АНАЛІТИЧНИЙ ЦЕНТР СУЧАСНОЇ ГУМАНІТАРИСТИКИ
ХАРКІВСЬКА АСОЦІАЦІЯ ПОЛІТОЛОГІВ

ЦИФРОВА МОДЕРНІСТЬ І ШТУЧНИЙ ІНТЕЛЕКТ: НОВІ РИЗИКИ, НОВІ РАЦІОНАЛЬНОСТІ

Матеріали
Всеукраїнської науково-практичної конференції
(м. Харків, 30 квітня 2026 р.)

Харків
«Право»
2026

Дика П. Я.,
здобувачка вищої освіти першого
(бакалаврського) рівня, IV курс,
ННІ міжнародних відносин,
Харківський національний економічний
університет імені С. Кузнеця

THINK TANK ЯК ІНСТРУМЕНТ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ В УКРАЇНІ

У сьогоднішніх реаліях повномасштабної війни Російської Федерації проти України інформаційна безпека є одним із ключових елементів національної безпеки держави [4]. Кібератаки, ворожі кампанії, так звані ІПСО та інші подібні виклики, які чинять не тільки негативний вплив на суспільство, але й на довіру до державних інституцій. Подібні труднощі характеризуються складністю та вимагають швидкої, але якісної реакції держави. Тому в цьому контексті особливу роль відіграють think tank – аналітичні центри, які здатні виконувати функції моніторингу, аналізу та прогнозування інформаційних загроз, формувати стратегічні рекомендації для державних органів. Вони радше є мостами між державними інститутами, громадянами та міжнародними партнерами, формуючи безпечну протидію постійним інформаційним атакам держави-агресора.

Необхідно зазначити, що наразі ключовими викликами сучасної інформаційної безпеки є гібридні інформаційні кампанії, що поєднують у собі системне поширення дезінформації, фейкових повідомлень і маніпулятивних наративів, спрямованих на формування викривленого сприйняття реальності. Такі операції, як правило, використовують цифрові платформи, соціальні мережі та мережі автоматизованих акаунтів. Також серйозну загрозу становлять кібератаки, об'єктами яких стають державні інформаційні системи, елементи критичної інфраструктури, військові та комунікаційні мережі. Наслідками таких впливів можуть бути як доступ до конфіденційних даних, так і повне порушення функціонування органів державної влади або ж тимчасова або повна зупинка надання ключових сервісів, що істотно послаблює загальну стійкість держави [3].

У таких умовах виникає потреба у діяльності аналітичних центрів, які в даному випадку виконують роль суб'єкта протидії інформаційним загрозам. Передусім вітчизняні think tanks здійснюють системний моніторинг національного та міжнародного інформаційного простору, зосереджуючи увагу на виявленні діяльності російських пропагандистських ресурсів, мереж анонімних Telegram-каналів, бот-мереж і цифрових платформ, за допомогою яких поширюється дезінформація. У межах роботи фіксуються та аналізуються основні ворожі наративи, зокрема щодо «втоми Заходу» чи «легітимності української влади», що активно тиражуються у межах інформаційно-психологічних операцій. Як правило, у подібних випадках фахівці досліджують взаємозв'язки між джерелами поширення повідомлень, визначають ключові каналита стратегічні цілі кожної операції. Згодом результати такого аналізу узагальнюються у спеціалізованих звітах, які передаються відповідним органам державної влади з метою забезпечення своєчасного та адекватного реагування на виявлені загрози.

Крім того, слід закцентувати, що аналітичні центри виконують і експертно-консультативну функцію, розробляючи практичні рекомендації для органів державного управління. Такі напрацювання використовуються міністерствами, відомствами та структурами сектору безпеки і оборони під час формування стратегічних комунікацій чи ухвалення рішень щодо обмеження діяльності деструктивних інформаційних ресурсів.

Таким чином, можемо виділити три ключові функції аналітичних центрів в питанні протидії інформаційній загрозі України: моніторинг, аналіз і рекомендації [2].

Показовим прикладом є дослідження Національного інституту стратегічних досліджень, присвячене атакам через ланцюги постачання (supply chain attacks). У відповідній аналітичній доповіді експерти НІСД детально проаналізували механізми використання вразливостей у програмному забезпеченні та комерційних сервісах для здійснення масштабних кібератак проти державних органів і критичної інфраструктури України. У доповіді, зокрема, розглянуто кібератаку типу NotPetya. Варто відзначити, що у детально розробленому звіті аналітики не лише реконструювали сценарії атак, а й запропонували низку рекомендацій щодо посилення кіберстійкості державних систем, удосконалення механізмів реагування та підвищення рівня координації між державними і недержавними структурами, спираючись не тільки на власні знання, але й досвід з-за кордону [1].

Незважаючи на подібні успішні кейси вітчизняних фабрик думок, залишається низка проблем, які ускладнюють їхню повноцінну роботу у сфері інформаційної безпеки. Однією з таких є нестача стабільного фінансування. Значна частина подібних установ функціонує переважно за рахунок грантової підтримки, що має тимчасовий характер, унаслідок чого ускладнюється довгострокове планування діяльності, утримання висококваліфікованих фахівців та інвестування в розвиток технічної інфраструктури [5, с. 99–100].

