DOI 10.34185/1562–9945–5–166–2026–13
УДК 004.056

Х.В. Ліп’яніна–Гончаренко, І.В. Ігнатєв, М.П. Комар, В.С Пойдич

ІНФОРМАЦІЙНА МОДЕЛЬ ДАНИХ, ВІДТВОРЮВАНІСТЬ І ПРОЦЕДУРНА ПІДЗВІТНІСТЬ У СИСТЕМІ МОНІТОРИНГУ ІНФОРМАЦІЙНИХ ЗАГРОЗ

Анотація. Статтю присвячено обґрунтуванню інформаційної моделі даних для систем моніторингу інформаційних загроз, орієнтованої на забезпечення відтворюваності обчислень та процедурної підзвітності. Автором запропоновано розглядати збагачений запис новинного повідомлення як єдиний чотиришаровий інтеграційний каркас. Він об’єднує первинні текстові поля, метадані джерела, оцінки аналітичних модулів (тематику, тональність, інверсію) та службові атрибути якості. Визначено технічні підстави забезпечення відтворюваності результатів через фіксацію конфігурацій і версійності компонентів. Доведено необхідність наскрізного аудитного сліду та інтеграції експертного контуру «людина–система» для аналізу чутливого контенту. Практична цінність полягає у створенні методологічної основи для побудови прозорих і підзвітних систем медіамоніторингу.
Ключові слова: інформаційна модель даних, моніторинг інформаційних загроз, відтворюваність результатів, процедурна підзвітність, аудитний слід, аналіз медіаконтенту, контур «людина–система», життєвий цикл даних

Постановка проблеми. Стрімке зростання обсягів цифрового медіаконтенту, висока швидкість оновлення новинних потоків і ускладнення форм інформаційного впливу зумовлюють потребу в створенні систем, здатних не лише автоматизовано аналізувати повідомлення, а й забезпечувати контроль якості даних, повторюваність результатів та прозорість процедур ухвалення рішень. Для задач моніторингу інформаційних загроз цього недостатньо досягати лише високих показників класифікації, оскільки практична придатність системи визначається також тим, наскільки коректно організовано дані, чи можна відтворити результат за однакових умов і чи існує аудитний слід, який дозволяє перевірити підстави автоматизованого висновку.

Особливої актуальності ця проблема набуває в умовах багатомовного та динамічного інформаційного середовища, де новинні повідомлення надходять із різних джерел, проходять різні процедури передоброблення, можуть містити перекладені або змішаномовні фрагменти та потребують послідовного проходження через кілька аналітичних модулів. За таких умов інформаційна модель даних повинна виконувати не лише функцію збереження запису, а й роль інтеграційного каркаса, який поєднує первинні текстові поля, метадані джерела, результати аналітичних модулів, службові параметри контролю якості, версійність компонентів і журнал рішень.

© Ліп’яніна-Гончаренко Х.В., Ігнатєв І.В., Комар М.П., Пойдич В.С, 2026
Copyright for this paper by its authors. Use permitted under License CC BY 4.0.
ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Аналіз останніх досліджень і публікацій. У сучасних дослідженнях, пов'язаних із моніторингом ризикового медіаконтенту, виокремлюються щонайменше чотири взаємопов'язані напрями: документування та формалізація даних, забезпечення відтворюваності експериментів, аудит і процедурна підзвітність алгоритмічних систем, а також прикладні системи виявлення неправдивих або маніпулятивних новин. Для задачі побудови системи моніторингу інформаційних загроз ці напрями є взаємодоповнювальними, оскільки якість рішення визначається не лише точністю аналітичного модуля, а й структурою запису даних, контролем життєвого циклу корпусу, можливістю повторного відтворення результатів і наявністю аудитного сліду [1]–[10].

Першу групу становлять підходи, зосереджені на структурованому описі даних і походження корпусів. У роботі E. M. Bender та B. Friedman запропоновано концепцію data statements, яка орієнтована на формалізований опис мовних даних з урахуванням їхнього соціального, мовного та прикладного контексту [1]. Подальшим розвитком цього напряму стали datasheets for datasets, у яких T. Gebru та співавтори пропонують стандартизований опис мотивації створення набору даних, його складу, процедури збирання, рекомендованих способів використання та обмежень [2]. З погляду побудови систем моніторингу інформаційних загроз такі підходи є принципово важливими, оскільки переводять корпус із рівня неформальної колекції текстів на рівень документованого об'єкта з фіксованими властивостями, проте вони зосереджені переважно на документуванні набору даних і не задають повної інформаційної моделі окремого запису новинного повідомлення, придатної до інтеграції з аналітичними модулями та журналом рішень [1], [2].

