Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему «**Розподілена аналітична система для виявлення і блокування фейків**»

Виконав: студент 2 курсу, групи КІ-21м
спеціальності 123 Комп'ютерна інженерія
Вальовський М. М.
Керівник к.т.н., проф., проф. каф. ОТ
Азарова А. О.
Опонент д.т.н. проф. каф.МБІС
Яремчук Ю. С.

Допущено до захисту
Завідувач кафедри ОТ
д.т.н., проф. Азаров О. Д.
«12» 06 2023 р.

Вінниця 2023

2

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки
Освітньо-кваліфікаційний рівень магістр
Спеціальність 123 Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри
обчислювальної техніки
проф., д.т.н. О. Д. Азаров
«20» 03 2023 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Вальовському Миколі Миколайовичу

1 Тема роботи **«Розподілена аналітична система для виявлення і блокування фейків»**, керівник роботи Азарова Анжеліка Олексіївна к.т.н., професор, затверджені наказом вищого навчального закладу від 20.03.2023 року № 68

2 Строк подання студентом роботи 9.06.2023 р.

3 Вихідні дані до роботи: методи засновані на класичних алгоритмах машинного навчання (SVM, Random Forest), методи, засновані на глибокому навчанні (LSTM, BERT, XLNet), мова програмування Python.

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): вступ, огляд існуючих рішень, фейки та методи їх виявлення, розроблення системи виявлення і блокування шейків, висновки.

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): електрична схема апаратної частини системи; список електронних компонентів; команди налаштування GSM-модуля; лістинг програми надсилання повідомлень; лістинг програми обробки зворотного зв'язку; лістинг програми контролера системи

6 Консультантів розділів роботи представлено в табл. 1.

3

Таблиця 1 — Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1, 2, 3	Азарова А. О., к.т.н., професор		
4	Нікіфорова Л.О., к.е.н., доцент		

7 Дата видачі завдання __.__._____ р.

8 Календарний план наведено в табл. 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів виконання магістерської роботи	Строк виконання етапів роботи	Примітка
1	Постановка мети та задач роботи	21.03.2021	
2	Огляд існуючих фейкових новин	22.03-02.04.2023	
3	Аналіз фейкового контенту в соціальних мережах	10.04-08.04.2023	
4	Дослідження методів виявлення та боротьби з шахрайством	09.04-29.04.2023	
5	Дослідження методів виявлення та боротьби із фейками	30.04-19.05.2023	
6	Розроблення комп'ютерної системи виявлення з фейків	20.05-25.05.2023	
7	Застосування методів попереднього навчання для створення системи виявлення фейків	26.05-.31.23	
8	Застосування методів глибокого навчання для розроблення системи боротьби з фейками	01.06-04.06.2023	
9	Розрахунок економічної частини роботи	05.06-06.06.2023	
10	Оформлення пояснювальної записки та ілюстративного матеріалу	08.06.2023	
11	Аналіз виконання роботи, висновки, додатки		
12	Перевірка якості виконання магістерської роботи та усунення недоліків		

Студент _____ Вальовський М. М.

Керівник роботи _____ Азарова А. О.

АНОТАЦІЯ

УДК 004.9

Вальовський М.М. Розподілена аналітична система для виявлення і блокування фейків. Магістерська кваліфікаційна робота зі спеціальності 123 — комп'ютерна інженерія, освітня програма — комп'ютерна інженерія. Вінниця: ВНТУ, 2023, 102 с.

Укр. мовою. Бібліогр.: 10 назв, рис. 12, табл. 8.

Дана магістерська кваліфікаційна робота присвячена створення розподіленої аналітичної системи для виявлення і блокування фейків шляхом застосування методів глибокого навчання.

Оскільки соціальні медіа мають величезний вплив на повсякденне життя суспільства і є найкращим засобом для висловлення своїх поглядів, то соціальні мережі також стали засобом для обміну подіями, що відбуваються навколо нас. Але деякі зловмисники використовують соціальні мережі з метою поширення фейків, щоб досягти своїх корисних цілей, особливо цей процес стає небезпечним в умовах війни росії проти України і намагань країни-агресорки створити проросійський медіапростір на теренах соцмереж та антиукраїнсько налаштовану аудиторію. Невиявлення вчасно вкидів російської пропаганди в мережу спричиняє їх подальшому поширенню та здійсненню негативного впливу на суспільство.

Отже, перевірка новин у соцмережах має не лише соціально зумовлені підстави, але й політично орієнтований вектор, саме тому розробленню такого інструментарію і присвячена дана магістерська кваліфікаційна робота.

Ключові слова: фейк, фейкова новина, соціальна мережа, Інтернет-простір, виявлення фейків, блокування фейків, розподілена аналітична система.

ANNOTATION

Valevskiy M.M.

Distributed analytical system for detecting and blocking fakes. Master's qualification route in the specialty 123 — computer engineering, educational program computer engineering. Vinnitsa, VTNU, 2023, 102 p.

In the Ukr. leng. Libr. name 10, figure 12, table 8.

This master's thesis is devoted to the creation of a distributed analytical system for detecting and blocking fakes by applying deep learning methods.

As social media has a huge impact on the daily life of the society and is the best medium to express one's views, social media has also become a medium to share the events happening around us. But some criminals use social networks to spread fakes to achieve their useful goals, especially this process becomes dangerous in the conditions of Russia's war against Ukraine and the aggressor country's efforts to create a pro-Russian media space on social networks and an anti-Ukrainian audience. Failure to detect Russian propaganda postings on the network in time causes their further spread and negative impact on society.

Therefore, the checking of news in social networks has not only socially determined grounds, but also a politically oriented vector, which is precisely why this master's thesis is devoted to the development of such tools.

Keywords: fake, fake news, social network, Internet space, fake detection, fake blocking, distributed analytical system.

ЗМІСТ

ВСТУП

В останні роки відбувся відтік користувачів з більш традиційних засобів масової інформації, таких як газети, радіо та телебачення, у нові формати: соціальні мережі, YouTube, підкасти, онлайн-журнали, новинні програми тощо. Однак такий підхід може спричинити небезпечні ситуації. Великий обсяг інформації, до якої люди отримують доступ, зазвичай не перевіряється і вважається достовірним. Саме в цей момент виникає термін «підроблені новини», які, власне, є фейковими.

Зловмисники використовують соціальні мережі з метою поширення фейків, щоб досягти своїх корисних цілей, особливо цей процес стає небезпечним в умовах війни росії проти України і намагань країни-агресорки створити проросійський медіапростір на теренах соцмереж та антиукраїнсько налаштовану аудиторію. Невиявлення вчасно вкидів російської пропаганди в мережу спричиняє їх подальшому поширенню та здійсненню негативного впливу на суспільство.

Отже, перевірка новин у соцмережах має не лише соціально зумовлені підстави, але й політично орієнтований вектор, саме тому питання розроблення засобів виявлення і блокування фейківє надзвичайно важливим, особливо в умовах ведення гібрідної війни росії проти України. Разом із тим, відповідний програмний інструментарій для створення інформаційної безпеки користувачів соціальних мереж та всього медіапростору не є розвиненим та потребує подальшого вивчення, що і зумовлює **актуальність** досліджень, проведених у даній магістерській кваліфікаційній роботі.

Мета роботи — покращення процесу виявлення і блокування фейків шляхом створення відповідної розподіленої аналітичної системи.

Задачі дослідження:

— провести огляд існуючих рішень;

— реалізувати методи, засновані на класичних алгоритмах машинного навчання (SVM, Random Forest);

— застосувати методи, засновані на глибокому навчанні;

— проаналізувати отримані результати і обрати найкращу модель для виявлення фейків;

— реалізувати створену розподілену аналітичну систему для виявлення та блокування фейків програмним кодом;

— здійснити тестування та коригування запропонованої комп'ютерної системи.

Наукова новизна отриманих результатів магістерської роботи полягає в удосконаленні підходу до пошуку та блокування фейків засобами методів машинного та глибокого навчання, що дозволяє підвищити вірогідність виявлення фейків та сворює можливість їх подальшого блокування.

Об'єкт дослідження — процес пошуку фейків у Інтернет-контенті з метою їх подальшого блокування.

Предмет дослідження — математичні моделі систем із самонавчанням для пошуку фейків.

Апробація. Результати магістерської роботи було апробовано на конференції ВНТУ (м. Вінниця, 2023).

Публікації. Результати дослідження було опубліковано в тезах доповіді на регіональній конференції (м. Вінниця, 2023).

1 ОГЛЯД ІСНУЮЧИХ ПІДХОДІВ ДО ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ РОЗПОВСЮДЖЕННЮ ФЕЙКОВОЇ ІНФОРМАЦІЇ

1.1 Основні поняття про фейки

Останні роки знаменуються активними дослідженнями у виявленні підроблених новин. Проте, більшість робіт у цій галузі зосереджено на ідеї вивчення та виявлення містифікацій у її основному каналі поширення: соціальних мережах. Прикладами цього є джерела [1] або [2], де ймовірність того, що цей пост буде хибним, вивчається з використанням його власних характеристик, таких як «лайки», «передплатники», «поділитися» тощо, за допомогою класичних методів машинного навчання (дерева класифікації, SVM, і т.д.). Застосовуючи такого роду наближення, найкращі результати отримані у [3], де виявляються click-bait новини, що досягають результатів з точністю 93% в інших роботах, таких як [4], використовуються апроксимації на основі графів для вивчення відносин між користувачами, які діляться новинами, та шляхів, якими слідує контент, для того щоб зупинити його розповсюдження та пом'якшити його потенційно обманний вплив. Хоча загальна тенденція полягає в тому, щоб проаналізувати способи розповсюдження містифікацій, вже почали з'являтися інші альтернативи, зосереджені на аналізі змісту новин. Так у статті [5], крім функцій користувача, які діляться новинами, використовується текст новини для розпізнавання підроблених новин, аналогічно статті [6], де новини вивчаються з метою виявлення хибних фактів у змісті. Що стосується використання сучасних алгоритмів глибокого навчання, компанія Fabula.ai використовує метод, який враховує як зміст новин, так і функції, вилучені із соціальних мереж, досягаючи результатів 93% [7]. У [8] порівнюється ефективність кількох алгоритмів (як класичного, так і глибокого навчання), за якого новини класифікуються за категоріями «істинний» та «підроблений», що дає результати з 95%. Нарешті, використовуючи лише зміст новин [9], пропонується метод на основі згорткової нейронної мережі для виявлення підроблених новин з використанням заголовків та зображення заголовка,

отримуючи результати з точністю 92%.

Найбільш споживаний продуктом людства є інформація, попит на неї завжди був високий. Особливо в сучасних умовах його роль і значення зростають більше, ніж раніше. Розвиток інформаційних технологій, особливо Інтернету, по-перше, прискорив підготовку та поширення інформації, по-друге, розширив можливості сприйняття до великого вікна. У цьому випадку правдивість чи хибність інформації, що поширюється, є другорядною. В результаті сутність інформації стає абстрактною, і вона починає використовуватися в різних цілях і інтересах. Іншими словами, неправдива та сфабрикована інформація негативно впливає на свідомість аудиторії та призводить до руйнування міжособистісних стосунків, норм і цінностей та звичаїв, прийнятих у суспільстві.

Наприклад, нині недостовірна інформація зустрічається не лише в соціальних мережах, а й у новинах серйозних ЗМІ, особливо інформаційних сайтів. Це призвело до того, що споживач контенту перестав аналізувати інформацію та сліпо сприйняв її. За останні роки ЗМІ та соціальні мережі перетворилися з каналу інформації на засіб комунікації. Діяльність блогерів у соціальних мережах стрімко набирає популярності та поступово привертає увагу з боку традиційних ЗМІ та електронних джерел інформації. Сьогодні найбільш обговорюваними є фото та відео хостинг матеріалів із соціальних мереж, блогів, форумів.

Сучасні засоби комунікації стають джерелом неперевіреної чи чутної інформації [3].

Новини, які містять неправдиву, вигадану або неправдиву інформацію, називають фейковими новинами. Брехня є еквівалентом фейку в сучасній англійській мові. Слово фейк може вживатися в двох значеннях: хитрість - підступ, підступ, обман, брехня, а також обман — жарт, веселощі. До нього відносяться брехня, фальсифікація, спотворення, обман, штучність, упередженість, плутанина, наклеп, шахрайство, хитрощі, плітки, тривога, пристрасть, заплутування, відволікання та інші [2]. У найширшому розумінні містифікація — це будь-яка дезінформація, яка поєднує плітки, вигадку,

пропаганду та таємниці, щоб зробити подію достовірною.

Це явище небезпечніше існуючої дезінформації. Брехня заснована на бажанні поширити неправдиву інформацію, а її новизна покликана завдати реальної шкоди. Можливість інформації допускає «помилкові» нескінченні можливості. Метою поширення неправдивої та оманливої інформації є навмисне заподіяння комусь або чомусь шкоди за допомогою неправдивої та недостовірної інформації, викликати сумніви та недовіру серед аудиторії, споживачів інформації та організацій, відомств, державних службовців, політиків, відомих осіб.

Цей вид репортажів є досить новим і з'явився нещодавно, а загалом до фальсифікації інформаційного простору належать такі діяння, як підробка документів, підробка та обман. Образи поширюються через ЗМІ та соціальні мережі з метою підвищення рівня невдоволення серед населення та організації різноманітних змов.

У 21 столітті завдяки стрімкому розвитку Інтернету «весь світ став віддаленим». Тепер ви можете за лічені секунди дізнатися про подію в одному куточку планети, яка сталася в іншій півкулі. Щодня в усьому світі відбувається незліченна кількість подій. Людина, за своєю природою, безпосередньо отримує сигнали з навколишнього середовища, особливо інформацію із ЗМІ чи соціальних мереж. У цьому сенсі більшість часу будь-яка новина, яка стає вірусною в соціальних мережах, вважається для неї правдою. Іноді вона навіть розуміє, що її ошукали, але не заперечує. Ось де найбільша проблема, інформація, у яку людина вірить, виявляється неправдивою. Лише одна неправдива інформація може змінити життя людини. Тому проблема неправдивої, недостовірної інформації стала однією з найважливіших тем не лише сучасної журналістики, а й усього суспільного життя [1]. Глобальні новини — активна форма ЗМІ, з якою може зіткнутися будь-який житель планети, незалежно від континенту та країни проживання. Наявність такої кількості запитань зумовлює необхідність визначення та дослідження теоретичного та практичного значення фейкової інформації як нового явища обговорюваної

інформації, а не просто виду інформації.

1.2 Особливості та типи фейкових новин

Останнім часом експерти з інформаційної безпеки, науковці та журналісти в сучасній академічній сфері серйозно підійшли до проблеми шахрайства.

Насправді інформаційне шахрайство також вважається новиною за своїм існуванням і змістом. Але вони містять інформацію, яка частково або повністю не перевірена, щоб привернути увагу людини. При поширенні такої інформації завжди враховується ступінь свободи громадськості, що посилює вплив шахрайства. Адже різниця фейкових новин здебільшого зумовлена їхньою перевагою над справжніми [6]. Звичайний читач, телеглядач, слухач чи користувач Інтернету не може відрізнити справжню інформацію від фейкової.

Щодо нещодавно перевіреної та офіційної інформації, то серед споживачів контенту склалася думка, що в суспільстві не до кінця розкривається правда, щось приховується. Звісно, винні ЗМІ та соціальні мережі, які так чи інакше відображають певні події чи замовчують певні факти, але люди самі були свідками описаної події або дізналися про неї з достовірних джерел. Навіть досвідчені журналісти, які працюють у ЗМІ, певний час не вірили в існування неправдивої, замовчуваної інформації. Але зараз існує думка, що суспільство саме чекає фейкових новин (раніше цю функцію виконували чутки та плітки), а поширювачами такої інформації є зловмисники або особи [3]. Через зростання Інтернету, особливо соціальних мереж, фейкові новини стали формою інформації, яка сприяє збільшенню аудиторії. Автори фейкових новин не аналізують те, що відбувається, а вигадують новини або використовують нестандартні методи в контексті реальних, але нудних подій. Найпопулярнішими методами поширення таких повідомлень є залякування, переконання, упереджене висвітлення та спотворення фактів, дезінформація. Фейкові новини зазвичай цікаві та спонукають до роздумів, тоді як фейкові новини починаються

з цікавих фактів. Цікаво, що 90% постійних читачів ігнорують стандартні повідомлення та звертають переконливу увагу на нестандартну інформацію [3].

Багато дослідників, які вивчають феномен «фейкових новин», намагалися класифікувати та диференціювати фейкові новини за типом. Навіть досвідчені журналісти, які працюють у ЗМІ, певний час не вірили в існування неправдивої, замовчуваної інформації. Але зараз склалося уявлення про те, що суспільство чекає фейкових новин (раніше цю функцію виконували чутки та плітки), а поширювачами такої інформації є злочинці або окремі особи [4].

Через зростання Інтернету, особливо соціальних мереж, фейкові новини стали формою інформації, яка допомагає збільшити аудиторію. Автори фейкових новин або вигадують новини без розслідування того, що відбувається, або використовують нестандартні методи в контексті реальних, але нудних подій. Найпопулярнішими методами поширення таких повідомлень є залякування, переконання, упереджене висвітлення та спотворення фактів, дезінформація. Фейкові новини зазвичай цікаві та спонукають до роздумів, а фейкові новини починаються з цікавих фактів. Цікаво, що 90% постійних читачів ігнорують стандартні повідомлення та звертають переконливу увагу на нестандартну інформацію [4].

Типи фейкових новин. Багато дослідників, які вивчають феномен «фейкових новин», намагалися класифікувати та диференціювати фейкові новини за типом. Згідно такої класифікації можна визначити визначити певні типи шейків, приведені нижче.

Випадково створена фейкова інформація. Її джерело — редакторська недбалість, редакційний поспіх, друк і некомпетентність. Її виникнення пояснюються поспіхом редакторів з публікацією матеріалу або нездатністю преси.

Містифікація, створена в межах інформаційної війни. Прикладом цього є українсько-російська війна, яка посилилася поширенням недостовірної інформації на телебаченні, в Інтернеті та соціальних мережах [7].

Неправдива інформація, створена комерційними структурами. Ця група

складається з розробки фальшивого наукового бренду. Бренди часто звертаються до «пошуку» ефективних слоганів, у результаті чого лінійка продуктів набуває популярності завдяки хибним інтерпретаціям завдяки своїм чудовим характеристикам. У цю групу також входять інструменти PR.

Містифікація, призначена для залучення читачів. Такі настрої включають фальшивий гумористичний матеріал зі злим умислом. З цією метою ЗМІ свідомо поширюють неправдиву інформацію та посилаються на свої надійні джерела.

Неправдива інформація, створена з невідомою метою. Ця категорія включає «жовті медіа», які включають неточну, оманливу або неправдиву інформацію, яка часто поширюється з розважальною метою. Остання категорія, яку слід згадати, належить К. Уордлу, директору First News Project. У своєму дослідженні Клер Оддл визначає основу для поширення фейкових новин за допомогою типів контенту, мотивації авторів і засоби, за допомогою яких такі повідомлення поширюються. За класифікацією дослідників виділяють сім категорій фейкових новин, а саме [8]:

— фейкові відео (пародії чи сатири);

— фейкові публікації з фейковими посиланнями, ця група включає непов’язані назви, матеріали, текст і зображення;

— неправильний зміст, до цієї групи відноситься неповна, спотворена або неправдива інформація, яка використовується з метою дискредитації фактів, подій або осіб;

— самозванець — дійсно надійні джерела інформації просто виглядають фальшивими;

— помилкові випадки, такі підробки відображають справжній вміст, доповнений неправдивою контекстною інформацією.

— неправдивий вміст, це класичні фейкові новини — відверто неправдива інформація, покликана ввести в оману чи нашкодити споживачеві;

— маніпулятивний контент — інформація, призначена для маніпулювання (справжня чи фейкова). Такий вміст можна підкріпити підробленими фотографіями чи відео.

Після поглибленого аналізу обсягу фейкових новин в українському інтернет-секторі можна вважати, що фейкові новини заслуговують на виділення за масштабом описаних подій. Тому рекомендується класифікувати фейкові новини на:

— локальні (що стосуються певної місцевості, міста, області чи області);
— регіональні (пов'язані з певною територією всередині країни);
— всеукраїнського (чи іншого національного масштабу);
— глобальний (для кількох країн).

За ступенем поділу фейкова інформація також поділяється на:

— політичне шахрайство;
— соціальні шахрайства;
— культурне шахрайство;
— спортивне шахрайство;
— економічні махінації;
— наукове шахрайство тощо.

Маніпулятивний контент. Інформація, призначена для маніпулювання (справжня чи фейкова). Такий вміст можна підкріпити підробленими фотографіями чи відео.

Після поглибленого аналізу обсягу фейкових новин в українському інтернет-секторі можна вважати, що фейкові новини заслуговують на виділення за масштабом описаних подій. Тому рекомендується класифікувати фейкові новини на:

— локальні (що стосуються певної місцевості, міста, області чи області);
— регіональні (пов'язані з певною територією всередині країни);
— всеукраїнського (чи іншого національного масштабу);
— глобальний (для кількох країн).

За ступенем поділу фейкова інформація також поділяється на:

— політичне шахрайство;
— соціальні шахрайства;

— культурне шахрайство;

— спортивне шахрайство;

— економічні махінації;

— наукове шахрайство тощо.

Будь-яке фейкове повідомлення зазвичай має неправильне відеозображення.

Профілі в соціальних мережах, створені від імені інших людей з використанням чужої фотографії.

Підроблені акаунти в Twitter (часто від імені знаменитості) [9].

Мало хто сумнівається в автентичності зображення чи відеокліпу, які вони бачать на власні очі, і лише деякі скористаються інструментами перевірки фактів (процес перевірки фактів, аудіовізуальні дані, точність, фактичність (включаючи спотворення, навмисне включення)) визначити істину та її першоджерело.знайти (якщо вказано).

Фальшиві фотографії, які циркулюють у соціальних мережах і на веб-сайтах, виглядають правдоподібно щодня. Найгірше, коли цю «брехню» використовують еліти, які лобіюють власні інтереси в усьому світі. Фейкові новини базуються не лише на зображеннях, для публікацій у соціальних мережах характерний мультимедійний принцип. Мультимедіа – це відображення різних форматів в одному медіаджерелі. У випадку медіаконкуренції важливо представити аудиторії весь спектр медіапродукту. Основну частину публікацій становить візуальна та текстова інформація. У такий спосіб вплив текстів забезпечує єдність і зв’язність твору, сильний комунікаційний ефект.

Ще один вид фейкових новин – це відео, змонтоване з раніше створених роликів або взагалі не відповідає тексту. Прикладом дезінформації в наш час є фейкові сторінки чи профілі в соціальних мережах.

Американський письменник Пол Хорнер роками заробляв на фейкових новинах. Пояснює, що люди просто поширюють інформацію і ніхто нічого не перевіряє. Те саме було із Трампом – він просто щось говорив, і люди йому вірили. [4]. За словами дослідників Крістофа Ейманса, Якоба Ферстера та

Джорджа Коха, для поширення брехні потрібно лише знайти правильну аудиторію.

Допомагають знайти таку спільноту рекламодавці та технологічні компанії, які надають зібрані дані про користувачів. Автори дослідження визнають, що дуже важко змінити нинішню систему, коли рекламодавці активно використовують дані, отримані з соціальних мереж. Хоча розпізнати фейкове повідомлення дуже важко, це реальна процедура. Достатньо базових інструментів фактчекінгу та перевірки фактів, викладених у матеріалі. З побічними ефектами відміни боротися важче.

Модель попиту та пропозиції інформації передбачає дві характеристики споживача:

— прагнення отримати достовірну інформацію, пізнати об'єктивну істину;
— особливі переваги при виборі теми [4].

Таким чином, читачі йдуть на компроміс: у них є стимул споживати точні інформаційні повідомлення, але їх задовольняють новини які їм більше до вподоби. Агрегатори фейкових новин знаходяться поза цією моделлю: головна мета публікації — швидко поширити неправдиву інформацію для великої аудиторії. Для цього процесу використовується дуже мало команд. Дослідження показали, що фейкові новини надходять від користувачів із меншою аудиторією до більшої кількості людей. На відміну від традиційних ЗМІ, основними каналами поширення фейкових новин є соцмережі та месенджери, де новини поширюються за допомогою «лайків». Сьогодні це не тільки показник соціального схвалення, що приваблює публіку, а й психологічний засіб, що створює певне ціннісно-емоційне відчуття об'єкта. Користувачі використовують як боти (нелюдські облікові записи), так і віруси для збору голосів, «лайків», завантаження та розповсюдження публікацій. У другому випадку активні (справжні) користувачі можуть не підозрювати, що їхній сайт використовувався для поширення якоїсь ідеї.

