https://doi.org/10.31891/2219-9365-2023-74-31
УДК 044

Мирослав КОМАР
Західноукраїнський національний університет
https://orcid.org/0000-0001-6541-0359
e-mail: mko@wunu.edu.ua
Христина ЛІП'ЯНІНА-ГОНЧАРЕНКО
Західноукраїнський національний університет
https://orcid.org/0000-0002-2441-6292
e-mail: kh.lipianina@wunu.edu.ua
Іван КІТ
Західноукраїнський національний університет
https://orcid.org/0000-0002-4526-0020
e-mail: kitivan400@gmail.com
Роман МАДАРАШ
Західноукраїнський національний університет
https://orcid.org/0009-0008-6814-5552
e-mail: madarash.roman.1998@gmail.com
Христина ЮРКІВ
Західноукраїнський національний університет
https://orcid.org/0009-0007-4917-3251
e-mail: kh.yurkiv@wunu.edu.ua

ІНТЕЛЕКТУАЛЬНИЙ МЕТОД ВИЯВЛЕННЯ ДЖЕРЕЛ МУЛЬТИЛІНГВАЛЬНОЇ ДЕЗІНФОРМАЦІЇ

У сучасному світі проблема дезінформації набуває особливої актуальності, адже фейкові новини можуть мати серйозний вплив на громадську думку та політичні процеси. У даній статті представлено розроблений інтелектуальний метод виявлення джерел мультилінгвальної дезінформації, що публікуються в інтернеті. Метод базується на застосуванні алгоритмів машинного навчання та технологій обробки природної мови для аналізу тексту, векторизації, визначення схожості текстів та класифікації. Особливістю методу є його здатність працювати в режимі реального часу, адаптуватися до нових форматів дезінформації та проводити аналіз текстів на різних мовах. В статті детально описані основні етапи розробленого методу, його структура та порівняння з існуючими аналогами. Результати роботи можуть бути корисними для вчених, що займаються проблемами виявлення дезінформації, а також для розробників систем моніторингу та аналізу контенту в соціальних мережах та інших платформах.

Ключові слова: дезінформація, фейкові новини, машинне навчання.

Myroslav KOMAR
West Ukrainian National University
Khrystyna LIPIANINA-HONCHARENKO
West Ukrainian National University
Ivan KIT
West Ukrainian National University
Roman MADARASH
West Ukrainian National University
Khrystyna YURKIV
West Ukrainian National University

INTELLIGENT METHOD OF DETECTING SOURCES OF MULTILINGUAL MISINFORMATION

In today's world, the issue of disinformation is becoming particularly relevant, as fake news can have a serious impact on public opinion and political processes. This paper introduces a developed Intellectual method of identifying sources of multilingual disinformation published on the internet. The method is based on the application of machine learning algorithms and natural language processing technologies for text analysis, vectorization, text similarity determination, and classification. A distinctive feature of the method is its ability to operate in real-time, adapt to new formats of disinformation, and analyze texts in different languages. The paper details the main stages of the developed method, its structure, and comparisons with existing analogs. The results of the work may be useful for scientists dealing with disinformation detection issues, as well as for developers of monitoring and content analysis systems on social networks and other platforms.

Keywords: disinformation, fake news, machine learning.

Постановка проблеми у загальному вигляді
та її зв'язок із важливими науковими чи практичними завданнями

Проблема дезінформації є глобально визнаною, особливо в контексті війни в Україні та росії як основного розповсюджувача фейкових новин. Росія систематично використовує маніпуляцію інформацією як інструмент у своїй агресії проти України, як підтверджено Радою Європейського Союзу [1]. Однією з ключових стратегій боротьби з дезінформацією є відкрита розвідувальна інформація, яка може бути важливою у виявленні та контролювання неправдивої інформації під час української війни [2].

Тактики "заперечення, відхилення та відволікання" використовуються росією для поширення дезінформації про війну в Україні. Організація перевірки фактів StopFake.org в Україні відіграла важливу роль у викритті багатьох з цих хибних наративів [3].

Аналітичні навички міркування виявилися корисними для виявлення дезінформації, особливо в Україні, де існує велика кількість пропаганди на користь росії [4]. Державний департамент США також вказав на декілька російських військових та розвідувальних організацій, які займаються інформаційним протистоянням, спрямованим на Україну, з метою показати Україну та її посадовців як агресорів, намагаючись вплинути на Західні країни та виправдати російську військову діяльність в Україні [5].

Отже, актуальність даного дослідження визначається розповсюдженням дезінформації, особливо в контексті війни в Україні, та необхідністю розробки інтелектуальних методів для виявлення джерел дезінформації з метою протидії стратегічним маніпуляціям, що здійснюються основним розповсюджувачем фейків на різних мовах.

Аналіз досліджень та публікацій

Протягом останніх п'яти років зафіксовано значний прогрес у вивченні та виявленні фейкових новин та дезінформації в соціальних медіа, підкреслюючи важливість цього дослідницького напрямку, застосовано різноманітні методи та технології для аналізу цього явища. Наприклад, в статті [6], авторами проаналізовано фейкові новини та дезінформацію в соціальних медіа з різних точок зору, вказуючи на переваги та недоліки деяких підходів. У той час, у статті [7] розглянуто використання алгоритмів машинного навчання для виявлення фейкових новин, акцентуючи на важливості цього підходу для вирішення проблеми, та показано ефективність багатошарового персептрону (точність виявлення - 8 з 10 фальшивих новин).

У ряді дослідженнях запропоновано інноваційні методи для аналізу та класифікації фейкових новин. Наприклад, авторами статті [8] запропоновано використовувати глибокі структуровані семантичні моделі (DSSM) та покращені рекурентні нейронні мережі для класифікації та ідентифікації фейкових новин в соціальній мережі X (Twitter) з точністю 99%. Majbouri Yazdi та співавторами [9] запропоновано підхід, що базується на K-means та Support Vector Machine, для поліпшення виявлення фейкових новин, показано, що запропонований метод показав кращі результати, ніж порівняльний метод, що базується на вилученні ознак.