Другий близький напрям пов'язаний із документуванням моделей і систем підтримки прийняття рішень. У праці про model cards запропоновано супроводжувати моделі короткими структурованими документами, які розкривають призначення моделі, умови її застосування, показники якості та обмеження [3]. У роботі F. Königstorfer і S. Thalmann показано, що традиційної програмної документації недостатньо для перевірки систем штучного інтелекту в регульованих сценаріях, а специфічна для ШІ документація є необхідною умовою підзвітності та проходження аудиту [4]. Для нашої задачі ці підходи цінні тим, що акцентують увагу на структурованому документуванні конфігурацій, обмежень і джерел доказів, однак вони також не розв'язують повністю проблему інтегрованого представлення даних, проміжних оцінок і службових атрибутів усередині єдиного запису новинного повідомлення [3], [4].

Третю групу утворюють дослідження, присвячені відтворюваності в галузі опрацювання природної мови. У роботі I. Magnusson, N. A. Smith і J. Dodge проаналізовано 10 405 відповідей на NLP Reproducibility Checklist і показано, що після її запровадження покращилося звітування про ефективність, параметри навчання та статистичні характеристики експериментів, однак відкритість коду, даних і процедур залишається неповною [5]. У праці A. Belz, M. Popovic і S. Mille запропоновано quantified reproducibility assessment — метод кількісного оцінювання ступеня відтворюваності результатів на основі багатьох повторних відтворень [6]. Ці дослідження мають безпосе-

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

реднє значення для систем моніторингу інформаційних загроз, оскільки демонструють, що відтворюваність не може забезпечуватися декларативно і потребує фіксації параметрів запуску, редакцій компонентів, структури вибірок і протоколів оцінювання. Водночас вони орієнтовані переважно на відтворення експериментів у NLP і не деталізують побудову інформаційної моделі даних як носія технічних підстав повторного відтворення в прикладній системі моніторингу [5], [6].

Четвертий напрям стосується аудиту та процедурної підзвітності систем штучного інтелекту. У роботі J. Mökander узагальнено правові, етичні та технічні підходи до аудиту ШІ та показано, що сучасний аудит алгоритмічних систем потребує як технологічно орієнтованих, так і процесно орієнтованих підходів [7]. У дослідженні M. Minkkinen, J. Laine і M. Mäntymäki запропоновано концепцію безперервного аудиту ШІ як майже реального часу електронної системи підтримки аудиторів, яка постійно перевіряє узгодженість системи з релевантними нормами й стандартами [8]. Для задачі моніторингу інформаційних загроз ці праці є особливо важливими, оскільки вони переводять питання підзвітності з рівня загальних принципів на рівень процедур, журналів, правил ескалації та контрольованої взаємодії людини із системою. Проте в них не розглянуто спеціально питання інформаційної моделі запису новинного повідомлення як первинного носія аудитного сліду в текстоцентричних системах аналізу медіаконтенту [7], [8].

П’ятий напрям репрезентують прикладні системи виявлення неправдивих новин і пояснюваного аналізу ризикового контенту. У роботі N. Cavus, M. Goksu і B. Oktekin представлено систему FANDC, у якій автори прямо вказують на брак систем виявлення неправдивих новин, здатних функціонувати в мережевому середовищі та в режимі, наближеному до реального часу [9]. У більш новій праці W. Ji та співавторів наголошено, що значна частина наявних рішень залишається «чорними скриньками», оскільки спирається на приховану взаємодію внутрішніх ознак і не забезпечує належної пояснюваності результатів [10]. Ці системи демонструють високий рівень розвитку прикладних методів класифікації та верифікації медіаконтенту, однак їхній головний акцент зосереджено на точності виявлення, а не на структурі запису даних, життєвому циклі корпусу, версійності словників, процедурній підзвітності та механізмах відтворення рішень у межах єдиного технологічного контуру [9], [10].

Отже, аналіз наукових джерел показує, що наявні рішення сформували важливий методологічний фундамент для побудови підзвітних систем аналізу медіаконтенту: data statements і datasheets задали підходи до документування даних [1], [2]; model cards та AI–specific documentation — до структурованого опису моделей і систем [3], [4]; дослідження з відтворюваності в NLP — до фіксації умов повторного відтворення результатів [5], [6]; а праці з аудиту ШІ — до розуміння процедурної підзвітності, журналювання та безперервного контролю [7], [8]. Водночас недостатньо розробленим залишається підхід, у межах якого ці вимоги поєднуються в єдиній інформаційній моделі запису новинного повідомлення, придатній до інтеграції з аналітичними модулями, збереження проміжних оцінок, формування аудитного сліду та підтримки контуру «людина–система». Саме ця прогалина й визначає доцільність розроблення інфор-

маційної моделі даних, орієнтованої на відтворюваність і процедурну підзвітність у системі моніторингу інформаційних загроз.

