Security of Infocommunication Systems and Internet of Things

2026 Vol 4, No 1

https://doi.org/10.31861/sisiot2026.1.01007

Received 30 March 2026; revised 09 April 2026; accepted 12 June 2026; published 30 June 2026

Evaluating Information Sources on Social Media: A Systematic Review and Conceptual Model

Dmytro Uhryn[1] and Artem Kalancha[2,*]

[1]Department of Computer Science, Yuri Fedkovych Chernivtsi National University, Chernivtsi, Ukraine
[2]Department of Computer Systems Software, Yuri Fedkovych Chernivtsi National University, Chernivtsi, Ukraine

*Corresponding author (E-mail: kalancha.artem@chnu.edu.ua)

ABSTRACT This article presents a systematic review and conceptual framework for analyzing information sources in social networks, with a focus on Telegram as the dominant news platform in Ukraine. The relevance of the study is determined by the dramatic shift in media consumption patterns following Russia's full-scale invasion in February 2022: Telegram's audience tripled from 20% to 60% within months, and by 2025 it remains the primary news source for 52% of the adult population, surpassing television (25%), YouTube (32%), and other platforms. Despite this dominance, only 29% of users trust Telegram channels, creating a paradox where mass consumption coexists with low trust and minimal verification – only 6% of Ukrainians consult fact-checking organizations. The article examines the mechanisms of information manipulation, including the five-level cascading narratives model (from "Russian World" to alternative information) and the five-level amplification pyramid that describes the transformation of deliberate disinformation into unwitting misinformation through state media, expert legitimization, portal localization, social media dissemination, and organic user spread. The 4D tactics framework (Dismiss, Distort, Distract, Dismay) systematizes the core techniques of these operations. A comparative analysis of ten methods for information source analysis spanning 2008-2025 reveals a clear evolution from isolated statistical approaches through graph-based methods to modern hybrid systems integrating natural language processing, graph neural networks, and attention mechanisms. The highest performance was demonstrated by the Lightning system (AUC 86.83%) and OnlineAgglomerative (93.2% accuracy). However, none of the reviewed methods simultaneously provides comprehensive semantic, temporal, and network analysis for source evaluation. To address this gap, the article proposes a conceptual model for assessing information source similarity (similarity_score) that integrates four components: cosine similarity of content embeddings, thematic clusterization, timed semantic influence for detecting temporal-semantic dependencies between sources, and network proximity in the information flow graph. The model is extensible and can incorporate additional metrics such as sentiment analysis, named entity recognition, and toxicity assessment. An information system architecture for practical implementation on Telegram data is also proposed.

KEYWORDS analysis of information sources, semantic analysis, network analysis, temporal dynamics, coordinated behavior.

I. INTRODUCTION

Social networks have changed the way people receive and distribute information. News no longer passes through the editorial filter of newspapers or TV channels. Anyone can create their own source of information (page or account) and publish any content without editorial control. This has given a voice to millions of people, but at the same time has created an environment where reliable and unreliable information spread at the same speed.

The problem is not new, but it is getting worse every day. During elections, crises, wars, social networks become a battlefield for the attention and trust of society. Disinformation spreads faster than it can be refuted or even detected. Coordinated influence campaigns are disguised as organic activity of ordinary users and the media, platform algorithms amplify emotional content because it generates more interactions, and people, overloaded with a stream of messages, often have neither the time, tools, nor knowledge to check the reliability of what they read.

Modern scholars are trying to understand the processes of information dissemination, who spreads it, why some messages go viral and others do not. But most studies focus on individual aspects: the content of messages, or the structure of connections between sources, or the temporal dynamics of the spread of a topic on the Internet. A comprehensive approach that would take into account all these dimensions simultaneously is still lacking.

The Ukrainian information space provides a unique opportunity to study these problems using the specific example of Russia's full-scale invasion, which caused a sharp change in Ukrainians' media consumption. According to the National Institute for Strategic Studies, the Telegram audience grew from 20% in 2021 to 60% in 2022 – a threefold increase in a few months [1].

This is due, first of all, to the public's need for operational information about air raids, shelling, evacuations, etc., and Telegram channels provided this faster than any television. The OPORA survey in May 2022 recorded the result: 76.6% of Ukrainians began to receive news from social networks, overtaking television (66.7%). Among social networks, Telegram became the leader with a share of 65.7% of users [2].

This change turned out to be not temporary, because according to the sociological group "Rating" in April 2025, 3 years after the start of the full-scale war, Telegram remains the main source of information for 52% of the adult population. This is more than YouTube (32%), the

telethon "United News" or Viber chats (25% each) [3]. At the beginning of 2024, there were more than 33 thousand active Telegram channels in Ukraine with 282.6 million subscriptions [4]. The distribution is uneven: a small number of large channels accumulate the majority of the audience, which, with a population of about 44 million, means that on average there are more than six subscriptions to Telegram channels per inhabitant of the country. In total, there are 23 million active accounts on social networks in Ukraine, i.e. 58.5% of the population [5]. A study by Gradus Research in September 2025 confirms the stability of these trends: 92% of respondents use Telegram every week, and 75% receive news through messengers [6]. The dynamics of changes are systematized in Table 1.

TABLE 1. Dynamics of the main news sources in Ukraine (2021–2025) compiled by author based on recent survey data.

Source	Dec. 2021	May 2022	Apr. 2025	Sept. 2025
Telegram / messengers	13%	65.7%	52%	75%
TV	67%	66.7%	25%	27%
Social Networks	44%	76.6%	–	60%
Video-Platforms (YouTube)	–	–	32%	54%
Online Media / Websites	29%	–	–	42%

Ukraine has found itself in a situation rare for democratic countries, where a messenger that does not moderate content and does not bear editorial responsibility has become the main source of news for the majority of the population. This makes the Ukrainian Telegram an ideal testing ground for studying how the information space functions without traditional quality control mechanisms.

Telegram's dominance creates an unexpected paradox. A study by Rating found that Telegram channels are trusted by only 29% of respondents, but used by 52% [3, 7]. For comparison: YouTube has 24% trust with 32% of users, newspapers have less than 3% trust, and 84% of respondents do not read them at all [8]. The scale of this gap becomes apparent when analyzing the entire chain from consumption to verification.

People are massively consuming content from a source that they mostly do not trust. There may be several explanations: speed is more important than reliability in war conditions; people have learned to filter information on their own and do not need to trust the source; There is virtually no alternative, and other media are even less convenient or accessible. The Media Literacy Index confirms this contradiction: 72% of Ukrainians have an above-average level, but digital literacy decreased from 55% to 48% during 2023–2024 [9], which prompts the search for means, including technical ones, to resolve this situation.

Telegram, like some other social networks, does not take responsibility for content moderation, does not detect coordinated influence campaigns, and does not verify the reliability of information. In September 2024, the National Security and Defense Council banned the use of the messenger on official devices of military and civil servants due to security risks. But public opinion is mixed: according to the National Institute of Statistics, only 9% of Ukrainians support a complete blocking of Telegram [1].

