



ДЕРЖАВНА НАУКОВА УСТАНОВА  
«ІНСТИТУТ ІНФОРМАЦІЇ, БЕЗПЕКИ І ПРАВА  
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ»

АПАРАТ ВЕРХОВНОЇ РАДИ УКРАЇНИ

## **ТРАНСФОРМАЦІЙНІ ПРОЦЕСИ ПРАВОТВОРЧОЇ ДІЯЛЬНОСТІ ТА ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ**

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

*Київ, 30 жовтня 2025 року*

Київ-Одеса  
2025

УДК 342.53:328.36:004.9  
Т 65

**Рекомендовано до друку**

*Вченою радою Державної наукової установи «Інститут інформації,  
безпеки і права Національної академії правових наук України»  
(протокол № 10 від 09.12.2025 р.).*

**Т 65 Трансформаційні процеси правотворчої діяльності та парламентського контролю :** матеріали наук.-практ. конф. (Київ, 30 жовт. 2025 р.) [Електронне видання] / упоряд.: В. М. Фурашев, С. О. Дорогих. Київ; Одеса : Фенікс, 2025. 108 с. Режим доступу: [https://ippi.org.ua/sites/default/files/zbirnik\\_tez\\_30.10.2025.pdf](https://ippi.org.ua/sites/default/files/zbirnik_tez_30.10.2025.pdf)

ISBN 978-617-8430-98-6

Збірник містить матеріали: щодо тенденцій, проблем і пріоритетів розвитку парламентського контролю із застосуванням технологій штучного інтелекту; напрямів, здобутків і проблем цифрової трансформації; інформаційного і правового моделювання удосконалення парламентської діяльності та перспективних напрямів розвитку систем і технологій у сфері здійснення парламентського та інших видів контролю.

Доповіді учасників конференції можуть бути корисними для фахівців, експертів і вчених, науково-педагогічних працівників і здобувачів вищої освіти.

**УДК 342.53:328.36:004.9**

*Матеріали подано в авторській редакції.*

ISBN 978-617-8430-98-6

© Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2025

© Апарат Верховної Ради України, 2025

© Колектив авторів, 2025

## З М І С Т

### **КРАСНОСТУП Г.М.**

Парламентський контроль: виклики та можливості в контексті державної інформаційної політики 5

### **КОРЖ І.Ф., КОРЖ Т.І.**

Роль штучного інтелекту в парламентській діяльності: міжнародний досвід 10

### **ДОРОГИХ С.О.**

Штучний інтелект у законотворчій діяльності: новий етап еволюції нормотворення 15

### **НИЖНИК А.І.**

Організаційно-правові засади цифрової трансформації парламенту 20

### **ЛАНДЕ Д.В., РИБАК О.О.**

Архітектура RAG для динамічного створення семантичних мереж у правовій сфері 25

### **ЛАНДЕ Д.В., КАЧИНСЬКИЙ А.Б.**

Семантичний показник посередництва вузлів у когнітивних мережах 29

### **ЛАНДЕ Д.В., КУЗЬМІНСЬКИЙ В.С.**

Диспетчер керування запитами для неоднорідних середовищ аналізу правових документів 34

### **ЛАНДЕ Д.В., ДАНИК Ю.Г., СТРАШНОЙ Л.Л.**

Застосування фреймворку безкодового програмування на основі великих мовних моделей у правовій сфері 38

### **ЛАНДЕ Д.В., КАЧИНСЬКИЙ А.Б.**

Ранжування та кластеризація понять графової моделі когнітивної війни через PCA та LLM 41

### **ЗАЯРНИЙ О.А.**

ІІІ-агенти як інструменти парламентського контролю Уповноваженого Верховної Ради України з прав людини: деякі особливості впровадження 45

### **БРАЙЧЕВСЬКИЙ С.М.**

Дві парадигми штучного інтелекту в парламентському контролі 50

### **ЛЕОНОВ Б.Д. КАЗЬМІРУК С.Д.**

Інноваційні підходи застосування ІІІ як інструменту парламентського контролю 55

### **ЛАНДЕ Д.В., ФУРАШЕВ В.М.**

Штучний інтелект у державному управлінні: від аналізу текстів 59

до інтелектуальної системи парламентського контролю

**КАЗЬМИРУК С.Д.**

Трансформаційні процеси застосування систем детекції брехні на основі ШІ в аспекті правотворчої діяльності та парламентського контролю 64

**ДОРОНІН І.М.**

Небезпека викривлення інформації в аспекті застосування технологій штучного інтелекту 67

**ЛАНДЕ Д.В., ДАНИК Ю.Г.**

Змагальний штучний інтелект в правовій сфері 72

**ЗАЄЦЬ Д.Г.**

Інформаційно-правова політика [прозорості] лобіювання в Україні 76

**ЛИХОСТУП С.В., МОРОЗ А.О.**

Вплив соціальних і політичних відносин в суспільстві на процеси парламентського контролю законодавчої діяльності 81

**ДУБНЯК М.**

Штучний інтелект у публічному адмініструванні: міжнародний досвід 87

**САВІНОВА Н.А.**

Свідомість людини під захистом європейського AI Act: виклики національним правовим системам 93

**ВАРИНСЬКИЙ В.О.**

Ризики використання ШІ в правосудді: огляд проблеми 97

**ФУРАШЕВ В.М., ДОРОГИХ С.О.**

Трансформація правотворчості та парламентського контролю в умовах цифровізації: концептуальні засади та практичні виклики 102

**Красноступ Г. М.**

кандидат юридичних наук, с.н.с., провідний науковий співробітник наукової лабораторії інформаційного права та інформаційної безпеки Наукового центру інформації і права Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України»

ORCID: <https://orcid.org/0009-0002-8074-3383>

## **ПАРЛАМЕНТСЬКИЙ КОНТРОЛЬ: ВИКЛИКИ ТА МОЖЛИВОСТІ В КОНТЕКСТІ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ**

Парламентський контроль є одним із ключових інститутів демократичного врядування, що забезпечує прозорість, підзвітність та ефективність діяльності органів виконавчої влади. У сучасному цифровому середовищі контрольні функції парламенту набувають нових форм, пов'язаних із розвитком інформаційних технологій, зростанням ролі цифрових платформ та викликами у сфері інформаційної безпеки.

В умовах воєнного стану в Україні значення парламентського контролю у сфері інформаційної політики особливо зростає, адже інформаційний простір стає полем гібридного протистояння та інструментом забезпечення стійкості держави.

Парламентський контроль є одним із ключових механізмів забезпечення прозорості, підзвітності та ефективності діяльності виконавчої влади. У сучасних умовах, коли державне управління, комунікації та інформаційні потоки дедалі більше переходять у цифрову площину, парламентський контроль набуває нових форм і інструментів. У цифрову епоху парламент не лише здійснює контрольні функції традиційними способами – через запити, слухання, звіти уряду, – але й мусить реагувати на виклики, пов'язані з інформаційною безпекою та іноземними інформаційними маніпуляціями та втручанням. В Україні ці процеси особливо актуальні в умовах правового режиму воєнного стану, коли

цифрові технології стали як інструментом державної стійкості, так і полем інформаційних атак.

На думку Чижевського Б. Г. парламентський контроль необхідно розглядати як важливу ділянку праці народних депутатів України, політиків, державних службовців, представників силових інститутів, промисловців, підприємців, науки, освіти, бізнесу, банківської справи, суспільних самоврядних організацій, профспілок із постійним зростанням вимог до якості визначеної площини та рівня співпраці.

Регламент Верховної Ради України встановлює порядок підготовки і проведення сесій Верховної Ради, її засідань, формування державних органів, визначає законодавчу процедуру, процедуру розгляду інших питань, віднесених до її повноважень, та порядок здійснення контрольних функцій Верховної Ради. При цьому, особливості здійснення контрольних функцій Верховної Ради у сферах національної безпеки і оборони визначаються Законом України «Про національну безпеку України».

Парламентський контроль – це сукупність повноважень та інструментів, за допомогою яких Верховна Рада України здійснює нагляд за діяльністю органів виконавчої влади та забезпечує дотримання принципів законності, підзвітності й відкритості. У контексті інформаційної політики парламентський контроль охоплює: нагляд за дотриманням свободи слова та прав журналістів; контроль за діяльністю державних медіа та регуляторних органів; моніторинг виконання законів в інформаційній сфері, у тому числі доступу до публічної інформації, у сфері медіа. Комітети Верховної Ради, зокрема Комітет з питань гуманітарної та інформаційної політики, Комітет з питань свободи слова відіграють ключову роль у здійсненні цього контролю.

Цифровізація державного управління відкриває нові можливості, проте водночас створює низку викликів:

- інформаційне перевантаження та складність аналітичної обробки великих масивів даних;

- кіберзагрози та ризики витоку інформації;

- алгоритмічна непрозорість рішень, прийнятих із використанням штучного інтелекту;

- зростання ролі приватних платформ у формуванні суспільного дискурсу;

питання захисту персональних даних і конфіденційності комунікацій.

При цьому, цифровізація розширює участь громадян у контролі – через електронні петиції, платформи зворотного зв'язку, моніторинг виконання законів.

Інформаційне перевантаження – великий обсяг даних, що потребує аналітичної обробки. Разом з цим, кіберзагрози, алгоритмічна непрозорість, недовіра до інформації, а також питання захисту персональних даних створюють нові ризики для здійснення ефективного парламентського нагляду.

У країнах ЄС формується концепція «digital parliamentary oversight» – цифрового парламентського нагляду, що передбачає використання інструментів електронної демократії та відкритих даних для моніторингу діяльності уряду.

Естонія впровадила парламентський нагляд за системою *e-Government* через електронні засідання та звіти уряду (Parliament of Estonia, *e-Government Reports*);

Велика Британія створила Комітет з питань цифрових технологій, культури, медіа та спорту, який аналізує питання дезінформації та цифрової безпеки (UK Parliament – DCMS Committee);

Франція практикує щорічне звітування уряду перед парламентом щодо ходу цифрових реформ та виконання національної стратегії цифрового переходу (Assemblée nationale – Rapport sur la transformation numérique).

Україна поступово адаптує ці підходи, поєднуючи цифрові механізми контролю з традиційними парламентськими інструментами.

Наприклад, відповідно до звернення Голови Верховної Ради України центральні органи виконавчої влади готують та подають Кабінетові Міністрів України інформацію щодо розроблених та поданих на розгляд Верховної Ради України проєктів законодавчих актів, розроблених на виконання доручень Кабінету Міністрів України, передбачених у прикінцевих положеннях законодавчих актів, прийнятих Верховною Радою України IX скликання.

Як це відбувається на практиці? На виконання пункту 1.14 Плану організації підготовки проєктів актів та виконання інших завдань, необхідних для забезпечення реалізації Закону України «Про медіа» та пункту 2

протоколу наради щодо врегулювання статусу та засад діяльності суб'єкта у сфері парламентського мовлення від 03 липня 2025 р., Міністерство культури України підготувало проєкт Постанови Верховної Ради України «Про деякі питання статусу та засад діяльності державного підприємства «Парламентський телеканал «Рада». На звернення Голови Верховної Ради України Уряд інформує Парламент про проведену роботу.

Таким чином, в Україні поступово формується сучасна модель парламентського контролю, яка поєднує цифрові інструменти моніторингу з традиційними механізмами парламентського нагляду. Впровадження елементів цифрового парламентського нагляду сприяє підвищенню прозорості діяльності уряду, забезпечує регулярне інформування парламенту про стан виконання законів і доручень Верховної Ради України, а також створює умови для більш ефективного контролю за реалізацією державної політики у стратегічних сферах, зокрема інформаційній та медійній.

Український досвід засвідчує прагнення адаптувати найкращі європейські практики, де парламент виступає не лише законодавчим, але й цифровим контрольним інститутом, здатним здійснювати системний нагляд за діями уряду, використовуючи інструменти відкритих даних, електронної звітності та публічної підзвітності. Такий підхід зміцнює принципи демократичного врядування, підвищує довіру громадян до державних інституцій і забезпечує сталий розвиток парламентського контролю в цифрову епоху.

З огляду на наведене, у цифрову епоху парламентський контроль стає не лише механізмом стримувань і противаг, а й ключовим інструментом цифрової демократії. Його ефективність визначається здатністю парламенту адаптуватися до нових технологічних умов, забезпечуючи баланс між інноваціями, прозорістю та безпекою. Для України це має особливе значення – як засіб зміцнення інформаційного суверенітету, державної стійкості та суспільної довіри в умовах війни та післявоєнного відновлення.

З цією метою для підвищення ефективності парламентського контролю у сфері інформаційної політики доцільно:

посилити цифрову та медіаграмотність народних депутатів шляхом системного навчання;

розвивати співпрацю парламенту з урядом, громадянським суспільством і міжнародними партнерами у сфері протидії дезінформації;  
запровадити електронні інструменти контролю – онлайн-платформи моніторингу виконання державних стратегій та доступу до відкритих даних;  
підтримувати ініціативи з фактчекінгу та перевірки інформації, доступні широкій громадськості.

### **Список використаної літератури:**

1. Чижевський, Б. Г. Парламентський контроль як одна із демократичних форм управління трансформаційними процесами. Матеріали Всеукраїнської науково-практичної конференції «Правові, економічні та соціально-політичні аспекти розвитку суспільства в умовах євроінтеграції». 2024. С. 38. URL: [https://ippi.org.ua/sites/default/files/konferenciya\\_25.04.2024.pdf](https://ippi.org.ua/sites/default/files/konferenciya_25.04.2024.pdf)
2. Про Регламент Верховної Ради України : Закон України від 10 лютого 2010 р. № 1861-VI. URL : <https://zakon.rada.gov.ua/laws/show/1861-17#Text>
3. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2469-19#n2>
4. Riigikogu. Parliamentary supervision : Introduction and history. URL: <https://www.riigikogu.ee/en/introduction-and-history/riigikogu-tasks-organisation-work/what-does-riigikogu/parliamentary-supervision/>
5. Parliament of the United Kingdom. Digital, Culture, Media and Sport Committee. Disinformation and 'fake news': Final Report (Eighth Report of Session 2017–19, HC 1791). London, 2019. URL: <https://committees.parliament.uk/work/6330/disinformation-and-fake-news/publications/reports-responses/>
6. Les Français et le numérique. // Ministère de l'Économie, des Finances et de la Souveraineté industrielle et énergétique. URL: <https://www.economie.gouv.fr/groupe1/le-rapport-sur-les-francais-et-le-numerique>

**Корж І.Ф.**

доктор юридичних наук, старший науковий співробітник, заступник керівника наукового центру, Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»

ORCID: <https://orcid.org/0000-0003-0446-5975>

**Корж Т.І.**

аспірант, Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»

## **РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ПАРЛАМЕНТСЬКІЙ ДІЯЛЬНОСТІ: МІЖНАРОДНИЙ ДОСВІД**

Загальновизнано, що парламенти можуть використовувати переваги штучного інтелекту (ШІ) у своїй діяльності. Цікавим і корисним для національного парламенту може мати міжнародний досвід у даній сфері.

Наприклад, окрім обговорення та прийняття нового законодавства, спрямованого на створення сталої правової бази, парламенти також можуть досліджувати, аналізувати та експериментувати у власній діяльності із застосуванням ШІ. Алгоритми машинного навчання можуть аналізувати величезні обсяги законодавчих документів, виявляючи закономірності, тенденції та відповідні ідеї.

Окрім зазначеного вище, ефективним є застосування ШІ керівництвом високого рівня для вирішення питання призначення на посади менеджерів нижчого рівня, а також для співробітників парламенту та депутатів, які зацікавлені у формуванні розуміння того, як використання ШІ може впливати на роботу парламенту в цілому. Особливо актуальним у процесі використання ШІ є підтвердження демократичного принципу щодо залучення громадськості до управління державними справами, а також щодо здійснення контролю за діяльністю публічної влади з боку громадськості.

Як зазначають в IPU [1] (англ. - Inter-Parliamentary Union; міжпарламентський союз, міжнародна організація, створена в 1889 році Фредеріком Пассі та Рандамом Крімером, що сприяє співпраці та діалогу між парламентами різних країн світу для зміцнення демократії, миру та сталого розвитку), на сьогодні існують відповідні можливості для впровадження на основі ІІІ в багатьох сферах парламентської діяльності. В загальному контексті ІІІ може підтримувати адміністративні, законодавчі та громадські процеси залучення, а також зусилля парламенту щодо забезпечення транспарентності у своїй діяльності. Однак, на сьогодні ще невелика кількість парламентів розробляє програми на основі використання ІІІ щодо своєї діяльності, які тестуються на пілотній або прототипній основі.

Необхідно зазначити, що кожен парламент має певні свої особливості і буде використовувати зазначені можливості по-різному, враховуючи свою національну культуру, виходячи із напрацьованих практик, наявності у них ресурсів та часових рамок. Однак, і це вказує на ефективність у використанні ІІІ, алгоритми машинного навчання можуть аналізувати величезні обсяги законодавчих документів, виявляти закономірності, тенденції та відповідні ідеї. Крім того, платформи аналізу даних на основі ІІІ можуть сприяти формулюванню політики на основі доказів, синтезуючи різноманітні джерела інформації та виділяючи ключові висновки для тих осіб, які приймають ті, чи інші рішення.

Важлива є функція ІІІ у виявленні подібностей та відмінностей у законодавстві. Алгоритми машинного навчання можуть порівнювати та зіставляти запропоновані проекти нормативних актів з чинним законодавством. Виявлення подібностей, розбіжностей чи суперечностей зможе допомогти уникнути конфліктів між нормативними актами та забезпечити нормативну узгодженість, а також дати змогу визначити різну впливовість подібних нормативних актів, тим самим виявити причини зазначеного.

Ще однією функцією ІІІ може бути сприяння законодавчій роботі парламенту, надаючи оцінку можливого впливу законопроектів та відображувати поправки до проекту, щоб розуміти їхній вплив на законопроект в цілому. Крім того, системи ІІІ можуть використовуватися для аналізу потенційного впливу запропонованих проектів, допомагаючи

депутатам приймати обґрунтовані рішення щодо життєздатності проєктів, виявляти неочікувані наслідки внесених пропозицій.

Системи ІІІ можуть бути використані для здійснення аналізу внесених поправок та голосування, що сприяє забезпеченню правильного їх узгодження із законопроєктами, а також позитивно впливає на транспарентність і легке розуміння змін і відповідного впливу запропонованих змін.

Особливо актуальним є використання систем ІІІ для збору комплексних даних та детального аналізу впливу прийнятого закону на суспільні відносини. Тим самим зазначене дозволяє депутатам зрозуміти, чи досягнуто очікуваних цілей і задач від дії закону, а також уявити, чи потребує закон перегляду і яким чином.