Попри значну кількість праць, присвячених документуванню наборів даних, опису моделей, відтворюваності експериментів та аудиту систем штучного інтелекту [1]–[10], у наявних дослідженнях недостатньо розробленим залишається підхід, у межах якого ці вимоги поєднувалися б у єдиній інформаційній моделі запису новинного повідомлення. Зокрема, більшість відомих рішень зосереджується або на документуванні наборів даних і моделей, або на окремих аспектах повторного відтворення результатів, або на загальних принципах аудиту, однак значно меншою мірою висвітлює питання інтеграції первинних текстових полів, метаданих, проміжних аналітичних оцінок, службових атрибутів контролю якості та журналу рішень у межах одного структурованого запису.

Недостатньо дослідженими залишаються також питання організації життєвого циклу даних у системах моніторингу інформаційних загроз, де контроль якості повинен виконуватися наскрізно на етапах збирання, очищення, збереження та використання даних, а результати аналізу мають супроводжуватися редакціями словників, конфігурацій, параметрами запуску та іншими службовими ознаками, необхідними для повторного відтворення. Окремої уваги потребує і процедурна підзвітність, оскільки в більшості прикладних систем питання аудитного сліду, причин ескалації та фіксації участі експерта не інтегровані безпосередньо в інформаційну модель даних. Саме тому актуальним науково–прикладним завданням є розроблення такої інформаційної моделі, яка б поєднувала структуроване подання новинного повідомлення, механізми відтворюваності результатів і засоби формування процедурно повного аудитного сліду в межах системи моніторингу інформаційних загроз.

Мета дослідження є обґрунтування інформаційної моделі даних, механізмів забезпечення відтворюваності та принципів процедурної підзвітності в системі моніторингу інформаційних загроз. Для досягнення поставленої мети у роботі розглянуто структуру запису новинного повідомлення, життєвий цикл даних, службові поля контролю якості, параметри повторного відтворення результатів, а також роль аудитного сліду й контуру «людина–система» у перевірці та поясненні автоматизованих рішень.

Викладення основного матеріалу дослідження. У межах розроблення системи моніторингу інформаційних загроз інформаційну модель даних доцільно розглядати не як сукупність ізольованих полів, а як формалізований спосіб подання новинного повідомлення, який забезпечує його послідовне проходження через усі етапи аналітичного опрацювання, збереження проміжних і підсумкових результатів, а також можливість їх повторного відтворення. Такий підхід дає змогу перетворити сирий текстовий матеріал із зовнішнього джерела на структурований запис, у межах якого поєднуються первинні текстові поля, службові метадані, результати аналітичних модулів і технічні ознаки контролю якості. Саме в цьому полягає ключова відмінність інформаційної моделі від простого набору атрибутів: вона виконує інтеграційну функцію і забезпечує цілісність даних у межах усієї технології моніторингу.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Новинне повідомлення в такій системі доцільно трактувати як мінімально самодостатній запис, що відповідає одній публікації в новинному потоці й містить достатній набір полів для ідентифікації, інтерпретації, аналітичного опрацювання та повторного відтворення результатів. Мінімальними для такого запису є заголовок, основний текст, джерело, дата публікації, мовна мітка та посилання або ідентифікатор. Саме ці поля дозволяють локалізувати публікацію в часі, визначити її походження, обрати належний ланцюг передоброблення та пов'язати результати різних модулів у межах одного об'єкта. У структурному сенсі запис новинного повідомлення має бути організований як багатошаровий об'єкт, де перший шар відповідає за походження запису, другий — за змістове текстове подання, третій — за результати аналітичних модулів, а четвертий — за службові параметри контролю якості, журналювання й відтворюваності.

У запропонованій моделі запис новинного повідомлення доцільно поділяти на чотири функціональні групи полів. До першої групи належать поля ідентифікації та походження: message_id, source_name, source_domain, url, published_date, collected_date. Вони забезпечують цілісність запису, дають змогу здійснювати дедуплікацію, часову аналітику та контроль джерел. До другої групи належать власне текстові поля: title_original, text_original, language_code, а за потреби також title_uk і text_uk, якщо в системі використовується переклад із фіксацією оригіналу. Саме ці поля утворюють змістове ядро запису, відносно якого виконуються всі подальші аналітичні перетворення.

Третю групу становлять результати аналітичного опрацювання. До них належать thematic_label, label_is_heuristic, topic_confidence, sentiment_score, sentiment_class, inversion_applied, а в розширеному варіанті — поля, пов'язані з подальшим правовим оцінюванням ризиків. Тематична мітка не повинна трактуватися як довільна категорія: вона має бути формалізованою рубрикою, яка задає контекст для інтерпретації тональності, інверсії полярності та ризиковості повідомлення. Аналогічно результати аналізу тональності повинні зберігатися не лише у вигляді дискретного класу, а й у вигляді числового індексу, придатного до порівняння, аудиту та подальшого використання в інтегрованому аналітичному контурі. Поле, пов'язане з інверсією полярності, має відображати як факт її застосування, так і різницю між первинною та скоригованою оцінкою.