Багато дослідників акцентують увагу на використанні штучного інтелекту та глибокого навчання для виявлення дезінформації. У статті [10] продемонстровано тематичний аналіз використання штучного інтелекту в автоматичному виявленні дезінформації, вказуючи на перспективи його використання в автоматичному виявленні фейкових новин. Tanvir та співавтори [11] працювали над використанням алгоритмів машинного та глибокого навчання для виявлення фейкових новин, створюючи модель, яку можуть використовувати користувачі соціальних мереж. Водночас Zhang і співавтори [12] представили BDANN, BERT-Based Domain Adaptation Neural Network, для багатомодального виявлення фейкових новин, демонструючи відмінні результати у порівнянні з іншими сучасними моделями, хоча зауважили, що використання малої кількості навчальних даних призводить до гірших результатів. Авторами статті [13] було представлено систему EXMULF для пояснення виявлення фейкових новин на основі мультимодального вмісту. Впровадження використання двонаправленої LSTM-рекурентної нейронної мережі для виявлення фейкових новин було представлено у [14]. Автори [15] працювали над виявленням фейкових новин за допомогою капсульних нейронних мереж.

Найближчими аналогами до даного дослідження є наступні роботи. В статті [16] описано серію класифікаторів, розроблених для аналізу мовних ознак у різних типах статей з фальшивими новинами, аналізу "клікабельності" заголовків дезінформації, та, нарешті, детальної верифікації дезінформації на основі Natural Language Inference. У статті [17] представлено метод DISCO, який має досягнення у автоматичному виявленні дезінформації з різних аспектів. У статті [18] описано метод автоматизованого виявлення дезінформації та інших типів помилкової інформації на різних соціальних та цифрових медіа-платформах. Інша стаття [19] описує дослідницькі зусилля по розробці моделей виявлення фальшивих новин та дезінформації, орієнтованих на мінімізацію перебоїв у ланцюгах постачання, за допомогою штучного інтелекту та машинного навчання.

Запропонований нами метод відрізняється від інших підходів завдяки своїй здатності працювати в режимі реального часу, ефективно виявляючи групи фейкової інформації, написаної різними мовами. Це

досягається завдяки використанню передових технологій обробки природної мови та інноваційних алгоритмів машинного навчання, які дозволяють системі проводити глибокий аналіз текстових даних з різноманітних джерел. Після ідентифікації груп фейкової інформації запропонований метод проводить кластеризацію цих груп для їх подальшого аналізу та виявлення джерел дезінформації. Цей підхід не тільки дозволяє виявляти фейки, але й адаптувати систему до нових форм дезінформації через перенавчання моделі на нових даних. Така структура забезпечує можливість постійно реагувати на зміни у сфері дезінформації, підтримуючи високий рівень точності та ефективності виявлення фейкової інформації в реальному часі.

Новизна запропонованого підходу полягає в здатності працювати в режимі реального часу, ефективно виявляючи та кластеризуючи групи фейкової інформації, написаної різними мовами, та перенавчаючи систему для постійної адаптації до нових форм дезінформації.

Формулювання цілей статті

Метою цієї статті є розробка інтелектуального методу виявлення джерел мультилінгвальної дезінформації. Метод має бути спроможним ідентифікувати та аналізувати фейкову інформацію в реальному часі, враховуючи мовні та контекстуальні особливості різних інформаційних джерел різними мовами. Для досягнення поставленої мети потрібно виконати наступні задачі:

- Розробити метод виявлення дезінформації, що базується на аналізі мультилінгвальних текстових даних з різних джерел та їх подальшої кластеризації для виявлення груп фейкової інформації.
- Представити структуру розробленого методу, вказавши на ключові компоненти та їх взаємодію у процесі виявлення та аналізу дезінформації.
- Здійснити детальне порівняння розробленого методу з існуючими аналогами, вказавши на переваги та недоліки кожного підходу, та підкреслити унікальні характеристики та переваги запропонованого методу в контексті ефективного виявлення дезінформації.

Виклад основного матеріалу

Відповідно, розробка ефективних методів виявлення та боротьби з дезінформацією є ключовим завданням для забезпечення інформаційної безпеки та стабільності. У цьому контексті пропонується інтелектуальний метод виявлення джерел мультилінгвальної дезінформації в режимі реального часу. Метод базується на комбінації передових технологій обробки природної мови та машинного перекладу, машинного навчання та аналітики великих даних, який має на меті виявити та аналізувати фейкову інформацію, ідентифікувати її джерела та адаптуватися до стратегій поширення дезінформації, що постійно змінюються.

На рисунку 1 представлено структуру запропонованого методу у вигляді сукупності наступних кроків:

Крок 1. Збір даних (блок 1). Збір даних є критично важливим етапом в процесі розробки методу для виявлення дезінформації. Правильно зібрані та структуровані дані дозволяють ефективно тренувати моделі машинного навчання та проводити аналітику. Розглянемо більш детальний опис цього кроку:

1.1. Збір текстових даних .

1.1.1. Визначення джерел. Визначення джерел для збору даних є важливим завданням. Джерела можуть включати новинні портали, соціальні мережі, блоги, форуми та інші платформи, де користувачі можуть публікувати або ділитися інформацією.

1.1.2. Автоматизація збору даних [20]. Розробка скриптів або використання існуючих інструментів для автоматичного збору даних. Це може включати веб-скрапінг, API запити до соціальних мереж та інше.

1.1.3. Фільтрація та валідація. Процес фільтрації та валідації даних для забезпечення їх якості та відповідності вимогам дослідження.

1.2. Збір метаданих.

1.2.1. Інформація про авторів. Збір даних про авторів текстів може включати інформацію про їхні профілі, історію публікацій, кількість підписників та інші соціальні показники, які можуть бути корисними для аналізу.

1.2.2. Інформація про джерела. Збір інформації про джерела текстів, таких як URL, дата публікації, кількість переглядів, лайків, коментарів та інші показники, які можуть бути важливими для аналізу контексту та популярності публікацій.

1.2.3. Структурування метаданих. Організація зібраних метаданих у структуровані бази даних для легкого доступу та аналізу в наступних етапах дослідження.

Цей крок закладає основу для подальшого аналізу та обробки даних, адже якість вихідних даних впливає на точність та ефективність всього методу виявлення дезінформації.

Крок 2. Попередня обробка даних (блок 2). Попередня обробка даних є фундаментальним етапом у процесі аналізу текстової інформації. Цей крок включає в себе різноманітні техніки та методи, які допомагають підготувати зібрані дані для подальшого аналізу. Ось більш деталізований опис цього кроку:

2.1. Використання бібліотек для обробки природної мови [21, 22].

2.1.1. Токенізація [23]. Процес розбиття тексту на окремі слова, фрази, символи або інші значущі елементи, називаються токенами. Це допомагає у подальшому аналізі та обробці тексту.

