Міністерство освіти і науки України
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»
Університет Ауреля Влайку (Румунія)
Університет «Лучіана Блага» (Румунія)
Центральна бібліотека Болгарської
Академії наук (Болгарія)
Коледж Санта-Фе (США)
Державний університет Сан-Паулу(Бразилія)
Університет Метрополітен Лондон (Великобританія)
Національний університет «Одеська політехніка» (м. Одеса)
Західноукраїнський національний університет (м. Тернопіль)
Державний архів Полтавської області
Центральна бібліотека Полтавської міської територіальної громади

Документно-інформаційні комунікації в умовах глобалізації: стан, проблеми і перспективи

МАТЕРІАЛИ
X МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
25 листопада 2025 року

Полтава

комунікації та медіація в умовах конфліктного врегулювання» / . Вінниця, 2024. 108 с.

3. Горон Д. Через російську агресію в Україні пошкоджені 1599 пам’яток культурної спадщини, — МКСК. URL: https://detector.media/infospace/article/244588/2025-10-02-cherez-rosiysku-agresiyu-v-ukraini-poshkodzheni-1599-pamyatok-kulturnoi-spadshchyny-mksk

4. Малюта О. Культурна дипломатія як засіб збереження української державності. Україна: культурна спадщина, національна свідомість, державність. Львів: Видавництво "Світ", 2023. № 38. С. 153–170.

Ольга Мізіна

м. Полтава

МЕТОДИ ВИЯВЛЕННЯ ФЕЙКОВИХ НОВИН ТА МАНІПУЛЯЦІЙ У МЕДІАПРОСТОРІ УКРАЇНИ

У сучасних умовах стрімкого розвитку цифрових технологій та зростання ролі соціальних мереж інформаційний простір України зазнає суттєвих трансформацій. Поряд із розширенням можливостей комунікації, доступу до даних та формування громадської думки спостерігається й інша тенденція – активне поширення фейкових новин, дезінформації та маніпулятивних медіаповідомлень.

Ці явища стають інструментом впливу на політичні процеси, соціальну стабільність, безпекові аспекти держави та поведінку окремих громадян. Особливу актуальність проблема набуває для України в умовах інформаційної війни, коли медіапростір стає ареною боротьби за інтерпретацію фактів, формування наративів і конструювання альтернативної реальності. У таких умовах виявлення неправдивої інформації та протидія маніпуляціям є не лише завданням журналістів і фактчекерів, а й важливим елементом медіаграмотності суспільства.

На сьогодні соціальні мережі в нашій країні в умовах війни є основним каналом поширення як правдивих новин, так і дезінформації, Україні необхідно мати ефективні механізми швидкого виявлення неправдивих повідомлень. Оперативна ідентифікація фейків дає змогу мінімізувати їхній негативний вплив на суспільну думку, запобігати панічним настроям та забезпечувати інформаційну безпеку держави.

Поєднання автоматизованих алгоритмів, зокрема систем аналізу тексту, машинного навчання та детекторів аномалій із професійною роботою фактчекерів, створює оптимальну модель роботи. Машини здатні швидко обробляти великі масиви контенту, виділяти підозрілі повідомлення та формувати первинні сигнали. Людські експерти, своєю чергою, забезпечують глибоку перевірку, контекстуальний аналіз і верифікацію висновків. Такий комплексний підхід не лише розширює масштаби моніторингу, а й підвищує точність та вірогідність аналітичних результатів [1, с. 34].

Виявлення фейкових новин у сучасному медіапросторі ґрунтується на використанні різних підходів, кожен з яких має свої сильні сторони та обмеження. Ось деякі з сучасних підходів до виявлення фейків: ручний фактчекінг, rule-based, ML, DL, hybrid. Спробуємо визначити найефективніші методи виявлення фейкових новин та маніпуляцій у медіапросторі України.

Під час ручного фактчекінгу (manual fact-checking) медіаексперти й аналітики вручну перевіряють інформацію, порівнюючи з надійними джерелами, офіційними даними, експертними коментарями та контекстом події. Висока точність і глибина аналізу, можливість урахувати контекст, підтекст, риторику, маніпулятивні техніки, ситуації, коли аналітик помічає нюанси, які машинний алгоритм може пропустити надають перевагу цьому методу. Натомість ручна перевірка інформації займає багато часу, має обмежену масштабованість, не завжди миттєво реагує на масові вкидання дезінформації, маніпулятивних матеріалів та швидко тиражованих фальшивих новин.

