# ARTIFICIAL INTELLIGENCE IN THE CYBERSECURITY FIELD

DOI 10.20535/2411-1031.2025.13.1.328970
УДК 004. 89:004.9

ДМИТРО ЛАНДЕ,
ОЛЕКСАНДР РИБАК

## ЗАСТОСУВАННЯ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ДЛЯ ІНТЕЛЕКТУАЛЬНОГО РОЗШИРЕННЯ СЕМАНТИЧНИХ МЕРЕЖ

У статті запропоновано методику формування та подальшого розширення семантичних мереж на основі аналізу тексту із застосуванням великих мовних моделей (LLM). Первинна семантична мережа розширюється за допомогою GPT-4, Llama-3 та DeepSeek-V3, а отримані результати проходять кількісну оцінку точності й повноти. Запропонована технологія семантичного нетворкінгу[1] базується на концепції «рою віртуальних експертів»[2], за якої кожна LLM доповнює семантичну мережу власними знаннями та зв'язками.

Окрім цього, розроблено підхід до інтеграції мереж, що уможливлює об'єднання результатів від різних LLM в узгоджену структуру. Використання механізму фільтрації слабких зв'язків підвищує достовірність остаточної мережі за рахунок відсікання хибнопозитивних зв'язків і зменшення інформаційного шуму, що сприяє більш точному й повному відображенню знань.

Для візуалізації семантичних мереж використовується програма Gephi – пакет програмного забезпечення з відкритим кодом для мережевого аналізу та візуалізації.

**Ключові слова:** семантичні мережі, великі мовні моделі (LLM), кібербезпека, OSINT, текстова аналітика.

**Постановка проблеми.** Семантичні мережі є потужним інструментом для структурування, представлення та аналізу знань у галузях обробки природної мови, штучного інтелекту й кібербезпеки. Завдяки появі великих мовних моделей (LLM), зокрема GPT-4, Llama-3 та DeepSeek-V3, значно розширилися можливості автоматизації побудови семантичних карт, що суттєво підвищує ефективність аналізу великих обсягів текстових даних.

Інтеграція технологій інформаційного пошуку та штучного інтелекту [3] розширює можливості автоматизованого аналізу текстових даних. Семантичні мережі моделюють взаємозв'язки між подіями та поняттями [4]. Семантичний нетворкінг об'єднує ці технології, сприяючи створенню структурованих мережевих моделей текстів на основі LLM [5].

Проте подальше розширення таких мереж із урахуванням додаткових знань, доступних мовним моделям, залишається важливим науковим викликом [6]. Зокрема, різні LLM можуть генерувати суперечливі або нерелевантні зв'язки, що зумовлює потребу в механізмах фільтрації та інтеграції. Також актуальним є питання оцінювання якості отриманих мереж, оскільки автоматично згенеровані зв'язки можуть містити помилки або зайву інформацію.

**Метою роботи** є розроблення методики розширення семантичних мереж на основі аналізу тексту за допомогою запитів до LLM, оцінювання якості отриманих мереж за показниками повноти та точності, а також підвищення якості виявлених зв'язків шляхом об'єднання знань різних моделей. Це дасть змогу сформувати узгоджену інтегровану семантичну мережу, що може бути корисною в автоматизованому аналізі текстів, OSINT та кібербезпеці.

### 1. Побудова первинної семантичної мережі

На першому етапі здійснюється аналіз вихідного документа $D$ за допомогою великої мовної моделі (LLM). Формування семантичної мережі базується на визначенні зв'язків між ключовими поняттями тексту.

Нехай $D$ – вихідний документ, що містить множину термінів (понять):

$$T = \{t_1, t_2, ..., t_n\}, \quad (1)$$

де кожне $t_i$ є окремим поняттям, виділеним у тексті.

Велика мовна модель (LLM) аналізує документ $D$ та визначає зв'язки між поняттями. Результат роботи LLM можна представити у вигляді множини пар, що описують зв'язки між поняттями:

$$E = \{(t_i, t_j) \mid t_i, t_j \in T, i \neq j\}, \quad (2)$$

де $(t_i, t_j)$ означає, що між поняттями $t_i$ та $t_j$ існує певний логічний або семантичний зв'язок, визначений LLM.

