Key words: OSPF, BGP, routing, multi-level architecture, routing protocols, Cisco Packet Tracer, convergence time, resource load.

Сведения об авторах

Кулнар Панабековна Аман – кандидат технических наук, доцент кафедры «Информатика и информационные технологии», Актюбинский региональный университет им. К. Жубанова, Республика Казахстан; e-mail: kulnar@inbox.ru. ORCID: https://orcid.org/0000-0002-0643-2280.

Алла Александровна Мусина* – магистр по направлению системный анализ и управление, преподаватель кафедры «Информатика и информационные технологии», Актюбинский региональный университет им. К. Жубанова, Республика Казахстан; e-mail: alla.mussina@mail.ru. ORCID: https://orcid.org/0000-0003-4179-4241.

Авторлар туралы мәліметтер

Күлнәр Панабекқызы Аман – техника ғылымдарының кандидаты, «Информатика және ақпараттық технологиялар» кафедрасының доценті, Қ. Жұбанов атындағы Ақтөбе өңірлік университеті,Қазақстан Республикасы; e-mail: kulnar@inbox.ru. ORCID: https://orcid.org/0000-0002-0643-2280.

Алла Александровна Мусина* – Жүйелік талдау және басқару мамандығы бойынша магистр, преподаватель кафедры «Информатика и информационные технологии», «Информатика және ақпараттық технологиялар» кафедрасының оқытушысы, Қ. Жұбанов атындағы Ақтөбе өңірлік университеті,Қазақстан Республикасы; e-mail: alla.mussina@mail.ru. ORCID: https://orcid.org/0000-0003-4179-4241.

Information about the authors

Kulnar Panabekovna Aman – Candidate of Technical Sciences, Associate Professor of the Department of «Informatics and Information Technologies», K. Zhubanov Aktobe Regional University, Republic of Kazakhstan; e-mail: kulnar@inbox.ru. ORCID: https://orcid.org/0000-0002-0643-2280.

Alla Alexandrovna Musina* – Master in the field of Systems Analysis and Control, Lecturer of the Department of «Informatics and Information Technologies», K. Zhubanov Aktobe Regional University, Republic of Kazakhstan; e-mail: alla.mussina@mail.ru. ORCID: https://orcid.org/0000-0003-4179-4241.

Поступила в редакцию 10.06.2025
Поступила после доработки 01.10.2025
Принята к публикации 06.10.2025

https://doi.org/10.53360/2788-7995-2025-4(20)-5

IRSTI: 28.23.13

B.Kh. Abdygalym[1,3], E. Adali[2], M.A. Sambetbayeva[1,3,*], Z.B. Sadirmekova[1], A.A. Nazymkhan[3]
[1]«Q» University,
050026, Republic of Kazakhstan, Almaty, str. Baizakov 125/185,
[2]Istanbul Technical University,
34437, Turkey, Istanbul, Beyoğlu, Inönü str. 65,
[3]L.N. Gumilyov Eurasian National University,
010008, Republic of Kazakhstan, Astana, Satpayev str. 2.
*e-mail: sambetbayeva_ma_1@enu.kz

A CONCEPTUAL MODEL FOR ONTOLOGY-BASED DETECTION OF INFORMATION OPERATIONS IN DIGITAL MEDIA

Abstract: *With the rapid growth of disinformation, cognitive manipulation and coordinated information campaigns in digital media, there is a need to develop intelligent methods for identifying and analyzing information operations. This paper proposes a conceptual model that integrates a multilingual annotated corpus, an ontological knowledge base and a semantic knowledge graph for the systematic study of mechanisms of information impact.*

The methodology of the research includes the construction of a specialized framework formed out of messages collected from Telegram channels, news portals and social networks. The data goes through a multi-level annotation using the Label Studio platform, where experts manually mark key entities, including military terms, target audiences, sources, actors, and emotional evaluations. The annotated corpus is semantically corresponded with the ontology of the subject field, formalized in OWL and enriched with the military thesaurus MIL_term, which provides consistency of terminology and support for multilingual analytics.