Популярність «альтернативних фактів» базується на сучасній реальності, коли соціальні мережі та онлайн-медіа дозволяють миттєво й необдумано

ділитися новинами без перевірки вмісту, що збільшує кількість людей, які потрапляють на брехню та пастки. Поява фейкових новин є природним явищем. Це головна загроза сучасного медіапростору: збільшення кількості фейкових новин і нездатність користувачів розпізнати правду, що може викликати паніку в суспільстві. На відміну від звичайних новин, головною метою фейкових новин є не інформування, а введення в оману шляхом навмисного поширення неправдивої інформації. Якщо поділити за метою створення фейкових новин, то їх можна поділити на: фейкові новини, створені для привернення уваги громадян до факту чи події; фейк створений для піару. Зараз експерти називають це «ерою постправди». Таке пояснення є відображенням сучасного цифрового суспільства, де почуття та емоції людей не такі цінні, як вони є насправді. Тепер вони дещо недоречні в контексті таких емоцій, як оцінка, афект, особисте підтвердження, ризик, факти та докази. У Сполучених Штатах, наприклад, важко стверджувати, що людина, яка не має кримінальних нахилів, може порушувати закон. У цьому випадку ця істина втрачає свою справжню цінність і навколо неї виникають різні фальшиві чутки. Останнім часом неправдиві, спотворені новини зустрічаються не лише в розважальних виданнях, Інтернеті чи соціальних мережах, а й у серйозних, офіційних та авторитетних ЗМІ. У чому причина цього? Правда полягає в тому, що за останні двадцять років основні ЗМІ та соціальні медіа змінили спосіб створення новин. В епоху до Інтернету редакції відправляли репортерів на місце подій, щоб отримати інформацію, і якщо з якихось причин вони не могли отримати інформацію з першого разу, інформацію отримували лише найнадійніші репортери. Лише в окремих випадках, коли можливості редакції були обмежені, вони користувалися послугами інформаційних агентств. Із появою Інтернет редактори почали відкривати спеціальні розділи, які моніторять сайти та соціальні мережі в пошуках цікавої та конкретної інформації для залучення великої аудиторії. Через брак досвіду підготовки новин, часові обмеження, неуважність і в тому фейкові новини проходять через фільтри навіть найавторитетніших і серйозних ЗМІ та соціальних мереж [4].

Як передбачав Е. Тоффлер у своїй книзі «Третя хвиля», дані стали

невичерпним ресурсом постіндустріального суспільства. Оскільки інформація стає все більш цінною, друковані та електронні ЗМІ (навіть найкращі) не можуть нести повний тягар інформації, доступної громадськості.

Тому ці ЗМІ мають поступитися місцем інтерактивним та мас-медіа, які можуть забезпечити максимальну різноманітність та реагувати на індивідуальні потреби в цивілізації «третьої хвилі».

Майже в кожній статті про сучасні тенденції та ЗМІ ви знайдете словосполучення «інформаційна ера» 21 століття. Теоретично Тоффлер зазначає, що постпродакшн-суспільство — це інформаціявона змінюється через вартість продукту, і відповідно якість також змінюється в залежності від попиту.

Міжнародні експерти виправдали своє занепокоєння тим, що джерела інформації все більше фальсифікуються і що людство вступає в нову еру – еру постправди. Згідно з Оксфордським словником, останній термін був визнаний терміном у 2016 році. На думку експертів із соціальних мереж, неминучий кінець інформаційного апокаліпсису відобразиться у стиранні межі між правдою та брехнею. Люди, які більшу частину дня проводять у соціальних мережах, більш байдужі до справжньої втоми і втрачають потребу розрізняти правду від брехні.

Наприклад, ви можете заробити конверсії (із цільовими налаштуваннями) у Facebook, Twitter і Google, використовуючи кліки, лайки та конверсії оголошень у твітах. Якість даних стала другорядною проблемою.

Основною причиною апокаліпсису є постійне використання дешевих і популярних інструментів, які руйнують нашу реальність. У цьому випадку кожен може змоделювати ситуацію, незалежно від того, відбулася вона насправді чи ні.

Таким чином, фейкові новини — це неправдиві або спотворені новини, призначені для введення в оману читачів і глядачів, незважаючи на можливість ідентифікації та перевірки фактів. Інформаційним продуктом також вважаються містифікації, тобто фейкові новини. Надаються лише реальні дані, частково або повністю видалені з їх структури. точки зору стилістики такі повідомлення нагадують звичайні повідомлення. Але, як ми вже згадували вище, вони відрізняються своєю частковою дійсністю або повним підтвердженням. За

останнє десятиліття вони розширили охоплення різноманітних інтернет-ресурсів і соціальних мереж. У результаті користувачі Інтернету щодня стикаються з мільйонами фальшивих повідомлень, розповсюджених спамом, вважають їх правдивими та ставлять їм «подобається».

Фейки зустрічаються в різних форматах: фальсифікація текстів, фото- та відеоматеріалів, іноді навіть штучні новинні матеріали, створені на замовлення відомих людей.

1.3 Вплив інформаційного шахрайства на формування медіапростору

Із кожним роком кількість інформаційних повідомлень, які розповсюджуються ЗМІ, зростає. Це дозволяють сучасні канали зв'язку. Як ми вже знаємо, це соціальні мережі, онлайн-ЗМІ та месенджери.

Зміни в концепціях основних засобів масової інформації протягом останніх десятиліть були здебільшого спричинені еволюцією онлайн-журналістики, яка ставить під сумнів два фундаментальні принципи журналістики: роль ЗМІ в сучасному світі та їхню об’єктивність у створенні контенту.

Розглядати таке явище необхідно, враховуючи взагалі поняття «новина», механізм відбору новинних матеріалів для публікації в нових соціальних мережах, рівень довіри аудиторії до інформації, що поширюється ЗМІ, як фейкові новини. Це поняття базується на знайомому терміні, але в даному випадку воно має інше негативне значення.

Глобалізація світу принесла в життя людей багато зручностей. З розвитком комп’ютерних технологій та їх широким використанням у повсякденному житті аудиторія не повинна намагатися блокувати ЗМІ, зосереджуючись лише на кількох джерелах, які повністю задовольняють її інформаційні потреби. Люди навчилися просіювати нескінченний потік інформації, який іноді може переповнювати їхній мозок, не залишаючи місця для роздумів. Редагування ідей є одним із викликів нашого покоління. Коли потік інформації безперервний, його важко зрозуміти, класифікувати, аналізувати дані та створювати власний

унікальний контент. Типовою реакцією на цей фактор є «раптове» розуміння інформації. Це працює для ланцюжка зображення-заголовок-текст.

Багато в чому становлення такого способу мислення пов'язане з розвитком концепції «нових соціальних медіа». На думку Л. П. Шестеркіної та І. Д. Борченко, це «середовище спілкування, засіб спілкування, в якому основним джерелом спілкування є Інтернет». Це поняття включає соціальні мережі, блоги, подкасти, інтернет-форуми, відеохостинг, комунікацію та інтерактивні платформи для обміну різноманітним контентом. Важливо розуміти, що концепція «соціальних медіа» заснована на взаємодії користувачів і медіаорганізацій. Розглянемо одну зі складових цього поняття: соціальні мережі [8]. Сучасний медіа-простір наповнений провокаційними заголовками, які привертають увагу користувачів. Як наслідок, новини, які повністю покладаються на «вау-ефект» і обрамляють факти (помилки чи хибні уявлення), привертають увагу та сприймаються як справжні новини. Але насправді ця інформація згубно впливає не лише на користувачів, які нею поширюються, а й на суспільство в цілому. Вигадування новинне має фактичної основи, вони публікуються та подаються як стандартний метод виробництва новин для створення легітимності. Фейкові новини важко виявити, оскільки вони подаються об’єктивно.

Нові соціальні медіа, які активно охоплюють традиційні медіа, є найкращим каналом комунікації за сучасного темпу технологічного розвитку та попиту аудиторії на актуальну інформацію. Все більше медіа залучаються до глобального процесу, і це завдання створення контенту для соціальних мереж і журналістів. Останній часто є номінальною платформою для розповсюдження інформації, але в цьому середовищі з’являються авторитетні чати та канали, які залучають більше людей, щоб фактично показувати та читати контент [9]. Наприклад, репортер Telegram має багато чатів, які зосереджені на потужному потоці інформації на основі «свідків» влади, які бажають залишитися анонімними. Таке середовище сприяє поширенню інформації та повідомлень на «офіційному», але не на змістовому рівні (наприклад, посилання на

некомпетентні чи неперевірені джерела). Існує чіткий розрив між формою і змістом. Не завжди варто покладатися на новини цього інформаційного простору, адже при виборі новин насамперед варто звернути увагу на такі особливості, як інформаційна конфліктність.

Основна проблема неправдивих публікацій у ЗМІ та соцмережах полягає в тому, що немає чіткого поділу на форму та зміст. Але є також певні ЗМІ, які поширюють інформацію, не перевіряючи отриману інформацію.

Екосистема фейкових новин базується на найглибших інстинктах людства. Фейкові новини – ефективна техніка комунікації, інструмент впливу на громадську думку. Автори дезінформації мають на меті принизити чи збентежити когось і отримати від нього вигоду (політичну чи економічну). Хоча фейкові новини швидко розвінчуються, вони маніпулюють психологією аудиторії, тим самим впливаючи на громадську думку та загрожуючи успільному порядку. Можна стверджувати, що шкідливі наслідки плагіату є більш шкідливими, ніж безпосередній вплив на аудиторію, коли вони читають це вперше. Дезінформація забруднює інформаційне поле та впливає на базову довіру аудиторії до новин. Однак відмови редакторів, офіційні відповіді в соціальних мережах або лідерів репортерської спільноти не завжди вітаються. Наприклад, репортер Telegram веде багато розмов, зосереджених на потужному потоці інформації, заснованому на державних «свідках», які бажають залишитися анонімними. Таке середовище сприяє поширенню інформації та повідомлень на «офіційному» рівні, але не на рівні змісту (наприклад, посилання на некваліфіковані чи неперевірені джерела). Існує чіткий розрив між формою та змістом. Не завжди варто покладатися на новини цього інформаційного простору, адже при виборі новин насамперед варто звернути увагу на такі особливості, як інформаційна конфліктність.

Основна проблема неправдивих публікацій у ЗМІ та соціальних мережах полягає в тому, що немає чіткого поділу між зовнішнім виглядом і змістом. Але також є деякі ЗМІ, які поширюють інформацію, не перевіряючи отриману інформацію.

Неправдива інформація поширюється від автора до споживача через складні веб-сайти, боти та соціальні мережі. ЗМІ та соціальні мережі.

Поширення фейкових новин і нездатність відрізнити їх від реальних фактів викликає занепокоєння навіть для урядів. Наприклад, соціальну мережу Facebook звинуватили в просуванні кандидатури Дональда Трампа шляхом поширення фейкових новин після виборчого скандалу в США. Насправді в Інтернеті є й інша інформація про двох кандидатів, але це лише додає цікавості. Крім того, фейкові новини від The New York Times, Washington Post, Huffington тощо. Він приваблює більше глядачів, ніж контент високоякісних видань, таких як було сказано вище, працює «вау-ефект». Фейкові дані ігнорують якісний контент. Зараз розробляються проекти, які допоможуть простим користувачам відрізнити достовірні спотворені факти від справжніх новин. Але випереджаючи наш час і технології, фейкові новини є більш небезпечними і незабаром будуть приховані. Лише матеріал, навмисно викинутий у публічний потік, загрожує громадському порядку. Такі повідомлення сприймаються активніше, а факти легше запам'ятовуються. Далі новина миттєво поширилася доступними сучасними каналами зв’язку. Але небезпека в тому, що багато профілів у соціальних мережах, спільнотах, Telegram-каналах розсилають такі повідомлення навмисно. Фейкові новини є серйозною проблемою сучасної інформаційної індустрії, і перевірити інформацію стає все важче. Публікація недостовірних новин може викликати паніку та страх серед аудиторії через свідоме поширення неправдивої інформації [5].

Отже, інформація є одним із основних понять сучасного медіапростору. Ці новини розповідають про мінливі фактори у світі. Підсумовуючи, слід зазначити, що «фейкова інформація» — це інформація, яка спотворює зміст новини у власній формі. За останні роки ЗМІ та соціальні мережі перетворилися з каналу інформації на засіб комунікації. Діяльність блогерів у соціальних мережах стрімко набирає популярності та поступово привертає увагу з боку традиційних ЗМІ та електронних джерел інформації. Нові соціальні медіа, які активно охоплюють традиційні медіа, є найкращим каналом комунікації за сучасного

темпу технологічного розвитку та попиту аудиторії на актуальну інформацію. Тому сучасні засоби комунікації стають джерелом неперевіреної інформації.

Фейкові новини стають все більш поширеним явищем у глобальному кліматі гострого попиту на новини — інформацію про певних людей, публічні події, які в ЗМІ подають як достовірну журналістську інформацію або частково замовчують.. Часто така інформація має гумористичний або сатиричний характер і створюється для розваги або для того, щоб привернути увагу до важливих соціальних проблем або щоб висміяти якесь незручне явище, поширене в конкретному суспільстві, щоб дезінформувати та дратувати громадськість. Зважаючи на це, ми вважаємо важливим досліджувати роль фейкових новин у сучасному житті.

1.4 Фейкова інформація як основна складова інфодемії

Термін «інфодемія» означає масове поширення інформації, що призводить до величезної кількості неправдивої інформації, суспільного «інформаційного перевантаження» і, як наслідок, зростання недовіри до ЗМІ. У більш вузькому значенні інфодемію також можна розуміти як панічний текст про державне прикриття, фальшиві поради неіснуючих лікарів, поширення чуток і теорії змови. Це є результатом однорідної надлишковості інформації [2].

Щоб відповісти на питання, чому під час криз і катастроф люди схильні поширювати неправдиві заяви та вірити їм, ми повинні звернутися до педагогічної та еволюційної психології, історії журналістики та досліджень фольклору. На даний час визначено наступні причини інфодемії.

Будь-якій спільноті властиво ділитися чутками. Це природний процес, який дозволяє зміцнити стосунки в соціальній групі. Згідно з експериментами, проведеними психологами Д. Саллівaном, М. Ландау і З. Ротшильдом з Канзаського університету, поширення чуток допомагає зменшити стрес і імітує контроль в умовах, коли людина не може вплинути на те, що відбувається [3].

Люди з політичною чи соціальною вагою, або навіть емоційно нестабільні люди схильні поширювати чутки [4]. Експеримент Ландау, Саллівана та Ротшильда показав, що люди з низьким почуттям контролю частіше поширюють чутки. Так, теорії змови пов’язані з пошуком винних у негативних подіях. Впевненість людей у достовірності інформації не грає ролі. Люди рівною мірою діляться інформацією, якій вірять, і інформацією, в якій сумніваються. Це продемонстрував тест у березні 2020 року рік: цільовій групі було поставлено завдання визначити, які повідомлення були представлені — правдиві чи хибні. Виходячи з цього, вони повинні були вирішити, ділитися чи не ділитися в соціальних мережах, і в результаті цільова група погоджувалася ділитися навіть повідомленнями, які вони визнали фейковими [5].

За словами дослідника Гарвардського університету Гері Аллена, кількість чуток і фейкових новин зростає відповідно до зростання нестабільності в державі [5]. У кількісних дослідженнях поширення чуток і фейкових новин, пов’язаних із катастрофами (наприклад, дослідження Келлі Грінхілл і Бена Оппенгейма з Університету Тафтса) і в повсякденному житті (дослідження соціологів С. Восуги, Д. Роя) і С. Арала) [5] фейкові новини. Не виявлено прямого зв'язку між схильністю до довіри та демографічними характеристиками. Таким чином, участь у поширенні фейкових новин не залежить від статі, віку чи освіти. Водночас, якщо прибрати фактор стресу, люди з вищою освітою легше знаходять фейкові новини та не погоджуються з їх розповсюдженням [5]. Проте слід зазначити, що населення старше 40 років часто відчуває труднощі в об’єктивній оцінці фактів щодо новин і достовірності.

Виходячи з цього, можна сказати, що інфодемія не виникає сама по собі. Фейкові новини пов’язані з емоційною стабільністю оповідача та слухача, а криза народжується в умовах відсутності балансу, що підтверджено експериментом. Крім того, емоційне збудження та відсутність почуття контролю надають достовірності неправдивим заявам. Якщо людина тривалий час відчуває неконтрольованість, він пояснить цю негативну ситуацію втручанням зовнішнього ворога. Таким чином, чим більш емоційно стабільна та

контрольована людина, тим менша ймовірність, що вона повірить на слово та поширить чутки. Звідси випливає, що інфодемічні історії поширюються під час соціальної кризи цілком природно.

Модель Брейнарда і Хантера стверджує, що поширення дезінформації схоже на те, як вона поширюється на інші групи через соціальні мережі («бульбашки»). «Бульбашка» відноситься до групи контактів або «агентів», які регулярно обмінюються інформацією. Тобто бульбашки — це системи обміну інформацією, створені самими людьми для захисту від чужої думки та нецікавої для них інформації. Таким чином, соціальні групи стають групами схожих людей і можуть бути реальними або віртуальними. Хоча віртуальні бульбашки можна виміряти за кількістю передплатників або лайків, фактичні бульбашки майже неможливо виміряти, тому важко сказати, наскільки вони великі. Кожна соціальна група унікальна, але людина може належати до кількох соціальних груп одночасно і таким чином може взаємодіяти з членами інших груп. Отже, кількість бульбашок у системі прагне до нескінченності [6].

Згідно з результатами дослідження Брейнарда і Хантера, 38,9% учасників кожної соціальної групи були схильні вірити неправдивій інформації. Загалом один контакт ділиться інформацією з 2,5% інших контактів, але, враховуючи кількість контактів, зрозуміло, що незважаючи на такий малий відсоток, інформація постійно циркулює в соціальних мережах. При цьому інформація може бути як неправдивою, так і правдивою одночасно. Існує певна класифікація інфодемічних наративів. Інфодемічні наративи — це ненадійні тексти, ключовий компонент і механізм виникнення інфодемій. Тексти можуть відрізнятися за довжиною та структурою, наприклад, розповідь або науковий текст, написаний експертом. Через це спільною рисою всіх наративів є те, що в першій чи другій формі люди підозрюють і виглядають дуже переконливо. Багатьом здається, що існує великий розрив між довірою до матеріалів і поширенням, але, це незавжди так. Наприклад, старенька жінка почула, що сезонні робітники (наймані) нападають на людей на вулицях, які через карантин залишилися без роботи та засобів до життя. Вона вірить у це, і в результаті традиційний наратив відомий

як наратив віри [9]. Тож жінка розповіла сусідам, щоб вони попередили інших про небезпеку.

Якщо розглядати наративи як екранізацію, стає зрозуміло, що їхня мета — об'єднати людей і опосередковано протистояти зовнішнім ситуаціям. Знайдіть ворога і посиліть «ядро контролю». У цьому сенсі наративи покликані забезпечити негайну допомогу «тут і зараз». Однак, якщо взяти до уваги довгострокові події, як каже П. Бутекен, стає зрозуміло, що вони продовжуватимуть впливати навіть після «цього часу і зараз». Наприклад, порада відмовитися від масок, оскільки «коронавірусу» не існує, призведе до сплеску випадків, який може тривати місяцями, а через півроку стати першопричиною рекордної кількості заражень.

Життєвий цикл інфодемічної історії складається з двох частин – видимої та невидимої. Видимою частиною історії є її публікація в соціальних мережах (соціальні групи, спільноти, особисті профілі тощо). Що невидиме, так це приватні повідомлення, тобто приватні повідомлення та пошта. Наприклад, деякі повідомлення навмисно поширюються в тематичних розмовах у шкільному класному батьківському чаті. Якщо історія там популярна, вона йде далі – до наступної бесіди, потім її показують у соцмережах і видно нам, дослідникам і людям поза межами бесіди батьків. Таким чином, ми можемо простежити лише видиму частину життєвого циклу історії — до цього ми не знаємо, куди і наскільки вона поширилася. Хоча «підводна» частина наративів може бути невидимою, «місце» важливіше для дослідників. Зрештою, саме орендна плата в публічному просторі підтверджує або ставить під сумнів змову викликає реакцію в суспільстві. Перехід від невидимої до видимої частини життєвого циклу історії — це перехід до активного поширення в інформаційному просторі, коли до процесу підключаються «великі» ЗМІ. Це в свою чергу призводить до змін у поведінці людей [6].

Після вивчення типології інфодемічних текстів, розробленої Першим проектом «Інтернет-ресурс виявлення фейкових новин», і результатів дослідження групи вчених, які опублікували результати.

Це можуть бути лікарські матеріали, в основному вони представлені у вигляді порад, засобів лікування та домашніх методів народної медицини, такі матеріали часто посилаються на «закриті джерела» або використовують імена лікарів, які такими не є.

Тексти попереджень — це тексти, які передвіщають, що має статися або вже почалося щось страшне, як правило, події, про які попереджають тексти, певною мірою пов'язані з суперечливою інформацією з різних інстанцій. Наприклад, знезараження водопровідної води, скидання дезінфікуючого порошку з гелікоптерів над містом, штрафи за жарти про коронавірус тощо. Таким матеріалам часто передують заяви органів влади, вирвані з контексту, таким чином неправильно інтерпретовані та спотворені. Плутані тексти про «катастрофи». Ці пости самі по собі не є фейковими новинами, але вони гіперболізують деякі факти або надають їм надмірно емоційного забарвлення. Такі матеріали завжди пишуться від першої особи (як правило, від очевидця або учасника події, який виступає першоджерелом). Ці тексти часто поширюються в соціальних мережах і з часом обростають відсутніми деталями, що робить їх підмножиною фейкових новин.

Ще є, так звані, консерваторські тексти. До них відносяться теорії змови. Наприклад, коронавірус — винахід Білла Гейтса, який хоче знищити людство в ім’я вакцини.

Один і той же матеріал може належати до кількох фальшивих повідомлень одночасно, поєднуючи свої властивості. Також із розвитком інфодемії неминуча поява якісно нових видів [6].

Слід зазначити, що різні типи текстів по-різному впливають на аудиторію. Так, наприклад, під час пандемії коронавірусу найпопулярнішими для поширення в соцмережах та суспільстві були не конспірологічні тексти, а псевдомедичні матеріали, а саме достовірні поради щодо профілактики захворювань. Найшвидше зростання інфодемічного шахрайства було зафіксовано в лютому-березні 2020 року, коли почала з’являтися інформація про коронавірус. Поява містифікацій посилюється тривожними новинами з Китаю та

Європи, які вже охоплені пандемією коронавірусу. Тоді в Італії почалася справжня медична криза, а російська влада заявляла, що в країні немає коронавірусу і більше його не буде. Це призвело до ситуації невизначеності, а як відомо, інфодемічні тексти народжуються в умовах втрати точного контролю [6].

Сучасна інфодемія – це епідемічна загроза для суспільства. Подібно до хвороби, вона також змінює поведінку тих, кого вона торкається в мережі та поза нею. Через це з'являється все більше наукових досліджень про те, як чутки та шахрайство «приваблюють» споживача та впливають на його поведінку. У 2001 році в журналі «Mathematical Sociology» була опублікована стаття, в якій описувалося поширення чуток за допомогою епідеміологічної моделі Е. Ноймера. Нарешті, він дійшов висновку, що деякі віруси мають надзвичайну «стійкість» і змінюються час від часу, але можуть зберігатися поколіннями у вигляді нових штамів вірусів. У той же час молодь (особливо студенти 18-25 років) більш схильна до чуток. Однак Ноймер вважає, що критичному мисленню заважає не вік, а відсутність належної практики. Як тільки молоді люди отримують нові чутки, вони, як правило, забувають їх, тому більшість чуток у цьому середовищі швидко зникають [6]. На думку Ноймера, головну роль в інфодемічному циклі відіграють скептики, які беруть на себе роль «імунітету», тобто намагаються придушити свій слух. Ноймер називає цей процес хімічним терміном «автокаталіз». У результаті під тиском конструктивних фактів із боку скептиків частина суспільства виділяється, відмовляючись від віри в чутки. Однак небажання змінити думку виникає за відсутності позитивних доказів складності чуток, тому чутки про далекі події зберігаються більше, ніж місцеві.