Очікується ефективним використання систем ІІІ для аналізу баз даних та онлайн-джерел з метою визначення експертів, ключових зацікавлених сторін, дослідницьких звітів та інших відповідних ресурсів, пов'язаних з конкретними законодавчими темами, забезпечення законодавчої роботи депутатів актуальною та достовірною інформацією. Як зазначалося вище, залучення громадськості до управління державними справами надає можливості цифровому парламенту сприймати громадські думки і подавати їх до парламентських комітетів та для проведення розслідувань. Зазначене збільшує обсяг обробки даних для працівників парламенту, і саме для виконання даного завдання можуть бути використані системи ІІІ, насамперед у визначенні тем та для групування подань.

Також, використання технології ІІІ для обробки текстів (NLP – обробка природної мови) та роботизована автоматизація різних процесів (RPA), спроможні допомогти автоматизувати рутинні адміністративні завдання, такі як планування зустрічей, складання порядку денного та управління документацією. Зазначене дозволяє виділити більше часу та ресурсів на більш важливі види діяльності, підвищуючи тим самим продуктивність та ефективність.

Системи ІІІ можуть бути використані для аналізу робочих розкладів депутатів, визначення та автоматичного планування засідань та парламентських сесій. Крім того, парламенти створюють та обробляють великі обсяги документів, таких як законопроєкти, звіти комітетів,

повідомлення та протоколи засідань, тому буде доцільним використання систем ІІІ для автоматичного впорядкування, маркування та архівування цих документів, що полегшує швидкий їх пошук та їх отримання за потреби.

Безцінним інструментом система ІІІ може бути для автоматичного перекладу законодавчих документів, особливо європейського парламенту, що дозволяє депутатам отримувати доступ до інформації бажаною мовою. Крім того, депутати отримують великі обсяги електронних листів та інших електронних повідомлень від своїх виборців та колег. У даному випадку системи ІІІ можуть використовуватися для автоматичної класифікації цих повідомлень, визначення найбільш термінових або релевантних (точно відповідає запиту або темі) та направлення їх відповідним особам для обробки.

Допоміжними ключовими завданнями в парламентах є створення звітів та аналіз даних. Системи ІІІ можуть використовуватися для збору та аналізу відповідних даних, використовуючи візуалізацію даних (процес представлення складних масивів даних у графічній формі (діаграми, графіки, теплові карти, що робить інформацію легкою для сприйняття, допомагає швидко виявляти закономірності, тенденції та аномалії, а також спрощує аналіз і прийняття рішень) та прогнознi моделі для створення детальних та легкозрозумілих звітів для депутатів.

Підвищення прозорості і підзвітності в парламенті є ще одною перевагою використання ІІІ, що дозволяє здійснити аналіз настроїв, оцінювати громадську думку щодо законодавчих пропозицій, дозволяючи депутатам краще розуміти та вирішувати проблеми своїх виборців. У свою чергу, інструменти пошуку на базі ІІІ можуть дозволити виборцям легко знаходити інформацію про законопроекти, голосування, комітети та інші аспекти парламентської роботи. Це сприяє прозорості, роблячи законодавчу інформацію більш доступною та зрозумілою для всіх.

Системи ІІІ можуть використовуватися для аналізу економічних (фінансових) даних, пов'язаних з парламентськими витратами та фінансовими інтересами депутатів, допомагаючи виявляти потенційні конфлікти інтересів, а також сприяючи прозорості та підзвітності, забезпечуючи громадський контроль над депутатами. Водночас, чат-боти на базі ІІІ, інструменти аналізу настроїв та системи створення мультимедійного

контенту можуть посилити залучення громадськості до роботи парламенту, сприяючи комунікації між громадянами та депутатами, пропонуючи розуміння громадської думки. Згадані чат-боти можуть надавати швидкі, персоналізовані відповіді на запити, поширювати інформацію про парламентські процедури та ініціативи. Зазначене дозволить виборцям активно брати участь у демократичному процесі, одночасно звільняючи парламентський персонал від тягаря ручного управління великими обсягами запитів.

Згідно зі Звітом про індекс ШІ за 2024 рік, підготовлений Стенфордським університетом, у світовому законодавчому ландшафті за останні роки спостерігається значне збільшення кількості законів, пов'язаних зі ШІ. З 2016 по 2023 рік парламенти 127 країн ухвалили загалом 123 законопроекти, що згадують про ШІ. Ці закони стосуються різноманітних питань, включаючи освітні реформи, недискримінацію в алгоритмах ШІ та створення навчальних програм зі ШІ. Це підкреслює зростаюче визнання необхідності нормативно-правових баз для відповідального управління розробкою та впровадженням технологій ШІ [2].

В контексті зазначеного важливого значення набуває міжпарламентська співпраця у сфері ШІ, створення міжпарламентських мереж ШІ, адаптування їх до свого контексту, культури та потреб. Така співпраця нині заохочується на всіх рівнях. Основа ефективної співпраці лежить у надійних мережах. Парламенти мають створювати офіційні мережі обміну знаннями про ШІ для постійного обміну досвідом. Такі мережі, як Центр інновацій у парламенті (CPU) IPU, вже існують як засоби для цих обговорень, де парламентські співробітники можуть обговорювати останні розробки та проблеми в управлінні ШІ [3].

### **Список використаних джерел**

1. The role of AI in parliaments. URL: <https://www.ipu.org/ai-guidelines/role-ai-in-parliaments> (дата звернення: 11.10.2025).
2. How parliaments can harness the benefits of AI democratically. URL: <https://www.wfd.org/commentary/how-parliaments-can-harness-benefits-ai-democratically> (дата звернення: 11.10.2025).
3. Inter-parliamentary cooperation for AI. URL: <https://www.ipu.org/ai-guidelines/inter-parliamentary-cooperation-ai> (дата звернення: 11.10.2025).

**Дорогих С.О.**

кандидат юридичних наук, провідний  
науковий співробітник Державної наукової  
установи «Інститут інформації, безпеки і  
права НАПрН України»

ORCID: <https://orcid.org/0000-0002-2748-1938>

## **ШТУЧНИЙ ІНТЕЛЕКТ У ЗАКОНОТВОРЧІЙ ДІЯЛЬНОСТІ: НОВИЙ ЕТАП ЕВОЛЮЦІЇ НОРМОТВОРЕННЯ**

У 1990-х роках у Верховній Раді України відбулася справжня технологічна революція — перехід від друкарських машинок до системи електронного опрацювання законопроектів. Цей крок став початком цифрової трансформації парламентської діяльності, що суттєво підвищив швидкість і зручність законопроектної роботи.

Сьогодні Україна стоїть на порозі нової епохальної зміни — впровадження технологій штучного інтелекту (ШІ) у сферу законотворчості. Якщо раніше автоматизація полягала у спрощенні технічних процесів, що дозволяло пришвидшити проходження законопроекту на усіх етапах його проходження, то зараз ідеться про принципово новий рівень — інтелектуальний аналіз правових текстів, виявлення колізій, дублювань, логічних суперечностей і навіть формування пропозицій щодо вдосконалення законодавства.

Розвиток цифрових технологій, зокрема великих мовних моделей (LLM), відкриває перед законодавчими органами унікальні можливості для підвищення ефективності, прозорості та якості нормотворчої діяльності. Проте впровадження ШІ у законотворчість потребує не лише технічних рішень, а й глибокого розуміння специфіки правової системи, етичних меж та питань відповідальності.

Сучасне українське законодавство характеризується надзвичайно великим обсягом документів і складною структурою нормативних актів.

Станом на сьогодні на офіційному веб-порталі Верховної Ради України міститься біля 300 тисяч нормативних документів — законів, підзаконних актів, міжнародних угод, постанов і розпоряджень.

Таке правове «надбудування» є результатом тридцятирічного процесу становлення незалежної держави, численних реформ, гармонізації з європейським правом і потреби оперативного реагування на нові соціально-економічні виклики.

Проте великий обсяг законодавчого матеріалу створює серйозні труднощі у правозастосуванні. Юристи, аналітики, державні службовці та науковці стикаються з такими проблемами:

- Надмірна фрагментарність законодавства — окремі норми дублюють одна одну або містяться в різних актах без логічної системності.
- Часті зміни та оновлення законів, що призводить до складнощів у відстеженні актуальної редакції.
- Відсутність єдиного підходу до термінології, що створює неоднозначність у тлумаченні норм.
- Суперечності між галузевими актами.
- Складність ієрархічних зв'язків між нормативними актами, особливо при імплементації норм ЄС.

У таких умовах традиційні методи правового аналізу вже не відповідають масштабам і складності сучасного правового масиву. Саме тут на сцену виходять технології штучного інтелекту, здатні працювати з великими обсягами даних, виявляти закономірності й структурувати правову інформацію.

Навіть для досвідченого юриста підготовка законопроєкту є складним і багатоетапним процесом, який потребує не лише знання матеріального права, але й глибокого розуміння законодавчої техніки — правил структурування тексту, формулювання норм, узгодження положень з іншими актами та оцінки можливих правових наслідків. Для парламентарія, який не має юридичної освіти, це завдання ускладнюється в рази: необхідно не лише зрозуміти сутність правового регулювання певної сфери, але й оформити ідею у вигляді нормативного тексту, який відповідатиме вимогам юридичної точності та системності. У таких умовах інструменти штучного інтелекту можуть стати незамінними помічниками, здатними не лише полегшити процес написання, а й підвищити загальний рівень якості законопроєктів, забезпечивши їхню внутрішню логіку, узгодженість і відповідність стандартам нормопроєктування.

Слід врахувати, що значна частина народних депутатів України не має юридичної освіти або фахової підготовки у сфері законотворчості. Це створює певні труднощі при формуванні якісних законопроектів, адже розробка нормативно-правового акту вимагає не лише політичного бачення, але й глибокого розуміння правової логіки, структури нормативних приписів, термінологічної точності та системності права. У цьому контексті використання штучного інтелекту може стати потужним інструментом підтримки депутатів, дозволяючи їм швидко зорієнтуватися у правовій тематиці, яку вони розглядають.

ШІ може аналізувати чинне законодавство, наявні законопроекти, судову практику й експертні висновки, формуючи короткі узагальнення або аналітичні довідки щодо певної сфери правового регулювання. Завдяки цьому депутат отримує можливість зрозуміти основні правові принципи та наявні проблеми без необхідності самостійно опрацьовувати сотні сторінок нормативних документів. Такі системи також можуть надавати підказки щодо структури законопроекту, логічних зв'язків між його розділами, виявляти суперечності з чинними нормами або міжнародними зобов'язаннями України.

Крім того, штучний інтелект здатен допомогти депутатам дотримуватися базових вимог законотворчої техніки — від правильного формулювання дефініцій і посилань до побудови чіткої ієрархії статей і пунктів. Це підвищить якість законотворчого процесу навіть без глибокої юридичної експертизи на початковому етапі розробки законопроекту. У перспективі такі інструменти можуть стати не просто допоміжним ресурсом, а невід'ємною частиною інтелектуального середовища парламенту, що забезпечує більшу прозорість, логічність і ефективність нормотворчої діяльності.

Враховуючи вищенаведене, штучний інтелект може стати ключовим інструментом у вдосконаленні законотворчої діяльності, особливо у сфері аналізу чинного законодавства та створення нових нормативно-правових актів. Насамперед, системи на основі ШІ здатні автоматично аналізувати великі масиви правових документів, виявляючи логічні суперечності, дублювання норм або прогалини у правовому регулюванні. Завдяки використанню методів **обробки природної мови (NLP)**, такі системи можуть

порівнювати тексти законів, знаходити невідповідності між термінами, колізії у визначеннях чи правових наслідках, а також пропонувати рекомендації для їхнього усунення.

Крім того, ШІ може допомагати у побудові правових зв'язків між актами різних рівнів — від законів до підзаконних документів, створюючи динамічні карти нормативної бази. Це дозволяє законодавцю швидко бачити, як нова норма вплине на вже існуючі положення, та уникати неузгодженостей.

У процесі створення нових законопроектів штучний інтелект може виступати як інтелектуальний консультант, який пропонує структуру документа відповідно до вимог законодавчої техніки, генерує можливі формулювання статей на основі аналізу схожих законів інших країн, або перевіряє, чи відповідає запропонований текст загальним принципам права. Застосування таких технологій дозволить не лише підвищити якість законопроектної роботи, але й значно зменшити час, необхідний для підготовки документів, забезпечивши при цьому більшу прозорість і послідовність у законодавчому процесі.

Враховуючи євроінтеграційний курс України, застосування штучного інтелекту у законотворчій діяльності може відіграти особливо важливу роль у процесі гармонізації національного законодавства із правом Європейського Союзу. Алгоритми ШІ здатні здійснювати глибокий порівняльний аналіз нормативних актів України та актів права ЄС — директив, регламентів, рішень Європейського суду тощо. Це дає змогу оперативно виявляти невідповідності, оцінювати ступінь адаптації українських норм до європейських стандартів і навіть пропонувати напрями змін. Такий підхід значно спрощує роботу парламентських комітетів і профільних експертів, особливо у складних сферах — цифрової економіки, захисту персональних даних, кібербезпеки, екологічного права чи антимонопольного регулювання.

Окрім того, ШІ може виконувати функцію аналітичного радника для депутатів, які не є фахівцями у галузі права ЄС, але беруть участь у підготовці законопроектів, пов'язаних із інтеграційними процесами. Інтелектуальні системи здатні пояснювати зміст європейських норм у доступній формі, наводити приклади їхньої реалізації в інших державах-членах ЄС, а також пропонувати адаптовані формулювання для українських

реалій. Таким чином, штучний інтелект може стати важливим посередником між національним і європейським законодавчим простором, сприяючи формуванню узгодженої та ефективної нормативної бази, що відповідає сучасним вимогам інтеграції.

Отже, впровадження штучного інтелекту у сферу законотворчості є не лише технологічною інновацією, а й необхідним етапом еволюції правової системи України. В умовах постійного зростання обсягів нормативних актів, частих змін законодавства та високих вимог до якості правових рішень, ШІ може стати потужним інструментом оптимізації законотворчого процесу. Його використання сприятиме підвищенню ефективності аналізу законопроектів, виявленню колізій, дублювань і прогалин, а також забезпечить системність та узгодженість нормативної бази. Це дозволить зменшити навантаження на парламентські структури, підвищити якість правових актів і прискорити процес їхньої підготовки.

У перспективі штучний інтелект може стати невід'ємним елементом цифрової демократії, де технології підтримують людину в ухваленні обґрунтованих, зважених рішень. Однак для цього важливо забезпечити належне правове регулювання використання ШІ у нормотворчій діяльності, розробити етичні стандарти, гарантії прозорості та відповідальності. Тільки за таких умов штучний інтелект стане не конкурентом, а партнером законодавця, що сприятиме підвищенню якості правового поля України та його відповідності європейським і міжнародним стандартам.

**Нижник А.І.**

Перший заступник керівника Головного  
юридичного управління Апарату Верховної  
Ради України

ORCID: <https://orcid.org/0000-0001-5495-2101>

## **ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПАРЛАМЕНТУ**

Факт схвалення українським парламентом рекомендацій Місії Європейського Парламенту як основи для внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України [1] вказує на визнання суспільної потреби у проведенні парламентської реформи. Зазначеними рекомендаціями передбачено зокрема здійснення заходів, спрямованих на посилення ефективності парламентського контролю, у тому числі й шляхом впровадження е-парламенту (пункт 23) та законодавчого забезпечення гарантій і прав парламентської опозиції (пункт 44).

У результаті зробленого нами аналізу стану їх реалізації виявлено відсутність послідовності між процесами практичного втілення цих рекомендацій. У зв'язку з чим актуальним є питання гармонійного поєднання втілення у парламентську дійсність процедурних керівних принципів щодо прав та обов'язків опозиції в демократичному парламенті [2] та стандартів е-демократії як таких, що мали б сприяти інтеграції України в Європейський Союз і НАТО.

Як відомо, Міжпарламентський Союз наголосив, що нові демократичні країни можуть виграти від закріплення прав парламентської опозиції в конституційних нормах та/або парламентських процедурах [3].

Упродовж 2006 – 2010 років в умовах конституювання в Україні організації державної влади на засадах коаліційної моделі парламентсько-урядової взаємодії, питання легітимації та функціонування парламентської опозиції були унормовані Регламентом ВРУ (глава 13), а після прийняття 8 жовтня 2010 року Закону N 2600-VI [4]- ці питання починаючи з 16 жовтня 2010 року і по нинішній час залишаються законодавчо не врегульованими.

Отже, маємо констатувати існування проблемної ситуації, що виникла внаслідок законодавчого «скасування правил» легітимації у парламенті парламентської опозиції – політичного опонента парламентської коаліції. Цих суб'єктів ми відносимо до системоутвірних складових парламентського буття і вважаємо інституційно-функціональною основою для розвитку організаційно-правового механізму внутрішньої парламентської демократії.

Попри відсутність у парламентському праві згаданих правил, Верховною Радою України поточного скликання починаючи з 16 січня 2020 року надано пріоритет законодавчим крокам, спрямованим на остаточне впровадження е-парламенту. Проте, у разі організації планомірного процесу впровадження е-парламенту варто зважати на такі взаємопов'язані та взаємозалежні компоненти: базисний (демократичні відносини та процеси) і технологічний (впровадження цифрових та інформаційно-комунікаційних технологій).

У цьому контексті видаються слушними та переконливими зроблені з позицій діалектичних закономірностей О. Барановим як визначення е-демократії, так і наступні твердження: «зміст (сутність) демократії в умовах електронної демократії визначається тією моделлю демократії традиційної форми (без використання ІКТ), яка реалізована на даний час у суспільстві... Таким чином, ефективність електронної демократії детермінується насамперед моделлю демократії, яка реалізована на даний час у суспільстві, та можливостями ІКТ, які застосовуються» [5].

Не заглиблюючись у сутність існуючих теорій е-демократії, що розроблені в межах концепції інформаційного суспільства, скористаємося дослідженням Тєро Пайварінта та Ойстейн Себо, які на основі систематизації різних теорій електронної демократії виділяють чотири основні моделі: 1) партійна електронна демократія (Partisan democracy); 2) ліберальна електронна демократія (Liberal democracy); 3) пряма електронна демократія (Direct democracy); 4) деліберативна демократія (Deliberative democracy) [6, с. 823].