The ontological model is transformed into an RDF-graph of knowledge, reflecting the relationships between entities, events, tactics and narratives. SWRL-rules are used to identify hidden patterns, and the developed SPARQL-queries allow to extract complex analytical patterns, including chains of "actor – tactic – narrative – audience". The proposed approach forms the basis for complex analysis of information flows, early detection of threats and construction of analytical scenarios, which makes it applicable for research and monitoring of information operations in multilingual digital environments.

Key words: *Information operations, Ontology, Semantic Classification, NLP, OWL, SPARQL, Social media monitoring.*

Introduction

With the rapid development of digital communications and social media, modern information flows are becoming more intense, decentralized and dynamic. At the same time, the use of disinformation, cognitive manipulation and coordinated influence campaigns is increasing [1-2]. In such conditions, the identification, analysis and monitoring of information operations becomes a key task for both researchers and specialists in the field of information security and data analysis.

Traditional approaches based on simple statistical methods and heuristics show limited effectiveness when dealing with large amounts of unstructured data [3-5]. Modern information operations use complex narrative constructs, a network of interconnected actors and dynamic message propagation tactics, which makes the task of detecting and analyzing them much more difficult. In addition, the high multilingual nature of information flows – especially in the context of military and geopolitical conflicts – reinforces the need to develop new intellectual models to understand the context and semantics of messages.

In recent years, considerable attention has been paid to the application of ontologies, semantic technologies and knowledge graphs to analyze complex domains. Ontologies allow you to formalize entities, their attributes and relationships, providing a single view of knowledge, which is critical for integrating data from different sources. The use of RDF graphs in combination with SWRL rules and SPARQL queries allows you to automate the process of extracting hidden patterns and analyze complex information scenarios more efficiently.

However, existing solutions are mainly limited to either creating separate annotated enclosures or building ontologies without integrating them into a single analytical platform. This results in insufficient data connectivity, low interoperability, and limited ability to extract complex semantic patterns.

This paper proposes a comprehensive conceptual model for identifying and analyzing information operations in digital media, which combines:

- Multilingual annotated case, created on the basis of data from Telegram channels, news portals and social networks.
- Multi-level data annotation using the Label Studio platform, including markup of military terms, target audiences, sources, actors, timing, and emotional assessments.
- The ontology of the subject area, formalized in OWL 2 and enriched with the military thesaurus MIL_term, providing consistency of terms and multilingual support.
- An RDF knowledge graph that reflects relationships between entities, events, tactics, and narratives.
- SWRL-rules for logical inference of new knowledge and detection of hidden patterns.
- SPARQL queries for extracting complex knowledge structures and building analytical scenarios.

The key goal of the research is to develop a universal architecture that combines corpus linguistics, ontological modeling and semantic analysis to ensure effective monitoring and analytical research of information operations. Unlike existing works, the proposed model is not limited to the creation of a corpus or ontology, but integrates them into a single flexible analytical ecosystem that can adapt to dynamic changes in tactics and narratives in the digital environment.

The proposed conceptual model lays the basis for building intellectual tools for analyzing information flows, which is especially important in the conditions of increasing intensity of hybrid conflicts and cyber-information threats.

Related work

In recent years, research into identifying and analyzing information operations in digital media has intensified significantly due to the growth of large-scale disinformation campaigns, cognitive manipulation and hybrid attacks. Modern approaches rely on the use of ontologies, knowledge

graphs, SWRL rules and SPARQL queries to analyze the relationships between the actor, tactics, narrative and audience. However, existing solutions have limitations that our work seeks to overcome.

The worksheet [6] proposes influence Operation Ontology (IOO), which formalizes actors, audiences and tactics, which helps to identify key elements of attacks. However, IOO is focused on static scenarios and does not solve the problem of integrating data from multilingual sources. The alike Cyber Information Ontology [7] increases the interoperability of the data, but does not take into account the specifics of the military context and advanced semantic analysis. The worksheet [8] explores the use of ontologies to represent uncertain information, and [9] proposed ontology to analyze attacks in mixed reality. However, both approaches are limited to narrow scenarios and do not integrate annotated enclosures with semantic analysis.

The use of SWRL rules and SPARQL queries [10] allows the formation of hybrid semantic models, but they are limited to closed data sets and do not support the unification of multilingual information. The worksheet [11] considers the technologies of streaming processing RDF, but their application in annotated packages remains limited.