2.1.2. Стемінг [24]. Процес видалення суфіксів, префіксів та інфіксів зі слів для повернення їх до їхньої основи. Це полегшує виявлення спільних тем та патернів у тексті.

2.1.3. Тегування частин мови. Процес визначення частин мови кожного слова у тексті, що може бути корисним для синтаксичного аналізу та визначення семантичних відносин між словами.

2.1.4. Розпізнавання іменованих сутностей (Named Entity Recognition). Визначення та класифікація іменованих сутностей у тексті, таких як імена осіб, організацій, місцезнаходжень тощо.

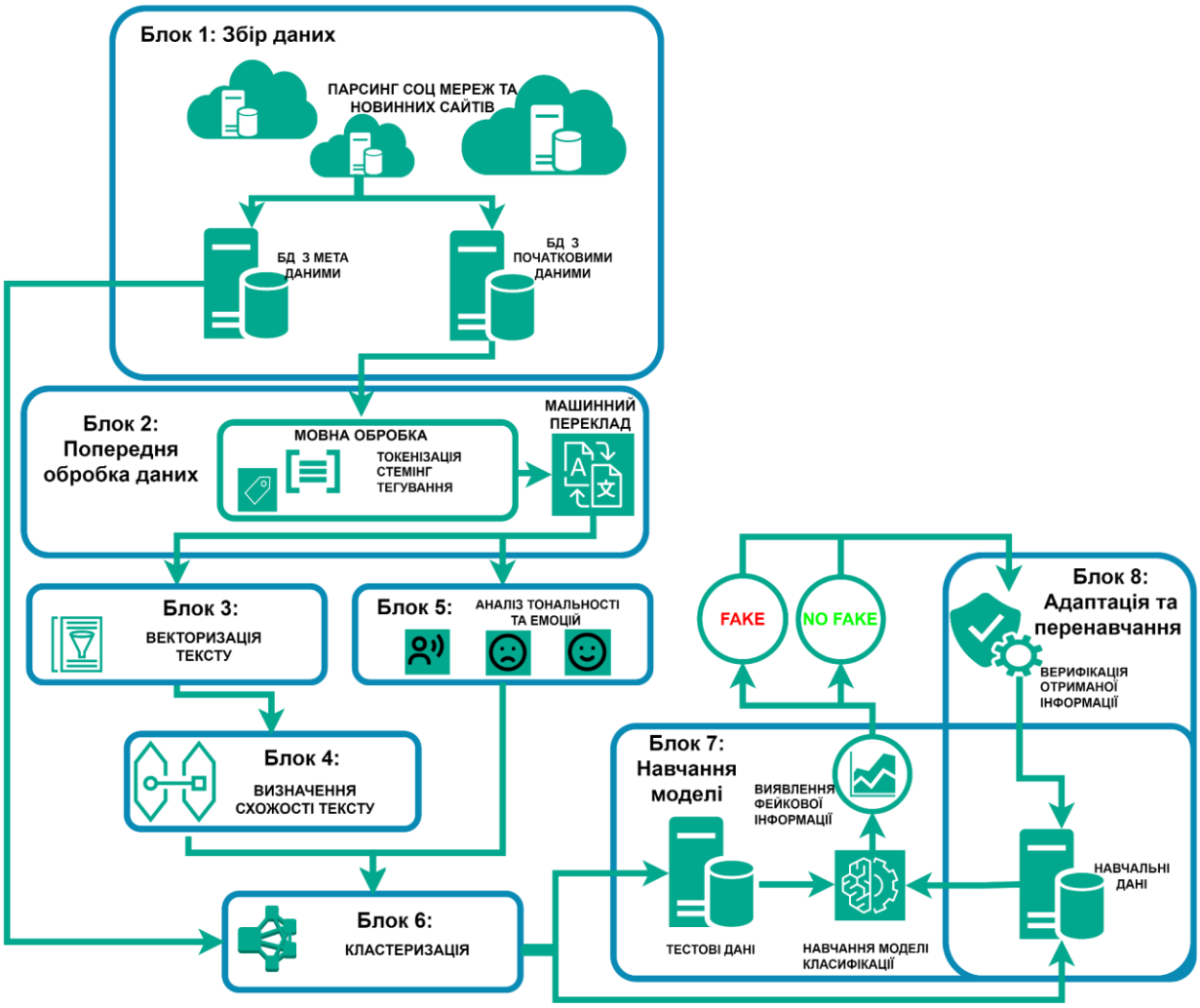

Рис.1. Структура інтелектуального методу виявлення джерел мультилінгвальної дезінформації

2.2. Переклад тексту на загальну мову.

2.2.1. Вибір мови для уніфікації. Важливо визначити мову, на яку буде перекладено весь текст, щоб забезпечити консистентність даних. Зазвичай вибирають англійську мову через її загальноприйнятість у науковому середовищі.

2.2.2. Машинний переклад. Використання автоматизованих інструментів перекладу, таких як Google Translate API або інші відкриті бібліотеки машинного перекладу для перекладу тексту на вибрану мову.

2.2.3. Валідація перекладу. Перевірка якості перекладу за допомогою додаткових інструментів або експертної оцінки, щоб забезпечити точність та зрозумілість перекладеного тексту.

Цей крок спрямований на підготовку даних для подальших етапів аналізу, забезпечуючи їхню якість та консистентність, що є критично важливим для успішного виявлення дезінформації.

Крок 3. Векторизація тексту (блок 3). Векторизація тексту є важливим етапом, який перетворює текстові дані в числовий формат, зручний для аналізу та обробки за допомогою методів машинного навчання [25]. Розглянемо детальніше цей процес:

3.1. Вибір методу векторизації.

3.1.1. Word2Vec [26]. Модель навчає векторні представлення слів у багатовимірному просторі таким чином, що слова, які часто зустрічаються разом, мають близькі векторні представлення.

3.1.2. GloVe. Інший підхід до векторизації слів, який використовує як локальний, так і глобальний статистичний аналіз корпусу тексту для визначення векторних представлень слів.

3.1.3. BERT. Сучасна модель, яка використовує механізм уваги для визначення відносин між словами в тексті і може вчити глибокі контекстні представлення слів.

3.2. Процес векторизації.

3.2.1. Тренування або завантаження моделей. Моделі можна натренувати на даних або використати попередньо натреновані моделі для векторизації тексту.

