ФОРМУВАННЯ ТЕОРЕТИКО-ГРАФОВОЇ МОДЕЛІ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ МЕНТАЛЬНОЇ ВІЙНИ

Качинський А. Б.[1], Ланде Д. В.[1]

[1]*Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»*
dwlande@gmail.com, akachynsky@gmail.com

У роботі запропоновано розширену мережеву модель інформаційно-психологічних ментальних війн, яка базується на формалізації через ієрархію з п'яти рівнів та подальшому перетворенні її на мережу з використанням великих мовних моделей (LLM). Мета дослідження – удосконалити існуючу ієрархічну модель шляхом автоматичного розширення понятійної бази, виявлення нових семантичних зв'язків та їх кластеризації для глибшого аналізу структури ментального впливу. За допомогою LLM, отримано мережу з понад 300 ключових понять, які описують цілі, акторів, засоби, політики та результати ментальної війни. Проаналізовано зв'язки між елементами, сформовано граф мережі, який було проаналізовано і візуалізовано у системі Gephi. Результати показали, що ментальні війни формуються через комплекс взаємодіючих факторів, серед яких домінують символічні, емоційні та когнітивні механізми. Отримана модель може служити основою для подальшого дослідження інструментів психологічного впливу, акторів інформаційної дії, а також способів протидії таким формам війни.

Ключові слова: інформаційно-психологічна ментальна війна, розширена мережева модель, штучний інтелект, великі мовні моделі

Вступ

Мета цієї роботи – розширити й удосконалити модель інформаційно-психологічних ментальних війн – сучасного

інформаційно-психологічного протистояння за допомогою великих мовних моделей (LLMs).

Останніми роками штучний інтелект (ШІ), зокрема великі мовні моделі [1-3] відкрив нові можливості для аналізу та моделювання семантичних мереж. Використання ШІ не лише дозволяє вдосконалювати наявні моделі, а й виявляти нові аспекти, які раніше залишалися поза увагою дослідників [4].

Спочатку модель «інформаційно-психологічної ментальної війна» розглядається як комплексна мережа з ієрархічною структурою [5].

Нехай $(H, \leq)$ – скінченна частково впорядкована множина з найбільшим елементом b. Множина H називається ієрархією, якщо виконуються наступні умови:

1. Існує розбиття множини H на шари (рівні ієрархії):

$$H = L_1 \bigcup L_2 \bigcup ... \bigcup L_h,$$

де $L_1 = \{b\}$ – перший рівень ієрархії містить лише найбільший елемент; $L_k \bigcap L_j = \varnothing$ для всіх $k \neq j$ – ці підмножини не перетинаються.

Кожен елемент з H належить рівно одному з L_k. Ці множини L_k називають шарами або рівнями ієрархії.

2. Умова сумісності з порядком:

Якщо $x < y$ і $y \in L_k$, то $x \in L_m$, де $m > k$.

Інакше кажучи, якщо один елемент менший за інший, то він повинен знаходитись на нижчому рівні ієрархії.

3. Умова послідовності (спадного/зростаючого переходу):

Для кожного елемента $x \in H$:

Якщо x^- – попередник x (тобто $x^- < x$, і немає жодного елемента z такого, що $x^- < z < x$), то $x^- \in L_{k+1}$, якщо $x \in L_k$.

Аналогічно, якщо x^+ – наступник x (тобто $x < x^+$, і немає елемента z, для якого $x < z < x^+$), то $x^+ \in L_{k-1}$, якщо $x \in L_k$.

Тобто кожен попередник лежить на наступному рівні, а кожен наступник – на попередньому рівні.

При такому розгляді проблему можна розкласти на простіші компоненти, після чого оцінити відносний ступінь взаємодії між елементами цієї ієрархічної структури.

У комплексній мережі «інформаційно-психологічної ментальної війни» можна виділити п'ять рівнів L_i:

L_1 – цілі ментальної війни;

L_2 – сили та засоби ментальної війни;

L_3 – актори ментальної війни;

L_4 – цілі акторів;

L_5 – політики, що реалізуються акторами.

Математична модель допомагає формалізувати взаємодії між підсистемами за допомогою графів, матриць зв'язків та цільових функцій, які описують загальну ефективність системи.