Unlike these worksheets, we offer a comprehensive conceptual model that combines annotated corpus (https://github.com/baiangali/multi_mil), ontological knowledge base (https://github.com/baiangali/mil_ontology), RDF graph and SWRL/SPARQL analysis into a single architecture. The integration of the military thesaurus MIL_term provides the processing of military terminology, and the combination of corpus linguistics, semantics and ontologies increases the accuracy, scalability and interpretability of the analysis of information operations.

Methodology

The development of a conceptual model for identifying information operations in digital media is based on the integration of corpus linguistics, ontological modeling and semantic technologies. The methodology includes successive stages:

- data collection;
- multi-level annotation;
- building ontology;
- formation of the RDF-graph of knowledge;
- application of SWRL rules to logical output;
- execution of SPARQL queries and analytical processing of results.

This comprehensive approach allows you to formalize entities, identify hidden relationships and build analysis scenarios aimed at early detection and monitoring of information operations.

The first stage was the creation of a multilingual corpus, assembled from Telegram channels, news portals and other digital platforms (Table 1). Parsing methods were used to extract data, including API, automatic message loading, keyword filtering, and time ranges. Particular attention was paid to the representativeness of the corps due to the variety of sources. After the data collection, the text was refined: Removal of links, HTML markup, emoji, media playholders and duplicates, as well as vocabulary normalization, lemmatization, tokenization and deletion of stop words, which provided a single data format for further annotation and integration into the ontological model.

Table 1 – Corpus statistics

Option	Value
Number of messages	1000
Total number of tokens	75.400
Number of annotated entities	6.970
Number of unique actors	480
Number of target audiences	310
Supported languages	Russian, English, Kazakh
Main sources	Telegram, Twitter, mass media
Storage format	JSON, CSV

The high saturation of the corpus is confirmed by the metric of information density:

$$D = \frac{Number\ of\ marked{-}up\ entities}{Total\ number\ of\ tokens} \quad (1)$$

For our corpus:

$$D = \frac{6970}{75400} \approx 0{,}092 \quad (2)$$

This value indicates a high concentration of semantically significant units, which makes the corpus an ideal basis for ontological analysis and the construction of an RDF-graph of knowledge.

The next step is a multi-level package annotation, which is performed by experts using the Label Studio platform. Markup is carried out in accordance with a single annotation guide and includes the identification of key entities: Military terms, target audiences, sources of information, actors, temporal and geographical references, as well as emotional evaluations of the text (Table 2). Additionally, the type of information impact is classified: Disinformation, demoralization, discrediting, provocation and creating panic.

Table 2 – Corpus Annotation Categories

Category	Number of labels	Examples of selected entities
MIL_TERM	2.450	«The command reported the use of [[multiple launch rocket systems]] MIL_term against enemy defensive positions».
TARGET_AUDIENCE	1.200	The main goal of the information campaign was [[population of border areas]] TARGET_AUDIENCE, among which rumors about the approaching offensive were actively spread
SOURCE	820	According to the data of [[Telegram-channel «Military Chronicle»]] source, in the eastern direction the military activity has been increased
ACTOR	1.100	The analytical report notes that the operation actively involved a block of countries [[NATO]] actor
EMO_EVAL	1.400	The publication caused [[panic among citizens]] EMO_eval, which increased social tensions in the region

Cohen's κ metric was used to estimate the consistency of the annotation, calculated by the formula:

$$k = \frac{P_0 - P_e}{1 - P_e} \quad (3)$$

Where P0 is the actual markup match between the annotations and Pe is the probability of a random match. In our case, k=0,84, which indicates high quality markup.

After the data was annotated, a formalized ontological layer was developed, created in OWL 2 format using Protégé. Ontology describes the main entities (Figure 1): Actors, tactics, narratives, audiences, and information channels. Unlike existing solutions, we have integrated the military thesaurus MIL_term, which allows for multilingual support and terminological consistency.