This creates a specific problem for the information space where people do not abandon a platform they do not trust. That ihs, content is consumed in a mode of constant skepticism, but skepticism rarely turns into verification. According to a survey conducted on the eve of a full-scale invasion [7], only 6% of Ukrainians turned to fact-checking organizations, while 40% look for alternative sources, and 24% simply perceive information as "one of the possible versions." The practical consequence of this is the lack of basic filtering of disinformation by users themselves.

To understand how the Telegram information space works and how to distinguish reliable sources from unreliable ones, systematic methods of analysis are needed, but there are serious obstacles here.

The first is scale. A single study can cover more than 138 million messages from 9,000 channels and groups [10]. No team of information space researchers is capable of processing such an array manually.

The second is the lack of criteria. There are no established ways to determine whether a source is reliable, influential, or associated with coordinated campaigns. Traditional approaches, such as expert assessments and reputation ratings, do not work in an environment where new channels appear every day, and old ones change their names or disappear forever.

The third is the fragmentation of methods. Some researchers study the content of messages, focusing on what channels write, what tone they use, whether there are signs of manipulation, etc. Others analyze the connections between sources at the level of explicit connections: who quotes whom, where the content is sent from, while still others focus on time dynamics: how quickly information spreads, whether there are signs of synchronous activity. Each approach provides a valuable but partial picture. There are almost no known approaches that combine all three dimensions or have a specific narrow task.

The purpose of this article is to analyze the state of the modern information space and its specificity for Ukraine in war conditions, to systematize existing methods for analyzing information sources in social networks, as well as to determine their advantages and disadvantages for the further development of complex approaches to assessing sources in dynamic environments.

To achieve this goal, three research questions were formulated:

1. What mechanisms of information manipulation are used in social networks and what role does Telegram play in their implementation?

2. What are the existing methods of analyzing information sources, what are their strengths and weaknesses, and what system limitations prevent a comprehensive assessment of sources?

3. How to combine semantic, temporal, and network analysis to form a comprehensive assessment of an information source?

The object of the study is Telegram as a component of the modern digital information space of Ukraine. The platform has two main types of communication environments: channels and groups. Channels operate

according to the "one-to-many" model where the author publishes and subscribers read. Groups implement the "many-to-many" model where participants can discuss content among themselves directly [11].

These two types of environments perform different functions in the information dissemination ecosystem. Studies show that 96% of channels act as sources of original content, which is then forwarded to other channels and groups. Among groups, this figure is only 40% [10]. Channels mainly produce content, while groups consume and retransmit.

The technical and political features of the platform create an environment favorable for information operations. As mentioned, Telegram does not moderate content, does not detect coordinated influence campaigns, does not limit the spread of unverified information, and the cloud architecture with data distribution between different countries complicates legal regulation and monitoring [11]. At the same time, Telegram provides a convenient software interface (Telegram API), which allows you to automatically receive messages and metadata of public channels and groups in a structured format. Access to public channels is open without special permissions - this significantly simplifies research data collection compared to platforms that restrict access to public content.

The subject of the study is methods for analyzing information sources in social networks. Existing approaches can be grouped into three main areas.

The first method is the analysis of the content of messages, where scientists study the thematic structure of the content, the emotional coloring of the texts, the presence of manipulative markers. For this, they use methods of automatic grouping of texts by topics, determining positive or negative tone, assessing the aggressiveness and toxicity of statements. Modern approaches are based on neural networks that convert texts into numerical vectors (embeddings) for further analysis.

The second method is the analysis of the network structure. Here, graphs of connections between channels are built based on referrals and links, which allows identifying influential nodes, clusters of related sources, and directions of information dissemination. One study of the information dissemination network shows that a small proportion of channels generate most of the content: 6% of users create 90% of forwarded messages [10].

The third is the analysis of time dynamics, where they study the speed of message dissemination, the duration of their relevance, and the reaction to external events. It was found that messages in groups remain active for an average of 105 days, in channels for only 17 days. That is, news links lose their relevance the fastest - in about 7 days [10].

The study has several limitations.

Language boundaries. Sources in Ukrainian and Russian, aimed at a Ukrainian audience, are analyzed. English-language content and its impact on a Western audience remain outside the scope of the study.

Channel types. Only public news and political channels are considered. Private groups, entertainment channels, and commercial communities are not included in the analysis.

Content types. The study focuses on text messages. Although Telegram supports photos, videos, and voice messages, most analysis methods are text-oriented. Visual content requires separate approaches and remains outside the scope of the review.

Methodological boundaries. The review covers methods based on statistical indicators and features extracted from texts: frequency characteristics, tonality, thematic clusters, network metrics. Approaches based on large language models (LLM) for deep text understanding and inference generation are not considered, as they require separate analysis and have other scalability limitations.

Time frame. The study focuses on the period after February 24, 2022, the beginning of Russia's full-scale invasion of Ukraine. This period is characterized by a sharp increase in activity on Telegram and its transformation into the main source of news for a significant part of Ukrainians.

II. INFORMATION MANIPULATION AND INFORMATION WARFARE

The analysis of information sources is impossible without understanding the mechanisms used to manipulate information. This section examines the theoretical foundations of information warfare and the main methods of manipulation, which allows us to form criteria for further evaluation of sources.

Information warfare encompasses actions aimed at using information as a weapon to achieve political, military, and strategic goals. In Russian military doctrine, information is viewed precisely as a type of weapon, which is a continuation of the Soviet tradition of using information for internal mobilization and demonization of the enemy [12].

The fundamental difference in the Russian approach is that cyber-security is subordinated to information security, while in the West these concepts are clearly delimited. Such an understanding allows us to control both technical data (integrity of network systems) and cognitive data (political information, narratives, propaganda) within a single system [12]. The information security doctrine of the Russian Federation openly formulates the philosophy of protecting the national "information space" from external threats.

In the context of a full-scale war against Ukraine, information operations began long before the main fighting began, which is consistent with the doctrinal position on the need to achieve information superiority before using conventional military means. Cyber preparation lasted for years: the Snake/Turla malware was directed against Ukrainian officials as early as 2010, and the web infrastructure for the Novorossiya project was registered in March 2014, even before the public announcement of the creation of this entity [12]. The cascade narrative model describes five levels of propaganda messages, each of which reaches a wider audience [13]. The narrowest level is the narrative of the "Russian world", which appeals to the cultural identity of Russian-speaking minorities in post-Soviet countries. The narrative of Slavic unity extends its reach to the population of Slavic countries by exploiting historical connections and opposing Western culture. Ostalgia works for the entire former socialist bloc, appealing to nostalgia for the stability and "greatness" of the USSR. Anti-rhetoric (anti-EU, anti-NATO, anti-immigration, anti-globalization) has a global reach and resonates with different audiences regardless of cultural

context or political spectrum. The broadest level is occupied by alternative information as an appeal to anyone who does not trust traditional media and seeks the "hidden truth". It is the last two levels that allow finding allies among the far-right and far-left movements in Western countries.