3.2.2. Перетворення тексту. Застосування вибраної моделі для перетворення кожного слова в тексті в векторні представлення.

3.3. Побудова векторних представлень.

3.3.1. Векторизація слів. Отримання векторних представлень для кожного окремого слова в тексті.

3.3.2. Векторизація текстів. Агрегація векторних представлень слів для отримання векторних представлень цілих текстів. Це можна зробити за допомогою усереднення, сумування або інших методів агрегації.

Цей крок готує дані для подальшого аналізу, перетворюючи текстову інформацію у формат, зручний для використання алгоритмами машинного навчання та глибокого навчання.

Крок 4. Визначення схожості тексту (блок 4). Цей етап фокусується на визначенні схожості між різними текстами, що дозволяє групувати або зіставляти тексти на основі їхнього вмісту. Розглянемо детальний опис цього кроку:

4.1. Вибір метрики схожості.

4.1.1. Косинусна схожість. Однією з популярних метрик схожості є косинусна схожість, яка вимірює кут між двома векторами в багатовимірному просторі. Ця метрика відзначається тим, що вона враховує орієнтацію векторів, а не їхню абсолютну відстань, що є важливим при аналізі текстових даних.

4.1.2. Альтернативні метрики. Інші метрики схожості, такі як Євклідова відстань або кореляційні метрики, можуть також бути використані в залежності від конкретних вимог та особливостей даних.

4.2. Порівняння векторів.

4.2.1. Обчислення схожості. Застосування обраної метрики для обчислення схожості між векторними представленнями текстів. Це може включати порівняння кожного тексту з кожним або використання більш складних структур даних, таких як дерева пошуку або індекси схожості, для ефективного порівняння.

4.2.2. Визначення порогових значень. Встановлення порогових значень для схожості, щоб визначити, які тексти вважаються схожими. Це може бути основано на експертній оцінці або статистичному аналізі розподілу значень схожості.

Цей крок є важливим для виявлення структур та зв'язків у даних, що може бути корисним для виявлення шаблонів дезінформації та проведення подальшого аналізу.

Крок 5. Аналіз тональності та емоцій (блок 5). Аналіз тональності та емоцій є ключовим для розуміння настрою та відтінків, які містяться у текстових даних. Це може допомогти визначити, чи є текст позитивним, негативним, або нейтральним, а також виявити можливі емоційні відгуки, які можуть бути асоційовані з дезінформацією. Розглянемо більш детальний опис цього кроку:

5.1. Вибір моделей аналізу тональності та емоцій [27].

5.1.2. Готові моделі. Існує багато попередньо натренованих моделей для аналізу тональності та емоцій, таких як VADER, TextBlob, або моделі, засновані на BERT та інших глибоких нейронних мережах.

5.1.3. Кастомізовані моделі. В залежності від конкретного випадку, може бути корисним розробити та натренувати власні моделі на специфічних для задачі даних.

5.2. Аналіз тональності.

5.2.1. Обчислення тональності. Застосування моделей для визначення тональності кожного тексту, що дозволяє визначити, чи є текст позитивним, негативним, або нейтральним.

5.2.2. Інтерпретація результатів. Аналіз результатів для визначення загального настрою даних та ідентифікації можливих аномалій або зразків.

5.3. Аналіз емоцій.

5.3.1. Обчислення емоційного відтінку. Застосування моделей для визначення емоційного відтінку тексту, такого як радість, смуток, гнів, здивування, страх, тощо.

5.3.1. Інтерпретація результатів. Аналіз отриманих емоційних відтінків для визначення, як емоції можуть бути пов'язані з дезінформацією та як їх можна використати для подальшого аналізу.

Цей крок важливий для глибшого розуміння контексту та емоційного впливу текстової інформації, що може бути корисним для виявлення дезінформації та аналізу її впливу на аудиторію.

Крок 6. Кластеризація текстів (блок 6). Кластеризація текстів є важливим етапом у виявленні та аналізі дезінформації, оскільки це дозволяє знаходити групи схожих текстів та виявляти загальні шаблони або теми. Розглянемо детальніше цей крок:

6.1. Вибір методу кластеризації.

6.1.1. K-Means [28]. Алгоритм, який групує дані на основі їхньої відстані до центроїдів кластерів.

6.1.2. DBSCAN (Density-Based Spatial Clustering of Applications with Noise) [29]. Алгоритм, який групує дані на основі їхньої густини та відстані між точками.

6.1.3. Agglomerative Clustering. Ієрархічний метод, який починає з кожного об'єкта як окремого кластера та поступово об'єднує їх на основі відстані між кластерами.

6.1.4. Gaussian Mixture Models (GMM). Метод, який вважає, що дані генеруються з змішування кількох гауссівських розподілів.

6.1.5. Affinity Propagation. Алгоритм, який визначає кластери шляхом надсилання повідомлень між парами даних до тих пір, поки не буде знайдено стабільний набір кластерів.

6.1.6. Spectral Clustering. Алгоритм, який використовує власні вектори графа схожості для визначення структури кластерів.

6.2. Процес кластеризації.

6.2.1. Обчислення кластерів. Застосування обраного алгоритму кластеризації для групування текстів на основі їхньої схожості або інших ознак.

6.2.2. Визначення оптимальної кількості кластерів. Використання методів, таких як метод ліктя або силуетного коефіцієнта, для визначення оптимальної кількості кластерів.

6.3. Аналіз результатів.

6.3.1.Інтерпретація кластерів. Оцінка отриманих кластерів для визначення загальних тем або шаблонів в текстах.

6.3.1. Визначення груп текстів. Ідентифікація груп текстів з подібними ознаками, що може допомогти в подальшому аналізі та класифікації текстів.

Цей крок є важливим для розуміння структури даних та виявлення можливих шаблонів дезінформації у текстовому матеріалі.

Крок 7. Навчання моделі класифікації (блок 7). Цей крок фокусується на розробці та навчанні моделі класифікації, яка може виявляти фейкову інформацію на основі аналізу тексту та інших виявлених ознак. Детальний опис цього кроку виглядає наступним чином:

7.1. Розробка моделі класифікації.

7.1.2. Вибір архітектури моделі [30]. Визначення та вибір оптимальної архітектури моделі для задачі, що може включати логістичну регресію, дерева рішень, випадковий ліс, градієнтний бустінг, опорних векторів, нейронні мережі та інші методи.