Четверта група охоплює службові ознаки контролю якості та відтворюваності. До неї належать processing_time_ms, text_hash, is_duplicate, missing_fields, а також версійні атрибути словників, конфігурацій, правил і параметрів запуску. Саме ці поля роблять запис не просто носієм аналітичного результату, а одиницею, придатною до аудиту та повторного відтворення. Наявність хешу тексту дає змогу контролювати незмінність повідомлення в оновленнях, ознака дубліката — уникати спотворення статистики потоку, а журнал відсутніх критичних полів — виявляти системні проблеми якості даних. У сукупності це означає, що інформаційна модель виконує не лише функцію зберігання, а й функцію процедурної організації всієї роботи системи.

На рис. 1 наведено модель даних і потоки між модулями системи моніторингу інформаційних загроз. Ця схема має принципове значення для логіки статті, оскільки де-

монструє, що об’єктом інтеграції в системі є не окремі алгоритми, а саме збагачений запис новинного повідомлення. Після етапів збирання, нормалізації метаданих, технічної перевірки якості та, за потреби, машинного перекладу формується єдиний запис, над яким послідовно виконуються модулі тематичної класифікації, аналізу тональності та інверсії полярності. Їхні результати не існують окремо, а інтегруються на етапі збагачення запису показниками. Таким чином, інформаційна модель забезпечує перехід від розрізнених процедур до єдиного інтегрованого конвеєра опрацювання.

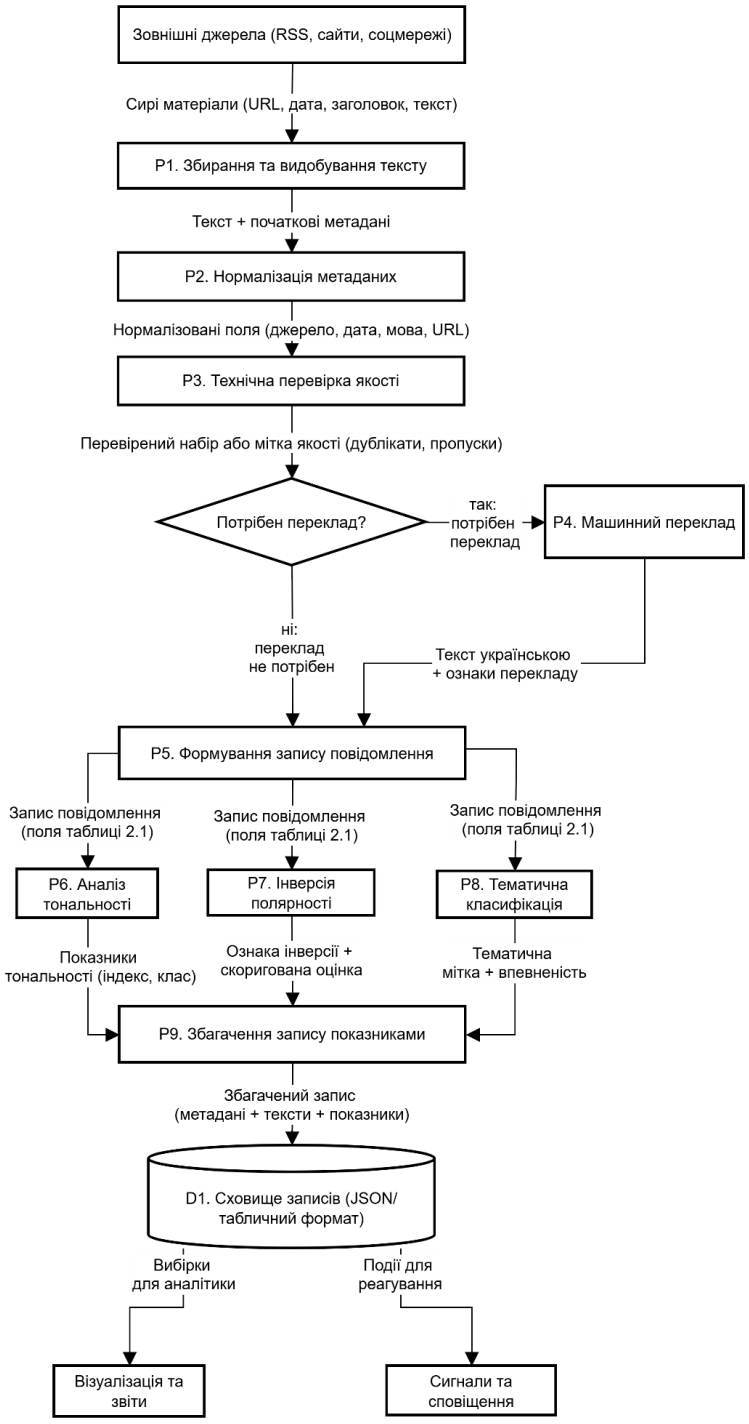


Рисунок 1 – Модель даних і потоки між модулями системи моніторингу інформаційних загроз

