НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«До захисту допущено»
В.о. завідувача кафедри

_____ М.В.Грайворонський
(підпис)

“____”_____2019 р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.040301 «Прикладна математика»

на тему: Дискредитація як елемент інформаційної війни в кіберпросторі

Виконав : студент 4 курсу, групи ФІ-51

Ніколаєнко Іван Євгенійович _____
(прізвище, ім’я, по батькові) (підпис)

Керівник

д.т.н., професор, Качинський Анатолій Броніславович _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ - 2019 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки 6.040301 «Прикладна математика»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)
«___»_____2019 р.

ЗАВДАННЯ
на дипломну роботу студенту

Ніколаєнку Івану Євгенійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Дискредитація як елемент інформаційної війни в кіберпросторі,

науковий керівник роботи: д.т.н., професор, Качинський Анатолій Броніславович

затверджені наказом по університету від « 27 » травня 2019 р. № 1414-с

2. Термін подання студентом роботи 10 червня 2019 р.

3. Вихідні дані до роботи: результати дослідження розповсюдження і вияву фейкових новин та дезінформації в них.

4. Зміст роботи: огляд термінів та дослідження динаміки їх використання, дослідження розповсюдження дезінформації та фейків в інформаційних медіа-потоках

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) _____
_____
_____
_____

6. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Ознайомлення з літературою	05.10.18 – 19.05.19	
2	Отримання навичок роботи з веб-додатками для проведення дослідження	10.12.18 – 05.05.19	
3	Збір даних	05.04.19 – 30.04.19	
4	Вибір методів дослідження	15.04.19 – 30.04.19	
5	Використання статистичного, розвідкового, порівняльного аналізів для оброблення результатів	25.04.19 – 19.05.19	
6	Оформлення дипломної роботи	15.05.19 – 7.06.19	

Студент _____ Ніколаєнко І.Є.
(підпис)

Керівник роботи _____ Качинський А.Б.
(підпис)

РЕФЕРАТ

Дипломна робота має обсяг 68 сторінок, містить 30 рисунків, 14 таблиць, а також 23 посилання.

Актуальність обраної теми зумовлена необхідністю та важливістю в умовах інформаційного протистояння знайти методи виявлення фейкової інформації, щоб запобігти її поширенню.

Об’єктом дослідження є явище дискредитації в умовах інформаційної війни.

Предметом дослідження є модель розповсюдження фейків в кіберпросторі.

Мета роботи – вдосконалення методів аналізу та виявлення дезінформації та фейків в інформаційних медіа-потоках, що дозволить підвищити інформаційну безпеку держави в умовах ведення інформаційної війни.

Для досягнення поставленої мети потрібно вирішити наступні задачі: дати визначення термінів «інформаційна війна», «фейк», «дискредитація»; за допомогою використання інструментів веб-аналітики перевірити модель розповсюдження фейкових новин; виділити етапи поширення фейків; провести аналіз 3-х обраних фейків, зробити висновок по результатам.

Ключові слова: інформація; інформаційна війна; інформаційна операція; фейк; засоби масової інформації; дискредитація; повідомлення.

ABSTRACT

The thesis has a volume of 68 pages, contains 30 drawings, 14 tables, and 23 bibliographic sources.

The topicality of the chosen topic is determined by the necessity and importance in the conditions of information confrontation to find methods for detecting fake information in order to prevent its dissemination.

The object of research is the phenomenon of discreditation in the conditions of information warfare.

The subject of research is a model for the distribution of fake information in cyberspace.

The purpose of the work is to improve methods for analyzing and detecting misinformation and fake information media streams, which will increase the information security of the state in the context of conducting an information warfare.

To achieve the goal, the following tasks need to be addressed: to define the terms "information warfare", "fake", "discreditation"; using the web-analytics tools to apply the fake news distribution model; to allocate phases of distribution of fakes; to conduct a content analysis of 3 selected fakes, comparing models of their distribution; to make a conclusion on the results of this analysis.

Keywords: information; information warfare; information operation; fake; mass-media; discreditation; message.

ЗМІСТ

ВСТУП

Проблеми інформаційних воєн актуалізувалися у зв'язку з глобалізацією інформаційних процесів, бурхливим розвитком і пануванням інформаційних технологій, що дозволяють політикам експлуатувати інформаційний простір, процес взаємодії масових комунікацій і їх аудиторії. Тому, сьогодні постають актуальними питання виявлення методів розповсюдження фейкових новин та дезінформації, яку вони містять, задля спричинення умисної шкоди в умовах інформаційного протистояння.

Об’єктом дослідження є явище дискредитації в умовах інформаційної війни.

Предметом дослідження є модель розповсюдження фейків у кіберпросторі.

Метою даної роботи є вдосконалення методів аналізу та виявлення дезінформації та фейків в інформаційних медіа-потоках, що дозволить підвищити інформаційну безпеку держави в умовах ведення інформаційної війни.

Для досягнення поставленої мети потрібно вирішити наступні задачі:

- дати визначення термінів «інформаційна війна», «дискредитація», «фейк»;
- виділити етапи поширення фейків;
- за допомогою використання парсингу новинної стрічки та інструментів веб-аналітики перевірити модель розповсюдження фейкових новин;
- провести аналіз 3-х обраних фейків;
- зробити висновок по результатам.

1 ОГЛЯД ТЕРМІНІВ ТА ДОСЛІДЖЕННЯ ДИНАМІКИ ЇХ ВИКОРИСТАННЯ

1.1 Аналіз попередніх досліджень

Інформація відіграє головну роль у сучасному світі, саме тому американський дослідник М. Маклуен вивів таку тезу: «Істинно тотальна війна — це війна за допомогою інформації».[3] Маклуен найпершим ввів поняття «інформаційна війна» у науковий обіг та заявив, що в наш час економічні зв'язки і відносини все більше і більше приймають вигляд обміну знаннями, а не обміну товарами. А існуючі засоби масової комунікації являються новими «природними ресурсами», що збільшують багатства суспільства. Сучасні війни переважно ведуться саме в інформаційному просторі за допомогою новітнього інформаційного озброєння, адже саме доступ до інформаційних знань та ресурсів постає на головний план.

Зараз в науковому обігу дуже велике різноманіття визначень і пояснень, що ж таке інформаційна війна, саме тому це свідчить про незаперечну актуальність інформаційних воєн. Як сказав Мартін Лібікі, учений з американського університету національної оборони: «Спроби повною мірою усвідомити всі грані поняття інформаційної війни нагадують зусилля сліпих, що намагаються зрозуміти природу речей не бачачи їх…». Провівши дослідження по інформаційним війнам, М. Лібікі виділив психологічну форму інформаційної війни та сформував завдання інформаційної війни – знищення соціуму.

У своїй роботі, Георгій Почепцов зазначає, що інформаційна цивілізація не сприймає дій у фізичному просторі, інформаційна цивілізація вбачає перемогу в інформаційному і віртуальному просторах. [7]

Шафранські, у своїй праці з теорії інформаційних воєн 1995 р. Шафранські написав: «Система цілей інформаційної війни може включати кожен елемент епістемології супротивника». Тобто будь-який елемент в системі знань може

стати такою ціллю. Стосовно супротивника це звучить наступним чином: «Знаючи цінності ворога й використовуючи його репрезентаційну систему, ми можемо рахуватись із завданнями, розмовляти з розумом супротивника вербальною та невербальною мовами».[15]

Дослідженням впливу інформації на суспільну взаємодію займатиля такі вчені С. Гріняєв, А. Крутських, І. Панарін, Г. Гадамер, К. Поппер, вони передбачили перспективи та загрози в комунікативній сфері. [2]

1.2 Визначення терміну «інформаційна війна»

На сьогодні людство живе в інформаційному суспільстві. Це сучасний тип суспільства, в якому володіння інформацією (а не матеріальними благами) є рушійною силою його змін та розвитку, і в якому процвітає людська інтелектуальна творчість. Інформаційне суспільство спричинило інформаційні війни. Але найпершим кроком, перш ніж визначати термін «інформаційна війна» слід сформувати поняття «інформація». Для цього представлено декілька визначень.

Словник Electronic World English «Encarta» дає таке визначення інформації: «знання: певні знання, отримані або надані про що- небудь, або кого-небудь; зібрані факти: зібрані факти та дані про конкретний предмет; відомості про факти: передача фактів і знань».

Доктрина Збройних Сил США визначає інформацію як «дані, зібрані з навколишнього середовища і перероблені в корисну форму; об'єднання частин інформації з контекстом що виробляє ідеї або дає знання; знання перетворюються на розуміння».[18]

Поняття «інформаційна війна» увібрало в себе в ході історичної еволюції цілий ряд явищ, що виявляються в житті громади під час взаємодії мас, народів, соціальних груп.

Інформаційна війна - це така форма інформаційного протистояння між суб'єктами (державами, економічними та іншими структурами), яка передбачає комплекс завдань для заподіяння шкоди інформаційній сфері конкуруючої сторони та захисту власної інформаційної безпеки.

Сьогодні інформація набуває матеріальної форми, і влада над нею стає дуже бажаною. Перед реалізацією будь-яких "матеріальних рішень" проходить випробування перш за все в інформаційній області. Результати цих випробувань і є ключовими. Концепція інформаційної війни є дуже популярною, особливо тому, що людство живе в так званій інформаційній ері.

Інформаційна війна спрямована на послаблення моральних сил противника, використовуючи інформаційне управління. Така війна дозволяє отримати конкурентну перевагу над ворогом, знищуючи соціальну психологію і психологію людини, що еквівалентно справжньому кровопролиттю.

Інформаційна війна включає в себе безліч різних концепцій, які важко зрозуміти, і з урахуванням сучасних темпів розвитку інформаційного суспільства, можна стверджувати, що багато нових, невідомих аспектів цієї війни досі невідомі, але процес їх дослідження розвивається стрімко.

Термін "інформаційна війна" використовується для визначення концепції війни 21 століття на основі електронних та інформаційних систем.

Інформаційна війна не нова річ. Ці слова змінювалися протягом багатьох років і розвивалися з появою нових технологій. Терміну "інформаційна війна" передував термін "інформація у війні". Концепція інформаційної війни була введена в 1992 році в директиві DOD TS3600.1.[13] Гарне джерело, яке виокремлювало різницю між використанням інформації у війні та новою концепцією інформаційної війни - доповідь Комітету з питань науки і техніки 1997 року. Цей звіт передбачав, що інформація у війні стосується тактичного та стратегічного обману. пропаганда війни, знищення систем управління і командування. Одним з прикладів інформації у війні є використання листів,

брошур, виступів і плакатів, що поширюються американцями та німцями під час Першої та Другої світових воєн у формі пропаганди.

Інформаційна війна, визначена Агентством оборонних інформаційних систем США (DISA), є "діяльністю, спрямованою на отримання інформаційної переваги на підтримку національної військової стратегії, що впливає на інформаційні системи противника, використовуючи та захищаючи власні інформаційні системи".

У Сполучених Штатах та інших сучасних державах, урядових установах і навіть департаментах Міністерства оборони (ВПС США, ВМС США, Агентства національної безпеки, армії США тощо) використовуються дещо інші визначення інформаційної війни та інформаційних операцій. Як і очікувалося, ці інституції тепер визначають інформаційну війну з точки зору суто військових дій як інформаційних операцій; однак це не означає, що цілі є виключно військовими.

Визначення інформаційної війни можна розділити на такі загальні категорії: наступальні дії, оборонні дії та експлуатаційні дії.

- Наступальні дії – заперечують, корумпують, знищують або використовують інформацію супротивника, або впливають на сприйняття супротивника.
- Оборонні дії – захищають себе та союзників від подібних дій.
- Експлуатаційні дії – дозволяють своєчасно використовувати наявну інформацію для поліпшення циклу прийняття рішень / дій та порушення циклу супротивника.

Крім того, військові типи інформаційної війни вміщують засоби електронної боротьби (наприклад, перешкоджання комунікацій), системи спостереження, точковий удар (наприклад, якщо проходить бомбардування систем телекомунікації і комутації), а також вдосконалене бойове управління (наприклад, використання інформаційних систем для постачання інформації, на підставі якої військові рішення повинні базуватися на переслідуванні війни).

1.3 Завдання інформаційних воєн

Головні завдання інформаційних воєн:

– дискредитація фактів історичної, національної ідентичності народу; зміна системи цінностей, що визначають світогляд і спосіб життя людей;

– створення у конкурента або суспільстві ворога атмосфери безсилля, негативного відношення до культури та історичної спадщини;

– маніпулювання громадською думкою і політичною орієнтацією мешканців держави з метою створення політичного напруження та стану, близького до хаосу;

– дестабілізація політичних відносин між партіями, об'єднаннями та рухами для створення конфліктів, розповсюдження недовіри, підозри, ескалації ворожнечі, гоніння за владою;

– провокація соціальних, політичних, національно-етнічних та релігійних конфліктів;

– провокації, застосування репресивних дій зі сторони влади по відношенню до опозиції ;

– пониження ступеня інформаційного постачання органів влади та управління, підбурювання неправильних управлінських рішень;

– ввід в оману громадськість про роботу структур державної влади, підриваючи їх авторитет, дискредитуючи їх дії;

– створення страйків, масових заворушень, інших проявів невдоволення та непокори;

– підрив авторитету на міжнародній арені певної держави, перешкоджання її співпраці з іншими державами;

– створення чи зміцнення опозиційних груп або рухів;

– применшення та знецінення визнаних світових наукових та технічних успіхів або інакших сферах, гіперболізація ролі помилок, недоліків, результату некоректних дій та некваліфікованих урядових рішень;

– створення у населення передумов до економічної, духовної чи військової поразки, залякування до боротьби та неможливості перемоги;
– представлення певного способу життя як поведінки та світогляду майбутнього, за яким неодмінно слідують інші народи;
– зниження морального духу населення та, відповідно, загальної обороноздатності і бойового потенціалу;
– здійснення іншого деструктивного ідеологічного впливу;
– заподіяння збитків системі безпеки інформаційно-технічної інфраструктури (машинно-технічним засобам, програмному забезпеченню, засобам та режиму захисту від несанкціонованого витоку інформації);
– захист від іншого деструктивного і інформаційно-психологічного та інформаційно-технічного впливу.[2]

Головним завданням інформаційної війни між державами є здійснення безпосереднього негативного деструктивного впливу на політичну силу держави за допомогою зменшення його майбутніх та фактичних можливостей щодо забезпечення власної безпеки, заподіяння складнощів у внутрішньому розвитку й проведенні активної зовнішньої діяльності, а також у підтриманні міжнародних відносин, умисне погіршення політичного іміджу, тобто зменшення впливу правлячої еліти, утвореної нею соціально-політичного режиму або допомога у вилученні її з органів державної влади.