У такому графі зв'язки є неспрямованими, а тому пара $(t_i, t_j)$ фактично не відрізняється від $(t_j, t_i)$.

Таким чином, первинна семантична мережа $G_0$ моделюється у вигляді графа:

$$G_0 = (T, E), \quad (3)$$

де: $T$ – множина вузлів (понять);

$E$ – множина ребер (зв'язків) між поняттями.

**2. Розширення мережі**

Розширення мережі відбувається шляхом додавання нових понять та зв'язків, які не містяться у вихідному документі $D$, але відомі LLM. Цей процес можна формалізувати наступним чином:

1) Визначення нових понять.

Для кожного поняття $t_i \in T$ (де $T$ – множина понять із первинної мережі $G_0$) формується запит до LLM з метою знаходження нових пов'язаних понять.

Як результат, отримуємо множину нових понять, знайдених для кожного $t_i$:

$$T_i^{'} = \{t_{i1}^{'}, t_{i2}^{'}, ..., t_{ik}^{'}\}, \quad (4)$$

де $t_{ij}^{'}$ – нове поняття, знайдене LLM для вузла $t_i$.

Загальна множина нових понять визначається як об'єднання всіх таких множин:

$$T' = \bigcup_{t_i \in T} T_i' . \quad (5)$$

Таким чином, $T'$ містить усі нові поняття, додані до початкової мережі.

2) Визначення нових зв'язків.

Для кожного нового поняття $t_i^{'} \in T \cup T'$, визначеного LLM, встановлюються зв'язки із відповідним початковим поняттям $t_i$.

Множина нових зв'язків для кожного поняття $t_i$ має вигляд:

$$E_i' = \{(t_i, t_j) \mid t_i, t_j \in T \cup T'\}. \quad (6)$$

Загальна множина нових зв'язків визначається як:

$$E' = \bigcup_{t_i \in T} E_i' . \quad (7)$$

Таким чином, $E'$ містить усі нові зв'язки, що доповнюють первинну мережу.

3) Формування розширеної мережі.

Розширена семантична мережа $G_1$ отримується шляхом додавання нових понять $T'$ та нових зв'язків $E'$ до первинної мережі $G_0$:

$$G_1 = (T_1, E_1), \quad (8)$$

де: $T_1 = T \cup T'$ – множина всіх понять після розширення;

$E_1 = E \cup E'$ – множина всіх зв'язків у розширеній мережі.

Таким чином, мережа $G_1$ містить як вихідні поняття та зв'язки, так і нові, знайдені за допомогою LLM.

**3. Демонстрація розширення семантичної мережі за допомогою трьох моделей (GPT-4, Llama-3, DeepSeek-V3)**

Для наочної демонстрації процесу розширення семантичної мережі скористаємося трьома великими мовними моделями: **GPT-4, Llama-3, DeepSeek-V3**. Ми порівняємо, які поняття та зв'язки генерує кожна з моделей на основі одного і того ж вихідного документа.

**Вихідний документ та побудова первинної мережі**

Як практичний приклад, розглянемо невеликий текстовий фрагмент, пов'язаний із попередженням про кібератаки:

*"У Держспецзв'язку попередили про спроби здійснення кібератак, нібито, від імені CERT-UA.*

*Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA отримала інформацію про непоодинокі випадки спроб підключень до комп'ютерів із використанням програми AnyDesk, нібито, від імені CERT-UA…"*

На основі цього тексту формуємо **початкову семантичну мережу** $G_0$ (табл. 1)**.** Запит до моделей:

*"Знайди у цьому тексті пов'язані поняття та представ їх у форматі «поняття_1;поняття_2»."*

Таблиця 1 – Результат побудови первинної мережі

| Вузол 1 | Вузол 2 |
|---|---|
| Спроби кібератак під виглядом CERT-UA | Кібератаки |
| Спроби кібератак під виглядом CERT-UA | Соціальна інженерія |
| Спроби кібератак під виглядом CERT-UA | AnyDesk |
| Отримання віддаленого доступу | Фішинг |
| Отримання віддаленого доступу | Дистанційний доступ |

**Візуалізована первинна мережа ($G_0$), за допомогою пакету програмного забезпечення Gephi,** представлена у вигляді графа на рисунку 1.