В Україні вже сформувалася розвинена екосистема фактчекінгу, яка поєднує зусилля медіа, громадських організацій та незалежних аналітичних ініціатив. Однією з ключових платформ є нині добре відомий флагманський проєкт StopFake, що спеціалізується на викритті російської пропаганди, перевірці вірусних фейків та освітній діяльності [2]. Проєкт активно застосовує як ручний аналіз, так і автоматизовані інструменти моніторингу інформаційного простору. Іншим важливим гравцем є фактчскінговий проєкт незалежної аналітичної платформи «Вокс Україна» [3]. Команда VoxCheck фокусується на перевірці заяв українських політиків, аналізі медійних маніпуляцій та створенні аналітичних баз даних, що дають змогу відстежувати тенденції у політичній комунікації. До екосистеми також входять фактчекінгові проєкти низки українських медіа та НГО: «По той бік новин» [4], ініціативи Detector Media [5], а також регіональні й тематичні команди, що спеціалізуються на окремих видах дезінформації. Вони відіграють важливу роль у моніторингу соцмереж, оперативній перевірці вкидів і поширенні матеріалів медіаграмотності. У сукупності ці проєкти формують багаторівневу систему протидії фейкам в Україні, яка поєднує експертизу, технології та суспільну просвітницьку діяльність.

Один із найстаріших та найструктурованіших підходів до автоматичного виявлення фейкових новин і маніпулятивного контенту є Rule-based системи. Вони базуються на основі заздалегідь визначених експертами правилах, шаблонах і логічних умовах, які дозволяють відфільтровувати потенційно неперевірену інформацію. Алгоритм працює за визначеним набором правил, а саме, виявленням фейків за словниками, шаблонами, структурними ознаками, типовими маркерами маніпуляцій та виявлення фейків. Ось деякі приклади правил, які використовують такі системи: 1) лінгвістичні правила: наявність емоційних маркерів: «Шок!», «Зрада!», «Сенсація!», «Шокуючі подробиці» тощо; вживання модальних конструкцій: «ймовірно», «можливо», «кажуть», «за непідтвердженими даними»; невідповідність відмінків, граматичні аномалії, що

часто зустрічаються у бот-контенті; 2) структурні правила: відсутність посилання на джерело; посилання на невідомі або сумнівні домени (наприклад, з дивними URL); хронологічні суперечності в тексті; 3) фактологічні правила: згадка організацій, подій або фактів, яких не існує; наведення неможливих фізичних параметрів (наприклад, військова техніка зі швидкістю, що суперечить реальності); метадані та технічні правила; надто часте повторення публікації в короткий проміжок часу; нетипові часові патерни (активність облікового запису вночі за київським часом); використання однотипних картинок або шаблонів бот-мереж. Rule-based системи в українському медіапросторі активно застосовуються як державними структурами, так і медіа, громадськими організаціями та волонтерськими проєктами, які займаються виявленням фейків, бот-мереж і пропагандистських вкидів. Вони працюють як окремі інструменти, так і компоненти більших аналітичних платформ.

Прикладами реалізації Rule-based системи в українському медіапросторі є фактчекінгові медіапроєкти (StopFake [2], VoxCheck [3], BezBrekhni [6]), системи моніторингу соцмереж (LetsData [7], SemanticForce [8], InfluenceMonitoring [9]); українські аналітики відкритих джерел інформації (Molfar, InformNapalm, волонтерські групи у Telegram) застосовують rule-based сценарії для відстеження фейкових акаунтів; виявлення інформаційних операцій за шаблонними слідами; визначення підозрілих джерел за ключовими поведінковими параметрами. Практичні приклади правил, характерних для автоматичного виявлення фейкових новин і маніпулятивного контенту в Україні – це лінгвістичні маркери роспропаганди («київський режим», «укронацисти», «влада кинула людей», «все програно»); наративні патерни («Захід втомився від України», «Україна капітулює», «Українці самі підірвали…»).

Гібридні методи виявлення фейкових новин поєднують у собі переваги кількох підходів – rule-based, ML та DL – для досягнення максимальної точності, швидкості та масштабованості. Система працює у багатошаровому

режимі, де кожен рівень компенсує слабкості іншого. Rule-based фільтр виявляє найочевидніші ознаки фейків: відомі пропагандистські кліше; маркери емоційної маніпуляції; шаблонні фрази бот-мереж; наративи, характерні для певних акторів. ML-класифікатор аналізує текст на основі статистичних закономірностей: структуру; лексику; схожість з уже відомими фейками. На цьому етапі відсіюється більша частина підозрілого контенту. DL-модуль виконує складні задачі: глибинний семантичний аналіз; визначення прихованих маніпуляцій; аналіз відео та зображень; виявлення дипфейків; аналіз авторського стилю. Завдяки людській перевірці контент, який моделі класифікують як «підозрілий», передають експертам-фактчекерам. Також відбувається зворотний зв'язок (feedback loop), коли експерти уточнюють оцінки; система навчається на нових прикладах; правила оновлюються; моделі стають точнішими.