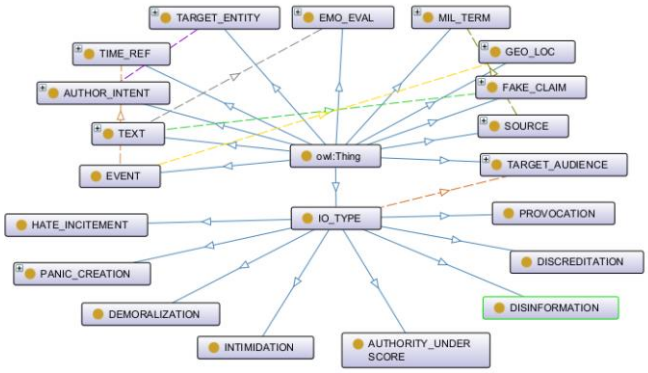

Figure 1 – Structure of the ontological model for the analysis of information operations

On the basis of ontology, an RDF-knowledge graph is built, which visualizes the relationships between entities and events (Figure 2). Such a graph allows you to represent complex relationships, for example, to identify chains: «actor uses tactics → shapes narrative → impacts audience → spreads through source». The RDF graph provides knowledge integration and support for semantic queries.

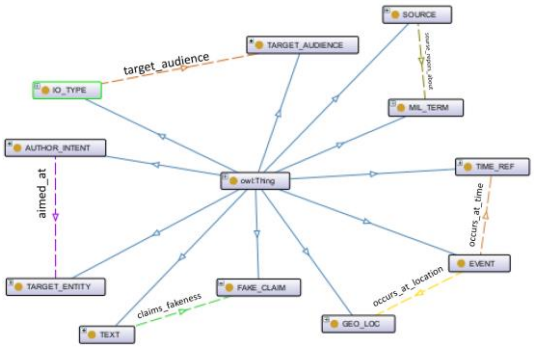

Figure 2 – semantic scheme of interrelations of ontology of information operations

To expand analytical capabilities, SWRL-rules are used, which provide a logical conclusion of new knowledge. For example, the following rule allows you to identify coordinated information operations:

$$Actor(x) \wedge UsesTactic(x,y) \wedge TargetAudience(x,z) \Rightarrow CoordanationIO(x) \qquad (4)$$

This means that if one actor uses the same tactics and affects one audience, then he is classified as a participant in a coordinated information attack.

The final step of the methodology is to perform SPARQL queries to extract knowledge from the RDF graph (Figure 3). These queries allow you to form flexible samples and identify hidden patterns.

SPARQL query:

```
PREFIX ex: <http://example.org/io#>

SELECT ?source ?sourceName ?term ?termLabel
WHERE {
 ?source a ex:SOURCE ;
       ex:sourceName ?sourceName ;
       ex:source_reports_about ?term .
 ?term ex:militaryTerm ?termLabel .
}
ORDER BY ?sourceName
```

source	sourceName	term	
Source001	"Telegram-канал"^^<http://www.w3.org/2001	MilitaryTerm001	"армия Казахстана"^^<http://www.w3.org/2001/XMLSchema#string>
Source002	"Анонимный паблик"^^<http://www.w3.org/2	MilitaryTerm002	"контратака дивизии"^^<http://www.w3.org/2001/XMLSchema#string>

Figure 3 – Visualization of the result of the SPARQL query

The execution of these queries allows us to identify key patterns: Frequency of references to actors, tactics used, emotional coloring and dynamics of changing narratives over time.

The proposed methodology is unique in that it combines annotated corpus, ontology, RDF graph, SWRL rules and SPARQL queries into a single analytical ecosystem (Figure 4). This provides a higher accuracy of knowledge extraction, interpretability of analytical results and the ability to scale the system to new information threats.

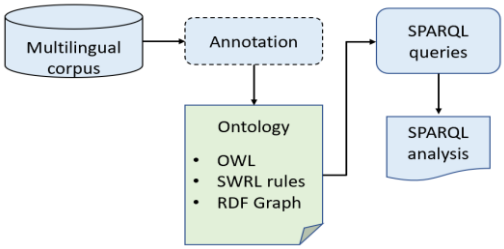

Figure 4 – Scheme of the analytical platform for identifying information operations

Results

The developed conceptual model was tested on a multilingual message body collected from Telegram channels, news portals, which allowed to conduct a comprehensive analysis of information flows, identify key actors, tactics and narratives, and determine the structure of hidden information

operations. The corpus contained 1000 messages, including more than 75.400 tokens and 6.970 tagged entities annotated by experts in Label Studio in six categories. On the basis of the case, a complete ontological model was created, which allowed to integrate knowledge in the form of an RDF graph and apply SWRL-rules for logical inference of hidden relations.