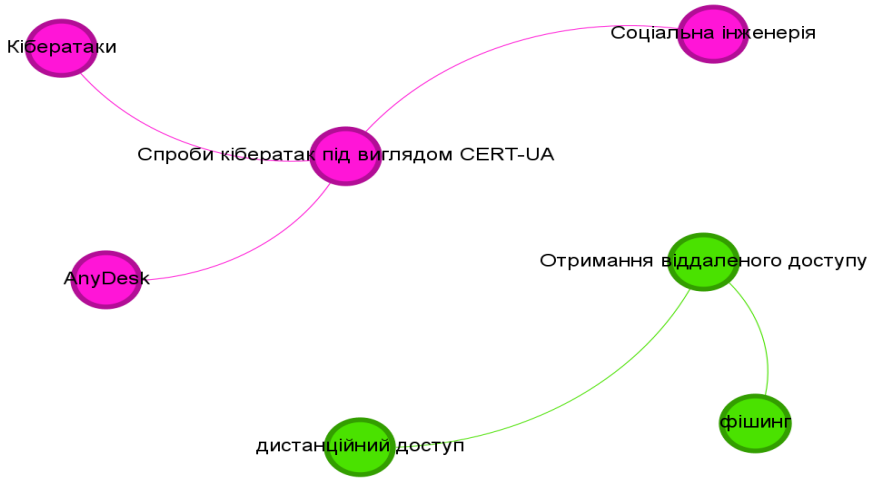


Рисунок 1 – Початкова семантична мережа, сформована на основі вихідного документа

**Розширення мережі за допомогою LLM**

На другому етапі звертаємося до трьох мовних моделей із запитом:

*"Розшир цю семантичну мережу, додавши поняття, що не містяться у вихідному тексті, але містяться у твоїй базі знань та мають логічний зв'язок з існуючими."*

Кожна модель генерує власне розширення мережі.

**Результати розширення від GPT-4**

GPT-4 додав кілька нових зв'язків (табл. 2).

Таблиця 2 – Нові семантичні зв'язки між поняттями, додані GPT-4

| Вузол 1 | Вузол 2 |
|---|---|
| Спроби кібератак під виглядом CERT-UA | Фальшиві домени |
| Спроби кібератак під виглядом CERT-UA | Маніпуляція довірою |
| AnyDesk | Віддалене адміністрування |
| AnyDesk | Віруси |
| Фішинг | Підроблені електронні листи |
| Фішинг | Соціальна інженерія |
| Дистанційний доступ | Отримання віддаленого доступу |
| Дистанційний доступ | Мережеві з'єднання |
| Кібератаки | Викрадення облікових даних |
| Отримання віддаленого доступу | Фішинг |
| Соціальна інженерія | Маніпуляція довірою |

Ці додавання сприяють розвитку семантичної мережі, але деякі зв'язки можуть вважатися менш прямими, зокрема, *"AnyDesk; Віруси"*, оскільки зв'язок між програмним забезпеченням для віддаленого доступу та вірусами не є очевидним. Загалом, згенеровано 18 релевантних та 6 менш релевантних зв'язки (рис. 2).

