Preprint

Generative Artificial Intelligence and Semantic Networking in the Legal Domain

Edited by

Professor Dmytro Lande

2025

FOREWORD

The collection of abstracts *"Generative Artificial Intelligence and Semantic Networking in the Legal Domain"* (edited by Professor Dmytro Lande, 2025) addresses current scientific and practical issues in the application of generative AI within public administration, with a particular focus on parliamentary oversight. The contributing authors explore methods for constructing dynamic semantic networks, introduce no-code frameworks with iterative self-control to counteract large language model (LLM) "hallucinations," employ RAG-based architectures for updating legal knowledge, and propose approaches for detecting cognitive threats, linguistic backdoors, and adversarial AI. Special emphasis is placed on the development of intelligent autonomous monitoring, modeling, and forecasting systems grounded in semantic analysis and integrated with national digital platforms such as Diia, e-Parliament, and ProZorro. The publication is intended for researchers, legal professionals, public officials, and AI system developers working on intelligent decision-support tools in law and governance.

FOREWORD

The modern world is undergoing a profound transformation driven by the exponential advancement of digital technologies, and particularly by generative artificial intelligence (GenAI). This transformation affects all spheres of social life, but its impact is felt most acutely in the legal domain, where issues of accuracy, transparency, accountability, and the rule of law are no longer merely academic—they have become strategic priorities. Ukraine, which amid wartime conditions is simultaneously building a digital state and modernizing democratic institutions, stands at the forefront of this global challenge. Consequently, scholarly research aimed at understanding and formalizing the interaction between artificial intelligence and the legal system has acquired exceptional relevance.

This collection addresses pressing issues related to the application of contemporary artificial intelligence technologies in public administration, with a particular focus on parliamentary oversight – one of the key mechanisms ensuring government accountability to society. The authors do not merely analyze the capabilities of GenAI for processing legal texts; they propose formalized, structured, and interpretable approaches that guarantee not only efficiency but also reliability, verifiability, and security of outcomes. From no-code programming with iterative self-control (to combat LLM "hallucinations") to RAG-based architectures for dynamic semantic network construction—each contribution illustrates a transition from intuitive GenAI use toward the development of intelligent control systems capable of autonomous analysis, modeling, and forecasting.

Special attention is given to the semantic dimension. In the legal sphere, what matters is not only the existence of a link between concepts but also its substantive nature: is it a technical error, lobbying influence, cognitive manipulation, or a systemic risk? To address this, the authors introduce novel metrics such as semantic betweenness centrality, as well as ranking and clustering methods that integrate both structural and semantic features. This enables users not merely to “see” a network but to understand its logic, identify critical influence nodes, and predict the consequences of legislative changes.

The collection also confronts urgent security challenges, particularly adversarial AI and linguistic backdoors—covert mechanisms of manipulation that can undermine trust in the legal system from within. The authors propose not only diagnostics for such threats but also countermeasures grounded in the integration of technological, legal, and ethical approaches.

The scholarly works presented in this volume result from fruitful collaboration among experts in computer science, cybersecurity, jurisprudence, and public administration. They reflect not just theoretical reflections but practice-oriented solutions already being implemented or integrated with state digital platforms such as Diia, e-Parliament, ProZorro, and others.

The publication of this collection aims to further advance the fields of information law, legal informatics, and intelligent decision-support systems in Ukraine. We hope it will serve as a valuable resource for researchers, practitioners, civil servants, legislators, and all those interested in the future of the legal system in the age of artificial intelligence.

Professor Dmytro Lande

Kyiv, 2025

CONTENTS

1. Artificial Intelligence in Public Administration: From Text Analysis to an Intelligent Parliamentary Oversight System (D. Lande, V. Furashev)
2. Application of a No-Code Programming Framework Based on Large Language Models in the Legal Domain (D. Lande, Y. Danyk, L.Strashnoy)
3. RAG Architecture for Dynamic Creation of Semantic Networks in the Legal Domain (D. Lande, O. Rybak)
4. Query Dispatcher for Heterogeneous Environments in Legal Document Analysis (D. Lande, V. Kuzminskyi)
5. Semantic Betweenness Centrality of Nodes in Cognitive Networks (D. Lande, A. Kachynskyi)
6. Adversarial Artificial Intelligence in the Legal Domain (D. Lande, Y. Danyk)
7. Ranking and Clustering Of Concepts in a Cognitive Warfare Graph Model Using PCA and LLMs (D. Lande, A. Kachynskyi)

Генеративний Штучний Інтелект і Семантичний Нетворкінг у Правовій Сфері

під редакцією

професора Дмитра Ланде

2025

АНОТАЦІЯ

Збірку тез *«Генеративний штучний інтелект і семантичний нетворкінг у правовій сфері»* (під редакцією професора Дмитра Ланде, 2025) присвячено актуальним науковим та практичним аспектам застосування генеративного ШІ в державному управлінні, зокрема в контексті парламентського контролю. У роботах колективу авторів розглядаються методи побудови динамічних семантичних мереж, безкодові фреймворки з ітеративним самоконтролем для запобігання «галюцинаціям» великих мовних моделей, архітектура RAG для актуалізації правових знань, а також підходи до виявлення когнітивних загроз, лінгвістичних бекдорів та змагального ШІ. Особливу увагу приділено розробці інтелектуальних систем автономного моніторингу, моделювання та прогнозування на основі семантичного аналізу, інтегрованих із національними цифровими платформами. Видання орієнтоване на науковців, юристів, державних службовців і розробників інтелектуальних систем підтримки прийняття рішень у сфері права та управління.

ПЕРЕДМОВА

Сучасний світ переживає глибоку трансформацію, спричинену експоненціальним розвитком цифрових технологій, а особливо – генеративного штучного інтелекту (ГШІ). Ця трансформація торкається усіх сфер суспільного життя, але особливо гостро вона відчувається в правовій сфері, де питання достовірності, прозорості, підзвітності та верховенства права стають не просто академічними, а стратегічними. Україна, яка в умовах війни одночасно будує цифрову державу та модернізує інститути демократії, перебуває на передовій цього глобального виклику. Саме тому наукові дослідження, спрямовані на розуміння та формалізацію взаємодії штучного інтелекту з правовою системою, набувають надзвичайної актуальності.

Цей збірник присвячено актуальним проблемам застосування сучасних технологій штучного інтелекту в державному управлінні, з особливим акцентом на парламентський контроль – один із ключових механізмів підзвітності влади перед суспільством. Автори збірника не просто аналізують можливості ГШІ для обробки правових текстів – вони пропонують формалізовані, структуровані та інтерпретовані підходи, які забезпечують не лише ефективність, а й надійність, верифікованість та безпеку результатів. Від безкодового програмування з ітеративним самоконтролем (для боротьби з «галюцинаціями» ВММ) до архітектури RAG для динамічного створення семантичних мереж — кожна робота демонструє перехід від інтуїтивного використання ГШІ до побудови інтелектуальних систем контролю, здатних до автономного аналізу, моделювання та прогнозування.

Особливу увагу приділено семантичному виміру. У правовій сфері важливий не лише факт існування зв’язку між поняттями, а його змістова природа: чи є це технічна помилка, лобістський вплив, когнітивна маніпуляція чи системний ризик? Для вирішення цього завдання запропоновано нові метрики, такі як семантична центральність за посередництвом, а також методи ранжування та кластеризації, що інтегрують як структурні, так і семантичні ознаки. Це дозволяє

не просто «побачити» мережу, а зрозуміти її логіку, виявити критичні вузли впливу та спрогнозувати наслідки змін у законодавстві.