Ми вважаємо, що запропонована класифікація моделей е-демократії може використовуватися лише у наукових цілях. Адже за існуючих нині усталених традиційних форм демократії сучасні інструменти здійснення е-демократії не змінюють природу прямої чи представницької демократії, а

лише є альтернативним (інноваційним) способом забезпечення участі громадян у публічному житті та на всіх стадіях політичного процесу. Інакше кажучи конституційовані форми безпосередньої та опосередкованої демократії не перетворюються у пряму і представницьку е-демократію через використання у демократичних процесах ІКТ. Хіба що у науковому сенсі пізнання нової якості цих явищ можна говорити про е-демократію як інтегровану інноваційну частину демократичного устрою суспільства, що виникає внаслідок успішного упровадження у суспільно-політичну сферу сучасних інформаційних технологій, здатних забезпечити дистанційний спосіб взаємодії держави і суспільства.

Як же співвідносяться у науковому та прикладному сенсі такі суспільно-політичні явища: е-демократія, е-урядування та е-парламент?

Якщо скористатися відповідними філософськими категоріями, то у наукових цілях зазначені суспільні явища можуть розглядатися відповідно як загальне (е-демократія), особливе (е-урядування) та одиничне (е-парламент). Запропонований підхід ґрунтується на характерних цим явищам властивостях.

Електронний парламент (E-parlament), як складова більш широкого поняття електронного урядування (E-government), є системою електронної взаємодії учасників парламентських процесів між собою, а також з іншими державними органами, бізнес-структурами, громадянами, зарубіжними та міждержавними утвореннями [7].

Отже е-парламент, е-урядування є лише складовими такого комплексного явища як е-демократія. Цей умовивід спирається також на відповідні європейські стандарти.

Зокрема у Рекомендаціях Комітету міністрів Ради Європи щодо е-урядування окреслено сучасний термінологічний апарат, основні критерії політики е-демократії, принципи, напрямки та інструменти е-демократії. Зокрема, «Е-демократія – це використання ІКТ в демократичних процесах, яке дозволяє (1) посилити участь, ініціативність та залучення громадян на національному, регіональному та місцевому рівнях публічного життя; (2) покращити прозорість демократичного процесу прийняття рішень, а також підзвітність демократичних інститутів; (3) покращити чутливість/ зворотну реакцію органів влади на звернення громадян; (4) сприяння публічним

дебатам та увагу громадян до процесу прийняття рішень. ІКТ повинні удосконалювати доступ та комунікацію з чиновниками та обраними політиками. ***Електронні засоби голосування на виборах та референдумах повинні доповнювати неелектронні традиційні способи***» [8].

У цьому контексті варто наголосити на таких принципах е-демократії:

«Е-демократія спирається на демократичні, гуманістичні, соціальні, етичні та культурні цінності суспільства, в якому вона запроваджується.

Е-демократія повинна бути сумісна та пов'язана із традиційними процесами демократії. ***Кожен процес демократії (електронний чи традиційний) відіграє свою роль і не може застосовуватись як універсальний***» [9].

Як бачимо, у згаданих рекомендаціях принципово розрізняються обидва процеси демократії – традиційний (безпосередній політичний діалог) та електронний (дистанційний політичний діалог).

Спосіб (традиційний чи електронний) реалізації гарантованого Основним Законом України народовладдя на основі форм безпосередньої та опосередкованої демократії має визначатися законом. Зважаючи на вимоги Конституції України (статті 19, 83, 85, 87, 88, 89 і 92) для належної реалізації парламентською опозицією як суб'єктом парламентського контролю закріплених гарантій на ініціювання скликання позачергової сесії, розгляду питання про недовіру уряду, на створення тимчасової слідчої комісії є потреба у невідкладному законодавчому унормуванні процедури легітимації парламентської опозиції на установчій (першій) сесії новообраної Верховної Ради України.

Таким чином, гіпотеза про існування у практиці українського парламенту тенденції випередження розвитку технологічного і регулятивного (забезпечувального компоненту) впровадження е-парламенту порівняно зі станом організаційно-правового забезпечення (нормативно-процедурного компоненту) реалізації гарантій та прав легітимною парламентською опозицією, підтвердилася.

### Список використаних джерел:

1. Постанова Верховної Ради України «Про заходи з реалізації рекомендацій щодо внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України» (Відомості Верховної Ради (ВВР), 2016, № 14, ст.149).
2. Резолюція ПАРЄ (2008). Процедурні керівні принципи щодо прав та обов'язків опозиції в демократичному парламенті <[http://w1.c1.rada.gov.ua/pls/mpz2/docs/753\\_1601\\_Opozytsija\\_rezoljutsija.htm](http://w1.c1.rada.gov.ua/pls/mpz2/docs/753_1601_Opozytsija_rezoljutsija.htm)>. (2021, серпень, 31).
3. Guidelines on the rights and duties of the opposition in parliament. Geneva: Inter-Parliamentary Union. [Електрон. ресурс]. – Режим доступу: <http://www.ipu.org/splz-e/gabon.htm>.
4. Закон України «Про внесення змін до Регламенту Верховної Ради України» від 8 жовтня 2010 року N 2600-VI <https://zakon.rada.gov.ua/laws/show/2600-17#Text>.
5. “Інформація і право” № 1(20)/2017 стор. 34.
6. Päivärinta T., Sæbø, Ø. Models of E-Democracy. Communications of the Association for Information Systems. 2006. № 17. P. 818-843.
7. Електронний парламент України: досвід створення. Наукове видання / За заг. ред. С.О. Довгого. – К.: Логос, 2015, стор.9.
8. Recommendation Rec (2004) 15 Electronic governance (“E-governance”), 2004 (Committee of Ministers of the Council of Europe).  
COE <[https://www.coe.int/t/dgap/democracy/Activities/GGIS/E-governance/Key\\_documents/Rec\(04\)15\\_en.pdf](https://www.coe.int/t/dgap/democracy/Activities/GGIS/E-governance/Key_documents/Rec(04)15_en.pdf)>. (2021, August, 31). [in English].
9. Recommendation CM/Rec(2009)1 on electronic democracy (e-democracy) (Committee of Ministers).  
COE <[https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Recommendation\\_CM\\_Rec2009\\_1\\_en\\_PDF.pdf](https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Recommendation_CM_Rec2009_1_en_PDF.pdf)>. (2021, August, 31). [in English].

**Ланде Д. В.**

доктор технічних наук, професор, керівник  
наукового центру ДНУ ІБП НАПрН України,  
завідувач кафедри НН ФТІ КПІ ім. Ігоря  
Сікорського

ORCID: <https://orcid.org/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 ( $G_0$ )** – BMM 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: законопроекти, парламентські звіти, наукові статті, ЗМІ, за допомогою інформаційно-пошукової системи (наприклад, Cyber Aggregator або парламентська база даних).

**Генерація адаптованої мережі ( $G_1$ )** – та сама BMM 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** (ступінь довіри: 0,7 — лише BMM; 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 долає 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](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 Державної наукової  
установи «Інститут інформації, безпеки і  
права НАПрН України»

ORCID: <https://orcid.org/0000-0003-3945-1178>

**Качинський А.Б.**

доктор технічних наук, професор, професор  
НН ФТІ КПІ ім. Ігоря Сікорського

ORCID: <https://orcid.org/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:

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

де  $\text{opt}_q$  – операція оптимізації за критерієм  $q$ :

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

Для знаходження  $\text{opt}_q$  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:

- $\sigma_{st}^{(q)} = |P_{st}^{(q)}|$  – 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<br>$S_{BCL}$ | $S_{BCR}$ | РАНГ<br>$S_{BCR}$ | $S_{BCC}$ | РАНГ<br>$S_{BCC}$ | $S_{BCS}$ | РАНГ<br>$S_{BCS}$ |
|-------------------------------------|-----------|-------------------|-----------|-------------------|-----------|-------------------|-----------|-------------------|
| 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  $S_{BCL}$  — швидкі кампанії);
- оцінювати економічну ефективність деструктивних сценаріїв (через  $S_{BCC}$ );
- прогнозувати масштаб поширення (через  $S_{BCS}$ ).

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 ; КПП 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 Державної наукової  
установи «Інститут інформації, безпеки і  
права НАПрН України»

ORCID: <https://orcid.org/0000-0003-3945-1178>

**Кузьмінський В.С.**

Аспірант ІСЗЗІ КПІ ім. Ігоря Сікорського

ORCID: <https://orcid.org/0000-0002-9063-9144>

## **ДИСПЕТЧЕР КЕРУВАННЯ 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 законопроектів, звітів, судових рішень часто включає як складні семантичні завдання (наприклад, інтерпретація норм), так і рутинно-алгоритмічні операції (наприклад, вилучення реквізитів, формування хронології подій). Використання ВММ для всіх етапів призводить до надмірної вартості та повільності, що унеможливляє 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 законопроекту»);
- 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. Ланде Д.В., Фурашев В.М. 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, DOI: 10.2139/ssrn.5285664 (Jun 22, 2025). – 12 p.

**Ланде Д.В.**

доктор технічних наук, професор, керівник  
наукового центру Державної наукової  
установи «Інститут інформації, безпеки і  
права НАПрН України»

ORCID: <https://orcid.org/0000-0003-3945-1178>

**Даник Ю.Г.**

доктор технічних наук, професор, професор  
НН ФТІ КПІ ім. Ігоря Сікорського

ORCID: <https://orcid.org/0000-0001-6990-8656>

**Страшной Л.Л.**

старший фахівець з архітектури даних

(Senior Data Architect), Університет

Каліфорнії (UCLA), Лос-Анджелес, США

ORCID: <https://orcid.org/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 законопроектів, 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 Державної наукової  
установи «Інститут інформації, безпеки і  
права НАПрН України»

ORCID: <https://orcid.org/0000-0003-3945-1178>

**Качинський А.Б.**

доктор технічних наук, професор, професор  
НН ФТІ КПІ ім. Ігоря Сікорського

ORCID: <https://orcid.org/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 запитамі, 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 законопроектів до виявлення маніпулятивних наративів 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>

**Заярний О.А.**

доктор юридичних наук, професор, професор  
кафедри інтелектуальної власності та  
інформаційного права Навчально-наукового  
інституту права Київського національного  
університету імені Тараса Шевченка  
ResearcherID: S-3358-2018  
ORCID: <https://orcid.org/0000-0003-4549-7201>

### **ІІІ-АГЕНТИ ЯК ІНСТРУМЕНТИ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ УПОВНОВАЖЕНОГО ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ: ДЕЯКІ ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ**

В умовах системної цифрової трансформації суспільства, обумовленої стрімким технологічним прогресом, а також зростанням викликів, спричинених військовою агресією та гібридними загрозами, цифровізація цифрова трансформація органів державної влади стає необхідною умовою для підвищення їхньої ефективності, прозорості та підзвітності. Одним із ключових напрямів такої трансформації є інтеграція технологій штучного інтелекту (далі - ІІІ) в механізмі парламентського контролю, зокрема, який здійснюється Уповноваженим Верховної Ради України з прав людини.

Ця державна інституція виконує критично важливі функції захисту прав і свобод громадян, і ефективність цього контролю значною мірою залежить від швидкості, послідовності, професійності та якості аналізу великих масивів даних.

У цьому контексті перспективним вбачається використання ІІІ-агентів для автоматизації широкого кола завдань. Однак, такий підхід до цифрової трансформації парламентського контролю, вимагає ґрунтовного аналізу правових засад, функціональних можливостей та потенційних ризиків використання ІІІ-агентів для відповідних цілей.

Відсутність спеціального законодавчого регулювання ІІІ в Україні, а також нагальна потреба гармонізації національного законодавства з

європейськими стандартами, зумовлює актуальність цієї роботи, зокрема, у контексті інтеграційних процесів та зміцнення правової держави.

Метою дослідження є аналіз можливостей, переваг та ризиків застосування ІІІ-агентів як інструментів парламентського контролю в діяльності Уповноваженого Верховної Ради України з прав людини, а також розробка науково обґрунтованих пропозицій щодо впровадження цих технологій у відповідності до міжнародних стандартів та з урахуванням сучасного стану правового регулювання відповідних правовідносин в Україні.

На сьогоднішній день в законодавстві, міжнародних стандартах і науковій літературі не сформовано єдиного визначення ІІІ [1, с. 210]. Так само, як і відсутнє універсальне визначення ІІІ-агентів.

Згідно з визначенням, сформульованим у положеннях Регламенту (ЄС) 2024/1689 «Про штучний інтелект», система ІІІ визначається як «програмне забезпечення, розроблене за допомогою однієї або кількох технік і підходів, що здатне генерувати вихідні дані, такі як контент, прогнози, рекомендації або рішення, для певних цілей» [2].

Виходячи із наведеного визначення, ІІІ-агент можна визначити як автономну програмну систему, яка здатна сприймати навколишнє середовище через сенсори, обробляти інформацію та самостійно приймати рішення для досягнення поставлених цілей.

У контексті передбачених законодавством України завдань парламентського контролю, які виконує Уповноважений Верховної Ради України з прав людини, ІІІ-агенти можуть виконувати низку важливих функцій, які значно підвищують ефективність діяльності та оптимізують найбільш типові юридичні процедури. Зокрема, йдеться про:

*Аналіз великих даних.* Швидка обробка звернень громадян, петицій, судових рішень, законопроектів та інших документів для виявлення системних порушень прав людини. ІІІ-агенти здатні оперативно виявити ключові тенденції та системні скарги, що дозволяє Омбудсману оперативно реагувати на найгостріші проблеми дотримання прав людини.

*Моніторинг законодавства.* Автоматичний пошук та аналіз чинних нормативно-правових актів та проектів законів для виявлення потенційних

колізій або норм, що суперечать Конституції України та міжнародним стандартам прав людини.

*Генерація аналітичних звітів.* Автоматичне створення анотацій, резюме та аналітичних довідок на основі проаналізованих даних, що значно прискорює підготовку парламентських звітів.

*Класифікація та каталогізація.* Автоматична категоризація звернень громадян за типами порушень, що дозволяє швидко виявляти найбільш гострі проблеми та спрямовувати їх до відповідних структурних підрозділів Секретаріату Уповноваженого Верховної Ради України з прав людини.

У механізмі парламентського контролю Уповноваженого можуть бути використані два основні види ШІ-агентів:

1. Агенти, побудовані на загальнопоширених мовних моделях (наприклад, ChatGPT, Gemini тощо). Їхня перевага — висока гнучкість, швидкість та можливість обробки природної мови, але вони можуть нести ризики через недостатню прозорість алгоритмів, що є критично важливим для публічного сектору.

2. Спеціалізовані моделі для потреб парламентського контролю, які створюються з урахуванням специфіки національного законодавства, міжнародних стандартів та вимог до конфіденційності даних. Саме такі моделі використовуються в європейських країнах. Так, в парламенті Італії [3] ШІ-системи використовуються для автоматичної класифікації законодавчих актів та розпізнавання сутностей текстів законодавчих актів. Парламент Фінляндії [4] застосовує ШІ для автоматизації підготовки документів, а Естонія [5], яка вважається однією з найбільш цифровізованих країн, успішно використовує ШІ-систему HANS для автоматичної транскрипції парламентських засідань, що значно підвищує ефективність підготовки стенографічних звітів та їхній подальший аналіз. Уряд Нового Південного Вельсу (Австралія) [6] також пілотує використання ШІ-системи "Co-counsel" для внутрішніх потреб Омбудсмана, яка зберігає високий рівень безпеки та конфіденційності даних, а також розробляє ШІ-асистентів для надання цілодобової підтримки громадянам.

Впровадження ШІ-агентів у механізм парламентського контролю Уповноваженого вимагає дотримання низки юридичних вимог, які закріплені в міжнародних актах та актах «м'якого» права, зокрема:

*Принцип прозорості та підзвітності.* Алгоритми ШІ повинні бути зрозумілими та верифікованими, а відповідальність за рішення, прийняті на основі їхніх рекомендацій, має залишатися за людиною-оператором. Цей принцип закладено в Рекомендації Комітету міністрів Ради Європи CM/Rec(2020)1, яка наголошує на необхідності встановлення механізмів відшкодування збитків у разі порушення прав через використання ШІ [7].

*Дотримання прав людини.* Застосування ШІ не повинно порушувати основні права, зокрема право на недискримінацію, приватність та захист персональних даних. Згідно з Рамковою Конвенцією Ради Європи «Про штучний інтелект, права людини, демократію та верховенство права» (2024), діяльність ШІ-систем має бути повністю узгодженою з цими принципами [8].

*Захист даних.* Системи ШІ, що працюють з конфіденційною інформацією, повинні відповідати найвищим стандартам кібербезпеки.

Не зважаючи на ряд переваг, які несе в собі застосування ШІ-агентів при здійсненні Уповноваженим Верховної Ради України з прав людини в механізмі парламентського контролю, основною перешкодою у реалізації відповідного підходу до цифрової трансформації є відсутність рамкового закону про ШІ.

На нашу думку, використання ШІ-агентів в публічному секторі має бути врегульоване спеціальним законом, аналогічним європейському Акту про ШІ (Regulation (EU) 2024/1689) [2], який класифікує системи за ступенем ризику та встановлює заборонені практики. В Італії, наприклад, національний закон про ШІ вже встановлює вимоги до прозорості та захисту персональних даних у всіх сферах, включаючи державний сектор [3].

Проведене дослідження вказує на значний потенціал ШІ-агентів у підвищенні ефективності парламентського контролю Уповноваженого Верховної Ради України з прав людини, що відповідає сучасним цілям цифрової трансформації державної влади. Водночас, їхнє впровадження має бути системним та відповідальним.

Виконанню вказаних завдань, на нашу думку, може істотно сприяти розробка та ухвалення Закону України «Про основні засади застосування штучного інтелекту», що визначить правовий статус ШІ-агентів, критерії їх класифікації за ступенем ризику та вимоги до прозорості й підзвітності [1, с. 221]. Поряд з цим, обґрунтованим вбачається внесення окремих змін і

доповнень до Закону України «Про Уповноваженого Верховної Ради України з прав людини» в частині визначення правових принципів, напрямів і умов застосування ШІ-агентів при здійсненні парламентського контролю за додержанням прав людини на території України.