The analysis of the annotation showed a high informativeness of the data (Table 3). The greatest density of information markers was demonstrated by messages related to military terminology and direct mention of actors, which confirms the relevance of the selected sources for building the model. Cohen's κ's inter-agency consent metric was 0,84, which indicates a high consistency of markup and corpus quality.

Table 3 – frequency of annotated entities

Category	Number of labels	Share (%)
MIL_TERM	2.450	35.1
TARGET_AUDIENCE	1.200	17.2
SOURCE	820	11.8
ACTOR	1.100	15.8
EMO_EVAL	1.400	20.1
Total	6.970	100

On the basis of the marked case, an ontology of information operations was built, developed in OWL 2 format using Protégé, which allowed to formalize 62 classes, 128 properties and 3.450 individuals associated with tactics, narratives, audiences and sources of messages (Figure 5).

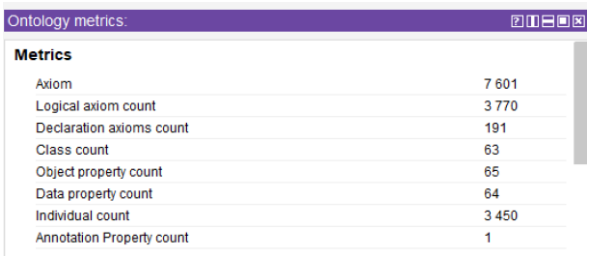

Figure 5 – the main characteristics of the ontology of information operations

To ensure terminological consistency, the military thesaurus MIL_term was integrated into ontology, which includes 2.450 terms in Russian, English and Kazakh languages. Ontology served as the basis for the construction of the RDF-graph of knowledge, which consists of 15.240 triplets and describes the relationships between actors, tactics, narratives and target audiences. This graph allowed us to move from simple data categorization to the construction of complex semantic patterns necessary for the analysis of information attacks.

SWRL rules and SPARQL queries were used for analytical data processing. SWRL provided a logical conclusion of new knowledge. After applying the rules to the RDF graph, it was possible to identify 327 unique patterns of «actor-tactic-audience» associated with 145 key narratives.

As a result of the conducted experiments, the effectiveness of the proposed conceptual model was proved. This approach demonstrates a significant superiority over traditional methods of text analysis, since the integration of annotated corpus, ontology, RDF-graph and SPARQL-queries allows for multi-level semantic analysis and interpretive analytical results applicable to the detection of threats in digital media.

Discussion

The results of the study show that the developed conceptual model provides a new level of analysis of information operations in digital media. The experiments confirmed that the proposed approach allows to identify key actors, their tactics, hidden narratives and coordinated strategies of message distribution, as well as network interconnections between sources. Unlike existing text analysis methods, the model combines an annotated corpus, ontological knowledge base and an RDF graph, which provides semantic understanding of data and a formalized representation of knowledge about the subject area.

The use of a corpus containing more than 6.970 labeled entities allowed military terms, emotional assessments and tactics to be linked to formalized classes of ontology, increasing the

accuracy of the analysis. The integration of the MIL_term thesaurus provided multilingual support (Russian, English, Kazakh) and expanded the applicability of the model for local and international scenarios. The built RDF knowledge graph of more than 15.000 triplets visualizes complex connections between actor, tactics, narrative, and audience. The experiments revealed 327 unique patterns, including 57 cases of coordinated attacks.

Dynamic analysis showed that during periods of high conflict activity, the number of attacks increases by more than 89%, which demonstrates the potential of the model for early monitoring of information threats. Compared to existing studies, the proposed approach provides higher accuracy and scalability due to the integration of SPARQL queries, SWRL rules and annotated enclosure.

Thus, the developed conceptual model forms a universal analytical platform for monitoring, identifying and analyzing information operations, combining linguistic, semantic and ontological methods and opening up opportunities for application at the national and international levels.