Важливе місце посідає визначення об’єктів інформаційної війни. Об’єктом можна назвати те до чого спрямована конкретна діяльність, – те, на що, з метою отримання позитивного для себе результату, намагається впливати суб’єкт інформаційної війни. Таким чином, основний об’єкт, на якому базується особистий інформаційний деструктивний вплив у рамках заходів інформаційної війни, є суспільна громадська думка та свідомість окремої людини.

Кожна автоматизована система завдяки стрімкому розвитку мереж перетворилася на потенційну мету вторгнення. Сьогодні, будь-яка людина, яка розуміється в комп’ютерах, може стати «борцем» у мережі, беручи участь у

інформаційній війні, адже інформаційні технології стають дедалі більш актуальними для життя людей.

Беручи до уваги комбінації попередніх тверджень, можна виділити інформаційну війну як фактор захисту інформації, систем та телекомунікацій. Інформаційні воїни, кібер-воїни, техно-шпигуни, онлайн терористи роблять нові виклики для кожного, хто під'єднується до Інтернету, або займається відвідуванням та підтримкою вільного простору для обміну інформацією та навчання.[14]

Слід пам'ятати, що ці армії інформаційних воїнів дивляться на цілі, представлені в Інтернеті, і головними з них є комерційні або невійськові. Вони мають фінансування та визначені цілій, і вони розробляють плани та складні прикладні програми для нападу на інформаційну інфраструктуру країни, що включає в себе ту, що знаходяться в Інтернеті.

«Війна» за визначенням, що вживаються у більшості країн світу є «наявність збройної боротьби між декількома державами». Тобто, інформаційна війна являє собою боротьбу між державами з використанням виключно інформаційного озброєння, тобто інформаційних технологій, які базуються на промисловому виробництві, розповсюдженні та нав'язуванні інформації.

Інформація оцінюється за ступенем зміни знань, тобто це означає, що інформаційна зброя в першу чергу пов'язана і направлена на промислове виробництво, розповсюдження і впровадження знання навчально спроможних інформаційних систем,.

Цікаво що, інформаційні битви цілком можуть протікати в «мирний» час, тобто без використання якихось інших видів озброєнь. Враховуючи вище сказане, принципової різниці між термінами «інформаційна війна» і «інформаційне протиборство» або «інформаційна боротьба» немає.

Термін «інформаційна війна» в українських джерелах

В українських наукових джерелах термін «інформаційна війна» був вперше застосований у 1997 році. З цього моменту вживаність терміну швидко набирала популярності завдяки активному розвитку інформаційних систем.

Українське законодавство згідно з рішенням Ради національної безпеки і оборони України від 29 грудня 2012 року надало наступне визначення: «інформаційна війна – форма протиборства між суб'єктами (державами, блоками, партіями тощо), що передбачає інформаційний вплив на населення з використанням засобів масової інформації, комп'ютерних мереж тощо з метою формування відповідної суспільної думки, підриву морального духу як усього суспільства, так і окремих його інституцій».[5]

1.4 Дослідження динаміки використання терміну «Інформаційна Війна» та «Information Warfare»

Під час роботи було досліджено динаміку зміни кількості використань терміну «інформаційна війна» в українських наукових публікаціях з часом, а також динаміку зміни кількості використань англійської варіації терміну - «Information Warfare». Серед найбільш поширених n-грам даних термінів використовувались найбільш часто вживані. Для дослідження використовувались такі сервіси: JSTOR, Google Scholar та ScienceDirect. Дані сервіси є одними з найбільших онлайнових сервісів з величезною базою даних наукових публікацій, журналів, книг.

Опис сервісів

Google Scholar — вільна доступна пошукова система, яка індексує повний текст наукових публікацій всіх форматів і дисциплін. Індекс Google Scholar включає в себе більшість рецензованих онлайн-журналів найпопулярніших наукових видавництв Європи та Америки.

Google Scholar - це пошукова система, яка спеціалізується на індексації наукових публікацій (статей, книг, препринтів та іншого). Як і універсальна пошукова система Google, Google Scholar повідомляє користувачеві назву, частину тексту і посилання на документ.

Робот Google Scholar переходить тільки на ті сайти, що мають відношення до науки, і збирає у свій індекс інформацію про місцезнаходження і зміст наукових робіт. У базу даних потрапляє інформація про безкоштовні повнотекстові статті, та такі ресурси, у яких доступні лише реферати або бібліографічні описи.

На сьогодні, за даними дослідників, Google Scholar містить близько 400 мільйонів документів, враховуючи статті, цитати та патенти, саме це робить дану пошукову систему найбільшою у світі науковим пошуковим центром. Інші статистичні оцінки, щ обули раніше опубліковані в PLOS ONE з вживанням методу Mark і Recapture, визначили охоплення в приблизно 80–90% всіх статей, опублікованих англійською мовою, з розміром в 100 мільйонів.

Онлайнова база даних **JSTOR** (від «Journal Storage») - політематичний архів електронних копій зарубіжних наукових журналів і книг, серед яких переважають англомовні видання (але також присутня велика кількість видань на різних європейських мовах) .

До складу бази даних JSTOR в першу чергу долучаються такі журнали, які:

- виписуються великою кількістю університетів

- мають високий індекс цитування
- рекомендовані фахівцями у певних областях
- існують якийсь час

Саме тому, основний склад ресурсу - авторитетні академічні видання з багатою історією. Тут не вийде знайти масові або науково-популярні журнали, про що говорить і підзаголовок ресурсу: Scholarly Journal Archive (науковий архів журналів).

Цифрова база даних JSTOR надає доступ до більш ніж 12 мільйонів наукових журналів, книг та первинних джерел у 75 дисциплінах.

ScienceDirect - сайт, який надає платний доступ до повного тексту наукових публікацій. Цей ресурс має одну з найбільших колекцій наукових досліджень, що доступна онлайн. Запущений сервіс у березні 1997 року. Засновниками є видавництво Elsevier. Містить майже 3500 наукових журналів і 34 000 електронних книг [2].

Журнали згруповано в чотири основні розділи:

- фізичні та інженерні науки;
- природні науки;
- медичні науки;
- громадські та гуманітарні науки.

Короткий зміст більшості публікацій доступно безкоштовно. Для доступу до повних текстів публікацій (в форматі PDF, або в форматі HTML для сучасних публікацій), необхідно оформлення платної підписки або оплата за тимчасовий перегляд.

Результати аналізу вживаності терміну інформаційна війна серед україномовних джерел

Для дослідження україномовних джерел було обрано період під час якого вперше у наукових роботах за даними Google Scholar був згаданий термін

«Інформаційна війна», а саме 1998-2018 роки. Пошукова система Google Scholar була використана, адже тільки в ній міститься база україномовних публікацій. В результаті була складена таблиця з динамікою використання даного терміну за обраний період.

Таблиця 1.1 – Таблиця кількості використаннь терміну «інформаційна війна» з часом

Рік	Google Scholar
1998	3
1999	2
2000	3
2001	3
2002	1
2003	7
2004	14
2005	9
2006	15
2007	9
2008	35
2009	61
2010	70
2011	75
2012	74
2013	105
2014	234
2015	364
2016	296
2017	313
2018	219

Для того щоб отримати уявлення про динаміку розповсюдження терміну, на основі даних (таблиця 1.1) побудовано графік (рисунок 1.1). Також на рисунку 1.2, на основі даних сервісу Google Books Ngram Viewer можна

побачити частотність вживання терміну «інформаційна війна» по відношенню до всіх друкованих видань.

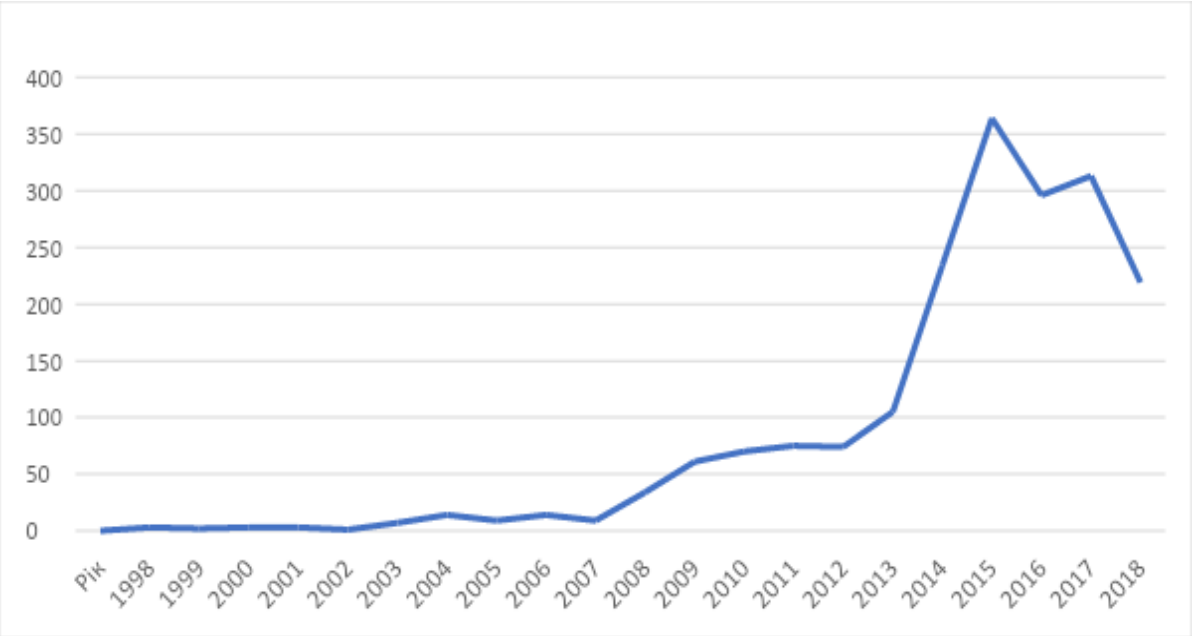

Рисунок 1.1 – Динаміка вживаності терміну «інформаційна війна» за даними Google Scholar

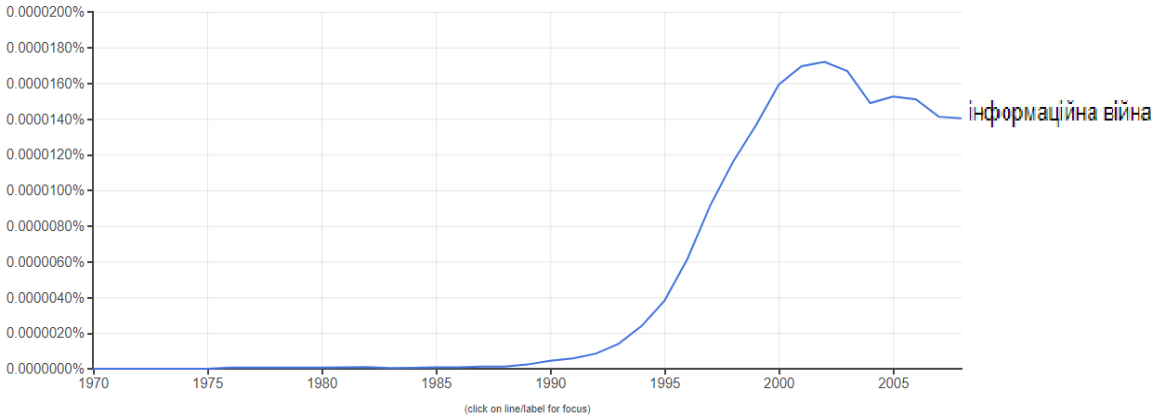

Рисунок 1.2 – Динаміка вживання терміну «інформаційна війна» серед друкованих видань за даними Google Books Ngram Viewer

Як можемо побачити з рисунку 1.1, з моменту першої згадки у 1998 році до 2007 року, був дуже повільний ріст вживаності даного терміну. Під час останніх 10 років, термін «інформаційна війна» значно частіше зустрічався в українських наукових публікаціях, що зумовлене значним розвитком інформаційних систем в Україні.

Результати аналізу вживаності терміну Information Warfare серед англгломовних джерел

Для дослідження англомовних джерел були використані сервіси Google Scholar[20], JSTOR[21] та Sciencedirect[22]. Були обрані варіації терміну «Information Warfare» (наприклад «Information War» тощо), які зустрічаються у наукових публікаціях найчастіше.

Таблиця 1.2 – Таблиця динаміки вживання терміну «Information War» з часом

Рік	Google Scholar	JSTOR	Sciencedirect
1998	141000	2625	3409
1999	169000	2986	2964
2000	182000	3841	3144
2001	206000	4186	3812
2002	235000	4811	3265
2003	253000	5291	3784
2004	299000	5869	3812
2005	308000	6679	4253
2006	317000	7088	4617
2007	315000	8504	4073
2008	313000	9002	5303
2009	311000	10442	5286
2010	366000	10834	4999

Продовження таблиці 1.2

Рік	Google Scholar	JSTOR	Sciencedirect
2011	329000	11583	5245
2012	364000	12950	5744
2013	412000	14199	6198
2014	321000	13953	6539
2015	269000	13724	7643
2016	258000	12448	7126
2017	159000	11899	7030
2018	145000	11690	7419

Для того щоб отримати уявлення про динаміку розповсюдження терміну, на основі даних (таблиця 1.2) побудовано графік (рисунок 1.3). Також на рисунку 1.4 можна побачити частотність вживання терміну «Information war» по відношенню до всіх друкованих видань.

Враховуючи кардинальну відмінність у розмірах баз даних обраних сервісів, побудований графік показує відсоткове відношення вживань терміну у конкретний рік в порівнянні з загальною кількістю використання у заданому сервісі.