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Збагачений запис новинного повідомлення виконує подвійне призначення. З одного боку, він є виходом попередніх аналітичних модулів, а з іншого — виступає вхідною основою для наступних етапів, зокрема для попереднього юридичного оцінювання ризиків цифрового медіаконтенту. Саме тому інформаційну модель даних доцільно трактувати як інтеграційний каркас усієї системи моніторингу інформаційних загроз. Така постановка дозволяє відмовитися від фрагментарного зберігання результатів і перейти до цілісної структури, у якій кожне новинне повідомлення має повну історію технічного та аналітичного опрацювання. Це створює методологічну основу не лише для автоматизованого моніторингу, а й для подальшої експертної верифікації, журналювання та порівняння результатів між експериментами.

Не менш важливою складовою системи є контрольований життєвий цикл даних. На рис. 2 наведено життєвий цикл даних у системі моніторингу інформаційних загроз. Ключовою особливістю цієї схеми є те, що контроль якості не обмежується одним локальним етапом, а виконує наскрізну роль і пов’язує всі інші стадії життєвого циклу. Це означає, що перевірка дублікатів, повноти полів, мови, ознаки перекладу, типу міток і журналювання має здійснюватися не лише після збирання, а й під час очищення, перед збереженням і безпосередньо перед використанням даних у навчанні, валідації та тестуванні моделей.

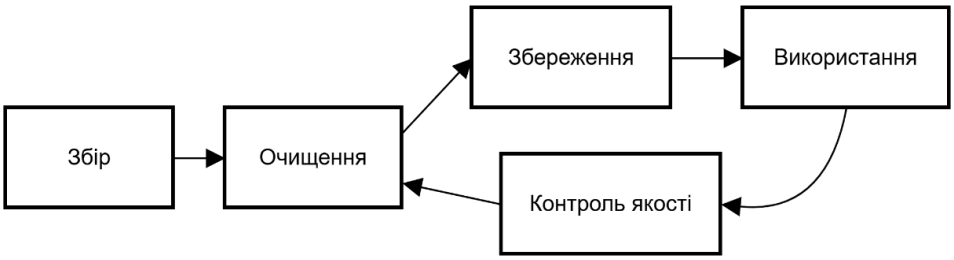


Рисунок 2– Життєвий цикл даних у системі моніторингу інформаційних загроз

Для задачі моніторингу інформаційних загроз корпус має бути не просто великим, а структурованим, простежуваним і контрольованим на всіх етапах життєвого циклу. Еталонна розмітка повинна залишатися достовірною основою для оцінювання методів, тоді як евристичні мітки можуть використовуватися лише як допоміжний інструмент масштабування. Організаційні мітки мають виконувати службову функцію керування потоком, але не повинні підміняти аналітичні класи. Саме тому контроль якості даних повинен охоплювати не лише текст, а й типи міток, часову мінливість, дрейф тем і лексики, змішування джерел без обліку та ризики, пов’язані з потенційними персональними даними. У сукупності це створює передумови не лише для коректного навчання й тестування моделей, а й для процедурно правомірного використання даних у прикладному контурі моніторингу.

Для системи моніторингу інформаційних загроз відтворюваність не може зводитися до формального повторення схожого виходу. Її слід розуміти як можливість відновити весь ланцюг обробки конкретного новинного повідомлення за фіксованих умов запуску. Саме тому система повинна зберігати значення seed для стохастичних процедур,

редакції словників, конфігурацій і правил, параметри передоброблення, дату та час запуску, редакції наборів даних, ідентифікатори навчальних і тестових підвибірок, а також журнали результатів обробки. За такого підходу відтворюваність означає, що за однакових вхідних записів, незмінних конфігурацій і фіксованих редакцій компонентів система повинна відтворювати той самий результат або мінімально допустиме відхилення, явно зафіксоване в протоколі експерименту.

У практичному вимірі це означає, що інформаційна модель даних повинна бути тісно пов'язана з механізмом версійності. Результат аналізу не може вважатися достатньо надійним, якщо неможливо встановити, якою саме редакцією словника, правила, конфігурації або моделі він був отриманий. Тому службові поля відтворюваності мають бути вбудовані безпосередньо у запис або в пов'язаний з ним журнал. Така організація дозволяє зіставляти результати між різними запусками, оцінювати вплив оновлень словників і правил, а також контролювати стабільність системи в часі. Відтворюваність у цьому випадку виступає не додатковою зручністю, а обов'язковою умовою наукової та прикладної валідності результатів моніторингу.

