



[DOI 10.28925/2663-4023.2026.32.1110](https://doi.org/10.28925/2663-4023.2026.32.1110)

УДК 004.056

Назаркевич Марія Андріївна

доктор технічних наук, професор,
професор кафедри інформаційних систем та мереж
Національний університет «Львівська Політехніка», м.Львів, Україна
ORCID: 0000-0002-6528-9867
Mariia.a.nazarkevych@lpnu.ua

Коротич Даниїл Ігорович

студент кафедри інформаційних систем та мереж
Національний університет «Львівська Політехніка», м.Львів, Україна
ORCID: 0009-0000-7060-641X
danyil.korotych.mitis.2024@lpnu.ua

Чолкан Роман Орестович

студент кафедри інформаційних систем та мереж
Національний університет «Львівська Політехніка», м.Львів, Україна
ORCID: 0009-0009-5772-7642
roman.cholkan.mitis.2024@lpnu.ua

РОЗРОБЛЕННЯ МЕТОДІВ ДЛЯ ВИЯВЛЕННЯ ФЕЙКОВИХ НОВИН НА ОСНОВІ АНАЛІЗУ ТЕОРІЇ ГРАФІВ

Анотація. Статтю присвячено розробленню та дослідженню методів автоматизованого виявлення фейкових новин на основі аналізу графових структур і алгоритмів виявлення спільнот у соціальних мережах. Стрімке зростання обсягів новинного контенту спричиняє складність оперативної перевірки його достовірності в умовах цифрового інформаційного середовища. Традиційні підходи, засновані виключно на лінгвістичному аналізі текстів і класичних методах машинного навчання є недостатніми для виявлення координованих дезінформаційних кампаній, які мають мережевий характер поширення. У роботі обґрунтовано доцільність використання графової моделі подання новин, у якій окремі повідомлення та інформаційні сутності розглядаються як вершини графа, а їхні взаємозв'язки – як ребра. Такий підхід дозволяє перейти від аналізу ізольованих новин до дослідження структурних закономірностей інформаційних потоків. Основну увагу зосереджено на застосуванні алгоритмів виявлення спільнот Louvain і Leiden, які забезпечують кластеризацію графа на основі оптимізації модульності та дозволяють ідентифікувати щільно пов'язані групи повідомлень. Запропоновано архітектуру програмного засобу для виявлення фейкових новин, що охоплює етапи завантаження та попереднього опрацювання даних, побудови графової моделі, кластеризації, аналізу результатів і візуалізації. Реалізація виконана за модульним принципом, що забезпечує гнучкість, масштабованість і можливість інтеграції альтернативних алгоритмів кластеризації. У межах експериментального дослідження проведено порівняльний аналіз результатів, отриманих із використанням алгоритмів Louvain і Leiden, на реальних даних соціальних мереж. Результати експериментів показали, що алгоритми здатні формувати спільноти з високим рівнем чистоти, проте алгоритм Leiden забезпечує більш стабільні та внутрішньо зв'язані кластери, що підвищує інтерпретованість результатів і точність ідентифікації дезінформаційних груп. Продемонстровано, що поєднання аналізу текстової подібності з урахуванням графових спільнот дозволяє ефективніше виявляти фейкові новини та координовані інформаційні впливи порівняно з підходами, орієнтованими лише на контент. Практична цінність роботи полягає у створенні програмного засобу з графічним користувацьким інтерфейсом, який забезпечує прозорий і відтворюваний процес аналізу новинних повідомлень у режимі реального часу. Запропонований підхід може бути використаний як основа для систем моніторингу дезінформації, підтримки прийняття рішень у сфері інформаційної безпеки та подальших наукових досліджень. Перспективи подальшої роботи пов'язані з використанням динамічних графів, мультимодальних даних та



пояснюваних моделей штучного інтелекту для поглибленого аналізу процесів поширення фейкових новин.

Ключові слова: фейкові новини; машинне навчання; соціальна мережа; метод Лейдена; метод Лувена.

ВСТУП

Стрімке зростання обсягів цифрового новинного контенту суттєво ускладнює задачу перевірки його достовірності. Інформаційні ресурси, новинні платформи та соціальні мережі функціонують у режимі постійного оновлення, що робить неможливим застосування виключно ручних або напівавтоматичних методів контролю якості інформації. У таких умовах актуальною стає розробка програмних засобів, здатних автоматично аналізувати великі масиви новинних даних та виявляти потенційно фейковий контент.

Більшість наявних рішень зосереджуються на аналізі текстового вмісту повідомлень, використовуючи лінгвістичні ознаки або методи машинного навчання. Хоча такі підходи демонструють прийнятні результати для задач класифікації окремих новин, вони не враховують структурні зв'язки між повідомленнями, джерелами та повторюваними інформаційними патернами. Унаслідок цього залишається поза увагою сам механізм поширення фейкових новин, який часто має координований і мережевий характер.

Альтернативним підходом є використання графових моделей, у яких новини та пов'язані з ними сутності подаються у вигляді вершин, а їх взаємозв'язки – у вигляді ребер. Такий спосіб подання даних дозволяє перейти від аналізу ізольованих повідомлень до дослідження інформаційної структури в цілому. Особливий інтерес у цьому контексті становлять алгоритми виявлення графових спільнот, які дають змогу групувати об'єкти на основі інтенсивності їхніх зв'язків і виявляти щільно пов'язані кластери.

З практичної точки зору важливим є не лише вибір алгоритму виявлення спільнот, а й його коректна інтеграція у програмний засіб, який забезпечує повний цикл обробки даних – від завантаження та підготовки вхідної інформації до побудови графової моделі, виконання кластеризації та інтерпретації отриманих результатів. У реальних прикладних системах алгоритм виявлення спільнот є лише одним із компонентів складнішої програмної архітектури, що включає модулі попереднього опрацювання даних, формування структури графа, управління параметрами кластеризації, а також засоби аналізу й візуалізації результатів.

Саме реалізаційний аспект таких систем часто залишається недостатньо висвітленим у наукових публікаціях, попри його вирішальну роль у практичному використанні графових методів. Недостатня увага до питань програмної реалізації може призводити до труднощів відтворення результатів, обмеженої масштабованості або некоректного застосування алгоритмів на реальних наборах даних. Тому розгляд архітектурних рішень, вибору структур даних, організації обчислювального процесу та інтеграції алгоритмів виявлення спільнот у єдиний програмний засіб є необхідною складовою прикладних досліджень у сфері автоматизованого аналізу фейкових новин.

У зв'язку з цим у даній роботі розглядається задача розробки та реалізації програмного засобу для виявлення фейкових новин із використанням графових спільнот. Основна увага зосереджена на побудові графової моделі на основі новинних даних, застосуванні алгоритмів виявлення спільнот Louvain і Leiden, а також



експериментальному порівнянню отриманих результатів. Запропонований програмний засіб орієнтований на практичне використання та може слугувати основою для подальшого розвитку систем аналізу інформаційних потоків.

Постановка проблеми. Сучасні інформаційні системи стикаються з необхідністю автоматизованого аналізу великих масивів новинних даних, у межах яких фейкові повідомлення часто поширюються не ізольовано, а у складі взаємопов'язаних груп. Зосередження лише на змістовому аналізі окремих повідомлень не дозволяє повною мірою виявляти координовані інформаційні впливи та повторювані патерни поширення дезінформації.

У цьому контексті актуальною є задача побудови програмних засобів, які поєднують аналіз новинного контенту зі структурним аналізом взаємозв'язків між повідомленнями, джерелами та іншими сутностями. Використання графових моделей і алгоритмів виявлення спільнот відкриває можливість автоматичного групування пов'язаних новин та ідентифікації потенційно фейкових кластерів. Водночас недостатньо дослідженими залишаються питання практичної реалізації таких підходів, зокрема інтеграції алгоритмів виявлення спільнот у програмні системи, вибору ефективних способів побудови графа та оцінювання результатів кластеризації. Розв'язання зазначеної проблеми спрямоване на підвищення точності, стабільності та прикладної придатності автоматизованих систем виявлення фейкових новин.

Аналіз останніх досліджень і публікацій. У [1] аналізується зростання поширення фейкових новин. Однак багато чого залишається невідомим щодо вразливості окремих осіб, установ та суспільства до маніпуляцій з боку зловмисників.

У [2] у дослідженні фейкових новин проаналізовано методи глибокого навчання та обчислення ієрархічних ознак. Багато дослідницьких робіт будуть спрямовані на обчислення, пов'язані зі згортковими нейронними мережами у різних застосуваннях, таких як обробка аудіо та мовлення, обробка та моделювання природної мови, пошук інформації, розпізнавання об'єктів та комп'ютерний зір, а також мультимодальне та багатозадачне навчання у категоризації новинних повідомлень.

У [3] дослідники докладають зусиль для виявлення та боротьби з фейковими новинами за допомогою різноманітних методів машинного навчання (ML) та глибокого навчання (DL). Проводиться огляд існуючих досліджень для розуміння та обмеження поширення фейкових новин. Зокрема проведено порівняльне дослідження, використовуючи широкий спектр класичних алгоритмів машинного навчання, таких як логістична регресія (LR), метод опорних векторів (SVM), дерево рішень (DT), наївний байєсівський алгоритм (NB), випадковий ліс (RF), XGBoost (XGB) та метод ансамбевого навчання таких алгоритмів, передових алгоритмів машинного навчання, таких як згорткові нейронні мережі (CNN), двонаправлена довга короткочасна пам'ять (BiLSTM), двонаправлені рекурентні одиниці з рекурентним розподілом (BiGRU), CNN-BiLSTM, CNN-BiGRU та гібридний підхід таких методів, та (3) моделей на основі трансформаторів DL, таких як BERT_{base} та RoBERTa_{base}.

Дослідники в галузі обробки природної мови (NLP) [4] проводять експерименти з використанням різних попередньо навчених методів вбудовування слів у чотирьох відомих наборах даних фейкових новин з реального світу – LIAR, PolitiFact, GossipCop та COVID-19 – для вивчення ефективності різних методів у різних наборах даних. Крім того, порівнюється між контекстно-незалежними методами вбудовування (наприклад, GloVe) та ефективністю BERT_{base} – контекстуалізованим представленням у виявленні фейкових новин. Порівняно з сучасними результатами у використаних наборах даних, ми досягаємо кращих результатів, покладаючись виключно на текст



новин. Ми сподіваємося, що це дослідження може надати корисну інформацію дослідникам, які працюють над виявленням фейкових новин.

Поява Всесвітньої павутини та швидке впровадження платформ соціальних мереж (таких як Facebook та Twitter) [5] проклали шлях для поширення інформації, якого ніколи раніше не було в історії людства. Зі сучасним використанням платформ соціальних мереж споживачі створюють та поширюють більше інформації, ніж будь-коли раніше, деяка з якої є оманливою та не має відношення до реальності. Автоматизована класифікація текстової статті як дезінформації є складним завданням. У цій роботі ми запропоновано використовувати ансамблевий підхід машинного навчання для автоматизованої класифікації новинних статей. Дослідження показує різні текстові властивості, які можна використовувати для відмінності фальшивого контенту від реального. Використовуючи ці властивості, навчаємо комбінацію різних алгоритмів машинного навчання, використовуючи різні ансамблеві методи, та оцінюємо їхню ефективність на 4 реальних наборах даних [6]. Експериментальна оцінка підтверджує кращу ефективність запропонованого ансамблевого підходу до навчання порівняно з окремими учнями.

У [7] Останнім часом було проведено багато пошукових зусиль, спрямованих на розуміння феномену фейкових новин. Авторам вдалося створити низку моделей, які дають дуже точні рішення, таким чином ефективно відокремлюючи фейкові новини від реальних. Зокрема, зосередили наш аналіз на моделях, які ранжують випадково вибрану фейкову новину вище, ніж випадково вибраний факт з ймовірністю понад 0,85. Для цих моделей ми виявили сильний зв'язок між характеристиками та прогнозами моделі, показуючи, що деякі характеристики чітко адаптовані для виявлення певних типів фейкових новин, що свідчить про те, що різні комбінації характеристик охоплюють певну область простору фейкових новин.

Мета статті. Метою даної роботи є розробка методів для виявлення фейкових новин на основі аналізу графових спільнот, а також експериментальне дослідження ефективності алгоритмів виявлення спільнот у межах побудованої системи. Для досягнення поставленої мети здійснюється аналіз існуючих підходів до автоматизованого виявлення дезінформації, обґрунтовується вибір графової моделі представлення даних і алгоритмів кластеризації, а також проводиться порівняння результатів, отриманих із використанням алгоритмів Louvain і Leiden.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Однією з ключових передумов розробки програмного засобу для виявлення фейкових новин є вибір моделі подання новинних даних. У задачах аналізу дезінформації важливим є не лише зміст окремих повідомлень, а й характер зв'язків між ними, зокрема повторюваність джерел, схожість інформаційних повідомлень, а також структурні закономірності їх поширення. У зв'язку з цим доцільним є використання графових моделей, які дозволяють формалізувати інформаційне середовище у вигляді множини взаємопов'язаних об'єктів.

У межах графового підходу новинні дані подаються у вигляді неорієнтованого або орієнтованого графа, де вершини відповідають окремим новинним повідомленням або інформаційним сутностям, а ребра відображають наявність зв'язку між ними. Тип зв'язку визначається особливостями конкретної реалізації програмного засобу та може базуватися, наприклад, на спільному джерелі публікації, тематичній подібності або

повторюваності інформаційних шаблонів. Таке подання дозволяє перейти від аналізу ізольованих текстів до дослідження цілісної структури інформаційного простору.

З теоретичної точки зору графове моделювання широко застосовується для аналізу інформаційних мереж і виявлення структурних закономірностей у процесах поширення контенту. У дослідженні [8] показано доцільність використання графового подання даних у поєднанні з методами штучного інтелекту для автоматизованого виявлення дезінформації в онлайн-середовищі. Отримані результати свідчать, що аналіз зв'язків між інформаційними повідомленнями дозволяє виявляти групи взаємопов'язаного контенту, що є важливим для подальшої кластеризації новин і застосування алгоритмів виявлення спільнот у прикладних програмних системах.

З практичної точки зору використання графової моделі є особливо важливим для реалізації програмного засобу, оскільки дозволяє чітко відокремити етапи обробки даних: формування вершин, встановлення зв'язків між ними та подальшу кластеризацію. Такий підхід [9] спрощує розширення системи, наприклад шляхом додавання нових типів зв'язків або зміни критеріїв побудови графа без суттєвого втручання у загальну архітектуру програмного рішення.

У розроблюваному програмному засобі графова модель використовується як базовий рівень абстракції для подальшого застосування алгоритмів виявлення спільнот. Виявлені спільноти інтерпретуються як групи взаємопов'язаних новин, які можуть відповідати повторюваним або координованим інформаційним повідомленням. Саме така інтерпретація узгоджується з сучасними підходами до аналізу дезінформації та створює теоретичне підґрунтя для використання алгоритмів Louvain і Leiden у межах програмної реалізації.

Для наочного представлення місця графової моделі в архітектурі програмного засобу доцільно використати компонентну діаграму (див. Рис. 1), яка відображає основні функціональні модулі системи та їх взаємодію.

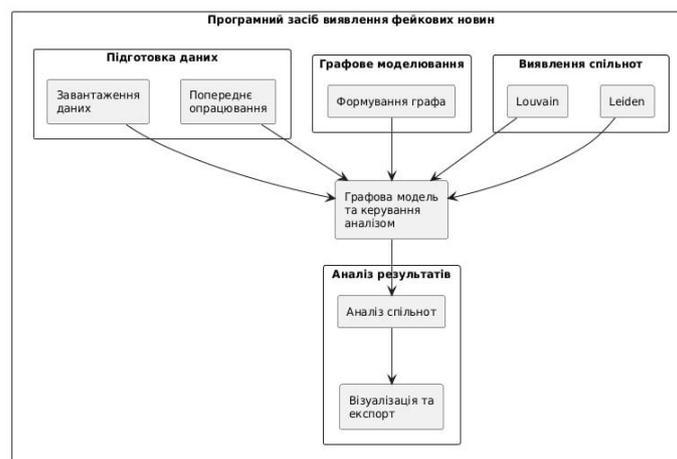


Рис. 1 Функціональна схема виявлення фейкової інформації

Центральним елементом запропонованої архітектури є графова модель, яка формується на основі попередньо опрацьованих новинних даних і слугує базою для застосування алгоритмів виявлення спільнот. Саме на цьому рівні здійснюється інтеграція структурної інформації про взаємозв'язки між повідомленнями з алгоритмічними методами кластеризації. Результати виявлення спільнот надалі підлягають аналізу та інтерпретації з метою ідентифікації груп новин, що можуть мати ознаки фейкового або координованого поширення [9].



Запропонована архітектурна модель узгоджується з теоретичними положеннями графового аналізу та забезпечує гнучкість програмної реалізації. Зокрема, модульна структура дозволяє змінювати або розширювати окремі етапи обробки даних – наприклад, використовувати альтернативні критерії побудови графа або порівнювати різні алгоритми виявлення спільнот – без необхідності суттєвої перебудови всієї системи. Це є важливою перевагою з точки зору практичного застосування програмного засобу в задачах аналізу дезінформації.

Таким чином, використання графового подання новинних даних і модульної архітектури програмного засобу створює теоретично обґрунтовану основу для застосування алгоритмів виявлення спільнот у задачі автоматизованого виявлення фейкових новин. У наступному підрозділі буде детально розглянуто алгоритми Louvain і Leiden, а також обґрунтовано їх вибір і роль у процесі кластеризації графових даних у межах запропонованого програмного рішення.

Алгоритми виявлення спільнот Louvain і Leiden у програмному засобі. Алгоритми виявлення спільнот відіграють ключову роль у реалізації програмного засобу для виявлення фейкових новин, оскільки саме вони забезпечують автоматизоване групування взаємопов'язаних інформаційних повідомлень на основі структури графа. У межах графового подання новинних даних задача виявлення спільнот зводиться до поділу множини вершин графа на підмножини таким чином, щоб зв'язки всередині кожної групи були щільнішими, ніж між різними групами.

У розроблюваному програмному засобі для кластеризації графових даних використано алгоритми Louvain і Leiden, які належать до класу модульнісно-орієнтованих методів виявлення спільнот. Алгоритм Louvain є одним із найбільш поширених підходів до кластеризації великих мереж завдяки своїй обчислювальній ефективності та здатності працювати з графами значного розміру. Його основна ідея полягає у поетапній оптимізації функції модульності шляхом локального переміщення вершин між спільнотами з подальшою агрегацією отриманих кластерів. Разом з тим, у прикладних задачах аналізу інформаційних мереж алгоритм Louvain може формувати спільноти з недостатньо зв'язаною внутрішньою структурою, що ускладнює інтерпретацію результатів. Для усунення цього недоліку у програмному засобі також реалізовано алгоритм Leiden, який є подальшим розвитком підходу Louvain. Алгоритм Leiden забезпечує формування більш коректних і внутрішньо зв'язаних спільнот, що підвищує стабільність і надійність результатів кластеризації, особливо у випадках аналізу складних інформаційних графів. Використання обох алгоритмів у межах одного програмного засобу дозволяє не лише виконувати кластеризацію новинних даних, а й здійснювати порівняльний аналіз результатів, отриманих різними методами. Такий підхід є важливим з точки зору експериментального дослідження, оскільки дає змогу оцінити вплив вибору алгоритму на структуру виявлених спільнот та їх подальшу інтерпретацію у контексті виявлення фейкових новин.

На основі викладених теоретичних положень у програмному засобі реалізовано узагальнений алгоритм автоматизованого виявлення фейкових новин із використанням графових спільнот, який включає такі основні кроки:

1. Завантаження вхідних даних. Зчитування новинних даних із зовнішнього джерела (наприклад, файлу формату Excel) та формування початкового набору інформаційних об'єктів.
2. Попереднє опрацювання даних. Фільтрація, нормалізація та підготовка даних для подальшого графового подання.

3. Побудова графової моделі. Формування множини вершин, що відповідають новинним повідомленням або інформаційним сутностям, а також встановлення ребер між ними відповідно до обраних критеріїв зв'язку.

4. Вибір алгоритму виявлення спільнот. Ініціалізація процесу кластеризації з використанням алгоритму Louvain або Leiden.

5. Виявлення спільнот. Виконання алгоритму кластеризації з метою поділу графа на спільноти взаємопов'язаних новин.

6. Аналіз отриманих спільнот. Обчислення характеристик кластерів і формування узагальнених результатів аналізу.

7. Візуалізація та збереження результатів. Подання результатів у вигляді графічних зображень та експорт даних для подальшого дослідження.

Такий алгоритм забезпечує відтворюваність результатів і дозволяє використовувати програмний засіб як інструмент експериментального аналізу фейкових новин. Описаний покроковий алгоритм відображає логіку функціонування програмного засобу на концептуальному рівні та демонструє послідовність основних етапів обробки новинних даних – від їх завантаження до формування та аналізу результатів кластеризації. Для наочного подання цього процесу та ілюстрації потоків управління між окремими етапами доцільно використати діаграму діяльності.

На Рис. 2 подано діаграму діяльності, яка відображає узагальнений алгоритм роботи програмного засобу та акцентує увагу на етапі вибору алгоритму виявлення спільнот. Діаграма наочно демонструє альтернативні гілки виконання, що відповідають застосуванню алгоритмів Louvain або Leiden, а також подальші етапи аналізу й візуалізації отриманих результатів.

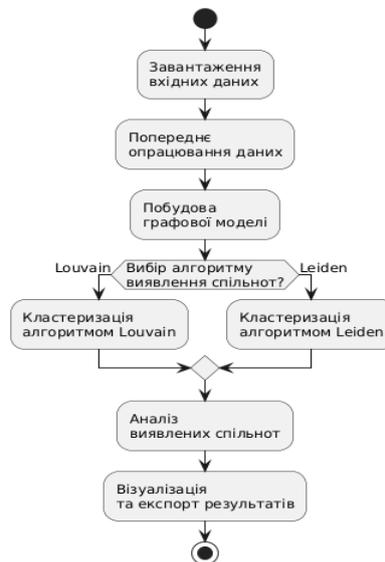


Рис. 2. Діаграма діяльності алгоритму роботи програмного засобу

Таким чином, використання алгоритмів Louvain і Leiden у межах розроблюваного програмного засобу є теоретично обґрунтованим і практично доцільним для задачі виявлення фейкових новин на основі графових спільнот. Запропонований алгоритм роботи системи забезпечує послідовну обробку новинних даних, інтегруючи етапи побудови графової моделі, кластеризації та аналізу результатів у єдиний аналітичний процес.



Застосування двох алгоритмів виявлення спільнот у межах однієї програмної реалізації створює можливість порівняльного аналізу їхніх результатів та оцінки впливу вибору алгоритму на якість і структуру сформованих кластерів. Це, у свою чергу, дозволяє підвищити надійність інтерпретації отриманих результатів і розширює можливості програмного засобу як інструмента експериментального дослідження процесів поширення дезінформації.

Описані теоретичні положення та алгоритмічна схема роботи програмного засобу слугують основою для подальшого розгляду практичної реалізації системи. У наступному розділі буде детально представлено програмну реалізацію запропонованого підходу, описано використані технології, а також наведено результати експериментального дослідження ефективності застосування алгоритмів Louvain і Leiden для виявлення фейкових новин.

Реалізація програмного засобу для виявлення фейкових новин. Розроблений програмний засіб реалізовано як окремий програмний модуль, орієнтований на автоматизовану обробку новинних даних, побудову графової моделі та виконання кластеризації із застосуванням алгоритмів Louvain і Leiden [11]. Реалізація виконана з урахуванням модульного підходу, що забезпечує розділення відповідальностей між компонентами системи та спрощує розширення функціональності.

Програмне рішення побудоване за принципом послідовної обробки даних і включає такі логічні рівні:

1. рівень завантаження та підготовки даних;
2. рівень побудови графової моделі;
3. рівень кластеризації графа;
4. рівень аналізу та збереження результатів.

Кожен рівень реалізовано у вигляді окремих класів або груп класів, які взаємодіють між собою через чітко визначені інтерфейси. Такий підхід дозволяє змінювати реалізацію окремих етапів без впливу на загальну логіку роботи системи.

Для роботи з вхідними новинними даними використовується клас `DataLoader`, який відповідає за зчитування інформації з файлу формату Excel та формування внутрішнього представлення даних. Клас інкапсулює логіку доступу до зовнішнього джерела даних і повертає структурований набір об'єктів, що відповідають окремим новинним повідомленням.

Окремо реалізовано клас `DataPreprocessor`, який виконує попереднє опрацювання даних, зокрема очищення, нормалізацію та відбір необхідних атрибутів. Результатом роботи цього класу є підготовлений набір даних, придатний для подальшого графового моделювання.

Побудова графа реалізується у класі `GraphBuilder`, який на основі підготовлених даних формує вершини та ребра графа. Вершини відповідають окремим новинним повідомленням або інформаційним сутностям, тоді як ребра відображають наявність зв'язку між ними відповідно до заданих критеріїв.

Клас `GraphBuilder` дозволяє параметризувати процес побудови графа, зокрема змінювати тип зв'язків між вершинами або їх вагові характеристики. Це забезпечує гнучкість програмного засобу та можливість експериментувати з різними моделями графового подання даних без модифікації інших компонентів системи.

Логіка кластеризації графа винесена в окремий клас `CommunityDetectionService`, який інкапсулює виклик алгоритмів Louvain і Leiden. Залежно від обраного режиму роботи система ініціалізує відповідний алгоритм і виконує процес виявлення спільнот над побудованим графом.

Для забезпечення гнучкості реалізації використовується єдиний інтерфейс для алгоритмів кластеризації, що дозволяє легко розширювати систему шляхом додавання нових методів виявлення спільнот. Результатом роботи цього класу є множина кластерів, кожен з яких відповідає окремій графовій спільноті.

Після завершення кластеризації результати передаються до класу ResultAnalyzer, який виконує узагальнення інформації про виявлені спільноти. На цьому етапі здійснюється аналіз розміру кластерів, їх структури та кількісних характеристик, що можуть бути використані для подальшої інтерпретації результатів у контексті виявлення фейкових новин.

Для збереження результатів реалізовано клас ResultExporter, який відповідає за експорт даних у зовнішні файли та формування візуальних представлень графа і виявлених спільнот. Це дозволяє використовувати програмний засіб не лише для автоматизованого аналізу, а й для подальшого дослідження та візуальної оцінки результатів кластеризації.

Загальна логіка роботи програмного засобу реалізована у керуючому класі ApplicationController, який координує виклик окремих модулів відповідно до алгоритму, описаного у попередньому розділі. Саме цей клас забезпечує послідовне виконання етапів завантаження даних, побудови графа, кластеризації та аналізу результатів.

Такий підхід дозволяє розглядати програмний засіб як цілісну систему, у якій кожен компонент виконує чітко визначену функцію, а загальна логіка роботи залишається прозорою та зрозумілою з точки зору програмної реалізації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Експериментальне дослідження було спрямоване на оцінку ефективності застосування алгоритмів Louvain і Leiden для виявлення спільнот у графі новинних повідомлень та аналізу їх потенційної придатності для ідентифікації фейкового контенту. Для цього на основі побудованої графової моделі було виконано кластеризацію даних з використанням обох алгоритмів, після чого проведено кількісний і якісний аналіз отриманих спільнот.

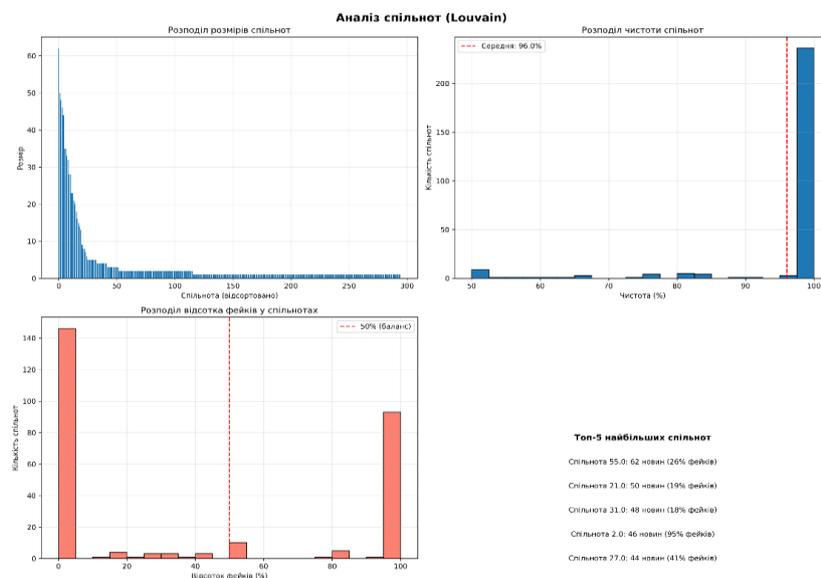


Рис. 3. Аналіз результатів кластеризації алгоритмом Louvain

На Рис. 3 представлено результати аналізу спільнот, отриманих із використанням алгоритму Louvain. Зокрема, наведено розподіл розмірів спільнот, розподіл їх чистоти, а також розподіл відсотка фейкових новин у межах кожної спільноти.

Аналіз розподілу розмірів спільнот показує, що алгоритм Louvain формує значну кількість малих спільнот поряд із декількома більшими кластерами. Така структура є типовою для алгоритмів, орієнтованих на оптимізацію модульності, та свідчить про здатність методу виявляти локальні групи тісно пов'язаних повідомлень. Водночас наявність великих спільнот указує на існування більш узагальнених тематичних або джерельних зв'язків між новинами.

Розподіл чистоти спільнот демонструє, що переважна більшість кластерів характеризується високими значеннями чистоти, середнє значення якої становить близько 96%. Це означає, що виявлені спільноти здебільшого складаються з новин одного типу – або переважно достовірних, або переважно фейкових. Такий результат підтверджує доцільність використання графової кластеризації як допоміжного інструмента для виявлення дезінформації.

Аналіз відсотка фейкових новин у спільнотах свідчить про наявність кластерів із чітко вираженою домінацією фейкового контенту. Зокрема, серед найбільших спільнот зафіксовано групи з часткою фейкових новин, що перевищує 90%, що може вказувати на координоване поширення дезінформації.

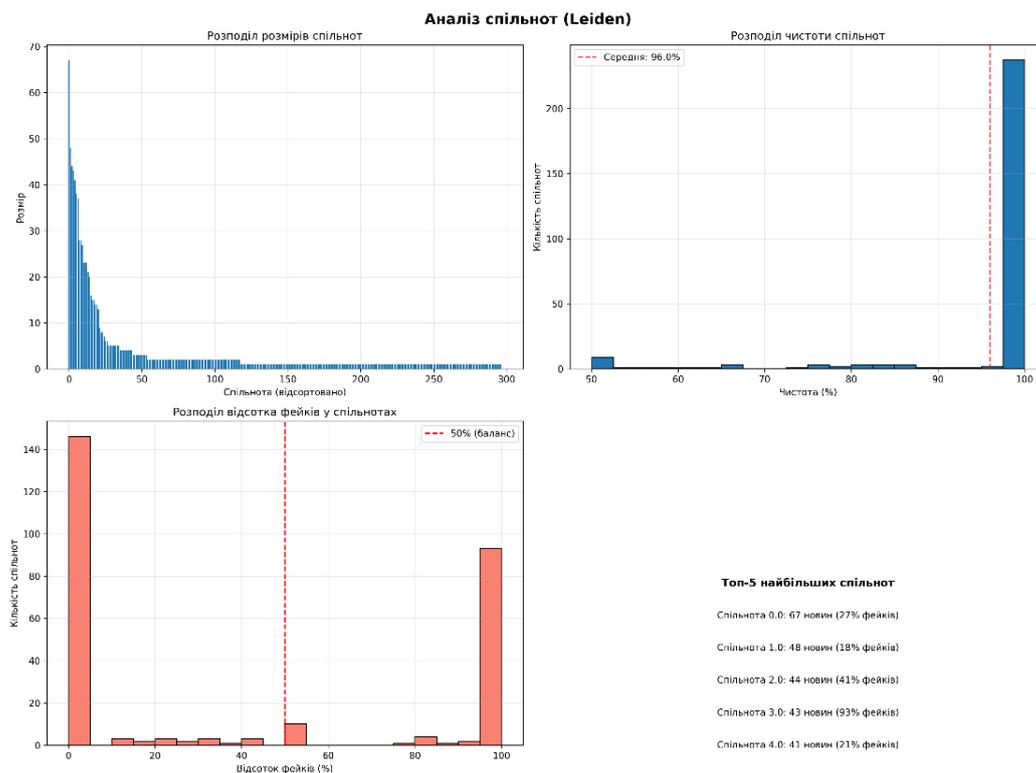


Рис. 4. Аналіз результатів кластеризації алгоритмом Leiden

На Рис. 4 наведено результати аналізу спільнот, отриманих із використанням алгоритму Leiden. Структура представлених діаграм аналогічна до попереднього випадку, що дозволяє безпосередньо порівнювати результати двох алгоритмів.

Розподіл розмірів спільнот, сформованих алгоритмом Leiden, також характеризується наявністю великої кількості малих кластерів, однак при цьому

спільноти мають більш рівномірну внутрішню структуру. Це узгоджується з теоретичними властивостями алгоритму Leiden, який гарантує внутрішню зв'язаність кожної спільноти.

Розподіл чистоти спільнот свідчить про збереження високих значень цього показника, середнє значення також наближається до 96%. При цьому у порівнянні з алгоритмом Louvain спільноти, отримані алгоритмом Leiden, демонструють меншу кількість граничних випадків, де в одному кластері присутня значна частка як фейкових, так і нефейкових новин.

Аналіз відсотка фейкових новин у спільнотах показує, що алгоритм Leiden більш чітко виділяє кластери з високою концентрацією фейкового контенту. Це підвищує інтерпретованість результатів і спрощує подальше використання кластерів як індикаторів потенційних дезінформаційних кампаній.

Аналіз роботи програмного засобу на рівні користувацького інтерфейсу. Для практичної перевірки працездатності розробленого програмного засобу було реалізовано графічний користувацький інтерфейс (Рис. 5), який забезпечує інтерактивну взаємодію з системою та наочне подання результатів аналізу. Інтерфейс орієнтований на послідовне виконання процесу перевірки новин і відображає як кінцевий вердикт, так і проміжні етапи обробки даних.

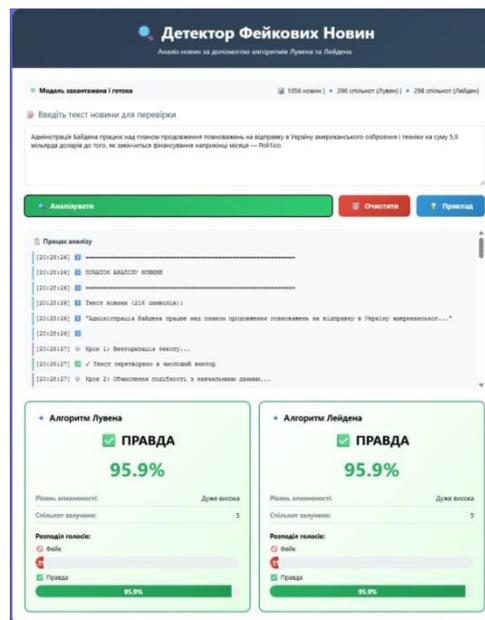


Рис. 5. Загальний вигляд графічного користувацького інтерфейсу

Користувачеві надається можливість ввести довільний текст новинного повідомлення у відповідне текстове поле (Рис. 6) та ініціювати процес аналізу. Після запуску аналізу система відображає статус готовності моделі, кількість новин у навчальному наборі, а також загальну кількість виявлених спільнот для алгоритмів Louvain і Leiden. Це дозволяє користувачеві оцінити масштаб оброблюваних даних і складність графової структури.

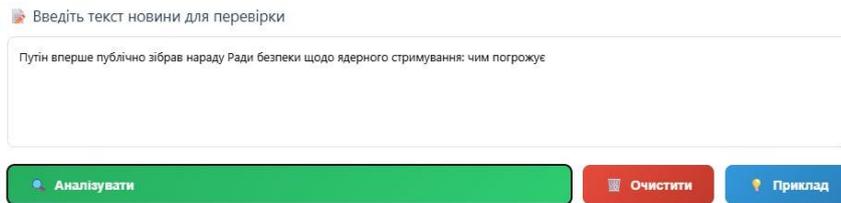


Рис. 6. Поле введення тексту новини

Процес аналізу кожної окремої новини реалізовано у вигляді послідовності логічних кроків, які детально відображаються у блоці “Процес аналізу” (Рис. 7). Це забезпечує прозорість роботи алгоритму та дозволяє простежити всі етапи ухвалення рішення.

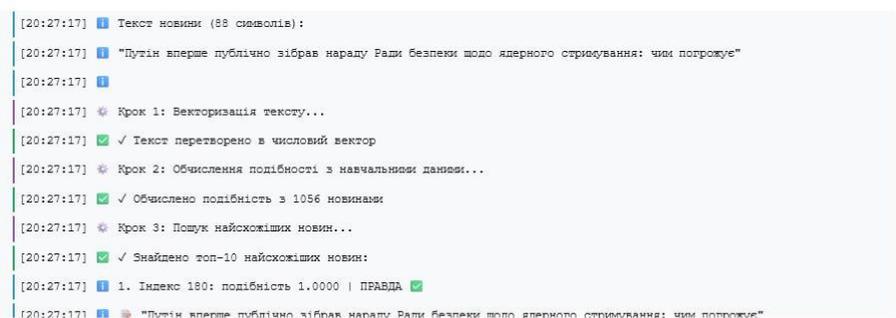


Рис. 7. Процес аналізу новини

На першому етапі система виконує векторизацію введеного тексту, у результаті чого новина перетворюється у числовий вектор ознак. Далі здійснюється обчислення подібності між цим вектором і всіма новинами з навчального набору, що дозволяє визначити найбільш схожі інформаційні повідомлення. На основі отриманих значень формується список топ-10 найближчих новин із зазначенням ступеня подібності та їх попередньої класифікації.

Наступним кроком є аналіз знайдених схожих новин у контексті графових спільнот. Для кожної схожої новини визначається відповідна спільнота, її чистота та вага впливу, що враховується під час підсумкового голосування. Такий підхід дозволяє врахувати не лише локальну текстову подібність, а й глобальну структуру інформаційного простору.

Фінальний етап аналізу полягає у формуванні вердикту для кожного з алгоритмів виявлення спільнот (Рис. 8). Результати подаються у вигляді двох окремих інформаційних блоків – для алгоритму Louvain і для алгоритму Leiden. Кожен блок містить підсумкову класифікацію (“Фейк” або “Правда”), числову оцінку впевненості, кількість задіяних спільнот та розподіл голосів між класами.

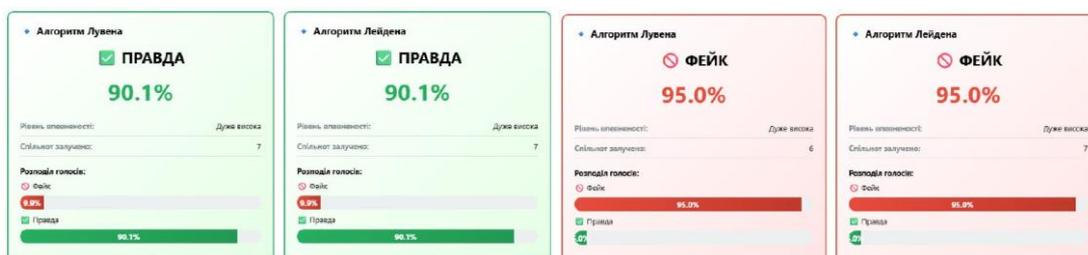


Рис. 8. Позитивний та негативний результат аналізу



Наочне подання результатів дозволяє легко порівнювати рішення, отримані різними алгоритмами. У наведеному прикладі обидва алгоритми незалежно один від одного класифікують новинне повідомлення як фейкове з максимальною впевненістю, що свідчить про узгодженість результатів і стабільність роботи програмного засобу.

Таким чином, реалізований користувацький інтерфейс не лише забезпечує зручну взаємодію з програмним засобом, а й виконує роль інструмента інтерпретації результатів аналізу. Детальне логування процесу обробки кожної новинної події дозволяє розглядати систему як прозорий і відтворюваний аналітичний інструмент, що є важливим з точки зору практичного застосування та подальших наукових досліджень у сфері виявлення дезінформації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У межах даної роботи було розроблено та досліджено програмний засіб для виявлення фейкових новин із використанням графових методів аналізу та алгоритмів виявлення спільнот Louvain і Leiden. Запропонований підхід базується на поданні новинних повідомлень у вигляді графової моделі, що дозволяє враховувати не лише зміст окремих текстів, а й структурні зв'язки між ними, які виникають у процесі поширення інформації.

У ході дослідження обґрунтовано доцільність використання графових спільнот як основи для аналізу дезінформації. Показано, що кластеризація новинних даних за допомогою алгоритмів Louvain і Leiden дозволяє виявляти групи взаємопов'язаних повідомлень із високою концентрацією фейкового або достовірного контенту. Результати експериментального дослідження підтвердили, що обидва алгоритми демонструють високу ефективність, при цьому алгоритм Leiden забезпечує формування більш стабільних і внутрішньо зв'язаних спільнот, що підвищує інтерпретованість результатів.

Практична цінність роботи полягає у реалізації повноцінного програмного засобу з графічним користувацьким інтерфейсом, який дозволяє аналізувати окремі новинні повідомлення в інтерактивному режимі. Реалізований механізм детального логування кожного етапу обробки забезпечує прозорість процесу аналізу та дозволяє розглядати систему як інструмент підтримки прийняття рішень у задачах моніторингу інформаційного простору. Отримані результати свідчать про те, що поєднання текстової подібності з аналізом графових спільнот є ефективним підходом до виявлення дезінформації.

Перспективи подальших досліджень пов'язані з розширенням функціональних можливостей запропонованого програмного засобу та поглибленням аналітичної складової. Зокрема, доцільним є інтегрування додаткових методів машинного та глибокого навчання для формування більш інформативних векторних представлень текстів. Перспективним напрямом є також використання динамічних графів для аналізу змін структури інформаційних спільнот у часі, що дозволить виявляти еволюцію дезінформаційних кампаній.

Крім того, подальші дослідження можуть бути спрямовані на масштабування системи для роботи з більшими обсягами даних, а також на адаптацію програмного засобу до аналізу новин із різних мовних та тематичних доменів. Запропонований підхід може слугувати основою для створення комплексних систем моніторингу дезінформації та бути використаним у наукових і прикладних дослідженнях у галузі інформаційної безпеки.



СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... Zittrain, J. L. (2018). The science of fake news. *Science*, 359(6380), 1094–1096. <https://doi.org/10.1126/science.aao2998>
2. Manzoor, S. I., & Singla, J. (2019). Fake news detection using machine learning approaches: A systematic review. In *Proceedings of the 3rd International Conference on Trends in Electronics and Informatics (ICOEI 2019)* (pp. 230–234). IEEE. <https://doi.org/10.1109/ICOEI.2019.8862584>
3. Jain, A., Shakya, A., Khatter, H., & Gupta, A. K. (2019). A smart system for fake news detection using machine learning. In *Proceedings of the International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT 2019)* (Vol. 1, pp. 1–4). IEEE. <https://doi.org/10.1109/ICICT46931.2019.8977659>
4. Alghamdi, J., Lin, Y., & Luo, S. (2022). A comparative study of machine learning and deep learning techniques for fake news detection. *Information*, 13(12), Article 576. <https://doi.org/10.3390/info13120576>
5. Ahmad, I., Yousaf, M., Yousaf, S., & Ahmad, M. O. (2020). Fake news detection using machine learning ensemble methods. *Complexity*, 2020, Article 8885861. <https://doi.org/10.1155/2020/8885861>
6. Khan, J. Y., Khondaker, M. T. I., Afroz, S., Uddin, G., & Iqbal, A. (2021). A benchmark study of machine learning models for online fake news detection. *Machine Learning with Applications*, 4, Article 100032. <https://doi.org/10.1016/j.mlwa.2021.100032>
7. Reis, J. C., Correia, A., Murai, F., Veloso, A., & Benevenuto, F. (2019). Explainable machine learning for fake news detection. In *Proceedings of the 10th ACM Conference on Web Science* (pp. 17–26). <https://doi.org/10.1145/3292522.3326027>
8. Nazarkevych, M., Vysotska, V., Yurynets, R., & Nakonechnyi, N. (2025). Methods of implementing disinformation detection in social networks based on artificial intelligence. *Cybersecurity: Education, Science, Technique*, 2(30), 209–223.
9. Danylyk, V., Vysotska, V., & Nazarkevych, M. (2024). Methods of identifying disinformation, fakes and propaganda in mass media based on machine learning. *Cybersecurity: Education, Science, Technique*, 1(25), 449–467.
10. Vysotska, V., Nazarkevych, M., & Shamota, D. (2025). Information technology for referencing Ukrainian-language news at detecting disinformation in cybersecurity.
11. Nazarkevych, M., & Nazar, N. (2025). Method for detecting sources of disinformation and inauthentic user behavior in chats.

**Maria Nazarkevych**

Doctor of Technical Sciences, Professor,
Professor of the Department of Information Systems and Networks National University "Lviv Polytechnic",
Lviv, Ukraine

ORCID: 0000-0002-6528-9867

Mariia.a.nazarkevych@lpnu.ua

Danyil Korotych

Student, Department of Information Systems and Networks
National University "Lviv Polytechnic", Lviv, Ukraine

ORCID: 0009-0000-7060-641X

danyil.korotych.mitis.2024@lpnu.ua

Roman Cholkan

Student, Department of Information Systems and Networks
National University "Lviv Polytechnic", Lviv, Ukraine

ORCID: 0009-0009-5772-7642

roman.cholkan.mitis.2024@lpnu.ua

DEVELOPMENT OF METHODS FOR DETECTION OF FAKE NEWS BASED ON GRAPH THEORY ANALYSIS

Abstract. The article is devoted to the development and research of methods for automated detection of fake news based on the analysis of graph structures and algorithms for detecting communities in social networks. The relevance of the study is due to the rapid growth of the volume of news content and the complexity of operational verification of its reliability in the digital information environment. It is shown that traditional approaches based exclusively on linguistic analysis of texts and classical machine learning methods are insufficient for detecting coordinated disinformation campaigns that have a network nature of distribution. The paper substantiates the feasibility of using a graph model of presenting news data, in which individual messages and information entities are considered as vertices of a graph, and their relationships as edges. This approach allows us to move from the analysis of isolated news to the study of structural patterns of information flows. The main focus is on the application of Louvain and Leiden community detection algorithms, which provide graph clustering based on modularity optimization and allow identifying densely connected groups of messages. The architecture of a software tool for detecting fake news is proposed, which includes the stages of data loading and preprocessing, graph model construction, clustering, analysis of results, and visualization. The implementation is carried out according to the modular principle, which provides flexibility, scalability, and the ability to integrate alternative clustering algorithms. As part of the experimental study, a comparative analysis of the results obtained using the Louvain and Leiden algorithms was conducted on real social network data. The experimental results showed that both algorithms are capable of forming communities with a high level of purity, but the Leiden algorithm provides more stable and internally connected clusters, which increases the interpretability of the results and the accuracy of identifying disinformation groups. It is demonstrated that the combination of text similarity analysis with graph communities allows for more effective detection of fake news and coordinated information influences compared to approaches focused only on content. The practical value of the work lies in the creation of a software tool with a graphical user interface that provides a transparent and reproducible process of analyzing news messages in real time. The proposed approach can be used as a basis for disinformation monitoring systems, decision support in the field of information security and further scientific research. Prospects for further work are related to the use of dynamic graphs, multimodal data and explainable artificial intelligence models for in-depth analysis of fake news dissemination processes.

Keywords: fake news; machine learning; social network; Leiden method; Louvain method.



REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... Zittrain, J. L. (2018). The science of fake news. *Science*, 359(6380), 1094–1096. <https://doi.org/10.1126/science.aao2998>
2. Manzoor, S. I., & Singla, J. (2019). Fake news detection using machine learning approaches: A systematic review. In *Proceedings of the 3rd International Conference on Trends in Electronics and Informatics (ICOEI 2019)* (pp. 230–234). IEEE. <https://doi.org/10.1109/ICOEI.2019.8862584>
3. Jain, A., Shakya, A., Khatter, H., & Gupta, A. K. (2019). A smart system for fake news detection using machine learning. In *Proceedings of the International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT 2019)* (Vol. 1, pp. 1–4). IEEE. <https://doi.org/10.1109/ICICT46931.2019.8977659>
4. Alghamdi, J., Lin, Y., & Luo, S. (2022). A comparative study of machine learning and deep learning techniques for fake news detection. *Information*, 13(12), Article 576. <https://doi.org/10.3390/info13120576>
5. Ahmad, I., Yousaf, M., Yousaf, S., & Ahmad, M. O. (2020). Fake news detection using machine learning ensemble methods. *Complexity*, 2020, Article 8885861. <https://doi.org/10.1155/2020/8885861>
6. Khan, J. Y., Khondaker, M. T. I., Afroz, S., Uddin, G., & Iqbal, A. (2021). A benchmark study of machine learning models for online fake news detection. *Machine Learning with Applications*, 4, Article 100032. <https://doi.org/10.1016/j.mlwa.2021.100032>
7. Reis, J. C., Correia, A., Murai, F., Veloso, A., & Benevenuto, F. (2019). Explainable machine learning for fake news detection. In *Proceedings of the 10th ACM Conference on Web Science* (pp. 17–26). <https://doi.org/10.1145/3292522.3326027>
8. Nazarkevych, M., Vysotska, V., Yurynets, R., & Nakonechnyi, N. (2025). Methods of implementing disinformation detection in social networks based on artificial intelligence. *Cybersecurity: Education, Science, Technique*, 2(30), 209–223.
9. Danylyk, V., Vysotska, V., & Nazarkevych, M. (2024). Methods of identifying disinformation, fakes and propaganda in mass media based on machine learning. *Cybersecurity: Education, Science, Technique*, 1(25), 449–467.
10. Vysotska, V., Nazarkevych, M., & Shamota, D. (2025). Information technology for referencing Ukrainian-language news at detecting disinformation in cybersecurity.
11. Nazarkevych, M., & Nazar, N. (2025). Method for detecting sources of disinformation and inauthentic user behavior in chats.

Отримано редакцією журналу / Received: 05.01.26

Прорецензовано / Revised: 21.02.26

Схвалено до друку / Accepted: 26.03.26