A key feature of the pyramid (see Fig. 1) is that each level provides a plausible rebuttal to the previous one. State media publish the original message; "independent" portals supposedly "confirm" it; ordinary users spread it as their own belief. By the time the message reaches the base, its origin is practically impossible to trace: it is perceived as the organic opinion of society. The lower levels of the pyramid function mostly unconsciously: people forwarding content do not know that they are part of a coordinated campaign. This is why social media platforms have become a more effective vector of amplification than disinformation portals, which the audience has already learned to identify [13]. The measurable result of the pyramid mechanism: over 70% of Serbs opposed sanctions against Russia is a direct reflection of the narratives broadcast in a coordinated manner through all levels [11]. The "4D" tactic systematizes four main techniques of Russian information operations [11].

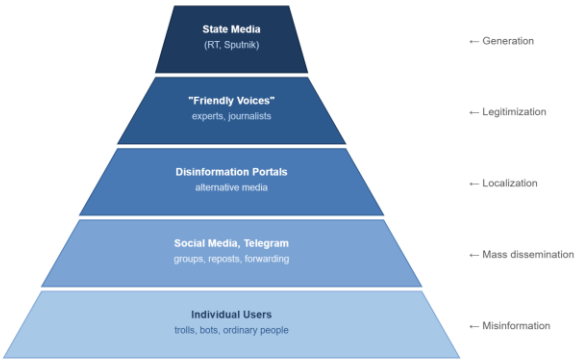


FIG. 1. The pyramid of amplification: from disinformation to misinformation compiled by author based on research [13].

Dismiss involves discrediting the source of information, declaring evidence "fake," and accusing opponents of bias, as was the case with the denial of the presence of Russian troops in Donbas in 2014–2015 despite abundant evidence. Distort involves manipulating information without full denial: selective quoting, changing the context, exaggerating or minimizing facts, including the use of video footage from other conflicts as "evidence" of events in Ukraine. Distract aims to shift attention through the tactic of "whataboutism," creating alternative informational pretexts, and generating informational "noise." Dismay creates an atmosphere of fear through threats, demonstrations of force, and the spread of apocalyptic scenarios, including nuclear blackmail, in order to paralyze the will to resist. Among the specific techniques for implementing these tactics is the use of "traveling actors," individuals who appear in different staged news stories as different characters: the Stopfake.org project documented numerous cases where the same people appeared in different staged reports on Russian television, playing either refugees or witnesses to "atrocities" by the Ukrainian army [14].

Analysis of disinformation campaigns reveals consistent thematic patterns. A study of a Telegram channel targeting the Russian-speaking diaspora in Germany revealed seven main trends: sanctions and the energy crisis; positive images of Russia and Putin; negative images of Ukraine and Zelensky; criticism of the US, Biden, and NATO; criticism of local politicians; glorification of the Russian army; negative images of Ukrainian refugees [15]. A comparative analysis in eleven European countries confirmed that these themes appear synchronously.

The narrative structure of propaganda is pyramidal: key theses are formulated at the level of top management, broadcast by traditional media and cyberspace, and then assimilated at the level of the "broad masses" with group adaptation [12]. Different groups independently select those elements of the narrative that correspond to their beliefs: nationalists emphasize historical greatness, supporters of leftist ideas - anti-capitalist rhetoric. This is what allows you to bypass critical analysis.

The described mechanisms create specific challenges for the analysis of information sources in social networks.

The first challenge is multi-level. The same message goes through several levels of amplification: from state media through experts and portals to individual users. At each level it is modified, losing obvious signs of the original source.

The second challenge is adaptability. Cascading narratives adapt to different audiences. The same message can sound like a defense of traditional values for a conservative audience and a criticism of capitalism for a leftist audience.

The third challenge is scale and speed. Studies show that the long-term impact of information operations leads to the fact that society assimilates the promoted narratives as its own rational tool of interpretation [11]. At the same time, the impact of disinformation is usually situational, when campaigns are effective in intensifying existing tensions in times of crisis, but are not able to create sustainable divisions or change the geopolitical orientation of societies [13].

These challenges require complex methods of analysis that combine the study of message content, network structure of distribution and temporal dynamics. These mechanisms are especially clearly manifested in Telegram, a platform that has become a key tool of information operations.

III. INFORMATION MANIPULATION ON SOCIAL NETWORKS AND TELEGRAM

The manipulation mechanisms described in the previous section operate primarily through social media. Here, the pyramid of amplification is most effective: from state media through a network of channels to millions of ordinary users. Social media creates an environment where disinformation spreads faster than in traditional media. An analysis of 125 verified fake news stories during the Russian-Ukrainian war showed that 48% of the disinformation content appeared during the first week of the conflict [16]. This shows that disinformation networks are able to mobilize quickly at critical moments.

Different platforms play different roles in the spread of manipulative content. If the international information space is taken into account then Twitter dominates as the main channel for disinformation (37% of content), followed by online media (18%), YouTube (17%), traditional media (11%), TikTok and Instagram (6% each) [16]. Traditional media, which are supposed to verify information, often repost unverified content from social media, which indicates systemic problems with verification and editing of information.

"False association" is the most common technique for creating fakes (58.4% of cases), when old materials are presented as current events [16]. More than half of disinformation content (50.4%) is materials from 2010-2021, reused in a new context. Video materials make up 48.8% of fakes, photos – 39.2%, text – only 12%. This emphasizes the visual nature of modern disinformation and the need to develop methods for analyzing not only textual content.

Echo chambers enhance the impact of manipulative content by forming closed information environments, where users consume content that confirms their previous beliefs [13].

Telegram's technical characteristics, described in the previous section, make the platform attractive for information operations. Analysts call it "the least open network for external monitoring" [15].

Analysis of Russian-language Telegram channels in different countries shows typical patterns of disinformation campaigns. Analysis of the channel for the Russian-speaking diaspora showed that in the first month after the invasion, 430 messages were published, grouped into seven thematic areas: sanctions, energy crisis; image of Russia and Putin; image of Ukraine and Zelensky; criticism of the USA, Biden and NATO; criticism of local politicians; glorification of the Russian army; negative image of Ukrainian refugees [15]. These patterns are typical for channels targeting Russian-speaking audiences in different countries. After blocking, the channel immediately resumed work under a new name, preserving all the previous content. A comparative analysis of Russian disinformation in eleven European countries found that the same topics appear simultaneously, which confirms the coordination of operations. Researchers point to a system of moderation by official Russia that encompasses not only traditional media but also social networks, which news to comment on and how [15].

The imbalance of information flows during a modern war is a characteristic feature of the Telegram space in general. A study of English-language verified channels revealed a ratio of 49 pro-Russian to 5 pro-Ukrainian [17, 18]. Although English-language content remains outside the scope of this study, such data illustrate the general trend - the pro-Russian ecosystem is much larger and better coordinated.

The disinformation infrastructure is very resilient, which makes it difficult to counter. Sanctioned channels immediately resume work under new names, preserving content and part of the audience. This requires systemic approaches aimed at the disinformation ecosystem as a whole, rather than individual channels.

According to a study conducted in December 2021, the level of information resilience of Ukrainian society was assessed as "below average" [7]. 68% of Ukrainians periodically doubted the reliability of media information, but only 6% turned to fact-checking organizations. The most popular verification strategies: searching for alternative sources (40%), analyzing "who benefits" (32%), and perceiving as one of the possible versions (24%). The war may have changed these indicators, but basic habits, such as rare use of fact-checkers and reliance on informal verification methods, emphasize the need for automated tools for source analysis.