7.1.3. Інженерія ознак. Визначення та створення ознак, які будуть використовуватися для тренування моделі, включаючи текстові ознаки, ознаки схожості, тональності, емоційні ознаки та інші виявлені ознаки.

7.2. Навчання моделі [31].

7.2.1. Розділення даних. Розділення даних на тренувальний, валідаційний та тестовий набори для оцінювання ефективності моделі.

7.2.2. Тренування моделі. Навчання моделі на тренувальному наборі даних, використовуючи відповідні методи оптимізації та функції втрат.

7.2.3. Оцінка моделі. Оцінка ефективності моделі на валідаційному та тестовому наборах даних, використовуючи метрики, такі як Accuracy, Recall, Recall, F1-Score тощо.

7.3. Оптимізація та налагодження моделі.

7.3.1. Тюнінг гіперпараметрів. Оптимізація гіперпараметрів моделі для покращення її ефективності.

7.3.2. Перехресна перевірка. Використання перехресної перевірки для отримання надійної оцінки ефективності моделі.

7.4. Інтерпретація результатів.

7.4.1. Аналіз важливості ознак. Визначення важливості кожної ознаки для класифікації та аналіз результатів для отримання інсайтів щодо впливу різних ознак на виявлення фейкової інформації.

7.4.2. Аналіз помилок. Аналіз помилок класифікації для ідентифікації областей для подальшого покращення.

Цей крок є важливим для створення надійної та ефективної системи для виявлення фейкової інформації та дезінформації.

Крок 8. Адаптація та перенавчання (блок 8). Цей етап має на меті забезпечити систему здатністю адаптуватися до еволюції та зміни форм дезінформації, що гарантує її тривалу ефективність у боротьбі з фейковими новинами [32]. Розглянемо деталі цього кроку:

8.1. Перенавчання системи.

8.1.1. Збір нових даних. Постійний збір нових даних з відкритих джерел для відображення останніх трендів та шаблонів дезінформації.

8.1.2. Оцінка потреби в перенавчанні. Аналіз поточної ефективності системи та визначення, чи виникла потреба в перенавчанні на основі нових даних.

8.1.3. Перенавчання моделі. Застосування процесу навчання моделі з використанням нових даних для адаптації моделі до нових форм дезінформації.

8.2. Оновлення моделей та алгоритмів.

8.2.1. Аналіз нових алгоритмів та технологій. Оцінка та аналіз нових алгоритмів та технологій, які можуть бути використані для покращення ефективності системи.

8.2.2. Оновлення алгоритмів. Внесення змін у алгоритми та методи, що використовуються на основі отриманих відомостей та аналізу результатів.

8.2.3. Тестування та валідація оновлених моделей. Проведення тестування та валідації оновлених моделей для забезпечення їхньої ефективності та надійності.

8.3. Моніторинг та оцінка.

8.3.1. Моніторинг ефективності системи. Постійний моніторинг ефективності системи для виявлення можливих проблем або областей для покращення.

8.3.2. Зворотній зв'язок та адаптація. Збір та аналіз зворотного зв'язку від користувачів та експертів для подальшого покращення та адаптації системи.

Цей крок є важливим для забезпечення того, щоб система постійно була актуальною та ефективною у виявленні та боротьбі з дезінформацією в довготривалій перспективі.

Таблиця 1

Порівняння з аналогами

№	Метод	Основні засади/компоненти	Висновки та результати
1 [16]	Стилістичні, семантичні, орфографічні та морфологічні особливості	Використання стилістичних, семантичних, ортографічних та морфологічних особливостей для побудови класифікаторів різних типів фейкових новин.	Стилістичні класифікатори недостатні для точного виявлення дезінформації, потрібна перевірка фактів для вірогідного спростування. Веб-додаток FactFinder показав обіцяючі покращення в автоматизації процесу перевірки фактів.
2 [17]	DISCO	Передній та задній кінці для обробки користувацьких запитів та виявлення дезінформації за допомогою графових методів машинного навчання.	Система DISCO ідентифікує виклики виявлення дезінформації та демонструє метод. Бажано, щоб майбутні системи виявлення дезінформації могли одночасно виявляти та пояснювати протягом всього циклу поширення дезінформації.
3 [18]	Виявлення дезінформації щодо COVID-19	Використання технік машинного навчання для виявлення неправдивої інформації, пов'язаної з COVID-19 на соціальних та цифрових платформах.	Деякі виклики, пов'язані з використанням публічних наборів даних про дезінформацію. Було показано, що деякі класифікатори більш чутливі до обсягу пошукових термінів. Моделі BERT показали кращі покращення на більшій частині класифікаторів порівняно з моделями вбудовування слів та речень.
4 [19]	Модель FNaD для постачальницьких ланцюгів	Використання AI та ML для фільтрації та верифікації інформації з інтернету для визначення її автентичності.	Пропонується шлях боротьби з SCD, створюючи FNaD за допомогою технік AI та ML. У майбутньому дослідження можуть сконцентруватися на більш конкретних випадках FNaD та операційних показниках в постачальницьких ланцюгах, інтегруючи їх з розширеними візуальними методами. Крім того, можна використовувати будь-який новий та ефективний алгоритм або техніку в запропонованій моделі в майбутньому.
Запропонований метод	Інтелектуальний метод глобального виявлення джерел дезінформації	Збір та попередня обробка даних, векторизація тексту, визначення схожості тексту, аналіз тональності та емоцій, кластеризація текстів, навчання моделі класифікації, адаптація та перенавчання системи.	Метод дозволяє виявляти групи фейкової інформації, написані різними мовами, у реальному часі, проводячи кластеризацію для виявлення цих груп, та перенавчання системи для постійної адаптації до змінних форм дезінформації. Система здатна реагувати на динаміку поширення фейкових новин та адаптуватися до нових форм дезінформації.

Аналізуючи порівняльну таблицю 1, можна зробити висновок, що розроблений метод відрізняється від інших аналогічних підходів декількома ключовими особливостями. Основною перевагою запропонованого методу є його здатність працювати в реальному часі та виявляти групи фейкової інформації, написані різними мовами, що дозволяє ефективно реагувати на змінний характер дезінформації. Окрім того, метод представляє собою комплексний підхід, який включає в себе кілька етапів обробки та аналізу даних, від збору інформації до адаптації та перенавчання системи на нових даних.