Збірник також не уникає гострих питань безпеки, зокрема змагального штучного інтелекту та лінгвістичних бекдорів – прихованих механізмів маніпуляції, що можуть підривати довіру до правової системи зсередини. Автори пропонують не лише діагностику таких загроз, а й механізми протидії, засновані на поєднанні технологічних, правових та етичних підходів.

Наукові роботи, представлені в цьому збірнику, є результатом плідної співпраці між фахівцями з комп'ютерних наук, кібербезпеки, юриспруденції та державного управління. Вони відображають не просто теоретичні роздуми, а практично орієнтовані рішення, які вже застосовуються або інтегруються з державними цифровими платформами.

Публікація цього збірника має на меті сприяти подальшому розвитку інформаційного права, правової інформатики та інтелектуальних систем підтримки прийняття рішень в Україні. Ми сподіваємося, що він стане корисним джерелом для науковців, практиків, державних службовців, депутатів та всіх, хто цікавиться майбутнім правової системи в епоху штучного інтелекту.

Дмитро Ланде

Київ, 2025 рік

Ланде Д. В.,
доктор технічних наук, професор,
керівник наукового центру ДНУ ІІБП НАПрН України,
завідувач кафедри НН ФТІ КПІ ім. Ігоря Сікорського
ORCID: 0000-0003-3945-1178
Фурашев В. М.
кандидат технічних наук, доцент, с.н.с.,
перший заступник директора ДНУ ІІБП НАПрН України,
ORCID: 0000-0001-7205-724X

ШТУЧНИЙ ІНТЕЛЕКТ У ДЕРЖАВНОМУ УПРАВЛІННІ: ВІД АНАЛІЗУ ТЕКСТІВ ДО ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ

Сьогодні, в умовах війни, Україна перебуває також в умовах глибокої цифрової трансформації державного управління. Однак ця трансформація має впливати не лише на виконавчу владу, а й на механізми парламентського контролю – один із ключових інструментів підзвітності влади перед суспільством [1].

Сучасний обсяг правової інформації – законопроекти, урядові звіти, скарги громадян, судові рішення – перевищує можливості ручного аналізу. Традиційні методи парламентського контролю, засновані на лінійному читанні документів, втрачають ефективність. У цих умовах застосування генеративного штучного інтелекту (ГШІ) стає не просто корисним доповненням, а стратегічною необхідністю для забезпечення прозорості, ефективності та проактивності парламенту [2].

Особливо важливим є перехід від текстової аналітики до формалізованих, структурованих систем контролю, де ГШІ виступає не як «чорний ящик», а як компонент інтелектуальної екосистеми, здатної до автономного аналізу, прогнозування та підтримки прийняття рішень в правовій сфері.

Мета роботи

Метою дослідження є узагальнення сучасних практик та перспективних напрямів застосування генеративного штучного інтелекту в парламентському контролі. Особливу увагу приділено:

– демонстрації можливостей ГШІ для аналізу нормативно-правових актів, виявлення суперечностей та прогалин;
– розробці методів побудови семантичних мереж знань на основі правових текстів;
– обґрунтуванню концепції інтелектуальної системи парламентського контролю, здатної до автономного моніторингу, моделювання та прогнозування.

Виклад основного матеріалу

1. Генеративний ШІ як інструмент аналітичного підсилення. Сучасні великі мовні моделі (LLM) дозволяють обробляти неструктуровані текстові дані – основну форму подання правової інформації. Уже сьогодні ГШІ ефективно використовується в правовій сфері для:

– аналізу урядових звітів (виявлення невиконаних зобов'язань, бюджетних ризиків);
– перевірки законопроектів на наявність технічних помилок, лакун, дублювання норм;
– обробки масових скарг громадян з виявленням системних проблем у діяльності державних органів.

Наприклад, за допомогою простого промпта: *«Перелічіть 10 причин суперечностей у визначеннях законодавчих документів»* [3] система генерує такі категорії, як *«Неоднозначність», «Відсутність узгодження», «Технічні помилки»*, що після експертної перевірки і узгодження стає основою для формалізованого аналізу.

2. Семантичні мережі як основа структурованого контролю. Ключовим методологічним проривом є перехід від аналізу окремих документів до побудови семантичних мереж [3], де правові поняття, норми та події з'єднані причинно-наслідковими зв'язками. Процес включає:

– витяг пар сутностей із текстів (наприклад, *«Податкові перевірки → Бізнес»*);
– формування CSV-файлів зі зв'язками;

– візуалізацію та аналіз у спеціалізованих інструментах – Gephi, GraphViz, SocNetV.

Ці інструменти дозволяють виявляти:

– центральні вузли (наприклад, «блокування податкових накладних» як системна проблема);
– кластери (тематичні групи норм або скарг);
– прогалини (відсутність зв’язків між поняттями, що вказує на нормативну неповноту).

3. Автономний інтелектуальний контроль. Найближчим майбутнім парламентського контролю є створення інтелектуальної системи, яка функціонуватиме автономно, без постійного втручання людини [4]. Така система зможе:

– автономно моніторити всі законопроекти, укази та постанови у реальному часі;
– прогнозувати наслідки прийняття норм шляхом побудови імітаційних моделей;
– генерувати алерти про суперечності чи ризики під час розгляду законопроектів;
– аналізувати зворотний зв’язок від громадян у соцмережах та на платформах, виявляючи нові теми для контролю.

Особливо перспективною є концепція «цифрового двійника законодавства» [5] – повноцінної моделі правової системи, яка симулює вплив нових норм на існуючу базу. Аналогічні моделі вже розробляються в Естонії та Сінгапурі.

Крім того, у майбутньому можливе застосування «рою віртуальних експертів» – колективу LLM-агентів, кожен з яких моделює фахівця певного профілю (юрист, економіст, кібербезпека). Такий колектив зможе проводити багатофакторний аналіз законопроектів, виявляючи приховані ризики.

4. Інтеграція з державними цифровими платформами. Для реалізації цих ідеї необхідна глибока інтеграція з існуючими платформами:

– e-Parliament — для доступу до законопроектів та історії їх розгляду;

- ЄДРНПА — для централізованого аналізу чинного законодавства;
- ProZorro — для моніторингу держзакупівель та виявлення корупційних ризиків;
- «Дія» — для аналізу звернень громадян та якості надання послуг.

Така інтеграція перетворить Верховну Раду на цифрову, інтелектуально підсилену інституцію, здатну до проактивного, ґрунтовного та прозорого контролю.

Висновки

Генеративний штучний інтелект вже сьогодні є стратегічним інструментом парламентського контролю, який дозволяє автоматизувати рутинні завдання та виявляти приховані закономірності в правовій сфері.

Перехід від аналізу текстів до семантичного нетворкінгу та візуалізації знань (через Gephi, GraphViz, SocNetV) забезпечує глибше розуміння структури правових систем.

Майбутнє – за інтелектуальною системою контролю, яка об’єднує автономний моніторинг, моделювання, прогнозування та колективний аналіз.

Україна має унікальну можливість стати світовим лідером у розробці цифрових інтелектуальних інструментів парламентського контролю, зокрема через інтеграцію з платформою «Дія» та впровадження етичних стандартів, які вже закладені у рекомендаціях EU4DigitalUA.

Ключовим завданням на наступному етапі є забезпечення відтворюваності, верифікації результатів та захисту від галюцинацій, що вимагає розробки формалізованих фреймворків (наприклад, безкодового програмування) та поєднання LLM із детермінованими алгоритмами.