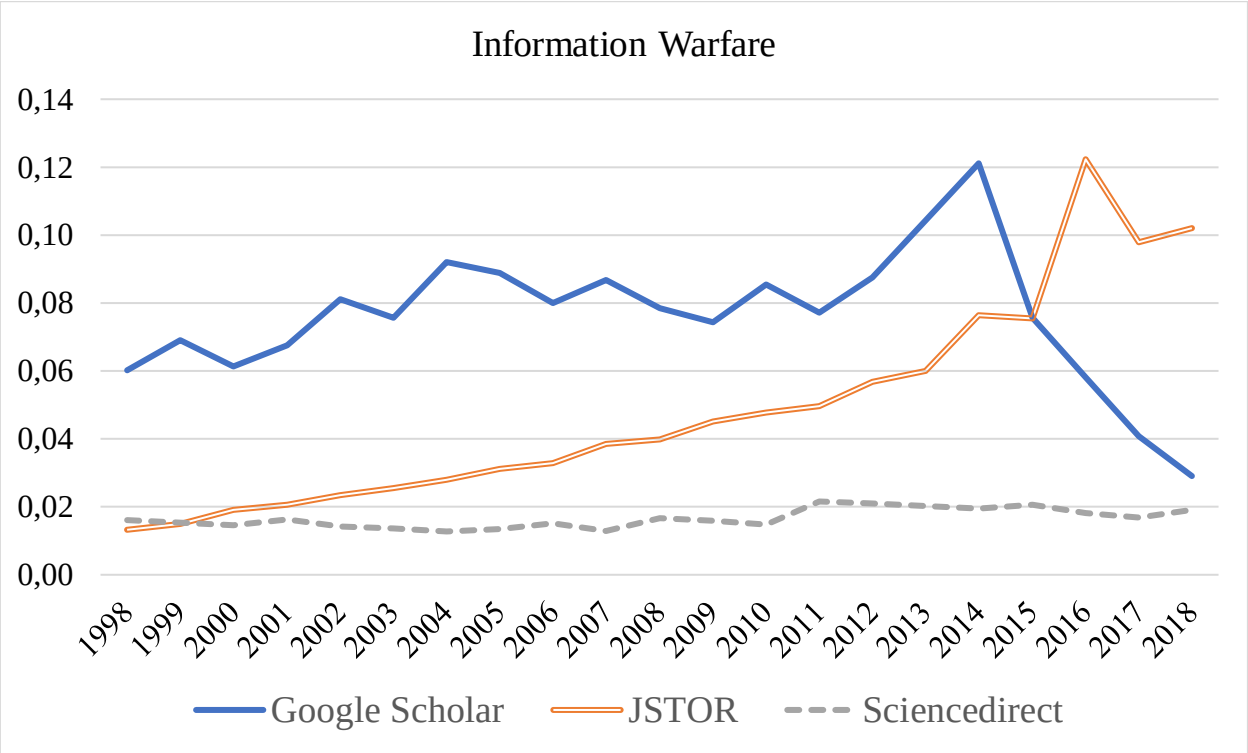

Рисунок 1.3 – Динаміка вживання терміну «Information Warfare» за даними Google Scholar, JSTOR та Sciencedirect у відсотковому значенні до загальної кількості публікацій

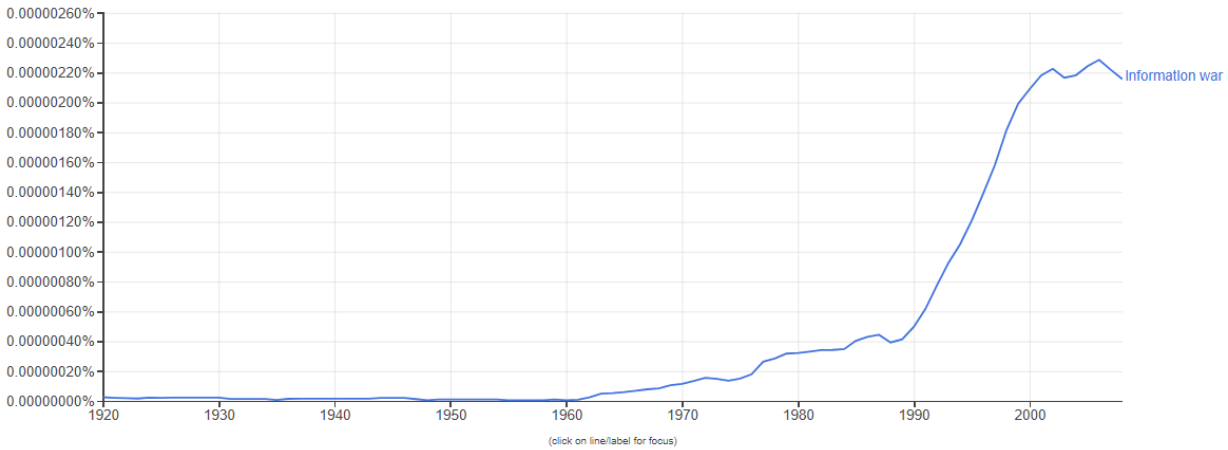

Рисунок 1.4 – Динаміка вживання терміну «Information War» серед друкованих видань за даними сервісу Google Books Ngram Viewer

У наведеній вище таблиці (таблиця 1.2) Можна побачити статистику по використанню англомовного варіанту терміну з сервісів Google Scholar, JSTOR та Sciencedirect, щодо використання англомовного терміну «Information Warfare», або спорідненого по значенню з ним, наприклад “information war”, для аналізу використовувалась найбільш поширена варіація терміну в період 1998 – 2018 років.

Судячи з частоти використання даного терміну, можна зазначити що вже впродовж останніх 50 років, за даними сервісу Google Scholar, термін є невід’ємною частиною наукового світу і регулярно згадується в наукових публікаціях. Однак з 2014 року, термін «Information Warfare» значно втратив свою популярність серед друкованих наукових видань, це можна побачити зі статистики по даним сервісу Google Scholar. За даними інших сервісів, термін «Information Warfare» та споріднені з ним, регулярно набирають популярності серед наукового світу. На рисунку 1.4 бачимо порівняння динаміки вживання з цих трьох сервісів.

1.5 Дискредитація

Одним з ключових методів ведення інформаційної війни є дискредитація. Дискредитація це удар по довірі. Усі навмисні дії дискредитації спрямовані на погіршення іміджу, авторитету і довіри. В інших випадках це може називатись недобросовісною конкуренцією. Доволі часто дискредитаційні дії можна помітити на політичній арені, де, наприклад, якомусь конкретному суспільному чи політичному діячові відмовляють у надаванні допомоги або похитують довіру людей.

Під час проведення публічних дебатів у демократичних громадах дискредитація конкурентів використовується для отримання підтримки та посилення власної позиції. Ця тактика покликана завдавати шкоди громадськості. Трапляється таке, коли певний чиновник діє таким чином щоб

підірвати гідність та авторитет органів влади в очах населення, задля дискредитації влади. Іноді це можуть кваліфікувати як зловживання службовим становищем або владою.

Кожна область, у якій застосовується дискредитація, спрямована на підрив довіри і авторитету суперника. Зараз під час дискредитації використовуються такі методи, як образа, обман, приниження, використовуються всі спроби щоб довести у підсвідомість людей думки про некомпетентність суперника. Втім дискредитація може бути не тільки мовою. Щоб підірвати довіру або авторитет, інколи вистачає виявлення негативних фактів, думок, компроматів. Висміювання можна віднести до різновиду лінгвістичної дискредитації. За думкою вчених, найефективніших результатів досягає саме мовна стратегія.[13]

Завдяки вмінню відрізняти явні маніпуляції і наклеп від звичайних громадян, дискредитація будь-якої конкретної особи не така продуктивна на сьогодні. Зараз політики або громадські діячі не прагнуть дискредитувати своїх суперників, втім вони докладають зусиль щоб піднести деякі установки або ідеї таким чином, щоб у людській підсвідомості могло скластися певне негативне сприйняття до всього, що раніше можна було вважати традицією чи частиною культури. Застосовується такого роду маніпуляція людською свідомістю.

Лінгвістична дискредитація може бути таких типів: когнітивна, семантична і риторична. Метою когнітивної стратегії є допомога адресатові в процедурі інтерпретації самої інформації (прийняти, пов'язати з вже відомим і усвідомленим як власних знанн), а потім перейти до висновків і узагальнень. Як частина стратегії дискредитації когнітивного типу, намічений план підриву довіри до влади реалізується шляхом введення інформації в розум адресата, зміст якого є свого роду звинуваченням «опонента» у невиконанні політики. Наприклад, показ реакції політиків на сумні наслідки природних явищ. При застосуванні семантичної стратегії використовується якість мовних засобів, за допомогою організації мовленнєвого висловлювання та привернення уваги.

Для ефективнішого залучення уваги і переконання, використовується риторична стратегія, в межах якої використовують різноманітні засоби ораторського мистецтва та риторичні техніки дієвого впливу на адресата, за рахунок надмірного привертання уваги.

Результати аналізу вживаності терміну «дискредитація» серед україномовних джерел

Було обрано період дослідження 1996-2018 років. За допомогою Google Scholar, в результаті, була складена таблиця по використанню терміну «дискредитація» за обраний період.

Таблиця 1.3 – Таблиця кількості вживання терміну «дискредитація»

Рік	Google Scholar
1996	57
1997	105
1998	115
1999	155
2000	189
2001	229
2002	268
2003	319
2004	347
2005	479
2006	645
2007	748
2008	895
2009	1070
2010	1120
2011	1380
2012	1370
2013	1680

Продовження таблиці 1.3

Рік	Google Scholar
2014	1900
2015	2180
2016	2230
2017	2560
2018	2610

Для того щоб мати уявлення про динаміку розповсюдження терміну, на основі зібраних даних (таблиця 1.3) з сервісу Google Scholar побудовано графік (рисунок 1.5). Також на рисунку 1.6 можна побачити частотність вживання терміну «інформаційна війна» по відношенню до всіх друкованих видань.

Рисунок 1.5 – Динаміка вживання терміну «дискредитація» за даними Google Scholar

Рисунок 1.6 – Динаміка вживання терміну
«дискредитація» за даними Google Ngram Viewer

Як можемо бачити, дані з рисунку 1.6, отримані за допомогою Google Ngram Viewer, показують, що перші згадки терміну «дискредитація» були ще у 1921 року і з того моменту регулярно вживався, а за даними Google Scholar після 2004 року відбувся різкий скачок популярності даного терміна. Адже дискредитація інформаційного суспільства стала невід'ємною частиною сучасного життя.

Результати аналізу вживаності терміну «Discreditation» серед англомовних джерел

Було обрано період дослідження 1996-2018 років. За допомогою використання онлайн баз даних сервісів Google Scholar, JSTOR, Sciencedirect. В результаті була складена таблиця 1.4 по використанню даного терміну за обраний період.

Таблиця 1.4 – Таблиця динаміки вживання терміну «Discreditation» з часом

Рік	Google Scholar	JSTOR	Sciencedirect
1996	1670	1419	387
1997	1720	1476	360
1998	1990	1428	346
1999	2150	1421	342
2000	2300	1460	466
2001	2320	1594	391
2002	2610	1657	403
2003	2770	1591	456
2004	3380	1671	489
2005	3600	1706	510
2006	3610	1796	585
2007	4020	1893	613
2008	4150	1883	581
2009	4520	2089	630
2010	4730	2094	629
2011	4890	2114	566
2012	5140	2240	656
2013	5870	2278	725
2014	5310	1970	756
2015	5180	1941	875
2016	5350	1402	742
2017	5020	1297	790
2018	4840	1200	760

На основі даних з наведеної вище таблиці 1.4, побудовано графіки 1.7 – 1.8 для отримання представлення про динаміку використання терміну,на рисунку 1.9 можна побачити частотність вживання терміну «Discreditation» по відношенню до всіх друкованих видань

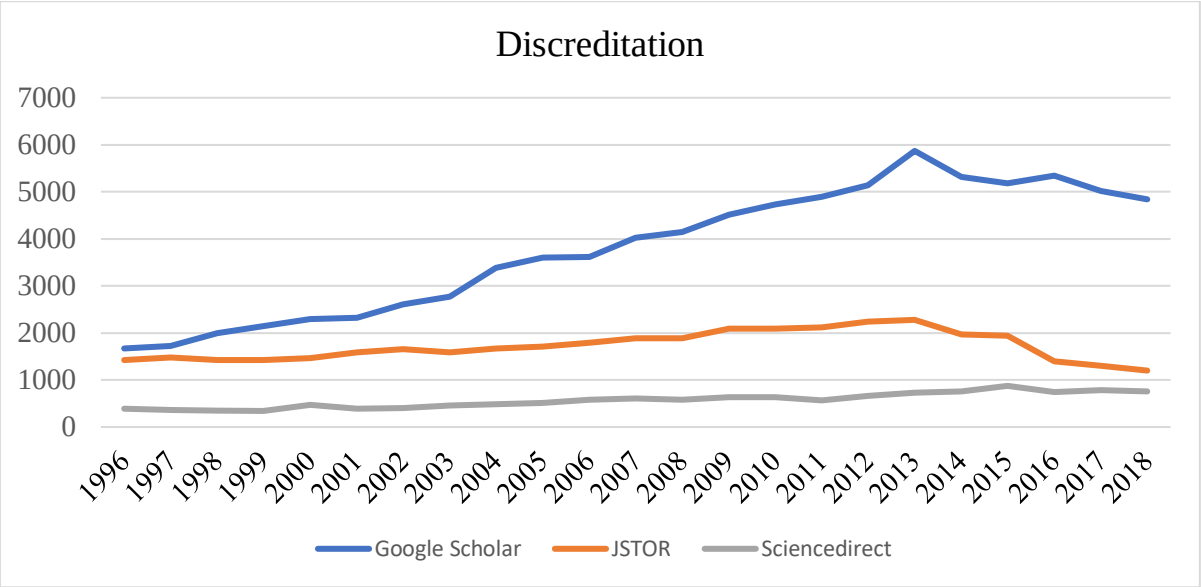

Рисунок 1.7 – Динаміка вживання терміну «Discreditation» за даними Google Scholar, JSTOR та Sciencedirect