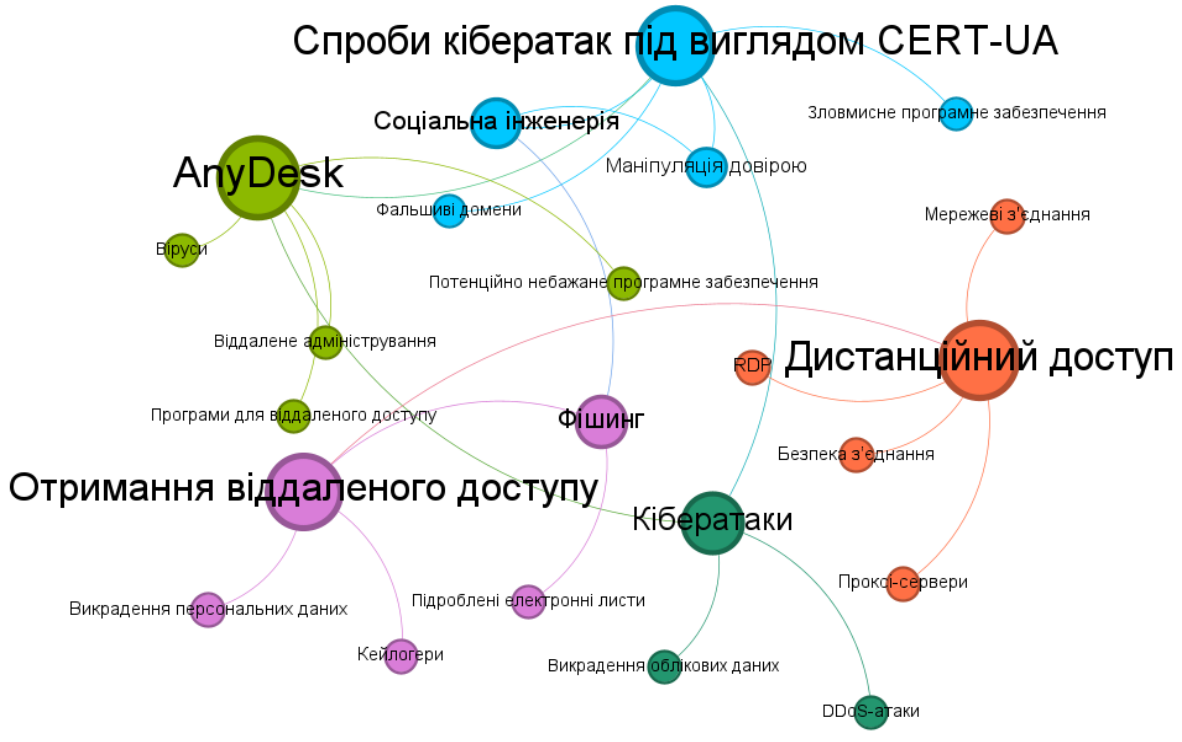


Рисунок 2 – Семантична мережа після розширення за допомогою GPT-4

**Результати розширення від Llama-3**

Llama-3 додала кілька нових зв'язків (табл. 3).

Таблиця 3 – Нові семантичні зв'язки між поняттями, додані Llama-3

| Вузол 1 | Вузол 2 |
|---|---|
| Отримання віддаленого доступу | Злам пароля |
| Кібератаки | Ransomware |
| Кібератаки | Вибухові програми |
| Соціальна інженерія | Фішинг |
| Соціальна інженерія | Привабливі повідомлення |
| AnyDesk | Віддалений доступ |
| AnyDesk | Дистанційне управління |
| Фішинг | Підставні веб-сайти |
| Дистанційний доступ | VPN |
| Дистанційний доступ | SSH |
| Злам пароля | Брутфорс |
| Збір конфіденційної інформації | Фішинг |
| … | … |

Llama-3 розширила мережу (рис. 3), додавши терміни, які зазвичай асоціюються з кіберзлочинністю, але не були безпосередньо згадані в вихідному документі. Деякі з цих зв'язків, як, наприклад, *"Злам пароля; Брутфорс"*, є дуже релевантними в контексті кібербезпеки, проте не в контексті даного документа. Було додано менш релевантних або непрямих зв'язків – 18, релевантних лише 9.


Рисунок 3 – Семантична мережа після розширення за допомогою Llama-3

**Результати розширення від DeepSeek-V3**

DeepSeek-V3 додав кілька нових зв’язків (табл. 4).

Таблиця 4 – Нові семантичні зв’язки між поняттями, додані DeepSeek-V3

| Вузол 1 | Вузол 2 |
|---|---|
| Спроби кібератак під виглядом CERT-UA | Віруси |
| Спроби кібератак під виглядом CERT-UA | Шкідливе програмне забезпечення (malware) |
| Спроби кібератак під виглядом CERT-UA | DDoS-атаки |
| Спроби кібератак під виглядом CERT-UA | Використання вразливостей програмного забезпечення |
| Отримання віддаленого доступу | TeamViewer |
| Отримання віддаленого доступу | Фішинг |
| Соціальна інженерія | Маніпуляція психологією жертви |
| Соціальна інженерія | Підроблені електронні листи (spoofing) |
| Соціальна інженерія | Використання довіри до авторитетних організацій |
| AnyDesk | Програми для віддаленого доступу |
| Фішинг | Підставні електронні листи |

У результаті, модель додала 8 релевантних зв'язків, що підсилюють зв’язок між вже існуючими поняттями в мережі (рис. 4). Однак також було виявлено 3 менш релевантних або непрямих зв'язків, що незначно знижує точність розширення.