Бібліографічні посилання

[1] Інтелектуальна система парламентського контролю : Від семантичного аналізу до інтелектуальної координації в державному управлінні з використанням штучного інтелекту : Монографія / Ланде Д.В., Фурашев В.М., Даник Ю.Г., Страшной Л.Л. – Київ: ТОВ «Інжиніринг», 2025. – 278 с.

[2] Д.В. Ланде, В.М. Фурашев. Парламентський контроль із застосуванням генеративного штучного інтелекту : монографія / Ланде Д.В., Фурашев В.М. – Київ: ТОВ "Інжиніринг", 2023. – 202 с.

[3] Dmytro Lande, Leonard Strashnoy. GPT Semantic Networking: A Dream of the Semantic Web – The Time is Now. – Kyiv: Engineering, 2023. – 168 p. ISBN 978-966-2344-94-3, DOI: 10.5281/zenodo.14278893

[4] Інформатика парламентського контролю : посібник. Д.В. Ланде, В.М. Фурашев, С.М. Брайчевський. – Київ 2022. – 256 с. ISBN 978-966-2344-80-6

[5] Menkhoff, T., Wong, C. and Ritter, W., 2024. Singapore’s approach towards developing vibrant urban innovation spaces. In Visions for the future: Towards more vibrant, sustainable and smart cities (pp. 1-33).

Ланде Д.В.,
доктор технічних наук, професор,
керівник наукового центру ДНУ ІІБП НАПрН України,
завідувач кафедри НН ФТІ КПІ ім. Ігоря Сікорського
ORCID: 0000-0003-3945-1178
Даник Ю.Г.,
доктор технічних наук, професор,
професор НН ФТІ КПІ ім. Ігоря Сікорського
ORCID: 0000-0001-6990-8656
Страшной Л.Л.,
старший фахівець з архітектури даних (Senior Data Architect), Університет Каліфорнії (UCLA), Лос-Анджелес, США,
ORCID: 0009-0008-5575-0286

ЗАСТОСУВАННЯ ФРЕЙМВОРКУ БЕЗКОДОВОГО ПРОГРАМУВАННЯ НА ОСНОВІ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ У ПРАВОВІЙ СФЕРІ

Сучасні інструменти штучного інтелекту, зокрема великі мовні моделі (ВММ), все частіше застосовуються в юридичній сфері – для аналізу нормативно-правових актів, моніторингу законодавчих змін, підготовки правових висновків тощо. Однак широке використання ВММ супроводжується серйозними ризиками: генерація недостовірної інформації («галюцинації»), відсутність механізмів перевірки результатів, непрозорість логіки висновків. Це створює загрози для правової безпеки, особливо в контексті парламентського контролю та регулювання штучного інтелекту. Тому виникає нагальна потреба в розробці надійних, самоконтрольованих систем автоматизації на основі ВММ, які б забезпечували високу точність, відтворюваність та зрозумілість результатів.

Мета роботи

Метою дослідження є розширення існуючого фреймворку безкодового програмування шляхом впровадження нових примітивів, спрямованих на забезпечення надійності та якості результатів ВММ у правовій сфері. Особливу увагу приділено застосуванню такого підходу для аналізу нормативних актів, виявлення лобістських впливів і підвищення прозорості правозастосування.

Виклад основного матеріалу

Безкодове програмування на основі ВММ передбачає побудову структурованих «запитів», що функціонують як програми, складені з базових

примітивів: *If-Condition* (умова), *Cycle* (цикл), *Function* (функція) [1]. Для складніших сценаріїв (наприклад, аналізу правових колізій або багатоетапного інтерпретування норм) до цього набору додаються *Label* та *Goto*, що дозволяють моделювати нестандартні логічні потоки [2, 3]. Однак базові примітиви не вирішують ключової проблеми – недостатньої надійності. Тому в роботі запропоновано третій рівень фреймворку, заснований на трьох нових примітивах:

Supercycle – організовує ітеративне виконання підзапиту до досягнення заданого рівня якості або вичерпання ліміту спроб. Це основний механізм протидії «галюцинаціям».

Control – об'єктивно оцінює результат за заданим критерієм (наприклад, точне збігання, косинусна подібність, чисельна збіжність). Лише після підтвердження якості цикл завершується.

Result – стандартизує вихідні дані, забезпечуючи зрозуміле форматування (текст, JSON, таблиця) та, за потреби, візуалізацію, що критично важливо для правового аналізу.

Композиція цих примітивів дозволяє перетворити ВММ з інструменту «одноразового запиту» на систему ітеративного самоконтролю, здатну до поетапної верифікації висновків.

На прикладі аналізу *Закону про штучний інтелект ЄС (EU AI Act)* [4] продемонстровано практичну ефективність підходу. Завдяки самоконтрольованим ітераціям вдалося виявити 6 із 8 критичних ознак лобістського впливу, що загрожують кібербезпеці та справедливому регулюванню:

- надмірно високий поріг обчислювальної потужності, що обмежує участь стартапів;
- нечіткі критерії «високого ризику», які дозволяють розробникам самостійно класифікувати свої системи;
- надмірні винятки для open-source моделей, які можуть приховувати комерційні інтереси.

Такий аналіз став можливим лише завдяки багаторазовій перевірці висновків, яку забезпечують примітиви *Supercycle* та *Control*. Це підвищує довіру до

результатів, що особливо важливо в умовах парламентського контролю, де рішення мають масштабні правові наслідки.

Висновки

Запропоноване розширення фреймворку безкодового програмування впроваджує принципи самоконтролю, верифікації та пояснюваності у роботу ВММ, що є критичним для їхнього застосування в правовій сфері.

Примітиви *Supercycle*, *Control* і *Result* дозволяють ефективно протидіяти галюцинаціям, забезпечуючи кількісну оцінку якості та стандартизований вихід – ключові вимоги для юридичної практики.

Підхід може бути застосований для аналізу законопроєктів, моніторингу регуляторних змін, виявлення прихованих інтересів у нормативних актах, а також підтримки парламентського контролю.

Подальші дослідження повинні бути спрямовані на інтеграцію фреймворку з офіційними правовими базами даних та розробку спеціалізованих метрик оцінки для юридичного контексту.

Бібліографічні посилання

[1] Dmitry Lande, Leonard Strashnoy. Semantic AI Framework for Prompt Engineering. ResearchGate Preprint. DOI: 10.13140/RG.2.2.21116.24964 (Mart 9, 2025).

[2] Dmitry Lande, Leonard Strashnoy. An Advanced No-Code Programming Framework for Complex Problems in LLM Environments. ResearchGate Preprint. DOI: 10.13140/RG.2.2.25307.89129 (May, 2025).

[3] Lande, D.V., Furashov, V.M. Application of the No-Code Programming Framework for Solving Parliamentary Oversight Tasks. Information and Law, 2025. – No. 2(53). – Pp. 88–103. DOI: 10.37750/2616-6798.2025.2(53).334055. (in Ukrainian).

[4] Ebers, M., 2023. The European Commission's Proposal for an Artificial Intelligence Act. In Research Handbook on EU Internet Law (pp. 271-292). Edward Elgar Publishing.