Іншим вагомим стримувальним чинником є недостатній рівень інформаційного обміну між державними та недержавними структурами. Бюрократичні бар'єри, обмеження доступу до офіційних даних та відсутність налагоджених каналів комунікації призводять до зниження повноти та достовірності аналітичних висновків, що негативно позначається на якості експертних рекомендацій. Складнощі виникають і в кадровому забезпеченні, бо в Україні відчувається дефіцит спеціалістів, здатних ефективно працювати з великими обсягами інформації, сучасними аналітичними платформами та спеціалізованими програмними продуктами. Низький рівень оплати праці також сприяє відтоку таких фахівців до приватного сектору або за кордон, що послаблює кадровий потенціал вітчизняних аналітичних центрів. Окрему увагу заслоговує факт, того що на сьогодні існує вкрай слабкий рівень взаємодії з регіональними структурами, адже переважна більшість think tanks зосереджена у столиці та великих містах, тоді як у регіонах відсутня розвинена мережа локальних аналітичних осередків, спроможних працювати на місцевому рівні.

Спираючись на вищеописані проблеми і, власне, світові тенденції, можна виокремити кілька напрямів розвитку аналітичних центрів України, зокрема і у сфері інформаційних загроз.

Перше і основне – це залучення та використання штучного інтелекту та автоматизованих систем аналізу даних. Українські інституції вже поступово впроваджують програмні рішення на основі штучного інтелекту для виявлення інформаційної активності, автоматизованого розпізнавання дезінформаційного контенту та моніторингу операцій у режимі реального часу.

Другим кроком може стати створення єдиної національної аналітичної платформи для обміну інформацією між органами державної влади, аналітичними центрами та структурами сектору безпеки, що забезпечить опера-

тивний доступ до даних про кібератаки, пропагандистські кампанії та нові механізми інформаційного впливу.

Третьою перспективою є розширення освітніх програм у сфері аналізу інформаційних загроз, протидії дезінформації, цифрової безпеки та стратегічних комунікацій, що сприятиме формуванню фахівців, здатних ефективно працювати із сучасними інструментами та технологіями.

І четвертим напрямом також є створення мережі регіональних аналітичних осередків, які забезпечуватимуть моніторинг локальних проявів інформаційних операцій і взаємодіятимуть з органами місцевої влади.

Підбиваючи підсумки, варто зазначити, що наразі попри наявність низки системних проблем, зокрема кадрових, технологічних та організаційних обмежень, аналітична діяльність у сфері інформаційної безпеки України демонструє помітні позитивні зрушення. Перспективи її розвитку пов'язані з упровадженням цифрових платформ збору й аналізу інформації, використанням технологій штучного інтелекту та автоматизованих систем моніторингу. Очікується, що важливу роль також відіграватиме взаємодія між державними структурами та аналітичними центрами, а також розвиток професійної підготовки фахівців, що загалом сприятиме зміцненню інформаційної безпеки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дубов Д., Бойко В., Гнатюк С. Атаки через ланцюжки постачань: формуючи стратегічну відповідь. *Національний інститут стратегічних досліджень*. URL: https://niss.gov.ua/sites/default/files/2022–06/ad_cyberresill_structure_var8_new_ed_01_gotove_0.pdf (дата звернення: 20.04.2026).

2. Дудатьєв А. В., Войтович О. П., Миронюк В. В. Інформаційно-аналітичні центри в управлінні інформаційною безпекою держави. *Вісник Хмельницького національного університету*. *Серія: Технічні науки*. 2020. № 1 (281). С 105–109. DOI: 10.31891/2307-5732-2020-281-1-105-109

3. Капітон А. М., Дзюбан О. С. Сучасні виклики інформаційної безпеки, еволюція загроз та стратегії захисту в майбутньому. *Інформаційні технології в сучасному світі*: матеріали Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених, 29 квітня 2025 р. Харків: ДБТУ, 2025. С. 22–23.

4. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради (ВВР).* 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469–19#Text (дата звернення: 20.04.2026).

5. Kachkovska L., Voznyuk Y. Countering information threats in Ukraine: current issues for solving at the state level. *Міжнародні відносини, суспільні комунікації*

Секція: Міжнародні відносини

Наукове видання

ЦИФРОВА МОДЕРНІСТЬ І ШТУЧНИЙ ІНТЕЛЕКТ: НОВІ РИЗИКИ, НОВІ РАЦІОНАЛЬНОСТІ

Матеріали
Всеукраїнської науково-практичної конференції
(м. Харків, 30 квітня 2026 р.)

Редактор *Т. О. Чернишова*

Підписано до друку 04.05.2026. Формат 60×84/16.
Ум. друк. арк. 6,9. Обл.-вид. арк. 6. Тираж 100 пр. Зам. № 662

ТОВ «Видавничий дім «Право»,
вул. Харківських Дивізій, 11/2, м. Харків, Україна
Для кореспонденції: а/с 822, м. Харків, 61023, Україна
Тел.: (050) 409-08-69, (067) 574-81-20
Вебсайт: https://pravo-izdat.com.ua
E-mail для замовників послуг: verstka@pravo-izdat.com.ua
E-mail для покупців: sales@pravo-izdat.com.ua
Свідоцтво суб'єкта видавничої справи ДК № 8024 від 05.12.2023

Виготовлено ТОВ «Промарт Плюс»,
вул. Весніна, 12, м. Харків, 61023, Україна,
тел. (097) 445-07-79
Свідоцтво суб'єкта видавничої справи ДК № 8388 від 16.07.2025