### Список використаних джерел

1. Заярний О. А. Законодавче забезпечення розробки і застосування технологій штучного інтелекту в умовах війни та європейської інтеграції України *Правове забезпечення євроінтеграції: загальноправовий та галузевий аспекти* : колективна монографія. – Рига : Baltija Publishing, 2025. – С. 207–224. URL: <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/view/597/16071/33923-1>
2. Regulation (EU) 2024/1689 of the European Parliament and of the Council on a European framework for artificial intelligence. EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>
3. Italy becomes first EU member state to pass an AI law. IAPP. URL: <https://iapp.org/news/a/italy-becomes-first-eu-member-state-to-pass-an-ai-law>.
4. NSW Ombudsman's work in AI spotlighted at international conference. NSW Ombudsman. URL: <https://www.ombo.nsw.gov.au/about-us/news-events/news/nsw-ombudsmans-work-in-ai-spotlighted-at-international-conference>.
5. How AI accelerates the legislative power of the Parliament of Estonia. Nortal. URL: <https://nortal.com/insights/how-ai-accelerates-the-legislative-power-of-the-parliament-of-estonia>.
6. Government submits to Parliament legislation to implement the first phase of EU Artificial Intelligence Act. Valtioneuvosto. URL: <https://valtioneuvosto.fi/en/-/1410877/government-submits-to-parliament-legislation-to-implement-the-first-phase-of-eu-artificial-intelligence-act>.
7. Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. Council of Europe. URL: <https://rm.coe.int/CoERSPublic/CM-Rec-2020-1.pdf>.
8. Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law. Council of Europe. URL: <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>.
9. The role of AI in parliaments. Inter-Parliamentary Union. URL: <https://www.ipu.org/ai-guidelines/role-ai-in-parliaments>.

**Брайчевський С. М.**

кандидат фізико-математичних наук

провідний науковий співробітник

## **ДВІ ПАРАДИГМИ ШТУЧНОГО ІНТЕЛЕКТУ В ПАРЛАМЕНТСЬКОМУ КОНТРОЛІ**

Парламентський контроль як особлива форма державного контролю за діяльністю органів виконавчої влади та посадових осіб є однією з головних складових правової системи в будь якому розвиненому суспільстві. В Україні він набуває особливої ваги через реалізацію програми децентралізації [1], яка є складним процесом, розподіленим у часі. Причина полягає в тому, що реформування повноважень органів місцевої влади розширює і ускладнює систему правових відносин на регіональному рівні.

Зауважимо, що здійснення парламентського контролю тісно пов'язано з опрацюванням публічної інформації [2], оскільки джерелом багатьох важливих відомостей є різноманітні публікації у відкритому медійному просторі. А це, в свою чергу, призводить до суттєвого зростання обсягу інформації, що піддається обробці, а також ускладненню самого процесу обробки. Тому все більш актуальними стають технічні можливості парламентського контролю, зумовлені швидким розвитком сучасних інформаційних технологій, особливо в зв'язку з реалізацією програми цифрової трансформації українського суспільства [3]. Вони не тільки спрощують виконання функцій парламентського контролю, але й якісно підвищують їх ефективність.

Слід визнати, що сьогодні в цьому плані реальних обрисів набуває практичне використання штучного інтелекту (далі AI). Його застосування в парламентській практиці стає темою для широких досліджень в усіх провідних країнах світу [4]. На цей час ще зарано говорити про повноцінне використання AI в парламентській практиці, скоріше питання стоїть в аналізі подібної можливості, але воно вже набуло конкретних обрисів. Тому, на нашу думку, актуальним є аналіз різноманітних підходів та методик застосування тих чи інших систем AI та сервісів на його основі для вирішення різних категорій проблем.

Нижче ми обговоримо дві принципово різні методики використання AI в широкому спектрі задач, що виникають в практиці парламентського контролю. Але, як ми побачимо, вони носять універсальний характер і цілком можуть бути охарактеризовані як дві парадигми AI.

Ті, хто займався роботою з системами AI на професійному рівні, знають, що він може працювати в двох режимах: автоматизованому та автоматичному. В першому з них AI працює під керівництвом та контролем оператора системи, яка його використовує. В другому керування AI (тобто звернення до нього та подальша обробка отриманих результатів) здійснюється безпосередньо апаратно-програмним комплексом без явної участі оператора. Цей режим має два основних різновиди. Система може звертатися до AI, що існує окремо від неї (найчастіше це робиться за допомогою API, які надаються зовнішнім користувачам на певних умовах). Або апаратно-програмний комплекс може містити власний вбудований AI, який розв'язує задачі, що виходять за межі можливостей звичайних тригерних алгоритмів. З технологічної точки зору ситуація цілком зрозуміла. Але між цими двома режимами існує концептуальна відмінність, яка дозволяє поглянути на них під ширшим кутом зору.

Одна з фундаментальних особливостей AI полягає в тому, що він не спроможний ставити перед собою задачі. Він здатний лише виконувати ті задачі, які ставить перед ним зовнішнє оточення. В процесі виконання поставленої задачі AI (на відміну від "звичайних" інформаційних систем) може діяти автономно, в тому числі на основі самонавчання розробляти власні алгоритми, але початкову задачу йому хтось (чи щось, наприклад апаратно-програмний комплекс, до складу якого він входить), мусить поставити. А це означає, що AI, який працює в автоматичному режимі, має принципові обмеження, створені контекстом його роботи. Тобто AI в автоматичному режимі може виконувати лише наперед заданий набір задач, хоча, можливо, і в "творчий" спосіб. Конкретна система AI може бути налаштована на вирішення питання про ідентичність зображень і успішно виконувати цю роботу. Але вона ніколи "за власною ініціативою" не почне складати вірші. Іншими словами, працюючи в автоматичному режимі, AI ніколи не зможе змінити цілеспрямованість роботи системи, до складу якої він входить. Підкреслимо, що в цьому є суттєва перевага автоматичного

режиму. Адже AI внаслідок властивості йому автономії (зумовленої можливостями самонавчання) може в принципі самостійно змінювати напрямок і характер своєї роботи, виходячи за межі тієї мети, для досягнення якої він був створений або задіяний. Таким чином, ви гарантовано отримаєте відповіді саме на ті питання, які були поставлені AI на стадії проектування, розробки та налаштування системи. Звичайно, питання про якість відповідей в кожному конкретному випадку лишається відкритим.

Хоча створення подібної інформаційної системи на рівні практичної експлуатації є справою майбутнього, певні кроки в даному напрямку вже мають місце. Прикладом може служити використання в практиці парламентського контролю інтелектуальних агентів, окремі аспекти якого розглядалися нами в попередній роботі [5]. А в перспективі природньо уявити як одну з базових форм парламентського контролю загальну систему моніторингу правового стану, яка засобами AI відстежує та аналізує всю наявну у відкритих джерелах інформацію на предмет відповідності правовим нормам, які вона отримує з єдиної бази даних нормативно-правових актів. Така система передбачає стандартний набір задач, але водночас є достатньо гнучкою, оскільки вона автоматично реагує на зміни контексту через оновлення з одного боку контенту відкритих джерел, а з другого боку, нормативно-правової бази даних.

З іншого боку, недоліком автоматичного режиму є те, що AI, працюючи в ньому, не здатен реагувати на зміни контексту своєї роботи, а отже і на зміну складу актуального набору задач, які треба відпрацьовувати. Так, наприклад, повномасштабне вторгнення призвело до появи якісно нових ситуацій, що вимагають вирішення низки нових проблем. І якби певний обсяг роботи з парламентського контролю виконувала створена раніше система з AI в автоматичному режимі, в змінених умовах її ефективність значно скоротилася б, оскільки нові задачі опинилися б поза її "увагою".

Суттєва відмінність автоматизованого використання AI полягає в тому, що цей режим дозволяє динамічно змінювати склад задач, які виконує відповідна інформаційна система. Важливо, що робить це людина, яка адекватно розуміє загальний контекст. І ця відмінність може вважатись концептуальною, тому що в даному випадку маємо не лише інший спосіб застосування штучного інтелекту, а його об'єднання з природним (людським)

інтелектом. Людина не просто керує процесом, вона доповнює можливості AI за рахунок функцій, які йому в найближчий історичний період є принципово недоступними.

Якщо в автоматичному режимі AI виконує роботу, яка завжди є актуальною через власну природу, в автоматизованому режимі він може виконувати разові завдання, які виникають внаслідок окремих, непрогнозованих ситуацій. Зрозуміло, що такі ситуації не можуть бути передбачені на стадії проектування системи, а тому для їх опрацювання має бути забезпечена можливість оперативної зміни складу задач.

Автоматичний режим має безперечні переваги для виконання стаціонарної, добре визначеної рутинної роботи, яку бажано здійснювати без явної участі людини. Така робота має виконуватись протягом невизначеного часу відповідно до встановленого графіка. Графік сам по собі може бути гнучкий і визначатись перебігом подій, але залежність від зовнішньої ситуації жорстко задана в програмному комплексі. Типовим прикладом роботи AI в автоматичному режимі може служити перевірка кожного законопроекту на відповідність Конституції. Законопроекти поступають нерегулярно, але система в разі появи нового виконує належний набір операцій.

Навпаки, автоматизований режим є сенс використовувати для вирішення разових непередбачених проблем, коли виникає потреба поставити інформаційній системі нову задачу, не закладену в програмний комплекс. Причому в даному випадку AI може не лише виконувати заздалегідь відомі стандартні процедури, але й самостійно шукати метод вирішення, можливо, невідомий користувачам системи. Така ситуація може виникнути, наприклад, при необхідності визначити наявність складу злочину у випадку, коли причини і наслідки тих чи інших дій в складному конфлікті є неочевидними.

Отже, підсумовуючи сказане вище, на більш загальному рівні можемо сказати, що AI в автоматичному режимі в певному розумінні є суб'єктом процесу обробки інформації, а в автоматизованому режимі – інструментальним засобом людини. Тому, проектуючи нові інформаційні системи та використовуючи вже існуючі, ми повинні ясно розуміти, що саме і в який спосіб хочемо з їх допомогою отримати.

## Література

1. Реформа децентралізації.  
<https://www.kmu.gov.ua/diyalnist/reformi/efektivne-vryaduvannya/reforma-decentralizaciyi> (дата звернення 16.10.2025)
2. ЗАКОН УКРАЇНИ Про доступ до публічної інформації (Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314) URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text> (дата звернення 16.10.2025)
3. Цифрова трансформація. <https://www.kmu.gov.ua/diyalnist/mizhnarodna-dopomoga/coordination/cifrova-transformaciya> (дата звернення 16.10.2025)
4. Керівні принципи застосування штучного інтелекту в парламентах. Редактори Фотіос Фіціліс, Йорн фон Люке, Франклін де Врієзе. 2024. Вестмінстерська фундація за демократію URL: <https://www.wfd.org/sites/default/files/2025-04/wfd-ai-guidelines-for-parliaments-2024-ukrainian.pdf> (дата звернення 16.10.2025)
5. Брайчевський С. М. Інтелектуальні агенти в сфері парламентського контролю. "Інформація і право". 2023. 1(44). С. 25-31 URL: <https://ippi.org.ua/braichevskii-sm-intelektualni-agenti-v-sferi-parlamentskogo-kontrolyu-s-25-3> (дата звернення 16.10.2025).

**Леонов Б.Д.**

доктор юридичних наук, професор,  
професор кафедри права ПЗВО  
«Міжнародний класичний університет імені  
Пилипа Орлика»

ORCID: <https://orcid.org/0000-0002-2488-7377>

**Казьмірук С.Д.**

аспірант Державної наукової установи  
Інститут інформації, безпеки і права  
Національної академії правових наук України  
ORCID: <https://orcid.org/0000-0001-8101-732X>

## **ІННОВАЦІЙНІ ПІДХОДИ ЗАСТОСУВАННЯ ШІ ЯК ІНСТРУМЕНТУ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ**

В умовах зростання інформаційних загроз надзвичайної актуальності набуває питання запровадження інноваційних підходів і високотехнологічного інструментарію на основі штучного інтелекту (далі — ШІ; англ. artificial intelligence, AI) у різні сфери управлінської діяльності, однією з яких є парламентський контроль. Такі інструменти мають допомагати реалізації функції парламентського контролю, який покликаний забезпечити підзвітність органів виконавчої влади перед парламентом.

Слід зазначити, що ШІ нині відіграє важливу роль у суспільстві і має величезний потенціал в майбутньому [1, с.53]. Зокрема, в державному управлінні інтеграція ШІ здатна прискорювати аналіз нормативно-правових актів, підтримувати гармонізацію та переклад європейського законодавства, а також забезпечувати проведення цифрової експертизи регуляторних актів.

В контексті європейської та євроатлантичної інтеграції України довіра до державних інститутів є одним із ключових вимірів парламентського контролю і саме в цій площині інструменти ШІ можуть підвищити ефективність опрацювання отримуваної інформації про фактичне виконання службовими особами своїх обов'язків та перевірки роботи органів виконавчої влади з точки зору дотримання вимог законодавства.

Більшість парламентів провідних країн світу мають довгострокові цифрові стратегії з використанням хмарних сервісів і алгоритмів на базі ШІ, які зміцнюють довіру населення до наглядових та контрольних процедур. Жваве обговорення в ЄС викликала ініціатива Європейської Комісії щодо розгляду акта з правового регулювання суспільних відносин, пов'язаних зі ШІ [2, с. 39].

Аналіз зарубіжного досвіду у сфері парламентського контролю свідчить про тенденцію поєднання перевірених процедурних інструментів із інноваційними цифровими технологіями аналізу та обробки даних ШІ.

У провідних країнах світу інститути парламентського контролю трансформуються від суто процедурних механізмів: слухань під присягою, опрацювання документів, діяльності тимчасових слідчих комісій до інноваційної цифрової системи, яка поєднує аналітику даних, інструментарій ШІ, захищені канали для отримання важливої інформації, стандартизовані шлюзи приймання доказів, кіберзахищену ІТ інфраструктуру та краудсорсингові форми участі громадян [3].

Серед запроваджуваних у світі інноваційних інструментів парламентського контролю виділяються:

1) аналіз даних та аналітики в державному аудиті. Наприклад, у США Рахункова палата (GAO) розробила й застосовує ШІ Accountability Framework для перевірки державних ІТ-рішень. У Європейській рахунковій палаті (ECA) ухвалено AI-стратегію на 2024–2025 роки з дорожньою картою впровадження аналітики з ШІ;

2) захищені канали отримання відомостей як джерело інформації для парламентських розслідувань. Наприклад, Директива ЄС 2019/1937 зобов'язує створювати внутрішні та зовнішні канали повідомлень про порушення, гарантуючи конфіденційність;

3) цифрові шлюзи приймання доказів для комітетів, які уніфікують метадані, формати та режим конфіденційності, зменшуючи транзакційні витрати на опрацювання великих обсягів даних. Наприклад, у Палаті громад Великобританії офіційні настанови для подання письмових та усних доказів визначають стандарти щодо структури матеріалів, форматів файлів, обсягу та процедур розгляду;

4) цільові сервіси ШІ для парламентів, які пришвидшують обробку значних обсягів документації, транскрипцію та переклад засідань, класифікацію подань від громадян та громадських організацій;

5) кіберзахищеність парламентської й урядової інфраструктури як системна передумова контрольних функцій. Наприклад, для інституцій ЄС з 2024 р. діє Регламент 2023/2841, що встановлює вимоги до управління кіберризиками, обміну інформацією, реагування на кіберінциденти;

6) краудсорсингові системи контролю у вигляді електронних петицій і масових звернень допомагають визначати пріоритети контролю з урахуванням суспільного запиту. Наприклад, у Великобританії встановлено мінімальні межі петицій: після 10 тисяч підписів уряд надає відповідь, а після 100 тисяч – Петиційний комітет розглядає питання про парламентські дебати;

7) відкриті фінансові дані та інтерактивні моделі. Наприклад, у США офіційний портал містить стандартизовані масиви даних про видатки, гранти й позики, які використовують в своїй діяльності як аналітичні підрозділи парламентських комітетів, так і правоохоронні органи цієї країни.

Отже, інноваційні підходи застосування ШІ в контексті парламентського контролю підвищують прозорість і доказовість інформації, яка перевіряється, забезпечують мінімізацію ризиків отримання недостовірної інформації. Такі підходи сприяють трансформації контролю із площини припущень у площину аналізу достовірних даних.

Водночас, еволюція ШІ не підмінює існуючі форми парламентського контролю, однак істотно підсилює достовірність та якість висновків, насамперед у роботі профільних комітетів і тимчасових слідчих комісій.

З урахуванням викладеного, вважаємо, що застосування ШІ є виправданим і перспективним інноваційним інструментарієм парламентського контролю. Поєднання існуючих процедур із інноваційними підходами застосування ШІ як інструменту парламентського контролю формує його нову модель, здатну реагувати на сучасні виклики, покращити якість державного управління та зміцнити довіру громадян до інститутів представницької демократії.

### Список використаних джерел

1. Фурашев В.М., Корж І.Ф. Штучний інтелект та адміністративна (контрольна) діяльність публічної влади: європейський погляд. *Інформація і право*. 2025. №1(52)/2025. С. 51-61. URL: <http://il.ippi.org.ua/article/view/324667>
2. Пилипчук В. Г., Баранов О.А., Гиляка О. С. Проблема правового регулювання у сфері штучного інтелекту в контексті розвитку законодавства Європейського Союзу. *Вісник Національної академії правових наук України*. 2022. № 2. С. 36-62 URL: <https://visnyk.kh.ua/uk/journals/visnik-naprn-2-2022-r/problema-pravovogo-regulyuvannya-u-sferi-shtuchnogo-intelektu-v-konteksti-rozvitku-zakonodavstva-yevropeyskogo-soyuzu>
3. U.S. Government Accountability Office (GAO). Artificial Intelligence: тематичний розділ. URL: <https://www.gao.gov/artificial-intelligence>

**Ланде Д. В.**

доктор технічних наук, професор, керівник  
наукового центру Державної наукової  
установи «Інститут інформації, безпеки і  
права НАПрН України»

ORCID: <https://orcid.org/0000-0003-3945-1178>

**Фурашев В. М.**

кандидат технічних наук, доцент, с.н.с.,  
перший заступник директора Державної  
наукової установи «Інститут інформації,  
безпеки і права НАПрН України»

ORCID: <https://orcid.org/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.

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.

**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 ідей 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, ґрунтового 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., Страшної Л.Л. – Київ: ТОВ «Інжиніринг», 2025. 278 с.

2. Ланде Д.В., Фурашев В.М. 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).

**Казьмірук С.Д.**

аспірант Державної наукової установи

Інститут інформації, безпеки і права

Національної академії правових наук України

ORCID: <https://orcid.org/0000-0001-8101-732X>

## **ТРАНСФОРМАЦІЙНІ ПРОЦЕСИ ЗАСТОСУВАННЯ СИСТЕМ ДЕТЕКЦІЇ БРЕХНІ НА ОСНОВІ ШІ В АСПЕКТІ ПРАВОТВОРЧОЇ ДІЯЛЬНОСТІ ТА ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ**

В умовах ускладнення безпекового середовища та зростання інформаційних загроз особливого значення набувають трансформаційні процеси впровадження систем детекції брехні: комп'ютеризованих поліграфологічних систем (computerized polygraph systems) виявлення прихованої і недостовірної інформації (поліграфа), інноваційних технологій виявлення (детекції) брехні, які базуються на ШІ та кіберзахищеному програмному забезпеченні на основі ШІ (далі – ШІ, англ. – AI) у правотворчій діяльності і парламентський контроль. Нині такі системи мають слугувати інструментарієм парламентського нагляду для оперативного виявлення корупційних ризиків, проблем неефективного використання коштів та порушення законодавства. Відсутність єдиного інструментарію для виявлення прихованої і недостовірної інформації зумовлює постійний пошук нових ідей для вирішення цієї проблематики. Зокрема, у рамках європейської і євроатлантичної інтеграції України довіра до державних інститутів є одним із ключових аспектів забезпечення національної безпеки держави.