Рівні L_1 та L_4 ієрархії включають певні набори цілей і підцілей. Нехай на рівні i є набір цілей $T_i = \{T_{i1}, T_{i2}, \ldots, T_{imi}\}$, де $i = \{1, 4\}$, а mi – кількість цілей на рівні i. Кожній цілі T_{ij} відповідає набір підцілей $F_{ij} = \{F_{ij1}, F_{ij2}, \ldots, F_{ijn}\}$, де ijn – кількість підцілей для цілі T_{ij}.

Елементи та підцілі на кожному рівні виконують конкретні функції (інформаційні, економічні, організаційні тощо) і можуть бути пов'язані з іншими елементами та підцілями F_{ijk} на тому ж або інших рівнях, утворюючи мережу взаємозв'язків. Це описується набором функціональних зв'язків між елементами та підцілями:

$$Links = \{(F_{ijk}, F_{i'j'k'}) \mid F_{ijk} \text{ is linked to } F_{i'j'k'}\}.$$

Набір функціональних зв'язків між елементами, цілями та підцілями формує граф, у якому вершинами є елементи, підцілі та цілі F_{ijk}, а ребрами – зв'язки між ними.

Для моделювання процесу досягнення головних цілей на кожному рівні можна визначити цільову функцію

системи «ментальної війни» Φ, яка залежить від виконання цілей і підцілей на різних рівнях:

$$\Phi = \alpha\, f(T_{ij}) + \beta\, (F_{ijk}),$$

де α, β – вагові коефіцієнти у межах інтервалу зі значеннями в діапазоні [0,1].

Розширення ієрархічної моделі до мережевої

У ієрархії ментальних воєн підцілі та концепти на кожному рівні визначаються експертами, у тому числі віртуальними [3], які допомагають формувати систему цілей. Якщо концепти можуть належати до кількох рівнів одночасно, ієрархія перетворюється на мережу, що ускладнює зв'язки між рівнями.

Якщо концепт f_i належить до кількох рівнів одночасно, це вводить нові зв'язки між рівнями. Таким чином, структура системи змінюється з чистої ієрархії на мережеву модель.. Якщо поняття f_i належить рівням T_a та T_b, то між цими рівнями існує зв'язок:

$$E = \left\{ (T_a, T_b) \mid f_i \in F,\, f_i \in T_a \cap T_b \right\}.$$

Ця формалізація відповідає послідовності дій, що передбачає можливість повторення процесу під наглядом експерта до досягнення остаточного розуміння предметної області:

1. Формування початкової схеми із відображенням базових зв'язків між поняттями.
2. Створення промптів для LLM з метою генерації нових понять і зв'язків.
3. Інтеграція нових зв'язків у початкову схему.
4. Обробка лінгвістичних даних – оцінювання нових та існуючих зв'язків, а також ранжування вузлів.
5. Аналіз даних і візуалізація шляхом завантаження даних у систему аналізу графів.
6. Формування та уточнення кластерів, визначення їхніх назв за допомогою LLM.
7. Фінальна перевірка та валідація розширеної моделі.

Аналіз і візуалізація

Об'єднані дані завантажуються в середовище програми Gephi для кластеризації на основі класів модулярності (рис. 1).

Серед понад 300 вузлів розширеної мережі отримані такі важливі поняття, що є суттєвими для розуміння суті інформаційно-психологічних ментальних війн:

- політика мовного контролю;
- маніпуляція страхом;
- символіка влади;
- формування нової свідомості;
- когнітивна перебудова;
- соціальна напруженість;
- критика інституцій;
- емоційна маніпуляція.