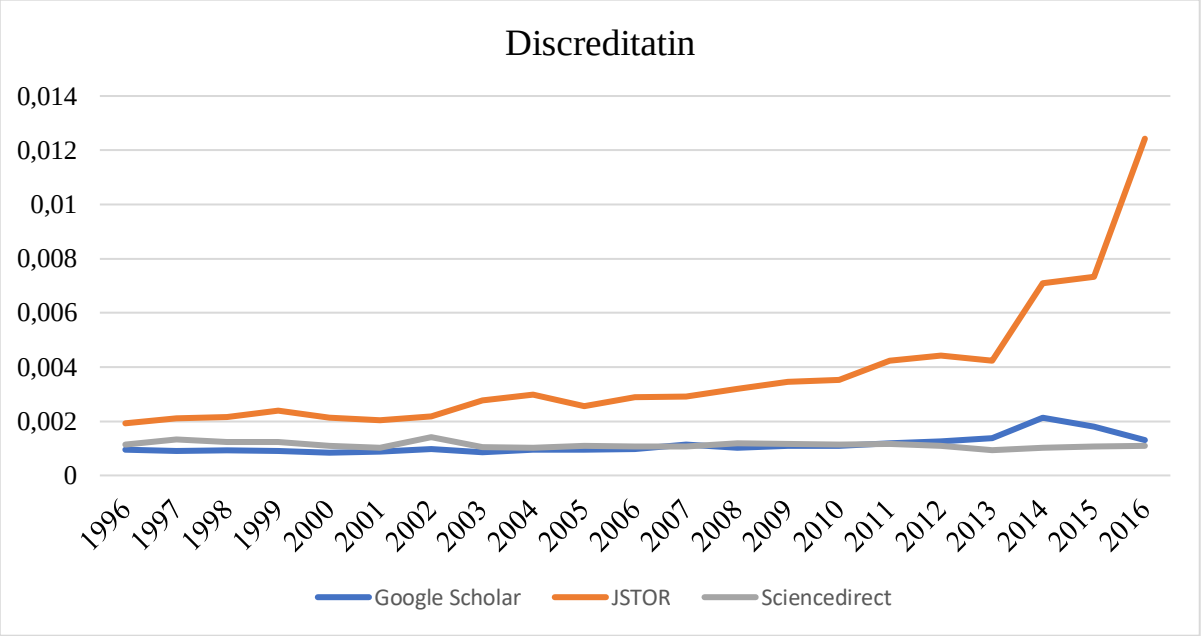

Рисунок 1.8 – Динаміка вживання терміну «Discreditation» за даними Google Scholar, JSTOR та Sciencedirect у відношенні до загальної кількості публікацій

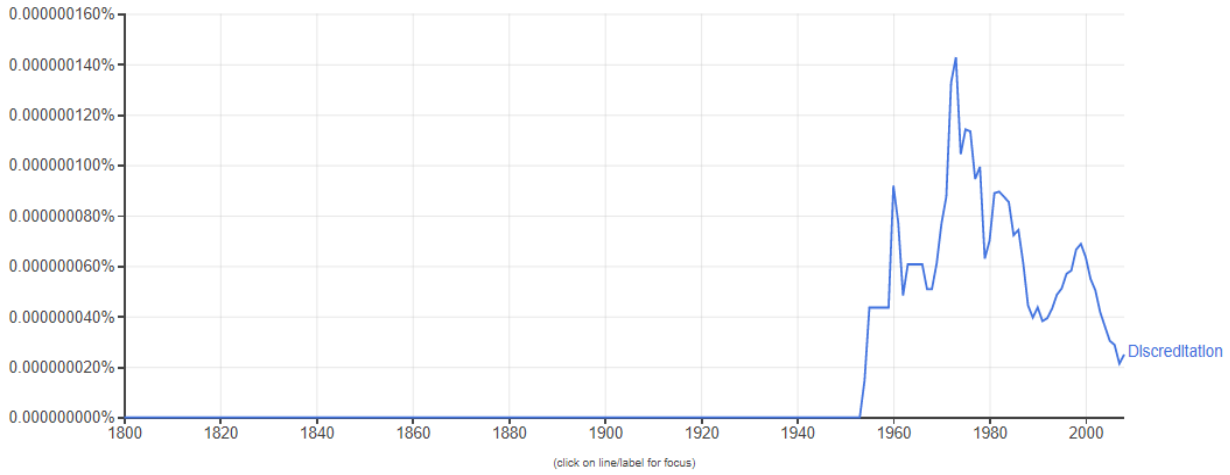

Рисунок 1.9 – Динаміка вживання терміну
«Discreditation» за даними Google Ngram Viewer

У таблиці 1.4 наведено дані з сервісів Google Scholar, JSTOR та Sciencedirect щодо використання англомовного терміну «*Discreditation*» в період 1996 – 2018 років. Варто помітити, що за даними сервісу Google Scholar, термін «*Discreditation*» вперше був використаний ще більше 70 років назад і, слід зауважити, що за даними сервісу JSTOR та ScinceDirect, у 1960 році даний термін вже дуже активно використовувався у наукових статтях та журналах. Також, враховуючи різницю між об'ємами баз даних цих трьох сервісів, побудований графік (рисунок 1.8), показує відсоткове відношення кількості вживаності терміну до загальної кількості публікацій.

1.6 Інформаційні операції

Під час дослідження поняття «інформаційна війна» та «дискредитація» не можна ігнорувати головну складову інформаційної війни.

Інформаційні операції – це комплексне використання основних можливостей операцій впливу, операцій з електронної боротьби, операцій з ведення мережної війни, узгоджених із зазначеними інтегрованими засобами

контролю, для впливу, порушення, корумпованості чи узурпування змагального людського та автоматизованого прийняття рішень, захищаючи власні.

Вплив інформаційних операцій

Використання можливостей впливати на поведінку, захищати операції, повідомляти наміри командира і проектувати точну інформацію для досягнення бажаних ефектів у когнітивному домені. Ці наслідки повинні призвести до різної поведінки або зміни циклу супротивного рішення, що узгоджується з цілями командира.

Операції впливу спрямовані на вплив сприйняття та поведінку лідерів, груп або цілих груп населення. Операції впливу використовують можливості впливати на поведінку, захищати операції, повідомляти про наміри командира і проектувати точну інформацію для досягнення бажаних ефектів у когнітивному домені. Ці наслідки повинні призводити до різної поведінки або зміни циклу прийняття рішення супротивника, який узгоджується з цілями командира. Військовими можливостями операцій впливу є психологічні операції (PSYOP), військовий обман (MILDEC), операційна безпека (OPSEC), операції контррозвідки (CI), операції контрапропаганди і державних справ (PA).

Психологічні операції, орієнтовані на когнітивний простір бойового простору, орієнтується на розум супротивника. Загалом, PSYOP прагне викликати, вплинути або посилити сприйняття, ставлення, міркування і поведінку іноземних лідерів, груп і організацій у спосіб, сприятливий для дружніх національних і військових цілей. PSYOP підтримує ці цілі шляхом розрахунку використання повітря, космосу та IO з особливим акцентом орієнтації на психологічні ефекти. В операційному відношенні він надає ефективні і універсальні засоби використання психологічної вразливості

ворожих сил для створення страху, плутанини і паралічу, що підриває їхній моральний дух і бойовий дух.

Військовий обман Військовий обман (MILDEC) вводить в оману або управляє сприйняттям супротивників, змушуючи їх діяти відповідно до дружніх цілей. Військовий обман не буде навмисно націлювати або вводити в оману громадськість США, Конгрес або засоби масової інформації.

Безпека операцій Безпека операцій (OPSEC) - це діяльність, яка допомагає запобігти нашим противникам отримати та використовувати критичну інформацію. OPSEC не є сукупністю конкретних правил і інструкцій, які можна застосовувати до кожної операції, це методологія, яка може застосовуватися до будь-якої операції або діяльності з метою заперечення критичної інформації противнику. Критична інформація складається з інформації та показників, які є чутливими, але не класифіковані. OPSEC має на меті визначити будь-яку некласифіковану діяльність або інформацію, яка, проаналізована з іншими видами діяльності та інформацією, може виявити захищені та важливі дружні операції, інформацію або діяльність.

Контррозвідувальна контррозвідка (КІ) визначається як зібрана інформація та заходи, що проводяться для захисту від шпигунства, інших розвідувальних заходів, саботажу або вбивств, що здійснюються іноземними урядами або їхніми сторонами, іноземними організаціями або іноземними особами або міжнародною терористичною діяльністю.

Контр-пропагандистські операції - це діяльність по виявленню і протидії пропаганді противника і викриванню супротивних спроб впливати на дружнє населення і розуміння ситуації збройних сил. Вони включають ті зусилля, щоб звести нанівець, нейтралізувати, зменшити наслідки або отримати перевагу від іноземних психологічних операцій або пропагандистських зусиль. Численні організації та можливості (наприклад, діяльність ISR, державні справи або інші військові підрозділи та командири) можуть ідентифікувати змагальні пропагандистські операції, які намагаються вплинути на дружні населення та військові сили. Командири всіх рівнів повинні об'єднувати діяльність,

спрямовану на поширення правдивої інформації; пом'якшити протидійні повідомлення; і порушувати, деградувати і відключати психологічні операції противника.

Операції з громадськістю Командири проводять операції з ПА, щоб оцінити інформаційне середовище в таких сферах, як громадська думка, та визнати політичні, соціальні та культурні зрушення. Операції з державними справами є ключовим компонентом інформаційних гнучких варіантів стримування і розбудовують прогнозну обізнаність командирів міжнародного суспільного інформаційного середовища та засоби використання інформації для здійснення наступальних і попереджувальних оборонних дій в операціях ВПС.

Операції з державними справами є головною діяльністю і першою лінією захисту від пропаганди та дезінформації суперника. Фейки легко ідентифікувати, коли істина добре відома. Операції з державними справами повинні координуватись і деконфікуватися з іншими діями операцій впливу, оскільки комунікаційні технології можуть надавати інформацію одночасно доступній для вітчизняної та міжнародної аудиторії. Операції з державних справ ніколи не повинні використовуватися для того, щоб ввести в оману громадськість, національних лідерів або ЗМІ.

Сучасний стан систем масових комунікацій надає можливість доведення інформаційних повідомлень в різних форматах практично до будь-якої людини. Це створює умови для ефективного проведення інформаційних операцій через різні канали поширення інформації.

Головні особливості інформаційних операцій

Інформаційна операція – це взаємопов’язана послідовність інформаційних впливів для досягнення поставленої мети.

Особливості інформаційних операцій:

- дозволяють приховати факт їх проведення, але при цьому отримати цільовий ефект;
- ефект від їх проведення реальний (зміна курсу акцій компанії, активні дії частини населення, зниження довіри до політичного або громадському діячеві);
- можуть бути не автономної акцією, а частиною великої кампанії, проведеної, в тому числі, і в інших, неінформаційних сферах;
- істотно менша вартість досягнення цілей в порівнянні з традиційними засобами (військовими, організаційними, політичними та ін.).

1.7 Фейки

Поширення фейків - це один із видів інформаційних операцій – взаємопов’язаних послідовностей інформаційних впливів для досягнення поставленої мети. Вони дозволяють приховати факт їх проведення, але при цьому отримати цільовий ефект, мають низку вартість проведення, ефект від їх проведення реальний (зміна курсу акцій компанії, активні дії частини населення, втрата довіри до політичного або громадського діяча). Фейкова новина спонукає до різкої розбіжності думок, різного роду конфліктів, включаючи політичні.

Сьогодні, мало не кожен день на екранах телевізорів, у стрічках новин можна зустріти слово «фейк» . Цей термін увібрав в себе різноманіття інтерпретацій. Зазвичай, під терміном «фейк» (англ. fake – підробка) розуміють перекручену неправдиву інформацію. Втім слід зрозуміти правильний сенс цього слова, фейк – це брехня, підробка, фальсифікація, яка розповсюджується цілеспрямовано для того, щоб дезінформувати та ввести в оману певну аудиторію.

Термін «фейкові новини» «Вікіпедія» трактує як повністю або частково вигадану інформацію про суспільні події, явища, певних осіб, яка подається в

ЗМІ під виглядом справжніх журналістських матеріалів. Часто носять гумористичний або сатиричний характер і створюються з метою висміювання або привернення уваги до важливих суспільних проблем чи тенденцій [11]. Запропоноване визначення фейкової інформації більше Тобто таке визначення фейкової інформації має позитивний і розважальний характер. Однак у сучасних українських соціальних медіа, фейкова інформація спрямована на дезінформацію, дискредитацію, введення в оману аудиторії, що в кінцевому

Зараз фейком може бути будь-що, відредаговані фото, штучно змонтовані відеоролики, написані або вигадані неправдиві новини, які важко відрізнити від правдивих. Ще фейками вважають заведені акаунти неіснуючих людей у соціальних мережах, через які поширюється недостовірна інформація. Основною метою фейкових повідомлень як інструмента інформаційної війни – це змусити людей сумніватися, запевнити аудиторію в правдивості поданої інформації. Задача стоїть в дезінформуванні аудиторії; сприянні розвитку власного бачення, політики або позиції; спричиненні агресію; похитнути позицію індивіда та вимусити його сумніватися; розповсюдженні паніки; редагування мислення аудиторії; індукування певної дії; підвищення увагу й зацікавленості аудиторії; запевнення аудиторії використанням вигаданих фактів; залякуванні аудиторії тощо.

Враховуючи вище сказане слід зробити наступне визначення фейку. Фейк – це навмисно змінена новина, подія чи журналістська публікація, що включає в себе неправдиву або спотворену інформацію, що дискримінує певну особу чи групу людей в очах аудиторії.

Як вже зазначено, фейками можуть бути фото, відео, новини, сторінки в соціальних мережах, створені від імені неіснуючої/іншої людини, програми, сайти, створені під виглядом відомих ресурсів з метою фішингу тощо. Виявити брехливість інформації, яку несе в собі фейк, набагато легше, якщо дотримуватися принципу обов’язкової перевірки і повторної перевірки інформації, що надходить в конкретне медіа за принципом «точність

важливіше швидкості». Істотним фактором оцінки достовірності інформації є той канал комунікації, за допомогою якого вона надійшла до редакції.