Необхідно зазначити, що ШІ нині відіграє важливу роль у суспільстві і має величезний потенціал в майбутньому. Завдяки своїм можливостям та потенціалу ШІ має значний вплив на технологічний прогрес у різних сферах життєдіяльності.

У майбутньому ШІ буде продовжувати вдосконалюватися і знаходити дедалі більше застосувань у нашому житті. Зокрема, інтеграція ШІ в державне управління допомагатиме аналізувати нормативно-правові акти та перекладатиме європейське законодавство. Дуже важливо, що завдяки ШІ-

інструментам робитиметься цифрова експертиза нормативно-правових актів. А надалі, ці рішення можна масштабувати для роботи уряду загалом [1].

Одним із ефективних напрямів виявлення ризиків корупції, неефективного використання коштів чи порушень законодавства через алгоритми ШІ - є застосування систем детекції брехні, які базуються на ШІ та кіберзахищеному програмному забезпеченні. Позитивний міжнародний досвід свідчить, що розвиток математичних алгоритмів систем детекції брехні на основі ШІ демонструє високу ефективність моделювання когнітивних функцій людини і ґрунтується на застосування інноваційних методів машинного навчання (machine learning).

Європейський Парламент також побіжно визначає, що характерним критерієм автономності робота та ШІ є здатність до самонавчання. Нині ми є свідками того, що наука і практика знаходиться на порозі створення роботів зі ШІ та системами самонавчання нового покоління. В цілому, як свідчить аналіз, у найближчій історичній перспективі постане вкрай актуальною проблема створення моделі правового регулювання розробки, впровадження і застосування роботів зі ШІ та можливостями для самонавчання [2].

Системи детекції брехні на основі ШІ являються інноваційним інструментарієм для адміністративного або кримінального розслідування, перевірки доброчесності персоналу, забезпечення кадрової і корпоративної безпеки, судово-психологічної експертизи та виявлення корупційних і фінансових ризиків. В контексті зазначеного перспективною є подальша системна інтеграція поліграфологічних систем (polygraph system), спеціальних методик (polygraph testing methods), кіберзахищеного програмного забезпечення (polygraph software) та ШІ.

Застосування систем детекції брехні згідно з міжнародними стандартами дозволить підвищити ефективність вирішення основних завдань в аспекті правотворчої діяльності та парламентського контролю:

- виявлення ризиків корупції, неефективного використання коштів чи порушень законодавства;
- підвищення ефективності проведення службових розслідувань (перевірок);
- забезпечення прозорості кадрової політики у разі прийняття на публічну службу;

- попередження інших ризиків, у процесі діяльності посадових і службових осіб.

Застосування ІІІ дозволить суспільству використати ІІІ для успішного вирішення повсякденних завдань і подальшого безпечного розвитку. При цьому розвиток систем детекції брехні з підтримкою ІІІ свідчить про нову еру застосування інноваційних систем виявлення прихованої і недостовірної інформації [3].

Отже, впровадження систем детекції брехні: комп'ютеризованих поліграфологічних систем (computerized polygraph systems) виявлення прихованої і недостовірної інформації (поліграфа), інноваційних технологій виявлення (детекції) брехні, які базуються на ІІІ та кіберзахищеному програмному забезпеченні у правотворчу діяльність і парламентський контроль сприятиме активізації європейської і євроатлантичної інтеграції України, відновленню довіри до державних інститутів, підвищенню ефективності виявлення ризиків корупції, неефективного використання коштів або порушень законодавства через алгоритми ІІІ.

На наше переконання, застосування систем детекції брехні на основі ІІІ є перспективним напрямом у сфері інформаційної безпеки, який підвищує якість, достовірність і об'єктивність парламентського контролю та слугує дієвим безпековим інструментом у процесах підготовки й проведення парламентських слухань.

### **Список використаних джерел**

1. Фурашев В.М., Корж І.Ф. Інформація і право. № 1(52)/2025. С. 53. Штучний інтелект та адміністративна (контрольна) діяльність публічної влади: європейський погляд. URL: <http://il.ippi.org.ua/article/view/324667>

2. Пилипчук В. Г., Баранов О.А., Гиляка О. С. Вісник НАПрНУ № 2, 2022 р С. 52. Проблема правового регулювання у сфері штучного інтелекту в контексті розвитку законодавства європейського союзу. URL: <https://visnyk.kh.ua/uk/journals/visnik-naprn-2-2022-r/problema-pravovogo-regulyuvannya-u-sferi-shtuchnogo-intelektu-v-konteksti-rozvitku-zakonodavstva-yevropeyskogo-soyuzu>

3. Oravec, Jo Ann. "From Polygraphs to Truth Machines: Artificial Intelligence in Lie Detection." Critical Humanities 2, 2 (2024). URL: С. 5 <https://mds.marshall.edu/cgi/viewcontent.cgi?article=1036&context=criticalhumanities>.

**Доронін І.М.**

доктор юридичних наук, доцент, керівник  
наукового центру Державної наукової  
установи «Інститут інформації, безпеки і  
права НАПрН України»

ORCID: <https://orcid.org/0000-0002-5991-6713>.

## **НЕБЕЗПЕКА ВИКРИВЛЕННЯ ІНФОРМАЦІЇ В АСПЕКТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ**

Проблема політики протидії викривленню інформації, а також іншого деструктивного поведіння з інформацією, що негативно впливає на належність її отримання, традиційно розглядається в аспекті «протидії дезінформації». Зазначений підхід був в основі впровадження в державну політику різного рівня, що втілювався в обмежуючих заходах, які дозволили поставити питання про відродження цензури в медіа.

У той же час в тіні залишались інші напрями та способи викривлення інформації. Мова йде про інші способи спотворення інформації (*distorting information*).

Як правило, у цьому аспекті розглядають «мізінформацію» (*misinformation*), що у двох словах може бути описана як «ненавмисна неправда». Цей термін охоплює доволі широкий обсяг можливих ситуацій, коли мова йде про розповсюдження інформації коли перший отримувач ненавмисно сприйняв її зміст, коли інформація розповсюджувалась зі змішуванням суті та коментарів; роздільне поширення інформаційного контенту (наприклад, окремо зображення від його пояснення); «хибний зв'язок» (мова йде про невідповідність заголовку змісту повідомлення, що спочатку проявлялось в англійських ЗМІ з їх манерою подання заголовків); сатира або гумор, які неточно сприйняті адресатами (проблема «старих першоквітневих жартів»), будь-які технічні, мовні, перекладацькі та інші помилки. У цих ситуаціях перший розповсюджувач та інші розповсюджувачі не знають щодо її неправдивості і здійснюють розповсюдження хибної інформації ненавмисно. Але негативний вплив на суспільну свідомість ідентичний дезінформації.

Іншим способом є «мелінформація» (malinformation), що у вітчизняній літературі прямо ототожнюється з дезінформацією. Хоча в даному випадку ситуація більш складна, оскільки цей вид спотворення інформації пов'язаний з явищами переміщення приватної інформації в публічну сферу або ж викидання її з контексту. Таке переміщення може проводитись зі свідомо дезінформаційною метою, або ж робитись в іншому контексті, а потім розповсюджуватись каналами ненавмисної хибної інформації. Значна кількість скандальної інформації навколо об'єктів великої суспільної уваги на кшталт британської королівської родини або скандально відомих осіб зі світу поп-музики чи кіно є проявом цього способу спотворення інформації.

Досить подібним до дезінформації є «інформаційне маніпулювання», тактика якого передбачає як спотворення власне інформації, так і встановлення контролю потоку та сприйняття інформації. У цьому аспекті найбільш часто вживають заходи пропаганди (як частини власне пропаганди, тобто інформації особливо упередженого або оманливого характеру, що використовується для просування або оприлюднення певної політики чи точки зору); маніпуляцію контенту (від обрізки відео-, фотоматеріалів, їх редагуванні, підміні вихідних даних і закінчуючи побудовою «діп фейків» як крайнього втілення і дезінформації, і маніпуляції), «імпостер» (використання брендів інших ЗМІ чи створення їх аналогів), «перекручування» (spin) як складний процес спотворення змісту інформації зі збереженням її зовнішньої суті; затоплення інформаційного простору (flooding), що полягає у перевантаженні адресата численними суперечливими версіями однієї й тієї ж події з метою посіяти загальну недовіру, плутанину та апатію; «астротурфінг» (astroturfing) створення хибного враження широкої, спонтанної народної підтримки політики, продукту чи справи шляхом координації фальшивих онлайн-ідентичностей (ботів) або платних коментаторів; а також вибіркова цензура та зловживання обмежувальними заходами в рамках політики чи законодавчого регулювання.

Оскільки найбільш вразливою, за умови відсутності надзвичайних подій, аудиторія стає під час виборчого процесу, в ЄС заходи протидії дезінформації та іншим проявам спотворення інформації розглядались як складова політики протидії іноземному маніпулюванню інформацією та втручанню (Foreign Information Manipulation and Interference (FIMI). Загалом

підхід був викликаний необхідністю застосування заходів в інтересах національної безпеки з метою унеможливлення впливу іноземних держав на результати виборів. У цьому контексті було ухвалено низку законодавчих актів (Digital Services Act (DSA) з досить широким охопленням сфер застосування та окрема частина EU Artificial Intelligence Act. Також вироблені окремі напрями для залучення елементів саморегуляції та со-регуляції приватного бізнесу.

Але якщо у випадку протидії чітко визначеному іноземному втручанням зазначені заходи мали певний ефект, то у випадках із дезінформаційною діяльністю внутрішніх учасників (політичних партій, корпорацій і т. ін.) використання таких засобів створювало постійні загрози для порушення прав людини у сфері медіа, зокрема, права на свободу слова та вільний обіг інформації. Окрім цього у випадках з спотворенням інформації не у контексті заходів з іноземного втручання загальні напрями політики були менш ефективними. У питаннях суспільної реакції на епідеміологічні заходи у період пандемії COVID-19 окремі напрями протидії, навпаки, підживлювали опозиційні настрої та суспільне невдоволення, що сприяло зросту політичного популізму в багатьох країнах ЄС.

При застосуванні систем штучного інтелекту в парламентському контролі досить важливою проблемою є вжиття належних заходів протидії спотворенню інформації не у контексті протидії іноземному втручання чи політичної пропаганди на шкоду національним інтересам. Загальний підхід до застосування ШІ в парламентському контролі полягає у визначенні поля для використання цієї технології в межах відповідних завдань парламенту. У Керівних принципах застосування штучного інтелекту в парламентах (Вестмінстерські принципи) визначені наступні напрями для парламентського контролю: аналіз матеріалів ЗМІ про діяльність парламенту; - аналіз даних соціальних мереж щодо діяльності парламенту; - виявлення маніпуляцій в інформаційному середовищі; - заходи зі зменшення упередженості / дискримінації в пропозиціях на основі ШІ для їх ліквідації [1]. Але, на нашу думку, цей документ, що підготовлений фахівцями недержавної організації Вестмінстерською фундацією за демократію (WFD) містить вельми обмежений підхід до напрямів парламентського контролю. Серед зазначених напрямів практичними фахівцями запропоновано

спрямування сфери застосування до питань автоматизації моніторингу та аналізу інформації, створення нових інструментів для аналізу даних, що надаватимуть змогу виявляти приховані тенденції та закономірності; підтримки інновацій у сфері парламентського контролю, а також виконання допоміжних функцій спілкування з громадянами (асистенти, чат-боти) і т. ін. [2, с. 195].

З урахуванням сприйняття способів спотворення інформації можливо констатувати певну обережність у застосуванні систем ШІ навіть у випадках аналізу інформації, оскільки основні на сьогодні інструменти у вигляді великих мовних моделей (LLM) не виключають надання неправдивої інформації, не кажучи про інші випадки її спотворення [3, 4, 5]. Існуючий в законодавстві ЄС (та меншою мірою – США) підхід до необхідності відображення окремих політик («подолання упередженості», «боротьба з дискримінацією», «чутливий контент», «забезпечення різноманітності») зумовлює і можливу неправдивість інформації, оскільки така політика загалом може бути сприйнята як засіб маніпуляції інформацією. У випадку з використанням «нецензурованих» LLM, щодо яких спостерігається зростання інтересу, то в цих випадках ризик розповсюдження спотвореної інформації важко визначити взагалі.

Таким чином варто констатувати, що найбільш складною проблемою та викликом для застосування технології ШІ у вигляді LLM у заходах парламентського контролю є спотворення інформації, що є перепорою як до застосування найбільш відомих LLM так і «нецензурованих» та вільних моделей. Саме з урахуванням таких викликів мають вироблятися напрями використання технологій ШІ у парламентському контролі.

### **Список використаних джерел**

1. Керівні принципи застосування штучного інтелекту в парламентах. 2024. URL: <https://www.wfd.org/sites/default/files/2025-04/wfd-ai-guidelines-for-parliaments-2024-ukrainian.pdf>
2. Ланде Д.В., Фурашев В.М. Парламентський контроль із застосуванням генеративного штучного інтелекту : монографія. Київ: ТОВ «Інжиніринг», 2023. 202 с.
3. Zhou, Jiawei & Zhang, Yixuan & Luo, Qianni & Parker, Andrea & Choudhury, Munmun. (2023). Synthetic Lies: Understanding AI-Generated Misinformation and

Evaluating Algorithmic and Human Solutions// CHI Conference on Human Factors in Computing Systems. Hamburg, Germany. 2023, April. DOI:10.1145/3544548.3581318

4. Pat Pataranutaporn, Chayapatr Archiwaranguprok, Samantha W. T. Chan, Elizabeth Loftus, and Pattie Maes. 2025. Slip Through the Chat: Subtle Injection of False Information in LLM Chatbot Conversations Increases False Memory Formation// Proceedings of the 30th International Conference on Intelligent User Interfaces (IUI '25). Association for Computing Machinery, New York, NY, USA, 1297–1313. <https://doi.org/10.1145/3708359.3712112>

5. Cheong, Inyoung, Epistemic and Emotional Harms of Generative AI: Towards Human-Centered First Amendment (September 02, 2025). Available at SSRN: <https://ssrn.com/abstract=5435335> or <http://dx.doi.org/10.2139/ssrn.543535>

6. Ahmed M., Knockel J. Extended Abstract: The Impact of Online Censorship on LLMs// Free and Open Communications on the Internet 2024 (2). URL: <https://petsymposium.org/foci/2024/foci-2024-0006.php>

**Ланде Д. В.**

доктор технічних наук, професор,  
керівник наукового центру Державної  
наукової установи «Інститут інформації,  
безпеки і права НАПрН України»  
ORCID: <https://orcid.org/0000-0003-3945-1178>

**Даник Ю. Г.**

доктор технічних наук, професор,  
професор НН ФТІ КПІ ім. Ігоря Сікорського  
ORCID: <https://orcid.org/0000-0001-6990-8656>

## **ЗМАГАЛЬНИЙ ШТУЧНИЙ ІНТЕЛЕКТ В ПРАВОВІЙ СФЕРІ**

У сучасних умовах цифрові технології, і зокрема штучний інтелект (ШІ), все глибше інтегруються в правову сферу – від підготовки законопроектів 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 законопроектів. 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.

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.

Змагальний ІІІ в правовій сфері проявляється у трьох основних напрямках:

**Генерація та детекція правової дезінформації.** Великі мовні моделі (LLM) здатні створювати правдоподібні, але фейкові законопроекти, 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, ЗІІІ 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.** ЗІІІ 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 ІІІ.** Серед найбільш небезпечних інструментів ЗІІІ 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 законопроект, 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. Ланде Д.В., Фурашев В.М. Парламентський контроль із застосуванням генеративного штучного інтелекту : монографія. 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.

**Засць Д.Г.**

аспірант Державної наукової установи

«Інститут інформації безпеки і права НАПрН  
України»

ORCID: <https://orcid.org/0009 0003 1502 9439>

## **ІНФОРМАЦІЙНО-ПРАВОВА ПОЛІТИКА [ПРОЗОРОСТІ] ЛОБІЮВАННЯ В УКРАЇНІ**

Інформаційно-правова політика держави в умовах розвинутого інформаційного суспільства є ключовим механізмом забезпеченням демократії через нормативне забезпечення прозорості всіх процесів взаємодії народу і влади, адже принциповими характеристиками управління «сьогодні визнаються такі їх особливості: керуючі впливи обов'язково цілеспрямовані, мають інформаційний характер і здійснюються за схемою зворотного зв'язку» [1, с. 26], а також ті, які вперше виникають в полі правового регулювання. Таким принципам прозорості повною мірою мають піддаватися всі процеси лобіювання, встановлені Законом «Про лобіювання» [2].

Саме для лобіювання прозорість необхідна критично: лобіювання, у разі закритості і відсутності прозорості, як процес взаємодії з владою, несе колосальні корупційні ризики, адже «таємниці лобі відомі лише обізнаним, - писав у 1845 р. писав прем'єр міністр Великої Британії В. Дізраелі, - Тільки потім вони повідомляються всім іншим» [3, р. 376]. А в сучасному світі це неможливо і недопустимо.

Оскільки лобіювання є одним з різновидів комунікації з владою, правове регулювання якої спрямовано на відкритість і прозорість такої комунікації та фінансування її, самий факт прийняття Закону України «Про лобіювання» вже є величезним кроком на шляху інформаційно-правової політики в цій площині.

Водночас, орієнтований виключно на регулювання консалтингового (комерційного) лобіювання Закон певною мірою не відображає соціальних очікувань щодо прозорості, оскільки:

1) не передбачає всіх наявних форм лобіювання, яке безпосереднього так і опосередкованого, що виводить з кола необхідної

прозорості таких учасників лобістських процесів як профспілки та громадські організації;

2) частково нівелює саму сутність лобіювання, подаючи її як суто професійну діяльність консалтингових лобістів, внаслідок чого втрачається гарантоване право всіх решти, крім консалтингових лобістів, на впорядковану лобістську діяльність.