Ланде Д. В.,
доктор технічних наук, професор,
керівник наукового центру ДНУ ІІБП НАПрН України,
завідувач кафедри НН ФТІ КПІ ім. Ігоря Сікорського
ORCID: 0000-0003-3945-1178
Рибак О. О.,
Аспірант ІСЗЗІ КПІ ім. Ігоря Сікорського

АРХІТЕКТУРА RAG ДЛЯ ДИНАМІЧНОГО СТВОРЕННЯ СЕМАНТИЧНИХ МЕРЕЖ У ПРАВОВІЙ СФЕРІ

Сучасна правова сфера, зокрема в контексті парламентського контролю, постійно стикається з викликами, пов’язаними зі швидким зростанням обсягів нормативно-правової інформації, появою нових правових явищ (наприклад, регулювання штучного інтелекту, цифрових прав, кібербезпеки) та зміною семантичного змісту правових понять у реальному часі. Традиційні методи моделювання знань – статичні онтології, ручне індексування – не здатні адаптуватися до таких змін. З іншого боку, великі мовні моделі (ВММ), хоча й мають потужний семантичний потенціал, обмежені застарілими знаннями та схильні до галюцинацій.

У цьому контексті надзвичайно актуальним стає розроблення методів, які поєднують генеративну силу ВММ із актуальною зовнішньою інформацією. Особливу цінність у правовій сфері має не просто текстовий аналіз, а **динамічне структурування знань** – побудова семантичних мереж, які відображають зв’язки між поняттями (наприклад, «штучний інтелект – регулювання – парламентський контроль – права громадян»), зберігають джерело інформації та можуть адаптуватися до нових законодавчих ініціатив [1].

Мета роботи

Метою дослідження є розробка та наукове обґрунтування архітектури **Extended Semantic Networking (ESN)** [2] – розширеного підходу на основі Retrieval-Augmented Generation (RAG), спрямованого не на генерацію тексту, а на динамічне створення та оновлення семантичних мереж у правовій сфері. Особливу увагу приділено застосуванню цього підходу для аналізу законодавчих ініціатив, виявлення прихованих зв’язків між правовими поняттями та підтримки

парламентського контролю шляхом візуалізації та аналізу семантичної структури нормативних актів.

Виклад основного матеріалу

Запропонована архітектура ESN принципово відрізняється від класичного RAG: замість того щоб використовувати зовнішні документи лише як контекст для генерації тексту, ESN перетворює їх на **структурні елементи для побудови динамічної семантичної мережі** [3]. Фреймворк складається з чотирьох етапів:

Генерація базової мережі (G_0) – ВММ на основі запиту (наприклад, «регулювання штучного інтелекту в ЄС») формує початкову семантичну мережу, що відображає її «канонічне» розуміння теми.

Пошук зовнішніх документів (D_{ext}) – система отримує актуальні джерела: законопроєкти, парламентські звіти, наукові статті, ЗМІ, за допомогою інформаційно-пошукової системи (наприклад, Cyber Aggregator або парламентська база даних).

Генерація адаптованої мережі (G_1) – та сама ВММ аналізує виявлені документи та виділяє нові концепції та зв'язки, що відображають поточний стан дискурсу.

Синтез розширеної мережі (G^*) – G_0 та G_1 об'єднуються в єдину динамічну мережу, де кожен зв'язок має:

- **вагу** (степінь довіри: 0,7 — лише ВММ; 0,8 — лише зовнішній джерело; 1,0 – підтверджено обома),
- **атрибут походження** (LLM, EXT або HYBRID).

Ця структура дозволяє не лише бачити, що пов'язано з чим, але й **розуміти, звідки походить цей зв'язок** – чи це загальноприйняте знання, чи нова правова норма, чи спільне підтвердження.

Формально семантична мережа у ESN задається як атрибутований орієнтований граф:

$$G = (V, E, W, S),$$

де V – вузли (правові поняття), E – зв'язки, W – вага довіри, S – джерело.

У рамках експерименту (вересень 2025 р.) було проаналізовано тему «генеративний штучний інтелект». Базова мережа G_0 містила лише технічні поняття (LLM, трансформери, fine-tuning). Після інтеграції зовнішніх даних (G*) мережа розширилася на **115% за кількістю понять** і включила критичні для правової сфери концепти:

- «регулювання штучного інтелекту»,
- «фабриковані судові прецеденти»,
- «парламентський контроль над алгоритмами»,
- «право на пояснення рішень AI».

Важливо, що ESN виявив **«містки» між сферами**: наприклад, поняття «синтетичні дані» пов'язує **технічний аспект** (генерація даних), **правовий** (захист персональних даних) та **етичний** (маніпуляції). Такі зв'язки є критичними для комплексного правового аналізу.

Мережа *G** була експортована у форматі GEXF та візуалізована в Gephi, що дозволило виявити центральні вузли (наприклад, «штучний інтелект») та ключові «мости» (наприклад, «великі мовні моделі»), через які проходять шляхи між технічними та правовими аспектами [4].

Висновки

Запропонована архітектура ESN ефективно подолує обмеження як статичних онтологій, так і класичного RAG, забезпечуючи **динамічне, атрибутоване та інтерпретоване** моделювання знань у правовій сфері.

Підхід дозволяє **відстежувати семантичний дрейф** правових понять у реальному часі — що особливо цінно для парламентського контролю, де законодавство має реагувати на нові технологічні виклики.

ESN забезпечує **високу прозорість**: кожен зв'язок має підтвердження та може бути верифікований юристом або аналітиком.

Фреймворк є **універсальним** і може бути інтегрований як у технічні системи (наприклад, правові бази даних), так і в no-code інструменти, що робить його доступним для практиків без програмістських навичок.

У перспективі ESN може бути застосований для:

- моніторингу законодавчих ініціатив;
- виявлення лобістських впливів через аналіз семантичних зв’язків;
- підтримки правозастосування шляхом побудови «життєвої» семантичної карти нормативної бази.

Бібліографічні посилання

[1] Ланде Д.В. Формування і аналіз мереж подій у сфері парламентського контролю на основі застосування систем штучного інтелекту. Інформація і право, 2024. – N 4(48). – С. 84-89. DOI: https://doi.org/10.37750/2616-6798.2024.1(48).300776

[2] Siriwardhana, S., Weerasekera, R., Wen, E., Kaluarachchi, T., Rana, R. and Nanayakkara, S., 2023. Improving the domain adaptation of retrieval augmented generation (RAG) models for open domain question answering. Transactions of the Association for Computational Linguistics, 11, pp.1-17.

[3] Dmitry Lande, Leonard Strashnoy, Oleksander Rybak. Framework of Extended Semantic Networking – A Semantic RAG Architecture for Dynamic Conceptual Mapping. SSRN Preprint: 5505220, DOI: 10.2139/ssrn.5505220 (Sep 23, 2025). – 17 p.

[4] Dmitry Lande, Anatolii Kachynskyi, Leonard Strashnoy Semantic Betweenness Centrality in Cognitive Warfare Networks. SSRN Preprint: 5421634, DOI: 10.2139/ssrn.5421634 (Sep 08, 2025). - 11 p.

Ланде Д.В.,
доктор технічних наук, професор,
керівник наукового центру ДНУ ІІБП НАПрН України,
завідувач кафедри НН ФТІ КПІ ім. Ігоря Сікорського
ORCID: 0000-0003-3945-1178
Кузьмінський В. С.,
Аспірант ІСЗЗІ КПІ ім. Ігоря Сікорського
ORCID: 0000-0002-9063-9144

ДИСПЕТЧЕР КУЕРУВАННЯ ЗАПИТАМИ ДЛЯ НЕОДНОРІДНИХ СЕРЕДОВИЩ АНАЛІЗУ ПРАВОВИХ ДОКУМЕНТІВ

Сучасні інструменти аналізу правових документів, зокрема в контексті парламентського контролю, все частіше інтегрують технології штучного інтелекту, зокрема великі мовні моделі (ВММ) [1]. Однак масове застосування ВММ супроводжується суттєвими обмеженнями: високими витратами на обробку кожного запиту, неефективним використанням обчислювальних ресурсів та надмірною складністю для завдань, які є чітко алгоритмізованими (наприклад, перевірка формату дати, класифікація типів документів, обчислення термінів).