На відміну від інших розглянутих методів, запропонований підхід включає більш глибокий аналіз тексту, що дозволяє виявляти не тільки фейкові новини, а й групи пов'язаної фейкової інформації. Це може бути особливо корисним для виявлення та протидії масовим кампаніям дезінформації.

Отже, запропонований метод відображає сучасні тенденції у використанні технологій машинного навчання та обробки природної мови для боротьби з фейковими новинами та дезінформацією в цифровому середовищі, водночас пропонуючи унікальні особливості, які роблять його ефективним інструментом для аналізу даних у реальному часі.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Розроблений інтелектуальний метод виявлення джерел мультилінгвальної дезінформації має значний потенціал у боротьбі з розповсюдженням фейкових новин в реальному часі. Особливістю методу є його здатність адаптуватися до нових форматів дезінформації, що підтверджує його гнучкість та можливість постійного самовдосконалення. Здатність аналізувати текст на різних мовах робить цей метод універсальним та підходящим для використання на міжнародному рівні.

Порівняння з існуючими аналогами вказало на комплексність запропонованого підходу, швидкість обробки даних та ефективність у виявленні груп фейкової інформації. Більшість існуючих систем зосереджені на виявленні окремих фейкових новин, у той час як система на основі запропонованого методу цілеспрямовано виявляє групи дезінформації та адаптується до нових зразків дезінформації, що свідчить про її вищий потенціал у боротьбі з дезінформацією на глобальному рівні.

Пропонована структура методу забезпечує масштабованість та можливість інтеграції з іншими інструментами аналізу даних. Перспективи подальшого розвитку включають розширення функціоналу системи, розробку додаткових інструментів верифікації, а також співпрацю з міжнародними організаціями для обміну даними та досвідом у боротьбі з дезінформацією. Наукові дослідження в області алгоритмів виявлення дезінформації та аналізу тональності тексту можуть значно підвищити ефективність системи та її внесок у боротьбу з глобальним розповсюдженням дезінформації.

Література

1. Disinformation and Russia’s war of aggression against Ukraine. Organisation for Economic Co-Operation and Development (OECD), 2022. URL: https://doi.org/10.1787/37186bde-en
2. Open source intelligence key to fighting Russian disinformation during Ukraine war. *Tech Monitor*. URL: https://techmonitor.ai/technology/emerging-technology/open-source-intelligence-ukraine-war
3. Zabjek A. 'Deny, deflect, distract': How Russia spreads disinformation about the war in Ukraine | CBC News. *CBC*. URL: https://www.cbc.ca/news/politics/disinformation-ukraine-stop-fake-org-1.6721522
4. How to fight pro-Russia disinformation in Ukraine | MIT Sloan. *MIT Sloan*. URL: https://mitsloan.mit.edu/ideas-made-to-matter/how-to-fight-pro-russia-disinformation-ukraine
5. Fact vs. Fiction: Russian Disinformation on Ukraine - United States Department of State. *United States Department of State*. URL: https://www.state.gov/fact-vs-fiction-russian-disinformation-on-ukraine/
6. Aïmeur E., Amri S., Brassard G. Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining*. 2023. T. 13, № 1. URL: https://doi.org/10.1007/s13278-023-01028-5
7. Sharma V. Machine Learning Algorithms via Detection of Fake News. *International Journal for Research in Applied Science and Engineering Technology*. 2020. T. 8, № 6. C. 780–784. URL: https://doi.org/10.22214/ijraset.2020.6125
8. Jadhav S. S., Thepade S. D. Fake News Identification and Classification Using DSSM and Improved Recurrent Neural Network Classifier. *Applied Artificial Intelligence*. 2019. T. 33, № 12. C. 1058–1068. URL: https://doi.org/10.1080/08839514.2019.1661579
9. Kasra Majbouri Yazdi, Adel Majbouri Yazdi, Saeid Khodayi, Jingyu Hou, Wanlei Zhou, & Saeed Saedy. (2020). Improving Fake News Detection Using K-means and Support Vector Machine Approaches. International Journal of Electrical, Electronic and Communication Sciences, 13.0(2). https://doi.org/10.5281/zenodo.3669287
10. Santos F. C. C. Artificial Intelligence in Automated Detection of Disinformation: A Thematic Analysis. *Journalism and Media*. 2023. T. 4, № 2. C. 679–687. URL: https://doi.org/10.3390/journalmedia4020043
11. Detecting Fake News using Machine Learning and Deep Learning Algorithms / Abdullah-All-Tanvir та ін. *2019 7th International Conference on Smart Computing & Communications (ICSCC)*, Sarawak, Malaysia, Malaysia, 28–30 June 2019. 2019. URL: https://doi.org/10.1109/icscc.2019.8843612

12. BDANN: BERT-Based Domain Adaptation Neural Network for Multi-Modal Fake News Detection / T. Zhang та ін. *2020 International Joint Conference on Neural Networks (IJCNN)*, м. Glasgow, United Kingdom, 19–24 лип. 2020 р. 2020. URL: https://doi.org/10.1109/ijcnn48605.2020.9206973

13. Amri S., Sallami D., Aïmeur E. EXMULF: An Explainable Multimodal Content-Based Fake News Detection System. *Foundations and Practice of Security*. Cham, 2022. С. 177–187. URL: https://doi.org/10.1007/978-3-031-08147-7_12

14. Bahad P., Saxena P., Kamal R. Fake News Detection using Bi-directional LSTM-Recurrent Neural Network. *Procedia Computer Science*. 2019. Т. 165. С. 74–82. URL: https://doi.org/10.1016/j.procs.2020.01.072

15. Goldani M. H., Momtazi S., Safabakhsh R. Detecting fake news with capsule neural networks. *Applied Soft Computing*. 2021. Т. 101. С. 106991. URL: https://doi.org/10.1016/j.asoc.2020.106991

16. Pathak A., Srihari R. K., Natu N. Disinformation: analysis and identification. *Computational and Mathematical Organization Theory*. 2021. Т. 27, № 3. С. 357–375. URL: https://doi.org/10.1007/s10588-021-09336-x

17. DISCO: Comprehensive and Explainable Disinformation Detection / D. Fu та ін. *CIKM '22: The 31st ACM International Conference on Information and Knowledge Management*, м. Atlanta GA USA. New York, NY, USA, 2022. URL: https://doi.org/10.1145/3511808.3557202