Рисунок 4 – Семантична мережа після розширення за допомогою DeepSeek-V3

## 4. Оцінка ефективності моделей за допомогою метрик точності, повноти та *F*-міри

Оцінка ефективності результатів розширення семантичних мереж була здійснена за допомогою трьох основних метрик: точність (*Precision*), повнота (*Recall*) та *F*-міра (*F-Score*).

*Точність (Precision)* визначає пропорцію релевантних зв'язків серед усіх доданих зв'язків:

$$Precision = \frac{TP}{TP + FP}, \tag{9}$$

де: $TP$ – кількість правильно класифікованих релевантних зв'язків;

$FP$ – кількість помилково доданих менш релевантних зв'язків.

*Повнота (Recall)* визначає пропорцію релевантних зв'язків серед усіх правильних зв'язків у реальності:

$$Recall = \frac{TP}{TP + FN}, \tag{10}$$

де: $FN$ – кількість пропущених релевантних зв'язків.

*F-міра (F-Score)* є середнім гармонічним точності та повноти, що дозволяє збалансувати ці дві метрики:

$$F - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}. \tag{11}$$

Розраховані метрики для трьох моделей представлені у таблиці 5.

Таблиця 5 – Показники точності, повноти та *F*-міри для трьох моделей

| Модель | *Precision* | *Recall* | *F-Score* |
|---|---|---|---|
| GPT-4 | 0.75 | 0.72 | 0.734 |
| Llama-3 | 0.333 | 0.75 | 0.461 |
| DeepSeek-V3 | 0.727 | 0.667 | 0.696 |

Аналіз показав, що Llama-3 має найвищу повноту (0.75), але найнижчу точність (0.333), що свідчить про значну кількість хибнопозитивних зв'язків. Це означає, що модель генерує багато нових зв'язків, але не всі з них є коректними.

GPT-4 продемонструвала найкращий збалансований результат ($F\text{-}Score = 0.734$), що вказує на високу якість сформованих зв'язків. DeepSeek-V3 також показала стабільні результати ($F\text{-}Score = 0.696$), близькі до GPT-4, що підтверджує її ефективність у знаходженні релевантних зв'язків із меншим рівнем шуму.

## 5. Інтеграція результатів від різних LLM

Для побудови інтегрованої семантичної мережі використовуються результати, отримані від кількох великих мовних моделей (LLM), зокрема GPT-4, Llama-3 та DeepSeek-V3. Оскільки кожна з моделей генерує власну версію розширеної мережі, їх необхідно об'єднати в єдину узгоджену структуру.

**Формування семантичних мереж різними LLM**

Кожна LLM створює свою розширену семантичну мережу $G_1(m)$, яка визначається як:

$$G_1(m) = (T(m), E(m)), \tag{12}$$

де: $T(m)$ – множина понять (як вихідних, так і нових), знайдених $m$-ю LLM;

$E(m)$ – множина зв'язків між поняттями, виявлених $m$-ю LLM.

**Об'єднання мереж у єдину інтегровану структуру**

Інтегрована семантична мережа $G_{int}$ формується шляхом об'єднання всіх знайдених понять та зв'язків:

$$G_{int} = (\bigcup_m T(m), \bigcup_m E(m)). \tag{13}$$

Таким чином, $G_{int}$ містить усі поняття та зв'язки, запропоновані хоча б однією з LLM.

**Визначення вагових коефіцієнтів для зв'язків**

Щоб оцінити надійність кожного зв'язку, вводиться ваговий коефіцієнт $\omega_{ij}$, який відображає, скільки LLM підтвердили наявність зв'язку між поняттями $t_i$ та $t_j$:

$$\omega_{ij} = \frac{|\{m \mid (t_i, t_j) \in E(m)\}|}{M}, \quad (14)$$

де: $M$ – загальна кількість використаних LLM.

Якщо всі LLM підтверджують зв'язок, його вага дорівнює 1, якщо ні – $\frac{1}{M}$.