Не менш важливою за відтворюваність є процедурна підзвітність. Для систем такого типу вона означає, що для кожного рішення повинен бути сформований аудитний слід, який дозволяє встановити, яке саме новинне повідомлення аналізувалося, які редакції словників, конфігурацій і правил були використані, які модулі спрацювали, які значення показників було отримано на виході, які пороги або умови ескалації було активовано, а також чи було передано випадок на експертний розгляд і яке остаточне рішення ухвалено в контурі «людина–система». За відсутності такої інформації неможливо ані перевірити підстави рішення, ані коректно виконати аудит помилок.

Процедурна підзвітність у цій системі має реалізовуватися не локально, а наскрізно. Це означає, що аудитний слід формується послідовно на всіх етапах проходження запису через конвеєр: від приймання та технічної перевірки до тематичної класифікації, оцінювання тональності, фіксації інверсії полярності та подальшої ескалації. Таким чином, журнал рішень повинен накопичувати не лише кінцевий результат, а й ланцюг операцій, який до нього привів. У прикладній системі моніторингу така логіка дозволяє розмежувати технічні, аналітичні та процедурні причини помилки, а отже — створює основу для вдосконалення словників, конфігурацій, правил та критеріїв ескалації.

Для чутливих повідомлень, що можуть мати підвищений рівень ризику або суперечливі ознаки, автоматизована система не повинна завершувати цикл без участі людини. Саме тому в структурі процедурної підзвітності принципово важливим є контур «людина–система». Його роль полягає в тому, щоб у спірних, високозначущих або процедурно складних випадках автоматизоване оцінювання не підміняло експертного рішення, а лише формувало підстави для ескалації, ранжування та попереднього обґрунтування. Для цього в аудитному сліді повинні фіксуватися не лише технічні параметри, а й підстава передачі випадку на експертний розгляд, факт участі експерта та остаточний статус рішення. Така організація дозволяє поєднати переваги автоматизованого моніторингу з вимогами контролю, підзвітності й процедурної коректності.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Отже, інформаційна модель даних у системі моніторингу інформаційних загроз виконує значно ширшу функцію, ніж просто зберігання записів новинного потоку. Вона поєднує в межах одного об'єкта первинні характеристики повідомлення, результати модулів аналітичного опрацювання та службові метадані, необхідні для контролю якості, процедурної підзвітності та відтворюваності. У зв'язку з цим її доцільно трактувати як інтеграційний каркас усієї системи. Саме така структура робить можливими повний життєвий цикл даних, повторне відтворення результатів, формування аудитного сліду та підтримку експертної ескалації в контурі «людина–система».

Висновки. У статті обґрунтовано, що інформаційна модель даних у системі моніторингу інформаційних загроз має розглядатися як формалізований спосіб подання новинного повідомлення, який забезпечує послідовне проходження даних через модулі системи, збереження проміжних і підсумкових результатів та можливість повторного відтворення обчислень. Показано, що така модель має поєднувати первинні текстові поля, метадані джерела, результати тематичної класифікації, аналізу тональності та інверсії полярності, а також службові параметри контролю якості й технічного супроводу.

Встановлено, що ключовою перевагою запропонованого підходу є організація збагаченого запису новинного повідомлення як єдиного інтеграційного об'єкта, відносно якого узгоджуються всі етапи опрацювання даних. Це дозволяє забезпечити зв'язок між етапами приймання, очищення, мовної обробки, тематичної рубрикації, оцінювання тональності, фіксації інверсії полярності та подальшого попереднього юридичного оцінювання ризиків цифрового медіаконтенту. Отже, інформаційна модель виконує функцію інтеграційного каркаса всієї системи моніторингу інформаційних загроз.

Показано, що відтворюваність результатів у таких системах має забезпечуватися не декларативно, а через фіксацію конкретних технічних підстав отримання результату, зокрема редакцій словників, правил, конфігурацій, параметрів передоброблення, часових міток запуску, хешів тексту та ідентифікаторів вибірок. Такий підхід створює умови для повторного запуску системи в однакових умовах, коректного порівняння результатів між експериментами та контролю впливу оновлень компонентів на підсумкові оцінки.

Обґрунтовано, що процедурна підзвітність системи повинна реалізовуватися через наскрізний аудитний слід, який формується на всіх етапах проходження повідомлення через конвеєр обробки. Аудитний слід має фіксувати не лише кінцевий результат, а й вхідні дані, активовані правила, редакції компонентів, проміжні оцінки модулів, причини ескалації та остаточний статус рішення. Саме така організація забезпечує можливість перевірки підстав автоматизованого висновку, аналізу помилок і вдосконалення системи на основі контрольованих процедур.