У правовій сфері це особливо проблематично: аналіз законопроєктів, звітів, судових рішень часто включає як складні семантичні завдання (наприклад, інтерпретація норм), так і рутино-алгоритмічні операції (наприклад, вилучення реквізитів, формування хронології подій). Використання ВММ для всіх етапів призводить до надмірної вартості та повільності, що унеможливлює постійний моніторинг у реальному часі.

Тому виникає нагальна потреба в інтелектуальному диспетчері запитів, який автоматично визначає найефективніше середовище виконання для кожного етапу обробки правової інформації — залежно від складності завдання [2].

Мета роботи

Метою дослідження є розширення безкодового фреймворку AgentFlow шляхом створення ресурсно-усвідомленого диспетчера запитів, здатного маршрутизувати обробку правових документів між трьома типами середовищ:

– Великою мовною моделлю (LLM) – для складного правового аналізу;

– Малою мовною моделлю (SLM) – для структурованого, але все ще мовного завдання;
– Детермінованою функцією коду (Code) – для алгоритмічних операцій, які не потребують інтелекту.

Особливу увагу приділено застосуванню цього підходу в парламентському контролі, де ефективність, достовірність та економія ресурсів є критичними.

Виклад основного матеріалу

На основі оригінального фреймворку AgentFlow [3], де універсальний «диригент» оркеструє виконання агентів за допомогою структурованих промптів, запропоновано його розширення – ресурсно-усвідомлений універсальний оркестратор [2].

Ключова інновація — компонент маршрутизації (Router), який аналізує логіку кожного агента і призначає йому один із трьох бекендів:

– LLM – якщо завдання вимагає глибокого правового міркування (наприклад, «проаналізувати конституційність законопроєкту»);
– SLM – для завдань середньої складності (наприклад, «виділити ключові терміни у тексті»);
– CODE – для чисто алгоритмічних операцій (наприклад, «перевірити, чи дата відповідає формату DD.MM.YYYY» або «обчислити термін подання скарги»).

Цей вибір може бути здійснений двома способами:

– Декларативно – розробник промпта явно вказує бекенд у JSON-описі агента;
– Автоматично – маршрутизатор аналізує текст логіки агента (наприклад, наявність слів «обчислити», «перевірити», «сортувати») та приймає рішення.

Для підтримки виконання через CODE запроваджено реєстр функцій коду – бібліотеку детермінованих функцій (наприклад, validate_date_format, calculate_deadline, extract_document_type), які викликаються локально, без звернення до зовнішніх API.

Важливо, що уніфікація вихідного формату забезпечує повну сумісність з іншими компонентами системи (планувальником, менеджером стану). Незалежно від того, чи результат отримано від LLM чи від функції Python, він має єдину структуру:

```
{
  "output": [...],
  "status": "success" | "error",
  "error": null | "Повідомлення про помилку"
}
```

Це дозволяє зберегти детермінованість виконання, критичну для юридичних застосувань, де помилка недопустима.

Приклад застосування в правовій сфері, а саме, при аналізі законопроєкту система може:

- використовувати CODE для вилучення дат, реквізитів, посилань на інші нормативні акти;
- залучити SLM для класифікації тематики статей («цифрова безпека», «адміністративна відповідальність» тощо);
- звернутися до LLM лише для глибокої юридичної оцінки, наприклад, виявлення колізій із Конституцією або міжнародними угодами.

Експериментальні розрахунки показують, що застосування такого підходу дозволяє зменшити витрати на обробку на 60–80%, при збереженні повної функціональності та точності.

Висновки

Запропонований диспетчер керування запитами ефективно вирішує проблему неефективного використання ресурсів у системах аналізу правових документів, впроваджуючи принцип «правильний інструмент для правильної роботи».

Підхід повністю сумісний з безкодовою парадигмою: кінцевий користувач (наприклад, юрист або аналітик парламентського комітету) не повинен знати про існування різних бекендів – він просто описує завдання природною мовою.

Система забезпечує високу економічну ефективність, надійність (завдяки детермінованим функціям) та масштабованість, що робить її придатною для постійного застосування в умовах парламентського контролю.

Архітектура є модульною та розширюваною: у майбутньому можна додавати нові бекенди (наприклад, спеціалізовані юридичні моделі або бази даних).

Цей підхід відкриває шлях до створення економічно стійких, постійно діючих систем моніторингу законодавства, які здатні обробляти тисячі документів на день без надмірних витрат.

Бібліографічні посилання

[1] Д.В. Ланде, В.М. Фурашев. Парламентський контроль із застосуванням генеративного штучного інтелекту : монографія / Ланде Д.В., Фурашев В.М. – Київ: ТОВ "Інжиніринг", 2023. - 202 с.

[2] Dmytro Lande, Leonard Strashnoy, Viktor Kuzminskyi. Extension of the Universal Conductor for Heterogeneous Execution Environments SSRN Preprint: 5522698, DOI: 10.2139/ssrn.5522698 (6 Oct 2025). – 13 p.

[3] Dmytro Lande, Leonard Strashnoy. AgentFlow - No-Code Agent Framework Based on Logical Primitives. SSRN Preprint: 5285664, OI: 10.2139/ssrn.5285664 (Jun 22, 2025). – 12 p.

Ланде Д. В.,
доктор технічних наук, професор,
керівник наукового центру ДНУ ІІБП НАПрН України,
завідувач кафедри НН ФТІ КПІ ім. Ігоря Сікорського
ORCID: 0000-0003-3945-1178
Качинський А. Б.,
доктор технічних наук, професор,
професор НН ФТІ КПІ ім. Ігоря Сікорського
ORCID: 0000-0001-9642-7006

СЕМАНТИЧНИЙ ПОКАЗНИК ПОСЕРЕДНИЦТВА ВУЗЛІВ У КОГНІТИВНИХ МЕРЕЖАХ

У сучасних умовах правова сфера, зокрема в контексті парламентського контролю, все частіше стикається зі складними інформаційними викликами – дезінформацією, когнітивною агресією, маніпуляціями правовим дискурсом. Для протидії таким явищам недостатньо лише знати, що поширюється, – важливо зрозуміти, як формуються ланцюжки впливу, які концепти виступають «мостами» між загальними цілями (наприклад, «дестабілізація суспільства») і конкретними наслідками (наприклад, «відмова від національної ідентичності») [1].

Класичні методи аналізу мереж, зокрема показник посередництва (betweenness centrality) [2], ґрунтуються лише на топологічній структурі графа — кількості найкоротших шляхів через вузол. Однак у правовій та політичній сферах найважливіший шлях — не обов’язково найкоротший. Він може бути найстійкішим до протидії, наймасштабнішим, найекономічнішим або найлегітимнішим. Тому існуючі метрики центральності недостатні для аналізу семантично навантажених систем, де зміст шляху важливіший за його довжину.

Це робить актуальним розроблення семантичного показника посередництва, який враховує контекстну цінність шляхів і дозволяє виявляти критичні вузли не в абстрактній мережі, а в конкретній стратегії впливу.

Мета роботи

Метою дослідження є запропонування та наукове обґрунтування моделі семантичної центральності за посередництвом (Semantic Betweenness Centrality, SBC), здатної визначати ключові концепти в когнітивних мережах залежно від

обраного семантичного критерію оптимальності шляху. Особливу увагу приділено застосуванню цього підходу в правовій сфері, зокрема для аналізу механізмів когнітивної агресії, виявлення прихованих ланцюжків маніпуляції та підтримки парламентського контролю за інформаційною безпекою.

