана політична реакція	fictional political reaction	демонізація діаспори	demonization of the diaspora
демонізація діаспори	demonization of the diaspora	дискредитація підтримки України	discrediting support for Ukraine
емоційний тригер	emotional trigger	відчуття зради	sense of betrayal
відчуття зради	sense of betrayal	гнів проти діаспори	anger against the diaspora
гнів проти діаспори	anger against the diaspora	образ ворога	image of the enemy
образ ворога	image of the enemy	внутрішній розкол	internal division
маніпуляція громадською думкою	manipulation of public opinion	поділ суспільства	division of society
поділ суспільства	division of society	зниження довіри до українських інституцій	decreased trust in Ukrainian institutions
зниження довіри	decline in trust	послаблює міжнародну підтримку	weakens international support

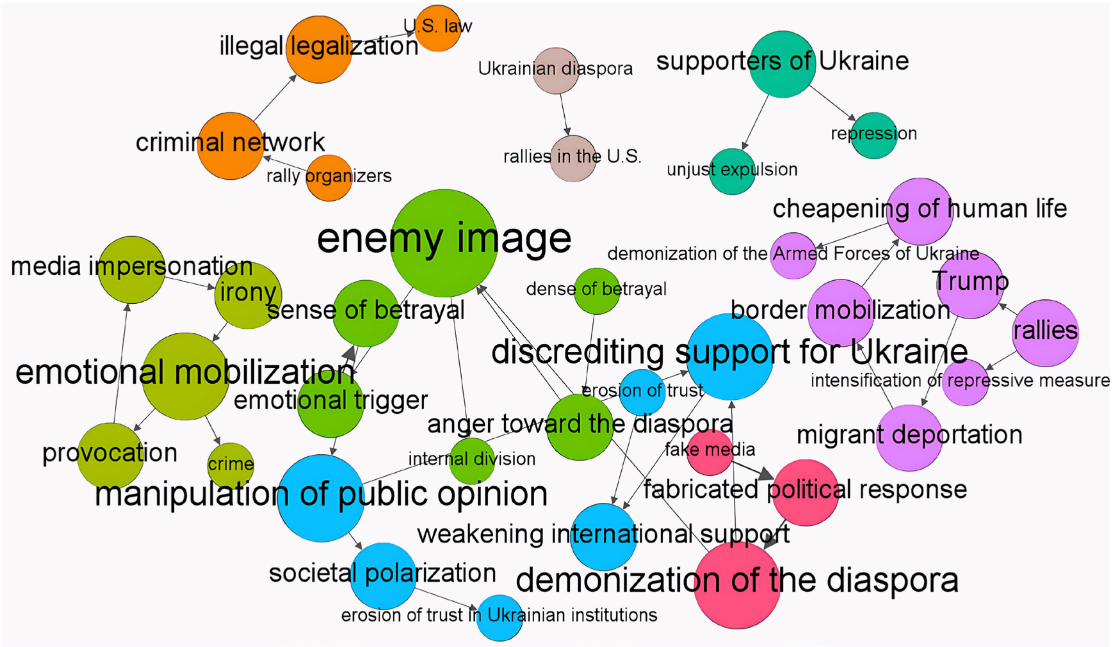

Fig. 1. Semantic network built on the basis of the message about "Ukrainian diaspora rallies in the USA"

The message corresponds to a typical IPSO pattern: "disinformation" → "enemy image" → "fear" → "destabilization".

Thus, the message contains typical IPSO features, in particular, the formation of an enemy image among the diaspora and manipulation of emotions to discredit support for Ukraine. Although the structural similarity with the reference network is moderate, LLM's internal intuition indicates a high probability of propaganda influence. Additional contextual research into the source and purpose of dissemination is recommended [10].