Висновки до розділу 1

У цьому розділі були оглянуті вже існуючі матеріали з обраної тематики: статті, книги та дослідження. Після цього був проведений детальний аналіз таких термінів як «дискредитація» та «інформаційна війна», для цього були побудовані таблиці та графіки, які відображають динаміку використання україномовного та англомовного варіантів термінів у наукових публікаціях, журналах та книгах.

В українських наукових джерелах дослідження терміну «інформаційна війна» вперше з’явились менш ніж 25 років назад. В цей же час міжнародна наукова спільнота вже регулярно використовувала та досліджувала інформаційну війну, як новітню загрозу майбутнього.

Термін «дискредитація» зазнає все більшої актуальності серед українського суспільства, адже в умовах гібридної війни, Україна піддається неабиякому впливу зі сторони агресора і тому необхідно чітко розуміти методи та інструменти ведення інформаційної війни.

2 ПРОВЕДЕННЯ АНАЛІЗУ НОВИН В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

2.1 Ідея та методика дослідження

Український інформаційний простір сьогодні зазнає значного впливу, так як війна триває не тільки на території країни, але й в її інформаційному полі.

І хоча українці користуються російськими ЗМІ для отримання інформації все менше, в інформаційному полі залишаються медіа, кінцевими власниками яких є проросійські політики, бізнесмени, чи взагалі власник прихований і встановити вплив Російської Федерації на редакційну політику практично неможливо. Втім, через такі медіа і поширюється, в першу чергу, небезпечна риторика, автори якої знаходяться у країні, яка веде війну проти України. Кремлівську риторику, фейки можуть підхоплювати і інші ЗМІ, сприймаючи таку інформацію як «альтернативну точку зору», чи таку інформацію, яка підвищить клікабельність.

Найголовнішою перемогою тих, хто поширює дезінформацію, є саме підхоплення цих матеріалів найбільш популярними, головними мас-медіа, навіть, якщо це згадування відбувається у формі спростування. Посилення й поширення наративу є одними з основних цілей пропагандистів.

Процес розповсюдження фейків має властивості інформаційних операцій.

- Високий ступінь подібності текстів, не будучи повними дублікатами.
- Невеликий інтервал часу, в який відбувається їх опублікування. Це дозволяє імітувати появу нової значущої події.
- Джерела, які опублікували їх, є маловідомими, регіональними або спеціалізованими ЗМІ. Поява повідомлень у великих інформаційних агентствах можлива тільки під час пасивної фази.

Методика дослідження

Деяке повідомлення включає в себе повний текст, дату та час появи, джерело публікації в ЗМІ і значення тематичного класифікатора.

$$news_k =< c_k, t_k, Dj_j, < n_k1, n_k2, ..., n_k0 >>$$

$$n_k a = \begin{cases} 1, c_k \in e_a \\ 0, c_k \notin e_a \end{cases}$$

де:
c_k – текст $news_k$,
t_k – дата та час появи $news_k$,
Dj_j – джерело публікації,
$n_k a$ – індикатор відповідності $news_k$ темі e_a.

Оцінюється число повідомлень визначеного типу та змісту в певні проміжки часу. Якщо їх кількість більше порогового значення, робиться висновок про проведення інформаційної операції. На основі динаміки інформаційних потоків, динаміка кількостіі повідомлень під час проведення інформаційної операції змінюється за законом (рис. 2.1).

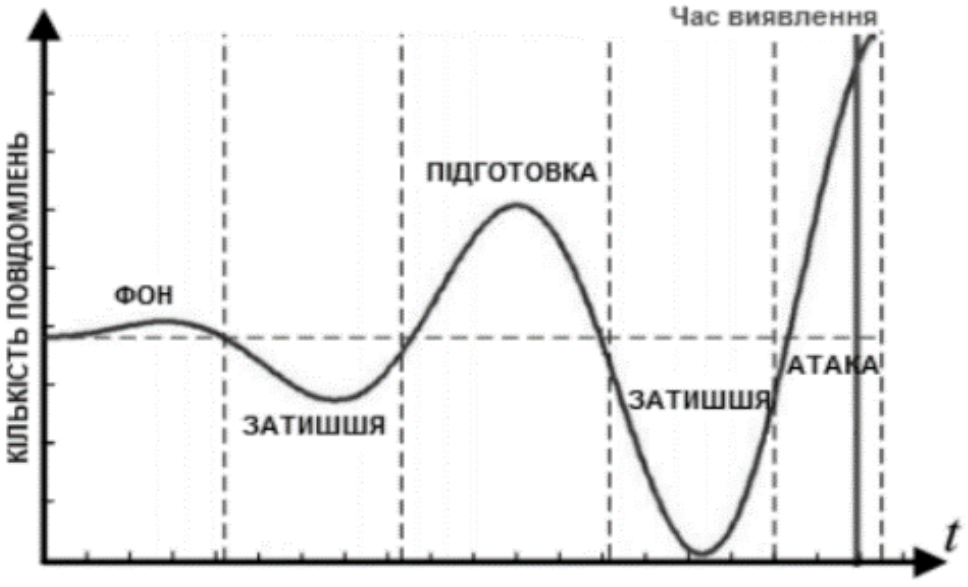

Рисунок 2.1 – Динаміка кількості тематичних повідомлень за обраний період.

Слід розглянути графову модель розповсюдження фейків, а саме: поширення фейку має певні етапи: фон (низький пошуковий попит за ключовими словами), попереднє затишшя, підготовка (незначний сплеск популярності запиту), затишшя, атака (значний сплеск запитові популярності новини), релаксація.

В роботі за допомогою використання інструментів веб-аналітики та парсингу новин новинної стрічки за обраний період я перевірив визначену модель вибраних мною новин на відповідність фейку.

Для дослідження було обрано три дискредитуючих новини-фейки, які були розповсюдженні російськими ЗМІ. Для того щоб дослідити ці новини необхідно було побудувати графіки зміни кількості запитів за кожною новиною (кількість за одиницю часу) і порівняти з запропонованим вище шаблоном на рисунку 2.1. У випадку їх збігу робиться висновок про факт проведення інформаційної операції.

Після цього є необхідним проведення детального контент аналізу кожної з цих новин для виявлення елементів дискредитації України. Для опрацювання статистичного матеріалу і отримання висновків використано методи Data/Text Mining, візуалізація даних, порівняльний аналіз, частотний аналіз, аналіз асоціацій, а також побудова діаграми «ящик з вусами».

2.2 Фейк №1

В якості першої фейк-новини я вибрав сюжет про «розп’яття хлопчика українськими військовими».

Як результаті проведеного дослідження було зібрано дані про кількість результатів щоденної пошукової видачі за запитами, що містили комбінації ключових слів: «военные», «ребенок», «распяли», «кровь», тощо. Було проведено попередній синтаксичний аналіз та аналіз релевантності отриманих

новин для виключення незадовільних або невідповідних за змістом результатів. Після опрацювання отриманих відомостей було побудовано графік динаміки кількості тематичних повідомлень за обраний період.

Рисунок 2.2 – Динаміка кількості тематичних повідомлень за обраний період

На рисунку 2.2 можна чітко виділити основні етапи проведення, інформаційної операції, які були наведені вище. Далі було проведено детальний контент аналіз.

Контент аналіз

Контент аналіз - це метод дослідження, який використовується для здійснення повторюваних і достовірних висновків шляхом тлумачення та кодування текстового матеріалу. Систематично оцінюючи тексти (наприклад, документи, усне спілкування та графіку), якісні дані можуть бути перетворені в кількісні дані. Хоча метод часто використовувався в соціальних науках, лише нещодавно він став більш поширеним серед організаційних вчених.

Аналіз контенту є цінним в організаційних дослідженнях, оскільки дозволяє дослідникам відновити і вивчити нюанси організаційної поведінки, сприйняття зацікавлених сторін і соціальних тенденцій. Це також важливий міст між суто кількісними і чисто якісними методами дослідження. З одного боку, аналіз вмісту дозволяє дослідникам аналізувати соціально-когнітивні та перцептивні конструкції, які важко вивчати за допомогою традиційних кількісних архівних методів. У той же час, це дозволяє дослідникам збирати великі зразки, які важко використовувати в суто якісних дослідженнях.

Незважаючи на те, що контент-аналітика все частіше використовуються дослідниками менеджменту як інструмент для аналізу тексту та якісних даних, багато дослідників не знайомі з різними методами аналізу контенту та способами вирішення проблем, властивих його застосуванням. Ці виклики включають пошук адекватних заходів, розробку проксі-словників і схем кодування, робота з текстами з різних джерел, забезпечення надійності та достовірності, а також проведення ручного та комп'ютерного аналізу вмісту.

Для проведення контент аналізу слід розібратися в термінології.

Водність – це відсоток вмісту в тексті, нічого не значущих слів, та слів що не несуть корисної інформації слів (стоп-слів). Максимально припустимим показником водності зазвичай вважають 60%.

Нудота тексту – це такий показник, що визначає частоту використання будь-якого слова в текстовому документі. Важлива не тільки частотність слів з ключової фрази , але і будь-яких інших слів, що вживаються в тексті.

Існує два показника нудоти, і розраховуються вони по-різному.

Показник класичної нудоти (ПКН)- це квадратний корінь з числа, що позначає частоту вживання слова в тексті.

$$\text{ПКН} = \sqrt{\text{ЧС}}\text{ , де}$$

ЧС – частота вживання слова,

ПКН – показник класичної нудоти.

Наприклад, якщо слово зустрічається в тексті 16 разів, його класична нудота дорівнює 4. При цьому обсяг тексту в розрахунок не береться.

Показник класичної нудоти не може бути меншим 2,64. Навіть якщо слово використано в тексті менше 7 разів, корінь квадратний в цьому випадку витягується з числа 7. Якщо показник вище цифри 7, текст може бути оцінений пошуковими системами як спам.

Академічна нудота документа – це відношення кількості повторів самого уживаного в документі слова до кількості слів у всьому тексті. Вона вимірюється у відсотках. Іншими словами, академічна нудота - це показник частотності.

Частотність – це процентний показник. Позначимо його буквою «Ч».. Тоді формула визначення частотності слова буде виглядати так:

$$КС: КСТ \times 100 = Ч\%, \text{ де}$$

КС – кількість повторень слова в різних формах (з урахуванням зміни відмінка, числа, роду),
КСТ – кількість слів у всьому тексті.

Сегодня ровно неделя с того дня, как киевские силовики вошли в оставленный ополченцами Славянск. Как раз этим временем датирована история, которую рассказала нам обитательница лагеря беженцев в Ростовской области. Она говорила о публичной казни. **Женщина** назвалась Галиной из Славянска, матерью четырёх **детей**, уроженкой Западной Украины, где недовольство родственников вызвало то, что её муж ушёл в ополчение. Разговор с Галиной оставил сложное чувство. Разум отказывается понять, как подобное вообще возможно в наши дни в центре Европы. Сердце не верит, что такое вообще возможно. "Центр **города**. **Площадь** Ленина. Наш Горисполком - это единственная **площадь**, куда можно согнать всех **людей**. На **площади** собрали **женщин**, потому что мужиков больше нет. **Женщины**, девочки, старики. И это называется показательная казнь. Взяли **ребенка** трех **лет** мальчика маленького с трусиках, в футболке, как Иисуса на доску объявлений прибили. Один прибивал, двое держали. И это все на маминых глазах. **Маму** держали. И **мама** смотрела, как **ребенок** истекает **кровью**. Крики. Визги. И еще взяли надрезы сделали, чтоб **ребенок** мучился. Там невозможно было. **Люди** сознание теряли. А потом, после того как полтора часа **ребенок** мучился и умер, взяли **маму**, привязали до танка без сознания и по **площади** три круга провели. А круг **площади** - километр". "Вам особенно после этого интервью, грозит большая опасность. Правильно ли я понимаю?" "Я как предатель Родины, потому что я родом из Закарпатской области. Меня же моя мать сказала: ты приедешь, я тебя сама **расстреляю**. И нацгвардия **расстреляет**. У меня две **расстрелянные** статьи. Я за себя не **боюсь**. Мне жалко **детей**. Если бы не **дети**, я бы взяла сама оружие и пошла в ополчение. Это не украинская армия, это не освободители, это твари. Они когда вошли в **город**, там ни одного ополченца не было. Они стреляли по **городу**. Мародерством занимались. У нас рассказывали бабушки старые, фашисты так не делали. Это группа СС "Галитчина". Они местные. Они над местными

Рисунок 2.3 – Мапа тексту

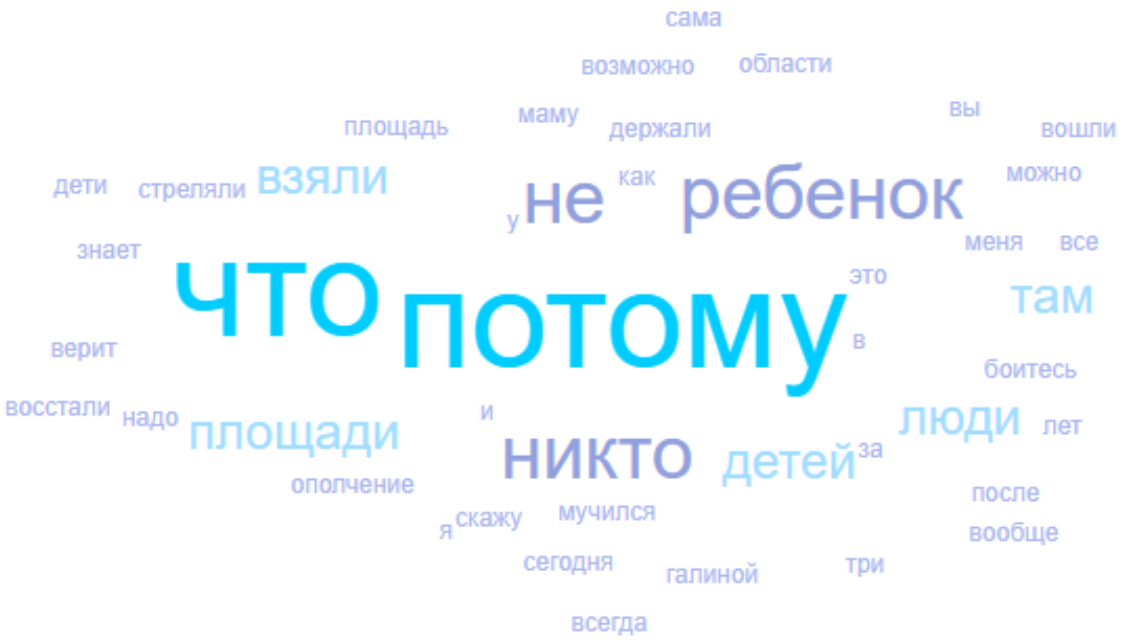

Рисунок 2.4 – Частотна мапа

На рисунку 2.3 зображена так звана мапа тексту яка візуально показує частотність вживання того чи іншого слова. Чим більшим шрифтом виділено слово, тим частіше воно використовується(не враховуючи допоміжних слів). Рисунок 2.4 зображає частоту всіх слів у тексті, враховуючи допоміжні.