Визначено, що для чутливих повідомлень обов'язковим елементом системи є контур «людина–система», у межах якого автоматизоване оцінювання не підміняє експертного рішення, а виконує функцію попереднього відбору, ранжування та аргументованої ескалації. Це дозволяє поєднати переваги автоматизованого моніторингу з

вимогами контролю, підзвітності та процедурної коректності, що є особливо важливим у задачах аналізу інформаційних загроз у новинних потоках.

Практичне значення одержаних результатів полягає в тому, що запропоновані підходи до побудови інформаційної моделі даних, організації життєвого циклу даних, забезпечення відтворюваності та формування аудитного сліду можуть бути використані як методологічна й програмно–організаційна основа для створення підзвітних систем моніторингу інформаційних загроз у динамічному багатомовному інформаційному середовищі.

ЛІТЕРАТУРА

1. Bender, E. M., & Friedman, B. (2018). Data statements for natural language processing: Toward mitigating system bias and enabling better science. *Transactions of the Association for Computational Linguistics, 6,* 587–604. doi:10.1162/tacl_a_00041.

2. Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé III, H., & Crawford, K. (2021). Datasheets for datasets. Communications of the ACM, 64(12), 86–92. doi:10.1145/3458723.

3. Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I. D., & Gebru, T. (2019). Model cards for model reporting. In Proceedings of the Conference on Fairness, Accountability, and Transparency (pp. 220–229). doi:10.1145/3287560.3287596.

4. Königstorfer, F., & Thalmann, S. (2022). AI documentation: A path to accountability. *Journal of Responsible Technology, 11,* 100043. doi:10.1016/j.jrt.2022.100043.

5. Magnusson, I., Smith, N. A., & Dodge, J. (2023). Reproducibility in NLP: What have we learned from the checklist? In *Findings of the Association for Computational Linguistics: ACL 2023* (pp. 12789–12811). Association for Computational Linguistics.

6. Belz, A., Popovic, M., & Mille, S. (2022). Quantified reproducibility assessment of NLP results. In *Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)* (pp. 16–28). Association for Computational Linguistics.

7. Mökander, J. (2023). Auditing of AI: Legal, ethical and technical approaches. *Digital Society, 2,* Article 49. doi:10.1007/s44206–023–00074–y.

8. Minkkinen, M., Laine, J., & Mäntymäki, M. (2022). Continuous auditing of artificial intelligence: A conceptualization and assessment of tools and frameworks. *Digital Society, 1,* Article 21. doi:10.1007/s44206–022–00022–2.

9. Cavus, N., Goksu, M., & Oktekin, B. (2024). Real–time fake news detection in online social networks: FANDC cloud–based system. Scientific Reports, 14, Article 25954. doi:10.1038/s41598–024–76102–9.

10. Ji, W., Lv, H., Zhao, H., et al. (2026). Explainable multi–granularity attribution reasoning framework for fake news detection. *npj Artificial Intelligence, 2,* Article 38. doi:10.1038/s44387–026–00093–3.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

REFERENCES

1. Bender, E. M., & Friedman, B. (2018). Data statements for natural language processing: Toward mitigating system bias and enabling better science. Transactions of the Association for Computational Linguistics, 6, 587–604. doi:10.1162/tacl_a_00041.
2. Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé III, H., & Crawford, K. (2021). Datasheets for datasets. Communications of the ACM, 64(12), 86–92. doi:10.1145/3458723.
3. Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I. D., & Gebru, T. (2019). Model cards for model reporting. In Proceedings of the Conference on Fairness, Accountability, and Transparency (pp. 220–229). doi:10.1145/3287560.3287596.
4. Königstorfer, F., & Thalmann, S. (2022). AI documentation: A path to accountability. Journal of Responsible Technology, 11, 100043. doi:10.1016/j.jrt.2022.100043.
5. Magnusson, I., Smith, N. A., & Dodge, J. (2023). Reproducibility in NLP: What have we learned from the checklist? In Findings of the Association for Computational Linguistics: ACL 2023 (pp. 12789–12811). Association for Computational Linguistics.
6. Belz, A., Popovic, M., & Mille, S. (2022). Quantified reproducibility assessment of NLP results. In Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers) (pp. 16–28). Association for Computational Linguistics.
7. Mökander, J. (2023). Auditing of AI: Legal, ethical and technical approaches. Digital Society, 2, Article 49. doi:10.1007/s44206–023–00074–y.
8. Minkkinen, M., Laine, J., & Mäntymäki, M. (2022). Continuous auditing of artificial intelligence: A conceptualization and assessment of tools and frameworks. Digital Society, 1, Article 21. doi:10.1007/s44206–022–00022–2.
9. Cavus, N., Goksu, M., & Oktekin, B. (2024). Real–time fake news detection in online social networks: FANDC cloud–based system. Scientific Reports, 14, Article 25954. doi:10.1038/s41598–024–76102–9.
10. Ji, W., Lv, H., Zhao, H., et al. (2026). Explainable multi–granularity attribution reasoning framework for fake news detection. npj Artificial Intelligence, 2, Article 38. doi:10.1038/s44387–026–00093–3.