У таблиці 6 представлено об'єднані зв'язки між поняттями, отримані після інтеграції результатів трьох мовних моделей (GPT-4, Llama-3, DeepSeek-V3). Кожен зв'язок має ваговий коефіцієнт, що визначає, скільки моделей підтвердили цей зв'язок:

– $\omega_{ij} = 1$ – зв'язок підтверджений усіма трьома моделями, що свідчить про його високу достовірність;

– $\omega_{ij} = 0.67$ – зв'язок підтриманий двома моделями, тобто є доволі надійним;

– $\omega_{ij} = 0.33$ – зв'язок запропонувала лише одна модель, що може вказувати на його меншу надійність.

Таблиця 6 – Об'єднані зв'язки між поняттями з ваговими коефіцієнтами

| Вузол 1 | Вузол 2 | Вага |
|---|---|---|
| Спроби кібератак під виглядом CERT-UA | Кібератаки | 1.00 |
| Спроби кібератак під виглядом CERT-UA | Соціальна інженерія | 1.00 |
| Спроби кібератак під виглядом CERT-UA | AnyDesk | 1.00 |
| Отримання віддаленого доступу | Фішинг | 1.00 |
| Отримання віддаленого доступу | Дстанційний доступ | 1.00 |
| AnyDesk | Програми для віддаленого доступу | 0.67 |
| Спроби кібератак під виглядом CERT-UA | Шкідливе ПЗ | 0.67 |
| Соціальна інженерія | Фішинг | 0.67 |
| Спроби кібератак під виглядом CERT-UA | DDoS-атаки | 0.33 |
| Кібератаки | Ransomware | 0.33 |
| Фішинг | Підставні веб-сайти | 0.67 |
| … | … | … |

На рис. 5 наведено результат об'єднаної семантичної мережі, сформованої після об'єднання зв'язків, отриманих від трьох LLM. Дані були завантажені у програмне середовище Gephi для візуалізації, де мережу додатково було оптимізовано вручну – виконано "естетичну" обробку з метою покращення читабельності, зручності сприйняття та виокремлення ключових вузлів і зв'язків.

**Фільтрація слабких зв'язків**

Щоб підвищити точність інтегрованої мережі, можна видалити малонадійні зв'язки, залишивши лише ті, для яких $\omega_{ij} > \theta$, де $\theta$ – порогове значення (наприклад, $\theta = 0.5$, тобто зв'язок має бути підтверджений щонайменше половиною моделей).

Таким чином, остаточна інтегрована мережа визначається як:

$$G_{int} = (\bigcup_m T(m), \{(t_i, t_j) \mid \omega_{ij} > \theta\}), \quad (15)$$

Використання вагових коефіцієнтів дозволяє фільтрувати слабкі зв'язки та залишати у фінальній мережі (рис. 6) лише найбільш підтверджені концептуальні відносини.