18. Alsmadi I., Rice N. M., O'Brien M. J. Fake or not? Automated detection of COVID-19 misinformation and disinformation in social networks and digital media. *Computational and Mathematical Organization Theory*. 2022. URL: https://doi.org/10.1007/s10588-022-09369-w

19. Detecting fake news and disinformation using artificial intelligence and machine learning to avoid supply chain disruptions / P. Akhtar та ін. *Annals of Operations Research*. 2022. URL: https://doi.org/10.1007/s10479-022-05015-5

20. METHOD OF CHOOSING A COMPETITIVE PRODUCT BASED ON THE EMOTIONAL COLOR OF THE CALLS / K. LIPIANINA-HONCHARENKO та ін. *Herald of Khmelnytskyi National University*. 2021. Т. 303, № 6. С. 86–88. URL: https://doi.org/10.31891/2307-5732-2021-303-6-86-88

21. Gramyak, Roman, Hrystyna Lipyanina-Goncharenko, Anatoliy Sachenko, Taras Lendyuk, and Diana Zahorodnia. "Intelligent Method of a Competitive Product Choosing based on the Emotional Feedbacks Coloring." In IntelITSIS, с. 246-257. 2021. https://ceur-ws.org/Vol-2853/paper31.pdf

22. Concept of the Intelligent Guide with AR Support / K. Lipianina-Honcharenko та ін. *International Journal of Computing*. 2022. С. 271–277. URL: https://doi.org/10.47839/ijc.21.2.2596

23. Intelligent Information System for Product Promotion in Internet Market / K. Lipianina-Honcharenko та ін. *Applied Sciences*. 2023. Т. 13, № 17. С. 9585. URL: https://doi.org/10.3390/app13179585

24. METHOD OF FORMING THE CONTEXT OF ADVERTISING AND TARGET AUDIENCE BASED ON ASSOCIATIVE RULES LEARNING / K. LIPIANINA-HONCHARENKO та ін. *Herald of Khmelnytskyi National University. Technical sciences*. 2022. Т. 313, № 5. С. 279–287. URL: https://doi.org/10.31891/2307-5732-2022-313-5-279-287

25. Intelligent Method of Forming the HR Management Short-Term Project / H. Lipyanina та ін. *Advances in Intelligent Systems and Computing*. Cham, 2020. С. 1045–1055. URL: https://doi.org/10.1007/978-3-030-63270-0_71

26. Neural Network Approach for Semantic Coding of Words / V. Golovko та ін. *Advances in Intelligent Systems and Computing*. Cham, 2019. С. 647–658. URL: https://doi.org/10.1007/978-3-030-26474-1_45

27. An Intelligent Method for Forming the Advertising Content of Higher Education Institutions Based on Semantic Analysis / K. Lipianina-Honcharenko та ін. *Communications in Computer and Information Science*. Cham, 2022. С. 169–182. URL: https://doi.org/10.1007/978-3-031-14841-5_11

28. Intelligent Method for Forming the Consumer Basket / K. Lipianina-Honcharenko та ін. *Communications in Computer and Information Science*. Cham, 2022. С. 221–231. URL: https://doi.org/10.1007/978-3-031-16302-9_17

29. Method of Forming a Training Sample for Segmentation of Tender Organizers on Machine Learning Basis. In COLINS (pp. 1843-1852), Lipyanina-Goncharenko, H., Brych, V., Sachenko, S., Lendyuk, T., Bykovyy, P., & Zahorodnia, D., 2021.

30. Method of Detecting a Fictitious Company on the Machine Learning Base / H. Lipyanina та ін. *Advances in Computer Science for Engineering and Education IV*. Cham, 2021. С. 138–146. URL: https://doi.org/10.1007/978-3-030-80472-5_12

31. Intelligent Method for Classifying the Level of Anthropogenic Disasters / K. Lipianina-Honcharenko та ін. *Big Data and Cognitive Computing*. 2023. Т. 7, № 3. С. 157. URL: https://doi.org/10.3390/bdcc7030157

32. Evaluation the Efficiency of Information Technology of Big Data Intelligence Analysis and Processing. Komar, M., Savenko, O., Sachenko, A., Lendiuk, T., Lipianina-Honcharenko, K., Hladiy, G., & Vasylkiv, N. 2022.