Table 6

Relationship between input data, methodology, and results (Case 2)

Component	Description
Inputs	«Message from a fake source about «Ukrainian diaspora rallies in the USA...»
Methodology	Codeless prompt implemented through primitives: – $F_{extract}$→ building a semantic network G_1; – «swarm of virtual experts» → score p_{LLM}; – comparison with the generalized network of the training collection G_3→ score p_c

Outputs	– semantic networkG_1 (refer to Table 5);
	– p_c = 0.61 (Stage 3);
	– p_{LLM} = 0.825 (Stage 4);
	– p_{final} = 0.7175(Stage 5);
	– classification: «High probability of belonging to IPSO»

6. Codeless method for determining signs of informational-psychological operations: discussion

Our results allow us to conclude that the proposed codeless method effectively detects signs of informational-psychological operations by reconstructing their internal semantic structure.

The sources of the formation of the collection of fake messages were determined, as well as a set of metadata (Table 1), the use of which provides deep segmentation of information patterns. The collected collection became the basis for building a generalized reference network, constructed on the basis of the logical primitives "Condition" (If-Else), "Cycle" (For-Loop), and "Function", which was then compared with the knowledge base of large language models. The results of using the algorithm for building a semantic network can be clearly seen in Table 5 and Fig. 1, which allowed us to highlight key concepts, for example, "image of the enemy".

The results of comparing semantic networks with the internal knowledge of large language models demonstrated the high efficiency of the combined similarity function (1) to (6). The use of the Jaccard vector coefficient (3) allowed for comparison not only at the level of lexical coincidences but also by deep semantics. As shown in Table 2, even in the absence of direct lexical correspondence between the concepts of "image of the enemy" and "fake news", the level of semantic similarity was 0.78. This indicates adequate recognition of equivalent semantic structures and confirms the feasibility of using embeddings-representation as a basis for semantic normalization.

The application of the concept of a swarm of virtual experts (Table 3) demonstrated the consistency of the assessments between different cognitive analysis profiles. The obtained values (linguist – 0.70, psychologist – 0.75, disinformation specialist – 0.8, sociologist – 0.65) gave an average score of 0.725 according to (19), which indicates a high probability of the analyzed text belonging to an informational-psychological operation. These results confirm that the system is able to objectively integrate different points of view and detect signs of manipulation regardless of the specific subject area. This approach provides a multidimensional perception of the results, when the emotional, cognitive, and social contexts are assessed in a consistent manner, which is especially valuable for practical media monitoring.

The proposed method solves several key problems.

First, it eliminates the dependence on annotated data, which limits the application of conventional ML methods [1, 7]. Instead, the internal knowledge of large language models is used as a dynamic source of generalized IPSO patterns. Thanks to this, the model can adapt to new rhetorical tactics without additional training. Integration is achieved, in particular, by using (8).

Second, the method automates the construction of semantic networks without the need for manual coding or expert markup. Due to the formalization of the process, a reproducible mechanism for constructing cause-and-effect chains is designed, which is scalable and suitable for processing large data sets. This eliminates the limitations inherent in classical graph methods [5, 6] and allows for analytics in a code-free environment.

Third, it provides flexible adaptation to new disinformation tactics through the combination of an external training collection $\left(G_3^*\right)$ and internal semantic intuition of LLM (G_2), which compensates for the shortcomings of static classifiers [8, 9].

Unlike hybrid models such as GBERT [8], which combine BERT and GPT only for classification, the proposed method models the holistic narrative of IPSO in the form of an interpreted semantic network (Table 5, Fig. 1). This makes it possible not only to detect fakes but also understand the mechanism of psychological influence, for example, how the formation of an "image of the enemy" leads to a "sense of betrayal" and subsequent "splitting of society". Such interpretability is a critical advantage in the context of media literacy, education, and strategic analysis.

However, our study has certain limitations that must be taken into account in practical application. First, the method is limited only to text content and does not take into account multimodal elements (images, videos), which are often key in modern disinformation [11]. Second, semantic normalization of concepts is based on the cosine similarity of embeddings according to formula (2), which can lead to false agreements in cases of polysemy or culturally specific metaphors. Thirdly, the weight coefficients (α, β) in aggregation functions (8) are set empirically, which reduces the adaptability of the system to different contexts (for example, military propaganda and medical disinformation).