Виклад основного матеріалу

На основі аналізу когнітивної мережі «Когнітивна війна» (290 вузлів, 310 зв'язків), побудованої за допомогою великого мовного моделювання та концепції «рою віртуальних експертів», було розроблено нову метрику – S_{BC} [3].

Замість того щоб рахувати лише найкоротші шляхи (як у класичному підході), SBC рахує шляхи, оптимальні за певним семантичним критерієм. У роботі розглянуто чотири такі критерії:

- L (довжина) — кількість переходів (мінімізація);
- R (стійкість до протидії) – скільки зусиль потрібно для нейтралізації (максимізація);
- C (ресурсна ємність) – витрати на реалізацію (мінімізація);
- S (масштабність впливу) – рівень поширення (локальний / національний / глобальний; максимізація).

Для кожного критерію $q \in \{L,R,C,S\}$ визначається окрема метрика S_{BC} $(q(v))$, що вимірює, наскільки часто вузол v з'являється на оптимальних за критерієм q шляхах між парами вузлів.

Для кожного критерію $q \in \{R, S, C, L\}$ можна визначити множину оптимальних шляхів:

$$P_{st}^{(q)} = \left\{ p \in P_{st} \mid q(p) = opt_q\left(\{q(p') \mid p' \in P_{st}\}\right)\right\},$$

де opt_q – операція оптимізації за критерієм q:

- максимізація для R і S,
- мінімізація для C і L.

Для знаходження opt_q виконуються такі дії:

- Ми збираємо значення критерію q для всіх шляхів між s і t,
- Знаходимо оптимальне значення (найменше або найбільше – залежно від q),

– Відбираємо усі шляхи, що досягають цього оптимального значення.

Нехай:

– $\sigma_{st}^{(q)} = \left|P_{st}^{(q)}\right|$ – кількість шляхів між s і t, оптимальних за q ,

– $\sigma_{st}^{(q)}(v)$ – кількість таких шляхів, що проходять через v.

Тоді семантична betweenness-центральність за критерієм q визначається як:

$$C_B^{(q)}(v) = \sum_{\substack{s,t \in V \\ s \neq t \neq v}} \frac{\sigma_{st}^{(q)}(v)}{\sigma_{st}^{(q)}}.$$

Ця формула – пряме узагальнення класичного показника посередництва, але замість геодезичних шляхів використовуються семантично оптимальні.

Кожна така $C_B^{(q)}$ відповідає певній логіці впливу, наприклад:

– $C_B^{(R)}$ показує, які вузли найважливіші для стійких, важкознищуваних ланцюгів;

– $C_B^{(S)}$ – які вузли ключові для масштабних, широкомасштабних операцій;

– $C_B^{(C)}$ – які вузли використовуються в економних, ресурсозберігаючих сценаріях.

– $C_B^{(L:)}$ – які вузли контролюють найшвидші, прямі шляхи.

Оскільки семантичних критеріїв оптимальності шляхів може бути безліч, наприклад, стійкість, масштабність, час, ризик, легітимність, емоційний заряд, культурна глибина, етична прийнятність тощо, то кожний такий критерій породжує окрему центральність.

Іншими словами, не існує єдиної, універсальної центральності. Її зміст визначається метою дослідження

Центральність вузла — не абсолютна властивість, а відносна характеристика, що залежить від мети аналізу.

Це чітко демонструється на прикладі аналізу шляхів до цілі «Колективна амнезія» (Табл. 1):

Таблиця 1. Семантична betweenness-центральність (SBC) і ранг вузлів за різними критеріями

ВУЗОЛ	**S_{BCL}**	**РАНГ S_{BCL}**	**S_{BCR}**	**РАНГ S_{BCR}**	**S_{BCC}**	**РАНГ S_{BCC}**	**S_{BCS}**	**РАНГ S_{BCS}**
Впровадження хибних наукових теорій	0.88	2	0.32	18	0.75	3	0.40	12
Теорія офіційної народності	0.15	47	0.92	1	0.15	47	0.89	2
Мистецтво	0.65	8	0.50	8	0.60	7	0.70	5
Зниження рівня критичного мислення	0.40	15	0.25	25	0.80	4	0.30	18

Ці дані свідчать, що:

- «Теорія офіційної народності» є ключовою для довгострокової, стійкої агресії, але марна для швидких операцій;
- «Хибні наукові теорії» — ефективний інструмент для швидкого та економного впливу, але легко нейтралізується;
- «Мистецтво» виступає універсальним мостом — зі стабільно високими показниками за всіма критеріями;
- «Зниження критичного мислення» — дешевий механізм, але з обмеженим радіусом дії.

У правовій сфері це означає, що аналітики парламентського контролю можуть:

- виявляти стратегічні ризики (через SBCR — стійкі ланцюжки);
- виявляти тактичні загрози (через SBCL — швидкі кампанії);
- оцінювати економічну ефективність деструктивних сценаріїв (через SBCC);
- прогнозувати масштаб поширення (через SBCS).

Такий підхід дозволяє переходити від пасивного моніторингу до контекстно-орієнтованого управління інформаційною безпекою.

Висновки

Запропонована модель семантичної центральності за посередництвом (SBC) принципово поширює класичний підхід, вводячи контекстну залежність центральності від цілей аналізу.

У правовій сфері це дозволяє точніше ідентифікувати критичні концепти, які використовуються в інформаційних операціях проти правової системи, національної ідентичності або демократичних інституцій.

Підхід має практичну цінність для парламентського контролю: організації можуть налаштовувати аналіз під конкретні загрози — від швидкої дезінформації до довготривалої ідеологічної агресії.

SBC забезпечує гнучкий інструментарій для стратегічного аналізу, де кожен показник відповідає певній логіці функціонування системи впливу.

У майбутньому підхід може бути інтегрований у системи автоматичного моніторингу законодавчого дискурсу, аналізу судової практики або оцінки ризиків у нормотворчості.

Бібліографічні посилання

[1] Качинський А. Б., Ланде Д. В., Новіков О. М. Теоретико-графові моделі інформаційно-психологічних війн. Моделювання ментальної війни із застосуванням генеративного штучного інтелекту : навч. посіб. для здобувачів ступенів магістра та PhD за спец. 125 Кібербезпека та захист інформації / А. Б. Качинський, Д. В. Ланде, О. М. Новіков, 2025 ; КПІ ім. Ігоря Сікорського. - Київ : ТОВ "Іжиніринг", 2025. - 242 с.

[2] Freeman, L.C., Borgatti, S.P. and White, D.R., 1991. Centrality in valued graphs: A measure of betweenness based on network flow. Social networks, 13(2), pp.141-154.

[3] Dmitry Lande, Anatolii Kachynskyi, Leonard Strashnoy Semantic Betweenness Centrality in Cognitive Warfare Networks. SSRN Preprint: 5421634, DOI: 10.2139/ssrn.5421634 (Sep 08, 2025). – 11 p.

Ланде Д. В.,
доктор технічних наук, професор,
керівник наукового центру ДНУ ІІБП НАПрН України,
завідувач кафедри НН ФТІ КПІ ім. Ігоря Сікорського
ORCID: 0000-0003-3945-1178
Даник Ю. Г.,
доктор технічних наук, професор,
професор НН ФТІ КПІ ім. Ігоря Сікорського
ORCID: 0000-0001-6990-8656

ЗМАГАЛЬНИЙ ШТУЧНИЙ ІНТЕЛЕКТ В ПРАВРВІЙ СФЕРІ

У сучасних умовах цифрові технології, і зокрема штучний інтелект (ШІ), все глибше інтегруються в правову сферу – від підготовки законопроєктів до аналізу судової практики та парламентського контролю [1]. Однак цей процес супроводжується виникненням нових загроз, пов’язаних із розвитком змагального штучного інтелекту (ЗШІ) – технологій, спрямованих на генерацію дезінформації, маніпуляції правовим дискурсом, підрив довіри до інституцій та проведення інформаційних операцій проти держави [2].

Особливо небезпечними є випадки, коли ЗШІ застосовують для створення фейкових правових документів, імітації офіційних повідомлень, підробки доказів або масштабної маніпуляції громадською думкою під час обговорення законопроєктів. Такі практики створюють серйозні ризики для верховенства права, прозорості нормотворчості та ефективності парламентського контролю.

Тому науковий та правовий аналіз механізмів ЗШІ, зокрема таких його проявів, як лінгвістичні бекдори, стає стратегічно важливим завданням для правової науки та практики.

Мета роботи

Метою дослідження є комплексний аналіз застосування змагального штучного інтелекту в правовій сфері, зокрема в контексті парламентського контролю та інформаційної безпеки. Особливу увагу приділено:

- виявленню механізмів маніпуляції правовим контентом за допомогою ЗШІ;

– аналізу лінгвістичних бекдорів як прихованих інструментів впливу на роботу великих мовних моделей (LLM);
– оцінці правових ризиків та пропозиції механізмів протидії.

Виклад основного матеріалу

Змагальний ШІ в правовій сфері проявляється у трьох основних напрямах:

Генерація та детекція правової дезінформації. Великі мовні моделі (LLM) здатні створювати правдоподібні, але фейкові законопроєкти, судові рішення, офіційні листи чи аналітичні висновки, які імітують стиль уповноважених джерел. Такі матеріали можуть бути використані для дезінформації депутатів, аналітиків або громадськості під час обговорення важливих реформ. На противагу цьому, ЗШІ також використовується для детекції фейків – через мультиагентні моделі, які аналізують текст з різних семантичних, стилістичних та фактичних ракурсів.

Застосування в інформаційних війнах проти правових інституцій. ЗШІ дозволяє моделювати й прогнозувати реакцію аудиторії на законодавчі ініціативи, створювати персоналізовані маніпулятивні кампанії, спрямовані на делегітимізацію парламенту чи судової влади, а також проводити когнітивні атаки на основі аналізу світоглядних упереджень цільової аудиторії.

Лінгвістичні бекдори – приховані механізми впливу на ШІ. Серед найбільш небезпечних інструментів ЗШІ виділяються *лінгвістичні бекдори* – спеціально вбудовані або навмисно введені тригери у великих мовних моделях, які активуються при використанні певних слів, фраз або синтаксичних конструкцій. Такі бекдори можуть:

– змінювати тон і зміст відповіді моделі (наприклад, перетворювати нейтральний правовий аналіз на пропагандистське повідомлення);
– генерувати хибні юридичні прецеденти або посилання на неіснуючі норми;
– блокувати певні теми (наприклад, при аналізі воєнного стану чи законів про національну безпеку).

На відміну від технічних бекдорів, лінгвістичні дуже складно виявити, оскільки вони маскуються під звичайні мовні конструкції. Вони можуть бути впроваджені:

- на етапі навчання моделі (через «отруєні» дані);
- на рівні архітектури (через приховані функції обробки тексту);
- через нейролінгвістичне програмування — з використанням специфічних мовних патернів, що викликають передбачувану реакцію.

У правовій сфері це може означати, що аналітична система, яка використовує LLM для підготовки висновків про законопроєкт, може навмисно давати упереджені рекомендації, не викликаючи підозри у користувача.

Правове регулювання та механізми протидії

На міжнародному рівні ключовим документом є Акт про штучний інтелект ЄС [3], який класифікує системи ЗШІ як високоризикові у разі їхнього застосування для маніпуляції громадською думкою, впливу на правосуддя або парламентські процеси. Він встановлює:

- обов’язкове тестування на безпеку перед розгортанням;
- принцип прозорості щодо джерел даних та механізмів прийняття рішень;
- заборону застосування ШІ для підміни демократичного дискурсу.

У національному законодавстві України питання регулюються:

- Законом «Про основні засади забезпечення кібербезпеки України», який передбачає протидію дезінформаційним кампаніям;
- Кримінальним кодексом, де передбачена відповідальність за кібератаки, шахрайство з використанням ШІ, розповсюдження завідомо неправдивої інформації;
- Законом «Про захист персональних даних», що регулює використання даних для навчання моделей.
- Проте існуючі норми не враховують специфіки лінгвістичних бекдорів, що вимагає розробки нових підходів, зокрема:

- обов’язкової сертифікації LLM, які використовуються в юридичній сфері;
- впровадження механізмів аудиту мовних моделей на наявність прихованих тригерів;
- розробки технічних стандартів для виявлення аномалій у поведінці ШІ під час аналізу правових текстів.

Висновки

Змагальний штучний інтелект становить реальну загрозу для правової сфери, особливо в контексті парламентського контролю, де достовірність інформації є основою прийняття рішень.

Лінгвістичні бекдори виступають одним із найбільш небезпечних інструментів ЗШІ – вони дозволяють приховано маніпулювати правовим аналізом, не залишаючи технічних слідів.

Існуюче законодавство є недостатнім для ефективного регулювання таких загроз. Необхідно розробити спеціалізовані правові та технічні механізми для аудиту, сертифікації та моніторингу ШІ-систем, що використовуються в державному управлінні.

Перспективним напрямом є інтеграція ЗШІ у системи протидії дезінформації – коли одна модель генерує потенційні загрози, а інша – аналізує їх і пропонує захисні заходи.

У майбутньому правова наука повинна розробити нову категорію – «лінгвістична кіберзлочинність», яка б охоплювала зловмисне використання мовних технологій для підриву правового порядку.

Використана література

[1] Д.В. Ланде, В.М. Фурашев. Парламентський контроль із застосуванням генеративного штучного інтелекту : монографія / Ланде Д.В., Фурашев В.М. – Київ: ТОВ "Інжиніринг", 2023. – 202 с.

[2] Ланде Д.В., Даник Ю.Г. Змагальний штучний інтелект в інформаційних і кібернетичних війнах. Інформація і право, 2025. – N 1(52). – С. 76-89. DOI: 10.37750/2616-6798.2025.1(52).324688

[3] Ebers, M., 2023. The European Commission's Proposal for an Artificial Intelligence Act. In Research Handbook on EU Internet Law (pp. 271-292). Edward Elgar Publishing.

Ланде Д. В.,
доктор технічних наук, професор,
керівник наукового центру ДНУ ІІБП НАПрН України,
завідувач кафедри НН ФТІ КПІ ім. Ігоря Сікорського
ORCID: 0000-0003-3945-1178
Качинський А. Б.,
доктор технічних наук, професор,
професор НН ФТІ КПІ ім. Ігоря Сікорського
ORCID: 0000-0001-9642-7006

РАНЖУВАННЯ ТА КЛАСТЕРИЗАЦІЯ ПОНЯТЬ ГРАФОВОЇ МОДЕЛІ КОГНІТИВНОЇ ВІЙНИ ЧЕРЕЗ PCA ТА LLM

У сучасних умовах гібридних конфліктів правова сфера, зокрема в контексті парламентського контролю, все частіше стикається з викликами, пов’язаними з когнітивною війною – системним впливом на свідомість громадян через маніпуляцію правовими поняттями, цінностями та правовим дискурсом. Такі атаки можуть включати фальсифікацію правових нарративів, делегітимізацію законодавчих ініціатив або підміну юридичних термінів (наприклад, «агресія» замінюється на «спецоперацію»).