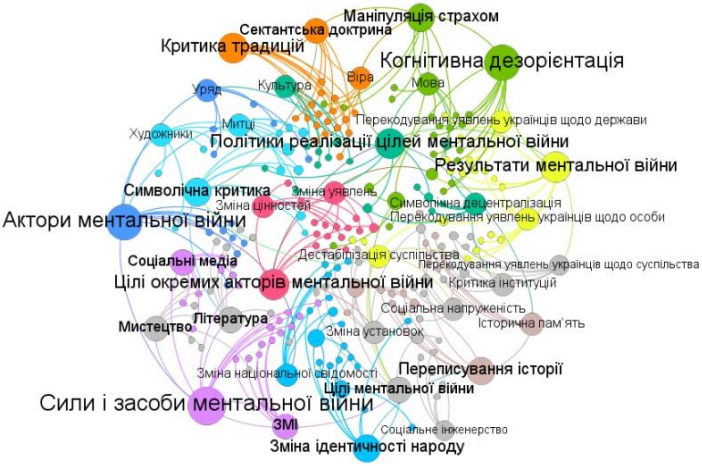

Рисунок 1. Розширена мережева модель ментальних війн

Висновки

Отримана розширена модель інформаційно-психологічних ментальних війн демонструє складну мережу зв'язків між ключовими та додатковими концептами, яка суттєво доповнює традиційне розуміння цієї теми. Застосування великих мовних моделей дозволило не лише автоматизувати процес формування понятійного апарату, а й виявити приховані семантичні залежності, важливі для стратегічного аналізу. Ієрархічна модель, запропонована на початковому етапі, недостатня для опису реальних взаємозв'язків. Перетворення її на мережеву модель забезпечило гнучкість та адаптивність до багаторівневого сприйняття, коли окремі поняття можуть одночасно належати кільком шарам системи, утворюючи нетривіальні зв'язки.

Кластеризація та ранжирування вузлів у рамках графової моделі надали можливість виокремити найбільш значущі концепти, які впливають на структуру ментальної війни. Серед них – політика мовного контролю, маніпуляція страхом, когнітивна перебудова, соціальна напруженість та емоційна маніпуляція. Ці елементи є центральними в механізмах символічного, психологічного та соціального впливу.

Таким чином, отримана мережева модель ментальних війн є динамічною, розширюваною та повторно використовуваною, що забезпечує її придатність як наукового інструменту для подальших досліджень в області інформаційно-психологічного впливу, протидії ментальним агресивним стратегіям, а також аналізу акторів та їхньої ролі в медійному просторі.

Список використаних джерел

1. Lande D., Strashnoy L. *GPT Semantic Networking: A Dream of the Semantic Web - The Time is Now*. Kyiv: Engineering, 2023. ISBN 978-966-2344-94-3.

2. Srinivasan Ramanujam. *The LLM Revolution: Transforming Industries with Large Language Models.* Kindle

Edition, 2024. https://www.amazon.com/ LLM-Revolution-Transforming-Industries-Language-ebook/dp/B0D7VS5BNK

3. Lande D., Strashnoy L. *Causality Network Formation with ChatGPT*. SSRN Electronic Journal. (May 30, 2023). – 16 p. DOI: 10.2139/ssrn.4464477

4. Lande Dmytro. OSINT in Cybersecurity: Educational Manual. – Kyiv: LLC "Engineering", 2024. – 522 p.

5. Kachynskyi A. The structural-functional model of the system for ensuring informational and informational-psychological security. Reports of the National Academy of Sciences of Ukraine, 2023. №1. pp. 16-23. (ukr. lang)

6. Wu F. Y. *The Potts model*. Rev. Mod. Phys. 54, 235 – Published 1 January 1982

ЗМІСТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

THEORETICAL AND APPLIED CYBERSECURITY

Матеріали III Всеукраїнської науково-практичної конференції

Випуск 3

Київ – 2025

Рекомендовано до друку Вченою радою
КПІ ім. Ігоря Сікорського
(протокол № 8 від 08 вересня 2025 р.)

Theoretical and Applied Cybersecurity. Матеріали III Всеукраїнської науково-практичної конференції (TACS-2025). – Київ: Політехніка. – 320 с.

До збірника увійшли матеріали доповідей, представлених на III Всеукраїнській науково-практичній конференції Theoretical and Applied Cybersecurity (TACS-2025, 29 травня 2025 р., м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням безпечного функціонування кіберпростору, безпеки промислових систем та систем критичної інфраструктури, криптографічних проблем кібернетичної безпеки, запобігання і протидії кібератакам, моделювання та протидії інформаційним операціям, технологій інформаційно-аналітичних досліджень на основі відкритих джерел інформації, застосування штучного інтелекту тощо.

Наведені матеріали з актуальних проблем інформаційної та кібернетичної безпеки, можливості застосування штучного інтелекту, системного аналізу при забезпеченні підтримки прийняття рішень, комп'ютерного моделювання процесів і систем.

Для фахівців у сфері інформаційних технологій, інформаційної і кібернетичної безпеки, а також для аспірантів і студентів старших курсів вищої школи відповідних спеціальностей.