Такі недоліки Закону можуть усунути наступні рішення, насамперед, інформаційно-правової політики. Так, правова політика лобіювання може :

1) відкоригувати розуміння лобіювання як впорядковану комунікацію між громадянським суспільством та бізнесом з суб'єктами правотворчої діяльності;

2) комерційну лобістську діяльність розуміти як професійну діяльність з лобіювання, яка існує поряд з лобістською діяльністю інститутів громадянського суспільства;

3) визначити реальне коло суб'єктів лобіювання і включити їх всіх до такого кола на законодавчому рівні, визначити їхні прав та обов'язки;

4) точно визначити предмет комунікації лобіювання;

5) поширити дію Реєстру прозорості на інституті громадянського суспільства, котрі займаються лобіюванням;

6) сформулювати повноваження НАЗК щодо контролю за лобістською діяльністю та прозорістю лобістських комунікацій, передбачивши відповідні повноваження:

- щодо забезпечення контролю за лобістською діяльністю в цілому на рівні ст. 11 Закону України «Про запобігання корупції»;

- щодо забезпечення прозорості лобістської комунікації – на рівні Закону України «Про лобіювання».

Вказані побажання стосуються правової політики в цілому, але й мають розподілятися на основні рівні відповідної політики і діяти в конкретно визначених напрямках на кожному з рівнів.

Сутність інформаційно-правової політики, як наряду правової політики держави, сьогодні розглядається «через програму діяльності щодо правового забезпечення всього спектру соціальних реформ, стабільності та правопорядку в країні, шляхом застосування основних положень

інформаційної культури суб'єктами усіх рівнів для забезпечення переходу до інформаційного суспільства» [4, с. 146].

В. М. Брижко під інформаційними відносинами розуміє відносини, що виникають у всіх сферах життя і діяльності людини, суспільства та держави при одержанні, використанні, поширенні й зберіганні інформації (тобто, в інформаційному процесі [5, с. 86].

Досліджуючи зміст інформаційної політики, Г. Красноступ вказує: «державна інформаційна політика забезпечується за допомогою дій, які за сутністю є комплексом цілеспрямованих організаційних і правових заходів, що впливають на об'єкт управління (певний державний інтерес), у результаті чого досягається необхідний для суспільства результат» [6]. І на це мають спрямовуватися дії влади, про це вказували науковці дослідники інформаційної політики постійно. Так, ще у 2000 р. І. Арістова підкреслювала: «першочергову увагу органи державної влада, політичні об'єднання і наукова громадськість повинні звернути до вирішення проблеми розвитку концептуальних основ державної інформаційної політики і формування інформаційного законодавства України з урахуванням основних особливостей сучасного розвитку української державності» [1, с. 334].

Оскільки «єдине, що тримало лобіювання як би поза політичної системи - це відсутність його правового регулювання» [7, с. 21], відповідно включення його в правове поле є, навпаки, підтвердженням ваги впорядкування такого інституту, його позитивного значення, та виведення його «з тіні на світло», мінімізуючи ризики політичної корупції.

І таке включення на рівні всіх рівнів інформаційної політики, як справедливо наголошує І. Арістова, має бути орієнтоване на світовий досвід, та, зокрема, досвід країн Європи [1, с. 117]. А як зазначає Н. Савінова, рівні правової політики «доцільно поділяти на доктринальний, концептуальний, законодавчий, правозастосувальний, правовиконавчий та науковий» [8, с. 168]. Такий детальний поділ, хоча і обґрунтовано визначений, викликає надто кропіткої роботи при розробці політики в реаліях, з урахуванням необхідності проходження всіх рівнів правової політики: від аналізу доктрини до наукового аналізу, зокрема, ефективності відповідного правового регулювання. Дійсно, така детальна градація рівнів більше важлива для наукового аналізу, дійсно, ефективності правової політики за

певними напрямками. Правозастосувальний та правовиконавчий рівні правової політики, про які пише Н. Савінова, в умовах тотожності застосування доцільно поєднувати в межах одного рівня з більш широким визначенням – правозастосовного, оскільки правовиконавчий рівень є його складовою.

Таким чином, резюмуючи вказані підходи, визначимо рівні інформаційно-правової політики за аналогією з рівнями правової політики в цілому як: доктринальний; концептуальний; законодавчий; правозастосовчий; науковий (експертний).

*Рівні інформаційно-правової політики прозорості лобістських комунікацій, за аналогією з рівнями правової політики, в цілому слід визначати як :*

*1) Доктринальний – рівень розуміння міжнародною та національною доктриною права та сталою практикою регулювання прозорості лобістських комунікацій в демократичній державі;*

*2) Концептуальний – рівень сприйняття політичною владою та правотворцем сутності доктринального розуміння відповідної політики і формування відповідного власного та колективного уявлення про її сутність;*

*3) Законодавчий – рівень на якому відбувається відбиття концептуального рівня на рівні законодавства;*

*4) Правозастосовчий – рівень відповідної правової політики, на якому здійснюється реалізація (застосування) описаних в законодавстві механізмів здійснення відповідних правовідносин;*

*5) Науковий (експертний) – рівень, на якому здійснюється експертна діяльність: спостереження та оцінка поточного стану реалізації відповідної правової політики, прогноз та проектування перспектив подальшої дії відповідної політики, розробляються рекомендації щодо покращення дії відповідної політики в цілому, або о окремих її рівнів, а також зміни напрямів відповідної політики чи припинення її взагалі.*

### **Список використаних джерел**

1. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти/ За загальною редакцією д-ра юрид. наук, проф. Бандурки О.М...: Монографія. – Харків: Вид-во Ун-ту внутр. Справ, 2000. – 368 с.

2. Закон України «Про лобіювання» від 23 лютого 2024 року № 3606-IX. Відомості Верховної Ради (ВВР), 2024, № 18, ст.77. URL: <https://zakon.rada.gov.ua/laws/show/3606-20#Text>
3. The Oxford English dictionary. Being a corrected re-issue with an introduction, supplement and bibliography of a new English dictionary on historical principles / [ed. by James A. H. Murray, Henry Bradley, W. A. Craigie, C. T. Onions]. – Vol. VI. – Oxford : Clarendon Press, 1970. – 820 p.
4. Бориславська О.М. Теоретико-методологічна ідентифікація поняття «інформаційно-правова політика». Порівняльно-аналітичне право. № 3 2015. С. 144-146. С. 146
5. Брижко В.М. Інформаційне суспільство. Дефініції. За ред. Р.А. Калюжного, М.Я. Швеця. Київ: Інтеграл, 2002.
6. Красноступ Г.М. Основні напрями правового забезпечення державної інформаційної політики. Офіційний веб-сайт Міністерства юстиції України. URL: : <http://old.minjust.gov.ua/30768>
7. Годний С.П. Лобіювання як засіб реалізації політичних інтересів. Innovative Solutions in Modern Science. 2017. № 1(10). С. 19-25.
8. Савінова Н.А. Кримінально-правова політика забезпечення інформаційного суспільства в Україні. Дис. докт. юрид. наук.: 12.00.08. Львів, 2013 р. 506 с.

**Лихоступ С.В.**

кандидат економічних наук, старший  
науковий співробітник, провідний науковий  
співробітник Державної наукової установи  
«Інститут інформації, безпеки і права НАПрН  
України»

**Мороз А.О.**

головний програміст відділу розробки та  
підтримки програмного забезпечення  
державне підприємство "Інформаційні судові  
системи"

## **ВПЛИВ СОЦІАЛЬНИХ І ПОЛІТИЧНИХ ВІДНОСИН В СУСПІЛЬСТВІ НА ПРОЦЕСИ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ ЗАКОНОДАВЧОЇ ДІЯЛЬНОСТІ**

Верховна Рада України, як єдиний законодавчий орган відповідно до своїх основних конституційних повноважень визначених статтею 85 Конституції України, постійно здійснює парламентський контроль за забезпеченням прав, свобод, обов'язків громадян, за виконанням Державного бюджету, за діяльністю органів виконавчої влади.

Парламент України є представником громадянського суспільства і від всього імені народу України контролює питання використання бюджетних коштів, дотримання законів, ефективності роботи міністерств та інших відомств. Громадянське суспільство в Україні включає мережу незалежних від держави інституцій, об'єднань та організацій і характеризується відповідними соціальними та політичними відносинами. Соціальні відносини передбачають комунікацію та співпрацю, а з іншого боку, і як наслідки цих процесів, політичні відносини виникають у процесі діяльності окремих груп соціальних структур, що визначають головні тенденції в питаннях політичної влади, її розподілу та використання в інтересах різних соціальних груп.

Важливу роль в забезпеченні парламентського контролю в формуванні законодавчого процесу відіграє саме громадянське суспільство. До його характерних рис відноситься : лобіювання ; суспільний тиск ; політична воля;

соціальна структура; політична культура; баланс політичних сил; механізми стримувань і противаг; консолідація опозиції тощо. Всі процеси, які торкаються громадянського суспільства в Україні, носять динамічний характер і являють собою справжній виклик ефективному парламентському контролю. А тому реалізація парламентського контролю Верховною Радою України спирається на розгалужену законодавчу базу і в першу чергу це 17 Законів України. А саме: основний Закон України - Конституція України; Закон України "Про регламент Верховної Ради України"; Закон України "Про статус народного депутата"; Закон України "Про Комітети Верховної Ради України"; Закон України "Про тимчасові слідчі комісії і тимчасові спеціальні комісії Верховної Ради України"; Закон України "Про уповноваженого Верховної Ради України з прав людини"; Закон України "Про Рахункову палату"; Закон України "Про державне бюро розслідувань"; Закон України "Про службу безпеки України"; Закон України "Про прокуратуру"; Закон України "Про державну прикордонну службу України"; Закон України "Про антитерористичний комітет"; Закон України "Про Національну Раду України з питань телебачення і радіомовлення"; Закон України "Про Кабінет Міністрів"; Бюджетний кодекс України; Закон України "Про Фонд державного майна України".

На даний час в Україні існують ряд науково-обґрунтованих і затверджених правил, які б визначали конструктивність інструментів здійснення парламентського, але насправді такий контроль не існує. Парламент України має власні традиції та практику здійснення нагляду. Проте, депутати ґрунтують свої дії на тому що, заходи зі здійснення парламентського контролю насамперед мають покращити систему державного урядування. А тому, і в цілому, Верховна Рада України здійснює парламентський контроль у різних організаційно-правових формах, але тільки у межах, визначених Конституцією України.

Діючі в Україні закони мають значний вплив на повсякденне життя, на права та добробут кожної людини, і саме якість цих законів ґрунтується і нерозривно пов'язана з процесом, який зумовив їх ухвалення. Зазвичай Верховна Рада ухвалює закони у відповідь на суспільні потреби чи проблеми, на виконання міжнародних зобов'язань тощо. Внаслідок цього основні принципи процесу розробки законів визначено в Конституції України

включаючи повноваження уряду, парламенту та повний перелік тих, хто має право на законодавчу ініціативу (органи влади, суспільство, громадяни).

В основному закони розробляє як виконавча влада так і парламент, але члени парламенту відіграють значну роль у процесі розгляду цих законів. Верховна Рада України здійснює контроль за тим, щоб ці закони не залишалися на папері, а були втілені в життя. Особливістю соціальних і правових відносин є право громадянського суспільства бути повністю обізнаними щодо широкого кола питань суспільно політичного життя країни. Парламентарі постійно спілкуються з населенням і дізнаються про громадську думку, на що спирається парламент і здійснює заходи щодо підвищення зацікавленості громадян у своїй діяльності так, щоб інтереси громадянського суспільства були відображені у законах та політиці.

Процес законодавчої діяльності та здійснення парламентського контролю в значній мірі спираються на соціальні та політичні відносини в суспільстві, як на стійку взаємодію між людьми та групами, які формують структуру суспільства, а також взаємозв'язки в рамках держави, що регулюються політичними інститутами. Соціальні відносини охоплюють взаємодію в спільнотах, політичні відносини стосуються управління, влади та прийняття рішень у суспільстві. Такі ж соціальні відносини складаються з соціальних організацій, інститутів, груп (наприклад, професійних, вікових) та спільнот (наприклад, етнічних) і формують соціальну структуру суспільства та забезпечують його функціонування.

Політичні відносини базуються на динамічних процесах в розвитку соціальної системи, елементами якої є державні та недержавні інститути: політичні партії, державні органи, громадські організації. Соціальні та політичні відносини нерозривно пов'язані. Особливістю суспільно-політичної ситуації в Україні на сучасному етапі є таке становище, коли не громадянське суспільство виступає фундатором правової держави, а сама держава повинна стати інструментом власної трансформації та формування громадянського суспільства.

В цій ситуації виникає необхідність функціонування системи управління за допомогою урядових та неурядових організацій, об'єднаних в політичну мережу - це поняття об'єднує механізми, процеси та інститути, через які громадяни та групи висловлюють свої інтереси, реалізують законні

права, виконують обов'язки, та балансують між розбіжностями. Характерними ознаками процесу такого управління є: участь (всі громадяни мають право голосу в прийнятті рішень прямо або при посередництві політичних інститутів, що представляють їх інтереси); верховенство права (чіткість та об'єктивність правових структур, особливо тих, що захищають права людини); прозорість (свобода інформації, її повнота та доступність для всіх, хто в ній зацікавлений); чутливість (усі інститути чітко реагують на потреби громадян); результативність та дієвість (максимально ефективно використання ресурсів для задоволення потреб громадян); підзвітність (уряд, приватний бізнес та структури громадянського суспільства підзвітні громадськості та інституційним носіям прав); стратегічне бачення (лідери та громадськість виходять з довгострокових перспектив управління та розвитку особистості, та чітко визначають ті заходи, які необхідні для їх реалізації).

В такій ситуації парламентський контроль відіграє важливу функцію демократії, яка передбачає участь народу в публічному управлінні державою, що гарантує взаємодію між політичною системою, державним сектором, співвідношення державних, муніципальних та народних інтересів, залучає суспільство до контролю всіх органів державної влади. Але посилення парламентського контролю потребує запровадження ряду заходів, що призведуть до:

- широкої взаємодії з організаціями громадянського суспільства, що представляють інтереси груп населення недостатньо представленими (молодь, літні люди, люди з інвалідністю, меншини тощо), з метою врахування аспектів та факторів різноманітності;

- створення механізмів регулярного діалогу з організаціями громадянського суспільства на різних рівнях влади за допомогою регулярних обговорень, консультативних органів - громадських рад, робочих груп створених на основі публічного, прозорого, відкритого та конкурентного відбору по визначеним критеріям;

- створення механізмів консультацій з громадськістю для груп громадянського суспільства, які не можуть бути представлені в регулярних обговореннях;

- широкого залучення, заохочення, підтримки надання гарантій щодо не перешкоджання та неправомірного обмеження організацій

громадянського суспільства або окремих осіб для внесення пропозицій під час публічних консультацій;

- використання сучасних інформаційних технологій з метою підвищення цілеспрямованостей політичних консультацій з дотриманням вимог щодо доступності веб- контенту;

- запобігання ризиків цифрової нерівності шляхом залучення друкованих ЗМІ, радіо та телебачення.

Функціонування відзначених вище процесів взаємного впливу соціальних і політичних відносин суспільства призведе до дієвих та ефективних наслідків парламентського контролю законодавчої діяльності.

### **Список використаних джерел**

1. Пустовіт Ж. М. Поняття, сутність та зміст функцій Верховної Ради України. [Електронний ресурс]. Режим доступу: [file:///C:/Users/User/Downloads/bmju\\_2012\\_11\\_5.pdf](file:///C:/Users/User/Downloads/bmju_2012_11_5.pdf)

2. Публічна політика в процесах реформування системи державного управління України / С. О. Телешун, С. В. Ситник, І. В. Рейтерович, О. Г. Пухкал. К. : НАДУ, 2016. 192 с.

3. Соціальна і гуманітарна політика : підручник / [авт. кол. : В.П. Трощинський, В.А. Скуратівський, М.В. Кравченко та ін.] ; за заг. ред. Ю.В. Ковбасюка, В.П. Трощинського. К. : НАДУ, 2016. 792 с.

4. Бойко Н. Інтернет як ресурс впливу громадян на владу в сучасному українському суспільстві. *Українське суспільство 1992–2013. Стан та динаміка змін. Соціологічний моніторинг*. К.: Інститут соціології НАН України, 2013. С. 375–381.

5. Журавльова Г. С. Форми та механізми парламентського контролю. *Вісник Центральної виборчої комісії*. 2007. № 1 (7). С. 51-55.

6. Щедрова Г. Політична конкуренція еліт у сучасній Україні : Монографія. Дніпро, 2016. 390 с.

7. Бойчук, М. А. Влада і громадянське суспільство: механізми взаємодії. К. : ТОВ «Атлант ЮЕмСі», 2006. 207 с.

8. Берназюк А.І. Парламентський контроль за реалізацією стратегічних актів. *Підприємництво, господарство і право. Конституційне право*. 2017. № 6. С.153-156.

9. Бондаренко В. А., Пустова Н. О. Парламентський контроль у системі державного контролю. *Науковий вісник Львівського державного університету внутрішніх справ*. Вип. 1. 2017. С. 159-171.
10. Аналіз державної політики та прийняття рішень парламентом України у здійсненні конституційних функцій: Посібник / В.А. Гошовська, П.В. Мироненко, М.М. Газізов, О.З. Босак. К. : НАДУ, 2010. 88 с.
11. Газізов М.М. Організаційно-правове регулювання лобістської діяльності в органах представницької влади [Електронний ресурс]. Режим доступу: [www.politika.cn.ua](http://www.politika.cn.ua). Експертна думка, 2010.
12. Куракін О. М. Парламентський контроль: характеристика національної моделі. *Науковий вісник Запорізького юрид. ін-ту*. 2010. № 2. С. 3-10.

**Дубняк М.**

кандидат юридичних наук, завідувач наукової лабораторії проблем штучного інтелекту і права Державної наукової установи «Інститут інформації, безпеки і права НАПрН України»  
ORCID: <https://orcid.org/0000-0001-7281-6568>

## **ШТУЧНИЙ ІНТЕЛЕКТ У ПУБЛІЧНОМУ АДМІНІСТРУВАННІ: МІЖНАРОДНИЙ ДОСВІД**

Відповідальне впровадження технологій штучного інтелекту (ШІ) має потенціал суттєво підвищити ефективність функціонування органів державної влади.

**По-перше**, застосування ШІ здатне забезпечити підвищення ефективності внутрішніх процедур шляхом автоматизації складних і повторюваних дій службовців, вивільненню їхнього часу для вирішення аналітичних і стратегічних завдань.

**По-друге**, ШІ може сприяти інклюзивності розробки окремих рішень. Використання великих масивів даних дозволяє виявити чутливі потреби громадян і закономірності розвитку місцевих спільнот.