Тому необхідно розробити стратегії для запобігання або уповільнення поширення інфодемій і збільшення поширення надійної медичної інформації, щоб інфодемічні тексти швидше досягали громадськості.

Водночас заборона фейкових новин у ЗМІ та соцмережах, а також кримінальне покарання за поширення фейкових новин не є ефективними. Тому підхід до управління та підтримки інфодемії потребує перегляду. Як адекватні заходи пропонуються заходи, спрямовані на підвищення медіаграмотності

населення, тобто розвиток навичок критичного та аналітичного мислення для незалежного оцінювання новин.

Інфодемічний феномен супроводжує будь-яку соціальну кризу, коли люди змушені пристосовуватися до нових непередбачуваних умов, емоційної нестабільності та стресу. Інфодемія є механізмом такої адаптації. Коли людина тривалий час перебуває в стані стресу і отримує точні відповіді на свої запитання, вона намагається відновити контроль і знайти ці відповіді самостійно. Таким чином, інфодемія є безперервним і природним процесом у кризових ситуаціях, що виникає внаслідок потреби людей у безпеці та заповнення інформаційних прогалин [64]. В основі будь-якої інфодемії лежать інфодемічні історії — містифікації, чутки та інша дезінформація. Їх головною особливістю є неймовірна швидкість, з якою вони поширюються і приживаються в суспільстві. Основними каналами розповсюдження зазвичай є соціальні мережі (Facebook, Twitter, месенджери), де з'являється більшість цих історій.

Шахрайство в соціальних мережах поширилося через великі та менші ЗМІ. Більшість дослідників погоджуються, що поширення дезінформації подібне до поширення будь-якої інфекційної хвороби: факти поширюються через соціальні групи та заражають критичні думки чи еліти.

Дослідники розрізняють різні типи інфодемічних текстів за темою та ознакою. Текст може входити до кількох груп одночасно. Вони також відрізняються за розміром і структурою і нагадують анекдотичні чи псевдонаукові дослідження. Проте мета таких матеріалів завжди одна – об'єднати людей і повернути їм силу контролю над тим, що відбувається, боротися зі змінами та емоційною напругою. Сьогодні головне завдання користувача – отримати досвід поточної інфодемії, щоб підготуватися до наступної. Журналістська спільнота має бути готова до боротьби з дезінформацією шляхом виважених дій, своєчасної реакції та швидкого заповнення інформаційних прогалин достовірною інформацією.

Це можна зробити лише шляхом перевірки фактів, підвищення прозорості та співпраці між журналістами та урядовцями. Щоб подолати або уповільнити

інфодемію, нам потрібно спланувати та забезпечити доступ кожного сегменту суспільства до актуальної та точної інформації в будь-який час, особливо під час гострої кризи. Таким чином, повністю підтверджується припущення про те, що інфодемічна криза є природним процесом для суспільства і підвищення медіаграмотності всіх категорій громадян, а також ретельна перевірка інформації, що поширюється в ЗМІ, може запобігти поширенню фейків.

2 ФЕЙКИ ТА МЕТОДИ ЇХ ВИВЛЕННЯ

2.1 Поширеність фейкового контенту в соціальних мережах

Фейкові новини — одна з головних тем, які обговорюють професійні журналісти та медіадослідники. У редакціях ЗМІ, на наукових семінарах і конференціях точаться гострі дискусії про те, як відрізнити фейк від правди та напівправди та про необхідність позначати новини, які не перевірені фактами. Це може бути дуже осудливо. Нік Ньюман у своєму огляді журналістських трендів за 2017 рік каже, що фейкові новини підірвуть демократичний порядок у всьому світі. Генеральний директор Apple Тім Кук закликав уряди всіх країн розпочати кампанію проти фейкових новин, які "вбивають людський розум". Водночас є експерти, які вважають фейки фейками, а це роздута проблема. Так, наприклад, Том Узанузевскі, один із менеджерів інформаційного агентства Associated Press, заявив, що фейкові новини купує рекламодавець. Він фактично спонсорує та заохочує розповсюдження. Найкращою відповіддю на фейкові новини є створення якісного матеріалу на ту ж тему з доказами та спростуваннями.

Щоб зрозуміти, чи загрожує брехня професії журналіста, потрібно визначити саме поняття, що вже є складною проблемою. Проблема в тому, що термін підробка став широко використовуватися для позначення фотографій, оброблених у Photoshop, а іноді й відео, відредагованих у відеоредакторі, як підробки; сторінки в соціальних мережах, створені від імені інших (переважно відомих) людей; анекдотичні історії про так звані видовища та джерела розваг. Сьогодні фейком можна назвати будь-яку підробку. Але якщо говорити про інформацію та новини, то це цілеспрямоване використання сфабрикованих та підготовлених новин, основною метою яких є дискредитація будь-якої установи, організації чи особи. Найбільш точними синонімами фейкових новин є дезінформація або брехня. Творець фейкових новин має намір щось дискредитувати або когось збентежити.

Хоча інформаційні агентства невдовзі відмовляться від фейкових новин,

вони оперують психологією сприйняття фейкових новин як маніпуляції.

Незважаючи на фальсифікацію документів і сам досвід, фейкові новини є продуктом сучасної цивілізації з вірусними відео та публікаціями в соціальних мережах. Цикл цифрових комунікацій став ідеальним середовищем для поширення фейкових новин. Як феномен містифікації перетворився на найбільшу перевагу Facebook для Reuters, Bloomberg та інших інформаційних агентств. Пересічний користувач глобальних мереж не володіє медіаграмотністю і не може відрізнити фейкові новини від справжніх. За даними дослідницької компанії Pew Research, кожне четверте повідомлення, яким американці діляться в Інтернеті, не є надійним. У сучасному світі дезінформація схожа на вірус, оскільки вона швидко привертає увагу читачів і поширюється з великою швидкістю. Для тих, хто поширює фейкові новини, важливо, щоб якомога більше людей поглинули дезінформацію та поширили повідомлення на сайті новин. Для фейків важливіше наповнити свідомість читачів фейковим життям, яке спотворює реальність і ставить під сумнів існування об'єктивних фактів. Людина, яка наситилася брехнею, втрачає імунітет до брехні і стає байдужою до різниці між добром і злом. За його словами, вони брешуть і обманюють. Ніхто не має монополії на правду! Деяким користувачам мережі здається, що вони поширюють новини, їх фейковий характер, ірраціональне задоволення та хаос. Інші вважають, що, поширюючи неправду, вони кидають виклик консервативним поглядам і поглядам і руйнують будівлю. Є джерела, які називають себе сатиричними сайтами та займаються вигадкою та борються з політичними режимами, які їм не подобаються [6].

Але професійне співтовариство комунікаторів і самі соцмережі намагаються боротися з творцями та розповсюджувачами фейкових новин. Facebook почав бачити фейкові новини в дописах користувачів. Зокрема, Seattle Tribune News

Кажуть, що смартфон Дональда Трампа став причиною останніх витоків інформації з Білого дому в пресу. Такі звіти супроводжуються записом «суперечлива заява» у звіті Politifact і Snopes.com. Ці дві дослідницькі організації

перевіряють повідомлення після запитів користувачів. Поки неясно, чи буде більше звернень користувачів, чи дві перевірені організації будуть залучені до перевірки новинних повідомлень. Зрозуміло, що найефективнішим заходом боротьби з брехнею є прищеплення та продовження медіаграмотності серед мас. Користувачі соціальних медіа повинні бути щеплені проти вільних новин і відрізняти фейкові новини, які приносять користь комусь, від їх поширення. Тоді наше інформаційне суспільство повинно заразитися цією інфекцією і стати несприйнятливим до паразитів соціальних мереж [6].

Найпоширенішою дезінформацією в соціальних мережах є інформація про поширення COVID-19. Різноманітна інформація про новий вірус заполонила світові офіційні та неофіційні ЗМІ та інтернет-видання. Ці публікації знаходять широкий відгук у коментарях читачів, блогах користувачів Інтернету.

Об’єктом розслідування є стрімке поширення фейкових новин про COVID-19 у соцмережах, весь світ перебуває на карантині, а Інтернет став для всіх основним джерелом інформації, включно з чутками. .

Згідно з даними системи управління репутацією SCAN, розробленої в «Інтерфакс», в топ-5 «альтернативних» теорій походження вірусу входять неправдиві повідомлення про те, що COVID-19 винайшли американці (1727 публікацій); COVID-19 — розроблено китайськими вченими (випуск 1218); COVID-19 — Джерело слухань 5G (717 публікацій); COVID-19 прилетів із космосу (350 дописів). Ця та подібні публікації спрямовані на підвищення інтересу аудиторії до інформації, прямо чи опосередковано пов’язаної з пандемією. Під час розслідування фейкових новин, намір автора фейку («Я хочу привернути увагу аудиторії, тому я це говорю»).

«Найкращі, найпереконливіші історії про коронавірус, незалежно від їх достовірності») відповідають очікуванням заявників перед текстом («Я хочу отримати якомога більше інформації про COVID-19 і якомога швидше», «авторитетний медіа та Інтернет Я хочу отримувати інформацію з джерел» і «Я довіряю інформації, що поширюється в ЗМІ та Інтернеті»). Іншими словами, наміри фейкових авторів і наміри споживачів отримати інформацію створюють

фейкові новини. і сприяють його поширенню.

Зібрані та перевірені фейкові новини можна класифікувати відповідно до запитів на інформацію: хто є винуватцем або хто є джерелом інфекції? Яка статистика поширення коронавірусу? Хто зі знаменитостей інфікований? Як перевірити, чи здоровий ти? Яких дій шахраїв і лиходіїв чекати громадськості? Які заходи вживає влада проти інфекції?

Відповіді на ці запити про перенаправлення явно або відверто шахрайські. Іншими словами, фальсифікований матеріал — це відповідь автора на інформацію, яку запитує адресат із посиланням на авторитетні джерела. ЗМІ та Інтернет вирували повідомлення про те, що «перший китаєць заразився коронавірусом від бліх, які вільно продаються для споживання на ринках Уханя». Така новина цілком задовольнила потреби адресата, адже існує міф про те, що китайці їдять будь-яку тварину, особливо якщо вони не піклуються про дотримання санітарних норм. Пізніше ця інформація почала широко поширюватися світом, а публічне звернення дало відповідь на хвилююче його питання [6].

Однак очікується, що китайський адресат отримає інформацію про інше джерело інфекції, оскільки традиційна система харчування в Китаї не викликала таких інфекцій. У відповідь на ці очікування незабаром з’явилася новина про те, що вірус міг бути привезений до Уханя американськими військовими. Про це 12 березня 2021 року повідомив офіційний представник МЗС Китаю

У своєму Twitter китайський дипломат Чжао Ліцзян включив відео виступу директора Центру з контролю та профілактики захворювань США (CDC) Роберта Редфілда перед Конгресом. На відео Редфілд виявив, що деякі американці, які вважалися померлими від грипу, мали COVID-19 після смерті. Для тих, хто чекає підтвердження теорії змови, є фейкова новина про те, що COVID-19 штучно культивували в секретних бактеріологічних лабораторіях США: «Американські військові вірусологи експериментували з ранами і синтезували небезпечний вірус. Вони почали це, щоб виграти торгову війну з Китаєм».

Варіант теорії змови: «Пити з-під крана — не можна!» Фейкові новини показують, що водопровідну воду таємно отруюють, щоб запобігти зараженню.

У соцмережах і ЗМІ поширилася інформація про те, що з гелікоптерів будуть розпилювати дезінфекційні засоби. Крім того, різні версії цієї містифікації уточнюють деталі та подробиці: «Сьогодні об 11:00 і до 5:00 ранку вертольоти розпилюють дезінфекційним засобом, вікна та балкони мають бути закриті, 11:00 — не можна виходити після 10:00 ранку, повідомили у військовому відомстві. У цій версії сказано: «Ніхто не повинен бути на вулиці об 11:00 сьогодні ввечері. Двері та вікна мають бути закриті, оскільки 5 вертольотів розпилюють дезінфікуючий засіб, щоб знищити COVID-19. Обробити цю інформацію для всіх контактів» [8].

Як відомо, певна частина населення звикла більше вірити народним засобам. Таким заявникам надсилають шахрайські повідомлення, в яких пропонують різні традиційні методи профілактики та лікування інфекції. З перших днів у соціальних мережах почали рекомендувати для профілактики народні засоби: спирт, дитячу сечу, трави, часник. На початку березня в WhatsApp було поширене голосове повідомлення відомого лікаря Леоніда Рошаля. потім покликали чоловіка зі схожим голосом, що вранці потрібно їсти часник. Інформація надійшла, коли Рошаль розповідав про наслідки цих заходів на одній зі своїх лекцій для студентів-медиків.

Як бачимо, зміст фейкових новин дуже різний і являє собою багато запитів споживачів щодо інформації про коронавірус.

Організація фейкових розмов спрямована на тип адресата, який безсумнівно довіряє авторитетному джерелу в Інтернеті. Це жінки, які в першу чергу, турбуються про здоров'я своїх близьких; матері, які турбуються про освіту своїх дітей, та іншим категоріям, які використовують Інтернет як джерело для отримання найновішої інформації.

Залежно від бажаної рецептивно-інтерпретаційної активності при отриманні повідомлень можна виділити два типи приймачів фальшивого контенту: раціонально-логічне та емоційно-емоційне.

Ще одна група, яка поширює дезінформацію про вакцину проти COVID-19, — це противники вакцинації. Твердження кампанії ґрунтуються на псевдонаукових дослідженнях, без достатніх підстав для достовірних результатів, без епідеміологічних даних або для підтвердження перевірок своїх гіпотез, особливо з використанням Інтернету, особливо через швидке поширення інформації та теорій (немає епідеміологічних даних). У березні 2020 року сім технологічних гігантів Facebook, Google, LinkedIn, Microsoft, Reddit, Twitter і YouTube виступили зі спільною заявою щодо боротьби з дезінформацією про коронавірус [7].

У червні 2020 року Facebook посилив рекламну політику, заборонивши рекламу, яка обіцяє ліки від COVID-19. Через місяць генеральний директор Facebook Марк Цукерберг оголосив, що соцмережа надасть Всесвітній організації охорони здоров'я (ВООЗ) право безкоштовно публікувати інформацію про поширення COVID-19.

Facebook також почав публікувати підтверджену інформацію про коронавірус COVID-19 у верхній частині сторінки новин. Цей «дата-центр» наповнений інформацією Всесвітньої організації охорони здоров'я і Центри контролю за захворюваннями США. В Україні також повідомили МОЗ, оскільки раніше відомство уклало угоду з Facebook про проведення інформаційної кампанії.

Тим часом Facebook змінив спосіб взаємодії з користувачами, які стикаються з шахрайством. Компанія почала надсилати повідомлення тим, хто лайкав, коментував або ділився неправдивою інформацією, яку видаляли за порушення умов обслуговування соцмережі. Повідомлення: «Ми видалили вашу улюблену публікацію, оскільки вона містить неправдиву та потенційно небезпечну інформацію про COVID-19». Натиснувши на повідомлення, користувач перейде на спеціальну сторінку, де знайде пост із поясненням причини його видалення з Facebook.

У березні компанія оголосила, що всі публікації у Facebook та Instagram, які обговорюють безпеку вакцини від COVID-19, будуть позначатися. У тексті

зазначається, що всі вакцини проходять тривале тестування на безпеку та ефективність перед тим, як отримати схвалення спеціалізованими регуляторними органами в усьому світі.

Facebook запустив нову систему, за допомогою якої користувачі можуть сказати, що підтримують вакцину від COVID-19.

Теми, які Facebook блокував під час пандемії, включають протести проти самоізоляції; протести проти карантину; вакцини неефективні проти цільових захворювань; хвороби безпечніші за вакцини; Вакцини небезпечні, токсичні та аутичні.

Але не все ідеально в алгоритмах соціальних мереж. Зрештою, у цей період Facebook неодноразово звинувачували у фальсифікації достовірних записів і поширенні фейків.

Згідно з дослідженням правозахисної групи Awaas, 10 найпопулярніших сторінок Facebook, які поширюють фейки та теорії змови про здоров'я, отримують майже в чотири рази більше переглядів, ніж 10 найкращих сайтів із доказами. Зокрема, 2020 року 82 веб-сайти, які поширюють фейки про здоров'я, зібрали 3,8 мільярда переглядів сторінок. Серед них найбільш помітними є 42 сайти «гіперрозповсюдження». У них 28 мільйонів передплатників, і лише за квітень 2020 року вони зібрали 800 мільйонів переглядів [7].

Алгоритми Facebook для контролю дезінформації також ненавмисно заблокували інформацію, яка рекламує вакцинацію проти COVID-19, від медичних працівників, громад та релігійних груп. Алгоритми соціальних мереж невірно визначають таку рекламу як політичну. Інформація від Центрів контролю захворювань (CDC), Каліфорнійської медичної асоціації та інших організацій і груп була заблокована. Пізніше Facebook визнав, що помилково ідентифікував деякі оголошення.

Ще у квітні 2020 року Twitter оголосив, що оновив свою політику щодо COVID-19. Зміни передбачають видалення твітів із необґрунтованими звинуваченнями про «підбурювання людей до дій та спричинення масової паніки, соціальних заворушень або загальних заворушень».

Тим часом Twitter оголосив, що на початку стрічки новин Twitter з’явиться інформаційне вікно, яке надаватиме своїм глобальним користувачам достовірну інформацію про щеплення від коронавірусу в їхніх країнах [6].

Натиснувши на посилання у вікні, користувач перейде на нову сторінку в Twitter з інформацією про вакцину, яка відображається в Колекція твітів від відомих організацій — Всесвітньої організації охорони здоров'я та Центрів контролю та профілактики захворювань (CDC). У так званому твіттер-гіді є кілька розділів: наслідки щеплення, можливі побічні ефекти, поради для вагітних тощо.

Twitter також додав ще одну функцію для боротьби з поширенням дезінформації та фейкових новин, попереджаючи користувачів про підозрілий контент, якщо він їм подобається.

Раніше соцмережа видавала подібне попередження при спробі переписати пост із суперечливою інформацією. За даними компанії, це зменшило поширення неправдивої інформації на 29%.

Twitter запустив пілотну програму Birdwatch для боротьби з дезінформацією в соціальних мережах. Крім того, у квітні 2021 року Twitter оголосив, що співпрацює з Associated Press (AP) і Reuters для боротьби з дезінформацією шляхом просування автентичного контенту.

У березні 2020 року YouTube почав рекламувати офіційні повідомлення про COVID-19. На сайті з'явився спеціальний розділ з інформацією про коронавірус COVID-19. Він призначений для надання офіційних новин та іншої інформації про пандемію від відповідних органів. У травні того ж року YouTube видав політику щодо неправдивої медичної інформації про COVID-19. Зокрема, ці обмеження стосуються матеріалів, які містять неправдиву інформацію про COVID-19 з офіційних джерел (таких як Всесвітня організація охорони здоров’я та місцеві органи охорони здоров’я). Теми, охоплені новими правилами, включають лікування, профілактику, діагностику та передачу вірусу.

У разі розміщення такого вмісту Video Hosting повідомить вас електронною поштою про те, що його було видалено. Винесли друге

попередження, а після трьох попереджень пропуск заблокували.

У жовтні 2020 року YouTube оголосив, що блокуватиме контент, який пропагує теорії змови про вакцину проти COVID-19. Компанія заявила, що покладатиметься на інформацію про вакцину від ВООЗ, Центрів з контролю та профілактики захворювань та експертів місцевих органів охорони здоров'я з усього світу [6].

У квітні відеоплатформа YouTube анонсувала серію громадських послуг для вакцинації від COVID-19. У 16-секундному та 31-секундному відео [7] користувачам платформи рекомендується «повернутися до місця призначення» після ін'єкції. (відеопосилання) Проект реалізується Платформою у партнерстві з Лондонським трестом вакцин здоров'я та тропічної медицини. У серпні 2020 року Google заборонив видавцям використовувати свою рекламну платформу для показу реклами поруч із контентом, який пропагує теорії змови про COVID-19. Компанія також забороняє рекламу цих теорій.

Якщо сайт публікує матеріал, який порушує ці правила, Google заборонить сайту використовувати свою рекламну платформу.

У той час компанія Alphabet Google заборонила рекламу, що містила суперечливі заяви про профілактику захворювань і неперевірені ліки, включаючи кампанії проти вакцинації або заохочення користувачів відмовитися від лікування.

У січні 2021 року Google News запустила глобальний фонд для боротьби з дезінформацією про вакцину від COVID-19. На цю ініціативу було виділено до 3 мільйонів доларів США.

Фонд проводитиме програми, спрямовані на перевірку фактів і розширення аудиторії для груп, які постраждали від дезінформації. Заявки розглядатиме журі з 14 членів з академічного, медіа, медичного та некомерційного секторів, а також представників Всесвітньої організації охорони здоров'я.

Telegram досі залишається однією з соціальних мереж, яка не запровадила жодної політики боротьби з дезінформацією, як-от блокування фейкової інформації про COVID-19.

Засновник Telegram каже, що компанія не буде блокувати фейкові пости про коронавірус, оскільки цензура часто ускладнює боротьбу з непорозуміннями [6]. У січні 2020 року Facebook, Twitter і Google оголосили про спільні зусилля по боротьбі з дезінформацією про вакцину проти COVID-19. Компанії будуть співпрацювати з аудиторами та державними установами по всьому світу. «Всеосяжні стандарти звітності даних» будуть розроблені ними та урядовими установами Великобританії та Канади.

27 березня 2020 року Facebook оголосив про запуск програми фактчекінгу в Україні. Партнерами Facebook є VoxCheck і StopFake, незалежна міжнародна мережа фактчекінгу.

Науковий інтерес до зростаючого потоку фейкових новин зумовлений не лише їх поширенням у сучасних ЗМІ та Інтернеті, а й впливом цього контенту на свідомість масової аудиторії [6].

Адресоцентричний підхід до опису фейкових новин такий: «Що хоче знати керівник?», «Які є типи адрес фейкових новин?». Це включає дослідження для вирішення їхніх проблем. Аналіз у цій сфері дозволяє визначити основні теми фейкових новин. З точки зору змісту, контент фейкових новин різний і відображає різні потреби споживачів в інформації про коронавірус. Новинний контент, розрахований сприйняття емоційно чуттєвого типу адресата, зазвичай, містить статистичних і цифрових даних, у ньому представлені конкретні факти; при цьому міститься оцінна лексика, представлені імпліцитно заклики до дій; у пунктуаційному плані такий дискурсивний контент містить оклику або питальні конструкції.

2.2 Фейк як інструмент інформаційної війни росії проти України

Україна веде війну з рф. Ще до трагічних подій 24 лютого 2022 року рф розв’язала проти нашого народу абсолютно новий вид війни, так звану

«гібридну». Характеризується поєднанням кардинально різних видів і способів ведення війни, їх узгодженим використанням для досягнення спільних цілей [7].

Типовими компонентами гібридної війни є:

— використання звичайних методів ведення війни (звичайна військова техніка та відповідний вид військового персоналу тощо);

— участь у іррегулярних збройних формуваннях (повстанці, терористи, диверсанти тощо) з числа іноземців та громадян країни-агресора;

— активне використання засобів інформаційної та кібервійни [7].

Водночас окупант може законно вийти з конфлікту. Через ці складові експерти називають «гібридну війну» війною XXI століття.

Оскільки термін «гібридна війна» не існує в міжнародно-правових документах, ведення гібридної війни дозволяє юридично звинуватити атакуючу країну в агресії проти іншої країни. Крім того, в українській військовій доктрині такого поняття немає – документ є системою державних приписів щодо причин, характеру та перебігу сучасних військових конфліктів [7]. До початку широкомасштабного військового вторгнення в незалежну Україну багато країн світу визнавали агресію рф де-факто, але не де-юре. Така ситуація дала путінському режиму можливість «зберегти обличчя» та уникнути відповідальності.

Ветеран американського дипломатизму, аналітик і офіцер розвідки Джон Р. Девіс молодший, опубліковав у Military Review статтю, де стверджує, що гібридна війна є проблемою не лише деяких урядів. Це знаряддя злочинних структур, розповсюдження наркотиків, торгівлі зброєю, людьми та тактика людей, які займаються відмиванням грошей та здирництво.

Відомий український вчений і політичний діяч, академік В. Горбулін, характеризуючи інформаційну складову «гібридної війни», показав, що інформаційний фронт «гібридної війни» виявляється в кількох сферах:

— населення зони конфлікту;

— населення окупованої країни, територія якої не охоплена конфліктом;

— громадяни країни-агресора;

— міжнародне співтовариство.

У випадку України ми маємо справу не лише з ворожою пропагандою, а й з тим, що інформаційні експерти називають «війною смислів/понять». Для передачі цих значень використовується цілий набір обміну даними.

Ключовим структурним елементом цієї війни є симулякри — образи, яких не існує в реальності. Прикладами таких симулякрів є: «Фашисти в Києві», «Звірства в концтаборах», «Розіп'ятий хлопчик», «Застосування українцями забороненої зброї». Стратегічною метою використання цього симулякра є заміна об'єктивних уявлень цільової групи про природу конфлікту необхідним агресору «інформаційним фантомом» [7].

Зміна понять, смислів, впровадження симулякрів, метод гібридної війни призвели до розколу українського народу на антипутінські та пропутінські сили (егоїзм, прагнення до легкої наживи, грабіжництва тощо). Одним із доказів перемоги путінського режиму в інформаційній війні є рішення про закриття 300 журналістів газети «Крим».

Із зростанням популярності Інтернету, легкістю доступу, появою соціальних мереж із сотнями мільйонів людей майже у всіх країнах, створенням міжнародних груп інтересів Інтернет почав використовуватися як джерело пропаганди, психологічного впливу та навмисне поширення дезінформації.

Із метою поширення дезінформації в мережі Інтернет створені відповідні ресурси, які навмисно наповнюються інформацією, яка є достовірною та заслуговує довіри, але не може бути достовірною на 100%. Слід зазначити, що інші головні ЗМІ також були залучені до введення деяких людей в оману в деяких країнах, щоб виправдати певні дії. Візьмемо, наприклад, інцидент (провокацію) Глевіца — операцію «Банки» СС у гітлерівській Німеччині, яка призвела до вторгнення СС до Польщі 1 вересня 1939 року. Ця атака вважається початком Другої світової війни. Тоді сам Гітлер, лідер Німеччини, сказав: «Я наводжу пропагандистський аргумент для ведення війни. Неважливо, наскільки це розумно» [7].

Ця подія широко висвітлювалася в друкованих виданнях і на тодішньому

радіо (було телебачення, але воно було значно менш масовим і впливовим).

За визначенням радіо не підходить для трансляції такої інформації [7].

Сьогодні телебачення набуло небувалої сили, але шахрайство відбувається з двох причин: неуважність, неперевірена інформація, некомпетентність журналістів і визначальний вплив влади на інформаційну політику країни в електронних ЗМІ. Перший неправдивий репортаж російського телебачення про нібито розіп'ятого бійцями ЗСУ хлопчика був класичним, але:

— він міг з'явитися лише в пропагандистській кампанії російських ЗМІ;

— такий матеріал може з'явитися лише за розпорядженням вищого органу.

Інформаційна війна в основному спрямована проти молоді. Тому поширення дезінформації зосереджено в популярних серед молоді соціальних мережах.

Для цього була використана так звана «Фабрика інтернет-тролів» у Санкт-Петербурзі — молоді люди, які видавалися за справжніх інтернет-користувачів, поширювали провокаційні гнівні повідомлення. Мета цієї кампанії – надати психотерапію молодим людям в Україні та інших країнах росії, які в силу свого віку ще не мають стійкого характеру та життєвого досвіду та легко піддаються брехні. «Фабрика інтернет-тролів» працює за принципом «багаторазово повторена брехня стає правдою».

«Куратор» доручає працівникам заводу створити враження, що багато громадян України вважають владу «хунтою» і хочуть повалення правлячого режиму в країні. Завдання приблизно таке: «підготувати 20 повідомлень з оригінальністю близько 75%. Повідомлення мають бути актуальними, щоб викликати безумовний інтерес. Нічого страшного в путіні, сепаратистів не можна назвати терористами» [4].

Прикладом такої діяльності може бути дезінформація про знесення величезного пам'ятника Батьківщини-Мати на Печерській горі [8]. Для створення підробки використано фото 1980-х років.

В інформаційній війні треба розуміти, що брехати можуть усі сторони.

Однак між ворогуючими сторонами на південному сході України існували значні розбіжності.

На українському телебаченні, люди можуть висловити свою думку в багатьох розмовах. Тобто через мікрофон можна висловлювати будь-яку думку, тому що свобода слова в Україні є нормою. На російському телебаченні це неможливо: кожне слово піддається цензурі, а на вулиці підготовлені люди відповідають на запитання, перебуваючи «в прямій взаємодії» [8].

Серед репостів: мультфільм про людину, яка візуально схожа на путіна, події на Донбасі тощо, щоденна діяльність звичайних користувачів українських соцмереж. У росії ж їх судять не лише за створення контенту, а й за репост та схвалення. А висловлювати свою думку, співчуття і незгоду часто просто небезпечно. Давайте розглянемо інший приклад, де вище керівництво рф пізніше було викрито у брехні (російських військ у Криму немає). У лідерів Західної Європи, США, Канади, Австралії та інших країн інша справа. Лідери західних демократій мають справу з реальною політичною опозицією, журналістами та незалежними й, часто, дуже впливовими організаціями громадянського суспільства, які пильно стежать за роботою урядів, чиновників і бізнесменів. Як і на виборах, виборці відразу усувають і дискредитують фальшивих людей з політики.

Інша ситуація на росії: справжня опозиція розгромлена, незалежної преси немає, символом рф є думки їхніх ЗМІ та пропутінських інтернет-джерел [8].

Порівняння цих та інших ситуацій дає відповідь на питання, кому можна довіряти, а кому ні.

Важливо звернути увагу на джерело цієї інформації. Для уважного спостерігача це багато значить.

Тому можна зробити висновки про деякі ознаки фейкових джерел:

— такі ресурси не мають назви «Про нас», власник і співробітники, автор публікації прихований;

— ресурс маловідомий і не цитується традиційними ЗМІ;

— повідомлення з таких джерел не підтверджуються іншими джерелами,

наприклад перевіреною особою, для якої ця інформація мала б бути відома;

— дизайн сайту фейкового ресурсу яскравий, але дизайнеру явно бракує смаку та бажання замовити дизайн;

— підроблені ресурси часто мають гучні назви (наприклад, «Національний антикорупційний портал», статус «Національний» надається лише національним організаціям і лише спеціальним указом Президента України) тощо [8].

Враховуючи вище викладене, можемо констатувати, що незважаючи на медійні технології ворога, який веде щодо України гібридну війну, одним із елементів якої є використання інформаційного простору, існують методи та способи визначення неправдивості новини, що надає їй статусу інформаційного фейку.

2.3 Класифікаційні напрями фейкових новин

Фейкові новини завдають серйозної шкоди всім аспектам людського життя, і будь-яка галузь може стати мішенню для кампаній з дезінформації. Сучасні технології класифікації текстів на основі машинного навчання дозволяють прискорити та частково автоматизувати процес виявлення шахрайства [8].

Стрімке зростання використання соціальних мереж супроводжується неконтрольованою публікацією та поширенням цифрового контенту.

Небажані новини, чати, веб-сайти, соціальні мережі, опитування тощо на поширення захищеної інформації, наданої в неструктурованому вигляді (текст, зображення, відео тощо) Перевірка автентичності такого контенту може зайняти багато часу.

Аналіз великої кількості «інформаційних шахрайств» дозволив виділити такі їх види:

Залежно від співвідношення достовірної та недостовірної інформації. «Звіти» абсолютно неправдиві, наприклад: «Уряд Ісландії вирішив виплачувати

5000 євро кожному іммігранту, який одружується з місцевою дівчиною». Подібні «фейкові новини» часто використовують для повідомлення про «смерть» знаменитостей, тому відповідальним за «новини про смерть» став журналіст Томмазцо де Бенедетті, відомий у Європі як автор багатьох фейкових новин і провокацій. «Нобелівська лауреатка» Світлана Алексієвич (яка раніше оголосила про «смерть» Михайла Горбачова і Башара Асада).

«Неправдива інформація» включає неправдиві відомості на загальному тлі відібраної достовірної інформації.

«Новини» побудовані на реальних частинах, окремі частини спотворені. До них належать, наприклад, аудіо- та відеозаписи, відредаговані зображення, ними можуть маніпулювати шахраї; цитати, вирвані з контексту або в певній послідовності тощо.

Залежно від достовірності обставин часу та місця події:

— інформаційне шахрайство відображає минулі новини.

— новина про подію, яка насправді сталася в одному місці, подається як подія в іншому.

Залежно від складу осіб, згаданих у «новині» є перераховані нижче.

«Публікації» містять посилання на будь-які передбачувані публічні заяви, опубліковані від імені підробленого облікового запису. Наприклад, англомаовний сайт Euronews TV повідомив, що міністр закордонних справ росії лавров у своєму Twitter ухвалив резолюцію із закликом визнати справжній статус регіональної ради Венето (Італія), зняття санкцій з Криму та росії, надавши скріншот сайту лаврова. Як виявилося, інформація була фейковою, і лавров на той момент не мав облікового запису в Twitter. Водночас російськомовний сайт телеканалу не розміщував фейкових новин.

«Фальшивий» стосується другорядного учасника події як головної дійової особи.

«Репортажі» ґрунтуються на неперевірених свідченнях людей, які нібито були свідками подій.

Залежно від мети створення та розповсюдження можна згадати про

«Інформаційне шахрайство», створене та розповсюджене з метою обману споживача. Сучасне медіасередовище включає нішу інформаційних джерел, призначених для виробництва фейкових новин (The Onion Media Project в США, FOGNEWS, HOBOSTI, FIBSTER, NetLore та ін.).

Також є «новини», що створюються та поширюються з метою отримання політичних переваг: дискредитації політичних опонентів (у тому числі у виборчих кампаніях), спричинення вуличних заворушень, силової зміни влади тощо.

Що стосується «неправди», то вона спрямована на дискримінацію людей за ознаками статі, раси, національності, мови, походження, майнового стану та стану, місця проживання, релігійної приналежності, переконань, членства в громадських об'єднаннях та за іншими обставинами. Яскравим прикладом є «новини про інформаційні війни», які ведуться паралельно з реальними бойовими діями в гарячих точках нашої планети.

Є ще «інформаційні обмани», створені та розповсюджені для збільшення Інтернет-трафіку. З багатьма подібними прикладами «оновлює» користувачів соціальних мереж, а також Viber, WatsApp тощо. Месенджери регулярно зустрічаються, вірусно поширюючись у соціальних мережах, збільшуючи доходи мобільних операторів за рахунок зростання інтернет-трафіку [8]. Напередодні новорічних свят у соцмережах по всій країні з'явилися повідомлення: «Інформація з нашої інфекційної лікарні. 10 дітей, 2 людини померли в реанімації. Це через китайські мандарини з гілкою!».

«Повідомлення» створюються та розповсюджуються з метою обману споживачів грошей чи іншого майна. Цей тип репортажів часто передбачає збір коштів на лікування важкохворих дітей, що після розслідування виявляється недостовірним.

«Спуфи», призначені для пошкодження інформації, що зберігається на комп’ютері користувача. Наприклад, під «новиною» про смерть відомого актора Бреда Пітта нібито з американського телеканалу Fox News був прихований шкідливий комп’ютерний вірус, який активувався при натисканні на новину [9].

«Повідомлення» створюються та розповсюджуються, щоб привернути увагу до особи, компанії, проекту чи діяльності. Наприклад, наприкінці 2015 року був «знищений» імідж дівчини, відомої новим «кумиром» серед російських підлітків — інтернет-мемом Риною. 23 листопада 2015 року 16-річна Ріна лежала на залізничній колії за кілька метрів від зустрічного вантажного поїзда. Фотографію обезголовленої дівчини майже відразу опублікували в мережі. Після резонансу, викликаного смертю Ріни, в соцмережі «ВКонтакте» поповзли чутки, що дівчина була учасницею спільноти, відомої як суїцидальна гра з користувачами. Через такі «новини» зростав інтерес до «гри» з гнівними, трагічними результатами [9].

«Інформаційні шахрайства», створені та поширені з метою маніпулювання ринком або отримання певної переваги в господарській діяльності. Так, вранці 14 липня 2017 року на Нью-Йоркській фондовій біржі раптово подорожчали акції компанії Twitter. Ціна зросла на 8%, що збільшило капіталізацію майже на два мільярди доларів. Сплеск заголовків спричинили фейкові новини про купівлю Twitter за 31 мільярд доларів. Фейк був розміщений на фейковому сайті Bloomberg.market, дизайн якого скопійований зі справжнього сайту агентства Bloomberg. Видавець заявив, що покупцем може бути Google.

Залежно від рівня прийняття довіри є:

— «фейки», які мають явно штучний характер.

— «нововведення» здатні викликати підозри у «фейковості» та спонукати споживачів перевірити отриману інформацію.

— «інформаційні шахрайства» настільки переконливо сфальсифіковані, що майже не залишається сумнівів у їх «фальшивості».

У дослідженні Trend Micro під назвою «Машина новин Akeasama». Використання пропагандистами кібербулінгу та публічних маніпуляцій показало, що «інформаційне шахрайство може контролювати суспільну свідомість її споживачів і творців [9]. Ілон Маск, засновник SpaceX і Tesla, виступив на зустрічі Національної асоціації керуючих США у сфері штучного інтелекту закликав до превентивних дій у регулюванні: «Роботи можуть почати

війну, випускаючи фейкові новини та прес-релізи, підробляючи облікові записи електронної пошти та маніпулюючи даними [9]. Фейкові новини органічно вписуються в новітню концепцію правди. «Постправда», названа словом року 2016 Оксфордського словника, описує або посилається на ситуації, в яких бракує об’єктивних фактів.

Наведений вище аналіз можливих класифікацій фейкових новин чітко показує небезпеку, яку створює це технологічне явище в контексті розвитку сучасних інформаційних технологій. Буквально безконтрольне поширення фейкових новин здатне розпалити «інформаційний тероризм» величезної руйнівної сили. Усвідомлення негативних сторін цього явища спонукає громадські та державні інституції до пошуку механізмів фільтрації фальшивих квитанцій.

2.4 Методи виявлення та боротьби з інформаційним шахрайством

Широке поширення інформації через соціальні мережі та негативний вплив масової дезінформації на суспільство змусили дослідників звернутися до нових методів виявлення інформаційного шахрайства за допомогою технологій великих даних та машинного аналізу. Сучасні автоматизовані системи аналізу повідомлень зазвичай працюють за одним із трьох принципів.

Аналіз стилю тексту, а не змісту. Суть методу полягає в тому, що фальсифікатори, ті, хто бажає ввести читача в оману, використовують певні прийоми для просування потрібної ідеї та уникнення брехні. Воно проявляється в певних стилістичних особливостях, які не завжди помітні людині: показниками підробки можуть бути певна частота і послідовність використання протиставлень, замін і сполучників, навіть рівень слів і складність тексту.

Аналіз розподілу. Цей метод заснований на використанні спеціальних моделей, які імітують закономірності епідемій інфекційних захворювань і дозволяють передбачити, як буде поширюватися дезінформація.

Аналіз активності користувачів. Метод полягає в оцінці причетності читачів до створення та розповсюдження фейкових новин. Користувачі поділяються на дві групи: «злочинці», які наживаються на створенні та розповсюдженні підробок, і звичайні користувачі, які поширюють інформаційні підробки без певних намірів, як правило, одночасно зі злочинцями. Крім того, існує кілька служб, які використовують моделі машинного аналізу для виконання лінгвістичного аналізу імен, тексту, мультимедійного вмісту, метаданих та інших параметрів. Такі сервіси (FakeBox, FightHoax, TrulyMedia, SocialTruth та ін.) досягають при тестуванні точності понад 95% [6]. Тест гігантської мовної моделі, розроблений в Массачусетському технологічному інституті, який працює за принципом статистичного аналізу та порівняння з довідковими даними, розпізнає машинно-генеровані тексти з точністю 72% [9]. Такі системи в основному шукають ознаки певного стилю написання, сенсаційні заголовки тощо. пошук працює за принципом порівняння та співвіднесення з текстами вже зазначених баз даних. Крім того, такі служби можуть з часом шукати облікові записи або псевдоніми авторів, які перевірено шахраями. Завдяки роботі системи вхідний вміст класифікується як правдивий або неправдивий.

Статистичний аналіз може базуватися, наприклад, на загальній кількості слів, середній кількості букв у слові, частоті вживання різних слів, кількості слів, що не повторюються. Можливий пошук синтаксичних ознак: частоти вживання формальних слів, особливостей розділових знаків, появи різних частин мови.

Індикатором достовірності можуть бути тематичні елементи тексту: цитати, зовнішні посилання, характер зображень. Сам аналіз можна проводити за допомогою семантичних технологій і класифікаторів на основі алгоритмів глибокого навчання. Крім того, існує кілька служб, які використовують моделі машинного аналізу для виконання лінгвістичного аналізу імен, тексту, мультимедійного вмісту, метаданих та інших параметрів. Такі сервіси (FakeBox, FightHoax, TrulyMedia, SocialTruth та ін.) досягають при тестуванні точності понад 95%. Тест гігантської мовної моделі, розроблений в Массачусетському

технологічному інституті, який працює за принципом статистичного аналізу та порівняння з довідковими даними, розпізнає машинно-генеровані тексти з точністю 72%. Такі системи в основному шукають ознаки певного стилю написання, сенсаційні заголовки тощо. пошук працює за принципом порівняння та співвіднесення з текстами вже зазначених баз даних. Крім того, такі служби можуть з часом шукати облікові записи або псевдоніми авторів, які перевірено шахраями. Завдяки роботі системи вхідний вміст класифікується як правдивий або неправдивий.

Статистичний аналіз може базуватися, наприклад, на загальній кількості слів, середній кількості букв у слові, частоті вживання різних слів, кількості слів, що не повторюються. Можливий пошук синтаксичних ознак: частоти вживання формальних слів, особливостей розділових знаків, появи різних частин мови.

Індикатором достовірності можуть бути тематичні елементи тексту: цитати, зовнішні посилання, характер зображень. Сам аналіз можна проводити за допомогою семантичних технологій і класифікаторів на основі алгоритмів глибокого навчання. Крім того, існує кілька служб, які використовують моделі машинного аналізу для виконання лінгвістичного аналізу імен, тексту, мультимедійного вмісту, метаданих та інших параметрів. Такі сервіси (FakeBox, FightHoax, TrulyMedia, SocialTruth та ін.) досягають при тестуванні точності понад 95%. Тест гігантської мовної моделі, розроблений в Массачусетському технологічному інституті, який працює за принципом статистичного аналізу та порівняння з довідковими даними, розпізнає машинно-генеровані тексти з точністю 72%. Такі системи в основному шукають ознаки певного стилю написання, сенсаційні заголовки тощо. пошук працює за принципом порівняння та співвіднесення з текстами вже зазначених баз даних. Крім того, такі служби можуть з часом шукати облікові записи або псевдоніми авторів, які перевірено шахраями. Завдяки роботі системи вхідний вміст класифікується як правдивий або неправдивий.

Статистичний аналіз може базуватися, наприклад, на загальній кількості слів, середній кількості букв у слові, частоті вживання різних слів, кількості слів,

що не повторюються. Можливий пошук синтаксичних ознак: частоти вживання формальних слів, особливостей розділових знаків, появи різних частин мови.

Індикатором достовірності можуть бути тематичні елементи тексту: цитати, зовнішні посилання, характер зображень. Сам аналіз можна проводити за допомогою семантичних технологій і класифікаторів на основі алгоритмів глибокого навчання. Крім того, використовуються рекурентні нейронні мережі, які змінюються з часом і зберігають нову лексико-семантичну інформацію. Використовуються також ієрархічні системи уваги (HAN), які фіксують деякі особливості структури документа. Спочатку вони генерують зображення речень, а потім на основі цього відтворюють весь документ. Водночас різні слова та словосполучення використовують різний рівень інформативності фактів.

Усі ці методи можуть показати відмінні результати, але в більшості випадків кращу продуктивність (як у розпізнаванні хибних новин, так і в інших завданнях класифікації) демонструють логістична регресія, байєсовські моделі, і вони добре працюють на різних базах даних і з різною обробкою. схеми.

Навчені мережі, як правило, показують точніші результати на різноманітних наборах даних, тоді як HAN працюють краще на більших наборах даних. Як правило, CNN дозволяють отримати понад 90% точності, і цю продуктивність можна покращити, якщо використовувати схеми, які компенсують брак пам’яті в першому. Однією з таких схем є «довготривала пам'ять». Це різновид рекурентної нейронної мережі з циклами та блоками, які дозволяють запам’ятовувати значення протягом певного періоду часу, що дозволяє відстежувати зв’язок між початком і закінченням слова аналізованого тексту.

Існуючі пристрої, що використовують попередню інформацію та інформацію в реальному часі, підвищують точність класифікаторів незалежно від методу машинного аналізу. Публічні набори даних цього типу містять: Kaggle, базу даних випадків шахрайства, що містить кілька тисяч випадків; BuzzFeed — список сайтів, які оновлюють заблоковану інформацію; Kaidmml — кураторські колекції фейкових новин; LIAR — це тестовий набір даних, що

містить 12 800 підтверджених висловлювань різних спікерів на різні теми.

Отже, враховуючи вищесказане, можна зробити висновок, що інформаційні фальсифікації та спотворення інформації в новинах по-різному впливають на життя людей, і жодна зі сфер життя та економіки не застрахована від дезінформаційних кампаній. Хоча фейкові новини не є прямою мішенню для наклепу, вони завдають шкоди бізнесу в різних галузях. Зменшення довіри до уряду, науки та охорони здоров’я призводить до зниження продажів і цін на акції та негативних соціальних результатів.

3 РОЗРОБЛЕННЯ СИСТЕМИ ВИЯВЛЕННЯ І БЛОКУВАННЯ ФЕЙКІВ

3.1 Формування навчального набору даних та попереднє їх оброблення для розроблення системи виявлення і блокування фейків

Dataset. Для розроблення системи виявлення фейків використаємо Dataset — набір навчальних даних, що має п'ять функцій: ідентифікатор, заголовок, автор, текст та мітка. Ідентифікатор однозначно ідентифікує новинну статтю. Заголовок та автор — це відповідно заголовок та автор новинної статті. Текст є змістом статті. Мітка вказує чи є стаття надійною (реальною) чи ні:

$$f(x) = \begin{cases} 0, & \textit{якщо новина реальна,} \\ 1, & \textit{якщо новина фейкова.} \end{cases}$$

Набір навчальних даних містить 20800 статей новин.

Попереднє оброблення даних. Видалення стоп-слів. Стоп-слова — це список найпоширеніших слів у мові (у англійській: “a”, “an”, “be”, “the”, . . . , в українській: та, або, чи, так,…), які часто не мають сенсу, але не завжди. Іноді інформація, яку шукаємо, може бути включена до стоп-слів, які видалили. Наприклад, у більшості випадків мовного перекладу, де важливо, щоб залишали всі стоп-слова. Однак, в такому випадку, використовується семантика тексту для прийняття рішень, отже можна припустити, що видалення цих слів може дати кілька переваг:

— зменшення шуму, оскільки, видаляючи стоп слова, можемо зосередитись на більш значущому змісті;

— зменшує кількість функцій навчання моделей, оскільки скорочується величезна кількість тексту.

Видалення чисел. У контексті заголовка та тексту статті новин числа просто не несуть великої кількості інформації, тобто зміст тексту не зміниться при їх видаленні. Тому краще забрати всі числа, щоб мінімізувати шум у наших даних. Для цього використовуємо рядкову константу string.digits(«0123456789»)

у Python, а також методи з рядкового модуля Python str.maketrans(in outtab) (повертає таблицю перекладу, яка відображає кожен символ у рядку intab на символ у тій же позиції у рядку outtab. Потім ця таблиця передається у функцію str.translate) і відповідно str.translate(table[, deletechars]) (повертає копію рядка, до якого всі символи були переведені з використанням таблиці створеної методом maketrans при бажанні видаляючи всі символи, знайдені у рядку deletechars), для ефективного перетворення всіх цифр у порожній рядок.

Видалення іншомовних слів. Далі виникла потреба прибрати всі іншомовні слова, Для цього використовується пакет langid у Python для визначення мови всіх текстів та подальше видалення всіх рядків з іноземними символами.

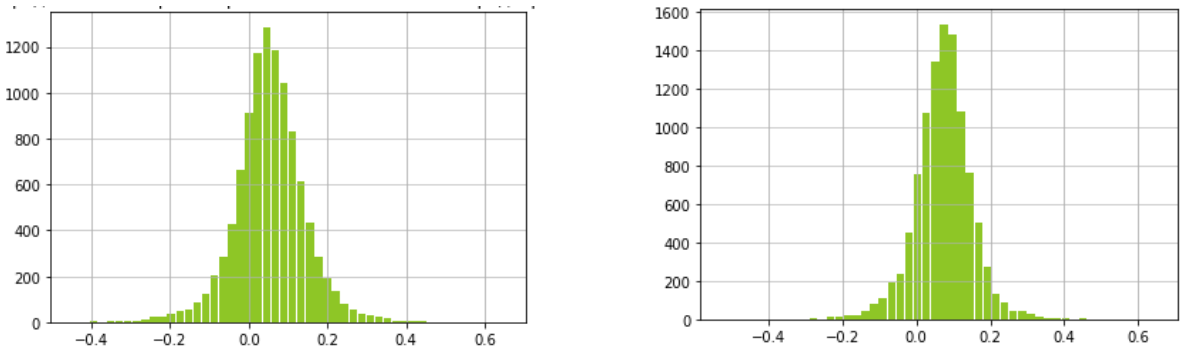
Видалення розділових знаків і спеціальних символів. Для цього використовуємо модуль string.punctuation (!"#$% &'()*+,-./:;<=>?@[\]^_'{|}~«») в Python, щоб знайти всі розділові знаки і видалити всі ці знаки з кожного слова в текстах, за винятком символів "#" та "@". Тому що ці символи використовуються для хештегів і згадок у Твіттері і часто додаються, щоб отримати більше результатів пошуку та актуальності, але часто відволікають від загального змісту самого новинного контенту Оскільки в завданні перш за все зацікавлені у словах і в їхньому основному контекстуальному значенні, що використовується в тексті, то припускаємо, що це непотрібні символи.

Щоб визначити хештеги і згадування, просто використовуються регулярні вирази, щоб видалити весь текст після хештег ("#") або символ ("@"), і припинити видалення тексту, коли досягнемо наступного пробілу. Також регулярні вирази використовуються для обробки тире ("—"), тому що воно використовується в різних лінгвістичних конструкціях, таких як об'єднання незалежних пропозицій, тому замінюємо його на прогалину. Після чого виникає ймовірність того, що в нашому тексті з'явилися дві або більше пробіли поспіль, їх також замінюємо на одиночну прогалину.

Після попереднього оброблення необхідно проаналізовати та здійснити розподіл даних (текст) у кількох різних аспектах. Отже, проаналізуємо дані,

побудувавши графік їхньої полярності настрою, найбільш популярних шинглів та біграм, а також розглянувши розподіл типів слів.

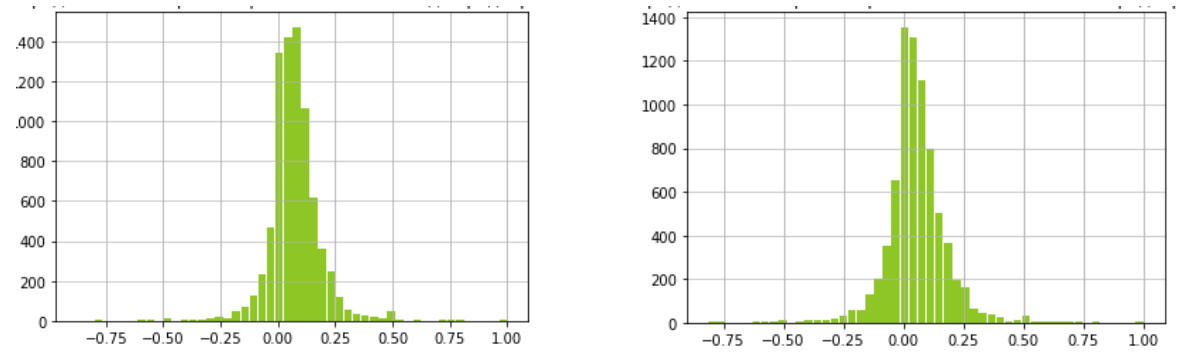
Графіки полярності настрою. Графіки полярності настрою показано для реальних та фейкових новин до і після обробки показано рис. 3.1 та рис. 3.2.



а) б)

Рисунок 3.1 — Полярність реальних новин:

а) до оброблення; б) після оброблення



а) б)

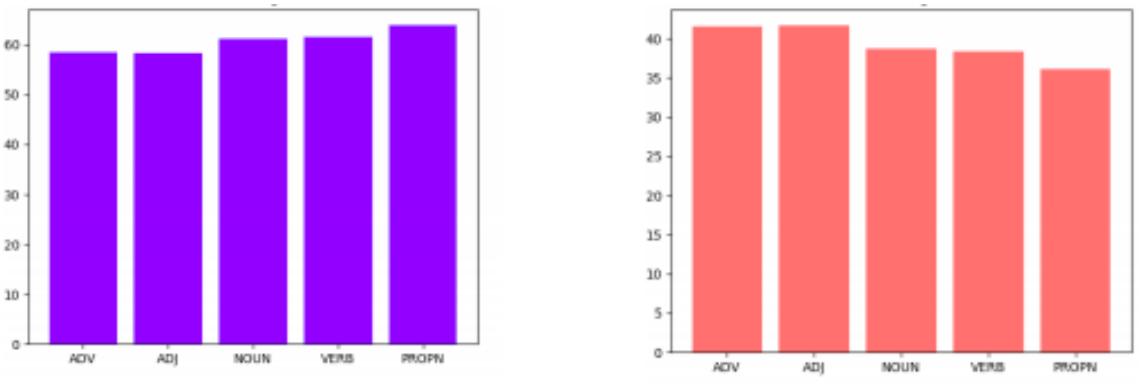
Рисунок 4.2 — Полярність фейкових новин:

а) до оброблення; б) після оброблення

Як до, так і після попереднього оброблення, розподіл полярності настрою підроблених новин та настрою реальних новин переважно однаково. Як для фейкових, так і для реальних новин можна помітити, що є трохи більше позитивних новин, ніж негативних. Також можна помітити, що, хоч і ненабагато, але підроблені новини більш полярні, ніж реальні новини. Існує більше викидів, і дані більш поширені.

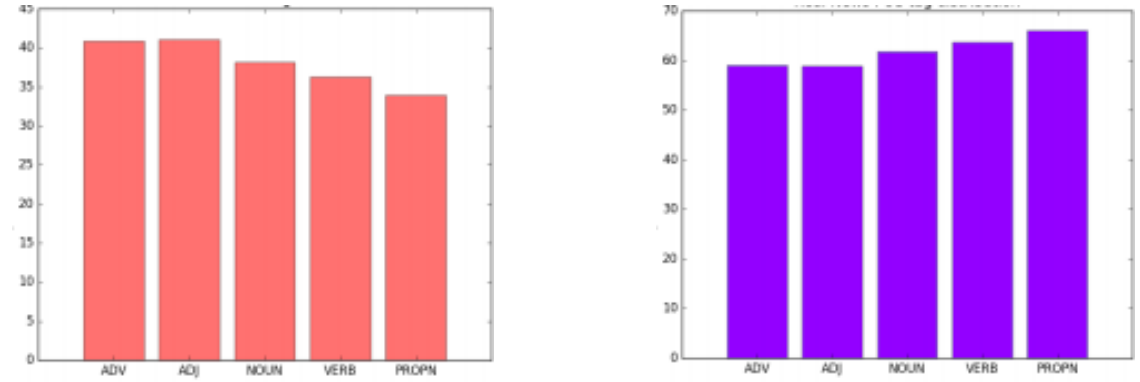
Графіки мовного розподілу. Розповсюдження POS-тегів показано для

реальних і фейкових новин до і після оброблення показано рис. 3.3 та рис. 3.4.



а) б)

Рисунок 3.3 — Розповсюдження POS-тегів до передоброблення новин:
а) реальних; б) фейкових



а) б)

Рисунок 3.4 — Розповсюдження POS-тегів після передоброблення новин:
а) реальних; б) фейкових

Як можна побачити різницю між реальними та підробленими новинами незначні. У підроблених новинах відсоток прислівників та прикметників вищий, ніж усі інші частини мови, тоді як відсоток займенників нижчий; однак у реальній новині є більш високий відсоток місць. Можливо, це вказує на те, що в підробці новини частіше використовують прислівники, щоб прикрашати свої пропозиції, на той час у реальних новинах використовують більше займенників, щоб акцентувати увагу на їх законності.

N-грама та біграма. Табл. 3.1 і 3.2, що наведено нижче, подають N-грами та біграми до та після попереднього оброблення.

Таблиця 3.1 — Unigram

Реальні новини		Фейкові новини	
До	Після	До	Після
the	nt	the	nt
to	trump	to	trump
of	людей	of	hillary
and	clinton	and	like
in	hillary	for	people
that	said	it	time
for	like	is	clinton
on	new	in	new

Таблиця 3.2 — Bigram

Реальні новини		Фейкові новини	
До	Після	До	Після
of the	mr trump	of the	hillary clinton
in the	united states	in the	donald trump
до the	new york	до the	united states
on the	mr trumps	on the	white horse
mr trump	white horse	and the	new york
at the	donald trump	that the	bill clinton
and the	mrs clinton	to be	clinton campaign
that the	said mr	for the	Clinton foundation
to be	york times	it is	secretary state
he said	islamic state	with the	nt know

Порівняння результату уніграми та біграми до та після попередньої

обробки показує, що наше рішення видалити стоп-слова є правильним вибором. Оскільки після видалення стоп-слів неважко помітити, що уніграма та біграма стають конкретнішими.

3.2 Застосування методів попереднього навчання

Розглянемо застосуванням різних моделей попереднього навчання.

Модель Word2Vec. Word2Vec — це набір моделей, які приймають на вхід текст і одержують у результаті роботи подання слів у векторному просторі на основі контексту. Ці моделі (ContinousBagOfWords і skipgram) є нейронною мережею, завданням якої є реконструкція контексту слів. Так, завдання CBOW — передбачення слова на основі контексту, а завдання skipgram — передбачити контекст на основі єдиного слова. Їхню архітектуру показано на рис. 3.5.

Розмір векторного простору IRn задається вручну, зазвичай n знаходиться в діапазоні від 100 до 400. Таким чином, цей метод має непереборну перевагу у вигляді невеликої розмірності векторів. На відміну, наприклад, від методів, які працюють зі словниками, де розмірність може досягати кількох тисяч.

Принцип роботи Word2Vec: максимізація косинусної близькості для векторного представлення слів, які з'являються у схожих контекстах, і, навпаки, її мінімізація для слів, які не зустрічаються у схожих контекстах. Після того, як векторні уявлення отримані, з'являється можливість, наприклад, знаходити близькість між двома словами, отримувати список найближчих елемен тів у векторному просторі тощо.

Крім того, можна отримувати вектор для цілих пропозицій, використовуючи, наприклад, усереднений вектор всіх слів в ньому.

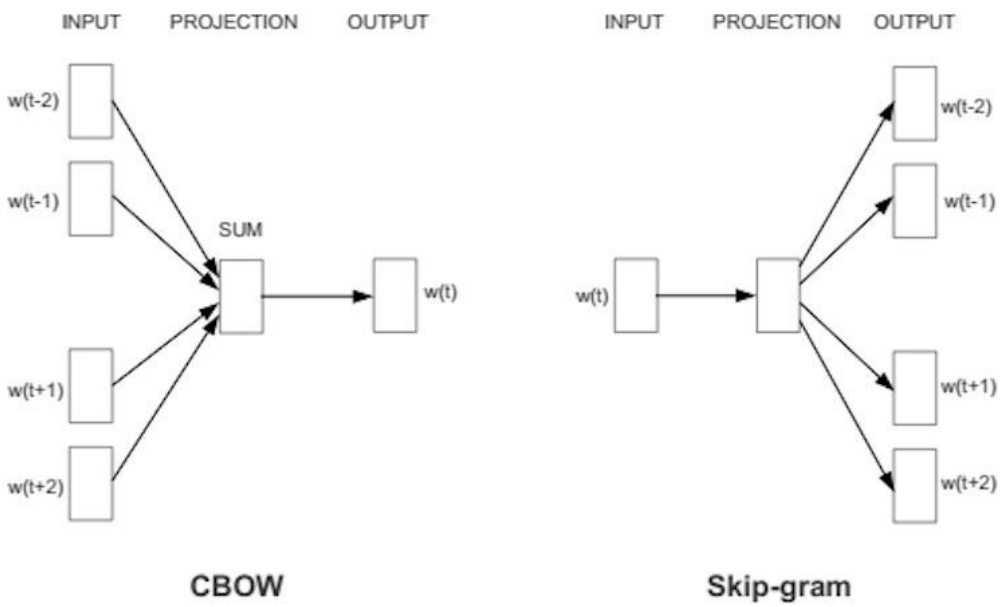


Рисунок 3.5 — CBOW та skip-gram архітектури

Для навчання моделі word2vec вибиралися новини, кількість слів у яких була більшою, за середню кількість слів за всіма новинами, вважаючи, що тексти, які коротшими, ніж середня довжина, мають менший контекст, і тому для якісного навчання варто від них відмовитися. За кількість функцій було обрано кількість за замовчуванням, яка дорівнює 100, оскільки хотілося проаналізувати невелику кількість функцій. Для цього проекту було обрано дуже простий та зрозумілий підхід. Отримавши вектор для кожної речення, тобто підсумовуючи всі векторні уявлення для кожного слова у реченні (тільки якщо слово належить моделі word2vec), далі сума ділиться на кількість слів у реченні, оскільки потрібно було переконатися, що розмір тексту не впливає на вкладення вектора, і, отже, було нормалізоване наше вкладення word2vec.

Модель TF-IDF Vectoraizer. Хоча TF-IDF є старою моделлю, її просто та ефективно використовувати на етапі попередньої підготовки. Обчислення TfidfVectorizer включає обчислення добутку частоти слова на зворотну частоту документа. Як випливає з цього терміна, TF-IDF обчислює значення кожного слова в документі за допомогою зворотної пропорції частоти слова в конкретному документі до відсотка документів.

Частота слова tf (t, d) обчислює скільки разів термін з’являється у

документі d. Словник побудований документом d. Частота слова має формулу:

$$tf(t, f) = \frac{n(t, d)}{V(d)},$$

де *n(t, d)* − входження слова *t* в документ *d*.

Для заданої колекції документів D, зворотна частота документів та idf (t, D) являє собою log кількості документів N поділений на df (t, D), кількість документів d в D, що містять термін t. У результаті звичайні слова D будуть мати низьку частоту, в той час як рідкісні слова будуть мати високу частоту. Таким чином, термін «частота» з великою ймовірністю відокремлюватиме підроблені новини, в яких часто зустрічаються менш поширені слова (навіть не граматичні) від реальних новин, які зазвичай складаються із загальних слів.

Таким чином, оцінка w(d, t) для слова збільшується з кількістю повторень, але буде нейтралізована, якщо слово зустрічається в занадто велику кількість документів:

$$w(t, d) = tf(t, d) \cdot idf(t, D).$$

Розглянемо систему фейків, яка складається з двох частин. Перша частина — передбачення, друга — схожість. Загальну структуру наведено на рис. 3.6.

Частина з передбаченням фейкових новин буде визначати, чи є новина фейком за допомогою Python-бібліотек pandas, word2vec та scikit-learn. Це бібліотеки для аналізу даних, оброблення тексту та машинного навчання.

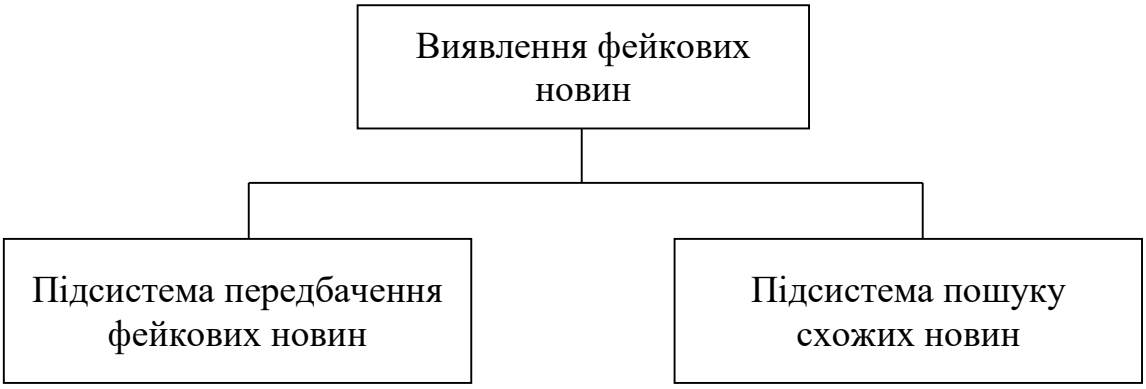


Рисунок 3.6 — Загальна структура програми розподільної системи

Модуль виявлення інформаційних атак виконує перевірку тексту за допомогою машинного навчання. Навчена модель зберігається і використовується при новій перевірці. Після відправлення тексту виконується його попередня обробка, а саме: текст очищується від стоп-слів та пунктуації, виконується стемінг та подальша токенізація. Після цього виконується векторизація – перетворення масиву слів у числове представлення на основі моделі «Word2Vec».

Схему роботи модуля представлено на рис. 3.7.

Word2Vec використовується для перетворення лінгвістичного контексту у числа. Вектори слів розташовані в просторі векторів таким чином, що слова із загальним контекстом розташовуються в цьому багатовимірному просторі в безпосередній близькості один від одного. Простіше кажучи, слова, близькі за значенням, будуть розміщені поруч. Ця модель фіксує синтаксичну та семантичну подібність між словами.

Друга підсистема буде шукати схожі новини з бази даних. Для реалізації доцільно використати sqlite, що допоможе в вирішенні поставленої задачі.

Для визначення схожих новин існує кілька підходів до кількісного визначення подібності, які мають однакову мету, але відрізняються підходом і математичним формулюванням.

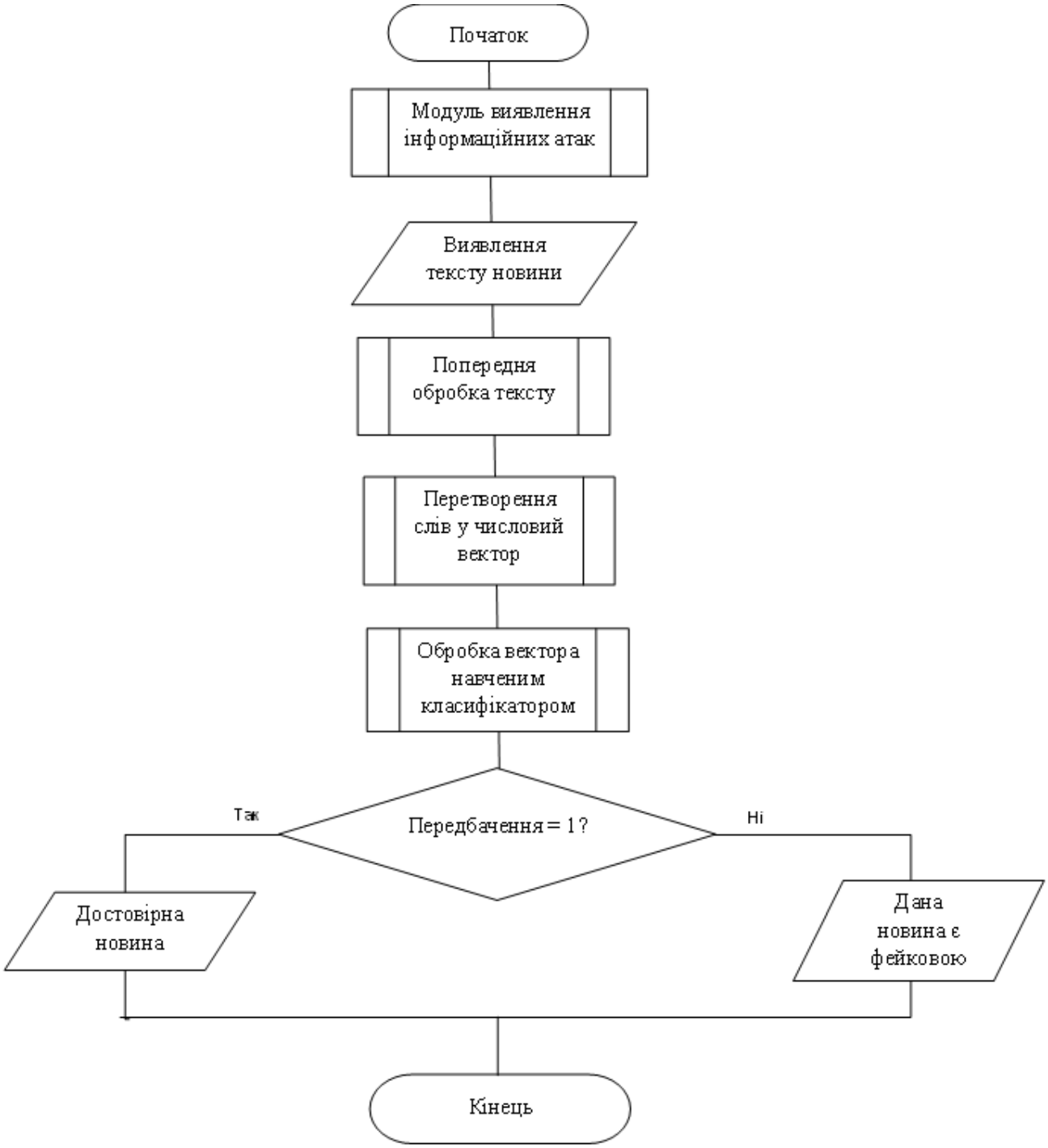


Рисунок 3.7 — Схема роботи модуля передбачення

Під час розробки підсистеми визначення схожих новин було обрано для використання косинусну подібність.

Косинусна подібність – це метод обчислення подібності двох векторів шляхом скалярного добутку та ділення його на величини кожного вектора [21].

Косинусна подібність є вигідною, тому що навіть якщо дві подібні новини розташовані далеко один від одного на евклідову відстань через розмір, вони все одно можуть мати менший кут між ними. Чим менший кут, тим вища схожість.

В базі даних будуть зберігатись id, час запису новини в БД, текст новини, ембеддінґ, label та ймовірність передбачення.

Алгоритм пошуку схожих новин наведено на рис. 3.8.

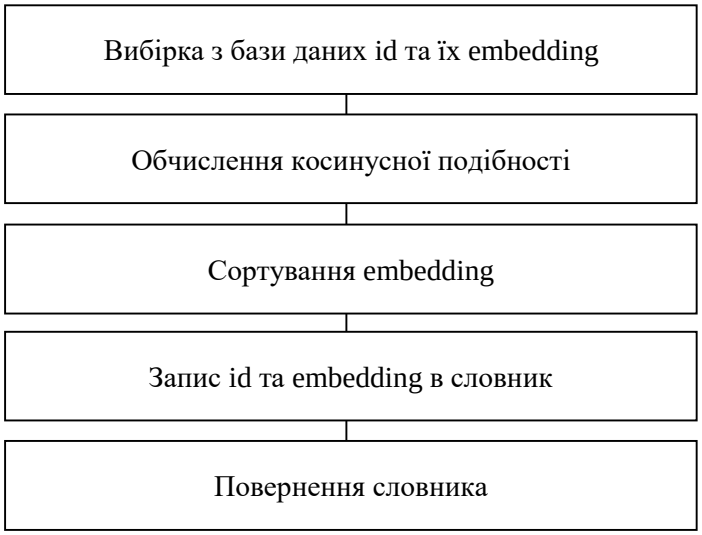


Рисунок 3.8 – Алгоритм пошуку схожих новин

Для розроблення системи виявлення фейкових новин доцільно використати технологію машинного навчання на основі алгоритму Word2Vec, який дозволяє векторизувати слова з корпусу новин, та класифікаційний алгоритм на основі нейронної мережі. Крім того, для зберігання та організації даних про новини була використана база даних SQLite. Засіб було розроблено з урахуванням принципу простоти використання та інтеграції з іншими інструментами для аналізу та обробки текстів.

Для навчання моделі було використано новини українською та московитською, як фейкові так і правдиві. Всі новини були взяті з офіційних сайтів та статей та на цій основі створено датасет який потім потрібно експортувати в базу даних.

Щоб знайти схожі новини потрібно перетворити у вектори і в кінці за допомогою косинусної подібності вже можна обчислити схожість, що визначається в межах від 0 до 1. Крім того, за допомогою подібності векторів можна визначати, наскільки новина схожа за змістом з відомими фейковими новинами, що може допомогти віднести її до цієї категорії і попередити користувачів про можливу недостовірність інформації.

3.3 Структура програмного засобу для реалізації системи виявлення та блокування фейків

Базові файли для відображення структури програмного засобу, що реалізує систему, що розробляється, подано на рис. 3.9.

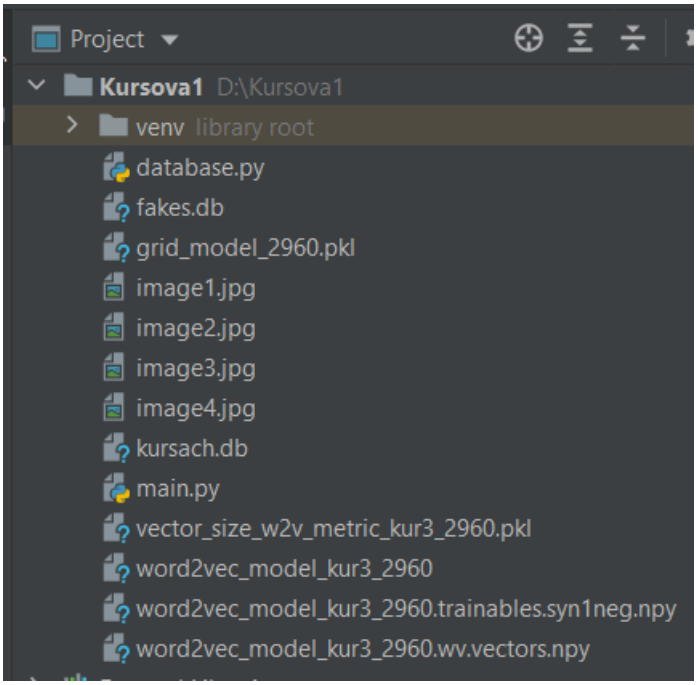


Рисунок 3.9 — Структура проєкту

Для програмної реалізації системи було обрано найбільш конструктивну та функціональну мову — Python, що є мовою загального призначення, яка може виконувати набір складних завдань машинного навчання та дає змогу швидко

створювати прототипи, які дозволяють протестувати програмний продукт для машинного навчання. Ця мова дуже гнучка, а отже, вона дозволяє користувачеві розробляти нові види програм.

Для створення програмної реалізації системи, що розробляється, використано середовище PyCharm, що забезпечує зручне та ефективне редагування коду.

Програмний засіб складатиметься з двох файлів під назвами *database.py* та *main.py*. У першому відбувається робота з базою даних: її створення, підключення та оброблення інформації. У головному вікні проєкту під назвою *main.py* реалізовано основну частина програми, а саме, приєднання файлів з моделями та створення самого сайту.

У наступному підрозділі описується створення бази даних.

База даних – сукупність взаємопов’язаних даних, якими можна керувати в СКБД. Вона структурована таким чином, щоб полегшити маніпулюванням даними за допомогою запитів. За допомогою цього інструменту можна швидко здійснювати пошук по даним [23].

У базі даних зберігаються id, час запису новини в бд, текст новини, ембеддінґ, label та ймовірність передбачення.

Так як для створення бази даних використовується бібліотека sqlite3, то варіянтів не багато для вибору типу даних. Для ймовірності передбачення найкращим вибором буде – real, для label – integer, а для решти – text:

```
con = sqlite3.connect("fakes.db")
cur = con.cursor()
con.commit()
cur.execute("""
create table data (
id text PRIMARY KEY,
datetime text,
text TEXT NOT NULL,
embedding text NOT NULL,
label integer NOT NULL,
proba float
);""")
```

Для створення датасету використано середовище GoogleColab.

За основу взято файл excel в якому зберігається 2963 новини, потім за допомогою коду його експортовано в датасет.

```
df = pd.read_excel('/content/drive/MyDrive/fakes/fakes_new_ds_2
960.xlsx')
```

Для початку новини записані в датасет, тому що він дуже зручний та має безліч інструментів для маніпулювання даних, а також для експорту в базу даних. Для кінцевого варіянту знадобилось додати лише функцію, що визначає поточний час та ембеддінґ:

```
def get_now():
      now = datetime.datetime.now().strftime('%Y-%m-
%d %H:%m:%S')#.isoformat()
      return now
def text_to_vect(check_row):
  check_row = [check_row]
  df = pd.DataFrame()
  df['text'] = check_row
  df['text_Tokenized'] = df['text'].str.lower().apply(word_toke
nize)
  words = set(w2v_model_reloaded.wv.index2word)
  df['text_vect'] = [np.array([w2v_model_reloaded.wv[i] for i i
n ls if i in words])
                                          for ls in df['text_
Tokenized']]
  text_vect_avg = []
  for v in df['text_vect']:
      if v.size:
          text_vect_avg.append(v.mean(axis=0))
      else:
          text_vect_avg.append(np.zeros(vector_size_n_reloaded,
 dtype=float))
  df['text_vect_avg'] = text_vect_avg
  check_Machine_Learning_df = pd.DataFrame(text_vect_avg)
  check_Machine_Learning_df.columns = ['Element_' + str(i+1) fo
r i in range(0, check_Machine_Learning_df.shape[1])]
  return check_Machine_Learning_df.values
```

Для функції text_to_vect попередньо потрібно завантажити моделі, які натреновані датасетом:

```
w2v_model_reloaded = Word2Vec.load("/content/drive/MyDrive/word
2vec/word2vec_model_kur3_2960_2")
```

```
vector_size_n_reloaded = pk.load(open("/content/drive/MyDrive/w
ord2vec/vector_size_w2v_metric_kur3_2960_2.pkl",'rb'))
model_reloaded = pk.load(open("/content/drive/MyDrive/models/gr
id_model_2960_2.pkl",'rb'))
```

Результат кінцевого датасету готового до експорту в базу даних (рис. 3.10):

	id	datetime	text	embedding	label	proba
0	0	2023-01-15 14:01:07	На МКС зафиксирован вброс бюллетеней на выбора...	[[0.28313988, 0.26887143, 0.0142212445, -0.214...	1	0.99
1	1	2023-01-15 14:01:07	Правозахисник Мстіслав Руаков заявив, що росій...	[[-0.7815896, -0.114596784, 0.1955945, -0.2547...	1	0.99
2	2	2023-01-15 14:01:07	У США шукають управу на тих, хто вирішив без г...	[[-0.60774815, -0.31783023, 0.40678737, 0.2247...	1	0.99
3	3	2023-01-15 14:01:07	Лікарі лікарні в Маріуполі масово звільнилися ...	[[-0.78071666, 0.1833523, 0.17970768, -0.36666...	1	0.99
4	4	2023-01-15 14:01:07	Суд Цюриха постановив повернути Україні золото...	[[-0.2429358, -0.18965775, -0.060354613, -0.37...	1	0.99

Рисунок 3.10 — Результат кінцевого датасету

Код, в якому здійснюється експорт датасету у вже створену базу даних:

```
df.to_excel('/content/drive/MyDrive/fakes/ds_for_db.xlsx')
```

3.4 Реалізація основних функцій системи розподіленої системи виявлення та блокування фейків

Для початку створено датасет, в який поміщено 2960 новин. Далі його завантажено в Google Colab, використовуючи такий фрагмент коду:

```
ds = pd.read_excel('drive/MyDrive/fakes/fakes_new_ds.xlsx', ind
ex_col=0)
```

Наступним кроком виконано перетворення слів у вектори, за допомогою Word2Vec. Пропущено через токенайзер та позбавлено датасет від стоп-слів.

Для вдалого моделювання необхідно визначити найкращий набір гіперпараметрів для кожного з класифікаторів. Гіперпараметри – параметри моделі, які встановлюються до етапу навчання моделі. Одним із методів вирішення даної задачі є алгоритм GridSearch [24]. Суть алгоритму – перебрати перелік гіперпараметрів моделі, виконати аналіз оцінки і отримати перелік

параметрів, при яких модель має найкращі результати. Фрагмент коду з використанням GridSearch:

```
from sklearn.model_selection import GridSearchCV, ParameterGrid
grid_model = GridSearchCV(model, params, cv=N_SPLITS)
grid_model.fit(X_train, y_train)
# Get the best estimator
model = grid_model.best_estimator_
y_dev_pred = grid_model.predict(X_dev)
print("Dev accuracy: {:.3f}".format(accuracy_score(y_dev, y_dev
_pred)))
y_test_pred = grid_model.predict(X_test)
print("Test accuracy: {:.3f}".format(accuracy_score(y_test, y_t
est_pred)))
```

Перейдемо до основного етапу – етапу виявлення. Для початку завантажено модель з файлу Excel. Далі створено змінну check, відповідно до якої буде відбуватись саме виявлення. Фрагмент коду з виконанням виявлення:

```
check = pd.read_excel('drive/MyDrive/fakes/test_df_15.xlsx', in
dex_col=0)
text = check['text']
def predict_new0(text):
  check['text_Tokenized'] = check['text'].str.lower().apply(wor
d_tokenize)
  check
  words = set(w2v_model_reloaded.wv.index2word)
  check['text_vect'] = np.array([np.array([w2v_model_reloaded.w
v[i] for i in ls if i in words])
       for ls in check['text_Tokenized']])
```

Далі проведемо тестування підсистеми виявлення фейків.

Наступним етапом було почато створення сайту. Доцільно використати бібліотеку Streamlit та середовище PyCharm. Для початку було створено меню, яке містить такі пункти: «Перевірити новину», «Види фейків», «Як боротися із фейками?». Фрагмент коду зі створенням меню показано нижче:

```
app_mode = st.sidebar.selectbox('Меню', ['Оберіть дію',
'Перевірити новину', 'Види фейків', 'Як боротись з фейками?'])
```

Вигляд меню зображено на рис. 3.11:

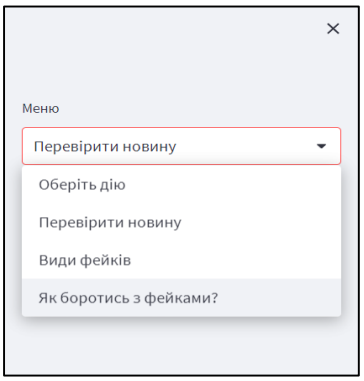


Рисунок 3.11 — Вигляд меню

Далі створено поле для введення новини та кнопку перевірки самої новини. Реалізацію даної задачі показано на рис. 3.12.

Рисунок 3.12 — Вигляд пункту меню «Перевірити новину»

Наступним кроком було під’єднання моделей з середовища Google Colab до PyCharm. Імпортовано основні бібліотеки для подальшої роботи. Було створено функцію, яка виконує виявлення фейку:

```
def predict_new(check_row):
    df = pd.DataFrame()
    df['text'] = check_row

    df['text_Tokenized'] =
df['text'].str.lower().apply(word_tokenize)
```

```
        words = set(w2v_model_reloaded.wv.index2word)
        df['text_vect'] = [np.array([w2v_model_reloaded.wv[i] for i
    in ls if i in words])
                           for ls in df['text_Tokenized']]
        text_vect_avg = []
          ...
    check_Machine_Learning_df = pd.DataFrame(text_vect_avg)
    check_Machine_Learning_df.columns = ['Element_' + str(i + 1)
    for i in range(0, check_Machine_Learning_df.shape[1])]
    return check_Machine_Learning_df.values
```

Завантаження моделей показано у наступному фрагменті коду:

```
     w2v_model_reloaded = Word2Vec.load("word2vec_model_kur3_2960")
vector_size_n_reloaded                                              =
pk.load(open("vector_size_w2v_metric_kur3_2960.pkl",'rb'))
model = pk.load(open("grid_model_2960.pkl",'rb'))
```

Далі, після оброблення кнопки «Check», викликано функцію з виявлення фейку:

```
    y_pred = model.predict(predict_new([news_text]))
```

Перевірка інформації на достовірність відбувається таким чином:

```
    st.write('Результат                передбачення:                ',
             "Достовірна новина" if y_pred == 1 else "Дана новина є
    фейковою")
    probability                                                      =
    ((model.predict_proba(predict_new([news_text])))[0]).round(2) *
    100
    probability = probability[0] if y_pred == 0 else probability[1]
    st.write('Ймовірність передбачення', probability, '%')
```

Для функції get_cos_koefs потрібно з бази даних записати в словник їх id та embedding:

```
    embs = np.array(list(id_emb.values()))
    ids = list(id_emb.keys())
```

Далі необхідно id та обчислити косинусну подібність вхідної новини та новин з бази даних за допомогою функції cosine_similarity, яка обчислює косинусну подібність всіх новин з бази даних з вхідною новиною, та перетворити в словник, потім відсортувати за спаданням.

```
d0 = dict(zip(ids, cosine_similarity(text_to_check, embs)[0]))
d0 =
dict(sorted(d0.items(),key=lambda item: item[1], reverse=True)
```

Потім створюється тимчасовий словник, в якому містяться id та embedding 2-ох найбільш схожих новин:

```
top_cos_koefs = {}
i = 0
for k, v in d0.items():
   top_cos_koefs[k] = v
   i += 1
   if i == thresh_value:
         break
```

Необхідно перевірити роботу функції get_cos_koefs.

Результат виконання функції get_cos_koefs в GoogleColab

Виклик функції get_cos_koefs:

```
top_similar_id = list(get_cos_koefs(get_id_emb()))
print(top_similar_id)
```

Результат функції get_cos_koefs наведено на рис. 3.13.

Рисунок 3.13 — Результат функції пошуку схожих новин

Вищенаведена функція повертає список id новин, що схожі на вхідну новину.

3.5 Тестування роботи системи

У даному підрозділі виконано тестування програмного застосунку. Для цього розглянуьл 4 новини: 2 з яких є фейковими, а 2 – достовірними.

Фейкова новина №1: «Ні, я не збираюся надати вам 6,2 мільярда доларів, як це зробив Джо»: твіт Ілона Маска про Володимира Зеленського».

Фейкова новина №2: «Міністерство оборони оголосило про успіх 11 ракетно-бомбових ударів по трубопроводах «Північний потік», «Північний потік-2» та «Болгарський потік». Удари нанесли сили ВПС московії, всі заплановані цілі повністю знищено. Державний відділ пояснив, що такий захід є вимушеною відповіддю московської сторони на відмову НАТО від розширення на схід. У найближчий час заплановано нанести удари по провідних країнах в Європі залізничними шляхами, а з 1 лютого сили московського ППО будуть збивати будь-які літаки, що рухаються дорогою до московії із заходу. Заступник міністра оборони Олександр Фомін пообіцяв і далі докласти максимальних зусиль до того, щоб схилити західних партнерів до конструктивних переговорів. На фоні про бомбардування трубопроводів зросла ціна на газ до 2800$. «Операція була проведена, і всі снаряди були потрапили в ціль, європейські ППО не змогли ефективно боротися з нашою атакою, – сказав Олександр Фомін. – У найближчий час ми сподіваємося повернутися за стіл переговорів з європейцями, які повністю зрозуміли серйозність наших намірів, отже, робота наших пілотів і ракетників заслуговує найвищої похвали».

Достовірна новина №1: «Україна – не «Титанік»: Зеленський прокоментував «евакуацію» іноземних дипломатів» [26].

Достовірна новина №2: «Прикордонник Сергій Кладько отримав відзнаку «За заслуги перед Вінниччиною»» [27].

Обрано навмисно як короткі, так і довгі новини, щоб перевірити ефективність роботи програмного засобу.

Результати перевірки програмного застосунку наведено на рис. 3.14–3.17.

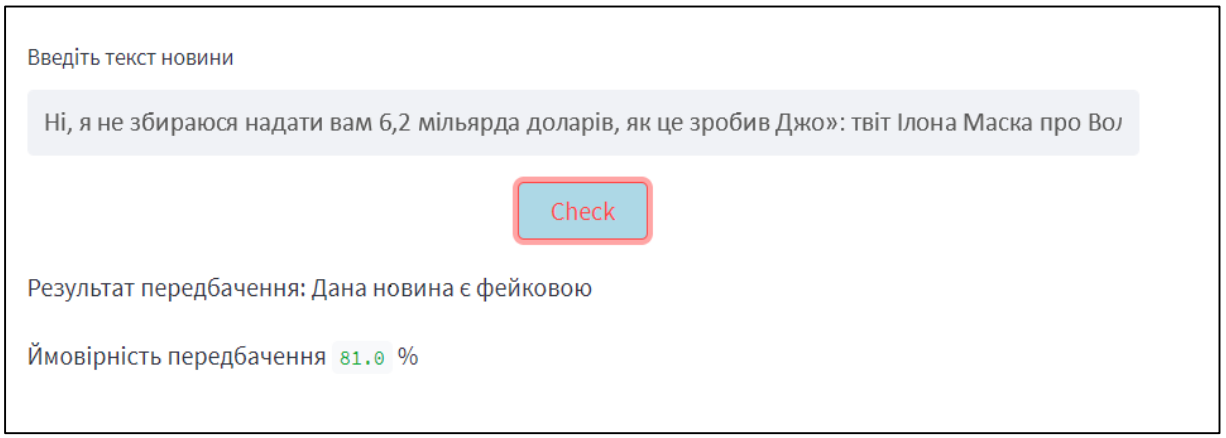


Рисунок 3.14 — Вигляд вікна перевірки фейкової новини №1

Перевірка 2 фейкової новини:

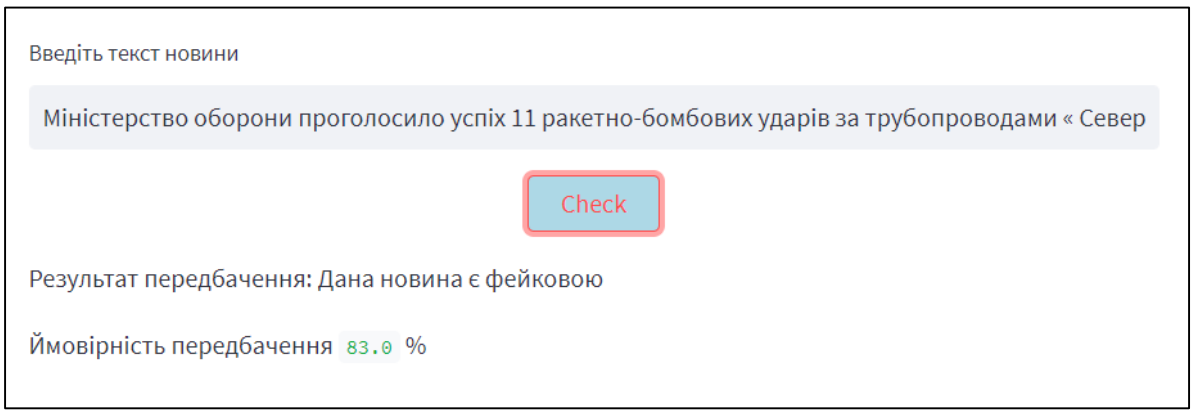


Рисунок 3.15 — Вигляд вікна перевірки фейкової новини №2

Перевірка 1 достовірної новини:

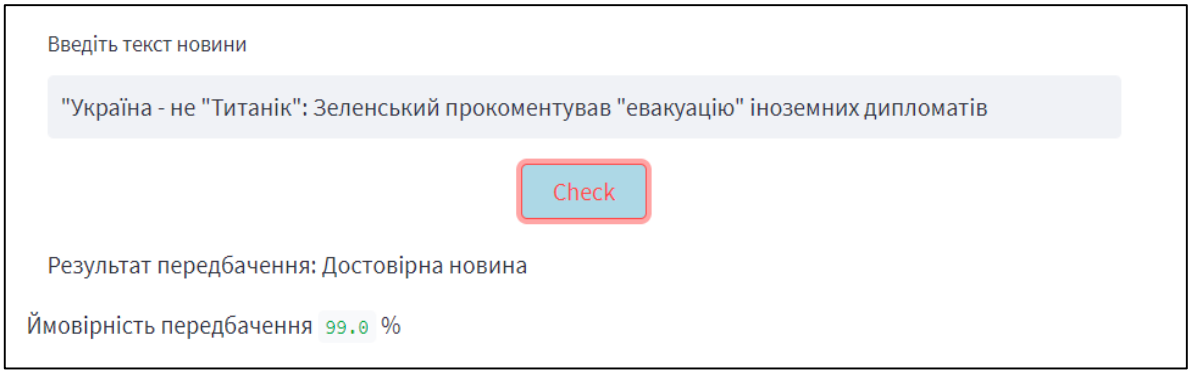


Рисунок 3.16 — Вигляд вікна перевірки достовірної новини №1

Перевірка 2 достовірної новини:

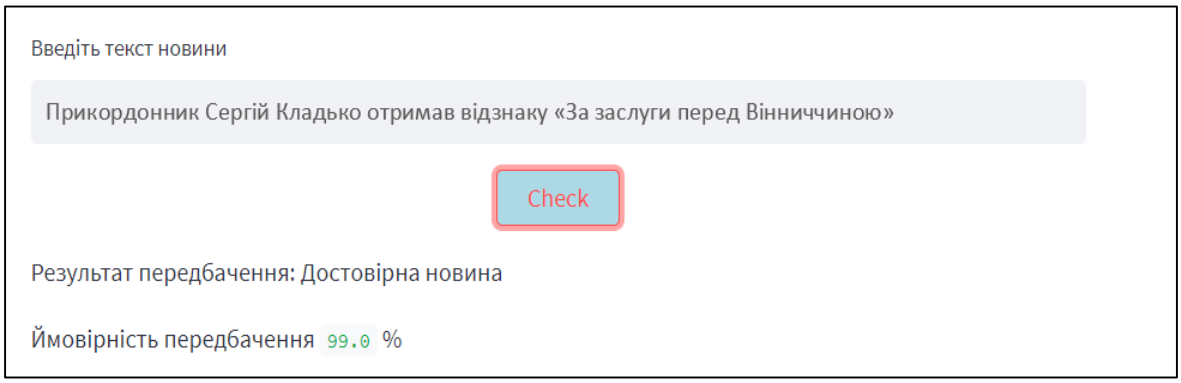


Рисунок 3.17 — Вигляд вікна перевірки достовірної новини №2

Перейдено до наступного підрозділу, в якому будуть показані результати пошуку схожих новин. Для тестування пошуку схожих новин було створено функцію *get_cos_koefs()*

Результат функції *get_cos_koefs()* на веб-сторінці:

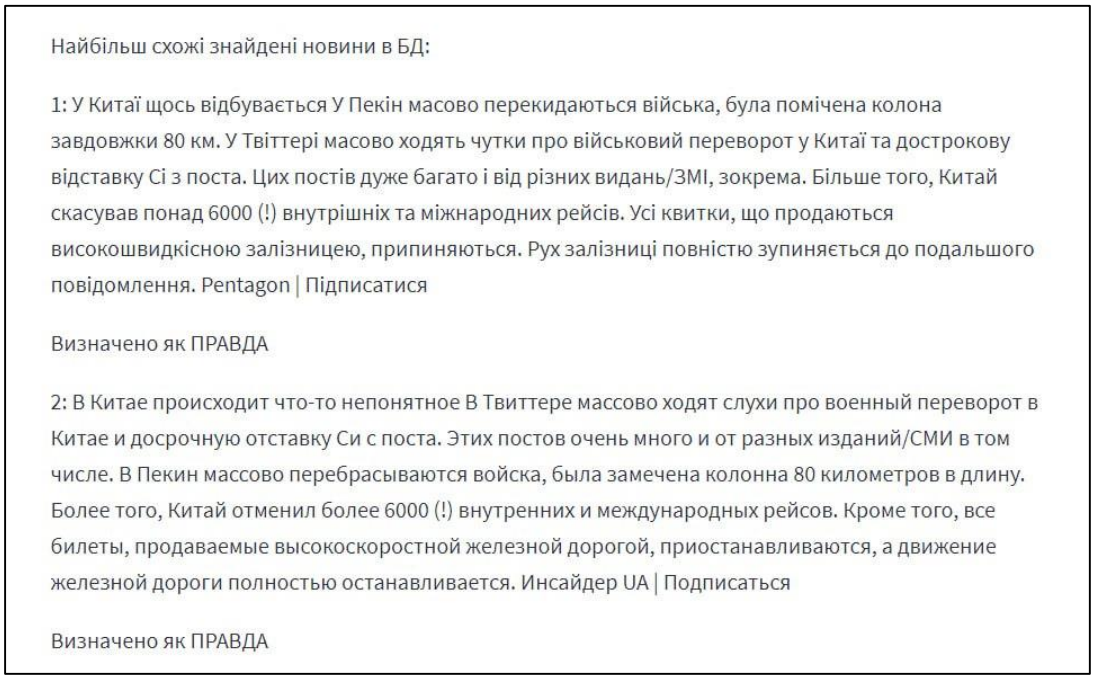


Рисунок 3.18 – Результат функції пошуку схожих новин на веб-сторінці

За результатом можна зробити висновок, що розроблена система виявлення фейків працює коректно.

4 ЕКОНОМІЧНА ЧАСТИНА

4.1 Комерційний та технологічний аудит науково-технічної розробки

Метою даного розділу є проведення технологічного аудиту, в даному випадку нового програмного модулю для виявлення фейкової інформації у соцмережах. Метою розробки програмного модулю для виявлення фейкової інформації у соцмережах є дослідження структури найпопулярніших новинних веб ресурсів із фейковими новинами.

Особливістю є те, що досліджено способи поширення фейків, які дозволяють уявити більш цільну картину функціонування соціальних мереж при поширенні фейкового контенту.

Аналогом може бути ACS 400 за ціною 8709 грн.

Для проведення комерційного та технологічного аудиту залучають не менше 3-х незалежних експертів. Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням п’ятибальної системи оцінювання за 12-ма критеріями, у відповідності із табл. 4.1.

Таблиця 4.1 – Рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можлива бальна оцінка

Бали (за 5-ти бальною шкалою)					
Кри-терій	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздат-ність продукту в реальних умовах

Продовження табл. 4.1

Ринкові переваги					
2	Багато аналогів на малому ринку	Ринкові п Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практика на здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві

Продовження табл. 4.1

11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Усі дані по кожному параметру занесено в табл. 4.2

Таблиця 4.2 – Результати оцінювання комерційного потенціалу розробки

Критерії оцінювання	ПІБ експертів		
	Експерт 1	Експерт 2	Експерт 3
	Бали		
Технічна здійсненність концепції	3	3	4
Наявність аналогів на ринку	3	3	4
Цінова політика	4	3	3
Технічні та споживчі властивості виробу	3	4	4
Експлуатаційні витрати	4	3	3
Ринок збуту	3	4	4
Конкурентоспроможність	4	3	3
Фахівці з технічної і комерційної реалізації	3	4	3
Фінансування	4	4	3
Матеріально-технічна база	4	3	3
Термін реалізації ідеї	3	4	3
Супровідна документація	3	3	4
Сума	41	41	41
Середньоарифметична сума балів	(41+41+41) / 3 = 41		

За даними табл. 4.2 можна зробити висновок щодо рівня комерційного потенціалу даної розробки. Для цього доцільно скористатись рекомендаціями,

наведеними в табл. 4.3.

Таблиця 4.3 Рівні комерційного потенціалу розробки

Середньоарифметична сума балів СБ , розрахована на основі висновків експертів	Рівень комерційного потенціалу розробки
0 - 1 0	Низький
11-20	Нижче середнього
21-30	Середній
31-40	Вище середнього
41-48	Високий

Як видно з табл., рівень комерційного потенціалу розроблюваного нового програмного продукту є високим, що досягається за рахунок того, що програмний продукт відрізняється від існуючих тим, що дана технологія є програмним засобом для виявлення фейкової інформації у соцмережах, який систематизує загальні підходи до опису і формалізації фейків, на основі яких визначено основні способи поширення фейкового контенту в соціальних мережах.

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

Основна заробітна плата розробників, яка розраховується за формулою:

$$З_о = \frac{M}{T_р} \cdot t \,, \tag{4.1}$$

де М – місячний посадовий оклад конкретного розробника (дослідника), грн.;

$T_р$ – число робочих днів в місяці, 23 днів;

t – число днів роботи розробника (дослідника).

Результати розрахунків зведемо до табл. 4.1.

Таблиця 4.1 – Основна заробітна плата розробників

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
Керівник проекту	28000	1217,39	30	36521,739
Програміст	25000	1086,96	30	32608,696
Всього				69130,43

Так як в даному випадку розробляється програмний продукт, то розробник виступає одночасно і основним робітником, і тестувальником розроблюваного програмного продукту.

Додаткова заробітна плата розробників, які приймали участь в розробці обладнання

Додаткова заробітна плата прийнято розраховувати як 13 % від основної заробітної плати розробників та робітників:

$$З_д = З_о \cdot 13\ \% / 100\ \% \qquad (4.2)$$

$З_д = (69130,43 \cdot 13\ \% / 100\ \%) = 8986,96$ (грн.)

Згідно діючого законодавства нарахування на заробітну плату складають 22 % від суми основної та додаткової заробітної плати.

$$Н_з = (З_о + З_д) \cdot 22\ \% / 100\% \qquad (4.3)$$

$Н_з = (69130,43 + 8986,96) \cdot 22\ \% / 100\ \% = 17185,83$ (грн.)

Оскільки для розроблювального пристрою не потрібно витрачати матеріали та комплектуючи, то витрати на матеріали і комплектуючі дорівнюють нулю.

Амортизація обладнання, що використовувалось для розробки в спрощеному вигляді амортизація обладнання, що використовувалась для розробки розраховується за формулою:

$$A = \frac{Ц}{Тв} \cdot \frac{t_{вик}}{12} \text{ [грн.].} \quad (4.4)$$

де Ц – балансова вартість обладнання, грн.;

Т – термін корисного використання обладнання згідно податкового законодавства, років

$t_{вик}$ – термін використання під час розробки, місяців

Розрахуємо, для прикладу, амортизаційні витрати на комп'ютер балансова вартість якого становить 20000 грн., термін його корисного використання згідно податкового законодавства – 2 роки, а термін його фактичного використання – 1,30 міс.

$$A_{обл} = \frac{20000}{2} \times \frac{1,3}{12} = 1086,96 грн.$$

Аналогічно визначаємо амортизаційні витрати на інше обладнання та приміщення. Розрахунки заносимо до табл. 5.2. Для розрахунку амортизації нематеріальних ресурсів використовується формула:

$$A_{н.р.} = Ц_{н.р.} * Н_а * \frac{t_{вик.}}{12} \quad (4.5)$$

Але, так як вартість ліцензійної ОС та спеціалізованих ліцензійних нематеріальних ресурсів менше 20000 грн, то даний нематеріальний актив (Microsoft Windows 10) не амортизується, а його вартість включається у вартість розробки повністю, $B_{нем.ак.}$ = 1100 грн.

Таблиця 5.2 – Амортизаційні відрахування матеріальних і нематеріальних ресурсів для розробників

Найменування обладнання	Балансова вартість, грн.	Строк корисного використання, років	Термін використання обладнання, місяців	Амортиза-ційні відрахуван-ня, грн.
Комп'ютер та комп'ютерна периферія (Ноутбук ASUS)	20000	2	1,30	1086,957
Офісне обладнення (меблі)	20000	4	1,30	543,478
Приміщення	950000	20	1,30	5163,043
Всього				6793,48

Тарифи на електроенергію для непобутових споживачів (промислових підприємств) відрізняються від тарифів на електроенергію для населення. При цьому тарифи на розподіл електроенергії у різних постачальників (енергорозподільних компаній), будуть різними. Крім того, розмір тарифу залежить від класу напруги (1-й або 2-й клас). Тарифи на розподіл електроенергії для всіх енергорозподільних компаній встановлює Національна комісія з регулювання енергетики і комунальних послуг (НКРЕКП). Витрати на силову електроенергію розраховуються за формулою:

$$В_е = В \cdot П \cdot Ф \cdot К_п, \qquad (4.6)$$

де В – вартість 1 кВт-години електроенергії для 1 класу підприємства, В = 6,2 грн./кВт;

П – встановлена потужність обладнання, кВт. П = 0,4 кВт;

Ф – фактична кількість годин роботи обладнання, годин.

$К_п$ – коефіцієнт використання потужності, $К_п$ = 0,9.

$$В_е = 0,9 \cdot 0,4 \cdot 8 \cdot 30 \cdot 6,2 = 535,68 \text{ (грн.)}$$

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками. Витрати за статтею «Інші витрати» розраховуються як 50…100% від суми основної заробітної плати дослідників:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.7)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати».

$$I_в = 69130{,}43 * 50\% / 100\% = 34565{,}22 \text{ (грн.)}$$

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов'язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов'язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов'язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін. Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100…150% від суми основної заробітної плати дослідників:

$$Н_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.8)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати».

$Н_{нзв}$ = 69130,43 * 150 % / 100 % = 103696 (грн.)

Сума всіх попередніх статей витрат дає загальні витрати на проведення науково-дослідної роботи:

$B_{заг}$ = 69130,43+8986,96+17185,83+6793,48+1100+4300+535,68+34565,22+ +103696 = 246293,25 грн.

Розрахунок загальних витрат на науково-дослідну (науково-технічну) роботу та оформлення її результатів наведено нижче.

Загальні витрати на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховуються ЗВ, визначається за формулою:

$$ЗВ = \frac{B_{заг}}{\eta} \text{ (грн)}, \quad (4.9)$$

де η – коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи.

Так, якщо науково-технічна розробка знаходиться на стадії: науково-дослідних робіт, то η=0,1; технічного проектування, то η=0,2; розробки конструкторської документації, то η=0,3; розробки технологій, то η=0,4; розробки дослідного зразка, то η=0,5; розробки промислового зразка, то η=0,7; впровадження, то η=0,9. Оберемо η = 0,5, так як розробка, на даний момент, знаходиться на стадії дослідного зразка:

$$ЗВ = 246293,25 / 0,5 = 492586 \text{ грн.}$$

4.3 Розрахунок економічної ефективності науково-технічної розробки

У ринкових умовах узагальнювальним позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку. Саме зростання чистого прибутку забезпечить потенційному інвестору надходження додаткових коштів, дозволить покращити фінансові результати його діяльності, підвищить конкурентоспроможність та може позитивно вплинути на ухвалення рішення щодо комерціалізації цієї

розробки.

Для того, щоб розрахувати можливе зростання чистого прибутку у потенційного інвестора від можливого впровадження науково-технічної розробки необхідно:

— вказати, з якого часу можуть бути впроваджені результати науково-технічної розробки;

— зазначити, протягом скількох років після впровадження цієї науково-технічної розробки очікуються основні позитивні результати для потенційного інвестора (наприклад, протягом 3-х років після її впровадження);

— кількісно оцінити величину існуючого та майбутнього попиту на цю або аналогічні чи подібні науково-технічні розробки та назвати основних суб'єктів (зацікавлених осіб) цього попиту;

— визначити ціну реалізації на ринку науково-технічних розробок з аналогічними чи подібними функціями.

При розрахунку економічної ефективності потрібно обов'язково враховувати зміну вартості грошей у часі, оскільки від вкладення інвестицій до отримання прибутку минає чимало часу. При оцінюванні ефективності інноваційних проектів передбачається розрахунок таких важливих показників:

— абсолютного економічного ефекту (чистого дисконтованого доходу);

— внутрішньої економічної дохідності (внутрішньої норми дохідності);

— терміну окупності (дисконтованого терміну окупності).

Аналізуючи напрямки проведення науково-технічних розробок, розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором можна об'єднати, враховуючи визначені ситуації з відповідними умовами.

Розробка чи суттєве вдосконалення програмного засобу (програмного забезпечення, програмного продукту) для використання масовим споживачем.

У цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

$$\Delta П_i = (\pm \Delta Ц_0 \cdot N + Ц_0 \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (4.10)$$

де $\pm\Delta Ц_о$ – зміна вартості програмного продукту (зростання чи зниження) від впровадження результатів науково-технічної розробки в аналізовані періоди часу;

N – кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки;

$Ц_о$ – основний оціночний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки, $Ц_о = Ц_б \pm \Delta Ц_о$;

$Цб$ – вартість програмного продукту у році до впровадження результатів розробки;

ΔN – збільшення кількості споживачів продукту, в аналізовані періоди часу, від покращення його певних характеристик;

λ – коефіцієнт, який враховує сплату податку на додану вартість. Ставка податку на додану вартість дорівнює 20%, а коефіцієнт $\lambda = 0{,}8333$.

ρ – коефіцієнт, який враховує рентабельність продукту;

ϑ – ставка податку на прибуток, у 2022 році ϑ =18%.

Припустимо, що при прогнозованій ціні 3500 грн. за одиницю виробу, термін збільшення прибутку складе 3 роки. Після завершення розробки і її вдосконалення, можна буде підняти її ціну на *500* грн. Кількість одиниць реалізованої продукції також збільшиться: протягом першого року – на 5000 шт., протягом другого року – на 4000 шт., протягом третього року на 3000 шт. До моменту впровадження результатів наукової розробки реалізації продукту не було:

*$\Delta П_1$ = (0*500 + (3500 + 500)*5000)* 0,8333* 0,25) * (1 - 0,18) = 2989583,214 грн.*

*$\Delta П_2$ = (0*500 + (3500 + 500)*(5000+4000)* 0,8333* 0,25) * (1 - 0,18) = 6149999,754 грн.*

*$\Delta П_3$ = (0*500 + (3500 + 500)*(5000+4000+3000)* 0,8333* 0,25) * (1 - 0,18) = 8199999,672 грн.*

Отже, комерційний ефект від реалізації результатів розробки за три

роки складе 17339582,64 грн.

4.4 Розрахунок ефективності вкладених інвестицій та періоду їх окупності

Розраховуємо приведену вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \qquad (4.11)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої науково-дослідної (науково-технічної) роботи, грн;

Т – період часу, протягом якою виявляються результати впровадженої науково-дослідної (науково-технічної) роботи, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, $\tau = 0,05...0,15$;

t – період часу (в роках).

Збільшення прибутку ми отримаємо починаючи з першого року:

ПП= (2989583,214/(1+0,1)[1])+(6149999,754/(1+0,1)[2])+(8199999,672/(1+0,1)[3]) = 2717802,92 + 5082644,425 + 6160781,121 = 13961228,47 грн.

Далі розраховують величину початкових інвестицій *PV*, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки. Для цього можна використати формулу:

$$PV = k_{інв} * ЗВ, \quad (4.12)$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію. Це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай $k_{інв}=2...5$, але може бути і більшим;

ЗВ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

$$PV = 2 * 492586 = 985172{,}98 \text{ грн.}$$

Тоді абсолютний економічний ефект $E_{абс}$ або чистий приведений дохід *(NPV, Net Present Value)* для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV, \quad (4.13)$$

$E_{абс}$ = 13961228,47 – 985172,98 = 12976055,49 грн.

Оскільки $E_{абс} > 0$ то вкладання коштів на виконання та впровадження результатів даної науково-дослідної (науково-технічної) роботи може бути доцільним.

Для остаточного прийняття рішення з цього питання необхідно розрахувати внутрішню економічну дохідність або показник внутрішньої но-рми дохідності *(IRR, Internal Rate of Return)* вкладених інвестицій та порівняти її з так званою бар'єрною ставкою дисконтування, яка визначає ту мінімальну внутрішню економічну дохідність, нижче якої інвестиції в будь-яку науково-технічну розробку вкладати буде економічно недоцільно.

Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій $E_в$. Для цього використаємо формулу:

$$E_в = \sqrt[T_ж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{4.14}$$

$T_ж$ – життєвий цикл наукової розробки, роки.

$$E_в = \sqrt[3]{(1 + 12976055{,}49/985172{,}98} - 1 = 1{,}420$$

Визначимо мінімальну ставку дисконтування, яка у загальному вигляді визначається за формулою:

$$\tau = d + f, \tag{4.15}$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2022 році в Україні d = (0,09…0,14);

f – показник, що характеризує ризикованість вкладень; зазвичай, величина f = (0,05...0,5).

$$\tau_{\min} = 0{,}14 + 0{,}05 = 0{,}19.$$

Так як $E_в > \tau_{min}$, то інвестор може бути зацікавлений у фінансуванні даної наукової розробки.

Розрахуємо термін окупності вкладених у реалізацію наукового проекту інвестицій за формулою:

$$T_{ок} = \frac{1}{E_в}, \tag{4.16}$$

$$T_{ок} = 1 / 1{,}420 = 0{,}70 \text{ р.}$$

Оскільки $T_{ок}$ < 3-х років, а саме термін окупності рівний 0,70 роки, то

фінансування даної наукової розробки є доцільним.

Висновки до розділу: економічна частина даної роботи містить розрахунок витрат на розробку нового програмного продукту, сума яких складає 492586 гривень. Було спрогнозовано орієнтовану величину витрат по кожній з статей витрат. Також розраховано чистий прибуток, який може отримати виробник від реалізації нового технічного рішення, розраховано період окупності витрат для інвестора та економічний ефект при використанні даної розробки. В результаті аналізу розрахунків можна зробити висновок, що розроблений програмний продукт за ціною дешевший за аналог і є висококонкурентоспроможним. Період окупності складе близько 0,70 роки.

ВИСНОВКИ

Для досягнення поставленої в роботі мети — покращення процесу виявлення і блокування фейків шляхом створення відповідної розподіленої аналітичної системи — насамперед, було проведено аналіз існуючих засобів та методів виявлення інформаційних фейків, а також доведено негативну роль неправдивої інформації.

Після поглибленого аналізу обсягу фейкових новин в українському інтернет-секторі зроблено висновок про те, що фейкові новини можна класифікувати, зокрема, за масштабом подій, які вони описують. Тому в роботі проведено дослідження новин, які можуть бути локальними, регіональними або глобальними. Також особливу увагу було приділено інформації, пов'язаної з різними типами шахрайств, таких, як політичні, соціальні, культурні, спортивні, економічні, тощо.

У магістерській роботі реалізовано методи, засновані на класичних алгоритмах машинного навчання таких, як SVM, Random Forest. Результати показують, що найвищий бал розпізнавання фейків досягається з алгоритмом Support Vector Machine.

Було застосовано методи, засновані на глибокому навчанні. Мережі глибокого навчання потребують великих обсягів немаркованих даних, щоб зробити точні висновки, тому для визначення фейків використовувалися Python-бібліотеки pandas, word2vec та scikit-learn.

Застосувавши отримані результати було створено модуль для виявлення фейків.

Модуль виявлення фейкових новин виконує перевірку тексту за допомогою машинного навчання. Навчена модель зберігається і використовується під час подальшої перевірки.

Після відправлення тексту виконується його попереднє оброблення, а саме: текст очищується від стоп-слів та пунктуації, виконується стемінг та подальша токенізація. Після цього відбувається векторизація — перетворення масиву слів

на числове представлення на основі моделі «Word2Vec».

Вектори слів розміщені в просторі векторів таким чином, що слова із загальним контекстом розташовуються в цьому багатовимірному просторі в безпосередній близькості один від одного.

Виконано розробку програмного застосунку для виявлення та блокування фейкових новин. Для цього було обрано сучасний метод машинного навчання та середовище Google Colab та PyCharm.

Було протестовано програмний засіб для чого було обрано 4 новини: 2 фейкових та 2 достовірних. Шляхом перевірки на правдивість представлених для тестування новин було виявлено те, що розробка працює коректно, оскільки у 3 випадках із 4 результат сягає більше 80%.

В економічному розділі було обгрунтовано доцільність впровадження запропонованої розподіленої системи виявлення та блокування фейків шляхом визначення терміна окупності розробки, що складає менше 3 років.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Research guides: fake news: develop your fact-checking skills: some news literacy vocabulary. Home – Research Guides at Benedictine University Library. URL: https://researchguides.ben.edu/c.php?g=608230&p=4220191 (date of access: 06.05.2023).
2. Голодомор: історична довідка. Інформаційний портал Сумської міської ради. URL: https://smr.gov.ua/uk/dovidka/do-85-richchia-holodomoru/12146-golodomor-istorichna-dovidka.html (дата звернення: 06.05.2023).
3. Новини України та Світу. Головні і останні новини – NV. URL: https://nv.ua/ukr/publications/65-rokiv-tomu-amerikanskij-zhurnal-collier-s-poprosiv-uchenih-i-pismennikiv-pofantazuvati-pro-tretoji-svitovoji-100662.html (Дата звернення: 06.05.2023).
4. Фейки, СТОП: як виявляти брехню та перевіряти факти? [Електронний ресурс] // Google. URL: https://youcontrol.com.ua/webinar/feyky-stopyak-vyiavliaty-brekhniu-ta-pereviriaty-fakty/ (Дата звернення: 06.05.2023).
5. Курбан О. В. Сучасні інформаційні війни в мережевому онлайн просторі [Текст]: навчальний посібник. Київ: ВІКНУ, 2016. 286 с.
6. Атака інформаційна URL: https://vue.gov.ua/Атака_інформаційна (Дата звернення 06.05.2023).
7. Хорошко В. О., Хохлачова Ю. Є. Information war. mass media as an instrument of information influence on society. part 1. Ukrainian scientific journal of information security. 2016. Vol. 22, no. 3. URL: https://doi.org/10.18372/2225-5036.22.11104 (Date of access: 06.05.2023).
8. Гнасевич Н. В., Рудакевич О. М. Вплив політичної пропаганди в інформаційнопсихологічних операціях: принципи, форми та засоби впливу. Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід: [Матеріали II Міжнародної науково-практичної конференції, м. Тернопіль, Тернопільський національний економічний університет, 21-22 квітня 2017]. Тернопіль: Економічна думка, 2017. 379 с.

9. Російська деза під час війни: фейки про АЕС, біженців та українських військових. URL: https://rayon.in.ua/news/494106-raketniy-udar-po-aesipereselentsi-turisti-rosiyska-deza-4-bereznya (Дата звернення 06.05.2023).
10. Російська пропаганда URL: https://uk.m.wikipedia.org/wiki/Російська_ про паганда#Кібервійна_—_інформаційна_війна_в_інтернеті (Дата звернення 06.05.2023).
11. Сасин Г. В. Інформаційна війна: сутність, засоби реалізації, результати таможливості протидії (на прикладі російської експансії в український простір. Вісник «Грані». Серія: Політологія: Зб. наук. пр. К., березень 2015. 22 с.
12. Інфа від тещі братового кума: які повідомлення у соцмережах шкідливі під час війни? URL: https://life.pravda.com.ua/society/2022/03/9/247739 (Дата звернення 29.05.2022).
13. Логістична нерухомість під час війни: масштаби руйнувань, диверсифікація, перспективі відбудови URL: https://propertytimes.com.ua/industrialnaya_nedvizhemostlogistichna_neruhomist_pid_chas_viyni_masshtabi_ ruynuvan_diversifikatsiya_ta_perspektivi_vidbudovi (Дата звернення: 29.05.2022).
14. Як зберегти психологічне здоров'я під час війни – поради від американського психіатра URL: https://ukrainian.voanews.com/a/psyhiatr-proviynu/6492615.html (Дата звернення 29.05.2022).
15. Інформаційний шум – що треба знати про поведінку в мережі під час війни URL : https://tyzhden.ua/News/254484 (Дата звернення 29.05.2022).
16. Machine learning for neuroimaging with scikit-learn / A. Abraham et al. Frontiers in neuroinformatics. 2014. Vol. 8. URL: https://doi.org/10.3389/fninf.2014.00014 (Date of access: 06.05.2023).
17. Word2Vec tutorial – the skip-gram model · chris mccormick. Chris McCormick · Machine Learning Tutorials and Insights. URL: https://mccormickml.com/2016/04/19/word2vec-tutorial-the-skip-gram-model/ (Date of access: 06.05.2023).