Researching Telegram has its own difficulties. Unlike Twitter and Facebook, Telegram does not have a special research API with extended access. At the same time, public channels are available through the standard Telegram API without additional approvals, which provides conditions for large-scale research, covering from hundreds of thousands to over tens of millions of messages.

The objects of further analysis may be the connections between channels through forwarding and referencing, the topics of content through language processing methods, the reactions of the information space to events over time. The following section systematizes existing approaches to such analysis, revealing the strengths and weaknesses, as well as the limitations of each study.

IV. RELATED WORKS

The previous sections showed that the analysis of information sources in social networks requires a comprehensive consideration of the content of messages, the structure of connections between sources, and the temporal dynamics of dissemination.

The first systematic approaches to the analysis of information flows in social networks appeared in the late 2000s. Researchers adapted methods from related fields, in particular, vector clocks from distributed computing [19]. The authors introduced the concept of "information latency" – a time distance that measures how outdated the information of one node is relative to another. An analysis of electronic correspondence of a large university (8160 employees, two years of observations) showed that the median latency between pairs of nodes is 7.5 days, although the topological distance is only 3 hops. The difference between the graph structure of the network and the real possibilities of information dissemination turned out to be fundamental.

The concept of a "network backbone" defined a subset of edges that provided the fastest information flow. This backbone turned out to be very sparse: the average degree of a node is about 5 contacts compared to 50 in a full communication network, but only a small fraction of the links are critical for information circulation. The next important step is to analyze the diffusion of information on Twitter, focusing on three dimensions of analysis: speed (when the first mention occurs), scale (the number of direct descendants), and range (the depth of the diffusion chain) [20]. The study, based on 22 million tweets from over 3 million users, showed that user properties – in particular, the frequency with which others mention them – are stronger indicators of information dissemination than characteristics of the messages themselves. The

MentionedRate indicator correlated up to 0.63 with the scale of diffusion, while predicting speed remained a difficult task (R^2 only 0.009-0.067).

The period 2013-2014 was marked by the development of lexicographic and probabilistic approaches. Lexical analysis using LIWC (Linguistic Inquiry and Word Count) allowed predicting the structure of retweet cascades based on 80 psycholinguistic features of the text [21]. Time-dependent cascade models (T-BaSIC) introduced time-varying parameters, as opposed to static independent cascade models [22]. T-BaSIC showed a 32% improvement in accuracy compared to baseline methods, but systematically underestimated the volume of cascades. The second period was characterized by the theoretical understanding of diffusion models and the beginning of the application of deep learning methods. A comparative analysis of six classical diffusion models (threshold, viral, dependent cascades, rumors, influential users and cellular automata) by eleven properties showed that no model is universal [23]. The influential user model turned out to be the best in terms of network properties, the viral model - in terms of probabilistic and temporal estimation.

This period was marked by the realization of the limitations of isolated analysis. Most early approaches considered either the network structure, or the temporal dynamics, or the semantics of the content separately. But the real dissemination of information depends on the simultaneous action of all these factors, which required the development of integrated approaches.

The modern stage is characterized by the integration of graph neural networks, natural language processing methods and attention mechanisms. The DLIC (Deep Learning Information Cascades) model combines a graph attention network (GAT) for learning spatial features of users with recurrent neural networks (GRU) for encoding the temporal sequences of cascades [24]. The time-decay attention mechanism assigns different weights to time intervals, and then the influence of previous messages decreases over time. Experiments on Twitter and Douban data showed a 2.2% improvement in the HITS@100 metric compared to the best baseline methods.

The Lightning system is a significant step in integrating network analysis with content processing [25]. The architecture combines GraphSAGE or GAT for network representation with the Longformer model for encoding text content into 768-dimensional vectors. Community-level prediction instead of individual users provided a significant improvement: 86.83% AUC compared to 77.01% at the user level.

To analyze the evolution of narratives, a streaming clustering (OnlineAgglomerative) was developed, which allows tracking changes in narratives in real time without a predetermined number of clusters [26]. The two-level architecture combines automatic clustering with expert validation (Human-in-the-Loop), achieving 93.2% accuracy in identifying trending stories.

Approaches combining thematic modeling (BERTopic) with community network analysis (Leiden algorithm) and sentiment analysis were developed for the analysis of disinformation campaigns [17]. A study of the "fascism/Nazism" narrative on Twitter covered over 6 million tweets and revealed differences in the network structures of English-speaking (polarized) and Russian-speaking (ideologically more diverse) audiences.

A large-scale analysis of marginal Telegram communities showed the possibilities of integrating semantic, temporal, and network analysis on large volumes of data. The combination of BERTopic for topic modeling, RoBERTa for sentiment analysis, and Google Perspective API for toxicity assessment revealed that a small percentage of users generate the majority of forwarded content, while toxic messages remain active for a longer period.

Modern visualization systems, such as MIDDAG, combine information path prediction, audience susceptibility assessment, event detection, and public opinion analysis in a single interactive interface [27]. Multi-platform analysis (Twitter, Reddit, news organizations from 15 countries) achieves 86.83% AUC for path prediction and 86.28% F1 for susceptibility assessment.

The evolution of methods for analyzing information sources shows a clear trend from isolated statistical approaches to integrated systems that combine semantic, temporal, and network analysis with the use of modern deep learning technologies and large language models.

For a systematic comparison of the considered methods, five criteria were defined: semantic analysis (the ability to analyze the content of messages), temporal dynamics (taking into account temporal patterns of distribution), network structure (analysis of the relationships between sources), analytical scalability (suitability for expanding the analysis), and measurable efficiency (availability of quantitative quality metrics). Table 2 summarizes the results of the comparison of the ten methods.

TABLE 2. Comparative analysis of methods for analyzing information sources in social networks compiled from researched papers.

Method	Task	Sem./Time /Network
Vector Clocks [19] (2008)	Flow analysis	-/+/+
Diffusion regression [20] (2010)	Diffusion forecast	-/+/-
T-BaSIC [22] (2013)	Cascade forecast	-/+/+
LIWC-cascades [21] (2014)	Classification of cascades	+/-/-
DLIC (GAT+GRU) [24] (2021)	Cascade forecast	-/+/+
Lightning [25] (2023)	Path forecast	+/-/+
BERTopic+Leiden [17] (2024)	Narrative analysis	+/-/+
Hoseini et al. [10] (2024)	Community analysis	+/-/-
OnlineAgglomerative [26] (2025)	The evolution of narratives	+/+/-
MIDDAG [27] (2024)	Complex system	+/-/+

As can be seen from Table 2, the evolution of methods demonstrates a gradual expansion of analytical coverage. Early approaches (2008–2014) focused on one or two aspects: vector clocks [19] analyzed only the temporal and network structure without taking into account the content of messages, and a regression model [20] predicted the diffusion scale with moderate accuracy ($R^2 = 0.46$) due to user properties, ignoring semantics. The lexicographic approach [21] was the first attempt to take content into account, achieving an F1 of 89% for cascade classification, but on a small dataset (13 thousand tweets from a single topic) and without modeling temporal dynamics. Graph methods (2021–2023) have significantly improved network analysis. The DLIC model [24] combined attention graph networks with recurrent networks for encoding time sequences, but worked on small data sets (12.6 thousand users) and did not take into account the content of messages. The Lightning system [25] integrated network analysis with meaningful text encoding, achieving an AUC of 86.83% on 640 million tweets. However, the temporal component in it is represented only by dividing the data into time slices, and not by modeling dynamics.