**По-третє**, ШІ може посилити підзвітність уряду, розширюючи можливості органів державної влади та незалежних інституцій у сфері моніторингу, аудиту та контролю. Наприклад, алгоритмічні системи дедалі частіше застосовуються у сферах державних закупівель, управління бюджетними витратами, адміністрування грантів, соціальних виплат і програм субсидій. Так, «*Transport Canada*» впровадила алгоритм оцінки ризиків для виявлення потенційно небезпечних вантажів ще до їх завантаження на авіарейси [1].

Крім того, використання ШІ здатне підвищити швидкість і точність реагування урядових структур на суспільні потреби, забезпечуючи надання проактивних, персоналізованих і людиноцентричних послуг [2, с.3]. Під час пандемії COVID-19 у Норвегії Адміністрація праці та соціального забезпечення застосувала розмовного агента *Frida*, який дозволив

громадянам цілодобово отримувати консультації та соціальні виплати, автоматизувавши близько 80 % запитів без залучення службовців [3].

Разом із тим, зростає занепокоєння щодо ризиків фрагментарного або некерованого впровадження ШІ у державному секторі. Серед ключових викликів: 1. посилення алгоритмічної упередженості, 2. відсутність прозорості у розробленні систем ШІ, 3. порушення конфіденційності й безпеки даних.

Такі ризики можуть призводити до несправедливих або дискримінаційних результатів, що матимуть значні соціальні наслідки.

Ефективне впровадження штучного інтелекту (ШІ) у діяльність органів публічної адміністрації потребує не лише технологічних інновацій, а й розбудови системи постійного моніторингу, оцінювання та демократичного контролю. Відповідальне використання ШІ передбачає не тільки підвищення результативності управління, а й недопущення ризиків у процесах автоматизованого прийняття рішень.

Аналіз міжнародної практики показав, декілька основних напрямків впровадження ШІ в діяльність публічної адміністрації, зокрема це: моніторинг та оцінювання впливу ШІ; практики розвитку екосистем державних даних для прийняття рішень; посилення ролі неурядових органів (прокуратура, суди, громадські організації) для здійснення контролю за практиками впровадження ШІ в діяльність публічної адміністрації; запровадження політик звітування (виконання вимог прозорості) органами публічної адміністрації про результати використання ШІ у звітному періоді.

Ключовим напрямом сучасної політики у сфері цифрового врядування є системний моніторинг використання ШІ для оцінки того, чи підвищується якість державних послуг, чи вдосконалюються процеси ухвалення рішень і чи зростає ефективність управлінських процесів. На глобальному рівні важливу роль у цьому відіграє *Моніторинг інцидентів зі штучним інтелектом* (AI Incidents Monitor, AIM), створений Організацією економічного співробітництва та розвитку (ОЕСР). Цей інструмент забезпечує збирання та аналіз даних про інциденти, ризики та шкоду, пов'язану із застосуванням ШІ у різних секторах, включаючи державний. Його метою є підвищення обізнаності політиків, розробників та експертів

про потенційні системні загрози, що дозволяє формувати більш збалансовані підходи до регулювання й впровадження технологій [4].

На національному та місцевому рівнях уряди також розвивають практики обробки **даних для прийняття рішень**, інтегруючи інструменти ШІ у системи моніторингу суспільних процесів. Так, муніципалітет *Неймеген* (Нідерланди) застосовує алгоритми комп'ютерного зору для підрахунку кількості людей у різних частинах міста. Отримані дані використовуються для аналізу транспортних потоків і рівня економічної активності, що дозволяє більш обґрунтовано формувати політику у сферах безпеки дорожнього руху, міської мобільності та підтримки підприємництва. Аналогічно, уряд штату *Квінсленд* (Австралія) впровадив системи машинного навчання для автоматичного розпізнавання об'єктів землекористування на супутникових знімках. Це рішення дало змогу значно скоротити витрати на картографування, підвищити точність даних для планування землекористування та покращити оперативність реагування на виклики біобезпеки й природні катастрофи [2, с.5].

Належний нагляд за розвитком і використанням ШІ органами публічної адміністрації дедалі частіше здійснюється не лише виконавчими органами влади, а й незалежними інституціями — парламентами, судами, органами аудиту, омбудсменами, а також в рамках процедур, визначених законодавством про захист персональних даних та доступу до публічної інформації. Таке розширення кола суб'єктів нагляду сприяє підвищенню підзвітності урядів та формуванню комплексної системи стримувань і противаг у сфері цифрового урядування. Показовим прикладом є діяльність *Офісу Генерального аудитора (Норвегія)*, який із 2023 року проводить аудит ефективності застосування ШІ в центральних органах виконавчої влади [5].

Забезпечення прозорості використання алгоритмічних систем є фундаментальною умовою демократичного контролю та захисту прав громадян. За наявності функціональних механізмів прозорості можливо гарантувати ефективне оскарження рішень, ухвалених за участю ШІ, або отримання належних засобів правового захисту. На сьогодні законодавчі основи для цього існують у більшості країн світу: законодавство про захист персональних даних і доступ до інформації ухвалене у 134 державах, включаючи всі 37 країн-членів ОЕСР [6].

Однак міжнародна практика свідчить, що лише наявність загальних гарантій прозорості є недостатньою. Необхідним є запровадження більш конкретних вимог до розкриття інформації про алгоритми, а також залучення незалежних наглядових інституцій до перевірки коректності, недискримінаційності та законності функціонування систем ШІ у публічному секторі. Так, *Рада з питань прозорості Чилі* розробляє *Загальну інструкцію щодо алгоритмічної прозорості*, яка зобов'язуватиме понад тисячу державних установ розкривати відомості про алгоритми, що використовуються при наданні адміністративних послуг. Це дозволить громадянам з'ясувати, чи зумовлені отримані ними рішення або послуги автоматизованими моделями, а також зрозуміти логіку алгоритмічного прийняття рішень [7].

Подібні ініціативи активно реалізуються і в інших країнах. Зокрема, у *США* державні установи зобов'язані щороку публікувати відкриті реєстри випадків використання ШІ, із зазначенням тих, що можуть впливати на права людини або громадську безпеку, а також із поясненням заходів, ужитих для мінімізації відповідних ризиків.

Такий підхід не лише підвищує довіру до цифрових рішень держави, а й створює передумови для громадського та парламентського контролю за етичною відповідальністю уряду у сфері використання технологій штучного інтелекту.

**Висновки.** Міжнародний досвід впровадження штучного інтелекту у публічне управління демонструє позитивний потенціал таких технологій у підвищенні якості процедур та здійснення функцій публічного адміністрування, прозорості та підзвітності. Зокрема, системи моніторингу, автоматизовані алгоритми аналізу даних і реєстри випадків використання ШІ сприяють ефективнішому прийняттю рішень, зменшенню людського чинника в адміністративних процесах та формуванню довіри громадян до цифрових сервісів. Відкритість алгоритмів, публікація переліків застосувань, проведення оцінок впливу й незалежний аудит — усе це створює основу для етичного та відповідального використання інтелектуальних систем у публічному адмініструванні.

Разом із тим, аналіз міжнародних практик засвідчує, що запровадження надмірно детальних вимог до звітування, аудиту та оцінки впливу може

призвести до протилежного ефекту. Замість спрощення рутинних адміністративних процедур та підвищення оперативності управлінських рішень, державні органи ризикують отримати додаткові бюрократичні навантаження — обов'язок готувати численні звіти, проходити формальні оцінки та погодження, що уповільнює впровадження інновацій. У результаті може виникнути нова форма **«цифрової рутинізації»**, коли автоматизація процедур співіснує з посиленням звітності та контролю, не знижуючи загальної адміністративної складності.

Оптимальною стратегією для України є **пошук балансу між прозорістю і гнучкістю**, між контролем і сприянням інноваціям. Вимоги до алгоритмічної відкритості, незалежного нагляду й оцінки впливу мають бути диференційованими залежно від рівня ризику, який створює конкретна система ШІ. Такий **пропорційний підхід** дозволить зберегти належний рівень підзвітності та захисту прав громадян, не створюючи надмірного регуляторного тиску на органи влади та розробників інтелектуальних систем.

Таким чином, головним викликом для національної політики у сфері штучного інтелекту є не лише забезпечення відповідального використання технологій, а й **уникнення перетворення регулювання на самоціль**. Важливо, щоб інструменти контролю і прозорості залишалися засобом підвищення ефективності державного управління, а не його новим обмеженням.

### Список використаних джерел:

1. Government of Canada. (2023, March 18). *Regulations amending the Canadian Aviation Security Regulations, 2012 (Air Cargo)*. *Canada Gazette, Part I*, 157(11). <https://gazette.gc.ca/rp-pr/p1/2023/2023-03-18/html/reg5-eng.html>
2. Ubaldi, B.-C., et al. (2024). *Governing with artificial intelligence: Are governments ready?* OECD Report No. 20, 32 p. Organisation for Economic Co-operation and Development. [https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/governing-with-artificial-intelligence\\_f0e316f5/26324bc2-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/governing-with-artificial-intelligence_f0e316f5/26324bc2-en.pdf)
3. How the Norwegian government used conversational AI to help citizens access social benefits during COVID-19. (2024). *Boost.ai*. <https://boost.ai/case-studies/how-conversational-ai-is-helping-norways-citizens-with-covid>

4. OECD. (n.d.). *AIM: AI incidents and hazards monitor*. Organisation for Economic Co-operation and Development. <https://oecd.ai/en/incidents>

5. «Auditing machine learning algorithms», a white paper for public auditors released by the Supreme Audit Institutions of Finland, Germany, the Netherlands, Norway and the UK: <https://www.auditingalgorithms.net/>.

6. OECD. (2022). *Personalisation: Develops a profile of an individual and then learns and adapts to that individual over time*. In *OECD Framework for the Classification of AI Systems* (p. 50). Organisation for Economic Co-operation and Development.

7. Paz, M., & Muñoz, A.-M. (2023). *Chile's road to algorithmic transparency: Setting new standards in Latin America*. OECD Observatory of Public Sector Innovation (OPSI). <https://oecd-opsi.org/blog/chile-algorithmic-transparency/>

**Савінова Н.А.**

доктор юридичних наук, старший науковий співробітник, головний науковий співробітник Наукової лабораторії інформаційних прав та безпеки людини наукового центру інформації і права Державної наукової установи «Інститут інформації безпеки і права Національної академії правових наук України»

ORCID <https://orcid.org/0000-0003-0289-7926>

## **СВІДОМІСТЬ ЛЮДИНИ ПІД ЗАХИСТОМ ЄВРОПЕЙСЬКОГО AI ACT: ВИКЛИКИ НАЦІОНАЛЬНИМ ПРАВОВИМ СИСТЕМАМ**

У 2024 р. в ЄС, після десяти років роботи експертних груп, був прийнятий Закон Про штучний інтелект (AI Act) [1], першою серед заборон містить пряму вказівку на недопустимість «використання практик ШІ *маніпулятивний вплив*, який полягає у використанні систем ШІ, які застосовують *підсвідомі, маніпулятивні або обманні техніки, здатні викривляти поведінку* особи з метою матеріальної або психологічної шкоди» (п. а ч. 1 ст. 5) (курсив мій, Н.С.).

У світовій науці права до цього часу існує підсвідоме табу на дослідження феномену свідомості: у 2009 р. Дебора Денно, підкреслюючи актуальність таких досліджень в ХХІ сторіччі, доводила: «Дослідження свідомості викликали великий інтерес у широкого кола дисциплін, крім однієї — права. ... дослідження свідомості можуть прояснити американське кримінальне право» [2]. Ситуація на законодавчому рівні з того часу не надто змінилася як в США, так і в розвинених країнах Європи.

В Україні також існує стійке табу на тезаурус забезпечення безпеки свідомості, безпосередньо пов'язаний з термінологією психології. Водночас, маємо надію що вимога AI Act щодо заборон розміщення на ринку та використання ШІ, здатного маніпулювати поведінкою людей через підсвідомі спливи, маніпуляції та обману, все ж таки переламають

позитивістські правові конструкції, відірвані від реалій, і звернуть увагу законодавця та окреслену необхідність.

Інновація щодо інститутуалізації свідомості, психіки, поведінкових реакцій, навіть, з урахуванням характеру поведінкових реакцій щодо «прийняття рішень» (див. ч. 1 ст. 5 AI Act) має відбуватися в різних галузях права.

Якщо говорити про безпосередньо заборони, то, звичайно, це має стосуватися, насамперед, Кримінального кодексу України (або хоча б проекту кримінального кодексу) та Кодексу про адміністративні правопорушення. Обидва акти містять значний перелік діянь, які, насправді, спрямовані саме на свідомість іншої людини, містять ознаки впливу і маніпулювання, метою їх є спотворення поведінки людини. Найочевиднішим прикладом такого «прихованого» під опис традиційними кримінально-правовими термінами є діяння, передбачене ст. 190 КК України «Шахрайство». Але воно стосується виключно тих випадків, коли «обман або зловживання довірою» здійснюється з метою отримати майно або право на майно: під впливом маніпуляцій, обману, запуску підсвідомих патернів людина, всупереч своїй стандартній поведінці, всупереч волі, віддає іншій особі майно.

Однак, до цього часу, наприклад, правоохоронці нічого не можуть зробити через некриміналізовані маніпулювання свідомістю без корисливої мети: секти, деструктивні утворення лишаються поза полем дії кримінального права через те що ... не торкнувшись питання впливів на свідомість отримання їх об'єктивної сторони неможливо. А звідси неможливо визначити і диспозицію норми: право не має розуміння свідомості.

В умовах війни РФ проти України з 2014 р. та повномасштабного вторгнення 2022 р. в умовах гібридної агресії зміст інформаційної експансії як способу впливу на свідомість через політику м'якої сили, фейки та пропаганду набули для України нового змісту. Але, попри це, питання кримінально-правового захисту свідомості людини нам поки побачити теж не вдається: кримінально-правові характеристики впливів маскуються під словоформи, які, фактично, приховують основну мету подібних посягань – свідомість людини, і, як наслідок, реакцію її психіки. Прикладом подібних

«приховувань» реальних впливів на свідомість під іншими конструкціями є, наприклад криміналізація глорифікації дій СРСР або РФ.

Хоча ми і йдемо від вимог убезпечення свідомості людини від маніпулювання нею III, і, за таких вимог, первинно, звертаємося до, в основному, кримінального права, нам необхідно пам'ятати, що саме кримінальне право є «чорним дзеркалом» конституційних гарантій. Тобто, захищає воно найвищі соціальні цінності, визначені в Конституції України.

Проте, в Конституції України, як і в конституціях (старих і нових) країн Європи відсутні гарантії безпеки свідомості людини. Свідомість там також не визначена як цінність, адже матеріалістичний світ позитивного права за останні понад вік розвитку психології, на правовому рівні не бачив необхідності захищати ментальну сферу людини. Хіба, що така сфера зазнала від фізичних впливів: як то тілесні ушкодження, які спричинили тяжку душевну хворобу. Останній термін, взагалі, здається родом з XVIII віку залишився в тезаурусі, зокрема, вітчизняного права.

Наприкінці доповіді і до уваги законотворця хочу навести один з прикладів визначення свідомості Дебори Деннон, як вже вказувалося, однієї з небагатьох науковців-революціонерів, які намагаються обернути увагу права до реалій уразливості свідомості. Пані Деннон, серед багатьох визначень свідомості вдалося «ухопити» саме те, яке дає правникам і психологам експертам точку опори для розуміння оцінок і цілісності свідомості, і втручання в неї. Визначення свідомості в праві, на її думку, це – *«сукупність думок, почуттів та відчуттів людини, а також повсякденні обставини та культуру, в яких формуються ці думки, почуття та відчуття»* [3]. Вкрай елегантне і просте визначення, яке, на думку доповідача, розкриває можливості з гарантування і убезпечення. І є точкою опори для експертів-психологів.

### **Список використаних джерел**

1. European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))  
URL: [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138\\_EN.html?utm\\_source=chatgpt.com#title2](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html?utm_source=chatgpt.com#title2)

2. Deborah W. Denno, Arthur A. McGivney 'Consciousness and Culpability in American Criminal Law' (2009) 126 *Waseda Proceedings of Comparative Law* 116 URL: [https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1909&context=faculty\\_scholarship](https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1909&context=faculty_scholarship)

3. Deborah W. Denno. 'Crime and Consciousness: Science and Involuntary Acts' (2003) 269 *Minnesota Law Review* 269-400 URL: [https://ir.lawnet.fordham.edu/faculty\\_scholarship/112](https://ir.lawnet.fordham.edu/faculty_scholarship/112)

**Варинський В.О.**

кандидат політичних наук, доцент;  
доцент кафедри філософії та україністики  
Національного університету «Одеська  
морська академія»

ORCID: <https://orcid.org/0000-0001-5837-6201>

## **РИЗИКИ ВИКОРИСТАННЯ ШІ В ПРАВОСУДДІ: ОГЛЯД ПРОБЛЕМИ**

У статті 6 Європейській конвенції про захист прав людини та основоположних свобод [1] закріплене право розгляду справ незалежним і «безстороннім судом», і не міститься вказівки на те, що таким суддею має бути людина. Натомість, конституції багатьох країн, серед яких і Україна (ст. 127) [2], містять прямі вказівки, що судочинство покладається на суддів, а цей статус за законодавством належить тільки людям. Таким чином, згідно діючих настанов сучасного законодавства, на штучний інтелект (далі – ШІ) не може бути покладена функція здійснення правосуддя.

Проте, доволі часто в наукових дискурсах правничих кіл точаться дискусії з приводу доцільності використання ШІ в правосудді. Сучасні проекти актів законодавства розроблюються, наприклад, з урахуванням необхідності сприйняття їх настанов автоматизованими системами, у т. ч. ШІ, на що прямо вказують проектні групи [3].

Дійсно, ШІ, завдяки своєму потенціалу та ефективності, точності та очікуваній доступності, ніби-то відкриває захоплюючі перспективи для досягнення справедливості в судовому процесі. Однак, поряд із цим, необхідно ретельно враховувати і ті ризики, котрі використання ШІ в правосудді може утворити.

Першим з ризиків використання ШІ в правосудді є упередженість та дискримінація. Саме перевага ШІ у обробленні кількості інформації, її систематизації, і, відповідно, кластеризації її, може призвести до дискримінаційних процесів відносно окремих груп. Останнє ж може призвести до упереджених результатів, підкреслення існуючої нерівності та дискримінації у системі правосуддя.