Перевагами гібридного підходу є: 1) найвища точність, коли комбінація різних інструментів дає змогу виявляти як прості фейки, так і складні маніпуляції; 2) висока масштабованість, алгоритми автоматично обробляють великий потік контенту, а людина працює лише зі складними випадками; 3) стійкість до нових типів дезінформації, моделі ML/DL навчаються на нових патернах, а rule-based правила оновлюються вручну; 4) можливість роботи з мультимедіа, гібридні системи охоплюють текст, фото, відео та аудіо; 5) мінімізація помилок, нейромережі компенсують «жорсткість» правил, а люди – можливі похибки алгоритмів.

В українському медіапросторі гібридні підходи використовуються у фактчекінгових організаціях, про які вже згадувалося раніше (StopFake, VoxCheck, Рейтинг довіри, проєкти НГО), що комбінують rule-based аналіз і ML-моделі для швидкого сортування контенту; системах моніторингу соцмереж та телеграм-каналів. Волонтерські ініціативи та IT-команди використовують ML для аналізу поведінкових патернів, а експерти — для глибинної перевірки. В аналітичних центрах проєкти з аналізу

пропагандистських наративів, у яких застосовують методи машинного навчання та глибинні нейронні мережі для розпізнавання семантичних атак у російських інформаційних кампаніях. Гібридні моделі застосовують у системах раннього попередження про інформаційні атаки.

Ручний фактчекінг дає високу точність, але не масштабується; rule-based системи швидкі, але негнучкі; ML і DL демонструють високу ефективність, але залежать від якості даних. Найефективнішими виявляються гібридні моделі, які поєднують алгоритми та експертні оцінки, забезпечуючи найкращий баланс між швидкістю, точністю та надійністю. Отже, гібридні методи – це найефективніший сучасний підхід до боротьби з фейками, оскільки вони поєднують швидкість алгоритмів і точність експертів, охоплюють усі типи дезінформації, адаптуються до нових маніпуляцій, забезпечують найвищий рівень інформаційної безпеки в умовах війни.

Проблема поширення фейкових новин та інформаційних маніпуляцій в Україні набуває особливої гостроти в умовах гібридної війни та інтенсивного використання цифрових медіа. Проведений аналіз засвідчує, що ефективне протидіяння дезінформації можливе лише за умови комплексного підходу, який поєднує різні методи перевірки інформації. Ручний фактчекінг залишається важливим інструментом глибокого аналізу та підтвердження достовірності даних, однак його масштабованість є обмеженою. Rule-based системи забезпечують швидке виявлення типових пропагандистських патернів, але не завжди успішно реагують на нові чи нестандартні форми маніпуляцій.

Алгоритми машинного навчання (ML) та глибинного навчання (DL) демонструють значно вищу ефективність у виявленні прихованих змістових ознак фейків, автоматизації моніторингу великих обсягів контенту та аналізі мультимедійних матеріалів, таких як зображення та відео. Найвищі результати забезпечують гібридні (hybrid) підходи, що комбінують переваги rule-based методів, алгоритмів ML/DL та експертної ручної перевірки, створюючи багаторівневу та гнучку систему виявлення маніпуляцій.

Українські фактчекінгові ініціативи успішно застосовують змішані підходи, удосконалюючи механізми інформаційної безпеки держави. Таким чином, надефективною стратегією протидії дезінформації в сучасному медіапросторі України є інтеграція автоматизованих алгоритмів і людської експертизи, що забезпечує як масштабованість, так і високий рівень точності під час роботи з фейковими матеріалами.

Джерела та література

1. Горбань Ю. Інформаційні операції та дезінформація: методи протидії. Київ : НІСД, 2021. 64 с.
2. StopFake.org – український проєкт з перевірки фактів. URL: https://www.stopfake.org (дата звернення: 15.11.2025).
3. VoxCheck : фактчекінговий проєкт Київської школи економіки. URL: https://voxukraine.org/voxcheck (дата звернення: 15.11.2025).
4. По той бік новин. URL: https://behindthenews.ua/ (дата звернення: 15.11.2025).
5. ГО «Детектор медіа». URL: https://surl.li/yeknec (дата звернення: 15.11.2025).
6. Фактчек-проєкт «Без брехні», заснований Громадською організацією «Центр аналітики і розслідувань». URL: https://without-lie.info/ (дата звернення: 15.11.2025).
7. Прогноз ризиків і дезінформації. Український стартап LetsData URL: https://salo.li/4E94375/ (дата звернення: 15.11.2025).
8. Модуль SemanticForce. Захист від дезінформації (DRP). URL: https://semanticforce.ai/ua/products/digital-risk-protection (дата звернення: 15.11.2025).
9. InfluenceMonitoring. Моніторинг Соцмереж та ЗМІ URL: https://salo.li/2B7E80C (дата звернення: 15.11.2025).