Among the shortcomings that should be noted is the dependence on the quality of LLMs. In the case of using outdated or biased models, a systematic error may occur in the reconstruction of reference networks. In addition, the method implies expert validation of the final results since LLM can generate logically plausible but actually false connections which is consistent with [17].

Further studies may investigate three areas: integration of multimodal analysis, which could make it possible to take into account visual and audio markers of disinformation; automatic calibration of weighting coefficients based on the context of the message (topic, geography, source), which would increase the accuracy of aggregation; expansion of the taxonomy of disinformation by including new types of manipulations (for example, "information fatigue", "algorithmic polarization"), which is relevant in the context of the evolution of information threats.

Thus, the proposed method not only resolves the identified problems but also opens up new opportunities for human-oriented analysis of disinformation, where AI acts not as a “black box” but as a tool of cognitive partnership.

7. Conclusions

1. A training collection of fake messages based on English-language sources was formed, which became a reference base for comparison. The collection contains materials from social networks, news outlets, research archives, search engines, etc., and is also accompanied by a certain set of metadata.

2. Using the approach devised, examples of semantic network G_1 were obtained: based on the analyzed message in JSON format (chapter 5. 5. 2), which reflects the cause-and-effect logic of influence: “Russia” → “information campaign” → “social networks” → “image of the enemy” → “fear” → “disorganization”, as well as for the case with a more pronounced influence of IPSO. This makes it possible to move from lexical analysis to structural modeling of narratives, which increases the accuracy and explainability of the results compared to conventional NLP methods. The application of the “Cycle” primitive to combine partial semantic networks in the case of long or multipart texts has been demonstrated. This eliminates the limitation on the length of the context and preserves the logical integrity of the analysis, which increases the reproducibility of the method.

3. Using the developed algorithms, G_1 was compared with models obtained from LLM (G_2) and the training collection of IPSOs $\left(G_3^*\right)$. After semantic normalization and calculation of metrics: $J_{emb} = 0.386$, structural similarity $S\left(E_1, E_3^*\right) = 0.50$, similarity of causal paths $S_{path} = 0.86$, generalized score $p_c = 0.55$. This showed that even with different wordings of the message it retains a common logic of psychological impact with known IPSOs.

4. A function of aggregation of scores from four independent expert profiles (linguist, disinformation specialist, psychologist, sociologist) has been proposed to detect signs of IPSOs in messages. The function in the form of a weighted average was tested on two test cases, in which values $p_{final} = 0.6375$ and $p_{final} = 0.7175$ were obtained. Its use confirmed the ability of the method to capture a typical propaganda pattern: “disinformation” → “image of the enemy” → “fear” → “destabilization”.

5. A codeless programming method has been proposed and tested, which provides: systematicity and reproducibility of analysis thanks to the primitives “Function”, “Cycle”, “Condition”, “Aggregation”; integration of external (training collection) and internal (LLM) sources of knowledge; quantitative assessment of the similarity of narratives; interpretability of results, which makes the method suitable for use in media monitoring, strategic communications, and media literacy training.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study, as well as the results reported in this paper.

Funding

The research was carried out with grant support from the National Research Foundation of Ukraine (Project registration number 2023.04/0087).

Data availability

The manuscript has associated data in the data warehouse.

Use of artificial intelligence

The authors used artificial intelligence technologies within the permissible framework in terms of working with prompts and searching for literary sources. In particular, large language models were used to build examples of semantic networks and demonstrate the work of the code-free method (Chapter 5). AI was used as a tool for auxiliary analytical modeling and generation of prompts, without automatically writing the main text of the paper.

Acknowledgement

We thank the Armed Forces of Ukraine for the opportunity to conduct studies in independent Ukraine.