References

1. Disinformation and Russia's war of aggression against Ukraine. Organisation for Economic Co-Operation and Development (OECD), 2022. URL: https://doi.org/10.1787/37186bde-en
2. Open source intelligence key to fighting Russian disinformation during Ukraine war. *Tech Monitor*. URL: https://techmonitor.ai/technology/emerging-technology/open-source-intelligence-ukraine-war
3. Zabjek A. 'Deny, deflect, distract': How Russia spreads disinformation about the war in Ukraine | CBC News. *CBC*. URL: https://www.cbc.ca/news/politics/disinformation-ukraine-stop-fake-org-1.6721522
4. How to fight pro-Russia disinformation in Ukraine | MIT Sloan. *MIT Sloan*. URL: https://mitsloan.mit.edu/ideas-made-to-matter/how-to-fight-pro-russia-disinformation-ukraine
5. Fact vs. Fiction: Russian Disinformation on Ukraine - United States Department of State. *United States Department of State*. URL: https://www.state.gov/fact-vs-fiction-russian-disinformation-on-ukraine/
6. Aïmeur E., Amri S., Brassard G. Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining*. 2023. Vol. 13, no. 1. URL: https://doi.org/10.1007/s13278-023-01028-5
7. Sharma V. Machine Learning Algorithms via Detection of Fake News. *International Journal for Research in Applied Science and Engineering Technology*. 2020. Vol. 8, no. 6. P. 780–784. URL: https://doi.org/10.22214/ijraset.2020.6125
8. Jadhav S. S., Thepade S. D. Fake News Identification and Classification Using DSSM and Improved Recurrent Neural Network Classifier. *Applied Artificial Intelligence*. 2019. Vol. 33, no. 12. P. 1058–1068. URL: https://doi.org/10.1080/08839514.2019.1661579
9. Kasra Majbouri Yazdi, Adel Majbouri Yazdi, Saeid Khodayi, Jingyu Hou, Wanlei Zhou, & Saeed Saedy. (2020). Improving Fake News Detection Using K-means and Support Vector Machine Approaches. International Journal of Electrical, Electronic and Communication Sciences, 13.0(2). https://doi.org/10.5281/zenodo.3669287
10. Santos F. C. C. Artificial Intelligence in Automated Detection of Disinformation: A Thematic Analysis. *Journalism and Media*. 2023. Vol. 4, no. 2. P. 679–687. URL: https://doi.org/10.3390/journalmedia4020043
11. Detecting Fake News using Machine Learning and Deep Learning Algorithms / Abdullah-All-Tanvir et al. *2019 7th International Conference on Smart Computing & Communications (ICSCC)*, Sarawak, Malaysia, Malaysia, 28–30 June 2019. 2019. URL: https://doi.org/10.1109/icscc.2019.8843612
12. BDANN: BERT-Based Domain Adaptation Neural Network for Multi-Modal Fake News Detection / T. Zhang et al. *2020 International Joint Conference on Neural Networks (IJCNN)*, Glasgow, United Kingdom, 19–24 July 2020. 2020. URL: https://doi.org/10.1109/ijcnn48605.2020.9206973
13. Amri S., Sallami D., Aïmeur E. EXMULF: An Explainable Multimodal Content-Based Fake News Detection System. *Foundations and Practice of Security*. Cham, 2022. P. 177–187. URL: https://doi.org/10.1007/978-3-031-08147-7_12
14. Bahad P., Saxena P., Kamal R. Fake News Detection using Bi-directional LSTM-Recurrent Neural Network. *Procedia Computer Science*. 2019. Vol. 165. P. 74–82. URL: https://doi.org/10.1016/j.procs.2020.01.072
15. Goldani M. H., Momtazi S., Safabakhsh R. Detecting fake news with capsule neural networks. *Applied Soft Computing*. 2021. Vol. 101. P. 106991. URL: https://doi.org/10.1016/j.asoc.2020.106991
16. Pathak A., Srihari R. K., Natu N. Disinformation: analysis and identification. *Computational and Mathematical Organization Theory*. 2021. Vol. 27, no. 3. P. 357–375. URL: https://doi.org/10.1007/s10588-021-09336-x
17. DISCO: Comprehensive and Explainable Disinformation Detection / D. Fu et al. *CIKM '22: The 31st ACM International Conference on Information and Knowledge Management*, Atlanta GA USA. New York, NY, USA, 2022. URL: https://doi.org/10.1145/3511808.3557202
18. Alsmadi I., Rice N. M., O'Brien M. J. Fake or not? Automated detection of COVID-19 misinformation and disinformation in social networks and digital media. *Computational and Mathematical Organization Theory*. 2022. URL: https://doi.org/10.1007/s10588-022-09369-w
19. Detecting fake news and disinformation using artificial intelligence and machine learning to avoid supply chain disruptions / P. Akhtar et al. *Annals of Operations Research*. 2022. URL: https://doi.org/10.1007/s10479-022-05015-5
20. METHOD OF CHOOSING A COMPETITIVE PRODUCT BASED ON THE EMOTIONAL COLOR OF THE CALLS / K. LIPIANINA-HONCHARENKO et al. *Herald of Khmelnytskyi National University*. 2021. Vol. 303, no. 6. P. 86–88. URL: https://doi.org/10.31891/2307-5732-2021-303-6-86-88
21. Gramyak, Roman, Hrystyna Lipyanina-Goncharenko, Anatoliy Sachenko, Taras Lendyuk, and Diana Zahorodnia. "Intelligent Method of a Competitive Product Choosing based on the Emotional Feedbacks Coloring." In IntelITSIS, pp. 246-257. 2021. https://ceur-ws.org/Vol-2853/paper31.pdf
22. Concept of the Intelligent Guide with AR Support / K. Lipianina-Honcharenko et al. *International Journal of Computing*. 2022. P. 271–277. URL: https://doi.org/10.47839/ijc.21.2.2596
23. Intelligent Information System for Product Promotion in Internet Market / K. Lipianina-Honcharenko et al. *Applied Sciences*. 2023. Vol. 13, no. 17. P. 9585. URL: https://doi.org/10.3390/app13179585
24. METHOD OF FORMING THE CONTEXT OF ADVERTISING AND TARGET AUDIENCE BASED ON ASSOCIATIVE RULES LEARNING / K. LIPIANINA-HONCHARENKO et al. *Herald of Khmelnytskyi National University. Technical sciences*. 2022. Vol. 313, no. 5. P. 279–287. URL: https://doi.org/10.31891/2307-5732-2022-313-5-279-287
25. Intelligent Method of Forming the HR Management Short-Term Project / H. Lipyanina et al. *Advances in Intelligent Systems and Computing*. Cham, 2020. P. 1045–1055. URL: https://doi.org/10.1007/978-3-030-63270-0_71
26. Neural Network Approach for Semantic Coding of Words / Golovko, V., Kroshchanka, A., Komar, M., Sachenko, A. Advances in Intelligent Systems and Computing, 2020, 1020, pp. 647–658. URL: https://link.springer.com/chapter/10.1007/978-3-030-26474-1_45.
27. An Intelligent Method for Forming the Advertising Content of Higher Education Institutions Based on Semantic Analysis / K. Lipianina-Honcharenko et al. *Communications in Computer and Information Science*. Cham, 2022. P. 169–182. URL: https://doi.org/10.1007/978-3-031-14841-5_11
28. Intelligent Method for Forming the Consumer Basket / K. Lipianina-Honcharenko et al. *Communications in Computer and Information Science*. Cham, 2022. P. 221–231. URL: https://doi.org/10.1007/978-3-031-16302-9_17
29. Method of Forming a Training Sample for Segmentation of Tender Organizers on Machine Learning Basis. In COLINS (pp. 1843-1852), Lipyanina-Goncharenko, H., Brych, V., Sachenko, S., Lendyuk, T., Bykovyy, P., & Zahorodnia, D., 2021.
30. Method of Detecting a Fictitious Company on the Machine Learning Base / H. Lipyanina et al. *Advances in Computer Science for Engineering and Education IV*. Cham, 2021. P. 138–146. URL: https://doi.org/10.1007/978-3-030-80472-5_12
31. Intelligent Method for Classifying the Level of Anthropogenic Disasters / K. Lipianina-Honcharenko et al. *Big Data and Cognitive Computing*. 2023. Vol. 7, no. 3. P. 157. URL: https://doi.org/10.3390/bdcc7030157
32. Evaluation the Efficiency of Information Technology of Big Data Intelligence Analysis and Processing. Komar, M., Savenko, O., Sachenko, A., Lendiuk, T., Lipianina-Honcharenko, K., Hladiy, G., & Vasylkiv, N. 2022.