Таблиця 2.1 показує основні параметри тексту, такі як «водність» і «нудота» та найбільш вживані слова тексту.

Таблиця 2.1 – Результати проведення контент аналізу

Водність	55%
Нудота	4.58
Топ 10 слів	ребенок, человек, площадь, мама, женщина, кровь, город, бояться, расстрелять, год

В наступній таблиці показана частостність вживання найпопулярніших слів та їх релевантність.

Таблиця 2.2 – Частота вживання слів у тексті

№	Слово	Частота	Релевантність
1	ребенок	10	2.18
2	человек	6	1.3
3	площадь	5	1.09
4	мама	4	0.87
5	женщина	3	0.65
6	кровь	3	0.65
7	город	3	0.65
8	бояться	3	0.65
9	расстрелять	3	0.65
10	год	2	0.43

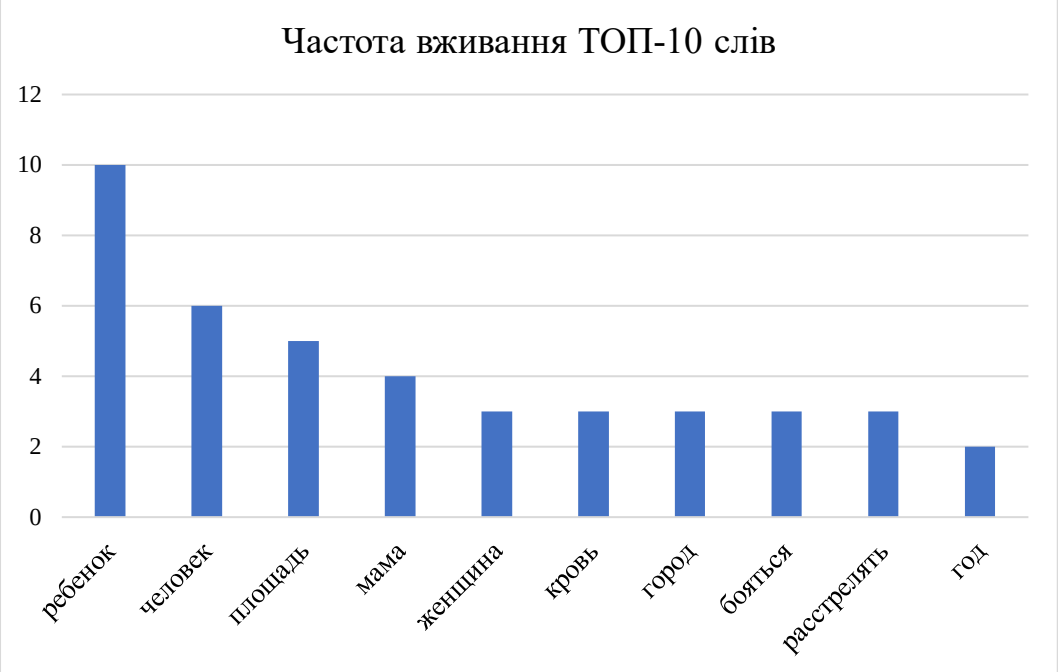

Рисунок 2.5 – Діаграма частоти вживання найпопулярніших слів

Закон Ципфа

Відповідно до закону Ципфа, котрий 1930 року відкрив лінгвіст Джордж Ципф, частоту, з якою певне слово виникає у тексті, можна вирахувати за допомогою нескладної математичної функції - відношення рангу слова в словнику частотності слів до частотності слова в мові становить сталу величину. Інакше кажучи, якщо всі слова доволі об’ємного тексту впорядкувати за зниженням частотності використання, тоді частота n–го слова у даному списку виявиться майже обернено пропорційною його порядковому номеру n (так званому рангу цього слова).

Для прикладу, друге за частотою вживаності слово трапляється приблизно вдвічі рідше, ніж перше, третє — в три рази рідше, ніж перше, і так далі.

Для чіткого визначення відповідності закону Ципфа застосовується формула

$$F = \frac{C}{R}$$

де:

F позначає, як часто використовується те чи інше слово;

R - номер слова по порядку(ранг);

C - постійна величина, яка відображає загальну кількість разів використання найчастішого слова у тексті.

Використовуючи даний закон є можливість виокремити слова якими заспамлений текст.

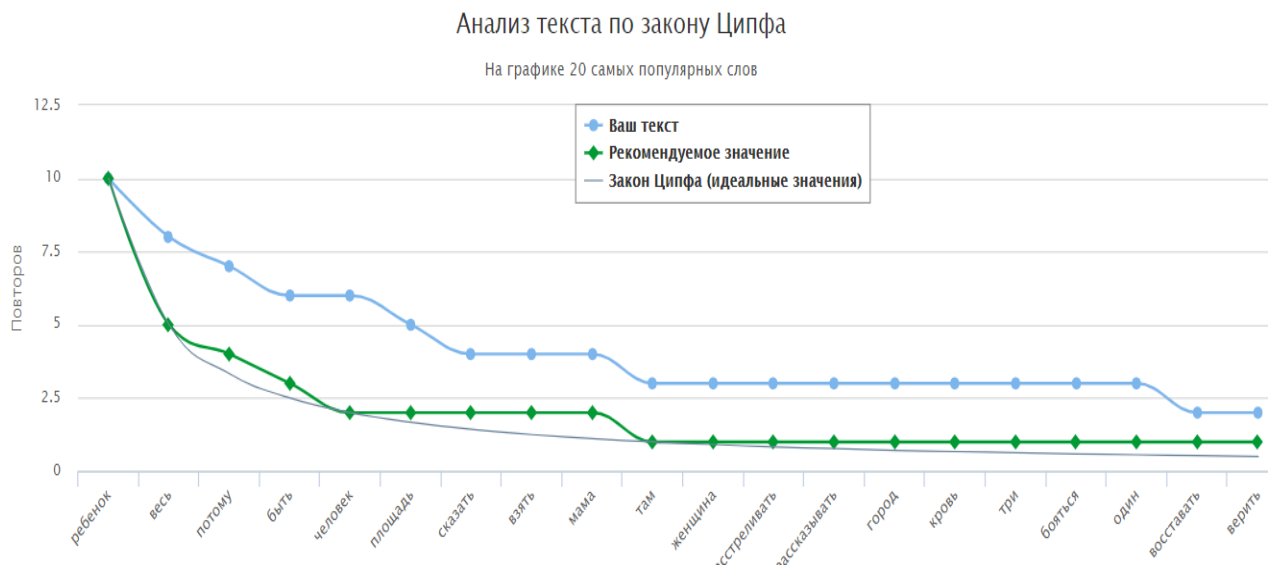

Рисунок 2.6 – Графік аналізу тексту по закону Ципфа

Як можна побачити з рисунку 2.6, текст аналізованої новини зовсім не відповідає рекомендованому значенню по закону Ципфа. На графіку чітко видно якими словами заспамлений текст, що був вибраний для аналізу.

Діаграма «ящик з вусами»

Наступним кроком для аналізу цього фейку стала побудова графіку «Ящик з вусами». Даний графік побудований за допомогою даних по рівню заспамленості тексту вибірки з 15 новин обраної теми.

Діаграма «Ящик з вусами», або ще відома як діаграма розмаху, коробковий графік — засіб візуалізації в описовій статистиці ряду числових даних через їх квантилі. Діаграма отримала свою назву за дуже характерний вид: точку або лінію, відповідну медіані або середньої арифметичної, оточує прямокутник («ящик»), довжина якого відповідає одному з показників розкиду або точності оцінки генерального параметра. Вже від цього «ящика» будуються так звані «вуса», які відповідають по довжині показам розкиду або точності. Діаграми даного типу часто використовуються, адже дають можливість отримати максимально повну статистичну характеристику сукупності що аналізується. Крім того, діаграми розмаху можна використовувати для візуальної експрес-оцінки різниці між двома і більше групами (наприклад, між датами відбору проб, експериментальними групами, ділянками простору, і т.п.).

Дана діаграма — непараметрична: вона зображає мінливість у вибірці статистичної сукупності, не роблячи ніяких припущень про базовий статистичний розподіл. Відстань між протилежними частинами коробки зображають ступінь дисперсії (розкиду), асиметрію в даних і відображають викиди. Крім самих точок, вони дозволяють візуально різні статистичні оцінки даних. Коробковий графік може бути як вертикальним так і горизонтальним.

Для побудови ящика з вусами, треба знати наступні величини: $Q_{25} = X_{[\frac{1}{4N}]}$ (перший квартиль), $Q_{50} = X_{[\frac{1}{2N}]}$ (медіана), $Q_{75} = X_{[\frac{3}{4N}]}$ (третій квартиль),

$Min = X_{[1]}$ (мінімум), $Max = X_{[N]}$ (максимум), Q_5 (5% персентиль), Q_{95} (95% персентиль) та множину екстремальних значень.

Отже, ящик з вусами в розрізі матиме наступний вигляд (рисунок 2.7).

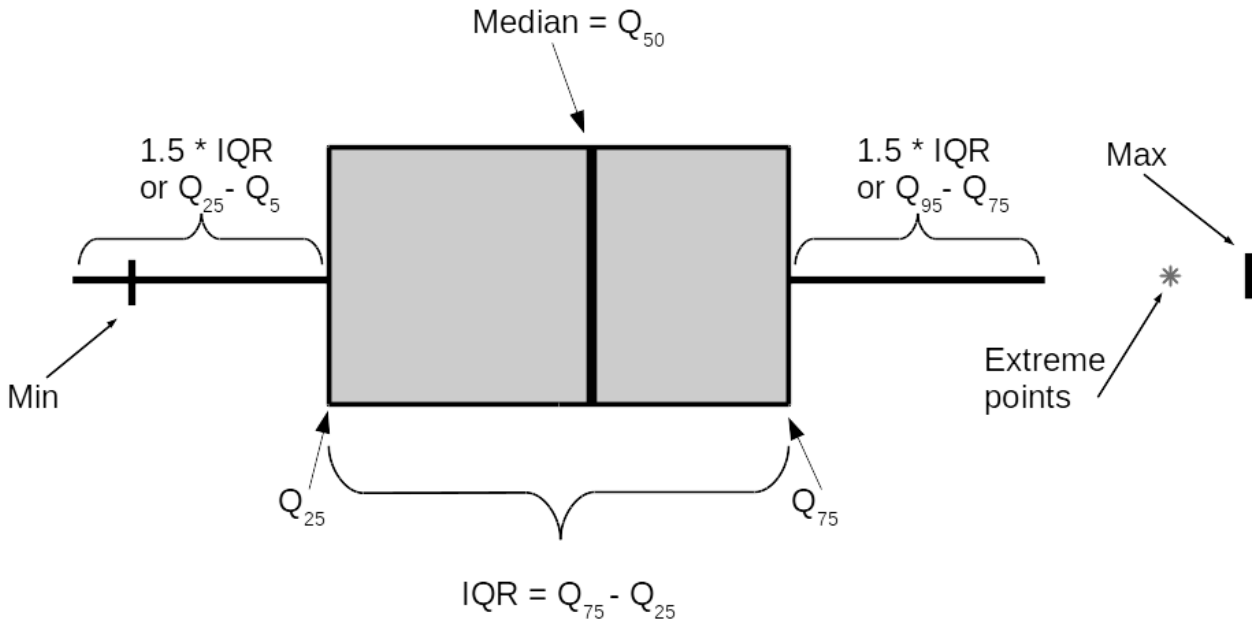

Рисунок 2.7 — Діаграма «ящик з вусами» в розрізі

Для вимірювання розкиду даних можна визначити ступіть відхилення кожного спостереження від середнього арифметичного. Зрозуміло, що чим більше відхилення, тим більше мінливість, варіабельність спостережень.

Вираховуємо дисперсію:

$$D = \sigma^2 = \frac{\sum_{i=1}^{n}(X_i - \bar{X})^2}{n}$$

Медіана являється характеристикою усереднення в наборі даних, для того щоб визначити її, слід, почавши з найменшого значення і закінчивши найбільним, класифікувати дані.

$$Me = x_0 + k \times \frac{\frac{\sum f}{2} - \sum f_{-1}}{f_{-}}$$

Середнє арифметичне – найбільш поширена оцінка середнього значення розподілу. Вкрай інформативне значення "центрального положення" спостереження змінної, особливо якщо повідомляється її довірчий інтервал. Для обрахування необхідні статистики, котрі дозволяють отримати висновок стосовно популяції в цілому. Однією з таких статистик є середнє.

$$\bar{X} = \frac{\sum_{i=1}^{n} X_i}{n}$$

де $\bar{X}$ — вибіркове середнє, n — обсяг вибірки, X_i – і-й елемент вибірки.

Щоб отримати таку форму опису розсіювання, на яку не буде впливати аномальне значення (викид), виключаючи екстремальні величини і визначаючи розмах.

