Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему

Метод виявлення інформаційної загрози за парсингом спільнот у соціальних інтернет-сервісах

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

КРМКБ. 180130.22.01.09 ПЗ

Виконав: студент 2 курсу, група КБм-22-1 Матвійчук А.В.
Підпис

Керівник: ст. викладач, к.т.н, доц. Муляр І.В.
Підпис

Нормоконтролер старший викладач Мостовий С.В.
Підпис

До захисту допускаю:
Зав. кафедри кібербезпеки, к.т.н., доц Кльоц Ю.П.
Підпис

14 грудня 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень Магістр

Галузь знань 12 Інформаційних технологій

Спеціальність 125 Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"30" 08 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Матвійчуку Андрію Вікторовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод виявлення інформаційної загрози за парсингом спільнот у соціальних інтернет-сервісах

Керівник роботи Муляр Ігор Володимирович.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання
кандидат технічних наук, доцент

Затверджена наказом № 30 ректора університету, додаток №25 від 15.08.2023

2. Строк подання студентом проєкту (роботи) на кафедру 15.11.2023

3. Вихідні дані до проекту (роботи) Соціальні інтернет-сервіси, загрозлива інформація, онлайн-спільноти

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Характеристики інформаційного забезпечення соціальних мереж, розробка математичної моделі процесів та компонентів соціальних мереж, методи виявлення інформаційних загроз в цих мережах, а також ключові складові засобів захисту соціальних мереж.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В. Старший викладач кафедри кібербезпеки		

7. Дата видачі завдання «01» вересня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір напряму дослідження і узгодження тематики КРМ з керівником	01.06.2023	
2	Ознайомлення з предметною областю; формулювання мети і задач дослідження; визначення об'єкта і предмета дослідження	04.09.2023	
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	18.09.2023	
4	Робота над розділом 2 – розробка моделей і методів для вирішення поставленої задачі	02.10.2023	
5	Робота над розділом 3 – розробка алгоритмів і технологій, їх аналіз	16.10.2023	
6	Робота над розділом 4 – апробація запропонованих рішень	06.11.2023	
7	Робота над науковою публікацією	10.11.2023	
8	Узгодження отриманих результатів, оформлення пояснювальної записки згідно вимог	15.11.2023	
9	Попередній захист роботи	17.11.2023	
10	Захист роботи на засіданні ЕК	06.12.2023	

Студент Підпис А.В. Матвійчук Ініціали, прізвище

Керівник проекту (роботи) Підпис І.В. Муляр Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод виявлення інформаційної загрози за парсингом спільнот у соціальних інтернет-сервісах

Автор роботи: Матвійчук Андрій Вікторович

Керівник роботи: к.т.н., доц. Муляр Ігор Володимирович

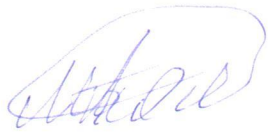
Загальний обсяг роботи: 87 сторінок, 24 рисунки, 1 таблиця, 2 додатки, 55 посилань.

Ключові слова: Соціальні інтернет-сервіси, загрозлива інформація, онлайн-спільноти.

Метою даної роботи є Розробка методу та інструментів для аналізу та виявлення впливу інформації в соціальних мережах, спрямованого на оптимізацію часових витрат на збір та обробку даних щодо поширення та характеристик повідомлень. Застосування формалізованих запитів та пошукового робота з використанням API-методів соціальних мереж дозволило здійснювати точний та цільовий пошук, а також отримувати необхідну інформацію про дискусії.

Розроблено архітектуру програмного комплексу для моніторингу та аналізу інформаційних загроз онлайн-спільнот у соціальних мережах. Детально описано ключові компоненти системи, їх функціональне призначення та технічні аспекти реалізації.

12.12.2023



ANNOTATION

Theme of qualification work: A method for detecting information threats by parsing communities in social Internet services

Author of the work: Matviichuk Andrii Viktorovych

Mentor: Ph.D. Muliar Ihor Volodymyrovych

Total volume of work: 87 pages, 23 figures, 1 tables, 2 appendices, 55 links.

Keywords: Social Internet services, threatening information, online communities.

The purpose of this paper is to develop a method and tools for analyzing and identifying the impact of information in social networks aimed at optimizing the time spent on collecting and processing data on the distribution and characteristics of messages. The application of formalized queries and a search robot using API methods of social networks allowed for accurate and targeted search, as well as obtaining the necessary information about discussions.

The architecture of a software system for monitoring and analyzing information threats to online communities in social networks has been developed. The key components of the system, their functional purpose and technical aspects of implementation are described in detail.