References

1. Hassan, S. U., Ahamed, J., Ahmad, K. (2022). Analytics of machine learning-based algorithms for text classification. Sustainable Operations and Computers, 3, 238–248. https://doi.org/10.1016/j.susoc.2022.03.001
2. Zgurovsky, M., Lande, D., Dmytrenko, O., Yefremov, K., Boldak, A., Soboliev, A. (2023). Technological Principles of Using Media Content for Evaluating Social Opinion. System Analysis and Artificial Intelligence, 379–396. https://doi.org/10.1007/978-3-031-37450-0_22
3. Ahmad Tamerin, A. S., Bakar, N. A. A., Hassan, N. H., Maarop, N. (2023). Counter-Narrative Cyber Security Model to Address the Issues of Cyber Terrorism. Open International Journal of Informatics, 11 (1), 96–113. https://doi.org/10.11113/oiji2023.11n1.30
4. Lande, D., Strashnoy, L. (2025). Semantic AI Framework for Prompt Engineering. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5172867
5. Lande, D., Strashnoy, L. (2025). Advanced Semantic Networking based on large language models. Kyiv: Engineering, 264.
6. Kingdon, A. (2021). The Meme Is the Method: Examining the Power of the Image Within Extremist Propaganda. Researching Cybercrimes, 301–322. https://doi.org/10.1007/978-3-030-74837-1_15
7. Guleria, P. (2024). NLP-based clinical text classification and sentiment analyses of complex medical transcripts using transformer model and machine learning classifiers. Neural Computing and Applications, 37 (1), 341–366. https://doi.org/10.1007/s00521-024-10482-x

8. Dhiman, P., Kaur, A., Gupta, D., Juneja, S., Nauman, A., Muhammad, G. (2024). GBERT: A hybrid deep learning model based on GPT-BERT for fake news detection. Heliyon, 10 (16), e35865. https://doi.org/10.1016/j.heliyon.2024.e35865
9. Piña-García, C. A. (2025). In-context learning for propaganda detection on Twitter Mexico using large language model meta AI. Telematics and Informatics Reports, 19, 100232. https://doi.org/10.1016/j.teler.2025.100232
10. Liu, Z., Zhang, T., Yang, K., Thompson, P., Yu, Z., Ananiadou, S. (2024). Emotion detection for misinformation: A review. Information Fusion, 107, 102300. https://doi.org/10.1016/j.inffus.2024.102300
11. Hu, L., Wei, S., Zhao, Z., Wu, B. (2022). Deep learning for fake news detection: A comprehensive survey. AI Open, 3, 133–155. https://doi.org/10.1016/j.aiopen.2022.09.001
12. Aïmeur, E., Amri, S., Brassard, G. (2023). Fake news, disinformation and misinformation in social media: a review. Social Network Analysis and Mining, 13 (1). https://doi.org/10.1007/s13278-023-01028-5
13. Barabash, O. V., Hryshchuk, R. V., Molodetska-Hrynchuk, K. V. (2018). Identification threats to the state information security in the text content of social networking services. Science-Based Technologies, 38 (2). https://doi.org/10.18372/2310-5461.38.12855
14. Lande, D., Hyrda, V. (2024). Use of large language models to identify fake information. Collection “Information Technology and Security,” 12 (2), 236–242. https://doi.org/10.20535/2411-1031.2024.12.2.315743
15. Strashnoy, L., Lande, D. (2024). Implementation Of The Concept Of A “Swarm Of Virtual Experts” In The Formation Of Semantic Networks In The Field Of Cybersecurity Based On Large Language Models. https://doi.org/10.2139/ssrn.4978924
16. Hryshchuk, R., Molodetska, K., Syerov, Y. (2019). Method of improving the information security of virtual communities in social networking services. CEUR Workshop Proceedings. Available at: https://ceur-ws.org/Vol-2392/paper3.pdf
17. Abels, A., Lenaerts, T. (2025). Wisdom from Diversity: Bias Mitigation Through Hybrid Human-LLM Crowds. Proceedings of the Thirty-Fourth International Joint Conference on Artificial Intelligence, 321–329. https://doi.org/10.24963/ijcai.2025/37