Conclusion and outcomes

This paper presents a conceptual model for identifying information operations in digital media, based on the integration of multilingual annotated corpus, ontological modeling, RDF knowledge graph, SWRL rules and SPARQL queries. The developed corpus includes 1000 messages and more than 6970 labeled entities, which allowed to create an ontology of the subject area in OWL 2 format, integrated with the military thesaurus MIL_term to provide terminological consistency and multilingual support. The built RDF graph of more than 15.000 triplets reflects the relationships between actors, tactics, narratives and audiences, allowing you to identify complex scenarios of information attacks. The experiments found 327 patterns, including 57 coordinated operations, and dynamic analysis showed a 89% increase in attack activity. The developed architecture forms the basis for intelligent systems for monitoring and analyzing information threats at the national and international levels.

References

1. Abdali S. Multi-modal misinformation detection: Approaches, challenges and opportunities / S. Abdali, S. Shaham, B. Krishnamachari // ACM Computing Surveys. – 2024. – Vol. 57, № 3. – P. 1-29.
2. From Virality to veracity / J. Rieskamp et al // Examining False Information on Telegram vs. Twitter. – 2024.
3. Zhao J. et al. Research on domain ontology construction based on the content features of online rumors. – 2024. – Vol. 14, № 1. – P. 12134.
4. Detecting propaganda techniques in code-switched social media text / M.U. Salman et al // arXiv preprint arXiv:2305.14534. – 2023.
5. Alghamdi J. Fake news detection in low-resource languages: A novel hybrid summarization approach / J. Alghamdi, Y. Lin, S. Luo // Knowledge-based Systems. – 2024. – Vol. 296. – P. 111884.
6. The influence Operation Ontology (IOO) / A.D.C. Tudela et al // arXiv preprint arXiv:2503.07304. – 2025.
7. A common core-based cyber ontology in support of cross-domain situational awareness / B. Donohue et al // ground/air multisensor interoperability, integration, and networking for persistent ISR IX. – SPIE, 2018. – Vol. 10635. – P. 65-74.
8. Partridge C. digitalizing uncertain Information / C. Partridge, A. Mitchell, A. Cola //arXiv preprint arXiv:2507.21173. – 2025.
9. SOK: Come together–unifying Security, Information Theory, and cognition for a Mixed Reality deception attack Ontology & Analysis Framework / A. Teymourian et al // arXiv preprint arXiv:2502.09763. – 2025.
10. Zhang L., Lobov A. Semantic web rule language-based approach for implementing knowledge-based engineering systems. – 2024. – Vol. 62. – P. 102587.
11. Languages and systems for RDF stream processing, a survey / P. Bonte et al // The VLDB Journal. – 2025. – Vol. 34, № 4. – P. 50.

Funding: *This research has been funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan Grant AP26195165.*

Б.Х. Абдығалым[1,3], Е. Adali[2], М.А. Самбетбаева[1,3,*], Ж.Б. Садирмекова[1], А.А. Назымхан[3]
[1]«Q» University,
050026, Қазақстан Республикасы, Алматы, Байзақова к. 125/185,
[2]Стамбул техникалық университеті,
34437, Туркия, Стамбул, Бейоглу, Иненю к. 65,
[3]Л.Н. Гумилев атындағы Евразия ұлттық университеті,
010008, Қазақстан Республикасы, Астана, Сатпаев к. 2.
*e-mail: sambetbayeva_ma_1@enu.kz

САНДЫҚ МЕДИАДАҒЫ АҚПАРАТТЫҚ ОПЕРАЦИЯЛАРДЫ АНЫҚТАУ ОНТОЛОГИЯСЫНЫҢ ТҰЖЫРЫМДАМАЛЫҚ МОДЕЛІ

Дезинформация ауқымының, когнитивті манипуляциялардың және цифрлық медиадағы Үйлестірілген ақпараттық науқандардың қарқынды өсуі жағдайында ақпараттық операцияларды анықтау және талдау үшін Интеллектуалды әдістерді әзірлеу қажеттілігі туындайды. Бұл жұмыста ақпараттық әсер ету механизмдерін жүйелі түрде зерттеу үшін көп тілді аннотацияланған корпусты, білімнің онтологиялық базасын және білімнің семантикалық графигін біріктіретін тұжырымдамалық модель ұсынылады.