Оскільки складність функціонування ШІ для пересічного «користувача» чи співробітника є, фактично, «чорною скринею», людям

важко зрозуміти і інтерпретувати процеси прийняття ним рішень. Відсутність прозорості і «людського» мислення буде викликати занепокоєння і обурення щодо належної правової процедури, оскільки люди, не маючи розуміння процедури прийняття рішень, втрачатимуть довіру до дій ШІ.

Окремим сегментом слід оцінювати і ризики етики використання ШІ. Компроміс між ефективністю та людяністю, виведення з процесу прийняття рішень емоцій і, відповідно, упередженості, та ризик надмірної технологізації процесів створюють певну загрозу основним принципам правосуддя: справедливості та гуманізму.

У разі використання роботи з великими базами даних, у т.ч. роботи ШІ, присутній ризик витоку даних. В правосудді ж, насамперед, переважно, ми маємо справу з персональними даними. І не тільки. Тут можуть бути елементи і слідчої таємниці, і відомості про свідків, у т.ч. захищених, і багато іншого, що не має виходити за межі документації. Водночас, при роботі технічного «помічника» - ШІ, завжди лишається вірогідність ризику витікання інформації, яку він збирає, обробляє, зберігає.

Водночас, інтеграція ШІ в систему правосуддя відкриває величезні перспективи підвищення ефективності, доступності і справедливості судочинства, і у разі врахування основних ризиків і обмеження використання ШІ в найбільш уразливих питаннях, його використання в правосудді, як технічного помічника людини, допустиме.

Саме на таке використання спрямовані п'ять принципів дотримання основних прав людини при використанні ШІ, закріплені в Етичній хартії Ради Європи з використання штучного інтелекту у судовій системі та її середовищі 2018 р. [4] (далі - Етична хартія ШІ в судовій системі):

- принцип дотримання основних прав людини при використанні ШІ;
- принцип недискримінації, а саме запобігання розвитку будь-якої дискримінації між окремими особами чи групами осіб;
- принцип якості та безпеки, який стосується обробки судових рішень і даних у безпечному технологічному середовищі;
- принцип прозорості, неупередженості та справедливості;
- принцип "під контролем користувача" (under user control).

Принцип дотримання основних прав людини при використанні ШІ зобов'язує бути переконаними в тому, що розробка та впровадження засобів штучного інтелекту і послуги сумісні з основними правами людини.

Згідно цього принципу обробка судових рішень і даних має служити чітким цілям, у повній відповідності до основних прав, гарантованих Європейською конвенцією з прав людини [1] і Конвенцією про захист осіб щодо автоматичної обробки персональних даних [4].

В межах цього принципу закладений і принцип рівності сторін та змагальності: «коли інструменти штучного інтелекту використовуються для вирішення спору або як інструмент для допомоги в ухваленні судових рішень або для надання вказівок громадськості, важливо переконатися, що вони не підривають гарантії права на доступ до судді та право на справедливий суд» [4].

Етична хартія ШІ в судовій системі передбачає, що у разі коли інструменти ШІ використовуються для вирішення спору або як інструмент для допомоги в ухваленні судових рішень або для надання вказівок громадськості, країнам учасникам необхідно забезпечити всі механізми для можливості переконуватися в тому, що вони не підривають гарантії права на доступ до судді та право на справедливий суд. Такою вимогою Хартія забезпечує дотримання рівності сторін і поваги до змагальності процесу.

Також в документі передбачений обов'язок використання ШІ з належною повагою до принципів верховенства права та незалежності суддів у процесі ухвалення рішень.

Перевага, при такому застосуванні ШІ, має приділятися підходам заснованими на нормах застосування етики та дотримання прав людини: починаючи з етапів проектування та навчання, в ШІ мають бути інтегровані правила, які забороняють прямі чи непрямі порушення фундаментальних цінностей, які захищаються конвенціями.

Виходячи зі змісту Етичної хартії ШІ в судовій системі, *принцип дотримання прав людини при використанні ШІ, полягає у первинному, матричному вживленні розуміння дотримання прав людини в ШІ, котрі можуть розроблятися для використання в правосудді, а також на такому ж рівні в системі мають бути закладені критеріальні положення забезпечення безпеки персональних даних та конфіденційної інформації.*

Принцип недискримінації зобов'язує при застосуванні ШІ в правосудді запобігти розвитку або посиленню будь-якої дискримінації між окремими особами або групами осіб.

Документом, під кутом розуміння врахування здатності систем при обробці інформації виявляти існуючу закономірність, котра проявлятиме дискримінацію до певних груп, або окремих осіб, передбачений обов'язок зацікавлених у впровадженні ШІ сторін обов'язок гарантувати, що методи не відтворюють або не посилюють таку дискримінацію та не призводять до детерміністичного аналізу по конкретній справі.

Етичною хартією ШІ в судовій системі також, відносно принципу недискримінації, встановлено що особливу увагу слід приділяти як на етапі розробки ШІ, так і на етапі розгортання, особливо коли обробка прямо чи опосередковано базується на «конфіденційних» даних. «Це може включати ймовірне расове чи етнічне походження, соціально-економічне походження, політичні погляди, релігійні чи філософські переконання, членство в профспілках, генетичні дані, біометричні дані, дані про здоров'я або дані про сексуальне життя чи сексуальну орієнтацію. Коли така дискримінація була виявлена, необхідно розглянути заходи щодо обмеження або, якщо можливо, нейтралізувати ці ризики, а також підвищити обізнаність зацікавлених сторін» [4], - прямо вказує Етична хартія. Водночас в документі робиться акцент на необхідності заохочування використання машинного навчання та міждисциплінарного наукового аналізу для боротьби з такою дискримінацією.

*Тобто, Етична хартія ШІ в судовій системі не допускає перенесення «дискримінуючих», систематизованих даних на судовий процес, проте, наполягає на стимулюванні врахування даних, отриманих під час судового розслідування справ в кримінологічних дослідженнях і моделюванні детермінацій злочинності, у т.ч. відносно соціальних груп.*

Принцип якості та безпеки: «щодо обробки судових рішень і даних використовувати перевірені джерела і нематеріальні дані з моделями, розробленими міждисциплінарним способом у безпечному технологічному середовищі»

Принцип прозорості, неупередженості та справедливості: «зробити доступні та зрозумілі методи обробки даних, санкціонувати зовнішні аудити».

Коли використовуються інструменти, які можуть мати правові наслідки або можуть суттєво вплинути на життя людей. Необхідно чітко уточнити, що ці заходи застосовуються до всього ланцюжка проектування та експлуатації, оскільки процес відбору, якість і організація даних безпосередньо впливають на фазу навчання.

Перший варіант — повна технічна прозорість (наприклад, відкритий вихідний код і документація), яка іноді обмежена захистом комерційної таємниці. Систему також можна пояснити зрозумілою та знайомою мовою (щоб описати, як отримуються результати), повідомляючи, наприклад, характер пропонованих послуг, розроблені інструменти, продуктивність і ризики помилок. Незалежним органам чи експертам можна доручити сертифікацію та перевірку методів обробки або надання консультацій заздалегідь. Органи державної влади можуть видати сертифікацію, яка регулярно переглядається.

Керуючись цими та іншими вивіреними та узгодженими з правом ЄС принципами, задля використання ШІ та одночасного зниження ризиків, зараз політики, розробники та законотворці мають співпрацювати з розробниками ракових обмежень його застосування ШІ в системі правосуддя, як одній з найвідповідальніших і найрізкованіших сфер.

### **Список використаних джерел**

1. Європейська конвенція про захист прав людини та основоположних свобод. URL: <https://www.coe.int/uk/web/compass/the-european-convention-on-human-rights-and-its-protocols>

2. Конституція України. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

3. Концепція реформи кримінального законодавства України. URL: <https://newcriminalcode.org.ua/concept>

4. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. URL: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>

5. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. URL: <https://rm.coe.int/1680078b37>

**Фурашев В. М.**

кандидат технічних наук, доцент, с.н.с.,  
перший заступник директора Державної  
наукової установи «Інститут інформації,  
безпеки і права НАПрН України»

ORCID: <https://orcid.org/0000-0001-7205-724X>

**Дорогих С.О.**

кандидат юридичних наук, провідний  
науковий співробітник Державної наукової  
установи «Інститут інформації, безпеки і  
права НАПрН України»

ORCID: <https://orcid.org/0000-0002-2748-1938>

## **ТРАНСФОРМАЦІЯ ПРАВОТВОРЧОСТІ ТА ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ В УМОВАХ ЦИФРОВІЗАЦІЇ: КОНЦЕПТУАЛЬНІ ЗАСАДИ ТА ПРАКТИЧНІ ВИКЛИКИ**

Як вірно зауважив Мирослав Дністрянський в статті «Система державної влади й місцевого самоврядування в Україні: проблеми й суперечності функціонування»<sup>1</sup>: «Різних оцінок роботи окремих органів державної влади України можна знайти дуже багато. Як справедливих, так й упереджених. А ось загальні проблеми ефективності державної влади й місцевого самоврядування, насамперед в контексті співвідношення різних гілок влади, центру й регіонів, структури територіального управління, на громадське обговорення практично не виносяться. А це водночас фундаментальні питання функціонування держави, які були і є актуальними в усі часи. З огляду на це, варто насамперед визначитися, чи 1) Україна має бути парламентською республікою, залишатися парламентсько-президентською чи трансформуватися в президентсько-парламентську або президентську; 2) чи потрібна Україні тотальна децентралізація; 3) як забезпечити ефективність державного управління й самоврядування на всій

---

<sup>1</sup> URL: <https://westnews.info/news/SISTEMA-DERZHAVNOyi-VLAD-J-MISCVOGO-SAMOVRYADUVANNYA-V-UKRAjINII-PROBLEMI-J-SUPERECHNOSTI-FUNKCIONUVANNYA.html>

території держави. І розглядати усі ці питання важливо з урахуванням усіх зовнішньополітичних й внутрішньополітичних викликів, які постали перед Україною, та ситуації в сучасному світі загалом».

В будь-якому разі, якщо мова йде про парламентську чи парламентсько-президентську модель республіки (це саме стосується й парламентсько-президентської та президентської форми правління, хоч і в меншій мірі), парламент не може ефективно функціонувати без механізмів контролю за виконанням власних рішень. Відсутність такого контролю суперечила б самій природі інформаційних систем, для яких характерний зворотний зв'язок між прийнятим рішенням та інформацією про його реалізацію. Без цього зворотного зв'язку система втрачає здатність до корекції, адаптації та своєчасного реагування на відхилення, що у правотворчій діяльності призводить до неефективності, накопичення правових деформацій і розбалансування механізму державного управління.

Навіть поверхова оцінка реєстрованих законопроектів суб'єктами законодавчої ініціативи (народними депутатами) має зростаючу тенденцію, що вказує на спрямоване витіснення законодавчою/законопроектною функцією Верховної Ради України контрольної функції парламенту, яка повинна забезпечувати високій рівень ефективності правового регулювання забезпечення життєдіяльності та цілісності суспільства та країни.

Враховуючи позицію рф по відношенню до України, особливо після 2014 року по даний час, необхідно постійно мати на увазі, що будь яка країна, суспільство повинна формувати таке своє середовище, у якому думки народу та діяльність системи державного управління мають однакову спрямованість по всім принциповим питанням/напрямам забезпеченням стійкого існування та розвитку.

Коли така або близько подібна єдність/розуміння, то перемога держави, суспільства гарантована по всім напрямам життєзабезпечення та розвитку, а також своєю цілісністю, в противному випадку - вірогідність поразки/програшу дуже висока.

Вище окреслене, науково-практичні досягнення у сфері автоматизованого формування, обробки, збереження та аналізу інформації та інші можливості дозволяють більш предметно ставити та поетапно реалізовувати трансформаційні процеси та процедури контролю повноти та

відповідності нормативно-правових документів всіх рівнів державного управління та місцевого самоуправління, а також відповідності (за необхідністю) подібним нормативно-правовим документам інших країн.

Трансформаційні процеси та процедури законотворчої діяльності та контролю повноти та відповідності нормативно-правових документів повинні стосовуватися всіх рівнів державного управління та місцевого самоуправління.

У чому полягає сутність правового моніторингу, в т.ч. і парламентського контролю? По-простому можна відповісти наступним чином:

а) встановленням рівня реальності виконання прийнятих нормативно-правових рішень;

б) встановленням необхідності внесення змін/осучаснення вже раніше прийнятих нормативно-правових рішень;

в) встановленням необхідності та потенційних термінів розгляду нормативно-правових рішень;

г) встановленням необхідності та ступеня терміновості встановлення нових нормативно-правових соціальних та суспільних відносин;

е) недопущення дублювання нормативно-правових прав та правил, а також правових прогалин, подолання правових колізій.

Слід також зауважити, що парламент за своєю сутністю є складною управлінською системою, діяльність якої підпорядкована загальним закономірностям циклу державного управління. Першим етапом цього циклу є збирання повної, достовірної та релевантної інформації про стан суспільних відносин, які потребують правового регулювання. Саме на цьому етапі виявляються проблеми чинного законодавства, правові прогалини, колізії або суспільні трансформації, що вимагають оновлення нормативно-правової бази. Інформаційний етап має ключове значення, оскільки якість правотворчого рішення безпосередньо залежить від повноти та об'єктивності даних, що лягають в основу розробки законопроекту.

Наступним етапом виступає прийняття управлінського рішення, яке в парламентському вимірі втілюється у формі ухвалення законів. Однак цикл управління не завершується на стадії нормотворення: після введення закону в дію відбувається збирання інформації про практику його застосування, аналіз

реальних наслідків та перевірка відповідності отриманих результатів задекларованим цілям. Якщо виявляється, що мета закону не досягнута, або суспільні умови змінилися, виникає потреба у внесенні змін, уточнень чи доповнень. Таким чином, парламент здійснює безперервний, циклічний процес правового управління, у якому законотворчість і парламентський контроль перебувають у тісному функціональному зв'язку та взаємно забезпечують ефективність один одного.

Цілком зрозуміло, що сучасні досягнення у кібернетичній/програмно-технічній сферах формування, збереження, прийому-передачі, аналізу та ін. дії з інформацією, а також наслідки початкових результатів ШІ дозволяють ставити питання опрацювання питань всебічного контролю, в т.ч. правового, парламентського, галузевого та ін. без суттєвого збільшення спеціалістів-правників та спеціалістів інших галузей та підпорядкованості. До аналогічного висновку прийшли спеціалісти Державної наукової установи «Інститут інформації, безпеки і права НАПрН України» в результаті проведення фундаментального наукового дослідження «Організаційно-правові і технологічні засади розвитку системи нормативно-правової інформації та парламентського контролю в умовах цифровізації».

Перспективи розвитку генеративного штучного інтелекту (ГШІ) у сфері парламентського контролю, у першу чергу, можуть стосуватись автоматизації моніторингу та аналізу інформації, що надходить з різних джерел, що може допомогти парламентарям швидко і ефективно отримувати інформацію, необхідну для їх роботи. По-друге, ГШІ може використовуватися для створення нових інструментів для аналізу даних, які можуть допомогти парламентарям виявляти приховані тенденції та закономірності. По-третє, системи ГШІ можуть використовуватися для підтримки інновацій у сфері парламентського контролю, знаходити нові підходи до вирішення проблем. Існує багато можливостей і конкретних застосунків ГШІ, які можуть бути використані у сфері парламентського контролю, наприклад, ГШІ може використовуватися для створення інтелектуального помічника, який може виконувати такі завдання, як моніторинг новин, аналіз даних та підготовка звітів. ГШІ може використовуватися для моделювання, прогнозування наслідків урядових рішень. Крім того, уже сьогодні можливе створення штучного

інтелектуального чат-бота для спілкування з громадянами, що допоможе парламентарям бути більш доступними для своїх виборців.

У той же час слід враховувати й ризики, пов'язані з використанням ШІ при здійсненні парламентського контролю. В першу чергу на думку спадають наступні ризики:

- питання прозорості алгоритмів при прийнятті рішень на основі використання штучного інтелекту;
- наявність алгоритмічної упередженості, загроза політизації та маніпуляції ШІ. Іншими словами кажучи: хто? як? на основі якої інформації буде навчати ШІ;
- питання захисту масивів даних, на основі яких буде функціонувати ШІ від зовнішнього втручання;
- недостатня цифрова та правова компетентність депутатів може завадити вірній інтерпретації інформації, отриманої за допомогою ШІ;
- й нарешті, неврегульованість правового статусу ШІ для використання в публічній діяльності органів державної влади та місцевого самоврядування.

**Висновок.** Для подальших наукових досліджень у сфері цифровізації парламентського контролю ключовим завданням є пошук оптимального балансу між перевагами, які надає використання штучного інтелекту, та потенційними ризиками, що супроводжують його впровадження. Технології ШІ відкривають безпрецедентні можливості для підвищення ефективності, прозорості та оперативності контролюючих процедур, однак їх застосування потребує належного правового, етичного й організаційного забезпечення. Лише за умови комплексного врегулювання цих аспектів ШІ стане інструментом, що посилює демократичну природу парламентського контролю, а не джерелом нових викликів для системи державної влади.

### **Список використаних джерел:**

1. Ланде Д.В., Фурашев В.М. Парламентський контроль із застосуванням генеративного штучного інтелекту : монографія / Ланде Д.В., Фурашев В.М. – Київ: ТОВ "Інжиніринг", 2023. - 202 с.
2. ЗАКОН УКРАЇНИ Про доступ до публічної інформації (Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314) URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text> (дата звернення 16.10.2025)

3. Цифрова трансформація. <https://www.kmu.gov.ua/diyalnist/mizhnarodna-dopomoga/coordination/cifrova-transformaciya> (дата звернення 16.10.2025)
4. Фурашев В.М., Корж І.Ф. Штучний інтелект та адміністративна (контрольна) діяльність публічної влади: європейський погляд. Інформація і право. 2025. №1(52)/2025. С. 51-61. URL: <http://il.ippi.org.ua/article/view/324667>
5. 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.
6. Ланде Д.В., Фурашев В.М. Парламентський контроль із застосуванням генеративного штучного інтелекту : монографія / Ланде Д.В., Фурашев В.М. Київ: ТОВ "Інжиніринг", 2023. 202 с.

Наукове видання

**ТРАНСФОРМАЦІЙНІ ПРОЦЕСИ ПРАВОТВОРЧОЇ ДІЯЛЬНОСТІ  
ТА ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ**

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

*Київ, 30 жовтня 2025 року*

ЕЛЕКТРОННЕ ВИДАННЯ

*Упорядники:*

*В. М. Фурашев, С. О. Дорогих*

Ум-друк. арк. 5,4.  
Зам. № 2512-04.

Видавець ПП «Фенікс»  
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).  
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.  
e-mail: fenix-izd@ukr.net