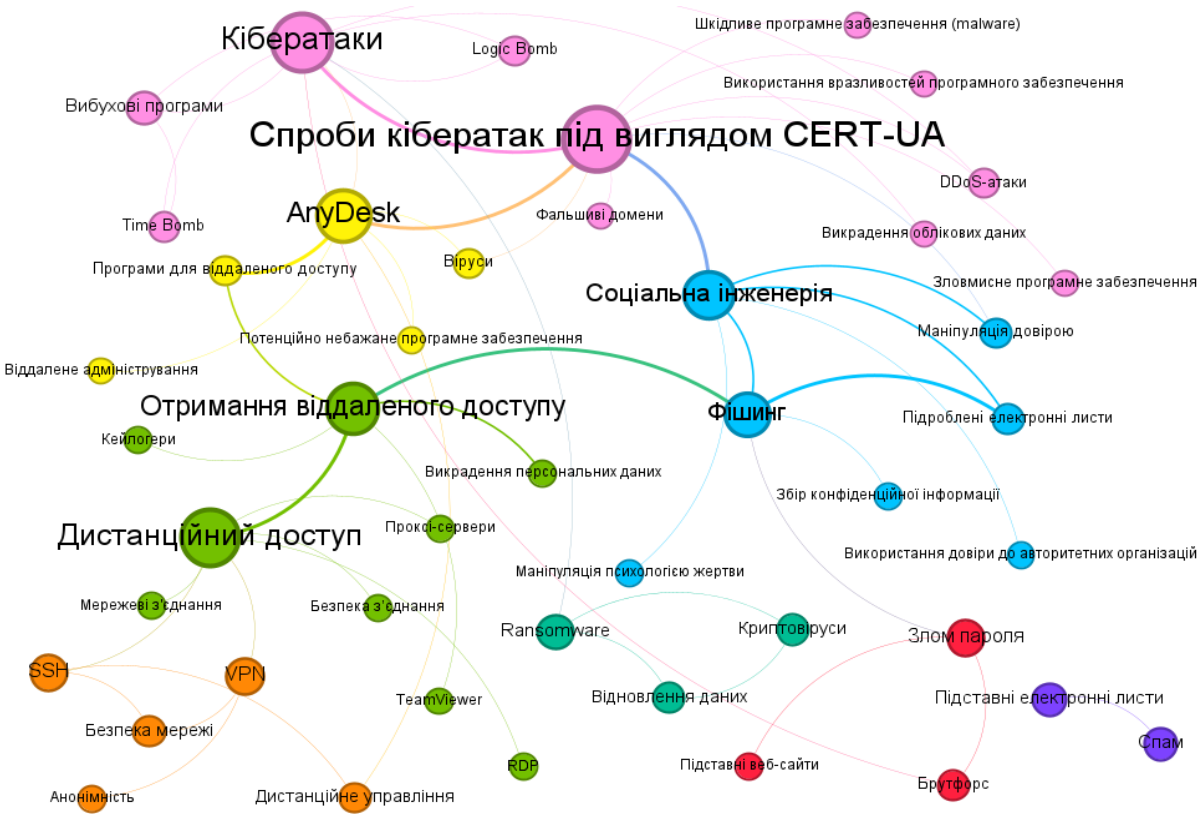


Рисунок 5 – Інтегрована семантична мережа після об'єднання результатів всіх LLM


Рисунок 6 – Інтегрована семантична мережа після фільтрації слабких зв'язків

**Висновки.** У статті розглянуто методику розширення семантичних мереж на основі аналізу тексту із застосуванням великих мовних моделей (GPT-4, Llama-3, DeepSeek-V3). Запропоновано підхід, що включає три основні етапи: побудову первинної семантичної мережі, її розширення за допомогою LLM та інтеграцію результатів від різних моделей.

Аналіз отриманих результатів показав, що GPT-4 та DeepSeek-V3 мають найбільш збалансовані показники точності та повноти, що підтверджує їхню здатність знаходити коректні семантичні зв'язки з мінімальним рівнем шуму. Натомість Llama-3 демонструє високу повноту, але низьку точність, що свідчить про схильність моделі до генерації великої кількості нових зв'язків, частина з яких є нерелевантними.

Фільтрація слабких зв'язків дозволяє значно підвищити якість інтегрованої мережі, залишаючи лише зв'язки, підтверджені щонайменше двома моделями. Це усуває похибки окремих моделей і сприяє формуванню узгодженої семантичної мережі, яка містить лише найбільш достовірні зв'язки.

Візуалізація інтегрованої мережі показала, що після об'єднання результатів різних LLM сформувалася структура зі щільними логічними зв'язками, яка може бути використана для поглибленого аналізу знань у спеціалізованих доменах, зокрема в кібербезпеці.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Д. Ланде, та Л. Страшной, *Семантичний нетворкінг на основі великих мовних моделей: монографія*. Київ, Україна: ТОВ "Інжиніринг", 2025.

[2] D. Lande, and L. Strashnoy, "Swarm of Virtual Experts in the Implementation of Semantic Networking", *ResearchGate Preprint*, Oct. 2024. [Online]. Available: https://doi.org/10.13140/RG.2.2.16686.11845. Accessed on: Jan. 15, 2025.

[3] О. Пучков, Д. Ланде, І. Субач, та О. Рибак, "Інтеграція технологій пошуку інформації та штучного інтелекту в галузі кібербезпеки", *Information Technology and Security*, т. 11, № 2, с. 206-215, 2023, doi: https://doi.org/10.20535/2411-1031.2023.11.2.293789.

[4] N. Ding, W. Mayer, Y. Geng, Y. Duan, and Z. Feng, "Generative semantic modeling for structured data source with large language model", in *Proc. 2023 IEEE Int. Conf. on High Performance Computing & Communications, Data Science & Systems, Smart City & Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC / DSS / SmartCity / DependSys)*, Melbourne, Australia, 2023, doi: https://doi.org/10.1109/hpcc-dss-smartcity-dependsys60770.2023.00164.