Для ефективної протидії необхідні інструменти, які дозволяють не лише виявляти такі маніпуляції, а й об’єктивно оцінювати вагу правових понять та групувати їх за семантичним змістом. Класичні методи аналізу графів (наприклад, Louvain, node2vec) [1-2] зосереджуються лише на топології мережі, ігноруючи змістовну сутність вузлів, що робить їх малопридатними для правового аналізу, де семантична когерентність є ключовою.

Тому актуальною є розробка методу, який би поєднував структурний аналіз, семантичне збагачення та інтерпретованість результатів — особливо для систем моніторингу інформаційних загроз у правовій сфері.

Мета роботи

Метою дослідження є розробка та апробація універсального методу одночасного ранжування та кластеризації понять у семантичних мережах, зокрема в контексті аналізу когнітивних загроз в правовій сфері. Особливу увагу приділено:

- інтеграції семантичних ознак, згенерованих за допомогою великих мовних моделей (LLM), у математичну модель аналізу;
- забезпеченню високої семантичної когерентності кластерів;
- створенню інтерпретованого ранжування понять за їхньою стратегічною вагою в системі когнітивного впливу.

Виклад основного матеріалу

Запропонований метод реалізується в кілька етапів:

1. Генерація семантичних ознак через LLM. Для кожного правового поняття (наприклад, «суверенітет», «загроза національній безпеці», «право на інформацію») за допомогою LLM [3] генеруються сім когнітивних дескрипторів, що відображають його роль у системі інформаційного впливу:

- дестабілізація правової реальності,
- емоційне зараження,
- ерозія правової ідентичності,
- моральна дезорієнтація,
- когнітивна втома,
- легітимізація неправомірних дій,
- симулякр історичної правди.

Ці оцінки генеруються за стандартизованими запитами, що забезпечує відтворюваність та об’єктивність, оскільки LLM виступає як консенсусна модель експертного судження.

2. Інтеграція з топологією мережі. До семантичних ознак додається повний вектор зв’язків вузла з рештою мережі (рядок матриці суміжності). Це дозволяє зберегти повну структурну інформацію, на відміну від класичних підходів, які використовують лише агреговані метрики (наприклад, степінь або центральність).

3. Ранжирування через PCA. Застосування методу головних компонент (PCA) [4] до об’єднаної матриці ознак дозволяє зменшити розмірність простору та визначити вагу кожного поняття як його відстань від початку координат у просторі головних компонент. Ця вага відображає комбінацію семантичної функції та структурного впливу.

4. Кластеризація з семантичним коригуванням. Початкова кластеризація доповнюється фінальним семантичним коригуванням через LLM: модель аналізує склад кластерів і пропонує їх переформування для забезпечення змістової цілісності (наприклад, виносить «втома від війни» із кластера «патріотизм» в окрему групу «апатія та байдужість»).

5. Інтерпретація через SHAP. Для кожного кластера застосовується SHAP-аналіз, що дозволяє визначити, які саме ознаки (семантичні або структурні) найбільше впливають на його формування. Наприклад, кластер «правова маніпуляція» може бути визначений високими значеннями «дестабілізації реальності» та зв’язками з поняттями «фейк», «брехня», «невідомість».

Метод апробовано на графі когнітивної війни (200 вузлів, 250 зв’язків), який містить правові, політичні та соціальні поняття. Серед топ-10 найважливіших понять за вагою — «зрада», «дезінформація», «захист дітей» — саме ті, що найчастіше використовуються в інформаційних операціях проти правової системи.

Висновки

Запропонований метод ефективно поєднує структурний аналіз і семантичну інтерпретацію, що робить його унікально придатним для застосування в правовій сфері, зокрема в умовах парламентського контролю за інформаційною безпекою.

На відміну від класичних підходів, метод забезпечує високу семантичну когерентність кластерів (4,7 з 5 за експертною оцінкою), що критично для аналізу правових наративів.

LLM використовується не як «зовнішній коректор», а як джерело науково обґрунтованих семантичних ознак, що інтегровані в математичну модель. Це підвищує об’єктивність та відтворюваність результатів.

Метод дозволяє ранжирувати правові поняття не лише за частотою або зв’язністю, а за їхньою стратегічною вагою у системі когнітивного впливу, що має пряме значення для оцінки ризиків дестабілізації правового порядку.

Підхід є універсальним і може бути адаптований для аналізу будь-яких семантичних мереж у правовій сфері: від моніторингу законопроєктів до виявлення маніпулятивних нарративів у судовій практиці чи медіа.

Бібліографічні посилання

[1] Teymourian, N., Izadkhah, H. and Isazadeh, A., 2020. A fast clustering algorithm for modularization of large-scale software systems. IEEE Transactions on Software Engineering, 48(4), pp.1451-1462. DOI: 10.1109/TSE.2020.3022212

[2] Girvan, M., & Newman, M. E. J. (2002). Community structure in social and biological networks. Proceedings of the National Academy of Sciences, 99(12), 7821–7826. DOI: 10.1073/pnas.122653799

[3] Rasool, Z., Barnett, S., Willie, D., Kurniawan, S., Balugo, S., Thudumu, S. and Abdelrazek, M., 2024, April. Llms for test input generation for semantic applications. In Proceedings of the IEEE/ACM 3rd International Conference on AI Engineering-Software Engineering for AI (pp. 160-165). DOI: 10.1145/3644815.3644948

[4] Grover, A., & Leskovec, J. (2016). node2vec: Scalable feature learning for networks. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '16), 855–864. https://doi.org/10.1145/2939672.2939754

ЗМІСТ

ПЕРЕДМОВА 5

ШТУЧНИЙ ІНТЕЛЕКТ У ДЕРЖАВНОМУ УПРАВЛІННІ: ВІД АНАЛІЗУ ТЕКСТІВ ДО ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ 7

ЗАСТОСУВАННЯ ФРЕЙМВОРКУ БЕЗКОДОВОГО ПРОГРАМУВАННЯ НА ОСНОВІ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ У ПРАВОВІЙ СФЕРІ 12

АРХІТЕКТУРА RAG ДЛЯ ДИНАМІЧНОГО СТВОРЕННЯ СЕМАНТИЧНИХ МЕРЕЖ У ПРАВОВІЙ СФЕРІ..... 15

ДИСПЕТЧЕР КУЕРУВАННЯ ЗАПИТАМИ ДЛЯ НЕОДНОРІДНИХ СЕРЕДОВИЩ АНАЛІЗУ ПРАВОВИХ ДОКУМЕНТІВ 19

СЕМАНТИЧНИЙ ПОКАЗНИК ПОСЕРЕДНИЦТВА ВУЗЛІВ У КОГНІТИВНИХ МЕРЕЖАХ..... 23

ЗМАГАЛЬНИЙ ШТУЧНИЙ ІНТЕЛЕКТ В ПРАВРВІЙ СФЕРІ 28

РАНЖУВАННЯ ТА КЛАСТЕРИЗАЦІЯ ПОНЯТЬ ГРАФОВОЇ МОДЕЛІ КОГНІТИВНОЇ ВІЙНИ ЧЕРЕЗ PCA ТА LLM 33