Current methods (2024–2025) cover most of the criteria, although none covers all completely. OnlineAgglomerative [26] most fully combines semantics, temporal dynamics and network analysis, achieving 93.2% accuracy in identifying trending topics. At the same time, network analysis in this approach is limited to detecting communities and does not include detailed modeling of connections between channels. MIDDAG [27] demonstrates the highest complexity as a system: AUC 86.83% for predicting spread paths and F1 86.28% for assessing audience vulnerability. However, both systems were tested on limited topics: the Russian-Ukrainian war and COVID-19, respectively.

The study of Telegram marginal communities [10] is notable for its scale, but each of the three components is partially implemented: semantic analysis is limited to detecting topics without deep analysis of narratives, temporal dynamics is reduced to message duration, and network analysis is limited to counting forwards without modeling the graph structure.

The comparison in Table 2 reveals several systemic limitations of existing methods.

Fragmentation by platform. Most methods were developed for a single platform (Twitter or Telegram) and were not tested on cross-platform data. Only MIDDAG [27] analyzes data from multiple platforms, but its focus is limited to the COVID-19 context. Methods developed for Twitter cannot be directly transferred to Telegram due to fundamental differences between the platforms. In particular, these include the lack of a retweet mechanism, a different distribution structure (forwarding instead of reposting), and a different architecture of channels and groups.

Lack of comprehensive source assessment. As the performance metrics show, existing approaches are optimized for different tasks: predicting diffusion paths (Lightning, MIDDAG), detecting topics (OnlineAgglomerative), analyzing community structure (BERTopic+Leiden).

Multimodality limitations. All considered methods focus on textual content, while video materials account for 48.8% of disinformation content [16]. Combining image and video analysis with textual analysis remains an unsolved problem.

The problem of establishing causality. Most methods show correlations, but do not establish cause-and-effect relationships. OnlineAgglomerative [26] uses Granger causality to analyze a time series, but this method determines statistical associations, not causality in the strict sense. Detection of coordinated inauthentic behavior remains an undeveloped area.

As Table 2 shows, none of the analyzed methods simultaneously takes into account all aspects of the dynamics of information dissemination – semantics, temporal patterns, and network structure. Early approaches are limited to one or two aspects, and modern hybrid systems, despite their wider coverage, implement individual components only partially. In addition, existing methods do not provide an assessment of the similarity between information sources. They either predict dissemination paths, or identify topics, or analyze the structure of communities, but do not compare sources with each other according to a set of content, temporal, and network characteristics. This leaves the problem of a comprehensive assessment of the reliability and role of a single source in the information ecosystem unsolved.

The following section proposes a concept for an approach aimed at partially overcoming these limitations of comprehensive analysis of messages from information sources.

V. SOLVING CONCEPT OF THE PROBLEM

The analysis in the previous sections shows that the mechanisms of information manipulation are multi-level and adaptive, and Telegram has become a key platform for their implementation in Ukraine, while existing analysis methods do not provide simultaneous consideration of content, time, and network structure. This limitation is fundamental: the reliability and influence of an information source are determined by the combined action of at least three factors. Semantic analysis without taking into account temporal dynamics does not allow us to identify how narratives adapt to events. A study of the evolution of narratives during the Russian-Ukrainian war showed that the thematic composition of content changed significantly in response to external events [26]. For example, after the publication of information about Bucha, the pro-Ukrainian community focused on documenting events in real time, while the pro-Russian community first minimized information and then switched to the narrative of "provocation". Static analysis of topics at any given point in time will not capture this adaptability.

Temporal analysis without a semantic component does not take into account that different types of content have different temporal dynamics. As mentioned above, toxic and emotionally extreme messages remain active longer than neutral content, and messages with links to news resources have the shortest period of relevance [10]. Without semantic classification of content, these patterns remain invisible.

Network analysis separately from semantics and time shows the structure of connections, but does not explain their nature. As noted in the previous section, channels forward significantly more content than groups, but only in combination with semantic analysis can we establish that a small fraction of users generate the majority of the forwarded content [10]. The characterization of these superspreaders requires a combination of structural and content features.

The semantic component of the complex analysis is aimed at characterizing the content patterns of the information source. It covers three main aspects: thematic structure, emotional coloring and linguistic markers.

Thematic structure is determined through thematic modeling using modern methods based on transformers. Models of the BERTopic class with multilingual vector representations (Multilingual-MiniLM, all-MiniLM) allow to detect hidden topics even in mixed Ukrainian-Russian-English content. Dimensionality reduction (UMAP) and clustering (HDBSCAN) ensure the detection of topics without a predetermined number of them. To compare the thematic profiles of two sources, the cosine similarity between their averaged vector representations is used. It quantitatively assesses how much the lexical fields and thematic orientation of the sources coincide.

Emotional coloring is assessed through sentiment analysis and toxicity analysis. RoBERTa models trained on the corresponding corpora show an accuracy of about 84% for determining tone. Google Perspective API provides a toxicity assessment on a scale from 0 to 1. The combination of these metrics allows us to characterize the source by the degree of aggressiveness and emotional manipulativeness of the content. Linguistic markers include the use of specific vocabulary, rhetorical devices and stylistic features characteristic of propaganda content.

The temporal component analyzes the dynamic characteristics of the source's publishing activity and reactions to external events. It includes three dimensions: patterns of publishing activity, speed of reaction and temporal sequence of influence. Patterns of publishing activity characterize the regularity and intensity of publications. Coordinated information operations often show synchronized activity: the same topics are developed simultaneously in different channels and countries [15]. The detection of such patterns indicates the organized, rather than organic, nature of information activity.

The speed of reaction to external events shows the source's responsiveness and its connection to the information agenda. As noted in the previous section, disinformation networks are able to mobilize quickly at critical moments: a significant part of the disinformation content appears within the first week after the event [16].

The temporal sequence of influence is analyzed through the Timed Semantic Influence (TSI) indicator, which combines Granger causality with the analysis of time lags between thematically similar publications. TSI allows us to determine whether the source is an opinion leader (its content systematically precedes the appearance of similar topics in other sources) or a relayer (reproduces the content of other sources with a delay).

The network component analyzes the structure of relationships between sources and their position in the information ecosystem. It covers three aspects: the topology of relationships, centrality and forwarding patterns.

The topology of relationships is determined by analyzing links, forwarding and mentions between channels. Building an information flow graph allows you to identify clusters of related sources and establish which ecosystem the source belongs to: pro-Ukrainian, pro-Russian, or neutral.

The centrality of a source characterizes its position in the network and potential influence. Centrality metrics (betweenness, eigenvector, PageRank) allow you to identify key nodes that function as information hubs or bridges between different communities. Forwarding patterns reflect information flows between sources. Analysis of forwarding chains allows you to track the origin and directions of content distribution.

The combination of these responses allows us to form a comprehensive assessment of the source, which takes into account: thematic proximity to known disinformation narratives, the nature of the emotional impact, synchronization with other sources, the role in the dissemination of content, and belonging to a certain information ecosystem. Such an assessment is more reliable than any separate metric, since it takes into account the multidimensional nature of information operations.

The relationship between the components is manifested in specific research tasks. Identifying coordinated inauthentic behavior requires simultaneous analysis of: semantic similarity of content (whether channels publish similar messages), temporal synchronization (whether these messages appear at the same time), and network structure (whether these channels are connected by referrals). The study showed that the pro-Ukrainian community focuses on military actions (46.5% of content), while the pro-Russian community focuses on international politics (52.4%) and domestic politics (31%), with only 16.7% on military actions [26]. This semantic difference becomes meaningful only in combination with the network context, i.e. understanding which channels belong to which community.

The combination of the described components is formalized through a model of assessing the similarity between two information sources a and b:

$$\text{score}(a, b) = f(\cos, \text{clust}, \text{TSI}, \text{net}), \qquad (1)$$

where a and b are two information sources, f is the aggregation function of the components, and each component is responsible for a separate aspect of the comparison: $\cos(a, b)$ "cosine_similarity" – cosine similarity of vector representations of the content of the sources. Messages from each source are converted into numerical vectors using BERTopic models or multilingual transformers (Multilingual-MiniLM). The cosine similarity between the averaged vectors of two sources assesses how close their vocabulary fields and thematic profiles are. Values from 0 (completely different topics) to 1 (identical content); clust(a, b) "clusterization" – belonging of sources to a common thematic cluster. Based on thematic modeling (HDBSCAN), sources are grouped by thematic

specialization. The component assesses whether sources *a* and *b* fall into the same cluster, adjacent clusters, or completely different thematic groups; TSI(a, b) – an indicator of temporal-semantic influence between two sources. Assesses whether the appearance of a certain topic in source b is systematically preceded by the publication of similar content in source a, using Granger causality and time lag analysis. A high TSI indicates a consistent influence of one source on another; Net(a, b) "Network" – network proximity of sources in the information flow graph. Takes into account the presence and intensity of direct (forwarding, linking) and indirect (semantic) connections, common contacts and belonging to the same network community.

The function f determines the method of aggregation of components. The choice of a specific form of aggregation (weighted sum, product, trained function) is the subject of further research and depends on the task: for the detection of coordinated operations, TSI and Network will have greater weight, for thematic comparison – cosine_similarity and clusterization.

The proposed model is not final and can be expanded with additional metrics. Among the promising components: tonality analysis (comparison of the emotional coloring of the content of two sources), recognition of named entities (which persons, organizations and locations are mentioned), toxicity analysis and stylistic markers. The modular structure allows adding new components without restructuring the overall architecture.

Practical application of the proposed model involves the creation of an information system that automatically processes messages from Telegram as the main information exchange platform in Ukraine. The system performs the following functions:

1. Collection and processing of messages from public channels via the Telegram API in a structured format with subsequent calculation of semantic, temporal and network characteristics of each source.

2. Construction of similarity values between sources for each component of the model (cosine_similarity, clusterization, TSI, Network) and calculation of the integral indicator similarity_score.

3. Visualization of both individual components of the comparison (for example, thematic similarity of two channels or the temporal influence between them) and integral similarity estimates for a set of sources in the form of similarity matrices, relationship graphs, and cluster diagrams.

In this study, the aggregation function f is implemented as a linear weighted sum of the four components, each previously normalized to the range [0, 1]:

$$score(a,b) = 0.36 \cdot cos(a,b) + 0.10 \cdot clust(a,b) + \\ + 0.40 \cdot \mathrm{TSI(a,b)} + 0.14 \cdot \mathrm{Net(a,b)}. \quad (2)$$

The weights were determined experimentally and reflect the relative contribution of each aspect to the overall assessment: temporal-semantic influence (TSI, 0.40) and cosine similarity (0.36) provide the dominant contribution, whereas network proximity (0.14) and cluster membership (0.10) play a supporting role. Since the weights sum to unity, the resulting score also lies in the range [0, 1].

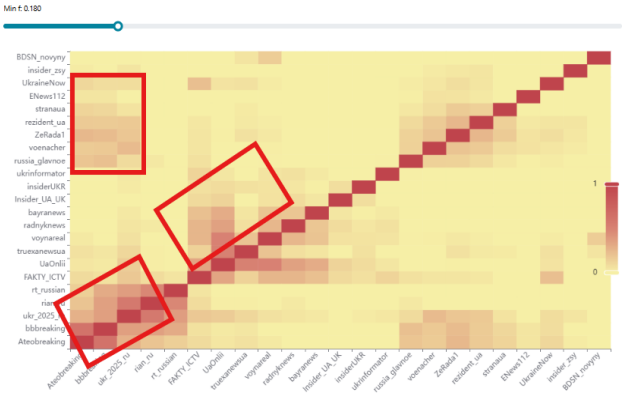


FIG. 2. Integral scores between 23 sources computed using existing analysis system.

Three distinct regions can be identified in the resulting heatmap (see Fig. 2), corresponding to groups of sources that share common characteristics and can therefore be assessed as coordinated groups of sources. The top-left region identify pseudo-Ukranian sources, like rezident_ua, ENews112, stranaua, which intersect with bottom-left region. At bottom-left corner we have pro-Russian sources with high similarity between them which indicate a intesive collaboration between them. The last center region highlight the cluster of pro-Ukranian sources which does not intersect with any of other 2 clusters.

Based on this approach we can analyze an unknown source by identifying with which sources it interact the most. It allow us to have fast and general overview of a source in dynamic informational space.

Such a system allows researchers and analysts to assess the role of an individual source in the information ecosystem, identify groups of coordinated channels, track the spread of narratives, and compare the reactions of different sources to the same event.

VI. CONCLUSION

The introduction formulates three research questions. Below are summarized answers to each of them.

What mechanisms of information manipulation are used in social networks and what role does Telegram play in their implementation?

The analysis showed that Russian information operations function through structured systems of cascading narratives (five levels of message adaptation from ethnic minorities to a global audience) and the pyramid of amplification (five levels of transformation of disinformation into misinformation). The "4D" tactic (Dismiss, Distort, Distract, Dismay) systematizes the main techniques of these operations. Telegram plays a special role due to the lack of content moderation, high anonymity, cloud architecture and convenient software interface. Studies record a significant asymmetry of information flows in favor of pro-Russian sources and the coordination of disinformation campaigns in different countries.

What are the existing methods for analyzing information sources, what are their strengths and weaknesses, and what systemic limitations hinder comprehensive source assessment?

A comparative analysis of ten methods (Table 1) revealed an evolution from isolated statistical approaches

(2008–2015) through graph methods (2015–2020) to modern hybrid systems (2020+). The highest performance indicators were demonstrated by the Lightning system (AUC 86.83%) and OnlineAgglomerative (accuracy 93.2%). At the same time, five systemic limitations were identified: fragmentation by platform, lack of comprehensive source assessment, limited multimodality, problems establishing causality, and insufficient consideration of coordinated inauthentic behavior. None of the analyzed methods provides a simultaneous combination of semantic, temporal, and network analysis.

How to combine semantic, temporal, and network analysis to form a comprehensive assessment of an information source?

The concept of a comprehensive approach is proposed, combining three components: semantic ("about what" and "how" the source publishes), temporal ("when" it reacts to events) and network ("with whom" it is connected in the ecosystem). The similarity assessment model of information sources similarity_score is formalized, which integrates cosine similarity, clustering, TSI and network proximity. The model is extensible and can be supplemented with new components. The architecture of an information system is proposed for the practical implementation of the model on Telegram data. It should be noted that the concept requires empirical verification on real data, and the specific form of the aggregation function is the subject of further research.

Therefore, this approach has few limitations based on its text-oriented nature without ingesting the media files. Extending the integral model requires a weight recalculation what may make existing factors less important in new version. Approach is not applicable to large-scale internet articles.

The scientific novelty of the study lies in: systematization of existing methods of analyzing information sources according to unified criteria (Table 1); formation of the concept of a comprehensive approach, combining semantic, temporal and network components; formalization of the source similarity assessment model (similarity_score).

The practical value is determined by the possibility of forming a comprehensive assessment of an information source, which is not achieved by any of the individual metrics. Such an assessment can be used to monitor the information space, identify coordinated information operations, support decision-making in the field of information security and develop content verification systems.

Further development of a comprehensive approach to the analysis of information sources can be carried out in several directions: empirical verification of the proposed concept on large Telegram data sets; expansion to cross-platform analysis to track the distribution of content between Telegram, Twitter, YouTube and other platforms; development of automated methods for detecting coordinated inauthentic behavior based on the identified activity synchronization patterns; combination of multimodal analysis to take into account visual content, which makes up a significant share of disinformation materials; application of cause-and-effect analysis methods to move from identifying correlations to establishing causal relationships. The implementation of these areas will contribute to the formation of effective tools to counter information operations and increase the resilience of the information space in the face of hybrid threats.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to Yuriy Fedkovych Chernivtsi National University for providing the opportunities, resources, and supportive environment that made this research possible.

AUTHOR CONTRIBUTIONS

A.K. – conceptualization, investigation, data curation, formal analysis, visualization, writing – original draft preparation; D.U. – supervision, methodology, writing-review and editing.

COMPETING INTERESTS

The authors have no competing interests.

REFERENCES

[1] National Institute for Strategic Studies, "Use of Telegram: Access to information vs. national security threat," (in Ukrainian), Kyiv, Ukraine, 2024. Accessed: Mar. 25, 2026. [Online]. Available: https://niss.gov.ua/news/komentari-ekspertiv/vykorystannya-telegram-dostup-do-informatsiyi-vs-zahroza-natsbezpetsi

[2] OPORA, "Media consumption of Ukrainians in conditions of full-scale war: OPORA survey," (in Ukrainian), Kyiv, Ukraine, May 2022. Accessed: Mar. 25, 2026. [Online]. Available: https://oporaua.org/polit_ad/mediaspozhivannia-ukrayintsiv-v-umovakh-povnomasshtabnoyi-viini-opituvannia-opori-24068

[3] Institute of Mass Information / Sociological Group "Rating," "Poll: Telegram is the main source of information for 52% of Ukrainians," (in Ukrainian), Kyiv, Ukraine, Apr. 2025. Accessed: Mar. 25, 2026. [Online]. Available: https://imi.org.ua/news/opytuvannya-telegram-ye-golovnyj-dzherelom-informatsiyi-dlya-52-ukrayintsiv

[4] Telemetrio, "Statistics of Telegram channels in Ukraine," 2024. Accessed: Mar. 25, 2026. [Online]. Available: https://telemetrio.com

[5] DataReportal and Prostir.ua, "Social networks 2026: important statistics for communications," (in Ukrainian), 2025. Accessed: Mar. 25, 2026. [Online]. Available: https://www.prostir.ua/?kb=sotsmerezhi-2026-vazhlyva-statystyka-dlya-komunikatsij-nuo

[6] Gradus Research, "Media consumption of Ukrainians," Sep. 2025. Accessed: Mar. 25, 2026. [Online]. Available: https://gradus.app/uk/open-reports/research-media-consumption-ukraine/

[7] A. E. Lebid, K. M. Vashyst, and M. S. Nazarov, "Information resilience as a means of countering the socio-psychological strategies of information wars," *Int. J. Media Inf. Literacy*, vol. 7, no. 1, pp. 157–166, 2022, doi: 10.13187/ijmil.2022.1.158.

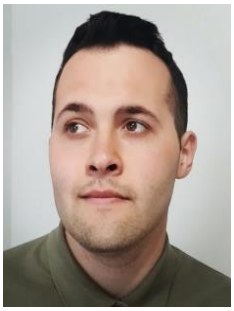
[8] Slovo i Dilo, "Ukrainians most often search for news on Telegram: survey," (in Ukrainian), Aug. 30, 2025. Accessed: Mar. 25, 2026. [Online]. Available: https://www.slovoidilo.ua/2025/08/30/novyna/suspilstvo/n