Зерттеу әдістемесі Telegram арналарынан, жаңалықтар порталдарынан және әлеуметтік желілерден жиналған хабарламалардан тұратын арнайы корпус құруды қамтиды. Деректер label Studio платформасын қолдана отырып, көп деңгейлі аннотациядан өтеді, мұнда сарапшылар негізгі нысандарды, соның ішінде әскери терминдерді, мақсатты аудиторияларды, дереккөздерді, актерлерді және эмоционалды бағалауды қолмен белгілейді. Аннотацияланған корпус OWL-де рәсімделген және mil_term әскери тезаурусымен байытылған доменнің онтологиясына семантикалық түрде сәйкес келеді, бұл терминологияның дәйектілігін және көптілді аналитиканы қолдауды қамтамасыз етеді.

Онтологиялық модель субъектілер, оқиғалар, тактика және әңгімелер арасындағы байланысты көрсететін білімнің RDF графигіне айналады. Жасырын заңдылықтарды анықтау үшін swrl ережелері қолданылады, ал SPARQL әзірлеген сұраулар күрделі аналитикалық заңдылықтарды, соның ішінде "актор – тактика – әңгіме – аудитория" тізбегін алуға мүмкіндік береді. Ұсынылған тәсіл ақпараттық ағындарды кешенді талдауға, қауіптерді ерте анықтауға және аналитикалық сценарийлерді құруға негіз болады, бұл оны көп тілді цифрлық ортадағы ақпараттық операцияларды зерттеуге және бақылауға қолдануға мүмкіндік береді.

Түйін сөздер: *Ақпараттық операциялар, онтология, семантикалық классификация, NLP, OWL, SPARQL, әлеуметтік медиа мониторингі.*

Б.Х. Абдығалым[1,3], Е. Adali [2], М.А. Самбетбаева[1,3,*], Ж.Б. Садирмекова[1], А.А. Назымхан[3]
[1]«Q» University,
050026, Республика Казахстан, Алматы, ул. Байзакова 125/185,
[2]Стамбульский технический университет,
34437, Турция, Стамбул, Бейоглу, ул. Иненю 65,
[3]Евразийский национальный университет имени Л.Н. Гумилева,
010008, Республика Казахстан, Астана, ул. Сатпаева 2.
*e-mail: sambetbayeva_ma_1@enu.kz

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ДЛЯ ОНТОЛОГИЙ ВЫЯВЛЕНИЯ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ В ЦИФРОВЫХ МЕДИА

В условиях стремительного роста масштабов дезинформации, когнитивных манипуляций и координированных информационных кампаний в цифровых медиа возникает необходимость разработки интеллектуальных методов для выявления и анализа информационных операций. В данной работе предлагается концептуальная модель, интегрирующая мультиязычный аннотированный корпус, онтологическую базу знаний и семантический граф знаний для систематического исследования механизмов информационного воздействия.

Методология исследования включает построение специализированного корпуса, сформированного из сообщений, собранных с Telegram-каналов, новостных порталов и социальных сетей. Данные проходят многоуровневую аннотацию с использованием платформы Label Studio, где эксперты вручную размечают ключевые сущности, включая военные термины, целевые аудитории, источники, акторов и эмоциональные оценки. Аннотированный корпус семантически согласуется с онтологией предметной области, формализованной в OWL и обогащённой военным тезаурусом MIL_TERM, что обеспечивает согласованность терминологии и поддержку многоязычной аналитики.

Онтологическая модель преобразуется в RDF-граф знаний, отражающий взаимосвязи между сущностями, событиями, тактиками и нарративами. Для выявления скрытых закономерностей применяются SWRL-правила, а разработанные SPARQL-запросы позволяют извлекать сложные аналитические паттерны, включая цепочки «актор – тактика – нарратив – аудитория». Предложенный подход формирует основу для комплексного анализа информационных потоков, раннего выявления угроз и построения аналитических сценариев, что делает его применимым для исследования и мониторинга информационных операций в мультиязычных цифровых средах.