[5] D. Lande, and L. Strashnoy, "Concept networking methods based on ChatGPT & Gephi", *SSRN Electronic Journal*, 2023, doi: https://doi.org/10.2139/ssrn.4420452.

[6] R. Jeyaram, R. Ward, and M. Santolini, "Reconstructing networks from text using Large Language Models (LLMs)", in *Proc. 12th Int. Conf. on Complex Networks and their Applications*, Menton, France, 2023. [Online]. Available: https://hal.science/hal-04514924v1. Accessed on: Jan. 15, 2025.

Стаття надійшла до редакції 23.03.2025.

## REFERENCES

[1] D. Lande, and L. Strashnoy, *Semantic Networking Based on Large Language Models: Monograph*. Kyiv, Ukraine: "Engineering Ltd", 2025..

[2] D. Lande, and L. Strashnoy, "Swarm of Virtual Experts in the Implementation of Semantic Networking", *ResearchGate Preprint*, Oct. 2024. [Online]. Available: https://doi.org/10.13140/RG.2.2.16686.11845. Accessed on: Jan. 15, 2025.

[3] O. Puchkov, D. Lande, I. Subach, and O. Rybak, "Integration of information search technologies and artificial intelligence in the field of cybersecurity", *Information Technology and Security*, vol. 11, no. 2, pp. 206-215, 2023, doi: https://doi.org/10.20535/2411-1031.2023.11.2.293789.

[4] N. Ding, W. Mayer, Y. Geng, Y. Duan, and Z. Feng, "Generative semantic modeling for structured data source with large language model", in *Proc. 2023 IEEE Int. Conf. on High Performance Computing & Communications, Data Science & Systems, Smart City & Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC / DSS / SmartCity /*

*DependSys)*, Melbourne, Australia, 2023, doi: https://doi.org/10.1109/hpcc-dss-smartcity-dependsys60770.2023.00164.

[5] D. Lande, and L. Strashnoy, “Concept networking methods based on ChatGPT & Gephi”, *SSRN Electronic Journal*, 2023, doi: https://doi.org/10.2139/ssrn.4420452.

[6] R. Jeyaram, R. Ward, and M. Santolini, “Reconstructing networks from text using Large Language Models (LLMs)”, in *Proc. 12th Int. Conf. on Complex Networks and their Applications*, Menton, France, 2023. [Online]. Available: https://hal.science/hal-04514924v1. Accessed on: Jan. 15, 2025.

DMYTRO LANDE,
OLEKSANDR RYBAK

## APPLICATION OF LARGE LANGUAGE MODELS FOR INTELLIGENT EXPANSION OF SEMANTIC NETWORKS

This paper proposes a methodology for constructing and further expanding semantic networks based on text analysis using large language models (LLM). The initial semantic network is expanded with the help of GPT-4, Llama-3, and DeepSeek-V3, and the obtained results undergo quantitative evaluation of precision and recall. The proposed semantic networking technology [1] is based on the concept of a "swarm of virtual experts" [2], where each LLM enhances the semantic network with its own knowledge and connections.

Additionally, an approach to network integration has been developed, enabling the consolidation of results from different LLMs into a unified structure. The use of a weak-link filtering mechanism enhances the reliability of the final network by eliminating false-positive connections and reducing information noise, contributing to a more accurate and complete representation of knowledge.

For semantic network visualization, the Gephi software is utilized – a free and open-source network analysis and visualization tool.

**Keywords:** semantic networks, large language models (LLM), cybersecurity, OSINT, text analytics.

**Ланде Дмитро Володимирович,** доктор технічних наук, професор, завідувач кафедри, Навчально-науковий фізико-технічний інститут Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна, ORCID 0000-0003-3945-1178, dwlande@gmail.com.

**Рибак Олександр Олегович,** аспірант**,** Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна, ORCID 0009-0004-1033-1599, rybak.oleksandr01@gmail.com.

**Lande Dmytro**, doctor of technical sciences, professor, chair of the department, Educational and scientific physico-technical institute at the National technical university of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine.

**Rybak Oleksandr**, postgraduate student, Institute of special communication and information protection at the National technical university of Ukraine “gor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine..