Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Удосконалення методу виявлення автоматично генерованої дезінформації у соціальних мережах під час інформаційних конфліктів

Виконав: ст. 2-го курсу, групи 2КІТС 22м
спеціальності 125– Кібербезпека
Освітня програма – Кібербезпека
інформаційних технологій та систем
(шифр і назва напряму підготовки, спеціальності)
Ковінько М. О.
(прізвище та ініціали)

Керівник: к.т.н., доцент каф. МБІС
Грицак А. В.
(прізвище та ініціали)
«04» грудня 2023 р.

Опонент: к.т.н., доцент каф. ОТ
Черняк О. І.
(прізвище та ініціали)
«04» грудня 2023 р.

Допущено до захисту
Голова секції УБ кафедри МБІС

Юрій ЯРЕМЧУК
“04” грудня 2023 р.

Вінниця ВНТУ - 2023 рік

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

Рівень вищої освіти ІІ-й (магістерський)
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітньо-професійна програма - Кібербезпека інформаційних технологій та систем

ЗАТВЕРДЖУЮ
Голова секції УБ, кафедра МБІС
_____ **Юрій ЯРЕМЧУК**
"20" Вересня 2023 р.

З А В Д А Н Н Я
на магістерську кваліфікаційну роботу студенту
Ковінько М. О.
(прізвище, ім`я, по-батькові)

1. Тема роботи Удосконалення методу виявлення автоматично генерованої дезінформації у соціальних мережах під час інформаційних конфліктів
Керівник роботи Грицак Анатолій Васильович, доцент кафедри МБІС, к.т.н.
(прізвище, ім`я, по-батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "18" вересня 2023 року № 247
2. Строк подання студентом роботи 04.12.2023
3. Вихідні дані до роботи: наукові статті по темі, існуюче програмне забезпечення по темі.
4. Зміст текстової частини: дослідити сучасні методи та підходи до виявлення автоматично генерованої дезінформації в соціальних мережах, особливо під час інформаційних конфліктів. Проаналізувати характеристики та методи впливу на користувачів соціальних мереж, а також мультимовне середовище у популярних соцмережах та його роль у поширенні дезінформації. Створити програмний засіб на основі розробленого методу, що дозволяє візуально спостерігати та аналізувати процеси поширення інформації в обраній соціальній мережі. Провести аналіз економічної ефективності розробленого програмного засобу, включаючи оцінку витрат на розробку та впровадження, а також потенційні переваги від його застосування у контексті інформаційної безпеки.

5. Перелік ілюстративного матеріалу (з точним зазначенням обов`язкових креслень)
У першому розділі наведено 9 рисунків, у другому 10 та у третьому розділі наведено 8 рисунків.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Основна частина	Грицак Анатолій Васильович, доцент кафедри МБІС, к.т.н.		
Економічна частина	Причепа Ірина Валеріївна, доцент кафедри ЕПВМ, к.е.н.		

7.Дата видачі завдання 20 вересня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи		Примітка
	Визначення напрямку магістерської роботи, формулювання теми	20.09.2023	24.09.2023	
	Аналіз предметної області обраної теми	25.09.2023	3.10.2023	
	Апробація отриманих результатів	4.10.2023	12.10.2023	
	Розробка алгоритму роботи	13.10.2023	25.10.2023	
	Написання магістерської роботи на основі розробленої теми	26.11.2023	16.11.2023	
	Розробка економічної частини	17.11.2023	23.11.2023	
	Передзахист магістерської кваліфікаційної роботи	24.11.2023	1.12.2023	
	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	2.12.2023	4.12.2023	
	Захист магістерської кваліфікаційної роботи	11.12.2023	15.12.2023	

Студент _____ ___Ковінько М. О._____
(підпис)

Керівник роботи _____ __Грицак А. В._____
(підпис)

АНОТАЦІЯ

УДК 004.89:070.16

Ковінько М.О. Удосконалення методу виявлення автоматично генерованої дезінформації у соціальних мережах під час інформаційних конфліктів. Магістерська кваліфікаційна робота зі спеціальності 125 – кібербезпека, освітня програма – кібербезпека інформаційних технологій та систем. Вінниця: ВНТУ, 2020. 105 с.

На укр. мові. Бібліогр.: 65 назв; рис.: 26.

У магістерській кваліфікаційній роботі було розроблено програмний засіб для вдосконалення методів виявлення фейкових новин у соціальних мережах за допомогою інтеграції штучного інтелекту. У теоретичній частині роботи було проаналізовано сучасні підходи до ідентифікації дезінформації та визначено ключові вимоги до методів виявлення. У практичній частині виконано розробку алгоритмів та програмної реалізації засобу, проведено випробування та аналіз результатів дослідження.

У технічній частині було розроблено інтерфейс та інструментарій для збору та аналізу даних з соціальних мереж, а також методики для автоматизації процесу виявлення фейкових новин.

У економічній частині роботи було проведено аналіз витрат, необхідних для розробки та впровадження програмного засобу, включаючи вартість ресурсів, обладнання та програмного забезпечення. Також було розглянуто потенційний комерційний ефект від реалізації розробленої програми, враховуючи її можливе використання державними структурами, медіаорганізаціями та приватними компаніями для поліпшення інформаційної безпеки та боротьби з дезінформацією.

Ключові слова: генерація, виявлення, дезінформація, соціальні мережі, штучний інтелект, машинне навчання, Facebook.

ABSTRACT

Kovinko M.O. Improving the method of detecting automatically generated disinformation in social networks during information conflicts. Master's qualification work in specialty 125 - cybersecurity, educational program - cybersecurity of information technologies and systems. Vinnytsia: VNTU, 2020. 105 c.

In Ukrainian. Bibliography: 65 titles; Figures: 26.

In the master's thesis, a software tool was developed to improve the methods of detecting fake news in social networks by integrating artificial intelligence. The theoretical part of the work analyzed modern approaches to identifying disinformation and identified key requirements for detection methods. In the practical part, the authors developed algorithms and software implementation of the tool, tested and analyzed the research results.

In the technical part, we developed an interface and tools for collecting and analyzing data from social networks, as well as methods for automating the process of detecting fake news.

The economic part of the work analyzed the costs required to develop and implement the software tool, including the cost of resources, hardware, and software. The potential commercial effect of the developed program was also considered, taking into account its possible use by government agencies, media organizations and private companies to improve information security and combat disinformation.

Keywords: generation, detection, disinformation, social networks, artificial intelligence, machine learning, Facebook.

ВСТУП

На сучасному етапі розвитку суспільства, коли інформаційна сфера набуває все більшої ваги, питання інформаційної безпеки держави стає надзвичайно актуальним. Особливо це стосується контексту інформаційних війн, де соціальні мережі використовуються як інструменти для поширення дезінформації. Методи математичного аналізу можуть внести значний вклад у вивчення інформаційної безпеки, зокрема у розробку технік виявлення та протидії дезінформації.

У контексті України, інформаційна безпека займає ключове місце у формуванні ефективної системи захисту від інформаційних атак, особливо у соціальних мереж, які є аренами інформаційних конфліктів. Активне використання соціальних мереж користувачами для обміну інформацією відкриває широкі можливості для зловмисників щодо реалізації атак через поширення маніпулятивної інформації.

У сучасному інформаційному світі, особливо в соціальних мережах, дезінформація є значною перешкодою, яка вимагає ретельної та організованої стратегії виявлення та реагування. В даній роботі буде зосереджено увагу на вдосконаленні поточних методів виявлення дезінформації, детальному розгляді їхніх недоліків і пошуку інноваційних способів потенційного підвищення точності та успіху розрізнення правди від брехні.

Тема дипломної роботи спрямована на удосконалення методів виявлення та аналізу процесів поширення інформації в соціальних мережах в умовах інформаційних війн. Особлива увага приділяється механізмам впливу на користувачів соціальних мереж.

Основними завданнями даної роботи є:

- Аналіз особливостей впливу на користувачів соціальних мереж генерованої дезінформації під час інформаційної війни;
- Удосконалення методу виявлення автоматично генерованої дезінформації у соціальних мережах під час інформаційних конфліктів;

- Розробка програмного засобу на основі удосконаленого методу для виявлення автоматично генерованої дезінформації;
- Аналіз економічної ефективності запропонованих рішень.

Тема цієї роботи є особливо актуальною у зв'язку з зростаючою роллю соціальних мереж як інструментів інформаційних війн, що вимагає розвитку нових підходів до інформаційної безпеки. Україна, як держава, що стикається з інформаційними викликами, має значний потенціал для розвитку цієї сфери, проте кількість досліджень у цій області ще недостатня. Розробка та вдосконалення методів для ефективного виявлення та перевірки дезінформації у соціальних мережах, особливо під час інформаційних криз та конфліктів, є досить актуальним. Це передбачає використання новітніх технологій штучного інтелекту та машинного навчання для аналізу великих обсягів даних, розпізнавання складних патернів і контекстів, що характерні для неправдивої інформації.

Об'єктом дослідження обрані суспільні відносини, які формуються в процесі інформаційного впливу на людей під час інформаційних війн, а предметом дослідження визначені процеси в соціальних мережах у період інформаційних конфліктів.

Предмет дослідження – соціальні мережі під час інформаційних конфліктів

Наукова новизна даної роботи полягає в удосконаленні методів аналізу поширення інформації у соціальних мережах в умовах інформаційної війни, що має важливе значення для підвищення рівня інформаційної безпеки країни.

1. ТЕОРЕТИЧНІ ОСНОВИ ВИЯВЛЕННЯ ДЕЗІНФОРМАЦІЇ У СОЦІАЛЬНИХ МЕРЕЖАХ

Інформаційно-психологічний вплив (ІПВ), а також інформаційно-психологічні операції (ІПСО), репрезентують собою дії, націлені на формування або зміну переконань, поведінки та світогляду осіб та колективів. В контексті соціальних мереж такі операції включають в себе різноманітні методики маніпуляції, що використовуються для досягнення стратегічних цілей у інформаційному просторі [1].

Серед них — стратегія утаємничення або вилучення ключових даних, що в соцмережах зустрічає складнощі через їхню відкритість для діалогу та зворотного зв'язку. Не дивлячись на це, можлива активність модераторів, які можуть видаляти чи блокувати такі матеріали. Ефективним також є переповнення інформаційного поля тривіальними даними, що ускладнює ідентифікацію значущого контенту.

Плутанина понять, яка дозволяє одній ситуації отримувати різноманітні трактування, також є ключовим інструментом інформаційних операцій, як і переведення уваги з суттєвого на другорядне. Величезний обсяг даних у соцмережах затруднює виокремлення основних тем, особливо якщо увага користувача розпорошується на безліч подій.

Маніпулювання суспільною думкою досягається також через розповсюдження архетипічних інформацій, які легко заповнюються індивідуальним змістом, і підсилюється віддачею переваги негативним новинам, які зазвичай привертають більше уваги, ніж позитивні. Така тактика відволікає від позитивних подій та сприяє формуванню негативного інформаційного фону [1].

Брехлива інформація у соцмережах може викликати не тільки недовіру, а й сіяти сумнів, який часто виявляється складним для перевірки.

В епоху, коли інформація стає широкодоступною, як зазначив засновник WikiLeaks Джуліан Ассандж, глобалізація не залишає місця секретам, але одночасно робить все більш проблематичним відділення правди від вигадки [1].

1.1 Концепція дезінформації та її вплив на суспільство

Дезінформація є важливим елементом інформаційної війни, яка проводиться з метою дестабілізації суспільства та підриву довіри до його інститутів. У рамках цього процесу, інформаційне протиборство використовується для досягнення політичних, психологічних і ідеологічних переваг, а також для впливу на масову свідомість.

Включаючи поширення оманливої громадської думки, «інформаційна війна» означає поширення неточних або спотворених даних. Вигадані новини, підроблені факти та пропаганда – це звичайна тактика, яка використовується для досягнення цієї мети, часто створюючи необґрунтовані упередження чи тривоги.

Ведення інформаційної війни може стосуватися двох рівнів взаємодії. На широкому рівні боротьба відбувається у сфері ЗМІ та соціальних мереж [2]. Тут боротьба за вплив на громадську думку має величезне значення. Однак на більш вузькому рівні війна передбачає цілеспрямовані військові операції з метою отримання переваги в інформаційному контексті під час військових конфліктів.

Суспільства, які страждають від неперевіреної інформації, можуть зрештою постраждати від політичної напруги та соціальної нестабільності, що робить наслідки дезінформації жахливими. Втрата довіри до надійних джерел і зростання популістських рухів, які полюють на страх і фанатизм, – лише деякі з серйозних проблем, які можуть виникнути внаслідок поширення дезінформації [2].

Омани становлять серйозну загрозу в соціальних мережах, оскільки вони можуть швидко поширюватися, завдаючи шкоди. Онлайн-платформи можна використовувати для створення розбіжностей серед людей, підриву довіри та формування суспільного сприйняття на користь політичних чи ідеологічних планів.

Стратегічне планування в інформаційній війні є ключем до отримання переваги та ефективного впливу на громадську думку противника та політичної стабільності. Без чіткої стратегії та знання того, як поширювати та контролювати

інформацію, неможливо успішно провести кампанію з дезінформації та забезпечити належний захист від інформаційних атак.

Вивчення громадської думки та аналіз політичних і соціальних контекстів дозволяють розробляти більш цілеспрямовані та дієві стратегії інформаційного впливу, які враховують вразливі аспекти суспільства і держави-опонента. Управління потоками інформації та визначення слабких точок в інформаційній системі противника дозволяють зосередити зусилля на найбільш чутливих для впливу сегментах.

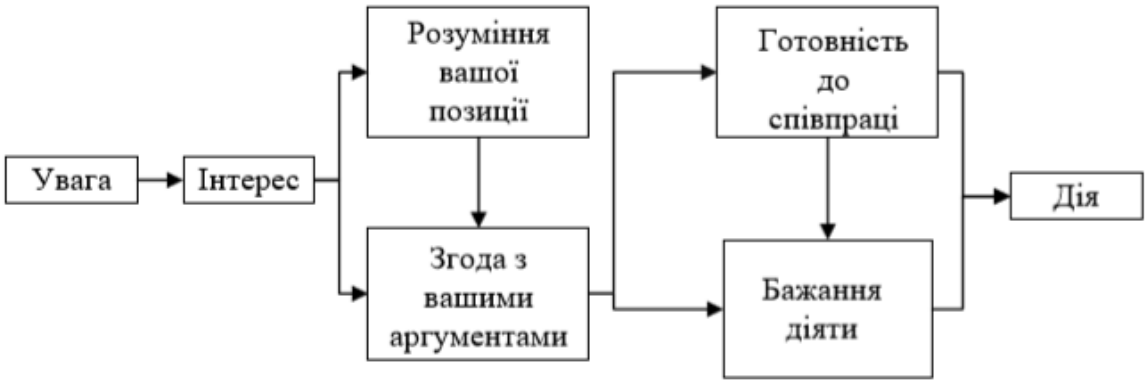


Рис. 1.1 – Психологічний механізм поширення інформації користувачами (за [1])

Відповідно до досліджень Курбана О.В [3]., методи інформаційної війни охоплюють широкий спектр засобів, від фізичного знищення джерел інформаційних загроз до складних технічних і електронних операцій. Фізичний вплив може включати знищення комунікаційної інфраструктури, радіолокаційних та інших систем збору даних. Такі заходи, як протирадіолокаційні ракети та графітові бомби, є прикладами засобів для унеможливлення функціонування ворожих інформаційних систем. Водночас, електромагнітне та радіоелектронне впливи можуть застосовуватись для перешкоджання або збоїв у роботі електронних систем супротивника [3].

Подальше розвиток стратегії інформаційної війни включає і використання кібер-засобів для ведення програмно-технічних атак. Це може включати в себе розповсюдження шкідливого програмного забезпечення, використання вірусів або

інших типів кібернетичної зброї, які можуть завдати шкоди критично важливим інформаційним системам та структурам противника.

Зрештою, ведення комплексного підходу до інформаційної війни вимагає глибокого розуміння всіх аспектів інформаційного простору та вміння адаптувати стратегії до мінливих умов і викликів.

Інформаційні методи впливу, справді, стають все більш важливими у сучасних конфліктах, де боротьба за "серця і розуми" людей ведеться за допомогою ЗМІ, Інтернету та інших платформ комунікації. Ці засоби дозволяють формувати громадську думку, поширювати пропаганду та дезінформацію, а також створювати ілюзію загального народного сприйняття подій, яким часто маніпулюють [4].

Методи програмних технологій, з іншого боку, включають злом, використання шпигунського та шкідливого програмного забезпечення, яке може порушити критичну інфраструктуру зловмисника, викрасти дані або створити хаос і недовіру в його інформаційних системах.

Гібридна війна, як концепція, об'єднує класичні військові дії з інформаційними війнами, економічними санкціями, дипломатичним тиском та іншими невійськовими заходами. Цей вид війни характеризується використанням різноманітних засобів і методів для досягнення політичних цілей, іноді без відкритого використання військової сили.

Валерій Герасимов, начальник Генерального штабу збройних сил росії, у 2013 році визначив концепцію гібридної війни, яка включала використання військової сили в поєднанні з інформаційними війнами, дезінформацією, кібератаками та використанням інших неконвенційних підходів. Ця концепція відображає зміщення акцентів у військовій стратегії, де не тільки сила і зброя вирішують результат конфлікту, але й інформаційний вплив, психологічні операції та боротьба за владу в інформаційному просторі [5].

Основною метою такої гібридної стратегії є дестабілізація ситуації всередині країни-супротивника, підрив довіри до її політичного керівництва та маніпуляція

громадською думкою для досягнення політичних цілей без широкомасштабного застосування звичайної військової сили.

Гібридні конфлікти застосовують широкий спектр інструментів і методик, що поєднують традиційні та невійськові засоби боротьби. Інформаційні операції грають ключову роль у гібридних війнах, оскільки вони дозволяють впливати на сприйняття, рішення та поведінку цільових аудиторій.

Прямі і непрямі інформаційні атаки є двома основними стратегіями в гібридній війні:

- **Пряма інформаційна атака** може включати цілеспрямоване впровадження дезінформації або пропаганди, щоб змінити сприйняття або поведінку громадян або уряду країни-супротивника.
- **Непряма інформаційна атака** зазвичай включає створення обставин, в яких супротивник сам приходить до невірних висновків або робить помилкові дії, виходячи з фальшивої або ввідної інформації.

Тактика, описана у вашому повідомленні, відображає різноманіття методів, які можуть використовувати держави або неурядові організації в гібридному конфлікті:

Фізичні атаки на інформаційну інфраструктуру, такі як електромережі або комунікаційні системи.

- **Кібератаки**, включаючи впровадження шкідливого ПЗ, вірусів і троянів.
- **Психологічні операції**, які можуть включати використання ЗМІ для поширення дезінформації або пропаганди.
- **Терористичні акти в інформаційному просторі**, такі як загрози або використання конфіденційної інформації.
- **Електронне придушення** комунікації і перевантаження мереж.
- **Маніпулювання інформацією**, включаючи вплив на операторів інформаційних систем.

- **Технічний вплив на обладнання**, щоб вивести з ладу бойову техніку та озброєння.

У випадку України, російська федерація використовувала гібридні методи ще до анексії Криму та конфлікту на сході України, зокрема, для здійснення політичного впливу та дестабілізації ситуації. Після 2014 року ці дії трансформувались у відкриті воєнні дії, проте інформаційна війна, цілеспрямовані кібератаки, політичні провокації та інші невійськові заходи продовжили грати важливу роль у цьому конфлікті [3].

Рисунок 1.2 – Інформаційна війна (за [2])

Включаючи різноманітну колекцію тактик, «асиметричні заходи», згадані раніше в тексті, охоплюють більше, ніж просто звичайний військовий конфлікт. Ці методи можуть включати економічні, політичні та соціальні дії, такі як сприяння

повстанським рухам, проведення підривної діяльності та запуск пропаганди чи інформаційних заходів для досягнення своїх цілей.

1.2 Роль соціальних мереж у формуванні громадської думки

Широкомасштабна інтеграція інформаційних технологій у суспільстві епохи постмодернізму спричиняє глибокі зміни у соціальних процесах та інституціях. Підвищення доступності інтернету значно розширює можливості для маніпуляцій свідомістю, оскільки цифровий простір стає майданчиком для впливу на особистісну самосвідомість та самоідентифікацію людини. У цьому контексті важливо усвідомити потенційні ризики, що їх приносить віртуалізація суспільного життя.

Прогресуюча віртуалізація життя робить реальний світ все менш безпосередньо сприйнятним, спонукаючи людей бачити його через фільтри масової інформації та інтернет-простору. Це призводить до розмивання границь між реальністю та віртуальним світом, відкриваючи шлях для створення утопічних проектів, які ігнорують ці демаркаційні лінії. Інтернет як простір, що містить необмежену кількість інформації, часто не піддається об'єктивній перевірці, роблячи своїх користувачів особливо вразливими до маніпуляцій [4].

Соціальні мережі, як невід'ємна складова інтернету, відіграють ключову роль у формуванні громадської думки. Вони стали ареною для інформаційних війн, де державні та недержавні актори, політичні організації, економічні угруповання, релігійні та етнічні спільноти змагаються за вплив на переконання та погляди людей. В контексті удосконалення методів виявлення автоматично генерованої дезінформації, соціальні мережі є ключовим полем битви, оскільки дозволяють швидко розповсюджувати інформацію та впливати на маси, часто зі значною точністю таргетування. Це створює необхідність розробки і впровадження більш вдосконалених технологічних і методологічних рішень для ідентифікації та протидії таким інформаційним загрозам.

Соціальні мережі, що отримали широке поширенняна початку 2000-х років, стали значущим чинником у трансформації інформаційного простору і впливу на

громадську думку. З моменту своєї появи, платформи як «Twitter» [22], «Facebook» [29] та «Instagram» [30] пройшли шлях від новаторських стартапів до глобальних мереж, що включають мільйони користувачів. Ці соціальні мережі стали не просто інструментами спілкування, але й могутніми засобами впливу, які можуть бути використані для формування та корекції поглядів і установок великої кількості людей [4].

Події 11 вересня 2001 року викликали переоцінку реалій безпеки, змінили уявлення про загрози та підкреслили необхідність пошуку спільнот зі схожими поглядами та ідеями. Соціальні медіа задовольняють цю потребу, забезпечуючи платформу, яка об’єднує людей з різних куточків світу, щоб висловлювати та обговорювати ідеї, про які раніше, можливо, не чули.

Однак така відкритість і доступність соціальних мереж також створює умови для їх використання в інформаційній війні. Організовані групи, державні та приватні організації виявили, що соціальні медіа можуть бути потужним інструментом для поширення інформації, яка відповідає їхнім інтересам, і маніпулювання громадською думкою. Використання алгоритмів таргетованої реклами, фільтрації контенту та створення ехокамер на базі соціальних мереж значно посилило вплив цих платформ.

У світлі цих фактів, соціальні мережі вимагають особливої уваги в контексті виявлення дезінформації. Їхня популярність та роль у сучасному інформаційному просторі роблять їх важливим полем для моніторингу та аналізу. Автоматизовані системи виявлення дезінформації, які враховують особливості спілкування в соціальних мережах, можуть стати ключем до захисту від інформаційного втручання та забезпечення достовірності інформаційного обміну.

Рисунок 1.3 – Інформаційне протиборство та його види (за [4])

Теорія соціальних мереж виходить із припущення, що поведінкові моделі і комунікативні процеси особистостей визначаються характером їхніх взаємовідносин. Ця теорія наголошує, що міцність соціальних зв'язків прямо впливає на частоту та інтенсивність комунікації між людьми, включаючи використання різноманітних медіа каналів. Інтернет і соціальні мережі, які є сучасними інноваціями в сфері комунікації, подальше зміцнюють ці зв'язки, дозволяючи людям та організаціям, які географічно роз'єднані, об'єднуватися на основі спільних інтересів.

Згідно з теорією соціальних мереж, віртуальна взаємодія не лише доповнює, а й посилює традиційні форми соціальної активності. Люди, які активно беруть участь у житті спільноти, також виявляють високий рівень персонального спілкування в Інтернеті. Це спостерігається у частому використанні електронної пошти, месенджерів та інших цифрових засобів комунікації для підтримки зв'язку. Ці висновки важливі для розуміння механізмів поширення інформації та дезінформації через соціальні мережі, оскільки вони підкреслюють значимість міцних соціальних вузлів у процесі впливу на громадську думку та поведінку. З огляду на це, вивчення та удосконалення методів виявлення дезінформації в соціальних мережах повинно враховувати ці соціальні взаємодії як фундаментальний аспект розробки ефективних інструментів аналітики [4].

Соціальні мережі трансформувалися в потужний інструмент інформаційних війн, використовуваний урядами, політичними та економічними організаціями, а також різними ідеологічними групами. Ця динаміка породжує протиріччя: з одного боку, є безмежний потік інформації, з іншого — зростає складність для індивіда в розрізненні правди від маніпуляції. Молодь, як найактивніші користувачі соціальних мереж, особливо схильна до ідеологічного впливу і маніпуляцій, що робить їх пріоритетною мішенню для інформаційних атак.

Соціальні мережі перетворюються на платформу для політичного впливу, де думки висловлюються відкрито і де влада може відчути суспільні настрої, реагуючи на них або ігноруючи. Вони стають інструментом для моніторингу протестних настроїв, підірвавши при цьому традиційну монополію влади на інформацію. Звідси владі вдається уникати стратегічних помилок, проте це ж робить інтернет-спільноту чутливою до маніпуляцій [2].

Завдяки децентралізованій природі та відсутності єдиного контрольного центру, соціальні мережі опиняються поза традиційними методами державного регулювання інформації, що надає їм унікальні можливості для координації опозиційних рухів і масових протестів. Як показали "кольорові революції" в різних країнах, соціальні мережі стали каталізатором змін, організуючи і надихаючи маси на боротьбу з існуючими режимами.

Блогосфера відіграє ключову роль в нейтралізації інформаційних блокад, створюючи альтернативні канали зв'язку там, де офіційні ЗМІ не здатні швидко реагувати або були придушені. У контексті удосконалення методів виявлення автоматично генерованої дезінформації, необхідно враховувати ці аспекти, адже соціальні мережі виступають не тільки як середовище комунікації, але й як поле для інформаційних операцій, що вимагають розвинених засобів виявлення та протидії.

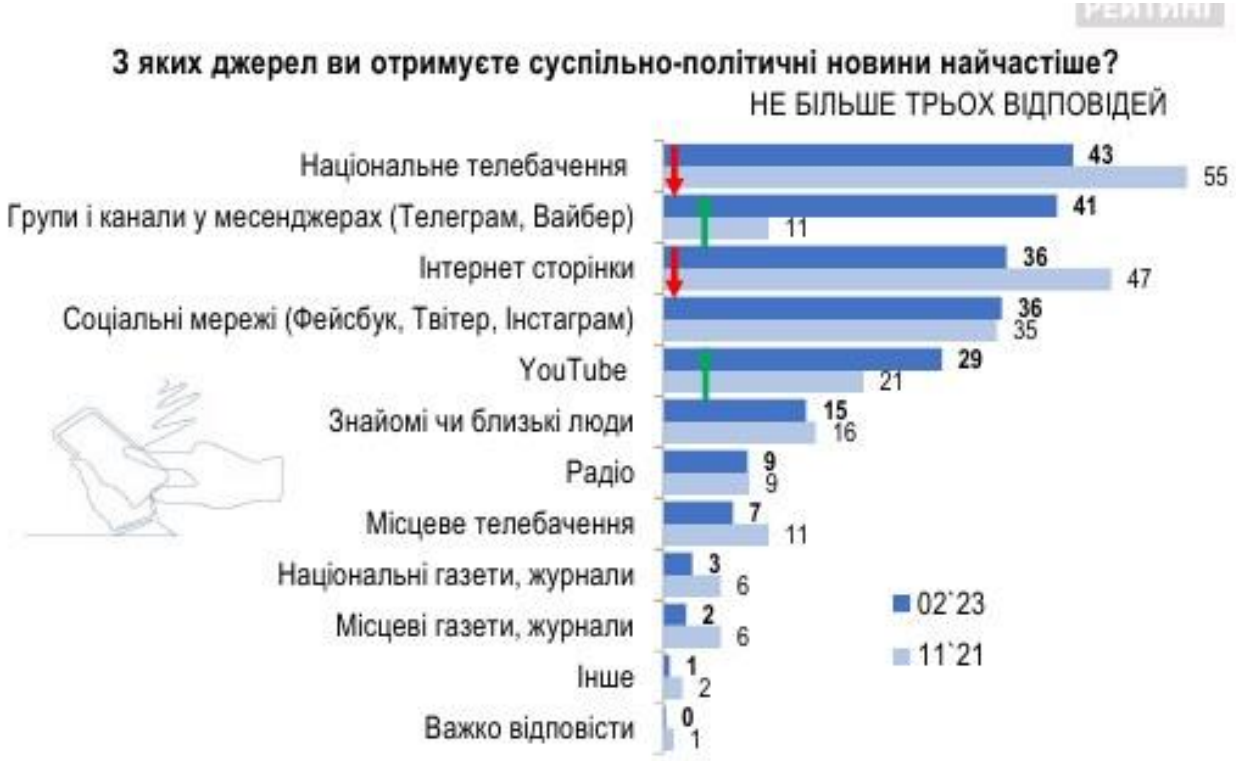


Рисунок 1.4 – Середовище впливу на свідомість людини (розроблено автором за інтернет даними [5])

Організаційно-інформаційний вплив на особистість має на меті не лише поверхневі зміни, але й глибинну трансформацію культурних та духовних аспектів суспільства. Однією з цілей такого впливу є переривання ланцюга національної пам'яті та цінностей, що веде до культурного розриву між поколіннями. Інформаційний вплив, якщо він систематичний і постійний, має потужний деструктивний потенціал, здатний підірвати суспільні традиції та цінності, переосмислювати культурні досягнення, та навіть знущатися з традиційного способу життя нації [4].

Такий злам культурного самосвідомості може призвести до кінця ідейного опору, змінюючи тип і стиль управління країною, заміняючи національні інтереси і цілі державного розвитку. Особливої шкоди може бути завдано через так званий «витік мізків», коли втрата наукових та культурних фахівців супроводжується економічними втратами, понесеними державою на їх освіту та розвиток.

Досягнення повного успіху в такому інформаційному конфлікті можливе, коли вдається втягнути в процес правлячу еліту противника, що часто досягається через використання різноманітних методів впливу та підкупу.

Створення мережі агентів впливу, що діють всередині країни-супротивника, може додатково посилити ефективність таких дій [6].

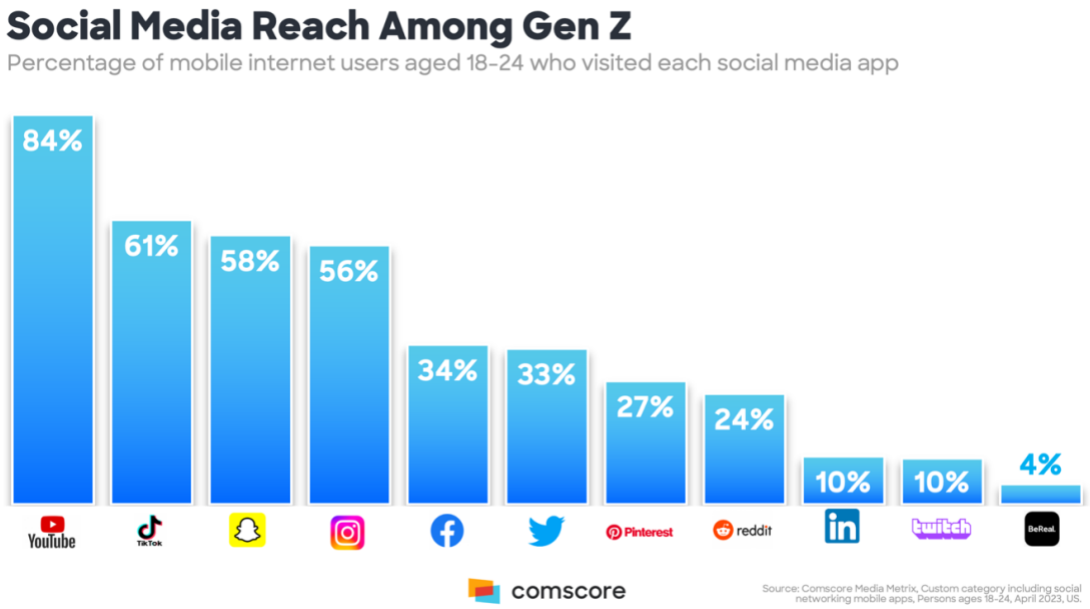


Рис. 1.5 Самі популярні соціальні мережі за данними comScore (за [6])

У контексті розробки методів виявлення автоматично генерованої дезінформації, важливо усвідомити, що соціальні мережі можуть використовуватися не тільки для швидкого поширення інформації, але й для стратегічної зміни культурних орієнтирів та цінностей суспільства. Це вимагає розробки складних аналітичних інструментів, здатних розпізнавати не тільки окремі факти дезінформації, але й виявляти та протидіяти комплексним інформаційним кампаніям, які мають на меті глибоку трансформацію суспільної свідомості.

Інформаційно-смисловий вплив має на меті дестабілізацію особистості, її дезорієнтацію у просторі культурних та духовних цінностей. Такий вплив може призвести до втрати індивідом зв'язку з національними традиціями та історичною пам'яттю. Інформаційно-емоційний удар нищить здатність до адекватного сприйняття реальності, викликаючи стани апатії або агресії. Інформаційно-

моральний вплив еродує встановлені норми, замінюючи їх новими, часто імплантованими ззовні концепціями добра та зла. Нарешті, інформаційно-історичний удар відчужує індивіда від його коріння, спричиняючи втрату ідентичності та почуття приналежності до певної культурної спадщини [4].

Розглядаючи різноманітність форм інформаційної війни, можна розрізняти інформаційно-психологічну, психолого-політичну та інформаційну війну як таку. Інформація стає ефективною зброєю лише тоді, коли вона сприймається цільовою аудиторією, привертаючи увагу, викликаючи емоційні реакції та зацікавленість. Саме тому важливо розвивати знання про інформацію, її моделювання, а також вивчати психотехнології та ноотехнологічні особливості людського сприйняття та реакцій.

Інформаційна складова гібридної війни виконує забезпечувальні функції на кожному з етапів конфлікту. На початку вона створює передумови для виникнення кризи, далі — дає підстави для втручання держави-агресора, і в кінці — формує медійне поле для легітимізації дій нападника [5].

У контексті вдосконалення методів виявлення дезінформації, особливу увагу слід звернути на розробку інструментів, здатних розпізнати не лише окремі факти неправдивої інформації, а й цілісні інформаційні кампанії, спрямовані на дестабілізацію суспільства і культури. Врахування цієї складності та мультидисциплінарного характеру інформаційної війни є ключовим у створенні ефективних систем протидії гібридним загрозам.

Соціальні мережі суттєво впливають на структуру та характер міжособистісних комунікацій, формуючи нові моделі взаємодії між користувачами. У мережах існує безліч типів соціальних зв'язків, які можуть бути поверхневими або глибокими, епізодичними або стабільними, формальними або інтимними. Визначальним у створенні віртуальної соціальної мережі є те, які саме зв'язки вибирає і підтримує індивід, що в свою чергу може базуватися на родинних, дружніх, професійних чи географічних зв'язках [4].

Вплив, який може бути здійснений через соціальні мережі, залежить від того, яка інформація або емоція передається. Методи впливу можуть варіюватися від переконання до навіювання чи навіть зараження, де останнє є найдавнішим методом і полягає у передачі емоційного стану від однієї особи до іншої, часто звертаючись до несвідомих реакцій людини.

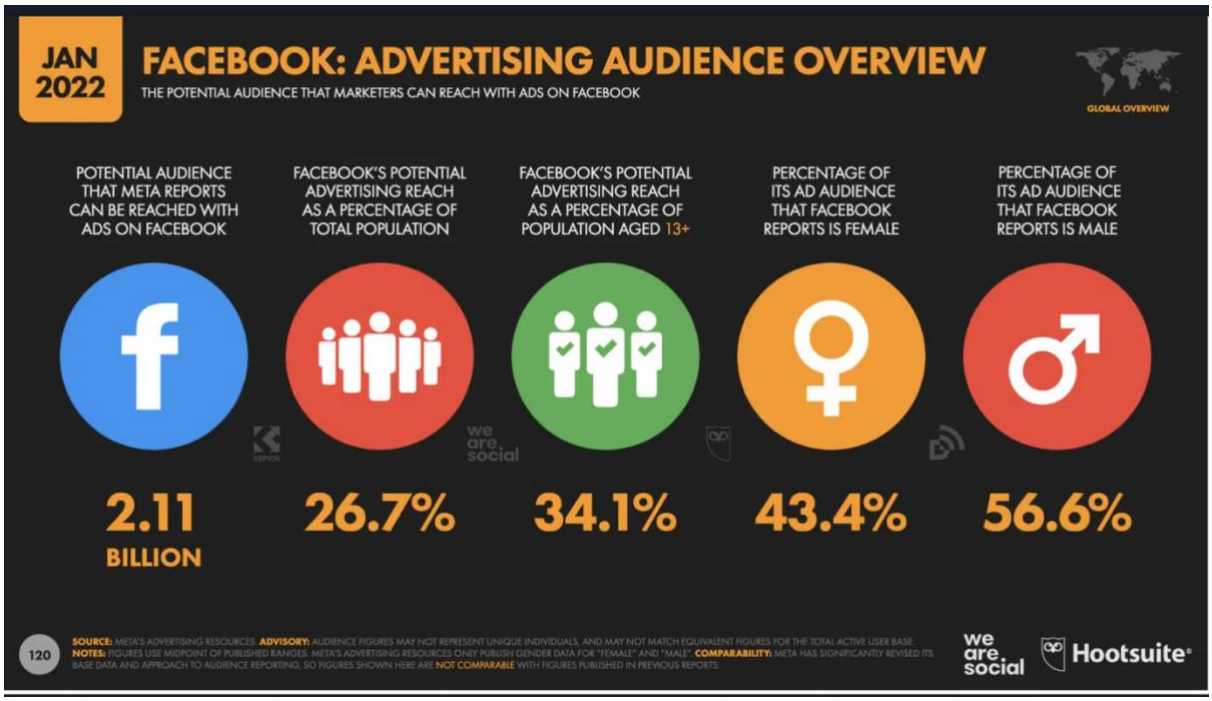


Рисунок 1.6 – Демографічна статистика соц. мережі Facebook (графік наведений іноземною мовою згідно з джерелом інформації [7])

У соціальних мережах інформаційний вміст будь-якого повідомлення ("поста") має потенціал до значного впливу, залежно від його контенту та контексту [4]. Спільноти, які створюють панічні настрої або поширюють фейкові новини, використовують ці платформи для досягнення своїх цілей, в тому числі шляхом зараження певними емоціями.

Піддатливість навіюванню та здатність до критичного сприйняття інформації варіюються в залежності від індивідуальних особливостей людини. Навіювання особливо ефективне для людей з менш стабільними установками та тих, хто схильний до стрімких коливань уваги [5].

В контексті боротьби з автоматично генерованою дезінформацією, розуміння цих механізмів є критично важливим. Соціальні мережі можуть служити не лише

платформами для обміну інформацією, але й потужними інструментами психологічного впливу. Методи виявлення та аналізу повинні бути здатні ідентифікувати не тільки зміст інформації, але й її потенційний вплив на емоції та поведінку користувачів, що дозволить розробляти ефективні стратегії протидії маніпулятивним технікам у цифровому просторі [7].

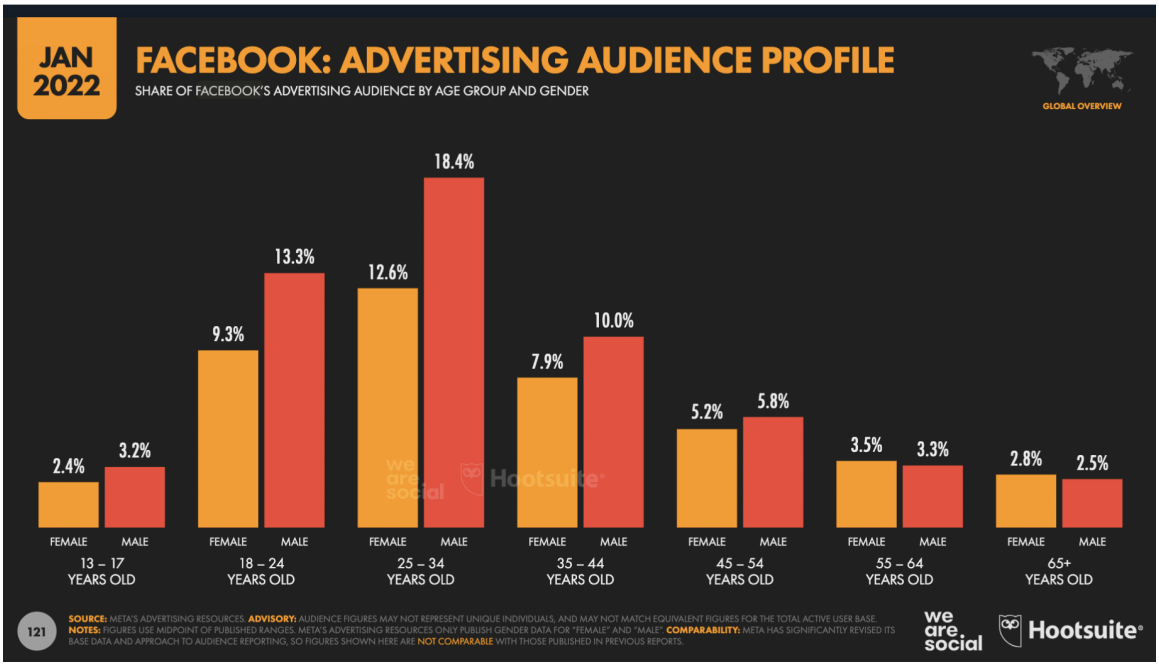


Рисунок 1.7 – Розподіл користувачів Facebook (графік наведений іноземною мовою згідно з джерелом інформації [7])

Методи навіювання в соціальних мережах часто покликані знизити критичне ставлення до інформації, використовуючи емоційний вплив. Так, прийом перенесення полягає у створенні асоціацій між новою інформацією та вже знайомими і позитивно сприйнятими об'єктами або явищами, щоб спонукати до позитивної реакції на цю інформацію. Негативне перенесення також можливе і веде до відторгнення інформації.

Переконання, у свою чергу, орієнтується на логічну сторону сприйняття та потребує більш високого рівня розвитку логічного мислення від одержувача [5]. Для ефективного переконання необхідно, щоб зміст і форма повідомлення відповідали рівню сприйняття та когнітивним здібностям особистості.

Процес переконання починається з оцінки джерела інформації. Якщо слухач виявляє несумісність нових даних з наявною у нього інформацією або сумнівається у правдивості джерела, довіра до цього джерела знижується. Авторитетність особи, що переконує, також піддається перевірці; логічні помилки можуть знецінити навіть офіційний статус або авторитет джерела [6].

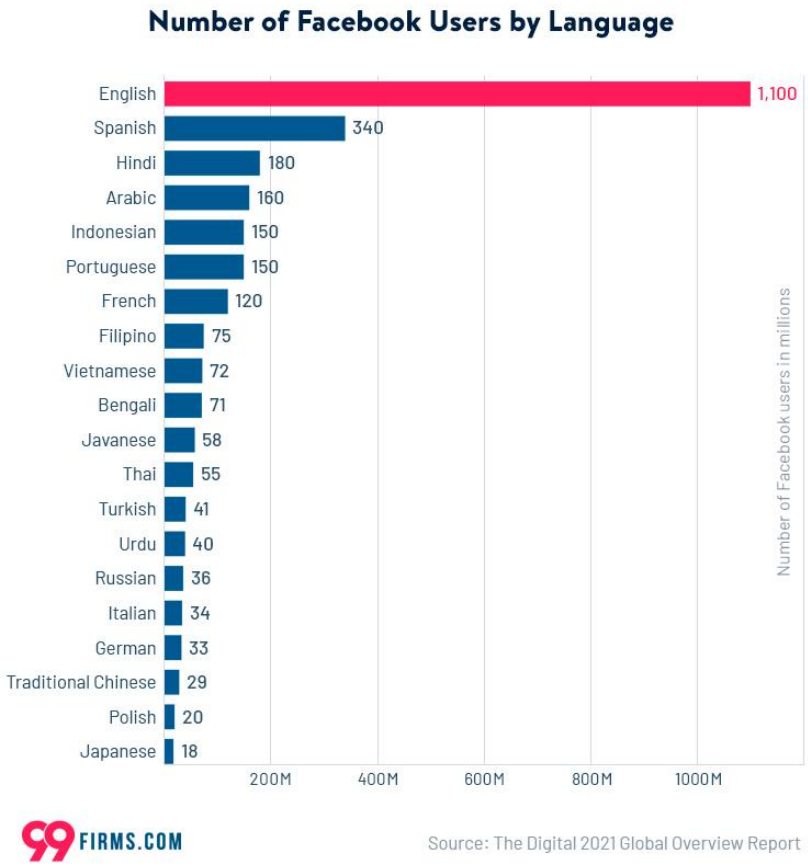


Рисунок 1.8 – Мовний розподіл користувачів Facebook (графік наведений іноземною мовою згідно з джерелом інформації [8)

Схожість установок між джерелом і одержувачем інформації сприяє ефективності переконання. Якщо є значна розбіжність, переконання може виявитися неефективним. У такому випадку оптимальною стратегією є налагодження спільності поглядів, яка може стати основою для подальшого переконання.

В контексті виявлення автоматично генерованої дезінформації в соціальних мережах, важливо аналізувати не тільки контент, але й методи впливу, які

використовуються для розповсюдження інформації [6]. Виявлення та розуміння цих методів може допомогти у створенні більш точних інструментів для ідентифікації маніпулятивних та введених в оману повідомлень, а також розвитку стратегій для зміцнення критичного мислення та медіаграмотності серед користувачів соціальних мереж.

1.3 Огляд методів виявлення дезінформації

Нейронні мережі та обробка природної мови (NLP) [9] відіграють ключову роль у виявленні дезінформації, особливо в умовах інформаційних конфліктів у соціальних мережах. Вони дозволяють аналізувати великі обсяги текстових даних, виявляючи приховані зразки, аномалії та викривлення в інформаційних потоках.

Глибинне навчання та NLP

- **Архітектури глибинного навчання**: Сучасні архітектури, такі як конволюційні нейронні мережі (CNN) та рекурентні нейронні мережі (RNN), включаючи LSTM і GRU, ефективно обробляють послідовні дані, що є характерними для мовних конструкцій [9]. Вони здатні визначати контекстуальні залежності та відтворювати складні моделі мови.
- **Трансформерні моделі**: Такі моделі, як BARD [10], GPT-4 [11], використовують механізми самоуваги для аналізу важливості окремих частин тексту, що дозволяє глибше розуміти контекст і нюанси мовлення. Це особливо важливо для виявлення тонкої та складної дезінформації.

Застосування NLP у виявленні дезінформації

- **Аналіз сентименту**: Цей метод дозволяє оцінювати емоційний заряд тексту, що може вказувати на маніпулятивні техніки в повідомленнях. Автоматизоване визначення тональності тексту допомагає виявляти спотворення або недостовірну інформацію.
- **Аналіз тематичної згадки (Topic Modeling)**: Використовується для виявлення основних тем в текстових даних. Це дозволяє ідентифікувати, чи

зосереджується конкретний інформаційний потік на певних темах, що є типовим для дезінформаційних кампаній.

- **Обробка природної мови для виявлення фейків**: Алгоритми NLP можуть визначати нелогічні, суперечливі або неправдоподібні висловлювання у текстах, що є ознаками дезінформації.

Одним з основних викликів у використанні NLP для виявлення дезінформації є постійна еволюція мовних патернів та методів маніпуляції [9]. Для боротьби з цими викликами, системи, що базуються на NLP, повинні постійно оновлюватися і адаптуватися до нових форм і методів дезінформації.

Рисунок 1.9 – Принцип роботи NLP для визначення дезінформації (за [9])

Іншим аспектом є необхідність врахування культурних та контекстуальних особливостей мови, що потребує більш складних і гнучких моделей NLP.

Впровадження та розвиток технологій, заснованих на нейронних мережах та NLP, відіграє ключову роль у вдосконаленні методів виявлення дезінформації, дозволяючи більш ефективно протистояти інформаційним загрозам у соціальних мережах.

Аналіз метаданих стає все важливішим інструментом у виявленні дезінформації в соціальних мережах. Метадані – це дані про дані, що містять

інформацію про автора, час публікації, геолокацію, тип пристрою, використані програмні засоби та інші характеристики, які можуть бути використані для аналізу і виявлення підозрілих або нехарактерних шаблонів поведінки [12].

Важливість метаданих у виявленні дезінформації

- **Визначення аномалій**: метадані можуть допомогти ідентифікувати незвичайні або підозрілі активності, такі як нехарактерні часові штампи для публікацій або аномалії в геолокації. Наприклад, публікації, що постійно здійснюються з різних країн протягом короткого часу, можуть вказувати на автоматизовані боти.
- **Аналіз зв'язків**: метадані дозволяють аналізувати зв'язки між акаунтами та групами користувачів. Це може включати аналіз мережевих графів, який виявляє координовані мережі, що здійснюють спільні дії для розповсюдження дезінформації.

Методи аналізу метаданих

- **Статистичний аналіз**: використання статистичних методів для аналізу метаданих може виявити відхилення від норми, які можуть вказувати на маніпулятивну поведінку.
- **Машинне навчання**: застосування алгоритмів машинного навчання для аналізу метаданих може допомогти в автоматичному виявленні складних шаблонів, пов'язаних з дезінформацією. Моделі можуть бути навчені на історичних даних для ідентифікації потенційних підозрілих активностей.

Аналіз метаданих пов'язаний з певними викликами, зокрема з питаннями конфіденційності та захисту даних [12]. Важливо збалансувати потребу у виявленні дезінформації з правами користувачів на приватність.

Крім того, існує потреба у розвитку більш точних і досконалих алгоритмів, які можуть адаптуватися до постійно змінюваних тактик і стратегій поширення дезінформації.

У сукупності, аналіз метаданих є важливою складовою комплексного підходу до виявлення дезінформації в соціальних мережах. Цей метод допомагає виявляти не лише окремі факти дезінформації, а й визначати загальні шаблони поведінки, що сприяють поширенню фальшивих новин і маніпулятивного контенту.

Аналіз графів соціальних зв'язків є потужним інструментом для виявлення дезінформації в соціальних мережах[12]. Цей підхід дозволяє виявити не лише індивідуальні акти дезінформації, але й складні мережеві структури та взаємодії, які лежать в основі координованих кампаній.

Визначення та аналіз графів

- **Структура графу**: граф соціальних зв'язків уявляє собою мережу, де вузли представляють користувачів, а ребра - зв'язки між ними (наприклад, дружба, підписки, спільні вподобання). Аналізуючи ці зв'язки, можна виявити взаємодії та поведінкові шаблони.
- **Виявлення спільнот**: алгоритми виявлення спільнот допомагають ідентифікувати групи користувачів з схожими інтересами або поведінкою. Такі групи можуть бути ознакою координованих дій, особливо якщо вони активно розповсюджують певні повідомлення.

Алгоритми аналізу графів

- **Алгоритми ранжування**: алгоритми, такі як PageRank [13], можуть використовуватися для визначення впливових користувачів або вузлів у соціальних мережах, які можуть сприяти розповсюдженню дезінформації.
- **Аналіз топології мережі**: вивчення структури графів допомагає ідентифікувати нетипові патерни зв'язків, які можуть вказувати на штучні або маніпулятивні мережі.

Застосування аналізу графів

- **Виявлення бот-мереж**: штучні акаунти часто створюються для масового розповсюдження дезінформації. Через аналіз графів можна ідентифікувати такі бот-мережі завдяки їхній нетиповій структурі та поведінці.

- **Ідентифікація координованих дій**: складні алгоритми аналізу графів можуть виявити приховані зв'язки та координовані дії, що часто є частиною дезінформаційних кампаній.

Аналіз графів соціальних зв'язків стикається з викликами, пов'язаними з обробкою великих обсягів даних та визначенням смислового контексту зв'язків. Крім того, необхідно враховувати постійну еволюцію соціальних мереж та зміну тактик розповсюдження дезінформації.

Використання аналізу графів соціальних зв'язків є важливим компонентом у боротьбі з дезінформацією, оскільки цей метод дозволяє розкрити складні мережеві структури та координовані дії, які лежать в основі багатьох дезінформаційних кампаній.

1.4 Використання візуальної інформації як засобів дезінформації

Візуальний контент, зокрема меми, стає все більш популярним інструментом для дезінформації. Через їхню легкість сприйняття та швидке поширення, меми є потужним засобом впливу на громадську думку, особливо в українському контексті.

Меми як інструмент дезінформації

- **Емоційний вплив**: Меми часто містять гумор, сарказм або іронію, що сприяє їх швидкому поширенню. Однак це також робить їх потужним засобом для передачі прихованих повідомлень або дезінформації.
- **Приклади українських мемів**: Популярні меми, які використовувалися в Україні для поширення дезінформації, можуть включати зображення відомих політиків або громадських діячів у несподіваному або карикатурному контексті, що змінює сприйняття громадськістю цих осіб.
- **Символіка та асоціації**: Меми часто використовують символіку, яка може мати певні культурні або історичні асоціації, спотворюючи або перекручуючи їх первісне значення для маніпуляції громадською думкою.

Візуальна інформація та її роль у дезінформації

- **Маніпуляції з зображеннями**: Використання фотошопу та інших графічних інструментів для зміни зображень може створити помилкове враження про події або осіб. Це особливо важливо у контексті політичної пропаганди та маніпуляцій громадською думкою.
- **Поширення через соціальні мережі**: Візуальний контент легко поширюється через соціальні мережі, що забезпечує швидке та ефективне розповсюдження дезінформації серед широкої аудиторії [14].

Виявлення дезінформації у візуальному контенті, особливо в мемах, є складним завданням через їхню багатогранність та суб'єктивність інтерпретацій. Необхідно розвивати складні методи аналізу зображень та контексту, включаючи використання технологій штучного інтелекту та машинного навчання для ідентифікації маніпулятивного вмісту. Крім того, важливим є розвиток медіаграмотності серед користувачів, щоб вони могли критично аналізувати візуальну інформацію та розпізнавати потенційну дезінформацію.

1.5 Інформаційні конфлікти та надзвичайні ситуації

Інформаційні конфлікти та надзвичайні ситуації в сучасному світі часто супроводжуються інтенсивним розповсюдженням дезінформації. У таких умовах, швидке поширення неперевіреної або навмисно сфабрикованої інформації може призвести до паніки, соціальної нестабільності та може негативно впливати на управління кризовими ситуаціями [15].

У контексті інформаційних конфліктів, інформація часто перетворюється на знаряддя політичної боротьби. В політичних конфліктах вона використовується не лише для передачі фактів, але й як спосіб впливу на громадську думку, досягнення конкретних політичних цілей, дискредитації опонентів або навіть маніпулювання виборчими процесами. Ця політизація інформації веде до створення інформаційних кампаній, які спрямовані на формування певного наративу або переконання громадськості у певних ідеях чи концепціях.

Соціальні мережі в сучасному цифровому світі відіграють вирішальну роль у поширенні інформації. Їхня специфіка полягає у швидкості та широті охоплення аудиторії, що робить їх ідеальним інструментом для швидкого розповсюдження як достовірної, так і фальшивої інформації. У ситуаціях інформаційних конфліктів, це особливо важливо, оскільки швидке поширення дезінформації через соціальні мережі може ускладнити процес відрізнення правдивих даних від маніпулятивних повідомлень, впливаючи на громадську свідомість та сприйняття реальності.

У надзвичайних ситуаціях, таких як природні катастрофи, великі аварії або терористичні акти, швидкість поширення інформації може мати рішуче значення. В цей час кожна хвилина важлива, і швидке розповсюдження даних може бути критично важливим для рятувальних заходів та уникнення подальших жертв. Проте, ця ж швидкість може спричинити паніку та дезорієнтацію, якщо поширювана інформація виявляється недостовірною або спотвореною. Невірна інформація може призвести до хаосу, спричинити непотрібний рух населення чи навіть завдати шкоди зусиллям рятувальних служб [15].

Потік надійних, точних і актуальних даних для громадськості дуже важливий для управління надзвичайними ситуаціями. Боротьба з фейковими новинами та дезінформацією вимагає швидкої ідентифікації та відкидання неправдивої інформації. Крім того, важливо пропонувати зрозумілу та доступну інформацію з авторизованих джерел, щоб запобігти спекуляціям і непорозумінням. Вкрай важливо переконатися, що офіційна інформація є чіткою та легкою для розуміння.

Ефективне управління інформацією в таких умовах вимагає злагодженої роботи урядових структур, ЗМІ, соціальних мереж та громадськості.

Встановлення надійних каналів комунікації, регулярне оновлення даних та відкритість для запитань та занепокоєнь громадян є важливими складовими успішного управління інформаційним потоком під час кризових ситуацій.

У сфері інформаційних конфліктів та надзвичайних ситуацій, особливу увагу слід приділити розробці комплексних стратегій для ефективного реагування на виклики, пов'язані з дезінформацією. Один з ключових аспектів полягає у

використанні передових технологій аналізу даних та моніторингу соціальних мереж, що дозволяє оперативно виявляти зміни в інформаційному просторі та швидко реагувати на них. Важливою частиною такої стратегії є підвищення рівня медіаграмотності населення, щоб люди могли самостійно розрізняти достовірні джерела інформації від недостовірних та критично оцінювати отриману інформацію [17].

Під час інформаційних криз, швидкість та точність реагування на поширення дезінформації стають вирішальними. Це вимагає від урядів, ЗМІ та інших інформаційних агентів не тільки моніторити інформаційний простір, але й активно долучатися до процесу формування громадської думки, надаючи чіткі, точні та перевірені дані. Особливо це стає актуальним у контексті боротьби з фейковими новинами, де необхідно швидко ідентифікувати та спростовувати неправдиву інформацію, щоб запобігти її негативному впливу на суспільство та запобіганню паніки.

Також нагальною стає потреба у створенні та підтримці міжнародних та внутрішніх мереж співпраці між урядовими структурами, незалежними медіа, громадськими організаціями та академічними установами. Це необхідно для ефективного обміну інформацією, ресурсами та досвідом у сфері виявлення та протидії дезінформації.

У контексті інформаційних конфліктів та надзвичайних ситуацій, таких як війна в Україні [18] та Державі Палестина [19], важливість надійної та точної інформації набуває особливої актуальності. В Україні, наприклад, інформаційні війни стали невід'ємною частиною військового конфлікту, при цьому використання соціальних мереж як засобу поширення інформації та дезінформації істотно впливає на громадську думку та міжнародну політику. Водночас, в Палестині, Ізраїлі та на росії інформаційні кампанії використовуються для мобілізації населення, впливу на міжнародне співтовариство та сформування загального наративу конфлікту.

Швидке та часто неконтрольоване розповсюдження інформації через соціальні мережі може призвести до великих непорозумінь та спотворення реальності, що особливо небезпечно у часи кризових ситуацій. Тому ефективне управління інформацією, включаючи швидку ідентифікацію та виправлення дезінформації, є критично важливим для забезпечення стабільності та запобігання подальшій ескалації конфлікту.

В кінцевому підсумку, вирішення проблеми дезінформації у сучасному інформаційному просторі вимагає комплексного підходу, який поєднує технологічні рішення, освітні ініціативи та активне взаємодію всіх зацікавлених сторін.

1.6 Внесок штучного інтелекту в ідентифікацію дезінформації

Внесок штучного інтелекту (ШІ) у виявлення дезінформації в соціальних мережах є надзвичайно значущим, оскільки він відкриває широкі можливості для аналізу великих обсягів даних з високою точністю та швидкістю. ШІ може виявляти складні шаблони та взаємозв'язки, які важко або неможливо ідентифікувати людським аналітикам [20]. Використання алгоритмів машинного навчання та глибокого навчання дозволяє не тільки аналізувати текстовий контент, але й ефективно обробляти візуальні та аудіальні дані.

Один із ключових підходів штучного інтелекту (ШІ) у виявленні дезінформації полягає у використанні нейронних мереж для аналізу шаблонів мовлення. Ці шаблони часто зустрічаються у маніпулятивних та дезінформаційних повідомленнях. Нейронні мережі, особливо ті, що базуються на моделях глибокого навчання, можуть розпізнавати тонкі та складні закономірності у великих обсягах тексту, які людське око може не вловити.

Одна з ключових функцій нейронних мереж - аналіз сентименту текстів. Цей процес включає визначення емоційного тону або настрою, що міститься у повідомленні. Наприклад, нейронна мережа може бути тренована розрізняти позитивні, негативні або нейтральні тональності тексту. Це виконується шляхом

навчання мережі на великій кількості текстових даних, де кожен текст має попередньо визначену емоційну оцінку.

Сентимент Скор=$\frac{\sum_{i}^{N} =1\omega i \times Si}{\sum_{I}^{N} =1\omega i}$, де *Si* - сентимент кожного слова або фрази, а *wi* - вага або значимість цього слова у контексті загального повідомлення.

Далі, нейронні мережі можуть використовуватися для розпізнавання більш складних шаблонів у текстах, що є характерними для маніпулятивних повідомлень. Це може включати викривлення фактів, використання натяків, апеляцію до емоцій аудиторії, або використання мови, що викликає ворожнечу. Тренування таких моделей може відбуватися на даних, які містять приклади реальних дезінформаційних кампаній.

Нейронні мережі в таких випадках використовують комбінацію різних технік обробки мови, таких як векторизація тексту, аналіз залежностей між словами, та розпізнавання контексту. Вони можуть аналізувати текст не тільки на рівні окремих слів або фраз, але й на рівні цілого речення або абзацу, розуміючи більш глибокий зміст та потенційно маніпулятивні аспекти [20].

Використання нейронних мереж у боротьбі з дезінформацією відкриває нові горизонти у виявленні та протидії цьому явищу. Ці методи дозволяють швидко аналізувати великі обсяги даних, виявляти складні шаблони та адаптуватися до постійно змінюючихся методів дезінформації.

Застосування штучного інтелекту (ШІ) виходить за рамки аналізу текстових даних, поширюючись також на область візуального контенту, включаючи зображення та відео. Алгоритми комп'ютерного зору, які є частиною ШІ, відіграють важливу роль у виявленні та аналізі візуальної дезінформації. Це особливо актуально в контексті сучасних соціальних мереж, де зображення та відео часто використовуються для поширення маніпулятивних повідомлень [16].

Одним з ключових завдань комп'ютерного зору є виявлення маніпуляцій з зображеннями. Це може включати в себе виявлення використання фотошопу, цифрових модифікацій або інших форм візуальних змін, які могли б ввести в оману

або спотворити реальність. Наприклад, алгоритми можуть шукати незвичайні відхилення у текстурах, освітленні, кольоровій гамі або геометрії зображення, які можуть свідчити про цифрові втручання.

Такі алгоритми можуть включати порівняння кольорових гістограм, аналіз країв об'єктів та виявлення нелогічних тіней або світлових відблисків. Вони також можуть використовувати глибоке навчання для вивчення характерних ознак природних зображень і порівняння їх з потенційно зміненими зображеннями.

У сфері відеоконтенту ШІ також може виявляти маніпуляції та дезінформацію. Це включає аналіз руху, змін у кадрах, а також виявлення глибоких підробок (deepfakes) [21], де обличчя або частини відео можуть бути замінені або суттєво змінені за допомогою ШІ.

Алгоритми глибокого навчання можуть виявляти невідповідності в рухах обличчя, аномалії в синхронізації звуку та зображення, а також інші ознаки, які є нехарактерними для автентичних відеозаписів. Наприклад, моделі нейронних мереж можуть бути треновані на великих наборах даних для виявлення незвичайних патернів руху губ або міміки, які часто зустрічаються в глибоких підробках.

Підхід ШІ до аналізу візуального контенту полягає у використанні поєднання різноманітних технік та методів, що дозволяє всебічно оцінити ймовірність маніпуляцій. Використання таких алгоритмів може значно підвищити точність виявлення дезінформації та внести значний вклад у боротьбу з фейковими новинами та іншими видами маніпулятивного контенту в соціальних мережах.

$$Dv = \frac{1}{N}\sum_{i}^{N} = 1\left|Vi - \widehat{Vı}\right| \quad ^{2}$$

де *Dv* - міра відхилення від оригінального зображення, *Vi* - оригінальне зображення, Vi^- зображення після обробки алгоритмом, *N* - кількість зображень.

Застосування штучного інтелекту (ШІ) у виявленні дезінформації відкриває нові перспективи у швидкому та точному аналізі великих обсягів даних, що

надзвичайно важливо для оперативного реагування на дезінформаційні загрози, особливо в динамічному та часто змінюваному середовищі соціальних мереж.

Сучасні алгоритми ШІ, зокрема, машинне навчання та глибоке навчання, здатні обробляти великі обсяги інформації набагато швидше, ніж це можливо за допомогою традиційних методів. Це досягається завдяки здатності ШІ аналізувати та вчасно ідентифікувати складні шаблони та взаємозв'язки, що можуть вказувати на дезінформацію. Наприклад, застосування алгоритмів ШІ для аналізу текстових даних дозволяє виявити зміни в тоні, стилі та частоті використання певних ключових слів, які можуть бути індикаторами маніпулятивного контенту.

Визначення відхилення в текстовому контенті: Використовуючи аналіз тексту, ШІ може виявляти аномалії у використанні мови, які можуть вказувати на дезінформацію. Це може бути виражено через наступну формулу:

$$T_d = \frac{1}{N}\sum_{i=1}^{N}(Text_i - ExpectedPattern_i)^2$$

де *Td* - відхилення тексту, Text*i* - реальний текстовий контент у повідомленні, ExpectedPattern*i* - очікуваний або нормальний шаблон мови, *N* - кількість аналізованих повідомлень.

Кластеризація для ідентифікації дезінформації: ШІ може використовувати кластерний аналіз для групування схожих повідомлень, що може допомогти ідентифікувати джерела дезінформації. Це можна виразити так:

$$Ck = min\sum_{i=1}^{N}\sum_{j=1}^{M}|Pij - Cij|^2$$

де *Ck* - кількість кластерів, *Pij* - повідомлення в датасеті, *Cij* - центр кластера, *N* - кількість повідомлень, *M* - кількість кластерів.

Оцінка достовірності візуального контенту: Для аналізу зображень та відео можна використовувати наступну формулу:

$$Va = \frac{1}{N}\sum_{i=1}^{N}(1 - \frac{|Ai - Ri|}{Ai})$$

де Va - точність аналізу візуального контенту, Ai - оригінальний атрибут зображення або відео (наприклад, текстура або освітлення), Ri - атрибут після обробки алгоритмом, N - кількість аналізованих зображень або відео [21].

У середовищі соціальних мереж, де інформація розповсюджується з високою швидкістю, здатність ШІ швидко виявляти та аналізувати потенційно недостовірні повідомлення є критичною для ефективного реагування на дезінформаційні загрози. Завдяки автоматизованому моніторингу та аналізу контенту, ШІ може допомагати у виявленні дезінформації у реальному часі, дозволяючи швидко реагувати на поширення фальшивих новин та маніпулятивних повідомлень.

Точність аналізу, що забезпечується застосуванням ШІ, є ключовою для боротьби з дезінформацією. Алгоритми ШІ можуть виявляти складні шаблони та аномалії, які людські аналітики можуть пропустити. Наприклад, використання алгоритмів глибокого навчання для аналізу зображень та відео дозволяє виявляти ретушовані фотографії або маніпульовані відеоролики, які можуть бути використані для поширення фейкових новин.

В цілому, використання ШІ у виявленні дезінформації в соціальних мережах відіграє ключову роль у боротьбі з недостовірною інформацією. ШІ забезпечує не тільки швидкість та точність аналізу, але й можливість адаптації до постійно змінюваних методів та стратегій дезінформації, що робить його незамінним інструментом у сучасному цифровому світі.

1.7 Висновки та постановка задач

У рамках першого розділу дипломної роботи проведено аналіз сучасних методик та підходів до ідентифікації автоматично генерованої дезінформації у соціальних мережах в умовах інформаційних конфліктів. У дослідженні особливу увагу приділено характеристикам дезінформації, її впливу на поведінку користувачів соціальних мереж, а також методам та стратегіям маніпуляції громадською думкою.

Основний акцент роботи було зосереджено на вивченні мультимовних особливостей в найпопулярніших соціальних мережах та аналізі їхньої ролі в процесі розповсюдження неправдивої інформації.

Основною метою цієї частини роботи було визначення та аналіз ключових факторів, що впливають на поширення дезінформації в соціальних мережах, зокрема, в контексті інформаційних війн.

Дослідження охоплювало різні аспекти цієї проблеми, включаючи технічні, психологічні та соціальні чинники, які сприяють поширенню фальшивої інформації. Особливо значущим було дослідження мовної різноманітності у соціальних мережах, яке допомогло виявити, як мовні бар'єри та культурні відмінності впливають на динаміку розповсюдження дезінформації.

На основі проведеного аналізу було вибрано конкретну соціальну мережу як об'єкт дослідження для подальшого розгляду та розробки методології виявлення та аналізу дезінформації. Вибір цієї мережі було обумовлено її популярністю, різноманіттям користувачів та масштабом впливу на суспільну думку, що робить її значущою для дослідження в рамках даної роботи.

На підставі проведеного аналізу у першому розділі, було визначено ключові напрями для подальшого дослідження та розробки, зокрема:

- **Удосконалення методу виявлення автоматично генерованої дезінформації у соціальних мережах під час інформаційних конфліктів:** Основна мета цього завдання полягає у розробці вдосконалених методів для ефективного виявлення та перевірки дезінформації у соціальних мережах, особливо під час інформаційних криз та конфліктів. Це передбачає використання новітніх технологій штучного інтелекту та машинного навчання для аналізу великих обсягів даних, розпізнавання складних патернів і контекстів, що характерні для неправдивої інформації. Завдання спрямоване на поліпшення точності та надійності ідентифікації дезінформації, включаючи використання алгоритмів глибокого навчання для адаптації до нових методів поширення дезінформації.

- **Розробка програмного засобу на основі удосконаленого методу:** Задача полягає у розробці надійного програмного рішення, що здатне аналізувати та перевіряти інформацію у соціальних мережах на предмет дезінформації. Цей інструмент забезпечує глибокий аналіз коментарів та публікацій, використовуючи алгоритми штучного інтелекту та машинного навчання для виявлення ознак маніпуляції та фальсифікації. Це дозволяє користувачам не тільки розуміти, як інформація поширюється у соціальних мережах, але й ефективно ідентифікувати й аналізувати потенційно неправдиву чи маніпулятивну інформацію, сприяючи таким чином підвищенню рівня інформаційної обізнаності та безпеки користувачів.
- **Аналіз економічної ефективності розробленого програмного засобу:** Це завдання передбачає оцінку вартості розробки, впровадження та подальшого використання розробленого програмного засобу, а також вивчення його потенційних переваг в контексті інформаційної безпеки. Важливо оцінити, чи виправдані вкладені ресурси та чи може програма забезпечити достатній рівень захисту від інформаційних загроз у соціальних мережах.

Дослідження концентрується на аналізі впливу інформаційних війн на поведінку та взаємодію в соціальних мережах. В контексті сучасного інформаційного простору, де інформаційні конфлікти стають дедалі поширенішими, розуміння динаміки розповсюдження інформації набуває великого значення.

Дослідження фокусується на визначенні та аналізі соціальних відносин, які формуються під впливом інформаційних потоків, а також на вивченні механізмів та методів, що використовуються для поширення інформації в періоди інформаційних війн. Це дослідження дозволяє краще зрозуміти, як інформація формує громадську думку та як вона може бути використана для маніпуляцій та впливу на соціальні групи.

Основною метою є виявлення патернів та трендів у поведінці користувачів соціальних мереж під час інформаційних конфліктів, що може надати цінну

інформацію для розробки стратегій протидії дезінформації. Це включає аналіз різноманітних тактик і стратегій, які застосовуються для маніпуляції інформацією, а також визначення ключових факторів, що сприяють ефективному поширенню дезінформації.

Таким чином, це дослідження спрямоване на розробку глибокого розуміння впливу інформаційних війн на соціальні мережі, ідентифікацію ключових викликів та можливостей для покращення інформаційної безпеки у цифровому світі. Це знання є надзвичайно важливим для розробки ефективних інструментів та методів протидії дезінформації та захисту інформаційного простору.

2. УДОСКОНАЛЕННЯ МЕТОДУ ВИЯВЛЕННЯ АВТОМАТИЧНО ГЕНЕРОВАНОЇ ДЕЗІНФОРМАЦІЇ У СОЦІАЛЬНИХ МЕРЕЖАХ ПІД ЧАС ІНФОРМАЦІЙНИХ КОНФЛІКТІВ

У сучасному світі інформації, особливо у сфері соціальних медіа, дезінформація є суттєвою перешкодою, яка потребує ретельної та організованої стратегії як для виявлення, так і для реагування. У цьому сегменті ми зосереджуватимемося на покращенні поточних методів виявлення дезінформації, ретельному дослідженні їхніх недоліків та інноваційних методах, які потенційно можуть підвищити точність і успішність розрізнення правди та брехні.

Основна мета — вивчити поточні методології та їхні обмеження. Це обстеження полегшить ідентифікацію важливих областей, які потребують доопрацювання та адаптації для відповідності сучасним стандартам інформаційної безпеки. Важливо, що дослідження буде надавати пріоритет встановлення комплексних і багатовимірних критеріїв для розпізнавання дезінформації. Такі критерії включатимуть лінгвістичні, психологічні та контекстуальні аспекти.

Тепер увага буде спрямована на пропозиції щодо покращення як аналізу метаданих, так і алгоритмів обробки природної мови (NLP) [9].

Мета полягає в тому, щоб створити нові алгоритми або змінити вже існуючі, які можуть ефективно обробляти величезні обсяги даних, які є звичайними для соціальних мереж. Ці алгоритми мають бути здатними виявляти приховані моделі дезінформації.

Оцінка функції штучного інтелекту у виявленні дезінформації буде ключовим аспектом цього розділу. Інтеграція штучного інтелекту дає можливість підвищити ефективність і точність обробки, а також виявляти складніші та складніші кампанії дезінформації.

У наступному розділі ми оцінимо запропоновані вдосконалення, щоб визначити їх ефективність. Таким чином, ми можемо зробити переконливі висновки про практичність розроблених методів і технологій при зустрічі з інформаційними конфліктами на сайтах соціальних мереж. Крім того, ми

заглибимося в перспективні напрямки для майбутнього розвитку та досліджень у цій галузі.

2.1 Аналіз існуючих підходів та їх обмеження у виявленні автоматично генерованої дезінформації

Були проведені репрезентативні дослідження, щоб визначити найпоширеніші підходи до виявлення автоматично створеної дезінформації в соціальних мережах, з наголосом на ключових методах і техніках, що використовуються для створення моделей виявлення [23].

Сфера автоматичного виявлення фейкових новин і захисту від них у соціальних мережах онлайн активно досліджується, і одним із поширених підходів є використання кількох функцій [23][24].

Крім того, глибоке навчання [24] є ще одним поширеним підходом до виявлення фейкових новин у соціальних мережах. Компанії та відомі особи використовують численні мережі соціальних медіа для реклами своїх продуктів і створення репутації.

Проте часто ці системи перевірки фактів зосереджені на політичних питаннях, і тому фейкові новини можуть швидко поширюватися мережею [24]. Фейкові новини не є новою проблемою на платформі соціальних мереж, але їх виявлення та ідентифікація є складним завданням через зміну тем, контексту, стилю та медіа-платформи [24].

Фейкові новини містять правдиві докази у фейковому контексті на підтримку неправдивих тверджень, тому люди використовують ручні підходи, такі як FaceChek.org і PolitiFact.com, для перевірки фактів [24].

Швидке поширення фейкових новин впливає на мільйони користувачів та їх справжнє середовище [24], але програмне забезпечення, створене в цій роботі, може допомогти виявити автоматично згенеровану дезінформацію в соціальних мережах.

Це програмне забезпечення пропонує виявлення генерованої дезінформації завдяки поєднанню штучного інтелекту та машинного навчання. Соціальні боти використовують дві стратегії для розповсюдження контенту, що не викликає довіри, у соціальних медіа – посилення взаємодії з контентом і націлювання на впливових користувачів [23].

Крім того, обговорювалося успішне використання п’яти генеративних моделей (RBM, DBN, DBM, GAN і VAE) у різних програмах класифікації [25]. Крім того, існуючі роботи для MID базуються на синтаксичних і лексичних моделях або особливостях думки [25], і більшість методів виявлення фейкових новин враховують лише особливості тексту, орієнтованого на дані [24].

Тому первинна схема класифікації, заснована на певному наборі критеріїв, наголошується на критичному обговоренні, а підходи, засновані на блокчейні, зазвичай використовуються для виявлення автоматично створеної дезінформації в соціальних мережах [23].

Було запропоновано низку підходів для зменшення поширення дезінформації в Інтернеті. Одним із найуспішніших підходів є прості й короткі ретракції [26]. Було виявлено, що такі відкликання ефективніші, ніж відповідна дезінформація. Інший підхід полягає у використанні методів виявлення на основі графіків, які ефективні для визначення мережі користувачів і типу вмісту, яким вони діляться.

Функціональні методи також використовуються для виявлення присутності ботів у соціальних мережах онлайн. Ці методи використовують методи машинного навчання та обробки природної мови для ідентифікації ботів.

Краудсорсинг – це ще один підхід, який передбачає використання людей-оцінювачів для виявлення присутності ботів. Це дозволяє користувачам позначати підозрілий вміст або облікові записи. Усі ці підходи виявилися ефективними в боротьбі з дезінформацією в Інтернеті. Однак ефективність цих підходів у порівнянні один з одним може бути визначена лише шляхом подальших досліджень та експериментів [26].

Зараз дослідники пропонують нові підходи до покращення виявлення автоматично створеної дезінформації в соціальних мережах [23]. Один із таких підходів передбачає використання метаевристичних алгоритмів оптимізації [23] з метою побудови ефективної моделі глибокого навчання для виявлення фейкових новин [24].

Ця модель використовуватиме соціальний контекст новинних статей для виявлення [24], а запропонований підхід використовує машинне навчання та класифікатори глибокого навчання в середовищі Chrome [24]. Для оцінки продуктивності розширення chrome використовується алгоритм глибокого навчання, який називається довгою короткочасною пам’яттю (LSTM) [24].

Іншим запропонованим підходом є метод виявлення фейкових новин для користувачів Facebook [24]. Глибоке навчання (DL) принесло комп’ютерам надзвичайну потужність, таку як здатність сприймати мову, схожу на людську, і навчати модель без вимоги до вилучення функцій або маркування даних [25]. DL також уможливила фреймворки для збирання, обробки та адаптації великої кількості інформації [25].

Його застосовують до фейкових новин, чуток, спаму тощо в онлайн-соціальних мережах, хоча існуючі дослідження не можна прямо порівняти через відсутність широкомасштабних загальнодоступних наборів даних [25]. Методи DL використовуються для покращення виявлення автоматично створеної дезінформації в соціальних мережах і для користі дослідженням MID [25].

Потрібна ефективна модель виявлення з можливістю обробки як вмісту, так і контексту, а також функцій на рівні спільноти за допомогою методу тензорної факторизації [24]. Існуючі методи виявлення в першу чергу зосереджуються на контенті або інформації, заснованій на соціальному контексті, отриманій із статей новин [24].

Цей підхід передбачає вивчення моделей розповсюдження фейкових новин у соціальних мережах і був перевірений на двох реальних наборах даних (BuzzFeed і PolitiFact) з точністю 821,230% для виявлення фейкових новин [24]. Крім того, Zhou

et al. розробив мережевий шаблонний підхід для виявлення фейкових новин [24], який спрямований на покращення виявлення дезінформації в твітах [26].

Алгоритм передбачає використання графа ретвітів для оцінки загальної прийнятності твітів і довіри до джерел [26], а проблема FND вперше розглядається як задача оптимізації [23]. Оманливий контент, зокрема фейкові новини в соціальних мережах, негативно впливає на людей і суспільство [23].

Таким чином, запропонований підхід FND складається з трьох етапів: попередня обробка даних, адаптація GWO та SSO для побудови нової моделі FND та тестування запропонованої моделі FND [23]. Алгоритми GWO та SSO були вперше адаптовані до проблеми FND, і запропонований підхід було оцінено з використанням трьох наборів реальних даних і порівняно з сімома контрольованими алгоритмами ШІ [23]. Результати показали, що алгоритм GWO має кращу продуктивність, ніж SSO та інші алгоритми AI, і його можна ефективно використовувати для вирішення різних типів проблем соціальних мереж [23].

Прагнучи покращити виявлення автоматично генерованої дезінформації в соціальних мережах під час інформаційних конфліктів, важливо оцінити поточні методи та їхні недоліки. Сучасні соціальні медіа-платформи, такі як Facebook [38] та Instagram [29], серед іншого, мають складні мережеві структури, які можна проаналізувати, щоб отримати цінну інформацію щодо виявлення дезінформації.

При дослідженні соціальних мереж топологію цих мереж часто зображують за допомогою візуальних графіків, які відображають зв’язки між учасниками. Такі інструменти, як Gephi [30], дозволяють людям створювати ці графіки, відстежуючи еволюцію соціальних мереж і поширення інформації в них. Тим не менш, цей підхід може бути недостатнім при роботі з автоматично згенерованою дезінформацією, оскільки цей тип інформації часто поширюється нетиповими способами, які не відповідають стандартним моделям соціальної взаємодії.

Сучасні моделі розповсюдження інформації базуються на передумові, що нещодавно приєднався до мережі поширює інформацію за допомогою тих учасників, які мають більший вплив.

Зібравши інформацію, її з певною часткою ймовірності можна поширити серед інших учасників. Тим не менш, у випадку дезінформації, яка генерується автоматично, ці моделі можуть не враховувати унікальні аспекти такого розповсюдження, включаючи використання ботів або організованих мереж для швидкого та широкого поширення неправдивих повідомлень [27].

Протягом конкретного періоду часу визначення кількості людей, до яких потрапить неправдива інформація, не забезпечується звичайними методами аналізу соціальних мереж. Незважаючи на те, що моделювання здатне надати приблизні оцінки середньостатистичних людей, які зазнають впливу, ці наближення можуть втратити точність у разі нерегулярного та раптового поширення дезінформації.

Під час поточного вивчення сучасних методів виявлення неправдивої інформації на платформах соціальних мереж ми досліджуватимемо методологію, яка базується на моделюванні поширення інформації. Цей підхід використовує графи, щоб продемонструвати, як спільноти структуровані в соціальних мережах, де учасники представлені вершинами, а їхні зв’язки — ребрами.

Алгоритм аналізу поширення інформації в цих мережах включає наступні кроки:

- На першому етапі наукового дослідження, саме в момент, коли t=0, система імітаційного моделювання імпортує граф спільноти, який був витягнутий із зовнішнього джерела даних.
- Під час проведення наукових досліджень нерідко первинна інформація з’являється всередині спільноти.
- У наукових дослідженнях процес вибору вершини для розподілу інформації базується на принципі максимальної зв’язності. У випадку, якщо існує кілька вершин, які мають однаковий максимальний ступінь зв’язності, остаточно вибирається вершина, яка з’являється першою в порядку сортування.
- У наукових дослідженнях було помічено, що коли нова вершина вводиться в мережу, вона, швидше за все, з’єднається з вершиною з найвищим ступенем

зв’язності. Ця нова вершина згодом стає центром для розповсюдження інформації, передаючи її всім іншим вершинам, які мають пряме з’єднання з нею.

- У ході наукових досліджень процес емулюється протягом десяти модельних часових кроків. Під час кожного з цих кроків проявляються два випадкових процеси: генерація нової вершини з невизначеною кількістю ребер, яким вона інцидентна, і передача інформації між вершинами, які вже існують, причому ймовірність цього появи позначається як змінна "r".
- Після завершення десяти передбачених дій проводиться підрахунок повідомлених вершин. Цей розрахунок потім використовується для визначення частки учасників мережі, які досягли покриття.

Проведення наукових досліджень вимагає скрупульозного підходу. У сфері поширення інформації в соціальних мережах моделювання динаміки цього процесу можливе за допомогою специфічного підходу [28]. Однак цей метод не позбавлений обмежень, особливо щодо дезінформації, яка генерується автоматично. На відміну від традиційних процесів поширення інформації, дезінформація може бути заздалегідь спланованою та цілеспрямованою, використовуючи ботів та інші автоматизовані системи для швидкого поширення. У світлі цього існує потреба в розробці більш складних моделей і алгоритмів, які можуть враховувати ці унікальні характеристики.

Вирішальним аспектом проведення наукових досліджень є вивчення різноманітних методів виявлення дезінформації. Важливо також ретельно оцінити точність поширення інформації. Надійним показником є кількість членів спільноти, які зараз активні. Отримання доступу до цієї інформації дозволяє дослідникам сформулювати більш надійні прогнози, що стосуються розповсюдження інформації в конкретній мережі.

Динаміка поширення інформації ефективно демонструється застосуванням алгоритму на графі спільноти. Це є влучною ілюстрацією операційних процесів розглянутого алгоритму в контексті наукових досліджень. На початку експерименту виділяється одна вершина, через яку запускається інформація, та

відстежується розвиток мережі та розповсюдження інформації протягом 10 кроків. З цього можна зробити висновок, що зі збільшенням імовірності *r* передачі інформації між учасниками мережі, швидкість її розповсюдження також зростає.

Особливу увагу потрібно приділити особливостям інформаційної війни в контексті соціальних мереж. Під час інформаційних конфліктів інформація може поширюватися значно швидше, ніж у звичайних умовах. Це створює додаткові виклики, оскільки користувачам надається менше часу для перевірки джерела інформації та оцінки її достовірності. Таким чином, швидкість поширення інформації під час інформаційних війн може сприяти більшому розповсюдженню дезінформації.

У цьому контексті стає очевидною необхідність розвитку більш вдосконалених методів аналізу, здатних адаптуватися до особливостей поширення інформації в умовах інформаційних конфліктів. Ці методи повинні враховувати не тільки структуру соціальних мереж, але й швидкі зміни в поведінці користувачів під впливом зовнішніх чинників.

Продовжуючи аналіз методів виявлення дезінформації, можна зупинитися на використанні часового коефіцієнта Kt для оцінки часу, який витрачають користувачі соціальних мереж на перевірку отриманої інформації. Цей коефіцієнт можна визначити за такою формулою, де t+1 — інтервал часу, а tI — середній час, необхідний для перевірки інформації. Вектор інформованості zd представляє когнітивний рівень користувача.

Формула дозволяє визначити, чи мали користувачі теоретичну можливість перевірити достовірність джерела інформації та самої інформації. Якщо Kt≤0*Kt*, це означає, що користувачі не мали часу на перевірку інформації, тоді як Kt>0*Kt* свідчить про наявність такої можливості.

Коли мова заходить про наукові дослідження, важливо пам’ятати про те, як інформаційна війна впливає на події протягом тривалого часу. Цікаво відзначити, що користувачі з часом втрачають інтерес до всього, що стосується цієї теми. Це

може бути пов’язано з тим, що повторювана інформація, якій бракує варіацій або свіжих ідей, може здатися користувачам банальною або не стимулюючою.

У рамках даного наукового дослідження була розроблена методика аналізу розповсюдження дезінформації в соціальних мережах, що включає оцінку ефективності виявлення неправдивої інформації. Ефективність цього процесу оцінюється шляхом порівняння кількості успішно ідентифікованої дезінформації з загальною кількістю аналізованих даних. Цей показник виражається у відсотках, де кількість точно виявленої дезінформації ділиться на загальний обсяг аналізованих даних, а результат множиться на 100%, щоб отримати кінцеву оцінку ефективності методу.

Вирішальним аспектом наукового дослідження є визнання неадекватності та обмежень стандартного методу вимірювання успіху поширення інформації. Цей підхід ігнорує наявність підроблених і неактивних сторінок на платформах соціальних мереж. Тому існує невідкладна потреба вдосконалити цю техніку для досягнення більш точних результатів. Одне із запропонованих рішень передбачає усунення неактивних користувачів з обчислень для отримання більш точного наближення фактичного охоплення, створеного активними учасниками мережі.

Після проведення ретельного наукового дослідження було встановлено, як зазначено у першому розділі, що середня кількість активних учасників у спільноті соціальних медіа становить приблизно 50% від загальної кількості учасників. Як наслідок, більш ефективна формула для визначення ступеня впливу передбачає розрахунок поширення інформації на основі половини всього пулу потенційних осіб, які можуть отримати інформацію, що точно відображає фактичну кількість активних користувачів. Потім кінцевий результат збільшується на 100%, щоб перетворити його у відсоток.

Покращена техніка враховує різні важливі елементи, такі як особливості соціальних мереж, риси спільнот, контекст інформаційної війни та інші детермінанти, які впливають на поширення інформації. Він забезпечує більш точне та достовірне відображення поширення інформації в соціальних мережах. Цей

удосконалений метод має надзвичайно важливе значення для виявлення та ретельного вивчення дезінформації, особливо у випадках інформаційних конфліктів.

2.2 Розробка критеріїв для ідентифікації дезінформації

Аналіз динаміки поширення дезінформації у соціальних мережах є ключовим елементом для розуміння сучасних інформаційних війн. Вплив соціальних мереж на формування громадської думки, особливо у контексті конфлікту між Україною та Росією, підкреслює необхідність ефективних методів виявлення та аналізу дезінформації. Ця магістерська робота зосереджена на розробці та застосуванні передових технологій штучного інтелекту для ідентифікації фальшивої інформації, з метою зміцнення інформаційної безпеки та захисту громадян від маніпулятивних впливів у цифровому просторі.

Застосування цього методу беззаперечно продуктивно. Однак цьому заважає той факт, що, незважаючи на велику кількість літератури про людську поведінку в безлічі ситуацій і областей, майже немає моделей, які досліджують процес обміну інформацією в соціальних мережах.

Мета цього наукового дослідження включала постановку специфічного завдання, яке полягало у вдосконаленні методів виявлення та аналізу дезінформації у соціальних мережах. Основною ціллю було розробити та впровадити ефективні алгоритми, засновані на штучному інтелекту та машинному навчанні, для ідентифікації та аналізу потенційно неправдивої або маніпулятивної інформації. Це дослідження мало на меті забезпечити більш надійні та точні інструменти для моніторингу й аналізу інформаційних потоків в соціальних мережах, що є особливо актуальним у контексті сучасних викликів інформаційної безпеки.

Для опису процесу поширення інформації в соціальній мережі пропонується наступний метод. Інформаційна взаємодія в соціальній мережі, що складається з N осіб в спільноті, представлених у вигляді поширення інформації в мережі $S\ (M; D)$, вершинами якої служать люди $M = \{M_1; M_2; \dots; M_N\}$, а безліч з'єднань $D = \{D_{ij}\}$ відображає потенційно можливий інформаційний обмін між ними і утворює

«матрицю інформаційного обміну в соц. мережі». Результат роботи матриці приведений на рисунку 2.1.

$$D_g = \{1, \text{якщо елемент } i \text{ спілкується з елементом } j;\ 0, \text{якщо ні}$$

Необхідно відзначити, що матриця D_{ij} не обов'язково повинна бути симетричною. З того, що j-ий користувач соціальної мережі ділиться інформацією з і-им, не випливає, що останній буде робити у відповідь те ж саме. Цілком імовірна ситуація, при якій і-ий користувач, отримавши інформацію від j-го, з якої-небудь причини не захоче ділитися з ним своїми думками.

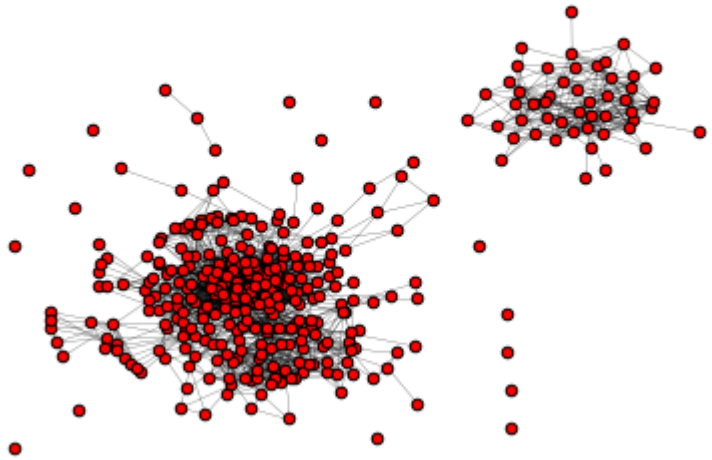


Рисунок 2.1 – Матриця інформаційного обміну в соціальній мережі (за [12])

Отримання інформації і-им елементом відбивається шляхом зміни з 0 на 1 відповідної координати в векторі інформованості $Z(z_1; z_2; \dots; z_N)$:

$$z_1 = \{1, \text{якщо } M_j \text{ має інформацію};\ 0, \text{якщо } M_i \text{ не має інформації.} \quad (2.1)$$

Процес інформаційного впливу на користувача з боку спільнот здійснюється наступним чином. Блок інформації I, який має певну тематику TI і несе в собі вектор керуючих «репостів» PI $(p_1; p_2; \dots)$, впроваджується в соціальну мережу

через окремих її членів $\underline{M} = \{\underline{M_l}\}(l = \underline{1; L}, L < N)$ зі свідомо позитивним ставленням до I.

Поширенню інформації між користувачами соціальних мереж сприяє міжособистісне спілкування. Цей обмін інформацією, однак, неможливо відстежити через характер мережі. Незважаючи на це, j-й елемент, що володіє інформацією I, здатний довести її до відома i-го елемента разом зі своєю думкою, що в кінцевому підсумку призводить до поширення зазначеної інформації. Цей процес є ключовим у сфері наукових досліджень.

У сфері наукових досліджень виникає проблема, коли намагаються формалізувати думки, які передаються через вербальні оцінки, оскільки вони не піддаються кількісній оцінці. Одним із запропонованих рішень є введення лінгвістичної змінної, позначеної як L «Рівень фактора», яка охоплює діапазон значень. Загалом цей набір термінів включає 9 елементів, які охоплюють як негативні QL, так і позитивні QL значення якості якості.

У сфері наукових досліджень існують різні техніки для побудови функцій належності. Однак, оскільки поставлене завдання передбачає перетворення вербальної інформації у формалізовану структуру, критично важливо вибрати метод формування функцій приналежності, який дозволяє генерувати непарні числа, що володіють певними якостями:

- безперервністю ($\mu\ (x)$ повинна бути визначена в будь-якій точці $x \in D$, де D область визначення непарних чисел);
- нормальністю ($3x \in D: \mu(x) = 1$);
- унітолерантністю ($3! [x\_1; x\_2\ ] \in D: \mu(x) = const = 1$ при $x \in [x\_1; x\_2]$).

Такі властивості непарних чисел забезпечуються тільки при формуванні функцій приналежності методами призначення і коригування параметрів. Ці методи дозволяють формувати трапецієподібні і трикутні непарні числа.

Виходячи з цього, в якості сімейства функцій приналежності для терм-множини лінгвістичної змінної L пропонується використовувати девятіуровневий класифікатор, в якому відповідні функції приналежності нечітких чисел, заданих на відрізку $[-1;\ 1]$, де в нечіткому трапецеїдальному числі XX $(\mathrm{a1}, \mathrm{a2}, \mathrm{a3}, \mathrm{a4})$: a1 і a4 - абсциси нижньої основи; A2 і a3 - абсциси верхнього підстави трапеції.

Суть даного нечіткого класифікатора в тому, що якщо про фактор невідомо нічого, крім того, що він може приймати будь-які значення в межах $[-1;\ 1]$ (принцип рівної переваги), і треба провести асоціацію між якісною і кількісної оцінками фактора, то запропонований класифікатор робить це з максимальною достовірністю

При цьому сума всіх функцій приналежності для будь-якого $x \in [-1;\ 1]$ дорівнює одиниці, що вказує на його несуперечливість.

В якості одного кроку (такту) по часу приймається тимчасовий інтервал, необхідний для одиничної реалізації всіх комунікаційних зв'язків, відображених у матриці інформаційного обміну D.

Сукупність $\underline{V_I}^{t+1} = \{\underline{V_k}^{t+1}\}$ відображає спектр інформаційного обміну користувачів соц. мережі щодо інформації I в момент часу $(t\ +\ 1)$. Статистичні параметри розподілу спектрів для різних введених інформаційних блоків в мережі дозволяють проводити їх моніторинг.

Згідно зі шкалою Харрінгтона, значення $\underline{V_k}^{t+1}$ можуть бути інтерпретовані таким чином:

$-1 \le \underline{V_k}^{t+1} \le -0{,}64$ - сильно виражене негативне ставлення, що спонукає до поширення інформації спільно зі своєю негативною думкою (репост з коментарем при репості) (стан користувача соц. мережі $S\ =\ S-$).

$-0{,}64 \le \underline{V_k}^{t+1} \le 0{,}64$ слабо виражений негативний $(-0{,}64 \le \underline{V_k}^{t+1} \le 0)$ або слабо виражене позитивне $(0 \le \underline{V_k}^{t+1} \le 0{,}64)$ ставлення до інформації, що не приводить до подальшого поширення інформації (стан користувача $S\ =\ S\,0$).

$0{,}64 \leq \underline{V_k^{t+1}} \leq 1$ сильно виражене позитивне ставлення, що спонукає до поширення інформації, доволі часто спільно зі своєю позитивною думкою (коментарем) (стан користувача $S = S+$).

Імовірність того, що користувач (Mk) буде поширювати йому відому інформацію, залежить не тільки від його відношення до даної інформації (від того, наскільки вона його емоційно зацікавлює), а й від рівня його комунікабельності. Для визначення рівня комунікабельності можуть застосовуватися різні тести.

Позначимо схильність Mk до поширення інформації (рівень його комунікабельності) як Ok. Даний параметр може бути оцінений значенням з множини (Низький; середній; Високий). Тоді для знаходження значення «Індикатора передачі інформації» k користувачем соц. мережі («Індикатора репосту») R_k^{t+1} в дискретний момент часу $(t + 1)$ може бути використана наступна формула:

$$R_k^{t+1} = \{0, \text{якщо } (S = S^0 \text{ і } O_k = \text{ Низький}) \text{ чи } (z_k = 0);\ 1\ . \qquad (2.2)$$

Сукупність «індикаторів передачі інформації» R_k^{t+1} назвемо «вектором репоста» $R^{t+1} = \{R_k^{t+1}\}$.

Процес інформаційного обміну припиняється, якщо відстань Геммінга p_μ між поточним вектором $\underline{V_I^{t+1}}$ вектором $\underline{V_I^t}$, отриманим на попередньому кроці за часом, не перевищує деякого заданого значення N^*:

$$p_\mu(\underline{V_I^{t+1}}; \underline{V_I^t}) \leq N^* \qquad (2.3)$$

Кількісна оцінка активності соціальної мережі між двома послідовними періодами часу вимірюється відстанню Хеммінга. Відстань Хеммінга — це обчислення кількості користувачів, які поділилися інформацією, про яку вони знають. Як тільки ця кількість стає незначною, вважається, що розподіл інформації I блоку досягнуто повністю.

У науково-дослідній роботі запропоновано алгоритмічну модель розповсюдження інформації в соціальній мережі. Цю модель можна підсумувати таким чином:

На попередньому етапі наукового дослідження основна увага приділяється побудові ключових функцій для соціальних мереж і «профілів користувачів». На цьому етапі розробляються матриці обміну інформацією та довіри, а також визначаються «цікаві» теми для різних груп користувачів. На цьому етапі також визначається початкове бачення користувача щодо поширеної інформації, його рівень комунікабельності, консерватизму та інші відповідні характеристики.

На першому етапі моделювання, відповідному нульовому кроці за часом ($t = 0$), блок інформації (I) доводиться до відома окремих користувачів соціальної мережі зі свідомо позитивним ставленням до даної інформації (елементи з множини $\underline{M} = \{\underline{M_l}\}(l = \underline{1; L}, L < N)$).

На даному етапі формуються:

- початковий «вектор інформованості» Z, в якому індекси інформованості користувача соц. мережі з ініціюючої безлічі $\underline{M}$ рівні 1, для інших - 0;
- початковий «вектор думок» користувача: V_1^0.

На другому етапі відбувається поширення інформації і обмін думками між користувачами мережі про цю інформацію на кроці часу $t = t + 1$:

- формується «вектор репоста» інформації I згідно з формулою (3);
- елементи, чий «індикатор репоста» дорівнює 1, передають інформацію іншим елементам відповідно до матриці інформаційного обміну D (формула 1).

На третьому етапі розраховується відстань Геммінга між поточним вектором $\underline{V_I^{t+1}}$ і вектором $\underline{V_I^t}$, отриманим на попередньому кроці за часом, і перевіряється виконання умови (4). Якщо умова виконується, то робота алгоритму припиняється, і отримані дані пред'являються для аналізу дослідникові чи особі, що перевіряє

поширення інформації. Інакше відбувається повернення до другого етапу моделювання.

Завдяки сучасним технологіям та лічильникам «лайків» відстежити кількісне поширення інформації доволі легко, але важливо також враховувати оцінку ефективності поширення інформації за проміжок часу ($t = t + 1$) в різних умовах:

- поширення інформації в звичайних умовах;
- поширення інформації в умовах інформаційної війни.

Оцінка ефективності поширення інформації відбувається знаючи кількість репостів та кількість учасників в спільноті за формулою $O_e = \frac{PI}{N} * 100\%$, але це необ'єктивне визначення оцінки ефективності поширення інформації тому, що в середньому в будь-якій спільноті 50% користувачів не активних та «фейкових». Тому цей метод потребує покращення.

Що пропонується в покращення: для обрахування оцінки ефективності поширення інформації (Oe) за покращеним методом потрібно взяти кількість активних учасників спільноти (Na) Na=N/2 (згідно з дослідженнями наведеними в розділі 1, між якими можливий інформаційний обмін, кількість репостів (PI), якщо реалізувати цей метод програмно, можна буде визначати кількість активних користувачів спільноти з точністю. Покращення також відбувається за рахунок поєднання штучного інтелекту та машинного навчання, що дозволяє підвищити точність визначення реальної активності учасників та їх взаємодії з контентом.

$O_e = \frac{PI}{N_a} * 100\%$, за проміжок часу ($t = t + 1$) (2.4)

Для того, щоб дослідити тривалість, необхідну для поширення знань у суспільстві, необхідно використовувати часовий інтервал (t = t + 1). Це важлива складова наукового дослідження.

У сфері наукових досліджень прийнято вважати, що активними користувачами вважаються ті, хто щомісяця займається будь-якою формою діяльності в межах спільноти.

Значний вплив свідомості індивіда на його дії та повсюдна роль соціальних медіа в сучасному суспільстві підкреслюють важливість використання прийомів інформаційного маніпулювання користувачами та розгляду поширення інформації в контексті інформаційної війни. Отже, дослідження поширення інформації користувачами соціальних мереж та використання методів інформаційного впливу є надзвичайно актуальними.

Алгоритм, розроблений для моделювання процесу поширення інформації в соціальній мережі, є основою для створення системи підтримки прийняття рішень у цій сфері. З реалізацією цього алгоритму на мові високого рівня, а також інтеграцією з штучним інтелектом та машинним навчанням, побудова такої системи стає не лише здійсненною, а й надзвичайно ефективною.

2.3 Інтеграція штучного інтелекту для покращеного виявлення автоматично створеної дезінформації

Інтеграція штучного інтелекту (AI) у виявлення дезінформації стає все більш популярною. Алгоритми ШІ забезпечують ефективний метод класифікації цілісності запиту користувача. Зокрема, штучні нейронні мережі (ШНМ) виявилися корисними в цьому процесі. ШНМ може передбачати з відносно дуже високою точністю навіть за невеликого обсягу даних, що важливо для раннього виявлення нової дезінформації та запобігання її поширенню [31].

Крім того, ШНН можна використовувати для виявлення неправдивих тверджень, таких як гомеопатичні засоби, які можуть запобігти, вилікувати чи захистити від COVID-19. Facebook розгорнув алгоритми машинного навчання для виявлення реклами з неправдивими заявами, тоді як Google представив «Fact Check Explorer» для перевірки достовірності інформації в Інтернеті [31].

ШНМ реалізовано в JavaScript Object Notation (JSON) та інтегровано з розширенням пошукової системи [31]. Навчений алгоритм ML передбачає точність

вихідного запиту, а також надаються додаткові рекомендації для підвищення обізнаності. Правильність запиту користувача відображається у вікні повідомлення, і вся ця процедура відбувається в режимі реального часу, щоб попередити користувача про потенційну дезінформацію [31].

Алгоритм ML, який використовується в розширенні, навчений класифікувати цілісність запиту, допомагаючи запобігти поширенню дезінформації [32]. Запропонований підхід (SEMiNExt) дозволяє раннє виявлення потенційно нових чуток з невеликої вибірки даних з високою точністю, тим самим максимізуючи безпеку для громадського здоров'я [31].

Інтеграція штучного інтелекту у виявлення автоматично генерованої дезінформації під час інформаційних конфліктів у соціальних мережах стає все більш необхідною [31]. Використання штучної нейронної мережі (ШМН) забезпечує спосіб прогнозування з більшою точністю навіть при роботі з невеликими обсягами навчальних даних [32].

У результаті користувачам потрібна допомога в прийнятті рішень щодо того, яку інформацію читати. Крім того, доступ до правдивого контенту є важливим для підтримки цілісності соціальних мереж. Метою запропонованого методу є підвищення якості пропозиції та точності системи рекомендацій, а також ефективне подолання розриву між виявленням фейкових новинних форм і довірою до системи рекомендацій у соціальних мережах [32].

Запропонований підхід має на меті знайти модель пропозиції, яка відповідає трьом ключовим характеристикам. Першою особливістю є адаптація двох метаевристичних алгоритмів, оптимізації сірого вовка (GWO) і оптимізації роя Salp (SSO), до проблеми виявлення фейкових новин (FND). Наскільки відомо авторам, це перший раз, коли ці алгоритми були адаптовані до проблеми FND [32].

Друга особливість — використання немаркованих даних для підвищення точності багатокласової класифікації при ідентифікації неправдивих новин під час інформаційних конфліктів у соціальних мережах. Нарешті, третя особливість — поєднання алгоритмів самонавчання з мажоритарним голосуванням, що може ще

більше підвищити ефективність багатокласової класифікації при виявленні автоматично створеної дезінформації [32].

Запропонований підхід FND складається з трьох етапів: попередня обробка даних, адаптація GWO та SSO для побудови моделі FND та використання запропонованої моделі FND для тестування [31]. Методологія була перевірена на обох наборах даних, і результати показують, що алгоритм GWO має найкращу продуктивність у порівнянні з алгоритмом SSO та іншими керованими алгоритмами штучного інтелекту [31].

Відсутність способів переконатися в правдивості інформації в соціальних мережах призвела до розвитку систем ідентифікації чуток. Крім того, швидке поширення інформації в соціальних мережах також сприяло виникненню потреби в системах виявлення дезінформації. Це особливо актуально з огляду на те, що основною перешкодою в соціальних мережах є швидке поширення дезінформації. Використання алгоритму GWO виявляється ефективним рішенням для вирішення різних типів проблем соціальних мереж [32].

Запропонований підхід розглядає проблему FND як задачу оптимізації, яка була оцінена з використанням трьох різних наборів даних реального світу. Підсумовуючи, виявлення фейкових і справжніх новин є необхідним для усунення недоліків соціальних медіа.

Штучний інтелект (AI) і обробка природної мови (NLP) — два потужні інструменти, які можна використовувати для автоматичного розпізнавання фейкових новин. У статті запропоновано гібридну модель глибокої нейронної мережі, яка поєднує моделі C-DSSM і Deep CNN для виявлення та класифікації фейкових новин [32].

Запропонована модель забезпечує кращі результати порівняно з існуючими сучасними методами. Запропонована модель отримала точність 92,60%, запам’ятовування 92,40%, точність 92,50% і оцінку F1 92,50% [33]. Щоб підвищити точність моделі, у статті представлено метод, заснований на взаємному посиленні, щоб включити знання людини про те, які докази важливіші [34]. Такий підхід є

зрозумілим і забезпечує дрібне міркування, яке відображає логічні процеси людського мислення. Крім того, у статті пропонується двоканальна графова мережа ядра з попереднім усвідомленням для моделювання тонких відмінностей між доказами [35].

У результаті запропонована гібридна модель дає кращі результати у виявленні та класифікації фейкових новин у соціальних мережах [36].

2.4 Проектування бази даних

Існує кілька етапів проведення нормалізації відношень за методом сутність-зв’язок.

Перший етап – визначення сутностей. Для вирішення завдання нормалізації відношень необхідно для початку визначити усі необхідні сутності (сутність – деякий об’єкт, що представляє інтерес для компанії): ГРУПА, УЧАСНИК, ЛАЙК, РЕПОСТ, ПОСТ, КОМЕНТАР, РЕЗУЛЬТАТ.

Кожна із вказаних сутностей повинна мати особливий ідентифікатор, не подібний із іншими сутностями.

Другий етап – визначення зв’язків між сутностями. Зв’язок – з’єднання між двома або більше сутностями. Зазвичай – це дієслово. У даному випадку:

- РЕЗУЛЬТАТ – містить – ГРУПА;
- ГРУПА – містить – ПОСТ;
- ПОСТ – містить – КОМЕНТАРІ;
- ПОСТ – має – РЕПОСТ;
- ПОСТ – має – ЛАЙК;
- УЧАСНИК – робить – РЕПОСТ;
- УЧАСНИК – пише – КОМЕНТАР;
- УЧАСНИК – ставить – ЛАЙК;

Третій етап – визначення атрибутів та ключів сутностей.

У нашому випадку атрибутами для вказаних сутностей будуть:

- ГРУПА (id_ група, назва групи);
- РЕЗУЛЬТАТ (id_рез, id_групи, дата, кількість користувачів, кількість постів, кількість репостів, кількість лайків, кількість коментарів);
- ПОСТ (id_поста, id_ група);
- РЕПОСТ(id_репоста, id_поста, id_учасника);
- УЧАСНИК (id_учасника, ПІБ, країна, стать);
- ЛАЙК (id_лайка, id_учасника, id_поста);
- КОМЕНТАР (id_коментаря, id_учасника, id_поста, текст коментаря).

Наступним етапом в проектуванні бази даних є визначення ступеня зв'язків між сутностями. Необхідно відзначити, що ступеня зв'язків визначаються для бази даних під час всього періоду її існування. Визначення зв'язків представлено у вигляді ER-діаграм. Загальний підхід до побудови бази даних з використанням ER-методу полягає в побудові діаграми ER-типу, який включає в себе всі сутності і зв'язку важливі з точки зору інтересів компанії.

Визначення ступеню зв`язку та класу належності сутностей «ГРУПА» та «РЕЗУЛЬТАТ» показано на рисунку 2.2.

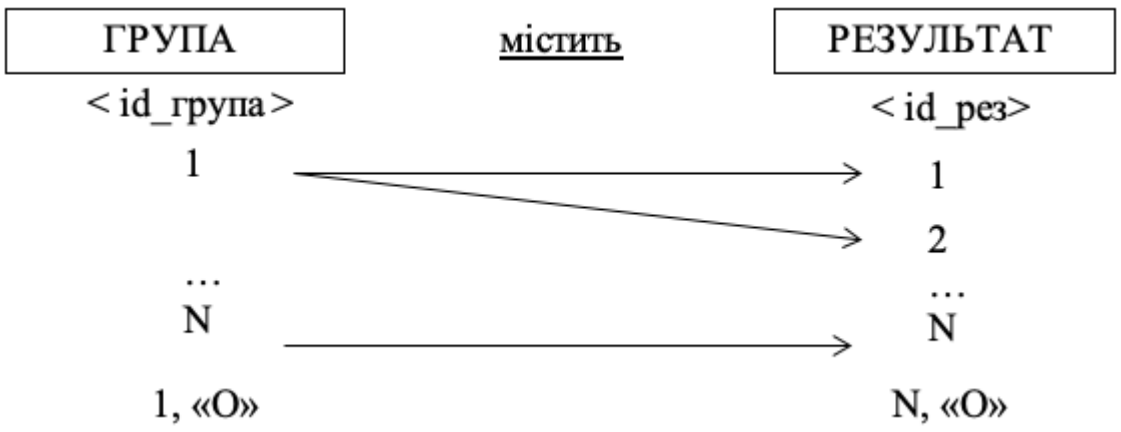


Рисунок 2.2 – Ступінь зв'язку сутностей «ГРУПА» та «РЕЗУЛЬТАТ»

Отже, ступінь зв’язку між сутностями 1:N, клас належності «О»:«О». Виходячи з правил, коли ступінь бінарного зв'язку є 1: N і його клас приналежності однозв`язної суті є обов'язковим, то достатньою є використання двох відносин по одному на всі суті.

Визначення ступеню зв`язку та класу належності «ГРУПА» та «ПОСТ» показано на рисунку 2.3.

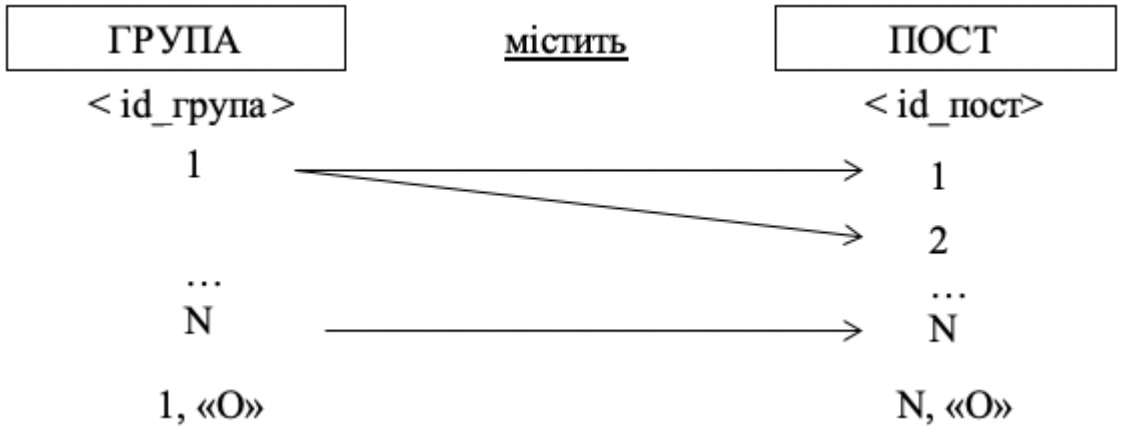


Рисунок 2.3 – Ступінь зв'язку та класу належності сутностей «ГРУПА» та «ПОСТ»

Із схеми можна побачити, що ступінь зв’язку для даного випадку 1:N, а клас належності «О»:«О».

Ступінь зв`язку та класу належності сутностей «ПОСТ» та «РЕПОСТ» показано на рисунку 2.4.

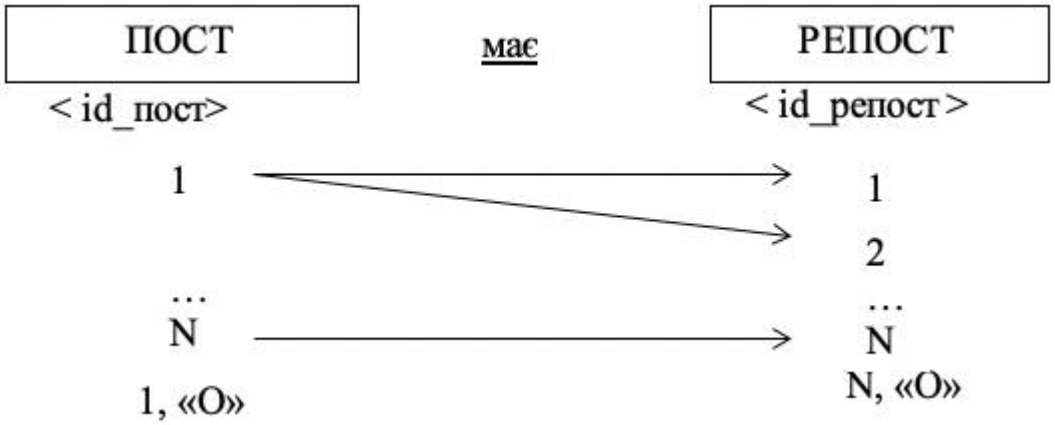


Рисунок 2.4 – Ступінь зв'язку «ПОСТ» та «РЕПОСТ»

Виходить, що ступінь зв’язку між сутностями 1:N, клас належності «О»:«О».

Ступінь зв`язку та класу належності сутностей «УЧАСНИК» та «РЕПОСТ» показано на рисунку 2.5.

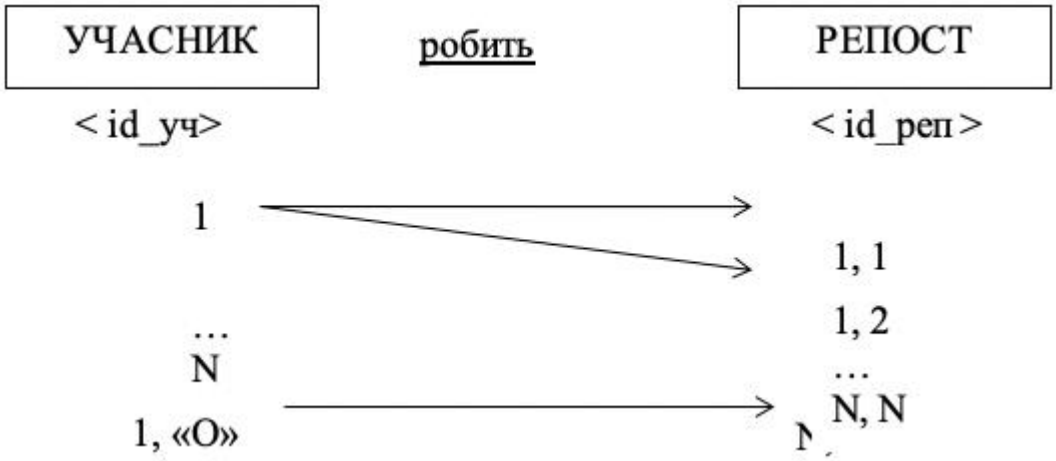


Рисунок 2.5 – Ступінь зв'язку та класу належності сутностей «УЧАСНИК» та «РЕПОСТ»

Отже, ступінь зв’язку між сутностями 1:N, клас належності «О»:«О».

Визначення ступеню зв`язку та класу належності сутностей «УЧАСНИК» та «ЛАЙК» показано на рисунку 2.6.

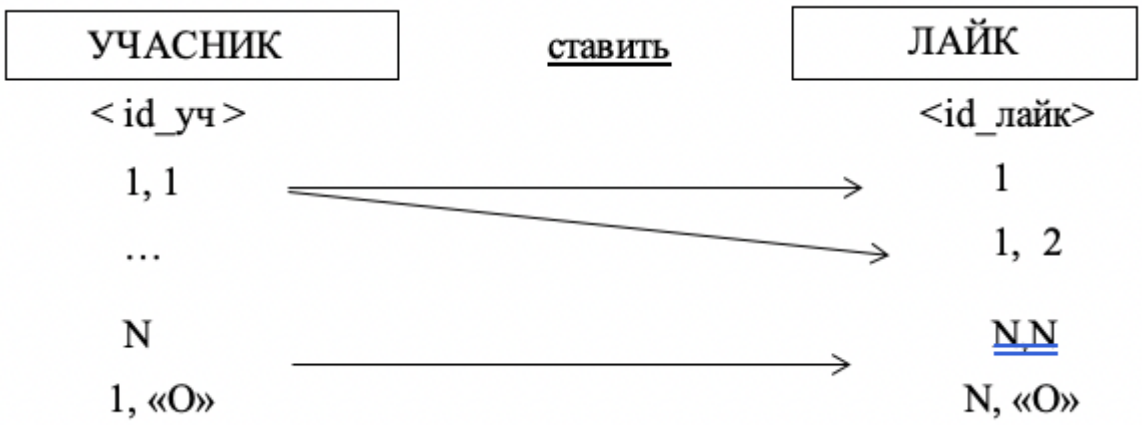


Рисунок 2.6 – Ступінь зв'язку та класу належності сутностей «УЧАСНИК» та «ЛАЙК»

Таким чином, ступінь зв'язку в даному випадку 1:N, а клас належності «О»:«О».

Визначення ступеню зв`язку та класу належності сутностей «ПОСТ» та «КОМЕНТАР» показано на рисунку 2.7.

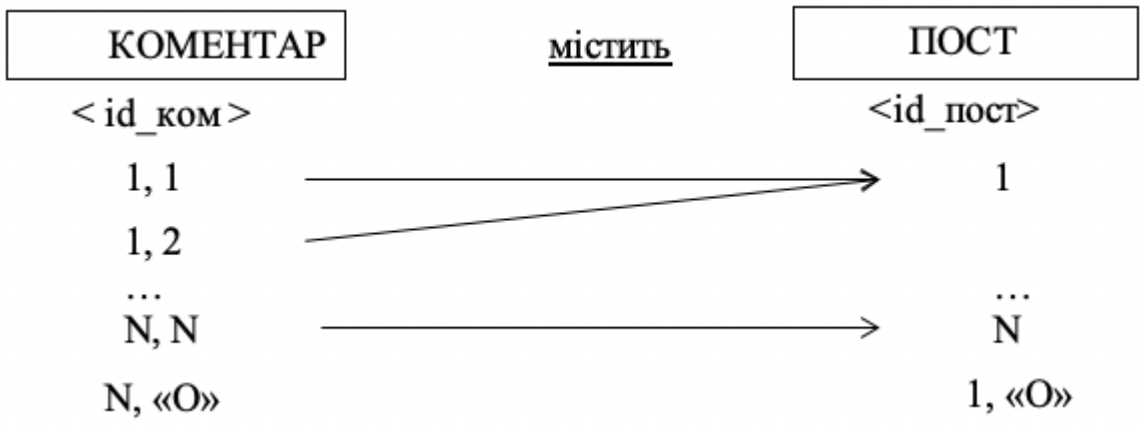


Рисунок 2.7 – Ступінь зв'язку та класу належності сутностей «КОМЕНТАР» та «ПОСТ»

Визначення ступеню зв`язку та класу належності сутностей «ЛАЙК» та «ПОСТ» показано на рисунку 2.8.

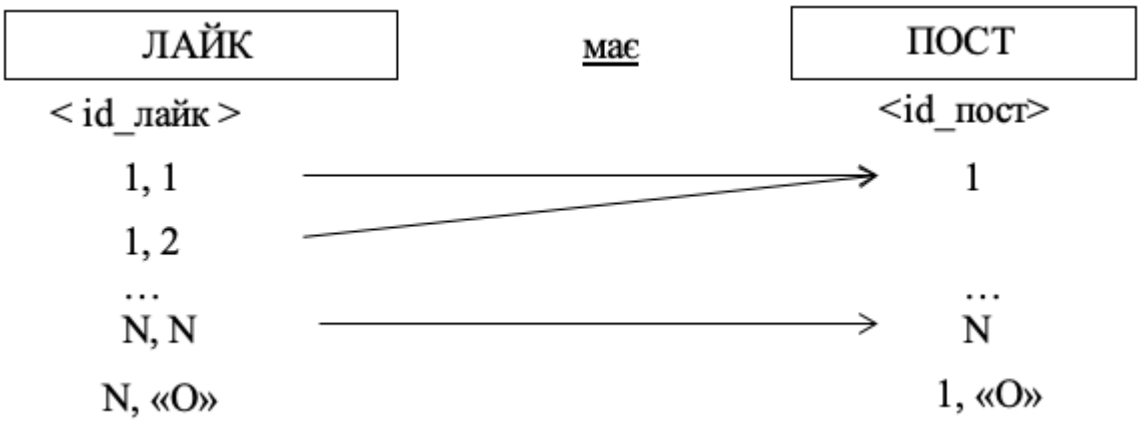


Рисунок 2.8 – Ступінь зв'язку та класу належності сутностей «ЛАЙК» та «ПОСТ»

Таким чином, ступінь зв'язку в даному випадку N:1, а клас належності «О»:«О».

В узагальненому вигляді результати проведених аналізів і досліджень можна представити у вигляді діаграми «сутність-зв'язок», яка ілюструє процес виявлення та аналізу дезінформації в соціальних мережах. Ця діаграма (рис. 2.9) візуально демонструє взаємозв'язки між різними компонентами системи аналізу

дезінформації, включаючи ідентифікацію джерел дезінформації, методи обробки даних, критерії оцінки вірогідності інформації, а також способи її класифікації та візуалізації.

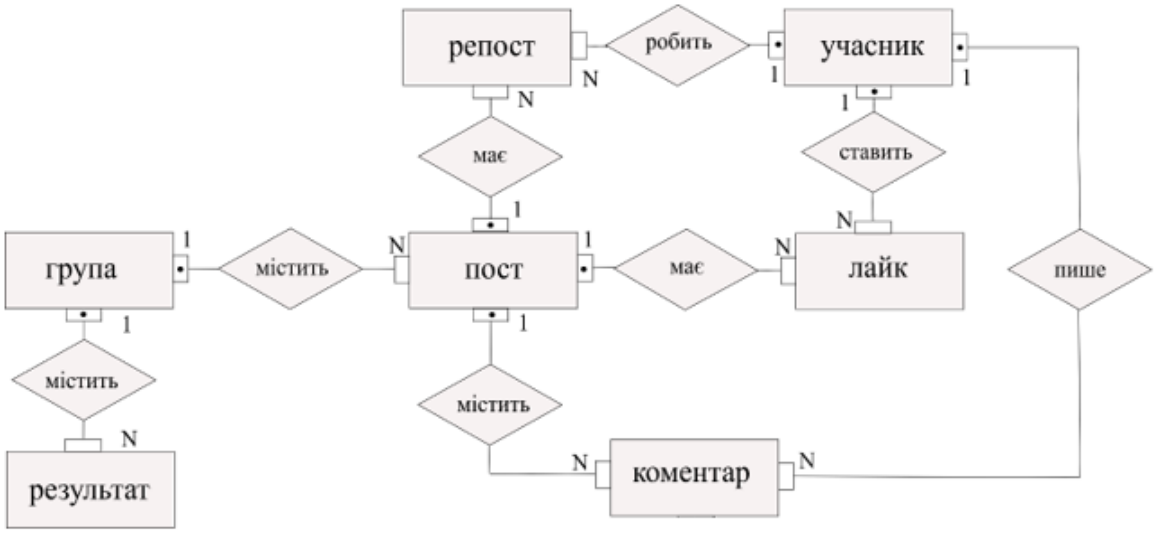


Рисунок 2.9 – ER-модель процесу виявлення та аналізу дезінформації в соціальних мережах

Перетворення бази даних до виду, що відповідає нормальним формам називається нормалізацією. Нормалізація дозволяє зробити базу даних безпечною від логічних і структурних проблем, які називаються аномаліями даних.

Наприклад, коли існує декілька однакових записів в таблиці, зчвляється ризик, що може порушити цілісность даних при оновленні таблиці. Таблиця, пройшла нормалізацію, менш схильна до таких проблем, тому її структура передбачає визначення зв'язків між даними, що виключає необхідність в існуванні записів з повторюваної інформацією.

Для реалізації поставленої задачі універсальне відношення буде мати вигляд: R (id_ група, назва групи, id_рез, дата, кількість користувачів, кількість постів, кількість репостів, кількість лайків, кількість коментарів, id_репоста, id_поста, id_учасника, ПІБ, країна, стать, id_лайка, id_учасника, id_коментаря, id_учасника, текст коментаря).

Якщо відношення знаходиться в першій нормальній формі (1НФ), то все не ключові атрибути функціонально залежить від ключа. Адже всі атрибути

знаходяться в повній ключовий залежності від <id_пост>, то R1 = R.

У другій нормальній формі відношення знаходиться, якщо воно знаходиться в першій нормальній формі [37], і при цьому будь-який його атрибут, який не входить до складу потенційного ключа, функціонально повно залежить від кожного потенційного ключа. Виходячи з цих правил, отримаємо такі відносини в 2НФ:

R1 (<id_поста>, id_ група).

R2 (id_репоста, id_поста, id_учасника).

R3 (id_учасника, ПІБ, країна, стать).

Утретій нормальні формі (3НФ) відношення буде, якщо воно знаходиться в 2НФ і кожен неключовий атрибут нетранзитивно залежить від початкового ключа.

В даному варіанті транзитивна залежність існує у відношенні R2 і R3:

R4 (id_лайка, id_учасника, id_поста);

Визначимо повну залежність:

R5 (<id_коментаря, id_учасника, id_поста, текст коментаря).

У зв'язку з тим, що планується розробка бази даних для компаній, відношення R6 має також транзитивну залежність:

< id_групи> id_поста → назва_ групи. →

Розкладемо відношення R7 на наступні відношення:

R8 (<id_поста, id_ група);

R9 (<id_ група, назва групи);

У результаті проектування за методом нормалізації відношень, кінцевими відношеннями будуть: R1, R3, R4 , R6, R8, R9

2.5 Алгоритм роботи програми

У рамках цієї дипломної роботи була розроблена програма, яка демонструє практичне застосування удосконаленого методу аналізу дезінформації у соціальних мережах. Цей інструмент призначений для ефективного виявлення і

класифікації потенційно неправдивої інформації, використовуючи передові алгоритми штучного інтелекту та машинного навчання. Програма стане корисним ресурсом для аналітичних установ, що займаються моніторингом інформаційної

Процес моніторингу взаємодії користувачів у спільноті зазвичай називають перевіркою активності зазначених користувачів.

Одним із способів оцінити ефективність реклами є використання рекламних структур, які вимірюють залучення користувачів. Ці структури дають змогу зрозуміти вподобання користувачів і дозволяють оцінити успіх певної реклами.

Ефективність тактики ведення інформаційної війни в соцмережах мають оцінити органи влади України.

Ця фраза стосується будь-яких інших вправ, які передбачають аналіз соціальних мереж.

У роботі над створенням зручного та ефективного інтерфейсу, у якому дані будуть представлені візуально у вигляді діаграм та графіків. Програмне забезпечення використовуватиме платформу Facebook API [38] для отримання відповідної інформації зі сторінок користувачів і спільнот у соціальній мережі. Цей унікальний підхід дозволяє отримувати необмежену кількість інформації, на відміну від інших програм, які використовують ботів або методи аналізу.

Пропонована програма має можливість досліджувати соціальну поведінку активних користувачів у певній спільноті. Він може ретельно перевіряти різні фактори, такі як лайки, дизлайки та репости. Програма також може порівнювати та оцінювати ці дані з інформацією, зібраною зі сторінок користувача.

Щоб ефективно використовувати програму, необхідно виконати певні вимоги. Вам потрібно буде вибрати певну спільноту, цільові записи або конкретні ключові фрази для пошуку в соціальних мережах для аналізу. Тривалість часу, необхідного для обробки даних програмою, залежить від кількості вхідних даних. Для аналізу об’ємних масивів даних і роботи з BigData необхідна значна обчислювальна потужність.

Удосконалений метод можна розбити на ряд етапів, представлених у такій послідовності:

Щоб почати процес, користувач повинен активувати програмне забезпечення. Після активації програми вона перейде в стан очікування під час ініціалізації її компонентів.

Компоненти програми запускаються на другому кроці. Цей процес передбачає перевірку підключення до Інтернету, і якщо активного підключення немає, відображається повідомлення про помилку.

Щоб підключити програмне забезпечення до Facebook API [38], першим кроком є встановлення зв’язку між ними. Після успішного підключення Facebook API [38] надсилає тестовий пакет, відомий як «facebook-body-parser». Якщо з будь-якої причини цей пакет не отримано, Facebook API [38] позначить помилку та перейде до другого кроку процесу.

Після завершення третього кроку наступним завданням є придбання тестового набору facebook-body-parser. Якщо тестовий пакет не отримано, генерується повідомлення про помилку, і система переходить до другого кроку.

П'ятий крок передбачає встановлення з'єднання з базою даних. Якщо підключення встановлено успішно, переходьте до наступного кроку. Однак, якщо підключення не вдається, система спробує підключитися повторно. Якщо повторне підключення пройшло успішно, перейдіть до наступного кроку. Якщо ні, з’явиться повідомлення про помилку «Перевірте підключення до Інтернету.

Щоб створити новий масив, потрібно виконати певні кроки. По-перше, необхідно ініціалізувати масив певним розміром. Потім кожному елементу в масиві потрібно присвоїти значення або залишити порожнім. Нарешті, масив можна змінювати або отримати доступ за потреби. Важливо зауважити, що при посиланні на будь-які дати, числа чи статистичні дані, пов’язані з масивом, їх слід подавати точно так, як вони є, без використання синонімів чи абстрактної мови.

Щоб створити нове завдання в програмі, необхідно виконати кілька кроків. По-перше, програма має перевірити, чи вже існує завдання, що робиться на кроці 6. Якщо завдання не існує, програма переходить до кроку 7, де створює нове завдання. Однак, якщо завдання існує, програма продовжить виконання без створення нового завдання.

Перевірка точності введених даних є важливим кроком, позначеним як крок 8. Якщо дані введені правильно, можна переходити до наступного кроку. Однак, якщо дані були введені неправильно, генерується повідомлення про помилку, і процес повертається до кроку 7 для виправлення та повторного введення даних.

У контексті наукового дослідження дев’ятий крок передбачає отримання даних через Facebook API [38]. Якщо запитані дані отримано успішно, процес можна продовжити до наступних кроків. Однак у разі збою отримання даних необхідно отримати повідомлення про помилку, і процес має перейти до сьомого кроку.

Десятий крок у цьому науковому дослідницькому проекті передбачає збереження даних, отриманих через Facebook API [38], шляхом їх запису в базу даних.

Одинадцятий крок передбачає підбір формули

$$lg\tau_{\text{ŋ}}(\sigma_{\text{ŋ}}) = K_i\,\sigma_{\text{ŋ}} + b_i, S = \sum_{j=1}^{p} \left[lg\tau_{\text{ŋ}} - \left(K_i\,\sigma_{\text{ŋ}} + b_i\right)^2\right],$$

побудова графіків, визначення їх точок перетину $Lg\tau_m$.

Дванадцятий крок передбачає підбір формули $Lg\tau_{\text{ŋ}}(T_i)$, побудову графіків визначення їх точок перетину $1/T_m$.

Тринадцятий крок передбачає побудову графіків $U_0(\sigma_i)$, побудову графіку активу , визначення V_0.

Наступним проводиться збереження даних. Якщо програмі не вдається зберегти дані, з’явиться повідомлення про помилку, і програма перейде до

наступного кроку. І навпаки, якщо дані успішно збережені, програма продовжить збереження графіків, які були створені, перш ніж перейти до наступного кроку.

П'ятнадцятий етап дослідження передбачає представлення отриманих результатів на моніторі комп'ютера.

На останньому етапі усі необхідні дані зібрано, проаналізовано та інтерпретовано. Розробка програми була вичерпно задокументована, а кінцевий продукт був ретельно протестований, щоб переконатися, що всі цілі були досягнуті. Після завершення програми дослідницька група тепер готова представити свої висновки своїм колегам і колегам у науковому співтоваристві.

Алгоритм роботи програмного додатку наочно зображено на блок-схемі (див. рис. 2.10). Ця діаграма полегшує розуміння принципу роботи програми завдяки чіткому та короткому зображенню її робочого процесу.

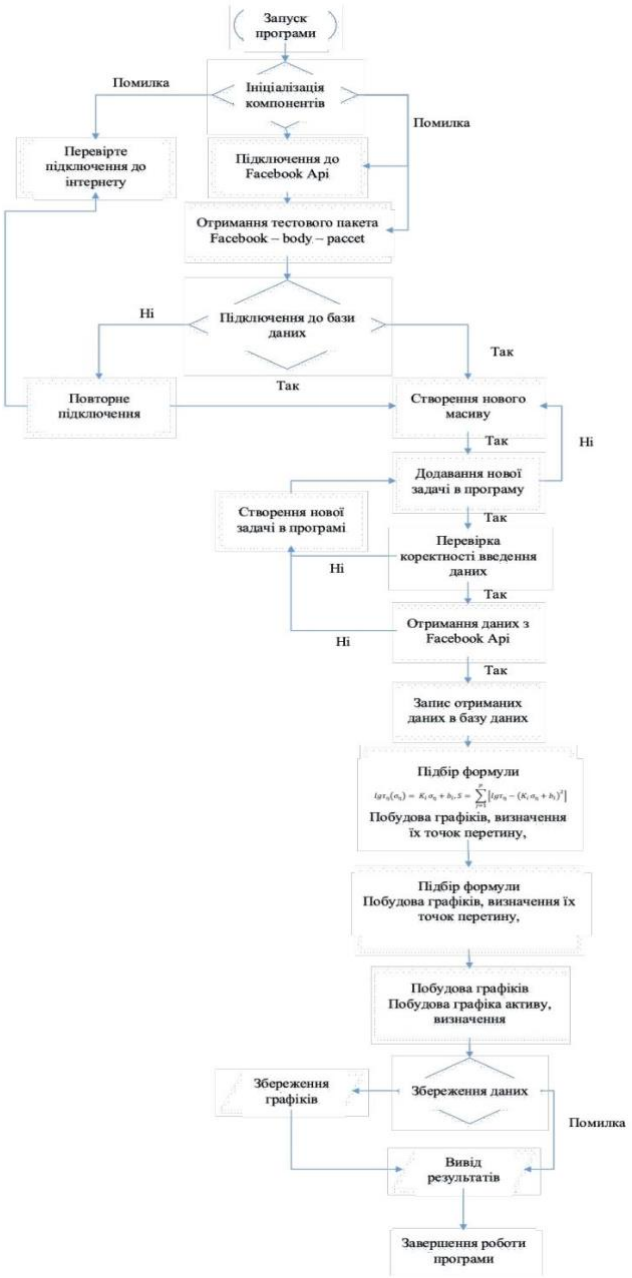


Рисунок 2.10 -- Блок схема програмного додатку

На основі створеного алгоритму буде розроблено програмний додаток з використанням вдосконалених алгоритмів на прикладі соціальної мережі Facebook. Підключення до API Facebook [38] здійснюється через певний обліковий запис у соціальній мережі, тому потрібен «вхід» у мережу. Якщо ви використовуєте програму без доступу до свого облікового запису Facebook, ви не зможете отримати всі дані.

2.6 Висновки та постановка задач

У другому розділі дипломної роботи було зосереджено увагу на вдосконаленні методів виявлення автоматично генерованої дезінформації в соціальних мережах під час інформаційних конфліктів.

Особливий акцент робився на аналізі існуючих підходів, виявленні їх недоліків та розробці більш досконалих критеріїв для ідентифікації дезінформації. Це дослідження допомогло зрозуміти ключові аспекти, які впливають на поширення недостовірної інформації, та визначити нові шляхи її виявлення.

Одним з важливих елементів роботи стало покращення алгоритмів обробки природної мови (NLP) та аналізу метаданих. Ці удосконалення дозволили значно підвищити точність та швидкість процесу ідентифікації дезінформації, забезпечуючи більш ефективний аналіз великих даних та виявлення потенційно маніпулятивних повідомлень.

Значною інновацією у дослідженні стало впровадження штучного інтелекту для розширення можливостей виявлення дезінформації. Завдяки застосуванню ШІ, було можливо не лише аналізувати текстовий контент, але й ефективно виявляти маніпуляції у візуальних матеріалах, таких як зображення та відео, що є особливо важливим у контексті широкого використання візуальних засобів комунікації у сучасному медіапросторі.

Результати дослідження підтвердили, що запропоновані удосконалення забезпечують високий рівень ефективності у виявленні дезінформації. Це включає в себе значне покращення у точності визначення фейкових новин, збільшення швидкості обробки даних, а також підвищення адаптивності системи до нових форм і методів дезінформації.

Висновки цього дослідження стануть важливим внеском у розвиток стратегій протидії інформаційним загрозам у соціальних мережах, що має велике значення у сучасному світі, де інформаційні конфлікти стають дедалі поширенішими та впливовішими.

У результаті проведеного у другому розділі дослідження було підтверджено значну ефективність запропонованих методів у виявленні дезінформації. Це стосується, зокрема, збільшення точності та швидкості обробки даних, а також покращення адаптивності системи до нових форм та методів дезінформації.

Ці удосконалення дозволяють системі більш ефективно реагувати на швидкозмінні умови інформаційних конфліктів, що є важливим внеском у стратегії боротьби з інформаційними загрозами в соціальних мережах, особливо у контексті сучасного цифрового світу.

На основі отриманих результатів було сформульовано наступні основні завдання для подальшої роботи:

- Розробка програмного засобу, що базується на удосконалених методах візуального моніторингу та аналізу поширення інформації в соціальній мережі Facebook. Це включає створення інструментів, здатних ефективно виявляти та аналізувати потоки інформації, ідентифікувати потенційні джерела дезінформації та оцінювати їх вплив на громадську думку.
- Аналіз економічної ефективності розробленого програмного забезпечення. Це завдання передбачає оцінку вартості розробки та впровадження програмного продукту в порівнянні з його потенційними перевагами для інформаційної безпеки.

3. ПРОГРАМНИЙ ЗАСІБ ДЛЯ РЕАЛІЗАЦІЇ УДОСКОНАЛЕНОГО МЕТОДУ

У даному розділі роботи ми зосередимо увагу на розробці програмного засобу для реалізації удосконаленого методу виявлення автоматично генерованої дезінформації у соціальних мережах. Основою для цього стане використання мови програмування Python, яка відома своїми потужними можливостями у сферах обробки даних та машинного навчання.

Технологія програмування в контексті нашого дослідження включає в себе визначення послідовності виконання технологічних операцій, перерахування умов, за яких виконується кожна операція, та детальний опис цих операцій. Основна мета - розробка програмного засобу, що дозволить реалізувати удосконалений метод виявлення дезінформації у соціальних мережах, а також детальний опис функціоналу цього додатку.

Застосування Python як мови програмування обрано через його широкі можливості у сфері обробки природної мови (NLP), аналізу метаданих та використання машинного навчання. Це дозволяє ефективно працювати з великими обсягами даних, характерними для соціальних мереж, і застосовувати складні алгоритми для точного виявлення дезінформації.

Розроблений у рамках дослідження програмний засіб буде протестовано на реальних даних, щоб перевірити його здатність виявляти дезінформацію в соціальних мережах. Це дозволить оцінити його практичну придатність та ефективність у реальних умовах інформаційних конфліктів.

3.1 Вибір мови програмування

Для реалізації програмного засобу, який використовуватиме удосконалений метод виявлення автоматично генерованої дезінформації у соціальних мережах, вибір мови програмування відіграє ключову роль. Серед широкого спектра мов програмування, таких як C# [39], C++ [40], Java [41] та інші, для цього проекту було обрано Python [42] та середовище PyCharm [43]. Причини вибору Python полягають у його високій гнучкості, ефективності у роботі з великими обсягами даних та

потужних можливостях для обробки природної мови та використання штучного інтелекту.

Python відомий своїм багатим набором бібліотек, які ідеально підходять для задач аналізу соціальних мереж. Для цього додатку ми використовуватимемо наступні бібліотеки:

Requests- для взаємодії з API Facebook, що дозволяє збирати дані з соціальних мереж [44].

Pandas - для обробки та аналізу даних, зібраних з соціальних мереж [45].

Numpy - для виконання числових обчислень та маніпуляцій з даними [46].

Scikit-learn - для машинного навчання та розробки алгоритмів, здатних ідентифікувати потенційну дезінформацію [47].

NLTK - для обробки природної мови, зокрема для аналізу текстового контенту коментарів [48].

Matplotlib - для візуалізації результатів аналізу [49].

Додатково, використання Python дозволяє інтегрувати ChatGPT API для розширеного аналізу та ідентифікації потенційної дезінформації. Це забезпечує можливість більш глибокого аналізу контенту, включаючи контекстуальне розуміння та розпізнавання складних мовних патернів.

Загалом, вибір Python і відповідних бібліотек забезпечує високу ефективність та гнучкість при розробці програмного засобу, що має сканувати спільноти у соціальних мережах, аналізувати коментарі та виявляти потенційну автоматично генеровану дезінформацію.

Розглянемо детальніше вибір засобів програмування, які будуть використовуватись при створенні додатку.

Перш за все, бібліотека Requests стане ключовим інструментом для взаємодії з API Facebook. Вона дозволяє легко виконувати HTTP-запити до соціальної мережі, отримувати важливі дані, такі як публікації та коментарі [50].

Для обробки та аналізу отриманих даних буде використовуватися бібліотека Pandas, яка є стандартом де-факто в області аналізу даних. Вона дозволяє легко структурувати дані у вигляді DataFrame [51], забезпечуючи широкий набір інструментів для маніпуляції та аналізу даних.

Для числових обчислень та статистичного аналізу буде використовуватися бібліотека Numpy, яка дозволяє ефективно працювати з великими масивами даних та виконувати складні математичні операції.

Scikit-learn, одна з найпопулярніших бібліотек машинного навчання для Python, буде застосовуватися для розробки алгоритмів класифікації та аналізу шаблонів. Вона надає широкий спектр алгоритмів, які можна легко інтегрувати у програмний засіб.

Для обробки природної мови будуть використані бібліотеки NLTK або spaCy, які дозволяють аналізувати мову, розбивати текст на слова, визначати частини мови та витягувати значущі дані з текстових повідомлень.

Для візуалізації даних буде використовуватися Matplotlib або Seaborn, які є потужними інструментами для створення графіків, діаграм та інших візуальних представлень даних. Це полегшить інтерпретацію результатів та підвищить інформативність програмного засобу.

Інтеграція з ChatGPT API дозволить розширити функціонал програми, додавши можливість генерації відповідей та аналізу контексту повідомлень. Використання ChatGPT допоможе в підвищенні точності в розпізнаванні мовних патернів та здатності до генерації природного мовлення.

Використання цих бібліотек та інструментів у комплексі дозволить створити ефективний та гнучкий інструмент для виявлення та аналізу потенційної дезінформації у соціальних мережах. Такий підхід забезпечує високу швидкість обробки даних, точність аналізу та можливість адаптації до різних типів даних та сценаріїв.

У контексті розробки програмного засобу для виявлення автоматично генерованої дезінформації у соціальних мережах, важливо розуміти відмінності між компіляцією та інтерпретацією коду. Обидва ці підходи мають свої специфіки, які впливають на вибір технологій та інструментів для розробки.

Компіляція полягає в перетворенні вихідного коду програми у машинний код за допомогою компілятора. Цей процес створює виконуваний файл, який можна запустити на цільовій системі. Такий підхід забезпечує вищу швидкість виконання програми, оскільки весь код перетворюється до початку його виконання. Однак це також означає, що будь-які зміни у коді вимагають його повторної компіляції.

На відміну від компіляції, інтерпретація виконує вихідний код безпосередньо, використовуючи інтерпретатор. Це означає, що вихідний код програми може бути змінений і негайно виконаний, що забезпечує гнучкість та швидкість розробки. Прикладом інтерпретованої мови є JavaScript [52], яка часто використовується в браузерах.

В контексті розробки програмного засобу для виявлення автоматично генерованої дезінформації у соціальних мережах під час інформаційних конфліктів, важливу роль відіграють API (Application Programming Interfaces). API - це набори функцій та процедур, які дозволяють створювати програми, які взаємодіють із іншими програмами або сервісами. Вони діють як будівельні блоки для розробки програмного забезпечення, значно спрощуючи процес програмування [53]. Це дозволить аналізувати контент на предмет потенційної дезінформації за допомогою алгоритмів обробки природної мови (NLP) і штучного інтелекту.

API можна поділити на дві основні категорії:

API-інтерфейси браузера: Ці API вбудовані в веб-браузери і дозволяють взаємодіяти з комп'ютерним оточенням або виконувати складні завдання. Наприклад, API Document Object Model (DOM) [54] дозволяє маніпулювати HTML і CSS, змінювати вміст веб-сторінок динамічно; API геолокації використовуються для визначення географічного положення користувача; Canvas [55] і WebGL API [56] дозволяють створювати анімовані 2D і 3D графіки, а аудіо та відео API, такі як

HTMLMediaElement [57] і WebRTC [58], використовуються для роботи з мультимедійним контентом.

Сторонні API-інтерфейси: Ці API не вбудовані в браузери і мають бути інтегровані з використанням відповідного коду. Наприклад, Facebook API дозволяє інтегрувати функціонал соціальної мережі у веб-сайти, забезпечуючи доступ до даних користувачів, публікацій та іншої інформації, що може бути корисною для аналізу та виявлення дезінформації. Google Maps API [59] використовується для інтеграції карт та географічної інформації.

Завдяки API, можна автоматизувати процес збору та аналізу даних, значно підвищуючи ефективність та швидкість обробки великих обсягів інформації. Це допоможе оперативно виявляти і реагувати на випадки автоматично генерованої дезінформації, що є особливо актуальним під час інформаційних конфліктів.

Таким чином, вибір Python як основної мови програмування для цього проекту забезпечує зручність та ефективність розробки, дозволяючи швидко адаптуватися до змінних вимог та випробувати різні методики аналізу даних.

3.2 Опис роботи програми

Встановлення бібліотек та ініціалізація середовища є першим кроком у розробці програми на Python. Для цього проекту потрібно використати бібліотеки, що дозволяють здійснювати HTTP-запити, а також аналізувати великі обсяги тексту та даних.

Спочатку необхідно встановити всі бібліотеки Python, що потрібні для роботи програмного додатку:

```
import sys
import scipy
import numpy
import matplotlib
import pandas
import sklearn
```

```
from pandas import read_csv
from pandas import DataFrame
from sklearn.model_selection import train_test_split
from sklearn.linear_model import LogisticRegression
import mysql.connector
from tkinter import *
import matplotlib.pyplot as plt
from matplotlib.backends.backend_tkagg import FigureCanvasTkAgg
import requests
import openai
import tkinter as tk
from tkinter import messagebox, simpledialog, filedialog
```

Далі, необхідно завантажити дані машинного навчання:

```
url = "https://raw.githubusercontent.com/jbrownlee/Datasets/master/iris.csv"
names = ['sepal-length', 'sepal-width', 'petal-length', 'petal-width', 'class']
dataset = read_csv(url, names=names)
```

Наступним є підготовка даних для машинного навчання:

```
array = dataset.values
X = array[:,0:4]
y = array[:,4]
X_train, X_validation, Y_train, Y_validation = train_test_split(X, y, test_size=0.20, random_state=1)
```

Використовуючи модель логістичної регресії, відбувається перевірка тестової моделі:

```
model = LogisticRegression(solver='liblinear', multi_class='ovr')
model.fit(X_train, Y_train)
```

```
predictions = model.predict(X_validation)
```

Далі, запустивши програмний додаток, користувачу необхідно буде здійснити авторизацію. Для цього застосовується база даних на MySQL:

```
class CommentAnalyzerApp:

def __init__(self, root):

self.root = root

self.root.title("Аналізатор коментарів Facebook")


self.username_label = tk.Label(root, text="Логін:")

self.username_label.pack()

self.username_entry = tk.Entry(root)

self.username_entry.pack()


self.password_label = tk.Label(root, text="Пароль:")

self.password_label.pack()

self.password_entry = tk.Entry(root, show='*')

self.password_entry.pack()


self.login_button = tk.Button(root, text="Увійти", command=self.authenticate)

self.login_button.pack()


self.api_token_label = None

self.api_token_entry = None

self.group_link_label = None

self.group_link_entry = None

self.analyze_button = None
```

```
def authenticate(self):
username = self.username_entry.get()
password = self.password_entry.get()
if True:
self.show_data_input_ui()

def show_data_input_ui(self):
self.username_label.pack_forget()
self.username_entry.pack_forget()
self.password_label.pack_forget()
self.password_entry.pack_forget()
self.login_button.pack_forget()
```

Далі, користувачу необхідно ввести API токен ChatGPT та Facebook:

```
self.api_token_fb_label = tk.Label(self.root, text="API токен Facebook:")
self.api_token_fb_label.pack()
self.api_token_fb_entry = tk.Entry(self.root)
self.api_token_fb_entry.pack()

self.api_token_chatgpt_label = tk.Label(self.root, text="API токен OpenAI:")
self.api_token_chatgpt_label.pack()
self.api_token_chatgpt_entry = tk.Entry(self.root)
self.api_token_chatgpt_entry.pack()

self.group_link_label = tk.Label(self.root, text="Посилання на групу Facebook:")
self.group_link_label.pack()
```

```
        self.group_link_entry = tk.Entry(self.root)
        self.group_link_entry.pack()

        self.analyze_button = tk.Button(self.root, text="Аналізувати",
command=self.analyze_comments)
        self.analyze_button.pack()

        def analyze_comments(self):
        facebook_token = self.api_token_fb_entry.get()
        chatgpt_token = self.api_token_chatgpt_entry.get()
        group_link = self.group_link_entry.get()

        pass

        def display_results(self, analyzed_comments):

        pass
```

Після вдалої авторизації, відбувається підключення до бази MySQL:

```
        comments = fetch_facebook_comments(group_link, facebook_token)
        chatgpt_results = analyze_comments_with_chatgpt(comments, chatgpt_token)

        ml_results = analyze_comments_with_ml(comments, ml_model)

        combined_results = list(zip(comments, chatgpt_results, ml_results))
        save_results_to_database(combined_results, {'host': 'localhost', 'database': 'disinfo', 'user':
'max', 'password': 'e621netbootr34'})
```

Далі відбувається автоматичний збір коментарів з Facebook:

```
def fetch_facebook_comments(group_link, facebook_token):

    return comments
```

Як тільки усі коментарі зібрані, надсилаються 2 запити на перевірку до бази даних та OpenAI.

```
def analyze_comments_with_chatgpt(comments, chatgpt_token):

openai.api_key = chatgpt_token

analyzed_comments = []


for comment in comments:

try:

response = openai.Completion.create(

engine="davinci",

prompt=f"Оцініть коментар на предмет дезінформації: '{comment}'",

max_tokens=50

)

analyzed_comments.append((comment, response.choices[0].text.strip()))

except Exception as e:

analyzed_comments.append((comment, f"Error: {str(e)}"))


return analyzed_comments


def analyze_comments_with_ml(comments, ml_model):

ml_results = []

for comment in comments:

prediction = ml_model.predict([comment])
```

```
ml_results.append((comment, prediction[0]))

return ml_results
```

За деякий час отриманий результат зберігається до бази даних для можливості його подальшого перегляду та навчання моделі машинного навчання:

```
def save_results_to_database(analyzed_comments, connection_details):

connection = mysql.connector.connect(**connection_details)

cursor = connection.cursor()


query = "INSERT INTO comment_analysis (comment, chatgpt_result, ml_result) VALUES (%s, %s, %s)"


for comment, chatgpt_result, ml_result in analyzed_comments:

cursor.execute(query, (comment, chatgpt_result, ml_result))


connection.commit()

connection.close()
```

Коли всі результати збережені, перед користувачем з’являється вікно з результатами аналізу:

```
def display_results(analyzed_comments):

root = Tk()

root.title("Результати аналізу коментарів")


frame = Frame(root)

frame.pack()


df = DataFrame(analyzed_comments, columns=['Коментар', 'ChatGPT', 'Машинне навчання'])
```

```
figure = plt.Figure(figsize=(6,5), dpi=100)

ax = figure.add_subplot(111)

bar = FigureCanvasTkAgg(figure, frame)

bar.get_tk_widget().pack(side=LEFT, fill=BOTH)

df.plot(kind='bar', legend=True, ax=ax)

ax.set_title('Результати аналізу коментарів')


if __name__ == "__main__":

root = tk.Tk()

app = CommentAnalyzerApp(root)

root.mainloop()
```

Далі, користувач може переглянути міні звіт або завантажити повний, й вже з ним проводи аналіз.

3.3 Приклад роботи програми

Перше вікно програми призначено для введення даних для авторизації, а саме «логін» та «пароль». Ці дані необхідні, аби отримати доступ до програми. Аби додати нового користувача, необхідно вручну прописати його інформацію через базу даних.

На даному етапі програма має простий, але зрозумілий інтерфейс, щоб не викликати складнощів з роботою.

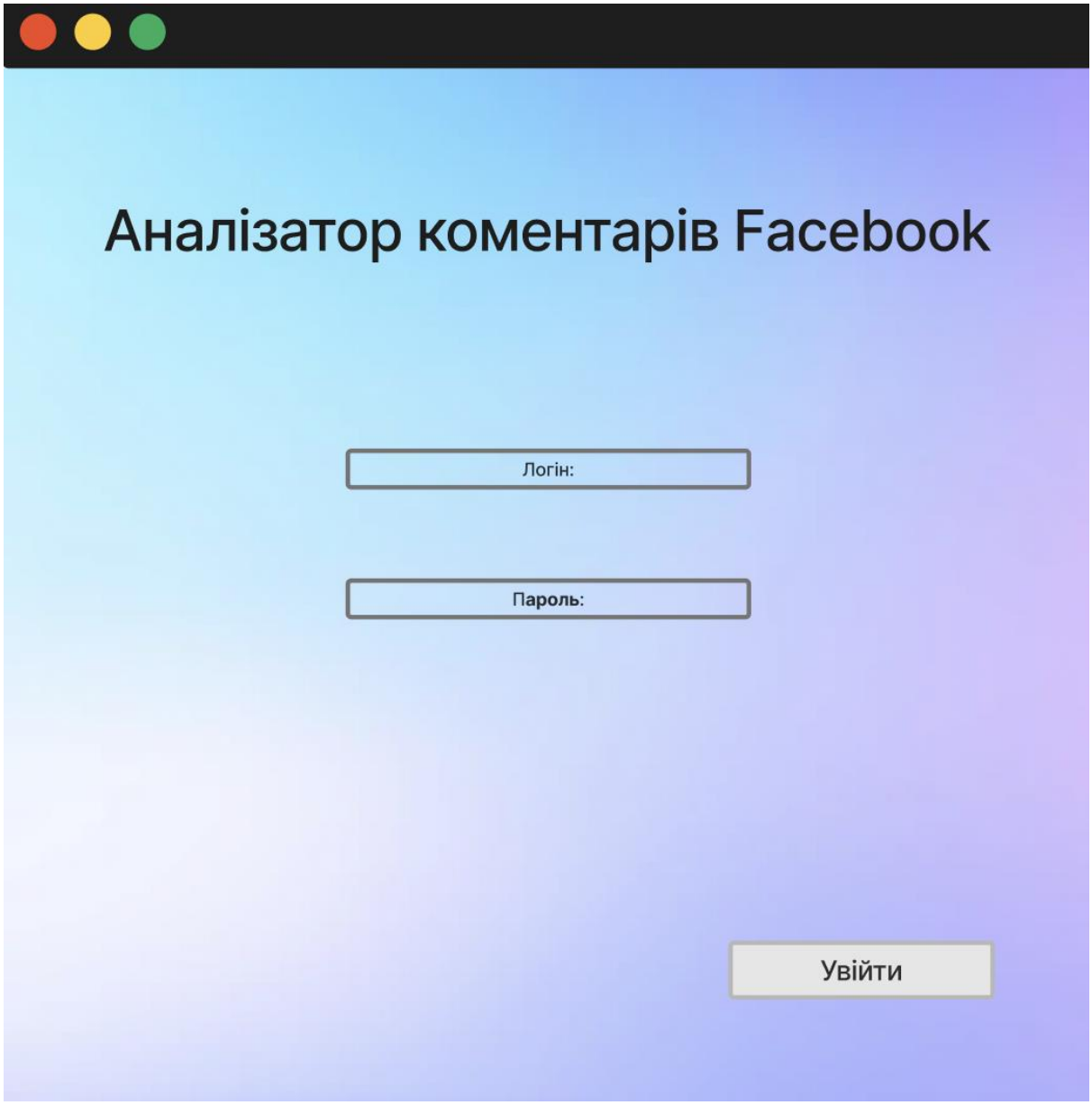


Рисунок 3.1 – Вікно авторизації до програмного застосунку

На другій сторінці необхідно ввести API токени Facebook та OpenAI, а також URL потенційної спільноти, перевірку якої будемо здійснювати.

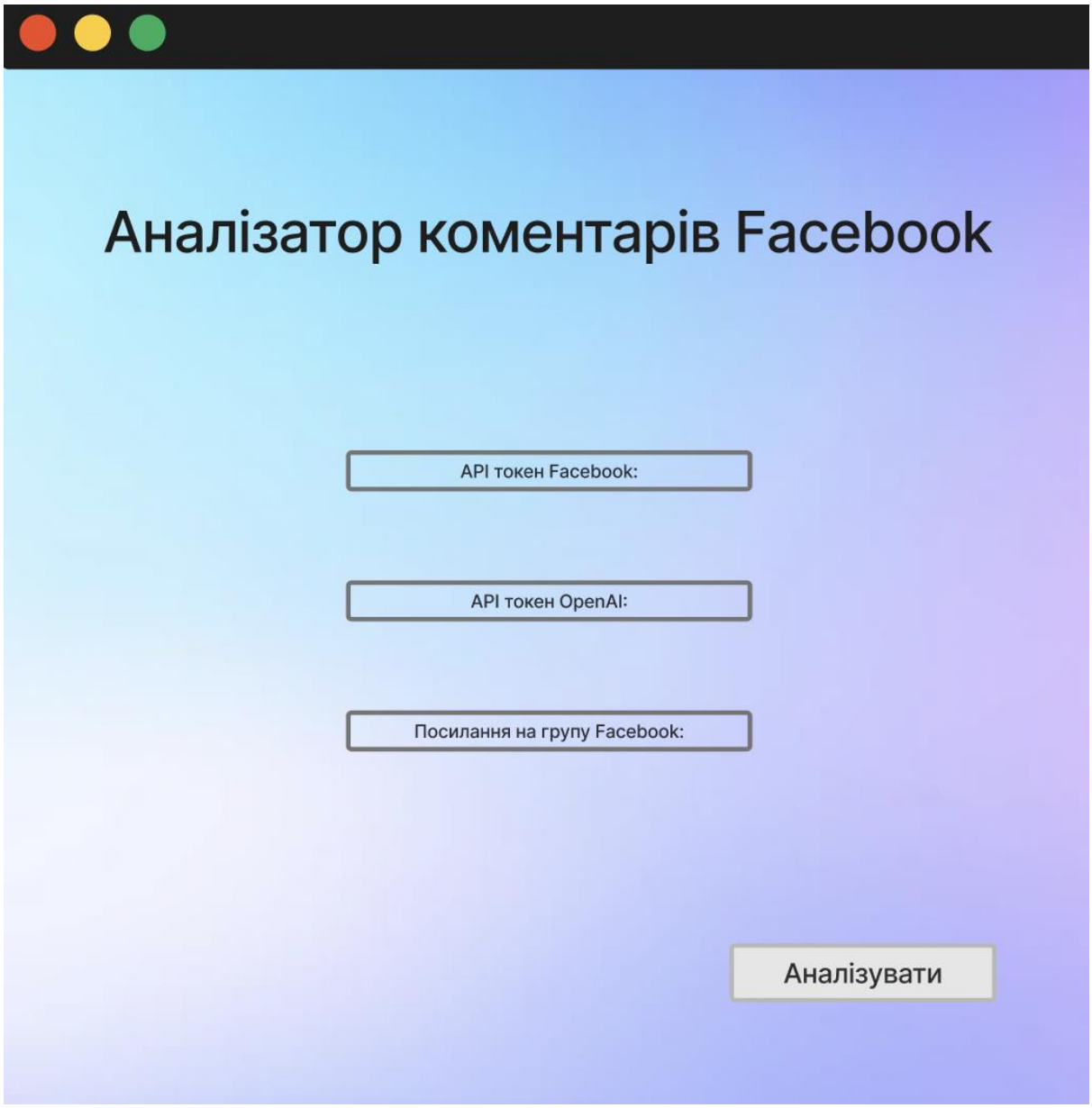


Рисунок 3.2 – Вікно введення основних даних для аналізу

Після введення всі даних, програма починає сканування, на що вказує кружечок завантаження.

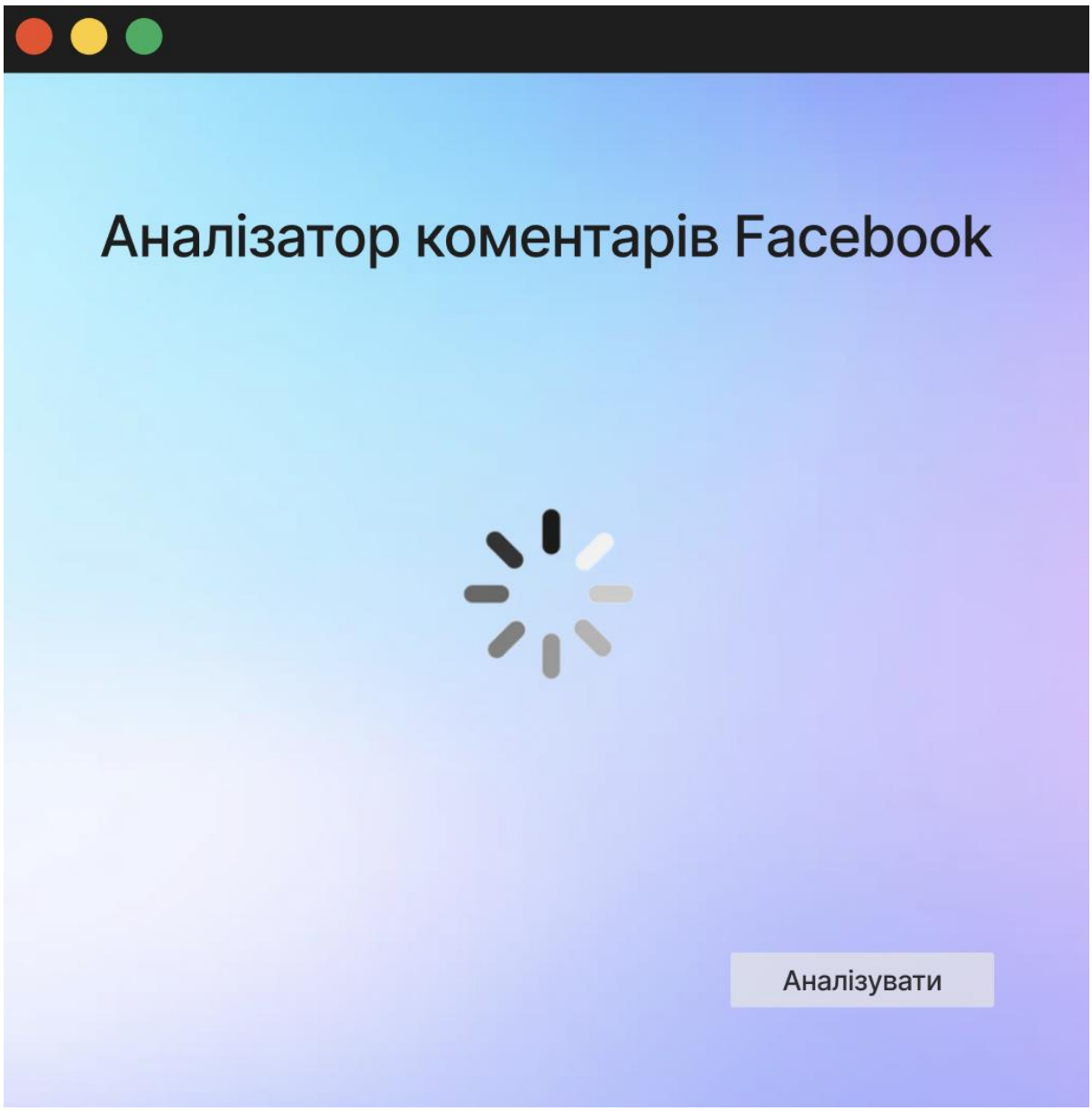


Рисунок 3.3 – Вікно очікування

По завершенню аналізу, перед користувачем з’являється міні-звіт по коментарям з найбільшою оцінкою генерації, а також можливість завантажити повний звіт.

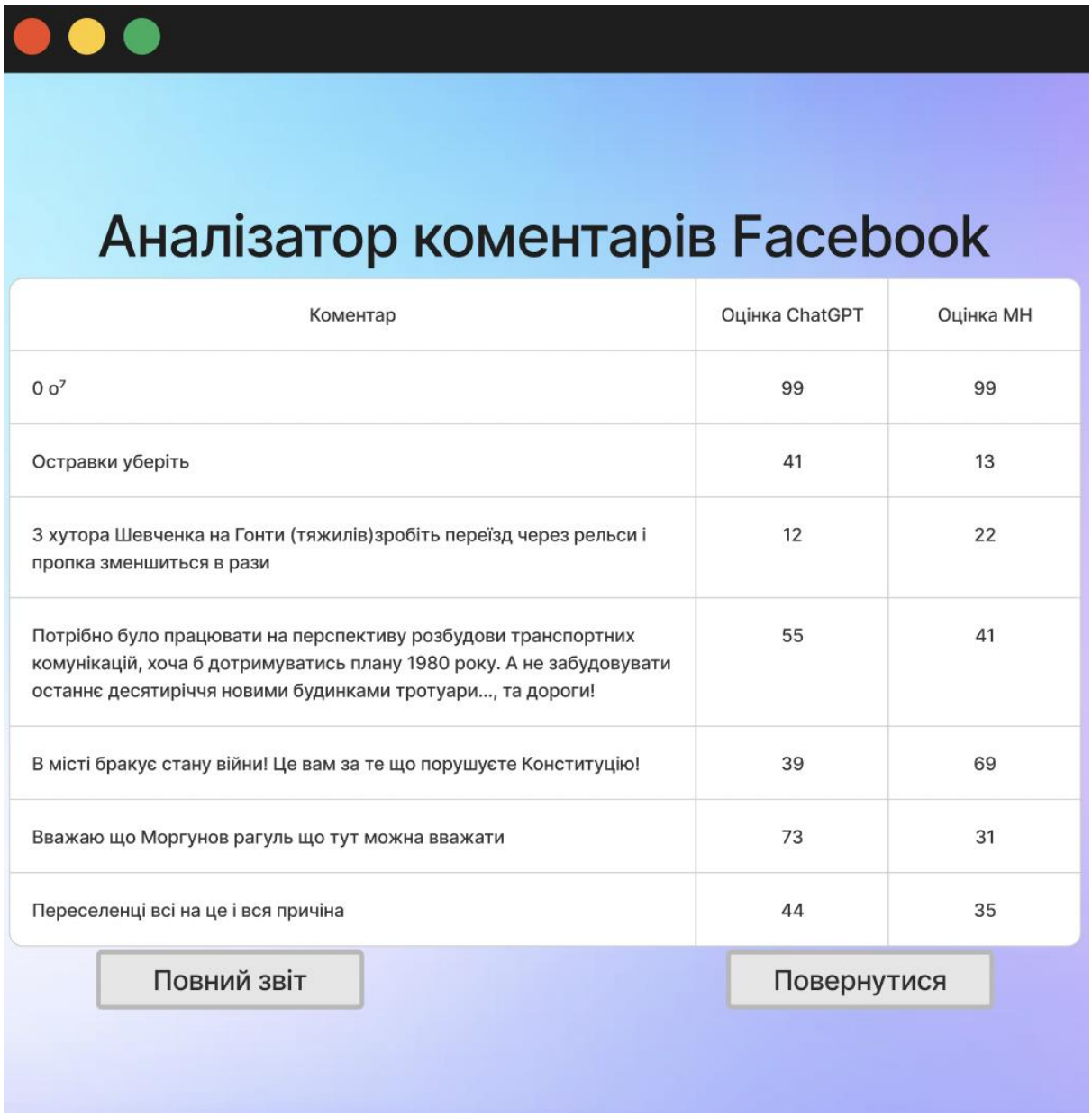


Рисунок 3.4 – Вікно часткового звіту

При натисканні кнопки «Повний звіт» відбувається запит до бази, що містить завчасно підготовлений шаблон звіту.

Перший екран містить основну інформацію про спільноту, таку як «кількість учасників», «кількість створених записів», «кількість коментарів», «кількість репостів».

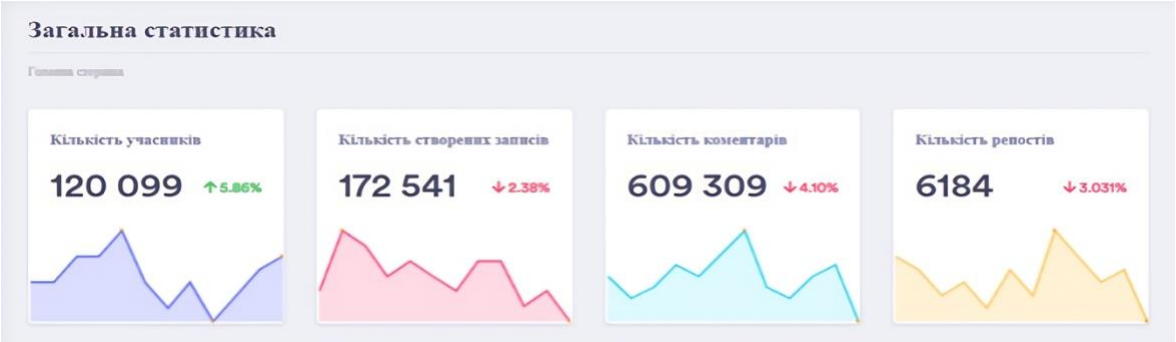


Рисунок 3.5 – Загальна статистика

Розглянемо кожен елемент детальніше:

- Кількість учасників – загальна кількість учасників у вибраній спільноті Facebook;
- Кількість створених записів – загальна кількість записів, створених спільнотою за весь час її існування;
- Кількість коментарів – загальна кількість коментарів, залишених під записом за весь час існування спільноти;
- Кількість репостів - загальна кількість натискань на кнопку «Поділитися» під записом у спільноті за весь час її існування.

Розрахунок базового індексу залучення: $BI = \left(\frac{A^{1.1}+B^{1.2}+C^{1.3}+D^{1.4}}{A+B+C+D}\right)^{1.5}$, де A — кількість учасників, B — кількість створених записів, C — кількість коментарів, D — кількість репостів.

Нормалізація індексу залученості з урахуванням експоненціального згладжування (EI):

$$EI = \frac{e^{BI}-e^{-BI}}{e^{BI}+e^{BI}}.$$

Розрахунок скоригованого індексу відносно часу (TI), де t — час у годинах від початку вимірювання:

$$TI = \frac{EI}{log(1+t)}.$$

Включення фактору для зовнішнього впливу (F):

$F = \frac{2 \cdot \pi \cdot TI}{F}$.

Загальний складний показник (CI) може бути розрахований як:

$CI = \int_0^F sin(TI \cdot x)dx$.

Остаточний показник (FI), що враховує відсоткову зміну (PC) від попереднього періоду (PP) до поточного періоду (CP):

$PC = (\frac{CP-PP}{PP}) \cdot 100\%, FI = CI \cdot PC$.

Для візуалізації результатів використовуємо умовну функцію щільності ймовірності (PDF) з параметром *FI*:

$$PDF(FI) = \frac{1}{\sqrt{2 \cdot \pi \cdot FI}} e^{-\frac{FI^2}{2}}$$

Наступний звіт містить такі показники, як «реакції користувачів» та «кількість репостів» коментарів по кварталам.

Рисунок 3.6 – Вікно аналізу реакцій користувачів

Розглянемо елементи звіту детальніше:

Аналіз реакцій користувачів - усереднено визначений емоційний стан спільноти за кількістю ключових слів у коментарях;

Кількість репостів – узагальнена кількість репостів новин. Розділено по кварталам для кращого розуміння.

Загальна кількість репостів $Qq=(Rq+Dq\cdot Rq)\cdot Cq+(RCq+Dq\cdot RCq)\cdot Cq+(RRq+Dq\cdot RRq)\cdot Cq$

Тут Dq і Cq - це коефіцієнти динаміки та контексту для кварталу q.

Для аналізу реакцій користувачів на новини, звіт містить такі показники, як «кількість лайків», «кількість емоцій», «кількість негативних реакцій» та «кількість позитивних реакій».

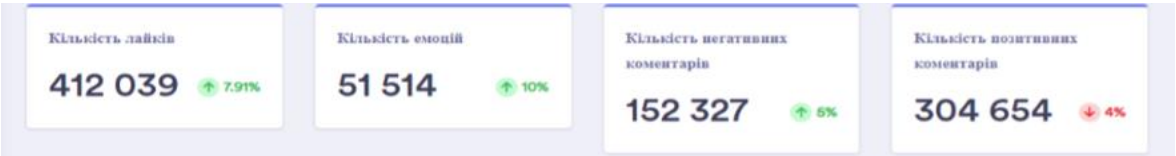


Рисунок 3.7 – Вікно підрахунку реакцій користувачів

Кількість лайків – це загальна кількість кліків людей, які додали «Клас» до записів або коментарів інших учасників спільноти.

Кількість реакцій – загальна кількість кліків людей, які оцінили «реакцію» на записах або коментарях інших учасників спільноти

Кількість негативних реакцій - це сума всіх знайдених коментарів, які містять ключові фрази, які натякають на негативний емоційний стан.

Кількість позитивних реакцій - це сума всіх знайдених відгуків, які містять ключові фрази, які передбачають позитивний емоційний стан.

Для підрахунку використовується наступна формула:

$$Z = (l \cdot (1 + \frac{\Delta L}{100})) \cdot (E \cdot (1 + \frac{\Delta E}{100})) \cdot (\frac{(N_c \cdot (1+\frac{\Delta N_c}{100}) \cdot I \cdot \alpha) + (P_c \cdot (1+\frac{\Delta P_c}{100}) \cdot I \cdot b)}{2})$$

Для підведення результату щодо «спамних» або неправдивих коментарів, використовується діаграма, що розділена на такі категорії, як: «Власна думка», «Скарга», «Відгуки», «Новини», «Пропозиції» та «Спам».

До категорії «Спам», потрапляють коментарі, що містять високу оцінку від ChatGPT та моделі машинного навчання.

Рисунок 3.8 – Діаграма «Аналіз коментарів»

Для прорахунку діаграми використовується наступна формула:

$$C_{total} = \sum_{i=1}^{n} C_i$$

$$C_i = (P_i \cdot C_{total} \cdot A_i \cdot E_i \cdot F_i)$$

де:

- lCtotal - загальна кількість коментарів,
- *Ci* - кількість коментарів у категорії i*i*,

- *Pi* - відсоток коментарів у категорії i*i* від загальної кількості (виражений як десятковий дріб),
- *Ai* - актуальність коментарів у категорії i*i* (виражена у формі вагового коефіцієнта),
- *Ei* - залученість аудиторії до коментарів у категорії i*i* (виражена у формі вагового коефіцієнта),
- *Fi* - частота згадування коментарів у категорії i*i* (виражена у формі вагового коефіцієнта).

3.4 Висновки та постановка задач

В рамках цього розділу було проведено всебічний аналіз існуючих технологій, програмних платформ і мов програмування, що забезпечило обґрунтований вибір оптимальних інструментів для створення програмного продукту.

Проведений аналіз включав оцінку різноманітних технологічних рішень, з акцентом на їхню здатність вирішувати конкретні задачі, пов’язані з виявленням дезінформації в соціальних мережах.

Вибір Python як головної мови програмування обумовлений його гнучкістю, масштабованістю та широким спектром доступних бібліотек для обробки даних, що є критично важливим для задач аналізу і обробки великих обсягів інформації.

Особлива увага була приділена інтеграції з API соціальних мереж, зокрема Facebook, та можливостям використання можливостей штучного інтелекту через API ChatGPT. Це дозволило розробити комплексне рішення, яке ефективно об'єднує автоматизований збір даних з соціальних мереж і застосування передових алгоритмів машинного навчання для їх аналізу. Такий підхід забезпечує глибоке розуміння контексту та значення інформації, що циркулює в соціальних мережах, та сприяє точному виявленню потенційної дезінформації.

Завдяки цьому комплексному підходу, програмне забезпечення, розроблене в рамках цієї роботи, відповідає ключовим вимогам щодо точності, швидкості

обробки даних та гнучкості у налаштуваннях. Воно здатне ефективно аналізувати великі обсяги інформації з соціальних мереж, ідентифікувати і класифікувати дезінформацію, що значно підвищує якість та надійність інформаційного простору.

Розробка та впровадження програмного продукту для аналізу дезінформації в соціальних мережах підтвердила його високу ефективність у виявленні та аналізі неправдивої інформації. Використання передових технологій штучного інтелекту та машинного навчання дозволило створити інструмент, здатний точно ідентифікувати потенційно шкідливий контент.

Завдяки цьому, програма забезпечила вагомий вклад у боротьбу з розповсюдженням фейкових новин, вирішивши ключову задачу, поставлену на початку дослідження.

На основі отриманих результатів та досвіду реалізації проекту можна визначити наступні напрямки подальшої роботи, які випливають з поставлених у вступі цілей:

- Проаналізувати економічну ефективність розробленого програмного засобу, зосередившись на оцінці витрат на розробку та експлуатацію в порівнянні з його ефективністю у виявленні дезінформації в соціальних мережах. Це дозволить оцінити економічну доцільність проекту та його потенційну рентабельність, що є ключовим для забезпечення його тривалої стабільності та розвитку.

4. ЕКОНОМІЧНА ЧАСТИНА

4.1 Комерційний та технологічний аудит науково-технічної розробки

У цьому розділі проводиться комплексний технологічний аудит з метою оцінки комерційного потенціалу розробленого інструменту для виявлення дезінформації в соціальних мережах. Дана розробка є ключовим результатом науково-технічної роботи, що зосереджується на дослідженні способів і методів отримання нових знань та пошук можливості їхнього застосування.

Об’єктом дослідження є процес розробки та програмна реалізація інструменту для виявлення дезінформації в соцмережах. Вона включає в себе аналіз великих обсягів даних із застосуванням сучасних методів машинного навчання та штучного інтелекту.

Для забезпечення об'єктивної оцінки розробки буде залучено комісію з трьох незалежних експертів. Оцінка буде проведена за п’ятибальною системою, ґрунтуючись на 12 заздалегідь визначених критеріях, які охоплюють наукові, технічні аспекти та комерційну життєздатність розробки.

Середнє арифметичне отриманих балів від експертів стане основою для визначення рівня комерційного потенціалу розробленого інструменту. Такий системний підхід дозволяє отримати цінну інформацію про ефективність, важливість та доцільність інноваційного рішення у контексті виявлення дезінформації.

У рамках розділу будуть представлені та проаналізовані результати оцінювання чотирьох альтернативних програмних рішень для виявлення дезінформації у соціальних мережах порівняно з розробленою програмою.

Це дозволить здійснити порівняльний аналіз комерційного потенціалу та якості кожної програми відносно удосконаленого методу.

Цей підхід відкриває можливості для глибокого розуміння комерційної цінності розробки та її місця на ринку інструментів для боротьби з дезінформацією в цифровому середовищі.

Оцінка комерційного потенціалу розробки базуватиметься на простих, але важливих критеріях, які дадуть змогу користувачам об'єктивно оцінити програму за ключовими показниками продуктивності та зручності використання. Ці критерії будуть відображені у вигляді таблиці 4.1 для зручного порівняння та аналізу.

Таблиця 4.1

Критерії оцінювання комерційного та технологічного потенціалу розробки

Критерії	**Опис**
1.	**Точність класифікації:** Наскільки точно програма ідентифікує фейкову та справжню інформацію? (Шкала: від поганої до відмінної)
2.	**Швидкість обробки:** Як швидко програма аналізує та класифікує інформацію? (Шкала: від повільної до швидкої)
3.	**Зручність використання:** Наскільки легко користувачеві взаємодіяти з програмою? (Масштаб: від складного до інтуїтивно зрозумілого)
4.	**Ефективність використання ресурсів:** Чи ефективно програма використовує системні ресурси? (Шкала: від неефективного до ефективного)
5.	**Адаптивність:** Чи може програма ефективно обробляти різні типи новинного контенту? (Масштаб: від обмеженого до універсального)
6.	**Рівень хибнопозитивних спрацьовувань:** Як часто програма помилково класифікує справжню інформацію як фейкову? (Шкала: від високого до низького)
7.	**Частота хибнонегативних спрацьовувань:** Як часто програма пропускає класифікацію фейкової інформації? (Шкала: від високого до низького)
8.	**Легкість навчання:** Наскільки просто навчити чи оновити програму? (Шкала: від складного до простого)
9.	**Можливість інтеграції:** Наскільки добре програма інтегрується з іншими інструментами чи платформами? (Шкала: від обмеженої до безшовної)
10.	**Механізм зворотного зв'язку:** Чи забезпечує програма чіткий зворотний зв’язок щодо своїх рішень щодо класифікації? (Масштаб: від незрозумілого до прозорого)

11.	**Вимоги до обчислювальних ресурсів:** Скільки обчислювальної потужності вимагає програма? (Шкала: від високого до низького)
12.	**Надійність:** Наскільки добре програма працює за різних умов та вхідних даних? (Шкала: від ненадійної до надійної)

Результати оцінювання незалежними експертами комерційного та технологічного потенціалу розробки наведено у таблиці 4.2.

Таблиця 4.2

Результати оцінювання незалежними експертами комерційного та технологічного потенціалу розробки

Критерії	**Бали (1-5)**			
	Експерт 1	**Експерт 2**	**Експерт 3**	**Середнє значення**
1.	4	3	4	
2.	4	4	3	
3.	4	3	3	
4.	3	4	4	
5.	4	3	4	
6.	4	4	4	
7.	3	4	4	
8.	3	4	4	
9.	3	4	4	
10.	3	2	3	
11.	4	3	4	
12.	4	4	4	
Сума	43	42	45	43,33

Виходячи з цього, загальне середнє значення вказує на достатній рівень комерційного потенціалу.

Сильні сторони розробленого програмного засобу для виявлення генерованої дезінформації в соціальних мережах полягають у високій точності аналізу, швидкості обробки даних та технічних характеристиках, зокрема в ефективності використання алгоритмів штучного інтелекту та машинного навчання. Однак, існують можливості для покращення, особливо в аспектах зворотного зв’язку з користувачами та інтеграції з різними платформами соціальних мереж. Це дозволяє програмі демонструвати значний потенціал для практичного застосування та успішного впровадження на ринок.

У подальшому аналізі будуть представлені результати оцінки трьома незалежними експертами за 12 критеріями чотирьох альтернативних програм для виявлення дезінформації в соціальних мережах. Це включає дві українські розробки – Texty.org.ua [60] та StopFake.org [61], а також міжнародні платформи – Snopes [62] і FactCheck.org [63]. Ці оцінки мають на меті всебічне порівняння та визначення комерційного потенціалу та відносної якості кожного інструменту у порівнянні з розробленим методом виявлення генерованої дезінформації у соціальних мережах, основаного на застосуванні передових технологій штучного інтелекту та машинного навчання.

У таблиці 4.4 представлено результати оцінювання трьома незалежними експертами українського програмного засобу Texty.org.ua:

Таблиця 4.4

Результати оцінювання незалежними експертами програми Texty.org.ua

Критерії	**Бали (1-5)**			
	Експерт 1	**Експерт 2**	**Експерт 3**	**Середнє значення**
1.	3	2	2	
2.	4	3	4	

3.	3	3	2	
4.	3	3	3	
5.	3	3	3	
6.	3	2	2	
7.	2	3	3	
8.	3	3	3	
9.	2	2	3	
10.	3	3	3	
11.	4	3	3	
12.	3	3	2	
Сума	36	33	33	34

Розрахункова середня оцінка для Texty.org.ua становить приблизно 34. Це нижче, ніж середня оцінка нашої програми, яка була більше за 40 що вказує на те, що наша програма має вищий рівень комерційного потенціалу за цими критеріями.

У таблиці 4.5 представлено результати оцінювання трьома незалежними експертами українського засобу StopFake.org:

Таблиця 4.5

Результати оцінювання програми StopFake.org

Критерії	**Бали (1-5)**			
	Експерт 1	**Експерт 2**	**Експерт 3**	**Середнє значення**
1.	2	3	2	
2.	4	3	3	
3.	2	3	3	
4.	2	2	3	
5.	3	3	3	

6.	3	3	3	
7.	3	2	3	
8.	3	2	3	
9.	3	2	3	
10.	2	2	2	
11.	4	3	3	
12.	2	3	3	
Сума	33	31	34	32,67

Розрахований середній рейтинг для StopFake.org становить 32,37 Це трохи нижче середнього рейтингу для Texty.org.ua, який становив 34, що вказує на те, що Texty.org.ua має дещо вищий рівень комерційного потенціалу за цими критеріями.

У таблиці 4.6 представлено результати оцінювання трьома незалежними експертами зарубіжного програмного засобу Snopes:

Таблиця 4.6

Результати оцінювання програми Snopes

Критерії	**Бали (1-5)**			
	Експерт 1	**Експерт 2**	**Експерт 3**	**Середнє значення**
1.	3	3	2	
2.	3	3	3	
3.	3	3	3	
4.	3	3	3	
5.	3	2	3	
6.	3	3	3	
7.	2	3	3	
8.	3	3	3	

9.	2	3	2	
10.	3	3	3	
11.	3	3	3	
12.	3	4	3	
Сума	34	36	34	34,67

Розрахований середній рейтинг для Snopes становить 34,67. Це означає, що Snopes є розумною альтернативою, але не значно кращою за українські аналоги, а тим більше за нашу розробку.

У таблиці 4.7 наведено результати оцінювання трьома незалежними експертами іноземного програмного засобу FactCheck.org:

Таблиця 4.7

Результати оцінювання програми FactCheck.org

Критерії	**Бали (1-5)**			
	Експерт 1	**Експерт 2**	**Експерт 3**	**Середнє значення**
1.	2	3	2	
2.	4	3	4	
3.	3	3	3	
4.	3	3	3	
5.	3	4	3	
6.	3	3	3	
7.	3	4	4	
8.	3	3	4	
9.	2	3	3	
10.	2	3	3	
11.	3	3	4	

12.	3	3	4	
Сума	34	38	40	37,33

Розрахований середній рейтинг для FactCheck.org становить 37,33.

Отже, після оцінювання та порівняння трьома незалежними експертами чотирьох альтернативних програм для виявлення генерованої дезінформації в соціальних мережах за 12-ма заздалегідь визначеними критеріями були отримані наступні висновки:

Texty.org.ua: ця програма отримала високу оцінку, але все ж не досягла рівня розробленої програми. Вона вирізняється простотою використання та легкістю освоєння, проте її загальна продуктивність є меншою порівняно з розробленим рішенням, що використовує методи штучного інтелекту та машинного навчання.

StopFake.org: так само, як і Texty.org.ua, показала порівняльні показники, але не змогла перевершити продуктивність розробленої програми.

Snopes: міжнародна програма, яка продемонструвала середні показники продуктивності, близькі до 35, що свідчить про можливості для покращення за різними параметрами. Її оцінка значно нижча за розроблену систему, яка базується на використанні штучного інтелекту та машинного навчання.

FactCheck.org: інша міжнародна програма, отримала середній рейтинг 37,33. Цей інструмент також поступається за продуктивністю розробленому рішенню в багатьох аспектах.

На основі цих оцінок стає зрозуміло, що розроблений вдосконалений метод виявлення генерованої дезінформації в соціальних мережах за допомогою штучного інтелекту та машинного навчання забезпечує значну конкурентну перевагу. Наша програма виявилася вищою за середні оцінки за всіма критеріями, демонструючи підвищену точність, швидкість обробки, використання ресурсів, адаптивність і надійність. Особливо слід відзначити її переваги в точності, швидкості обробки та технічних характеристиках.

Представлене рішення пропонує значно надійніший і ефективніший підхід до виявлення генерованої дезінформації, випереджаючи як українські, так і міжнародні альтернативи.

4.2 Прогнозування витрат на виконання науково-дослідної (дослідно-конструкторської) роботи

Прогнозування витрат на виконання науково-дослідної роботи є критично важливим кроком у будь-якому комплексному проєкті. Цей процес фінансового планування має важливе значення для забезпечення ефективного виконання проєкту та ретельного врахування всіх фінансових аспектів. Щоб полегшити цей процес, ми структурували прогнозування на три окремі етапи. На першому етапі ми заглиблюємося в оцінювання витрат, безпосередньо пов'язаних із робочою силою, залученою до проєкту. Другий етап розширює обсяг, щоб охопити загальні витрати проєкту, від інфраструктури та технологій до збирання та розробки даних. Нарешті, на третьому етапі враховуються витрати на впровадження результатів дослідження та введення в дію результатів проєкту. Разом ці етапи пропонують систематичний підхід до складання бюджету та фінансового менеджменту для дослідницьких та проектних починань.

Основну зарплату розробника розрахуємо за формулою (4.1):

$$З_о = \frac{М}{Т_р} \cdot t, \qquad (4.1)$$

де M – місячна зарплата розробника;

T_p – кількість робочих днів у місяці, T_p = 21 день;

t – кількість днів роботи.

Місячна зарплата складає 18000 грн., t = 60 днів.

Тоді, базовий оклад розробника становить:

$$З_р = \frac{20000}{21} \cdot 60 = 51428{,}57 \text{ грн.}$$

Розрахуємо основну зарплату для керівника (при місячному посадовому

окладі становить 25000 грн.):

$$З_к = \frac{25000}{21} \cdot 60 = 71428{,}57 \text{ грн.}$$

Розрахуємо витрати на оплату праці:

$З_о = З_р + З_к = 51428{,}57 + 71428{,}57 = 122857{,}14$ грн.

Додаткова заробітна плата розраховується у розмірі 10% від основної зарплати розробника та керівника [43]:

$$З_д = З_о \cdot 0{,}1 = 122857{,}14 \cdot 0{,}1 = 12285{,}71 \text{ грн.}$$

Нарахування на зарплату складають 22% від сум базової та додаткової грошової оплати (формула 4.2):

$$H_{зп} = (З_о + З_д) \cdot 0{,}22 \qquad (4.2)$$

Розрахуємо нарахування на оклад розробника:

$$Н_{зп} = (122857{,}14 + 12285{,}71) \cdot 0{,}22 = 29731{,}43 \text{ грн.}$$

Розрахуємо відрахування на амортизацію устаткування за формулою (4.3). Для розробки було обрано базову модель Apple MacBook Air M1 8/256GB [64], адже на ній було проведено тестування програми й вона показала найкращі результати продуктивності.

$$A = \frac{Ц \cdot H_a}{100} \cdot \frac{T}{12}, \qquad (4.3)$$

де $Ц$ – вартість устаткування, $Ц$ = 39 499 грн.;

H_a – річна норма амортизації, H_a = 20%;

T – термін використання устаткування, T = 4 місяці.

$$А = (\frac{39499 \cdot 20}{100} \cdot \frac{4}{12}) = 2333 \text{ грн.}$$

Також розрахуємо амортизацію за середовища розробки програми.

$$A = \frac{Ц \cdot H_a}{100} \cdot \frac{T}{12}, \qquad (4.3)$$

де $Ц$ – вартість програмного забезпечення, $Ц$ = 4 365 грн.;

H_a – річна норма амортизації, H_a = 20%;

T – термін використання ПЗ, T = 4 місяці.

$$\text{А} = (\frac{4365 \cdot 20}{100} \cdot \frac{4}{12}) = 291 \text{ грн.}$$

При розробці були використані матеріали, кількість та вартість яких зведені в таблицю 4.8.

Таблиця 4.8

Матеріали, використані для реалізації проєкту

Найменування матеріалу, марка, тип, сорт	Ціна, грн.	Витрачено	Вартість витрачених матеріалів, грн.
Папір А4	200	3	600
Флеш USB	200	1	200
Папка для паперів	50	2	100
Файли	20	1	20
Ручка	30	4	120
Всього:			1040

Отже, вартість витрачених матеріалів, М = 1040 грн.

Розрахуємо витрати на електроенергію за формулою (4.4):

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot К_{впі}}{\eta_i} \qquad (4.4)$$

де *Wyi* – встановлена потужність обладнання на певному етапі розробки, кВт; *Wyi* = 0,005 кВт

ti – тривалість роботи обладнання на етапі дослідження, год; *ti = 7 год · 60 днів = 420* (год.) на місяць.

Це – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії, = 7,5 грн/кВт;

Квпі – коефіцієнт, що враховує використання потужності, *Квпі <1*; *Квпі* = 0,8

η*i* – коефіцієнт корисної дії обладнання, η*i<1*. η*i* = 0,72

$B_e = \frac{(7{,}5 \cdot 0{,}005 \cdot 420 \cdot 0{,}8)}{0{,}72} = 17{,}5$ грн.

Інші затрати приймаються у розмірі 100-200% від базового окладу розробника. Використаємо значення в розмірі 100%, тоді:

$B_{ін} = 1{,}0 \cdot 12285{,}71 = 122857{,}14$ грн.

Розрахуємо загальну суму затрат на впровадження ПЗ за формулою (4.5):

$$В_{заг} = Ц + З_о + З_д + Н_{зп} + А + М + В_е + В_{ін} \qquad (4.5)$$

Отже, загальна сума витрат дорівнює:

$B_{заг} = 39499 + 4365 + 291 + 122857{,}14 + 12285{,}71 + 29731{,}43 + 2333 + 1040 + 17{,}5 + 122857{,}14 = 335\,276{,}92$ грн

Розрахуємо загальні витрати на завершення науково-технічної роботи за формулою (4.6):

$$ЗВ = \frac{В_{заг}}{\beta} \qquad (4.6)$$

де β – коефіцієнт, який характеризує стадію виконання проєкту. У нашому випадку розробка знаходиться на стадії дослідного зразка, тому β = 0,5.

$$ЗВ = \frac{335\,276{,}92}{0{,}5} = 670553{,}84 \text{ грн.}$$

4.3 Розрахунок економічної ефективності науково-технічної розробки

Прогнозування комерційних ефектів від впровадження розробленої програми аналізу дезінформації в соціальних мережах, що використовує методи штучного інтелекту та машинного навчання, зосереджується на оцінці її потенційного впливу на різні сфери комерційної діяльності. Оцінка передбачає аналіз того, як програма може додавати економічну вартість, оптимізувати процеси прийняття рішень, та вирішувати специфічні завдання у сфері інформаційної безпеки та аналізу даних. Цей процес включає оцінку потенційної затребуваності програми серед різних груп користувачів, включаючи державні організації, приватні компанії та незалежних аналітиків, які зацікавлені в надійних інструментах для ідентифікації та аналізу дезінформації в соціальних мережах.

У нашому випадку прогнозований комерційний ефект від реалізації результатів проєкту буде розрахований наступним чином (4.7):

$$\Delta П_i = (\pm \Delta Ц_0 \cdot N + Ц_0 \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot \left(1 - \frac{\vartheta}{100}\right), \qquad (4.7)$$

де $\pm\Delta Ц_o$ – зміна вартості програмного засобу у результаті впровадження науково-технічної розробки;

N – кількість користувачів, що користувалися альтернативним програмним засобом до моменту інтеграції результатів нової науково-технічної розробки;

$Ц_o$ – основна метрика ефективності, яка вказує на продуктивність підприємства за певний рік після інтеграції результатів досліджень і розробок. $Ц_o = Ц_б \pm \Delta Ц_o$;

$Ц_б$ – вартість програмного засобу за певний рік до моменту інтеграції результатів досліджень і розробок;

ΔN – зростання бази користувачів програмного засобу протягом досліджуваних інтервалів часу завдяки вдосконаленню окремих атрибутів продукту;

λ – коефіцієнт, що включає оплату податку на додану вартість. Ставка податку на додану вартість становить 20%, а коефіцієнт (λ) = 0,8333.

ρ – коефіцієнт, що враховує рентабельність засобу;

ϑ – ставка податку на прибуток, у нашому випадку, ϑ =18%.

Розглянемо сценарій, коли прогнозована ціна одиниці товару становить 4000 грн., а період збільшення прибутку – 3 роки. Після завершення розробки та доопрацювань вартість може бути збільшена на 500 грн. Крім того, збільшиться кількість користувачів на 4000 у перший рік, на 3000 одиниць у другий рік і на 2000 у третій рік. До інтеграції результатів досліджень і розробок продавався аналог програмного додатку. До 2023 року продавався єдиний аналог – Botometer, який мав близько 4000 користувачів. 20 000 000 х 0,8333 х 0,205

Перейдемо до розрахунків сценарію щодо впровадження реалізації розробки:

$\Delta П_1$ = (500 · 4000 + (4000 + 500) · 4000) · 0,8333 · 0,25 · (1 – 0,18) = 3416530 грн.

$\Delta П_2$ = (500 · 4000 + (4000 + 500) · (4000 + 3000)) · 0,8333 · 0,25 · (1 – 0,18) = 5722687,75 грн.

$\Delta П_3$ = (500 · 4000 + (4000 + 500) · (4000 + 3000 + 2000)) · 0,8333 · 0,25 · (1 – 0,18) = 7260126,25 грн.

Прогнозований комерційний ефект від інтеграції результатів дослідження та розробки за три роки становить 16399344,34 грн.

4.4 Розрахунок ефективності вкладених інвестицій та періоду їх окупності

Визначимо поточну вартість загального приросту чистого прибутку (ПП) в результаті потенційної інтеграції та комерціалізації науково-технічного розробки, на отримання якого може розраховувати інвестор за формулою (4.8):

$$ПП = \sum_{1}^{T} \left(\frac{\Delta П_i}{(1+\tau)^t} \right), \qquad (4.8)$$

де $\Delta П_i$ – приріст чистого прибутку за кожний із років, у яких наявні результати проведених та виконаних досліджень та розробок, в грн;

T – тривалість періоду, в момент якого стають очевидними результати інтегрованих досліджень та розробок, вимірюється роками.

τ – ставка дисконту, яка враховує річний прогнозований рівень інфляції в країні, $\tau = 0{,}1$;

t – період часу, у роках.

Також, слід зазначити, що зростання прибутку ми будемо отримувати з першого року:

$$ПП = \left(\frac{3416530}{(1+0{,}1)^1}\right) + \left(\frac{5722687{,}75}{(1+0{,}1)^2}\right) + \left(\frac{7260126{,}25}{(1+0{,}1)^3}\right) = 13290070{,}68 \text{ грн.}$$

Тепер, розрахуємо початкову суму інвестицій (PV), яку потенційний інвестор має спрямувати на реалізацію та комерціалізацію науково-технічної розробки, за допомогою наступної формули (4.9):

$$PV = k_{інв} \cdot ЗВ, \qquad (4.9)$$

де $k_{інв}$ – коефіцієнт, що включає витрати інвестора на інтеграцію науково-технічного засобу та його комерціалізацію, враховує такі витрати, як підготовка об’єкта, розробка програми, навчання персоналу, маркетингова діяльність. Як правило, $k_{інв}$ знаходиться в діапазоні від 2 до 5;

$ЗВ$ – загальна сума витрат на здійснення досліджень і розробок та оформлення їх результатів, грн.

$PV = 2 \cdot 670553{,}84 = 1341107{,}68$ грн.

За формулою (4.10), визначимо абсолютний економічний ефект, який позначається як E_{abc} або чистий поточний дохід (NPV), який є результатом потенційного впровадження та комерціалізації досліджень і розробок:

$$E_{абс} = ПП - PV, \qquad (4.10)$$

$E_{абс} = 13290070{,}68 - 1341107{,}68 = 11948963{,}63$ грн.

Після інтеграції нашої розробки, $E_{abc} > 0$, це свідчить про те, що впровадження нашого проєкту призведе до позитивного чистого прибутку або економічної вигоди. Це свідчить про те, що наша розробка позитивно вплине на проєкт або підприємство, зробивши його фінансово життєздатнішим і потенційно прибутковішим, ніж це було раніше.

Отже, інвестування коштів у проєкт може бути доцільним.

Для прийняття обґрунтованих рішень щодо інвестицій у дослідження і розробку вкрай важливо оцінити їх відносну (річну) ефективність. Ця оцінка допомагає нам зрозуміти економічну життєздатність цих інвестицій з часом. Відносна ефективність дає зрозуміти річний прибуток або вигоди, які можна очікувати від інвестованого капіталу. Аналізуючи цю відносну ефективність, зацікавлені сторони можуть краще оцінити довгострокові фінансові перспективи ініціатив наукового розвитку та прийняти обґрунтовані інвестиційні рішення. Тому, використовуючи формулу (4.11), розрахуємо відносну (річну) ефективність і порівняємо її з дисконтною ставкою [65]:

$$\mathrm{E_в} = \sqrt[\mathrm{Т_ж}]{1 + \frac{\mathrm{E_{абс}}}{PV}} - 1, \qquad (4.11)$$

де $T_{ж}$ – життєвий цикл наукової розробки, у роках.

$$E_в = \sqrt[3]{1 + \frac{11948963{,}63}{1341107{,}68}} - 1 = 1{,}14.$$

Розрахуємо мінімальну ставку дисконту, за формулою (4.12):

$$\tau_{min} = d + f, \qquad (4.12)$$

де d – середньозважена процентна ставка за депозитними операціями в комерційних банках, d = 0,14;

f – ризикованість вкладень, f = 0,05.

τ_{min} = 0,14 + 0,05 = 0,19.

Як бачимо, $E_в > \tau_{min}$, а це означає, що інвестор може бути зацікавлений у фінансуванні нашого проєкту.

Тепер, обчислимо термін окупності коштів, інвестованих у наший проєкт, за формулою (4.13):

$$T_{ок} = \frac{1}{\text{Е}_\text{в}}, \qquad (4.13)$$

$$T_{ок} = \frac{1}{1{,}14} = 0{,}88 \text{ р.}$$

Згідно з проведеними розрахунками, термін окупності проєкту становить менше трьох років, що свідчить про високу імовірність швидкого генерування позитивних грошових потоків від реалізації програми для виявлення генерованої дезінформації в соціальних мережах. Це вказує на значну економічну привабливість проєкту з точки зору його спроможності окупити вкладені кошти та початкові витрати у відносно короткий проміжок часу.

4.5 Висновки

У цьому розділі представлено детальну економічну оцінку науково-технічного проєкту, спрямованого на розробку і вдосконалення методів ідентифікації автоматично генерованої дезінформації в соціальних мережах. Основні висновки та ключові аспекти кожного підрозділу включають:

Підрозділ 4.1 - Комерційно-технологічний аудит:

У цьому підрозділі було виконано глибокий технологічний аудит, щоб оцінити комерційний потенціал розробленого інструменту виявлення дезінформації. За результатами оцінювання трьома незалежними експертами, загальний середній бал склав 43,33, що вказує на високий комерційний потенціал проєкту. Програма вирізняється високою точністю, швидкістю обробки даних і технічними можливостями, при цьому існують напрямки для подальшого удосконалення, зокрема в механізмах зворотного зв’язку та інтеграції. Програма демонструє значний потенціал для практичного застосування та успіху на ринку.

Також у розділі представлені результати порівняльного аналізу нашої розробки з чотирма альтернативними програмами для ідентифікації дезінформації в соціальних мережах. На основі цього аналізу стає зрозуміло, що наш удосконалений метод виявлення дезінформації з використанням штучного

інтелекту та машинного навчання володіє конкурентною перевагою, демонструючи вищі середні оцінки за всіма критеріями. Це підкреслює високу точність, швидкість обробки, адаптивність та надійність нашого рішення. Наш метод перевищує як українські, так і міжнародні альтернативи, пропонуючи надійний та ефективний спосіб виявлення фейкової інформації в соціальних мережах.

Підрозділ 4.2 - Прогнозування витрат:

Цей підрозділ присвячений прогнозуванню витрат, пов’язаних з проведенням дослідження і розробкою програмного забезпечення. Витрати були розділені на три основні етапи: витрати на робочу силу, загальні витрати на проект і витрати на впровадження результатів дослідження. Загальна сума витрат на розробку програмного продукту була оцінена у 670553,84 грн.

Підрозділ 4.3 - Розрахунок економічної ефективності:

В цьому розділі було проведено аналіз економічної ефективності розробленого продукту, розглядаючи прогнозований комерційний ефект за трирічний період. Було враховано збільшення ціни за одиницю продукту та зростання обсягу продажів, що призвело до прогнозованого загального комерційного ефекту в розмірі 16399344,34 грн за три роки. Цей розрахунок відображає потенціал розробленого програмного забезпечення як вигідної інвестиції з точки зору його здатності окупити початкові витрати та забезпечити прибутковість.

Підрозділ 4.4 - Розрахунок інвестиційної ефективності та терміну окупності: У цьому підрозділі було виконано детальний розрахунок інвестиційної ефективності та оцінено термін окупності вкладених коштів у проект розробки програмного забезпечення для виявлення автоматично генерованої дезінформації. За допомогою фінансового аналізу визначено поточну вартість загального приросту чистого прибутку, загальну суму початкових інвестицій (PV) та абсолютний економічний ефект (Eabc). Аналіз підтвердив, що Eabc є позитивним, що свідчить про чистий прибуток і економічну вигоду від реалізації проєкту.

Також було розраховано відносну (річну) ефективність проєкту, яка виявилася вищою за мінімально припустиму норму прибутку (τmin), це свідчить про зростаючий інтерес потенційних інвесторів. Термін окупності інвестицій у проект було розраховано у 0,88 року, що вказує на можливість швидкого відновлення вкладених коштів, роблячи проект привабливим для інвестицій.

Загалом, цей розділ демонструє значний комерційний потенціал і фінансову життєздатність розробки програмного забезпечення для виявлення автоматично генерованої дезінформації в соціальних мережах. Результати підтверджують, що інвестиції у розробку є вигідними, оскільки вони пропонують значні переваги у термінах економічної ефективності та потенційної прибутковості, роблячи цей проект привабливим для інвесторів та бізнес-сектору.

ВИСНОВКИ

У рамках цієї магістерської дипломної роботи було досягнуто суттєвого прогресу в розробці методів аналізу дезінформації в соціальних мережах, особливо в контексті її автоматичного генерування. Робота зосереджувалася на створенні програмного засобу, здатного ефективно ідентифікувати та аналізувати потенційно неправдиву інформацію, використовуючи передові технології штучного інтелекту та машинного навчання. Спеціальний акцент було зроблено на інтеграції з API соціальних мереж та використанні алгоритмів глибокого навчання для поліпшення точності та швидкості обробки даних, що дозволяє розпізнавати складні шаблони та контексти в інформаційних потоках.

У першому розділі дипломної роботи була проведена детальна аналітика, яка охоплювала аналіз впливу інформаційних війн на індивідуальну та групову психологію. Зокрема, були розглянуті специфічні методики та стратегії інформаційно-психологічного впливу, які використовуються у гібридних війнах. Окрім цього, у роботі особливий акцент був зроблений на вивченні соціальних мереж, що має значний вплив на процеси поширення та сприйняття інформації.

У другому розділі дипломної роботи основна увага була приділена розробці та вдосконаленню алгоритмів для аналізу дезінформації у соціальних мережах. Цей процес включав аналіз існуючих методів та їх обмежень, а також створення нових підходів, що більш точно ідентифікують дезінформацію. Особливий акцент був зроблений на використанні технологій штучного інтелекту та машинного навчання, що дозволяють розпізнавати складні взірці та моделі в поведінці користувачів та контенті.

У третьому розділі зосереджено увагу на практичній реалізації програмного засобу. Були обрані підходящі програмні інструменти, середовища та мови програмування, що відповідають потребам проекту. Детально описано процес створення програми, включаючи інтерфейс користувача та логіку обробки даних.

У четвертому розділі дипломної роботи було зосереджено увагу на економічній оцінці та комерційному потенціалі розробленого програмного засобу

для аналізу дезінформації в соціальних мережах. Важливою складовою цього розділу стало прогнозування витрат, пов'язаних з розробкою, впровадженням і подальшим використанням програми, а також оцінка потенційного комерційного ефекту від її реалізації на ринку. Було проведено детальний аналіз витрат на розробку та обслуговування програми, включаючи витрати на робочу силу, технічну інфраструктуру та маркетинг.

Ключовою частиною аналізу стало визначення ефективності інвестицій та періоду їх окупності. Використання статистичних та фінансових методів дозволило встановити часові рамки, протягом яких інвестиції у проект можуть бути повернуті, а також оцінити загальну прибутковість розробки. Аналіз показав, що завдяки високій потенційній популярності та потребі у програмі для аналізу дезінформації, проект має всі шанси стати фінансово успішним.

Окрім цього, робота має значний практичний внесок у сферу управління інформаційною безпекою, особливо в умовах інформаційної війни. Програма дозволяє ефективно аналізувати поширення інформації в соціальних мережах, ідентифікувати джерела та механізми розповсюдження дезінформації. Це дає змогу аналітичним структурам управління безпекою краще розуміти, як контролювати та запобігати поширенню небажаної інформації, що є ключовим аспектом у забезпеченні інформаційної стабільності та безпеки. Враховуючи сучасні виклики в інформаційному просторі, така розробка є необхідною для забезпечення якісного аналізу даних та ефективного реагування на інформаційні загрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Топологічні маркери інформаційно-психологічних операцій (ІПСО) в умовах війни в медіа [Електронний ресурс]. – Режим доступу: https://www.philol.vernadskyjournals.in.ua/journals/2023/1_2023/part_2/42.pdf

2. Дезінформація та виборчі кампанії [Електронний ресурс]. – Режим доступу: https://rm.coe.int/disinformation-and-electoral-campaigns-ukrainian-version-/16809fa92

3. Курбан О.В. Стратегія та тактика інформаційної війни. – Київ: ВІКНУ, 2016. – С.85-90.

4. Данько Ю.А. Соціальні мережі як форма сучасної комунікації: плюси і мінуси. -- УДК 316.472.45+316.772, 2012. – С.179-184.

5. За рік війни українці стали споживати новини з месенджерів вчетверо частіше, — дослідження [Електронний ресурс]. – Режим доступу: https://detector.media/infospace/article/208248/2023-02-22-za-rik-viyny-ukraintsi-staly-spozhyvaty-novyny-z-mesendzheriv-vchetvero-chastishe-doslidzhennya/

6. What are the most visited social media platforms among Gen Z [Електронний ресурс]. – Режим доступу: https://www.comscore.com/Insights/Blog/What-are-the-most-visited-social-media-platforms-among-Gen-Z

7. 19 Facebook Demographics to Inform Your Strategy in 2023 [Електронний ресурс]. – Режим доступу: https://blog.hootsuite.com/facebook-demographics/

8. How Many Users Does Facebook Have [Електронний ресурс]. – Режим доступу: https://99firms.com/blog/how-many-users-does-facebook-have/#gref

9. Top NLP Algorithms & Concepts [Електронний ресурс]. – Режим доступу: https://www.datasciencecentral.com/top-nlp-algorithms-amp-concepts/

10. Google BARD [Електронний ресурс]. – Режим доступу: https://bard.google.com

11. OpenAI [Електронний ресурс]. – Режим доступу: https://chat.openai.com

12. Андреєв В. І., Хорошко В. О., Чередниченко В. С., Шелест М. Є. Основи інформаційної безпеки. – К.: Вид. ДУІКТ, 2009. – 292 с.

13. Page Rank Algorithm and Implementation [Електронний ресурс]. – Режим доступу: https://www.geeksforgeeks.org/page-rank-algorithm-implementation/

14. GPTBot від OpenAI: Блокувати чи Ні? [Електронний ресурс]. – Режим доступу: https://morekoda.com/gptbot/

15. Роль інформаційно-психологічних операцій під час кризово-комунікаційного реагування [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/371821621_Rol_informacijno-psihologicnih_operacij_pid_cas_krizovo-komunikacijnogo_reaguvanna

16. Богуш В. М., Юдін О. К. Інформаційна безпека держави. – К.: «МК-Прес», 2005. – 432 с.

17. Російсько-українська війна (з 2014)" [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Російсько-українська_війна_(з_2014)

18. Про місцеве самоврядування в Україні [Текст]: закон України від 21.05.1997 р. № 280/97-ВР / Верховна Рада України. // Відомості Верховної Ради. – К., 1997. – № 24. – С. 170.

19. Ізраїльсько-палестинський конфлікт [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Ізраїльсько-палестинський_конфлікт

20. Докладніше про генеративний ШІ [Електронний ресурс]. – Режим доступу: https://support.google.com/websearch/answer/13954172?hl=uk

21. Дослідження методів класифікації зображень, отриманих з використанням технології DeepFake [Електронний ресурс]. – Режим доступу: https://openarchive.nure.ua/server/api/core/bitstreams/711325f7-1c88-4c8f-8271-1ce45abe0293/content

22. X.com (Twitter) [Електронний ресурс]. – Режим доступу: https://x.com

23. Aïmeur, E., Amri, S., Brassard, G. "Fake news, disinformation and misinformation in social media: a review. [Електронний ресурс]. – Режим доступу: https://link.springer.com/article/10.1007/s13278-023-01028-5

24. Sahoo, S., Gupta, B. "Multiple features based approach for automatic fake news detection on social networks using deep learning." [Електронний ресурс]. – Режим доступу: https://www.sciencedirect.com/science/article/pii/S1568494620309224

25. Islam, M., Liu, S., Wang, X., Xu, G. "Deep learning for misinformation detection on online social networks: a survey and new perspectives. [Електронний ресурс]. – Режим доступу: https://link.springer.com/article/10.1007/s13278-020-00696-x

26. Kumar, K., Geethakumari, G. "Detecting misinformation in online social networks using cognitive psychology. [Електронний ресурс]. – Режим доступу: https://link.springer.com/article/10.1186/s13673-014-0014-x

27. Ozbay, F., Alatas, B. [Електронний ресурс]. – Режим доступу: https://www. eejournal.ktu.lt/index.php/elt/article/view/23972

28. Про інформацію [Текст]: закон України від 02.10.1992 р. № 2658-XII / Верховна Рада України. // Відомості Верховної Ради. – К., 1992. – № 48. – С. 650.

29. Facebook [Електронний ресурс]. – Режим доступу: https://facebook.com

30. Instagram [Електронний ресурс]. – Режим доступу: https://instagram.com

31. Gephi [Електронний ресурс]. – Режим доступу: https://gephi.github.io

32. BASTIAN M., HEYMANN S., JACOMY M. "Gephi: An Open Source Software for Exploring and Manipulating Networks" // Proc. of the 3rd International ICWSM conference, in American Journal of Sociology. - 2009. - P. 361-362.

33. Web Search Engine Misinformation Notifier Extension (SEMiNExt): A Machine Learning Based Approach during COVID-19 Pandemic [Електронний ресурс]. – Режим доступу: www.mdpi.com/2227-9032/9/2/156

34. Бондаренко М.Ф., Білоус Н.В., Руткас А.Г. Дискретна математика. –Харків: Компанія СМІТ, 2004. – 480 с.

35. Towards the Detection of Fake News on Social Networks Contributing to the Improvement of Trust and Transparency in Recommendation Systems: Trends and Challenges [Електронний ресурс]. – Режим доступу: www.mdpi.com/2078-2489/13/3/128

36. A Novel Approach for Detection of Fake News on Social Media Using Metaheuristic Optimization Algorithms [Електронний ресурс]. – Режим доступу: www.eejournal.ktu.lt/index.php/elt/article/view/23972

37. Automated hybrid Deep Neural Network model for fake news identification and classification in social networks [Електронний ресурс]. – Режим доступу: pubs.iscience.in

38. Towards Fine-Grained Reasoning for Fake News Detection [Електронний ресурс]. – Режим доступу: ojs.aaai.org/index.php/AAAI/article/view/20517

39. Facebook API [Електронний ресурс]. – Режим доступу: https://developers.facebook.com/docs/graph-api/

40. C# [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/C_Sharp

41. C++ [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/C%2B%2B

42. Java [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Java

43. Python [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Python

44. Requests [Електронний ресурс]. – Режим доступу: https://pypi.org/project/requests/

45. Pandas [Електронний ресурс]. – Режим доступу: https://pandas.pydata.org

46. Numpy [Електронний ресурс]. – Режим доступу: https://numpy.org

47. Scikit-learn [Електронний ресурс]. – Режим доступу: https://scikit-learn.org/stable/

48. NLTK [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Natural_Language_Toolkit

49. Matplotlib [Електронний ресурс]. – Режим доступу: https://pypi.org/project/matplotlib/

50. HTTP Методи запиту [Електронний ресурс]. – Режим доступу: https://w3schoolsua.github.io/tags/ref_httpmethods.html

51. DataFrame [Електронний ресурс]. – Режим доступу: https://pandas.pydata.org/docs/reference/frame.html

52. JavaScript [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/JavaScript

53. What is an API: Definition, Types, Specifications, Documentation [Електронний ресурс]. – Режим доступу: https://www.altexsoft.com/blog/what-is-api-definition-types-specifications-documentation/

54. Document Object Model (DOM) [Електронний ресурс]. – Режим доступу: https://developer.mozilla.org/en-US/docs/Web/API/Document_Object_Model

55. <canvas> [Електронний ресурс]. – Режим доступу: https://developer.mozilla.org/en-US/docs/Web/HTML/Element/canvas

56. Getting started with WebGL [Електронний ресурс]. – Режим доступу: https://developer.mozilla.org/en-US/docs/Web/API/WebGL_API/Tutorial/Getting_started_with_WebGL

57. HTMLMediaElement [Електронний ресурс]. – Режим доступу: https://developer.mozilla.org/en-US/docs/Web/API/HTMLMediaElement

58. WebRTC API [Електронний ресурс]. – Режим доступу: https://developer.mozilla.org/en-US/docs/Web/API/WebRTC_API

59. Build awesome apps with Google’s knowledge of the real world [Електронний ресурс]. – Режим доступу: https://developers.google.com/maps

60. Texty.org.ua [Електронний ресурс]. – Режим доступу: https://texty.org.ua

61. StopFake.org [Електронний ресурс]. – Режим доступу: https://www.stopfake.org/uk/golovna/

62. Snopes.com [Електронний ресурс]. – Режим доступу: https://www.snopes.com

63. FactCheck.org [Електронний ресурс]. – Режим доступу: https://www.factcheck.org

64. Ноутбук Apple MacBook Air 13 M1 (MGN93) Silver [Електронний ресурс]. – Режим доступу: https://allo.ua/products/notebooks/apple-macbook-air-13-m1-mgn93-silver.html

65. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

ДОДАТКИ

Додаток А

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ
Голова секції "Управління інформаційною безпекою" кафедри МБІС
д.т.н., професор
_____ Юрій ЯРЕМЧУК
"20" _____ 2023 р.

ТЕХНІЧНЕ ЗАВДАННЯ

до магістерської кваліфікаційної роботи на тему:

Удосконалення методу виявлення автоматично генерованої дезінформації у соціальних мережах під час інформаційних конфліктів

08-72.МКР.005.00.121.ТЗ

Керівник магістерської кваліфікаційної роботи
к.т.н., доцент
_____ Грицак А.В.

Вінниця – 2023 р.

1. Найменування та область застосування

Програмний засіб для виявлення автоматично генерованої дезінформації в соціальній мережі Facebook.

Область застосування: дослідження поширення дезінформації в умовах інформаційної війни та в умовах миру або у особистих цілях.

2.Підстава для розробки

Розробка виконується на основі наказу ректора ВНТУ №203 від 18.09.2022 р.

3. Мета та призначення розробки

3.1 Мета розробки: розробка ефективного інструменту для виявлення автоматично генерованої дезінформації в соціальній мережі Facebook в умовах інформаційної війни.

3.2 Призначення: розроблений програмний засіб визначає генеровану дезінформацію в соціальній мережі.

4. Джерела розробки

4.1. Morris M., Ogan C. The Internet as Mass Medium / M. Morris, C. Ogan // Journal of Communication. – 1996. – Vol. 46, № 2. – P. 40 – 46.

4.2. Дані з офіційного сайту Facebook [Електронний ресурс]. – Режим доступу: https://developers.facebook.com/docs/

4.3. Курбан О.В. Стратегія та тактика інформаційної війни. – Київ: ВІКНУ, 2016. – С.85-90.

4.4. Бондаренко М.Ф., Білоус Н.В., Руткас А.Г. Дискретна математика. – Харків: Компанія СМІТ, 2004. – 480 с.

5. Вимоги до програми

5.1 Вимоги до функціональних характеристик:

5.1.1 Програмний додаток для оцінки дезінформації повинен мати набір елементів, що забезпечують обробку отриманої інформації з офіційної сторінки соціальної мережі Facebook.

5.1.2 Програмний засіб повинен мати зручний, легкий у використанні інтерфейс користувача;

5.1.3 Реалізація методу не повинна вимагати спеціальних ліцензійних програмних додатків;

5.1.4 Програмний засіб повинен виконувати процес автентифікації користувачів у системі.

5.2 Вимоги до надійності:

5.2.1 Програмний засіб повинен працювати без помилок, у випадку виникнення критичних ситуацій необхідно передбачити виведення відповідних повідомлень;

5.2.2 Бази даних повинні бути налаштовані на автоматичне створення резервних копій;

5.2.3 Програмний засіб повинен виконувати свої функції.

5.3 Вимоги до складу і параметрів технічних засобів:

– доступ до мережі інтернет;

– оперативна пам’ять – не менше 8192 Mb;

– середовище функціонування – операційна система MacOS;

– вимоги до техніки безпеки при роботі з програмою повинні відповідати існуючим вимогам та стандартам з техніки безпеки при користуванні комп’ютерною технікою.

6. Вимоги до програмної документації

6.1 Обов’язкова поетапна інструкція для майбутніх користувачів, наведена у пункті 3.3.

7. Вимоги до технічного захисту інформації

7.1 Необхідно забезпечити захист розроблюваного програмного засобу від несанкціонованого використання.

7.2 Неможливість отримання доступу незареєстрованих користувачів до інформаційних ресурсів.

8. Техніко-економічні показники

8.1 Цінність результатів використання даного проекту повинна перевищувати витрати на його реалізацію.

8.2 Має бути реалізований таким чином, щоб підходити для використання широкого загалу.

9. Стадії та етапи розробки

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Початок	Закінчення
1	Визначення напрямку магістерської роботи, формулювання теми	20.09.2023	24.09.2023
2	Аналіз предметної області обраної теми	25.09.2023	3.10.2023
3	Апробація отриманих результатів	4.10.2023	12.10.2023
4	Розробка алгоритму роботи	13.10.2023	25.10.2023
5	Написання магістерської роботи на основі розробленої теми	26.11.2023	16.11.2023
6	Розробка економічної частини	17.11.2023	23.11.2023
7	Передзахист магістерської кваліфікаційної роботи	24.11.2023	1.12.2023
8	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	2.12.2023	4.12.2023
9	Захист магістерської кваліфікаційної роботи	11.12.2023	15.12.2023

10. Порядок контролю та прийому

10.1 До приймання магістерської кваліфікаційної роботи надається:

– ПЗ до магістерської кваліфікаційної роботи;

– програмний додаток;

– презентація;

– відзив керівника роботи;

– відзив опонента

Технічне завдання до виконання прийняв _____ Ковінько М.О.

Додаток Б

Лістинг програми

```
import sys

import scipy

import numpy

import matplotlib

import pandas

import sklearn

from pandas import read_csv

from pandas import DataFrame

from sklearn.model_selection import train_test_split

from sklearn.linear_model import LogisticRegression

import mysql.connector

from tkinter import *

import matplotlib.pyplot as plt

from matplotlib.backends.backend_tkagg import FigureCanvasTkAgg

import requests

import openai

import tkinter as tk

from tkinter import messagebox, simpledialog, filedialog

url = "https://raw.githubusercontent.com/jbrownlee/Datasets/master/iris.csv"

names = ['sepal-length', 'sepal-width', 'petal-length', 'petal-width', 'class']

dataset = read_csv(url, names=names)

array = dataset.values

X = array[:,0:4]

y = array[:,4]

X_train, X_validation, Y_train, Y_validation = train_test_split(X, y, test_size=0.20, random_state=1)

model = LogisticRegression(solver='liblinear', multi_class='ovr')
```

```
model.fit(X_train, Y_train)

predictions = model.predict(X_validation)

class CommentAnalyzerApp:

def __init__(self, root):

self.root = root

self.root.title("Аналізатор коментарів Facebook")


self.username_label = tk.Label(root, text="Логін:")

self.username_label.pack()

self.username_entry = tk.Entry(root)

self.username_entry.pack()


self.password_label = tk.Label(root, text="Пароль:")

self.password_label.pack()

self.password_entry = tk.Entry(root, show='*')

self.password_entry.pack()


self.login_button = tk.Button(root, text="Увійти", command=self.authenticate)

self.login_button.pack()


self.api_token_label = None

self.api_token_entry = None

self.group_link_label = None

self.group_link_entry = None

self.analyze_button = None


def authenticate(self):

username = self.username_entry.get()

password = self.password_entry.get()
```

```
if True:
self.show_data_input_ui()

def show_data_input_ui(self):
self.username_label.pack_forget()
self.username_entry.pack_forget()
self.password_label.pack_forget()
self.password_entry.pack_forget()
self.login_button.pack_forget()
self.api_token_fb_label = tk.Label(self.root, text="API токен Facebook:")
self.api_token_fb_label.pack()
self.api_token_fb_entry = tk.Entry(self.root)
self.api_token_fb_entry.pack()

self.api_token_chatgpt_label = tk.Label(self.root, text="API токен OpenAI:")
self.api_token_chatgpt_label.pack()
self.api_token_chatgpt_entry = tk.Entry(self.root)
self.api_token_chatgpt_entry.pack()

self.group_link_label = tk.Label(self.root, text="Посилання на групу Facebook:")
self.group_link_label.pack()
self.group_link_entry = tk.Entry(self.root)
self.group_link_entry.pack()

self.analyze_button = tk.Button(self.root, text="Аналізувати", command=self.analyze_comments)
self.analyze_button.pack()

def analyze_comments(self):
facebook_token = self.api_token_fb_entry.get()
```

```
        chatgpt_token = self.api_token_chatgpt_entry.get()
        group_link = self.group_link_entry.get()

        pass

        def display_results(self, analyzed_comments):

        pass
        comments = fetch_facebook_comments(group_link, facebook_token)
        chatgpt_results = analyze_comments_with_chatgpt(comments, chatgpt_token)

        ml_results = analyze_comments_with_ml(comments, ml_model)

        combined_results = list(zip(comments, chatgpt_results, ml_results))
        save_results_to_database(combined_results, {'host': 'localhost', 'database': 'disinfo', 'user': 'max', 'password': 'e621netbootr34'})


def fetch_facebook_comments(group_link, facebook_token):
        return comments
        def analyze_comments_with_chatgpt(comments, chatgpt_token):
        openai.api_key = chatgpt_token
        analyzed_comments = []

        for comment in comments:
        try:
        response = openai.Completion.create(
        engine="davinci",
        prompt=f"Оцініть коментар на предмет дезінформації: '{comment}'",
```

```
            max_tokens=50
            )
            analyzed_comments.append((comment, response.choices[0].text.strip()))
            except Exception as e:
            analyzed_comments.append((comment, f"Error: {str(e)}"))

            return analyzed_comments
class DataProcessor:
    def __init__(self, filename):
        self.filename = filename
        self.data = []

    def read_file(self):
        try:
            with open(self.filename, 'r') as file:
                self.data = file.readlines()
        except FileNotFoundError:
            print(f"File {self.filename} not found.")
            sys.exit(1)

    def process_data(self):
        processed_data = []
        for line in self.data:
            processed_line = line.strip().upper()
            processed_data.append(processed_line)
        self.data = processed_data

    def write_data(self):
        try:
            with open(f"processed_{self.filename}", 'w') as file:
                for line in self.data:
                    file.write(line + '\n')
```

```
        except Exception as e:
            print(f"Error writing file: {str(e)}")

class NetworkManager:
    def fetch_data(self, url):
        try:
            response = requests.get(url)
            response.raise_for_status()
            return response.text
        except requests.exceptions.HTTPError as errh:
            print(f"Http Error: {errh}")
        except requests.exceptions.ConnectionError as errc:
            print(f"Error Connecting: {errc}")
        except requests.exceptions.Timeout as errt:
            print(f"Timeout Error: {errt}")
        except requests.exceptions.RequestException as err:
            print(f"Error: {err}")

def main():
    file_processor = DataProcessor("sample.txt")
    file_processor.read_file()
    file_processor.process_data()
    file_processor.write_data()

    net_manager = NetworkManager()
    url_data = net_manager.fetch_data("https://api.github.com")
    print(url_data)

    current_time = datetime.now()
    print(f"Current time: {current_time.strftime('%Y-%m-%d %H:%M:%S')}")
         def analyze_comments_with_ml(comments, ml_model):
         ml_results = []
         for comment in comments:
```

```
            prediction = ml_model.predict([comment])
            ml_results.append((comment, prediction[0]))
            return ml_results
            def save_results_to_database(analyzed_comments, connection_details):
            connection = mysql.connector.connect(**connection_details)
            cursor = connection.cursor()
class WebScraper:
    def __init__(self, urls):
        self.urls = urls
        self.data = Queue()

    def fetch_url(self, url):
        try:
            response = requests.get(url)
            if response.status_code == 200:
                return response.text
            else:
                return None
        except requests.RequestException as e:
            print(f"Error fetching {url}: {e}")
            return None
    def parse_data(self, raw_html):
        soup = BeautifulSoup(raw_html, 'html.parser')
        titles = soup.find_all('h2')
        for title in titles:
            self.data.put(title.text.strip())

    def scrape(self):
        threads = []
        for url in self.urls:
            thread = threading.Thread(target=self.worker, args=(url,))
            threads.append(thread)
```

```
            thread.start()

        for thread in threads:
            thread.join()
    def worker(self, url):
        raw_html = self.fetch_url(url)
        if raw_html:
            self.parse_data(raw_html)

class DatabaseManager:
    def __init__(self, db_name):
        self.conn = sqlite3.connect(db_name)
        self.cursor = self.conn.cursor()

    def create_table(self):
        self.cursor.execute('''CREATE TABLE IF NOT EXISTS data (title TEXT)''')

    def insert_data(self, data):
        self.cursor.execute("INSERT INTO data (title) VALUES (?)", (data,))
        self.conn.commit()

    def read_data(self):
        self.cursor.execute("SELECT * FROM data")
        return self.cursor.fetchall()

    def close(self):
        self.conn.close()
def main():
    urls = ["https://news.ycombinator.com/", "https://www.reddit.com/r/Python/"]
    scraper = WebScraper(urls)
    scraper.scrape()

    db_manager = DatabaseManager("scraper.db")
```

```
    db_manager.create_table()

    while not scraper.data.empty():
        title = scraper.data.get()
        db_manager.insert_data(title)

    print("Stored Titles:")
    for title in db_manager.read_data():
        print(title)
    db_manager.close()
query = "INSERT INTO comment_analysis (comment, chatgpt_result, ml_result) VALUES (%s, %s, %s)"
            for comment, chatgpt_result, ml_result in analyzed_comments:
            cursor.execute(query, (comment, chatgpt_result, ml_result))
            connection.commit()
            connection.close()
            def display_results(analyzed_comments):
            root = Tk()
            root.title("Результати аналізу коментарів")

            frame = Frame(root)
            frame.pack()
class FileManager:
    def __init__(self, base_path):
        self.base_path = base_path

    def read_file(self, file_path):
        try:
            with open(file_path, 'r') as file:
                return file.read()
        except IOError as e:
            print(f"Error reading file {file_path}: {e}")
```

```
            return None

    def write_file(self, file_path, data):
        try:
            with open(file_path, 'w') as file:
                file.write(data)
        except IOError as e:
            print(f"Error writing file {file_path}: {e}")

    def list_directory(self, dir_path):
        return [file for file in os.listdir(dir_path) if os.path.isfile(os.path.join(dir_path, file))]

class DataProcessor:
    def __init__(self, file_manager):
        self.file_manager = file_manager

    def process_data(self, file_name):
        file_path = os.path.join(self.file_manager.base_path, file_name)
        data = self.file_manager.read_file(file_path)
        if data:
            return self.analyze_data(data)
        return None

    def analyze_data(self, data):
        try:
            json_data = json.loads(data)
            return json_data
        except json.JSONDecodeError as e:
            print(f"Error decoding JSON data: {e}")
            return None

def recursive_search(path):
    if os.path.isfile(path):
```

```
        print(f"Found file: {path}")
    elif os.path.isdir(path):
        for item in os.listdir(path):
            recursive_search(os.path.join(path, item))

def main():
    base_path = "path/to/your/directory"
    file_manager = FileManager(base_path)
    data_processor = DataProcessor(file_manager)

    for file_name in file_manager.list_directory(base_path):
        print(f"Processing file: {file_name}")
        result = data_processor.process_data(file_name)
        if result:
            print(f"Processed data: {result}")

    recursive_search(base_path)
```

```
            df = DataFrame(analyzed_comments, columns=['Коментар', 'ШІ', 'Машинне навчання'])
            figure = plt.Figure(figsize=(6,5), dpi=100)
            ax = figure.add_subplot(111)
            bar = FigureCanvasTkAgg(figure, frame)
            bar.get_tk_widget().pack(side=LEFT, fill=BOTH)
            df.plot(kind='bar', legend=True, ax=ax)
            ax.set_title('Результати аналізу коментарів')

            if __name__ == "__main__":
            root = tk.Tk()
            app = CommentAnalyzerApp(root)
            root.mainloop()
```

Додаток В

Ілюстративний матеріал

Удосконалення методу виявлення автоматично генерованої дезінформації у соціальних мережах під час інформаційних конфліктів

Виконав: ст. гр. 2КІТС-22М Ковінько М.О.
Керівник: к.т.н., доцент каф. МБІС Грицак А.В.

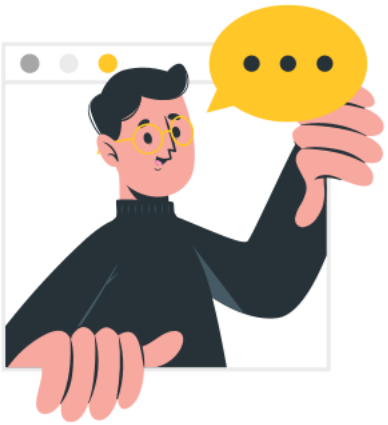
Актуальність роботи

01 **Інформаційна війна**
Зростаюча роль соціальних мереж як інструментів інформаційних війн.

02 **Використання нових технологій**
Активний розвиток штучного інтелекту в усіх сферах відкриває нові можливості для аналізу Big Data.

03 **Велика кількість дезінформації**
Сучасні технології на базі ШІ відкривають нові інструменти спотворення інформації.

04 **Проблема виявлення**
Складність виявлення підроблених відео, текстів, зображень - це проблема сьогодення



Об’єкт дослідження

Суспільні відносини, які формуються в процесі інформаційного впливу на людей під час інформаційних війн

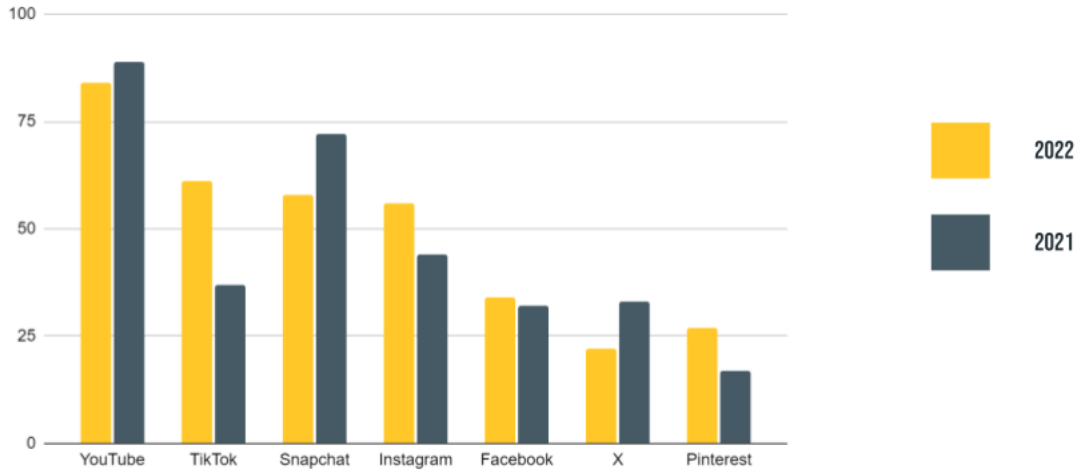
Суб’єкт дослідження

Визначені процеси в соціальних мережах у період інформаційних конфліктів

Вивчення психологічного механізму поширення інформації користувачами

Рис. 1.1 – Психологічний механізм поширення інформації користувачами

Дослідження інструментів розповсюдження дезінформації



Вивчення мультимовних особливостей

Основний акцент роботи було зосереджено на вивченні мультимовних особливостей в найпопулярніших соціальних мережах та аналізі їхньої ролі в процесі розповсюдження неправдивої інформації.

Багатокласова класифікація при виявленні автоматично створеної дезінформації

Запропонований підхід FND складається з трьох етапів:

- Попередня обробка даних
- Адаптація GWO та SSO для побудови моделі FND
- Використання моделі FND для тестування

Визначення процесів виявлення та аналізу дезінформації

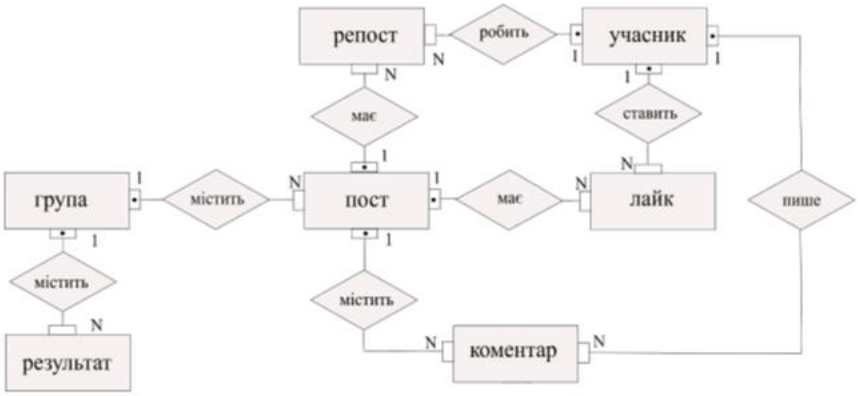


Рисунок 2.9 – ER-модель процесу виявлення та аналізу дезінформації в соціальних мережах

Методи покращення

Алгоритм дій покращеного методу:

- Аналізуємо активних учасників спільноти
- Досліджуємо тривалість, необхідну для поширення знань у суспільстві
- Визначення впливу свідомості індивіда
- Моделюємо процес поширення інформації в соціальній мережі
- обраховуємо оцінки ефективності поширення інформації

$$Z = (l \cdot (1 + \frac{\Delta L}{100})) \cdot (E \cdot (1 + \frac{\Delta E}{100})) \cdot (\frac{(N_c \cdot (1 + \frac{\Delta N_c}{100}) \cdot I \cdot \alpha) + (P_c \cdot (1 + \frac{\Delta P_c}{100}) \cdot I \cdot b)}{2})$$

175 000 000 000

Параметрів у моделі вивчення

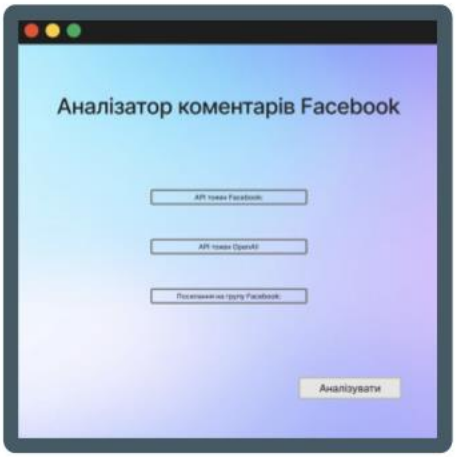
45 GB

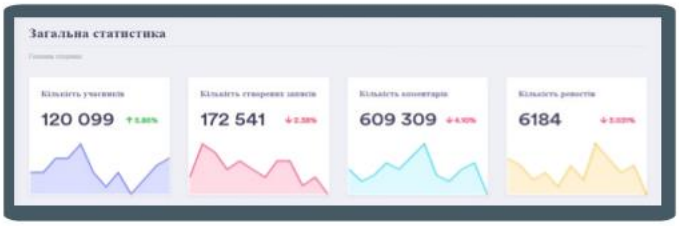
Навчальних даних

100 F/S

Файлів на секунду пропускна здатність

Демонстрація роботи застосунку





Результати проведених аналізів

	Коефіцієнт 1	Коефіцієнт 2	Коефіцієнт 3
Власна думка	0,06	0,38	0,38
Скарга	0,11	0,53	0,38
Спам	95,2	9,4	1,16

Висновки

Розроблено та вдосконалено алгоритм для аналізу дезінформації у соціальних мережах.

Цей процес включав аналіз існуючих методів та їх обмежень, а також створення нових підходів, що більш точно ідентифікують дезінформацію.

Особливий акцент був зроблений на використанні технологій штучного інтелекту та машинного навчання, що дозволяють розпізнавати складні взірці та моделі в поведінці користувачів та контенті.

Додаток Г

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА
НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Удосконалення методу виявлення автоматично генерованої дезінформації у соціальних мережах під час інформаційних конфліктів

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ: Кафедра менеджменту та безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 97 % Схожість 3 %

Аналіз звіту подібності (відмітити потрібне):

1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ (підпис) Коваль Н.П. (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ (підпис) Ковінько М.О. (прізвище, ініціали)

Керівник роботи _____ (підпис) Грицак А.В. (прізвище, ініціали)