18. Li Z. A beginner’s guide to word embedding with gensim word2vec model. Medium. URL: https://towardsdatascience.com/a-beginners-guide-to-word-embedding-with-gensim-word2vec-model-5970fa56cc92 (Date of access: 06.05.2023).
19. PyCoach T. Yes, python has a built-in database. here’s how to use it. Medium. URL: https://towardsdatascience.com/yes-python-has-a-built-in-database-heres-how-to-use-it-b3c033f172d3 (Date of access: 06.05.2023).
20. Talk M. D. Streamlit hands-on: from zero to your first awesome web app. Medium. URL: https://towardsdatascience.com/streamlit-hands-on-from-zero-to-your-first-awesome-web-app-2c28f9f4e214 (Date of access: 06.05.2023).
21. Cosine Similarity – Understanding the math and how it works? (with python). Machine Learning Plus. URL: https://www.machinelearningplus.com/nlp/cosine-similarity/ (Date of access: 06.05.2023).
22. Мова програмування Python: чому вона — кращий варіант для початківця. URL: https://blog.jungo.dev/uk/2021/07/mova-programuvannya-python-chomu-vona-krashhyj-variant-dlya-pochatkivczya/ (дата звернення: 06.05.2023).
23. SQLite tutorial – an easy way to master sqlite fast. SQLite Tutorial. URL: https://www.sqlitetutorial.net (Дата звернення: 06.05.2023).
24. Hyperparameter search in machine learning. arXiv.org. URL: https://arxiv.org/abs/1502.02127 (Date of access: 06.05.2023).
25. Бойко М. Україна – не «Титанік»: Зеленський прокоментував «евакуацію» іноземних дипломатів. ТСН.ua. URL: https://tsn.ua/politika/ukrayina-ne-titanik-zelenskiy-prokomentuvav-evakuaciyu-inozemnih-diplomativ-1964437.html (Дата звернення: 06.05.2023).
26. Панорама. URL: https://panorama.pub/news/rossiya-otravila-kube-v-kachestve-gumanitarnoj-pomoshhi-raketnye-kompleksy-iskander (Дата звернення: 06.05.2023).
27. Fake News Detection Using Machine Learning Ensemble Methods. URL: https://www.hindawi.com/journals/complexity/2020/8885861/ (Date of access: 06.05.2023).

28. Боровська Т. М., Колесник І. С., Северілов В. А. Моделювання банківської системи. *Інформаційні технології та комп'ютерна інженерія.* Вип. 1. № 1. С. 53–61. 2016.
29. Комплексні системи захисту інформації : [навчальний посібник] Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін. Вінниця : ВНТУ, 2018. 118 с.

Додаток А

Технічне завдання

Міністерство освіти та науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ

_____проф., д.т.н. О. Д. Азаров

«___» _____ 20__ р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

«**Розподілена аналітична система для виявлення і блокування фейків**»

08-23.МКР.001.00.000 ПЗ

Науковий керівник
к.т.н., проф. каф. ОТ
_____ Азарова А. О.
виконав:
магістрант 2 курсу,
_____Вальовський М. М.

Вінниця 2023

1. Підстава виконання магістерської кваліфікаційної роботи

1.2 Наказ про затвердження теми магістерської кваліфікаційної роботи від 20.03.2023 р. № 68.

2 Мета і призначенням МКР

2.1 Метою роботи є створення розподіленої аналітичної системи для виявлення і блокування фейків.

2.2 Призначення розробки — виконання магістерської кваліфікаційної роботи.

3. Вихідні дані для виконання МКР

Вихідні дані для виконання МКР: алгоритми машинного навчання (SVM, Random Forest, LSTM, BERT, XLNet, мова програмування Python.

4. Вимоги до виконання МКР

МКР повинна задовольняти такі вимоги:

— забезпечити протокол взаємодії апаратної частини з комп’ютером;

— провести моделювання та тестування системи;

5. Етапи МКР та очікувані результати

Етапи роботи та очікувані результати приведено в табл. А.1.

Таблиця А.1 — Етапи МКР

№ з/п	Назва етапів виконання магістерської роботи	Термін виконання етапів роботи	Примітка
1	Постановка мети та задач роботи	21.03.2021	
2	Огляд існуючих фейкових новин	22.03-02.04.2023	
3	Аналіз фейкового контенту в соціальних мережах	10.04-08.04.2023	
4	Дослідження методів виявлення та боротьби з шахрайством	09.04-29.04.2023	
5	Дослідження методів виявлення та боротьби із фейками	30.04-19.05.2023	
6	Розроблення комп’ютерної системи виявлення з фейків	20.05-25.05.2023	
7	Застосування методів попереднього навчання для створення системи виявлення фейків	26.05-.31.23	
8	Застосування методів глибокого навчання для розроблення системи боротьби з фейками	01.06-04.06.2023	
9	Розрахунок економічної частини роботи	05.06-06.06.2023	
10	Оформлення пояснювальної записки та ілюстративного матеріалу	08.06.2023	

11	Аналіз виконання роботи, висновки, додатки		
12	Перевірка якості виконання магістерської роботи та усунення недоліків		

6 Матеріали, що подаються до захисту МКР

До захисту МКР подаються: пояснювальна записка МКР, ілюстративні та графічні матеріали, протокол попереднього захисту МКР на кафедрі, відзив наукового керівника, відзив опонента, протоколи складання державних екзаменів, анотації до МКР українською та іноземною мовами, довідка про відповідність оформлення МКР діючим вимогам.

7 Порядок контролю виконання та захисту МКР

Виконання етапів розрахункової та графічної документації МКР контролюється науковим керівником згідно зі встановленими термінами. Захист МКР відбувається на засіданні Державної екзаменаційної комісії, затвердженою наказом ректора.

8 Вимоги до оформлення МКР

При оформлюванні МКР використовуються:

— ДСТУ 3008: 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302: 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

— Методичні вказівки до виконання магістерських кваліфікаційних робіт зі спеціальності 123 — «Комп’ютерна інженерія». Кафедра обчислювальної техніки ВНТУ 2022.

Додаток Б

Графіки полярності настрою людей для реальних та фейкових новин до і після оброблення

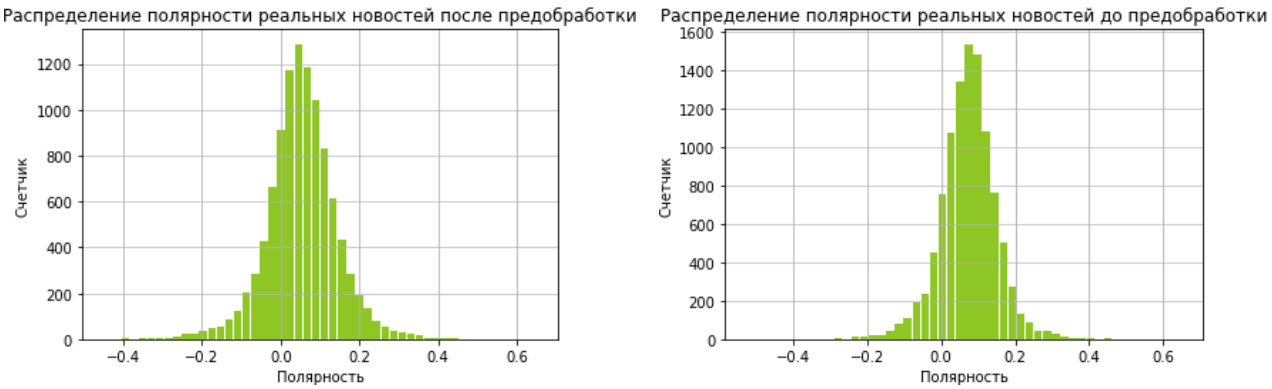


Рисунок Б.1 — Полярність реальних новин:

а) до оброблення; б) після оброблення

Додаток В

CBOW та skip-gram архітектури

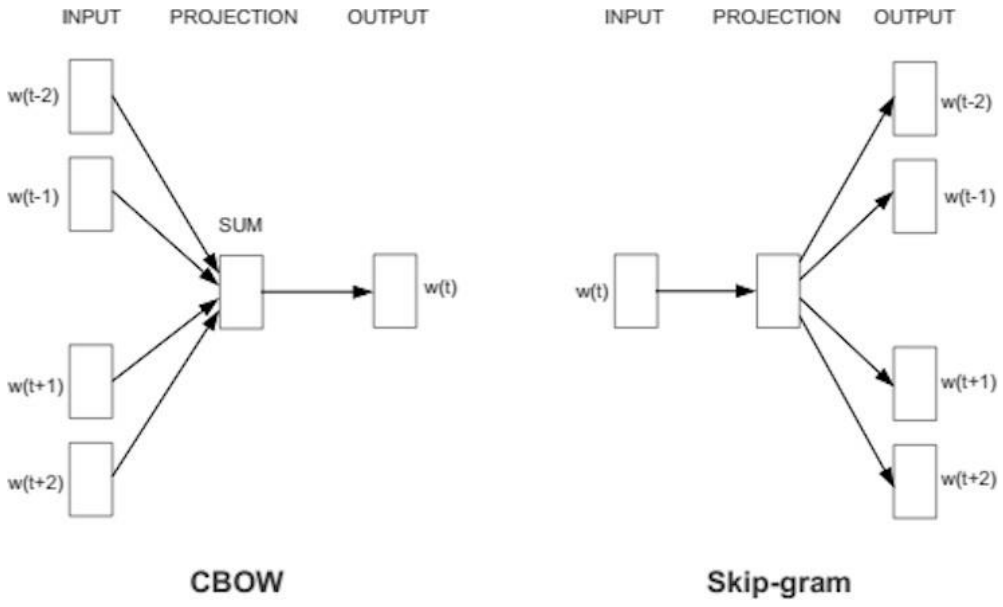


Рисунок В.1 — CBOW та skip-gram архітектури

Додаток Г

Структура мережі LSTM

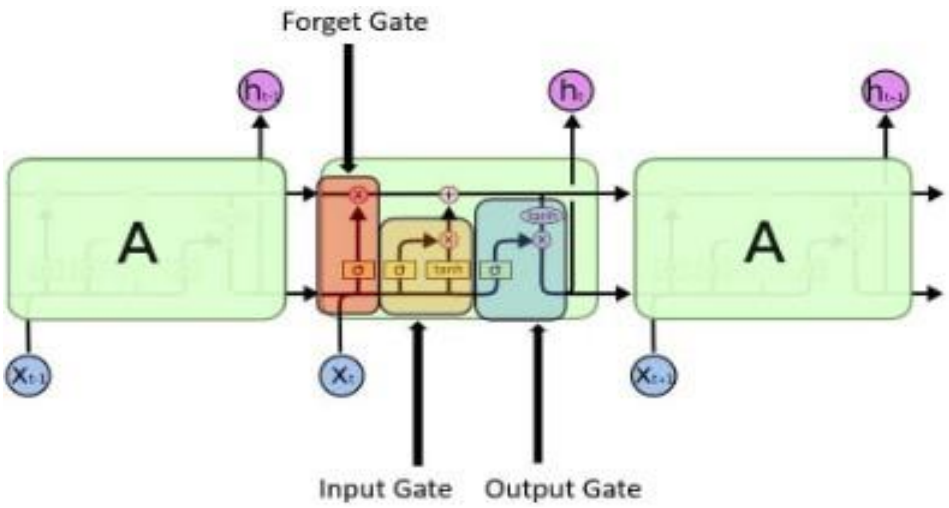


Рисунок Г1 — Структура мережі LSTM

Додаток Д

Лістинг програмного засобу

main.py

```
import random
import pickle as pk
import streamlit as st
import pandas as pd
import numpy as np
from gensim.models import Word2Vec
from nltk.tokenize import word_tokenize
import sklearn
import nltk
nltk.download('punkt')
from gensim.models import KeyedVectors
from gensim.models.doc2vec import Doc2Vec
from gensim.models.doc2vec import TaggedDocument
from gensim.models import Phrases
from gensim.models.phrases import Phraser
import gensim.downloader as api
from sklearn.metrics.pairwise import cosine_similarity, euclidean_distances
from sklearn.feature_extraction.text import TfidfVectorizer, CountVectorizer
from database import DB
import gensim
import uuid
import datetime
db = DB() #спочатку кода
def get_now():
      now = datetime.datetime.now().strftime('%Y-%m-%d %H:%m:%S')#.isoformat()
      return now

def get_cos_koefs(id_emb: dict, threshold=False, thresh_value=3):
  embs = np.array(list(id_emb.values()))
  ids = list(id_emb.keys())

  d0 = dict(zip(ids, cosine_similarity(text_to_check , embs)[0]))
  d0 =dict(sorted(d0.items(), key=lambda item: item[1]))

  top_cos_koefs = {}
  if threshold:
    for k, v in d0.items():
      if v > thresh_value:
        top_cos_koefs[k] = v
  else:
    i = 0
    for k, v in d0.items():
      top_cos_koefs[k] = v
      i += 1
      if i == thresh_value:
        break

  return top_cos_koefs
def get_top_similar_texts(*ids):
    res = db.get_top_similar_texts(*ids)
    # наступний увесь вивід в додатку реалізувати через стрімліт, тут для
прикладу
    st.write('Найбільш схожі знайдені новини в БД: \n')
    for j, id in enumerate(ids):
```

```
        for i in res:
            if id == i[0]:
                st.write(f'{j + 1}: {i[1]}')
                st.write('\nВизначено як ', 'ФЕЙК\n' if i[2] == 1 else
'ПРАВДА\n')
    return res
dt_now = get_now()
id = str(uuid.uuid4())[:8]
def predict_new(check_row):
    df = pd.DataFrame()
    df['text'] = check_row

    df['text_Tokenized'] = df['text'].str.lower().apply(word_tokenize)

    words = set(w2v_model_reloaded.wv.index2word)

    df['text_vect'] = [np.array([w2v_model_reloaded.wv[i] for i in ls if i in
words])
                       for ls in df['text_Tokenized']]
    text_vect_avg = []

    for v in df['text_vect']:
        if v.size:
            text_vect_avg.append(v.mean(axis=0))
        else:
            text_vect_avg.append(np.zeros(vector_size_n_reloaded,
                                          dtype=float))  # the same vector size
must be used here as for model training

    df['text_vect_avg'] = text_vect_avg
    check_Machine_Learning_df = pd.DataFrame(text_vect_avg)
    check_Machine_Learning_df.columns = ['Element_' + str(i + 1) for i in
range(0, check_Machine_Learning_df.shape[1])]

    return check_Machine_Learning_df.values
w2v_model_reloaded = Word2Vec.load("word2vec_model_kur3_2960")
vector_size_n_reloaded =
pk.load(open("vector_size_w2v_metric_kur3_2960.pkl",'rb'))
model = pk.load(open("grid_model_2960.pkl",'rb'))
# print(model)
# print(w2v_model_reloaded)
@st.cache(suppress_st_warning=True)
def get_fvalue(val):
    feature_dict = {"No": 1, "Yes": 2}
    for key, value in feature_dict.items():
        if val == key:
            return value


def get_value(val, my_dict):
    for key, value in my_dict.items():
        if val == key:
            return value

app_mode = st.sidebar.selectbox('Меню', ['Оберіть дію', 'Перевірити новину',
'Види фейків', 'Як боротись з фейками?'])
if app_mode == 'Перевірити новину':
    from PIL import Image

    image = Image.open('image4.jpg')

    st.image(image, width=700)
    customized_button = st.markdown("""
        <style >
```

```
        .stDownloadButton, div.stButton {text-align:center}
        .stDownloadButton button, div.stButton > button:first-child {
            background-color: #ADD8E6;
            color:#000000;
            padding-left: 20px;
            padding-right: 20px;
        }
            }
        </style>""", unsafe_allow_html=True)
    news_text = st.text_input('Введіть текст новини')  # read the text
    if news_text:
        text_to_check = predict_new([news_text])
    col1, col2, col3, col4, col5 = st.columns(5)
    with col3:
        but = st.button('Check')
    if but:
        y_pred = model.predict(text_to_check)

        print('---///--===', y_pred)
        prediction = 'Достовірна новина'
        #st.write(y_pred)
        st.write('Результат передбачення: ',
                 "Достовірна новина" if y_pred == 1 else "Дана новина є
фейковою")
        probability = ((model.predict_proba(text_to_check))[0]).round(2) * 100
        probability = probability[0] if y_pred == 0 else probability[1]
        st.write('Ймовірність передбачення', probability, '%')
    st.write('Чи хочете Ви побачити схожі новини?')
    col1, col2, col3, col4, col5 = st.columns(5)
    if news_text:
        with col3:
            but1 = st.button('Так')
        if but1:
            res_get_id_emb = db.get_id_emb()
            top_similar_id = list(get_cos_koefs(res_get_id_emb).keys())
            result = get_top_similar_texts(*top_similar_id)
            print(get_cos_koefs(res_get_id_emb))
            print(top_similar_id)
            print(result)
        # db.insert_data('data', (5, news_text, prediction, y_pred, 'UA'))
if app_mode == 'Оберіть дію':
    st.title('Що таке фейки?')
    st.write(
        'Фейкові новини (від англ. «fake» – брехня, фальш) – це неправдива
інформація, яка цілеспрямовано розповсюджується зацікавленими особами, що
переслідують свої (зазвичай політичні) цілі, або бажають заробити на інтернет-
трафіку. Поширюють обман, знищують засади цивілізованості та є небезпекою для
демократії ')
    st.image("image1.jpg")
if app_mode == 'Види фейків':
    st.title('Види фейків')
    st.write('Класифікувати фейки можливо за різними критеріями: ')
    st.write(
        '- за методом поширення: масово медійні (створюють для поширення в
рейтингових ЗМІ) і локальні (поширюються під час розмов, у соціальних
спільнотах, блогах тощо);')
    st.write(
        '- за зовнішньою формою поширення: фотофейк, відеофейк, фейковий
журналістський матеріал, фейковий допис, чутка;')
    st.write(
        '- за територіальною спрямованістю: внутрішні (спрямовані на громадян
конкретної території, держави) та зовнішні (спрямовані на представників
міжнародної спільноти); ')
    st.write(
```

```
        '- за направленістю (аудиторія): представники певних соціальних
верств/певного віку (наприклад, студенти, пенсіонери) та всі громадяни;')
    st.write(
        '-  за метою: сіяння паніки, розпалення міжнаціональної (расової,
релігійної тощо) ворожнечі; поширення хибної думки; маніпулювання свідомістю;
розважальний характер; звернення уваги на когось/щось; підготовка суспільства до
сприйняття якоїсь події, явища, рішення тощо.')
    st.image("image2.jpg")
```

database.py

```
import sqlite3
from streamlit import cursor
class DB:

    def __init__(self):
        self.conn = None
        self._db_path = self.db_path

    @property
    def db_path(self):
        return 'fakes.db'  # TODO Path подставить

    def connect_to_db(self):
        try:
            conn = sqlite3.connect(self.db_path)
            return conn
        except Exception as e:
            print(e)

    def insert_data(self, table_name, data):
        conn = self.connect_to_db()
        cursor = conn.cursor()
        cursor.execute(f"INSERT INTO {table_name} VALUES {data}")
        conn.commit()
        conn.close()

    def get_id_emb(self):
        conn = self.connect_to_db()
        cursor = conn.cursor()
        res = dict(cursor.execute("""select id, embedding from
data""").fetchall())
        res = {k: list(map(float, v[3:-2].split())) for k, v in res.items()}
        conn.commit()
        conn.close()
        return res

    def get_top_similar_texts(self,*ids):
        conn = self.connect_to_db()
        cursor = conn.cursor()
        res = cursor.execute(f"""select id, text, label from data where id in
{ids}""").fetchall()
        conn.commit()
        conn.close()
        return res
```

database.ipynb

```
from google.colab import drive
drive.mount('/content/drive')
import pandas as pd
import numpy as np
```

```
import pickle as pk

from nltk.tokenize import word_tokenize
from sklearn.svm import SVC
import statistics

from gensim.models import Word2Vec
from gensim.models import KeyedVectors

from gensim.models.doc2vec import Doc2Vec
from gensim.models.doc2vec import TaggedDocument

from gensim.models import Phrases
from gensim.models.phrases import Phraser

import gensim.downloader as api
import nltk
nltk.download('punkt')
from sklearn.datasets import make_hastie_10_2
from sklearn.ensemble import GradientBoostingClassifier
%matplotlib inline
import warnings
warnings.filterwarnings('ignore')
df = pd.read_excel('/content/drive/MyDrive/fakes/fakes_new_ds_2960.xlsx')
df.rename(columns = {'Unnamed: 0':'id'}, inplace = True)
del df["lang"]
import datetime

def get_now():
      now = datetime.datetime.now().strftime('%Y-%m-%d %H:%m:%S')#.isoformat()
      return now
df["datetime"] = get_now()
df["proba"] = 0.99
df.insert(1, 'datetime', df.pop('datetime'))
w2v_model_reloaded = Word2Vec.load("/content/drive/MyDrive/word2vec/word2vec_mod
el_kur3_2960_2")
vector_size_n_reloaded = pk.load(open("/content/drive/MyDrive/word2vec/vector_si
ze_w2v_metric_kur3_2960_2.pkl",'rb'))
model_reloaded = pk.load(open("/content/drive/MyDrive/models/grid_model_2960_2.p
kl",'rb'))
def text_to_vect(check_row):
  check_row = [check_row]
  df = pd.DataFrame()
  df['text'] = check_row

  df['text_Tokenized'] = df['text'].str.lower().apply(word_tokenize)
  words = set(w2v_model_reloaded.wv.index2word)
  df['text_vect'] = [np.array([w2v_model_reloaded.wv[i] for i in ls if i in word
s])
                                              for ls in df['text_Tokenized']]
  text_vect_avg = []
  for v in df['text_vect']:
      if v.size:
          text_vect_avg.append(v.mean(axis=0))
      else:
          text_vect_avg.append(np.zeros(vector_size_n_reloaded, dtype=float)) #
the same vector size must be used here as for model training


  df['text_vect_avg'] = text_vect_avg
  check_Machine_Learning_df = pd.DataFrame(text_vect_avg)
  check_Machine_Learning_df.columns = ['Element_' + str(i+1) for i in range(0, c
heck_Machine_Learning_df.shape[1])]
```

```
  return check_Machine_Learning_df.values
df['embedding']= df['text'].apply(func)
df.insert(3, 'embedding', df.pop('embedding'))
df['embedding'] = df['embedding'].apply(str)
df['id'] = df['id'].apply(str)
import sqlite3
con = sqlite3.connect("fakes.db")
cur = con.cursor()
print("Successfully Connected to SQLite")
con.commit()
df.to_sql('data', con)
```

Функція *get_cos_koefs()*:

```
def get_cos_koefs(id_emb: dict, threshold=False, thresh_value=3):
  embs = np.array(list(id_emb.values()))
  ids = list(id_emb.keys())

  d0 = dict(zip(ids, cosine_similarity(text_to_check , embs)[0]))
  d0 =dict(sorted(d0.items(), key=lambda item: item[1], reverse=True))

  top_cos_koefs = {}
  if threshold:
    for k, v in d0.items():
      if v > thresh_value:
        top_cos_koefs[k] = v
  else:
    i = 0
    for k, v in d0.items():
      top_cos_koefs[k] = v
      i += 1
      if i == thresh_value:
        break

  return top_cos_koefs
```

Додаток Е

111

Додаток Е

Протокол перевірки кваліфікаційної роботи

на наявність текстових запозичень

Назва роботи: «Розподілена аналітична система для виявлення і блокування фейків»

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра обчислювальної техніки, ФІТКІ

Показники звіту подібності Unicheck

Оригінальність 97,5 Схожість 2,5 %

Аналіз звіту подібності (відмітити потрібне):

- ✓ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.
- ☐ 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.
- ☐ 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 Захарченко С. М.

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи Вальовський М. М.

Керівник роботи Азарова А. О.