Міжквартільний розмах – це різниця між 1–м і 3–м квартилями, тобто між 25–м і 75–м перцентилями. У нього входять центральні 50% спостережень в упорядкованому наборі, де 25% спостережень знаходяться нижче центральної точки і 25% – вище.

Інтердецільний розмах містить в собі центральні 90% спостережень, тобто ті спостереження, які розташовуються між 5–м і 95–м персентилями.

Для побудови діаграми «ящик з вусами» використовуємо такі дані з таблиці 2.3

Таблиця 2.3 – Дані для побудови діаграми «ящик з вусами»

Показник	Фейк 1
Кількість	15
Середнє	39,60
Станд. відхил.	3,30
Мінімум	32,00
Квартиль1	37,70

Продовження таблиці 2.3

Показник	Фейк 1
Медіана	39,51
Квартиль3	41,87
Максимум	44,03
Низ	37,70
2Q Коробка	1,82
3Q Коробка	2,36
Вуса–	5,70
Вуса+	2,16

За даними таблиці побудовано графік (рисунок 2.8)

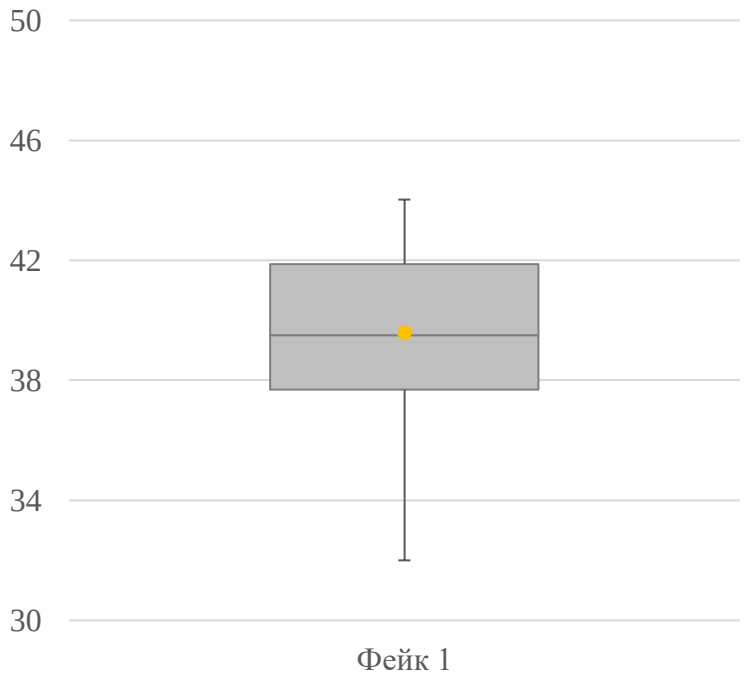

Рисунок 2.8 — Ящик з вусами

На рисунку 2.8 представлена діаграма «ящик з вусами», яка показує мінімальне і максимальні значення вибірки, медіану. Це дає змогу чітко зрозуміти середній рівень заспамленості тексту по першій новині.

2.3 Фейк №2

В якості другої фейк-новини я вибрав сюжет про «заклики до вбивства снігурів в Україні».

У ході аналізу отримано дані про кількість результатів щоденної пошукової видачі за запитами, що містили комбінації ключових слів: «убивать», «детей», «снегири», «синицы», тощо. Також проведено синтаксичний аналіз для виключення недоцільних результатів.

В результаті опрацювання даних було побудовано графік динаміки кількості тематичних повідомлень за обраний період (рисунок 2.9).

Рисунок 2.9 – Динаміка кількості тематичних повідомлень за обраний період

На рисунку 2.9 можна чітко виділити основні етапи проведення, інформаційної операції. Далі було проведено детальний контент аналіз тексту новини.

Рисунок 2.10 – Мапа тексту

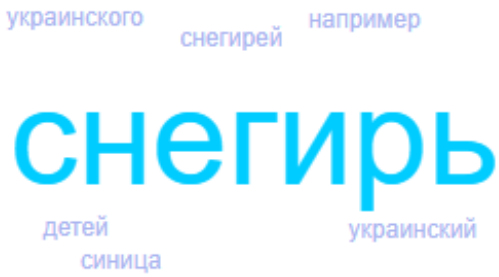

Рисунок 2.11 – Частотна мапа

На рисунку 2.10 побудована так звана мапа тексту що показує частотність вживання слів у тексті. Чим більшим шрифтом виділено слово, тим частіше воно використовується(не враховуючи допоміжних слів). Рисунок 2.11 зображає частоту всіх слів у тексті, враховуючи допоміжні.

Таблиця 2.4 показує основні параметри тексту, такі як «водність» і «нудота» та найбільш вживані слова тексту.

Таблиця 2.4 – Результати проведення контент аналізу

Водність	64%
Нудота	19.64
Топ 10 слів	украинский, снегирь, украина, ребенок, раскраска, синица, педагог, урок, природоведение, борьба

В наступній таблиці представлена частостність вживання найбільш популярних слів у тексті та їх релевантність.

Таблиця 2.5 – Частота вживання слів у тексті

№	Слово	Частота	Релевантність
1	снегирь	9	1.51
2	украинский	7	1.51
3	украина	4	1.13
4	ребенок	4	1.13
5	раскраска	3	0.75
6	синица	3	0.75
7	педагог	3	0.75
8	урок	3	0.75
9	природоведение	1	0.37
10	борьба	1	0.37

Рисунок 2.12 – Діаграма частоти вживання найпопулярніших слів

Наступним кроком аналізу обраної новини став аналіз тексту за законом Ципфа.

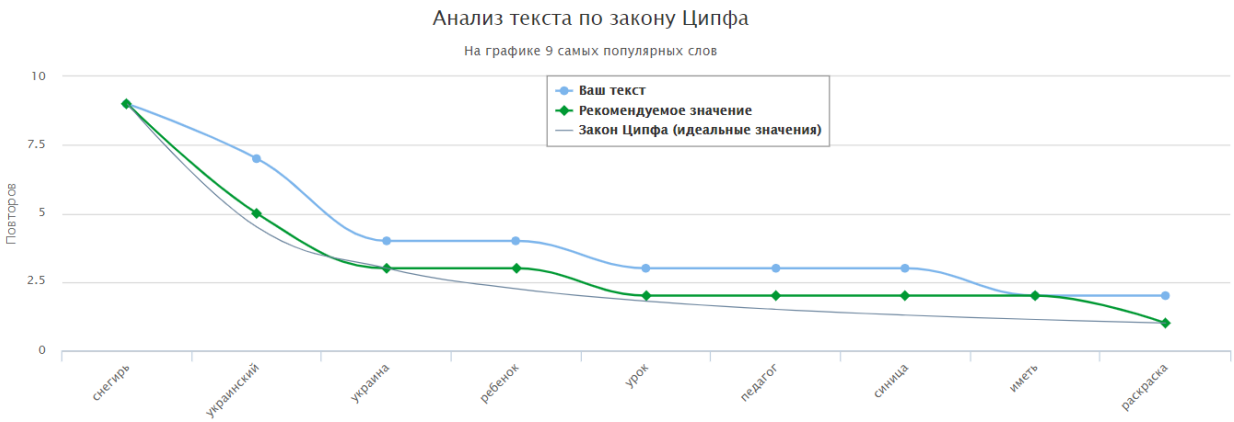

Рисунок 2.13 – Графік аналізу тексту по закону Ципфа

З рисунку 2.13 видно, що текст аналізованої новини не відповідає рекомендованому значенню і тим паче ідеальному, яке має бути по закону Ципфа. На графіку видно якими словами заспамлений текст, що був вибраний для аналізу.

Наступним кроком для аналізу цієї фейкової новини стала побудова діаграми «Ящик з вусами». Дана діаграма побудована за допомогою даних по рівню заспамленості тексту вибірки з 15 новин обраної теми.

Таблиця 2.6 – Дані для побудови діаграми «ящик з вусами»

Показник	Фейк 1
Кількість	15
Середнє	38,61
Станд. відхил.	3,24
Мінімум	31,64
Квартиль1	36,70
Медіана	38,59
Квартиль3	40,78
Максимум	44,58
Низ	36,70
2Q Коробка	1,89
3Q Коробка	2,19
Вуса–	5,06
Вуса+	3,80

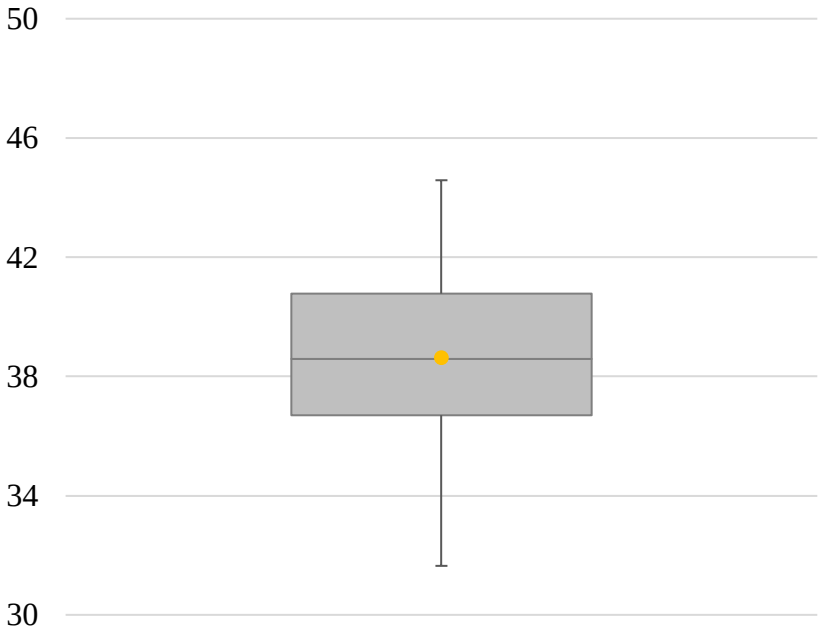

Рисунок 2.14 — Ящик з вусами

На рисунку 2.14 представлена діаграма «ящик з вусами», яка показує мінімальне і максимальні значення вибірки, медіану. Це дає змогу чітко зрозуміти середній рівень заспамленості тексту по другій новині.

2.4 Фейк №3

В якості другої фейк-новини я вибрав сюжет про «штрафи за вживання російської мови».

У ході аналізу отримано дані про кількість результатів щоденної пошукової видачі за запитами, що містили комбінації ключових слів: «язык», «закон», «разрешено», «русскоязычные», тощо. Також проведено синтаксичний аналіз для виключення недоцільних результатів.

В результаті опрацювання даних було побудовано графік динаміки кількості тематичних повідомлень за обраний період (рисунок 2.15).

Рисунок 2.15 – Динаміка кількості тематичних повідомлень за обраний період

На рисунку 2.15 можна чітко виділити основні етапи проведення, інформаційної операції. Далі було проведено детальний контент аналіз тексту новини.

На «мову» должны быть переведены и сайты, находящиеся в **украинском** сегменте интернета. **Русский** и английский **языки** будут разрешены, как вспомогательные, а вот в автоматической загрузке должна будет стоять именно укроверсия веб-ресурсов. Это тоже приведет к катастрофе, так как, согласно исследованиям IT-компаний, порядка 60%-65% всех **украинских** сетевых ресурсовсуществуют сегодня исключительно в **русскоязычном** виде.

Квота на **украинский язык** на телевидении и в радиовещании пока сохранена на уровне 75%. Исключительно украиноязычной становится теперь вся сфера обслуживания – от парикмахерских, автомоек, гастрономов и кафе до интернет-магазинов. Ситуация откровенно безумная – если официант даже в месте компактного проживания **русскоязычного**, венгерского или румынского **населения** поздоровается с клиентом на родном **языке**, его ждут за это жестокие санкции…

Кроме того, в **законе** есть указания на то, что **украинский язык** должны использовать в своей работе предприятия всех форм собственности. Не на **украинском** можно будет общаться только с иностранцами и лицами без гражданства.

На **украинский язык** полностью переводится медицинское обслуживание. Другие **языки** могут в виде исключения использоваться при общении в случае согласия обеих сторон, однако **документы** все равно будут заполняться только на «мове».

Согласно **закону**, на **Украине** будут созданы два новых «карательных» органа: Национальная комиссия по стандартам **украинского языка** и секретариат Уполномоченного по защите

Рисунок 2.16 – Мапа тексту

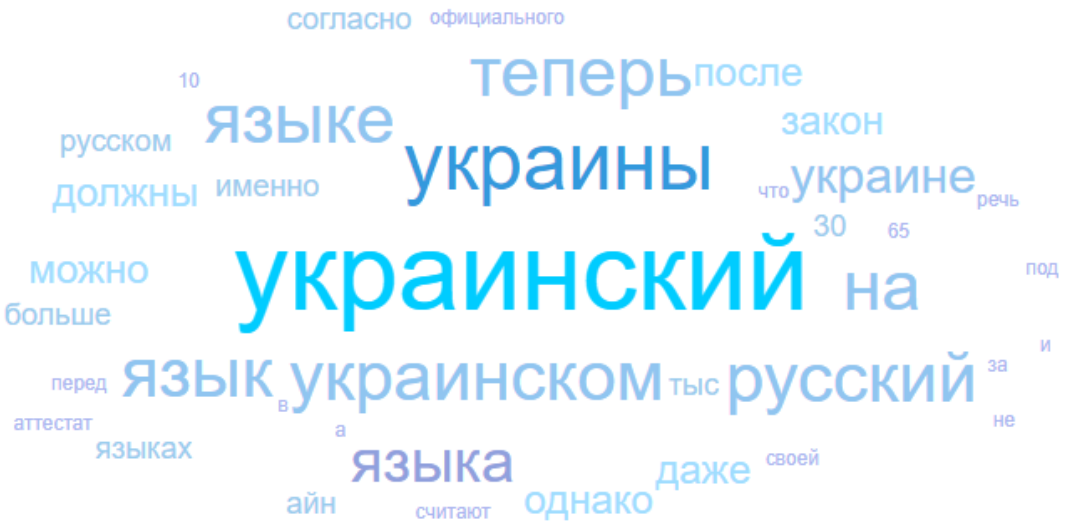

Рисунок 2.17 – Частотна мапа

На рисунку 2.16 побудована мапа тексту, що показує частотність вживання слів у тексті. Рисунок 2.17 зображає частоту всіх слів у тексті, враховуючи допоміжні.