ajchastishe-ukrayinczi-shukayut-novyny-telegram-opytuvannya
[9] Detector Media and IREX, “Media literacy index of Ukrainians for 2024,” (in Ukrainian), May 6, 2025. Accessed: Mar. 25, 2026. [Online]. Available: https://detector.media/infospace/article/240621/2025-05-06-indeks-mediagramotnosti-ukraintsiv-za-2024-rik/
[10] M. Hoseini, P. de F. Melo, F. Benevenuto, A. Feldmann, and S. Zannettou, “Characterizing information propagation in fringe communities on Telegram,” in *Proc. Int. AAAI Conf. Web Social Media*, vol. 18, no. 1, 2024, pp. 583–595, doi: 10.1609/icwsm.v18i1.31336.
[11] I. Životić and D. Obradović, “Telegram as a specific playground of the Kremlin's information operations in Serbia,” *Nat. Secur. Future*, vol. 25, no. 1, pp. 65–92, 2024, doi: 10.37458/nstf.25.1.3.
[12] M. L. Jaitner, “Russian information warfare: lessons from Ukraine,” in *Cyber War in Perspective: Russian Aggression against Ukraine*, K. Geers, Ed. Tallinn, Estonia: NATO CCD COE, 2015, ch. 10, pp. 87–94.
[13] M. Boksa, “Russian information warfare in Central and Eastern Europe: strategies, impact, countermeasures,” German Marshall Fund, Washington, DC, USA, Policy Paper no. 15, Jun. 2019.
[14] A. Aliaksandrau, “Brave new war: the information war between Russia and Ukraine,” *Index Censorship*, vol. 43, no. 4, 2014, doi: 10.1177/0306422014560963.
[15] A. Yarova, “Thematic patterns of Russian disinformation,” *Baltic J. Legal Soc. Sci.*, no. 4, pp. 158–165, 2022, doi: 10.30525/2592-8813-2022-4-19.
[16] K. Babacan and M. S. Tam, “The information warfare role of social media: fake news in the Russia-Ukraine war,” *Erciyes Iletisim Dergisi*, no. 3, pp. 75–92, Oct. 2022, doi: 10.17680/erciyesiletisim.1137903.
[17] I. Alieva, I. Kloo, and K. M. Carley, “Analyzing Russia's propaganda tactics on Twitter using mixed methods network analysis and NLP,” *EPJ Data Sci.*, no. 1, 2024, doi: 10.1140/epjds/s13688-024-00479-w.
[18] A. Gruzd, Y. Li, and P. Mai, “Shaping Western perceptions: the role of English-language verified Telegram channels in framing the narratives around the Russia-Ukraine war,” *J. Commun. Technol.*, vol. 7, no. 2, p. 75, 2025, doi: 10.51548/joctec.7.2.2025.04.
[19] G. Kossinets, J. Kleinberg, and D. Watts, “The structure of information pathways in a social communication network,” in *Proc. 14th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, 2008, pp. 435–443, doi: 10.1145/1401890.1401945.
[20] J. Yang and S. Counts, “Predicting the speed, scale, and range of information diffusion in Twitter,” in *Proc. Int. AAAI Conf. Web Social Media*, vol. 4, no. 1, 2010, pp. 355–358, doi: 10.1609/icwsm.v4i1.14039.
[21] E. Kafeza, A. Kanavos, C. Makris, and P. Vikatos, “Predicting information diffusion patterns in Twitter,” in *Artificial Intelligence Applications and Innovations (IFIP Adv. Inf. Commun. Technol., vol. 436)*, L. Iliadis, I. Maglogiannis, and H. Papadopoulos, Eds. Berlin, Germany: Springer, 2014, doi: 10.1007/978-3-662-44654-6_8.
[22] A. Guille, H. Hacid, C. Favre, and D. A. Zighed, “Information diffusion in online social networks: a survey,” *SIGMOD Rec.*, vol. 42, no. 2, pp. 17–28, May 2013, doi: 10.1145/2503792.2503797.
[23] K. A. Dmytriienko, “Comparative analysis of information dissemination models in the online environment,” *Cybersecurity: Educ., Sci., Technique*, vol. 4, no. 20, pp. 272–282, Jun. 2023, doi: 10.28925/2663-4023.2023.20.272282.
[24] Z. Chen, J. Wei, S. Liang, T. Cai, and X. Liao, “Information cascades prediction with graph attention,” *Front. Phys.*, vol. 9, Aug. 2021, Art. no. 739202, doi: 10.3389/fphy.2021.739202.
[25] A. K. Taylor, N. Wen, P.-N. Kung, J. Chen, V. Peng, and W. Wang, “Where does your news come from? Predicting information pathways in social media,” in *Proc. 46th Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval (SIGIR)*, 2023, pp. 2511–2515, doi: 10.1145/3539618.3592087.
[26] P. Gerard, S. Volkova, L. Penafiel, K. Lerman, and T. Weninger, “Modeling information narrative evolution on Telegram during the Russia-Ukraine war,” in *Proc. Int. AAAI Conf. Web Social Media*, vol. 19, no. 1, 2025, pp. 602–614, doi: 10.1609/icwsm.v19i1.35834.
[27] M. D. Ma, A. K. Taylor, N. Wen, Y. Liu, P.-N. Kung, W. Qin, et al., “MIDDAG: where does our news go? Investigating information diffusion via community-level information pathways,” in *Proc. AAAI Conf. Artif. Intell.*, vol. 38, no. 21, 2024, pp. 23811–23813, doi: 10.1609/aaai.v38i21.30573.

Dmytro Uhryn

Dmytro Illiich Uhryn is a Professor at the Department of Computer Science of Chernivtsi National University. He holds a Doctor of Technical Sciences degree and has been awarded the academic title of Professor. His research interests include information technologies for decision support, swarm intelligence systems, and domain-specific geographic information systems.

ORCID ID: 0000-0003-4858-4511



Artem Kalancha

Artem Dmytrovych Kalancha is a third-year PhD student at the Department of Software Engineering of Computer Systems. His research focuses on the analysis and comparison of information sources using natural language processing (NLP) methods.

ORCID ID: 0009-0004-1451-7470

Оцінка інформаційних джерел у соціальних мережах: систематичний огляд та концептуальна модель

Дмитро Угрин[1], Артем Каланча[2,*]

[1]Кафедра комп'ютерних наук, ЧНУ ім. Ю. Федьковича, Чернівці, Україна
[2]Кафедра програмного забезпечення комп'ютерних систем, ЧНУ ім. Ю. Федьковича, Чернівці, Україна

Автор-кореспондент (Електронна адреса: kalancha.artem@chnu.edu.ua)

ABSTRACT У цій статті представлено систематичний огляд та концептуальну основу для аналізу джерел інформації в соціальних мережах, з акцентом на Telegram як домінуючу новинну платформу в Україні. Актуальність дослідження визначається різкою зміною моделей споживання медіа після повномасштабного вторгнення Росії в лютому 2022 року: аудиторія Telegram потроїлася з 20% до 60% протягом кількох місяців, і до 2025 року він залишається основним джерелом новин для 52% дорослого населення, перевершуючи телебачення (25%), YouTube (32%) та інші платформи. Незважаючи на це домінування, лише 29% користувачів довіряють каналам Telegram, створюючи парадокс, коли масове споживання співіснує з низькою довірою та мінімальною перевіркою – лише 6% українців консультуються з організаціями, що займаються перевіркою фактів. У статті розглядаються механізми маніпуляції інформацією, включаючи п'ятирівневу каскадну модель наративів (від «русского мира» до альтернативної інформації) та п'ятирівневу піраміду посилення, яка описує перетворення навмисної дезінформації на несвідому дезінформацію через державні ЗМІ, легітимізацію експертів, локалізацію порталів, поширення в соціальних мережах та органічне поширення серед користувачів. Структура тактик 4D (Dismiss, Distort, Distract, Dismay) систематизує основні методи цих операцій. Порівняльний аналіз десяти методів аналізу джерел інформації, що охоплює період з 2008 по 2025 рік, демонструє чітку еволюцію від ізольованих статистичних підходів через графові методи до сучасних гібридних систем, що інтегрують обробку природної мови, графові нейронні мережі та механізми уваги. Найвищу продуктивність продемонстрували система Lightning (AUC 86,83%) та OnlineAgglomerative (точність 93,2%). Однак жоден з розглянутих методів одночасно не забезпечує комплексного семантичного, часового та мережевого аналізу для оцінки джерела. Щоб усунути цю прогалину, у статті пропонується концептуальна модель для оцінки подібності джерел інформації (similarity_score), яка інтегрує чотири компоненти: косинусна подібність вбудованого контенту, тематична кластеризація, часовий семантичний вплив для виявлення часово-семантичних залежностей між джерелами та мережева близькість у графі інформаційного потоку. Модель є розширюваною та може включати додаткові метрики, такі як аналіз настроїв, розпізнавання іменованих сутностей та оцінка токсичності. Також запропоновано архітектуру інформаційної системи для практичної реалізації на даних Telegram.

KEYWORDS аналіз інформаційних джерел, семантичний аналіз, мережевий аналіз, часова динаміка, координована поведінка.