Ключевые слова: *Информационные операции, онтология, Семантическая классификация, NLP, OWL, SPARQL, мониторинг социальных сетей.*

Сведения об авторах

Баянғали Хайерберліұлы Абдығалым – магистр технических наук, докторант кафедры информационных систем, Евразийский национальный университет имени Л.Н. Гумилева, Инженер программист «Q» University, Республика Казахстан; e-mail: bayangali.abd@gmail.com. ORCID: https://orcid.org/0009-0001-8872-7428.

Eşref Adali – доктор наук, профессор факультета вычислительной техники и информатики, Стамбульский технический университет, Стамбул, Турция; e-mail: esrefadali@gmail.com.

Мадина Аралбаевна Самбетбаева* – Phd, ассоциированный профессор кафедры информационных систем, Евразийский национальный университет имени Л.Н. Гумилева, ведущий научный сотрудник «Q» University, Республика Казахстан; e-mail: sambetbayeva_ma_1@enu.kz. ORCID: https://orcid.org/0000-0001-9358-1614.

Жанна Бакировна Садирмекова – ведущий научный сотрудник «Q» University, ассоциированный профессор, Республика Казахстан; e-mail: Janna_1988@mail.ru. ORCID: https://orcid.org/0000-0002-7514-9315.

Ақсәуле Абзалқызы Назымхан – магистрант кафедры информационных систем, Евразийский национальный университет имени Л.Н. Гумилева, Республика Казахстан; e-mail: aksaulenazymhan@gmail.com.

Авторлар туралы мәліметтер

Баянғали Хайерберліұлы Абдығалым – техникалық ғылымдар магистрі, ақпараттық жүйелер кафедрасының докторанты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, «Q» University бағдарламашы инженері, Қазақстан Республикасы; e-mail: bayangali.abd@gmail.com. ORCID: https://orcid.org/0009-0001-8872-7428.

Eşref Adali – ғылым докторы, Есептеу техникасы және информатика факультетінің профессоры, Стамбул техникалық университеті, Стамбул, Түркия; e-mail: esrefadali@gmail.com.

Мадина Аралбайқызы Самбетбаева* – PhD, Ақпараттық жүйелер кафедрасының қауымдастырылған профессоры, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, «Q» University жетекші ғылыми қызметкері, Қазақстан Республикасы; e-mail: sambetbayeva_ma_1@enu.kz. ORCID: https://orcid.org/0000-0001-9358-1614.

Жанна Бакировна Садирмекова – «Q» University жетекші ғылыми қызметкері, қауымдастырылған профессор, Қазақстан Республикасы; e-mail: Janna_1988@mail.ru. ORCID: https://orcid.org/0000-0002-7514-9315.

Ақсәуле Абзалқызы Назымхан – Ақпараттық жүйелер кафедрасының магистранты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Қазақстан Республикасы; e-mail: aksaulenazymhan@gmail.com.

Information about the authors

Bayangali Khayerberliuly Abdygalym – master of technical sciences, Phd student of the Department of Information Systems, L.N. Gumilyov Eurasian National University, Software engineer at «Q» University, Republic of Kazakhstan; e-mail: bayangali.abd@gmail.com. ORCID: https://orcid.org/0009-0001-8872-7428.

Eşref Adali – doctor of sciences, professor at the Faculty of Computer Engineering and Informatics, Istanbul Technical University, Istanbul, Turkey; e-mail: esrefadali@gmail.com.

Madina Aralbaevna Sambetbaeva* – PhD, associate professor of the Department of Information Systems, L.N. Gumilyov Eurasian National University, leading researcher at Q University, Republic of Kazakhstan; e-mail: sambetbayeva_ma_1@enu.kz. ORCID: https://orcid.org/0000-0001-9358-1614.

Zhanna Bakirovna Sadirmekova – leading researcher at Q University, associate professor, Republic of Kazakhstan; e-mail: Janna_1988@mail.ru. ORCID: https://orcid.org/0000-0002-7514-9315.

Aksaule Abzalkyzy Nazimkhan – master's student of the Department of Information Systems, L.N. Gumilyov Eurasian National University, Republic of Kazakhstan; e-mail: aksaulenazymhan@gmail.com.

Received 23.09.2025
Accepted 21.10.2025