Таблиця 2.7 показує основні параметри тексту, такі як «водність» і «нудота» та найбільш вживані слова тексту.

Таблиця 2.7 – Результати проведення контент аналізу

Водність	42%
Тошнота	6.78
Топ10 слів	украинский, язык, украина, русский, закон, население, русскоязычный, документ, страна, говорить

В таблиці 2.8 представлена частота вживання найбільш популярних слів у тексті та їх релевантність.

Таблиця 2.8 – Частота вживання слів у тексті

№	Слово	Частота	Релевантність
1	украинский	31	4.57
2	язык	30	4.42
3	украина	14	2.06
4	русский	12	1.76
5	закон	10	1.47
6	население	7	1.03
7	русскоязычный	5	0.73
8	документ	4	0.58
9	страна	4	0.58
10	говорить	4	0.58

Рисунок 2.18 – Діаграма частоти вживання найпопулярніших слів

Наступним кроком аналізу обраної новини став аналіз тексту за законом Ципфа.

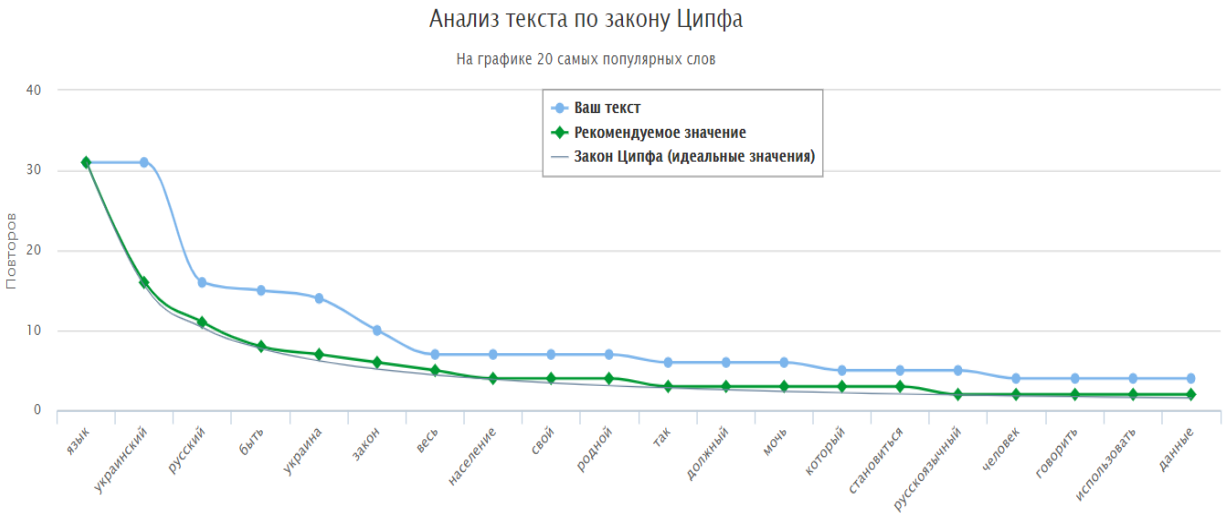

Рисунок 2.19 – Графік аналізу тексту по закону Ципфа

З рисунку 2.19 видно, що текст аналізованої новини не відповідає рекомендованому значенню і тим паче ідеальному, яке має бути по закону

Ципфа. На графіку видно якими словами заспамлений текст, що був вибраний для аналізу.

Наступним кроком для аналізу цієї фейкової новини стала побудова діаграми «Ящик з вусами». Дана діаграма побудована за допомогою даних по рівню заспамленості тексту вибірки з 15 новин обраної теми.

Таблиця 2.9 – Дані для побудови діаграми «ящик з вусами»

Показник	Фейк 1
Кількість	15
Середнє	37,42
Станд. відхил.	4,42
Мінімум	31,00
Квартиль1	33,78
Медіана	36,13
Квартиль3	41,69
Максимум	45,00
Низ	33,78
2Q Коробка	2,35
3Q Коробка	5,56
Вуса–	2,78
Вуса+	3,31

Рисунок 2.20 — Ящик з вусами

На рисунку 2.20 представлена діаграма «ящик з вусами», яка показує мінімальне і максимальні значення вибірки, медіану. Це дає змогу чітко зрозуміти рівень заспамленості тексту по третій новині. Середнє значення знаходиться на рівні 37,42%, медіана сягає 36,13%.

Порівняння результатів

Таблиця 2.10 – Дані для побудови діаграми «ящик з вусами» для 3-х фейків

Показник	Фейк 1	Фейк 2	Фейк 3
Кількість	15	15	15
Середнє	39,60	39,61	37,42
Станд. відхил.	3,30	3,24	4,42
Мінімум	32,00	32,64	31,00
Квартиль1	37,70	37,70	33,78
Медіана	39,51	39,59	36,13
Максимум	44,03	45,58	45,00

Продовження таблиці 2.10

Показник	Фейк 1	Фейк 2	Фейк 3
Низ	37,70	37,70	33,78
2Q Коробка	1,82	1,89	2,35
3Q Коробка	2,36	2,19	5,56
Вуса–	5,70	5,06	2,78
Вуса+	2,16	3,80	3,31

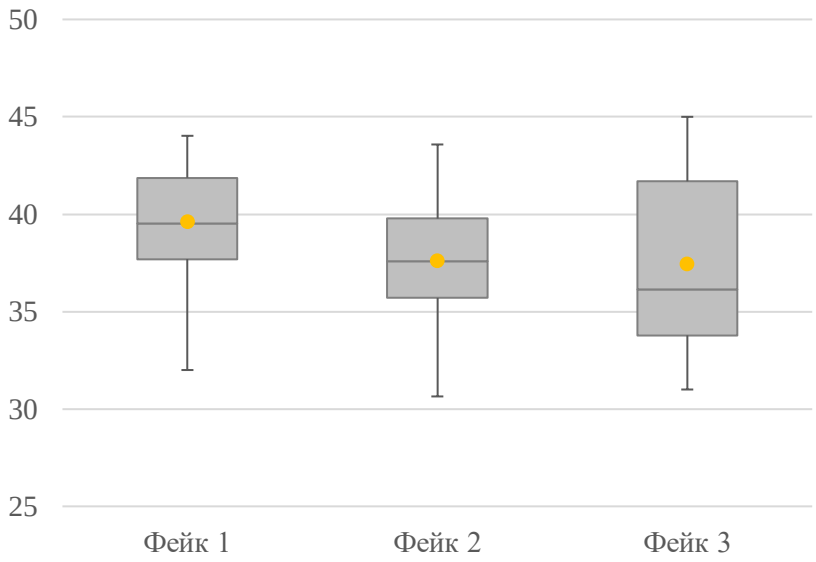

Рисунок 2.21 — Ящик з вусами для трьох фейків

Як можна побачити з рисунку 2.21, середній рівень заспамленості тексту проаналізованих новин сягає 37%-40%, значення медіани також знаходиться на схожому рівні і сягає 36%-39%.

Висновки до розділу 2

У другому розділі для дослідження було використано три фейкові новини. Було проведено кількісний і якісний аналіз статистичних даних за допомогою методів контент-аналізу, порівняльного аналізу.

Для кожної новини були побудовані графіки її поширення за певний проміжок часу і порівняно з запропонованою моделлю поширення фейкових новин, для цього кожен графік з динамікою кількості повідомлень за обраний період було розділено на етапи розповсюдження, такі як фон, попереднє затишшя, підготовка, затишшя, атака, релаксація.

Після проведення контент аналізу було отримано дані по таким параметрам як частотність, нудотність та водність. Також був проведений аналіз тексту за законом Ципфа. Результат даного виду аналізу представлений у графіку, на якому зображена частотність найбільш популярних слів у конкретному тексті, яку можна порівняти з рекомендованим значенням популярності слів за законом Ципфа. Значення, запропоновані за законом Ципфа вважаються ідеальними.

За результатами дослідження заспамленості тексту було побудовано діаграму «ящик з вусами» для порівняння зібраних даних трьох новин

ВИСНОВКИ

Інформаційна війна між Росією і Україною зумовила актуалізацію теми розповсюдження недостовірної інформації.Сучасна інформаційна ера стрімко трансформується і призводить до появи нових засобів і методів ведення війни. Росія випереджає Україну в декілька кроків у розвитку механізмів і технологій.

Значний відсоток інформації про резонансні події в Україні — не відповідають дійсності. Головною причиною цього є застосування інформації з метою нав'язування людям думки, вигідної лише для однієї сторони конфлікту для інформування людей.

У ході цієї роботи було надане визначення термінам «інформаційна війна», «дискредитація» та досліджено динаміку їх використання на основні кількості публікацій в українських та світових наукових джерелах. Також було досліджено термін «фейк» та визначено основні етапи поширення фейків в інформаційному просторі, а саме фон, попереднє затишшя, підготовка, затишшя, атака, релаксація.

Процес розповсюдження фейків був розглянутий на прикладі трьох новин у засобах масової інформації. Після проведення аналізу по обраним новинам, було визначено динаміку їх розповсюдження, виокремлено кількісні та якісні характеристики текстів. Також було визначено ключові слова, які безпосередньо впливають на сприйняття інформації у людей та відсотки заспамленості трьох вибірок текстових новин обраної теми і проведений порівняльний аналіз,

Проведене дослідження лише частково відображає методи впливу на населення під час ведення інформаційної війни. Перспективним напрямком подальших досліджень може бути аналіз рівня ефективності протидії російській інформаційній війні проти України у майбутньому, а також вивчення міжнародного досвіду у боротьбі з інформаційною війною.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Дубов Д. В., Ожеван М. А. Кібербезпека: світові тенденції та виклики для України. Аналітична доповідь. [Текст] – К. : НІСД, 2011. – 30 с.

2. Додонов О.Г., Горбачик О.С., Кузнєцова М.Г. Інформаційне суспільство: технології та безпека // Інформація та відкритість влади як засоби демократизації суспільства: Зб. матеріалів «круглого столу». [Текст] / К.: Альтпрес. – 2003. – С. 119-124.

3. Горбулін В.П., Качинський А.Б. Методологічні засади розробки стратегії національної безпеки // Стратегічна панорама. [Текст] / Горбулін В.П. – 2004. – № 3. – С. 15 - 24.

4. Качинський А.Б. Безпека, загрози та ризик [Текст] / А.Б.Качинський. – К. ІПНБ РНБО ; НА СБ України, 2004. – 472 с.

5. Про рішення Ради національної безпеки і оборони України від 29 грудня 2012 року "Про Стратегічний оборонний бюлетень України" [Електронний ресурс]. – Режим доступу: https://zakon2.rada.gov.ua/laws/show/771/2012/paran16#n16

6. Курбан О. В. Сучасна гібридна війна: нові форми агресії / О. В. Курбан. – [Електронний ресурс]. – Режим доступу: http://ua.racurs.ua/1063suchasna-gibrydna-viynata-yiyi-vidobrajennya-u-virtualniy-realnosti-chastyna-2.

7. Ткаченко А. В., Качинський А. Б. Ідентифікація фейкових новин в соціальних ЗМІ. [Текст] / А. В. Ткаченко

8. Горбулін В.П., Інформаційні операції та безпека суспільства: загрози, протидія, моделювання .[Текст] / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде– 2009 – Київ Видавництво «Інтертехнологія». С. 64 – 72

9. Остроухов В.В. Інформаційна безпека -– [Електронний ресурс]./ В.В. Остроухов – Режим доступу: https://westudents.com.ua/glavy/51894-12-nformatsyna-vyna-yak-forma-vedennya-nformatsynogo-protiborstva.html.

10. Потемкин А.В. Распознавание информационных операций средств массовой информации сети Интернет [Текст] / А.В Потемкин– «НАУКОВЕДЕНИЕ» –2015. — Т. 7, № 3. — Режим доступа: http://naukovedenie.ru/PDF/139TVN315.pdf

11. Фейкові новини — Вікіпедія [Електронний ресурс] / Режим доступуhttps://uk.wikipedia.org/wiki/%D0%A4%D0%B5%D0%B9%D0%BA%D0%BE%D0%B2%D1%96_%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8

12. Павлов Д. М. Особливості технологій політичної пропаганди [Текст] / Д. М. Павлов // Науково-теоретичний альманах «Грані». – 2018. – Т. 21. – № 2. – С. 141-149.

13. Ильченко С.Н.. Фейк в практике электронных СМИ: критерии достоверности. // Медиаскоп. [Текст] /С.Н. Ильченко — 2016. — № 4. — Режим доступа: http://www.mediascope.ru/2237.

14. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник [Текст] / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

15. Грищук Р. В. Основи кібернетичної безпеки: монографія [Текст] / Р. В. Грищук, Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника. – Житомир: ЖНАЕ, 2016. – 636 с.: іл.

16. Грайворонський М. В. Безпека інформаційно-комунікаційних систем [Текст] / М. В. Грайворонський, О. М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с.

17. Бурячок В. Л. Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем [Текст] / В. Л. Бурячок, О. Г. Корченко, Л. В. Бурячок // Захист інформації. – 2012. – № 4(57). – С. 5–12.

18. Soviet Active Measures by Other Means(Estonian Journal of Military Studies), [Електронний ресурс] / 2016, С. 140–169 Режим доступу : www.ksk.edu.ee/publikatsioonid):

19. Блавацький С. А. Что такое асимметричная война. Асиметрична війна. [Електронний ресурс] / С. А. Блавацький– Режим доступу : http://lnu.edu.ua/mediaeco/zur-kryt /n7/blavat-asymetr.htm

20. Google Scholar [Електронний ресурс] – Режим доступу до ресурсу: https://scholar.google.com

21. JSTOR [Електронний ресурс] – Режим доступу до ресурсу: https://www.jstor.org/

22. ScienceDirect [Електронний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/

23. Google Ngram Viewer [Електронний ресурс] – Режим доступу до ресурсу: https://books.google.com/ngrams