Received 17.06.2026.
Accepted 17.08.2026.
Published 30.10.2026

Data information model, reproducibility and procedural accountability in the information threat monitoring system

Analysis of recent research and publications. Scientific papers on countering disinformation distinguish approaches to documenting datasets via data statements and datasheets (E. Bender, T. Gebru), as well as models via model cards (M. Mitchell). Reproducibility in NLP systems has been studied by I. Magnusson and A. Belz, while continuous AI auditing has been addressed by J. Mökander and M. Minkkinen. However, existing publications lack an approach that integrates reproducibility, analytical assessment logging, and an audit trail directly within a unified information model of an individual message record.

The aim of the study is to substantiate a comprehensive data information model, mechanisms for ensuring computational reproducibility, and principles for building end–to–end procedural accountability in applied information threat monitoring systems.

Main body of the research. The paper proposes to consider the information model as the integration framework of the media monitoring system. An enriched news message record, structured as a four–layer object, is chosen as the modeling target. The first layer covers identification and origin fields (IDs, URLs, dates). The second layer contains primary text fields and language tags for both original and translated text. The third layer integrates the outputs of analytical modules: thematic rubrics, sentiment scores, and polarity inversion flags. The fourth layer accumulates service quality and technical support attributes (text hash, duplicate flags, versions of dictionaries, and configurations). The end–to–end data lifecycle is structured so that quality control links all stages from collection to utilization. The technical foundation for the reproducibility of results is defined as the mandatory capturing of seed values, model configurations, and linguistic resource versions in the system log. Procedural accountability is implemented via an end–to–end audit trail that records the processing chain of a message. To minimize risks when handling sensitive content, the integration of a human–in–the–loop expert architecture is substantiated, where the final decision is made and logged incorporating expert validation.

Conclusions. The study proves that the effectiveness of monitoring systems depends on the transparency and verifiability of the data architecture. The proposed information model ensures a transition from fragmented storage to a holistic integration pipeline. Capturing the technical parameters of data processing guarantees full reproducibility of results under identical conditions. The end–to–end audit trail and the expert loop provide the necessary conditions for verifying automated conclusions, distinguishing between errors, and continuously improving the system. The practical value lies in establishing a methodological framework for developing accountable information threat mitigation systems.

Keywords: data information model, information threat monitoring, reproducibility of results, procedural accountability, audit trail, media content analysis, human–in–the–loop, data lifecycle.

Ліп'яніна–Гончаренко Христина Володимирівна – доктор технічних наук, доцент кафедри інформаційно–обчислювальних систем і управління, Західноукраїнський національний університет, м. Тернопіль.
ORCID: https://orcid.org/0000–0002–2441–6292
Ігнатєв Ігор Васильович – викладач кафедри кібербезпека, Західноукраїнський національний університет, м. Тернопіль.
ORCID: https://orcid.org/0000–0003–0729–9247
Комар Мирослав Петрович – д.т.н., професор кафедри інформаційно–обчислювальних систем і управління, Західноукраїнський національний університет, м. Тернопіль.
ORCID: https://orcid.org/0000–0001–6541–0359

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Пойдич Владислав Сергійович – викладач кафедри інформаційно–обчислювальних систем і управління, Західноукраїнський національний університет, м. Тернопіль.
ORCID: https://orcid.org/0009–0007–5290–051X

Lipianina–Honcharenko Khrystyna Volodymyrivna – doctor of technical sciences, associate professor at the department of information computer systems and control, West Ukrainian National University, Ternopil.
ORCID: https://orcid.org/0000–0002–2441–6292

Ihnatyev Ihor Vasylovych – lecturer at the department of cybersecurity, West Ukrainian National University, Ternopil.
https://orcid.org/0000–0003–0729–9247

Komar Myroslav Petrovych – doctor of technical sciences, professor at the department of information computer systems and control, West Ukrainian National University, Ternopil.
ORCID: https://orcid.org/0000–0001–6541–0359

Poidych Vladyslav Serhiiovych – lecturer at the department of information computer systems and control, West Ukrainian National University, Ternopil.
ORCID: https://orcid.org/0009–0007–5290–051X