12.12.2023

ЗМІСТ

ВСТУП

Сучасні глобалізаційні процеси сформували єдиний світовий інформаційний простір, де дані постійно змінюються, зберігаються та передаються окремими особами, громадами та державами. У світі, перенасиченому інформацією, цей процес має особливе значення. Просторовий інформаційний потік пронизує всі сфери взаємодії суспільства з навколишнім світом та слугує фундаментом для формування загальної картини всесвіту. Інформація присутня як у фізичному середовищі у вигляді природних об'єктів і явищ, так і в суспільстві у вигляді знань, навичок і умінь. Утворений інформаційний кіберпростір стає важливою ареною для проведення інформаційних конфліктів, метою яких є вплив на психологію та усвідомлення особистостей, що підкреслює роль інформаційної війни як важливого елемента сучасного світу [1, 2].

Зараз соціальні мережі інтернету є однією з найбільш популярних віртуальних платформ для здійснення соціальної комунікації в онлайн-середовищі. Вони задовольняють основні потреби користувачів у взаємодії, відчутті належності до віртуальних спільнот, здобутті нових знань, самовираженні, забезпеці тощо. У той же час великі країни можуть використовувати соціальні мережі для досягнення власних переваг у національному інформаційному просторі та впливу на суспільні та політичні процеси в країні, громадську думку, загострення соціальних, міжрелігійних та міжнаціональних конфліктів тощо. Тому забезпечення інформаційної безпеки країни на соціальних мережах є актуальною проблемою як в Україні, так і в усьому світі.

У цій роботі досліджується інфополе, яке виконує роль середовища для функціонування інформаційних агентів. В якості таких агентів розглядаються взаємозв'язані сутності "повідомлення - джерело". Повідомлення розглядаються як інструменти для передачі інформаційного впливу. Інформаційні повідомлення можуть бути розповсюджені далі, містити посилання на подібні за змістом

повідомлення або на інші об'єкти реального чи віртуального світу .

Для розгляду механізмів впливу інформації на суспільство через інфополе, у цьому дослідженні використовуються методи мультиагентного моделювання. Зазвичай ці методи використовуються для аналізу складних систем, де неможливо дати аналітичний опис всіх процесів.

Багато досліджень, що стосуються взаємодії акторів у соціальних інтернет-сервісах [3], розглядають їх як засіб для формування динамічного інофополя. Сучасні соціальні інтернет-сервіси мають велику кількість акторів, які є вузлами комунікації і пов'язані різними відносинами, утворюючи канали для обміну контентом. Віртуальні спільноти акторів у соціальних інтернет-сервісах, які формуються на основі спільних інтересів, можуть динамічно змінювати свою структуру. Самі процеси взаємодії між акторами відзначаються високою чутливістю до будь-яких змін в початкових умовах або параметрах інофополя. У результаті інформаційних операцій у соціальних інтернет-сервісах, які можуть бути розглянуті як зовнішні збурення в системі, можуть виникати непередбачувані і некеревоні процеси у соціальній комунікації акторів, не лише в віртуальному, але й у реальному житті. Щодо останніх досліджень у цьому напрямку вони були проведені такими науковцями: Арістова Н.О., Трач О.Р., Малихін О.В., Пелещишин А.М., Молодецька К.В., Гумінський Р. В. та ін.

Незважаючи на обширну кількість досліджень, присвячених інформаційній війні, сьогодні мало досліджень, які аналізують це явище з погляду механізмів впливу і формування громадської думки. Це стало важливим стимулом для нашого аналізу та вивчення даної теми.

Наукове завдання полягає у розробці і технології для аналізу та виявлення впливу інформації в соціальних мережах, використовуючи методи парсингу, що ґрунтуються на мультиагентних моделях поширення інформації.

Мета і задачі дослідження. Розробка методу та інструментів для аналізу та виявлення впливу інформації в соціальних мережах, спрямованого на оптимізацію часових витрат на збір та обробку даних щодо поширення та характеристик повідомлень.

В роботі вирішено такі основні завдання:

1. Проведено аналіз онлайн-спільнот, та розглянуто особливості їх організації в соцмережах в Інтернеті.

2. Розроблено математичні моделі для аналізу інфополя онлайн- спільнот.

3. Створено метод виявлення інформаційного впливу, що базується на аналізі статистичних параметрів розподілу характеристик контенту в ресурсах соціальних мереж.

4. Розраховано показник інформаційної загрози спільноти.

5. Розроблено технологію для створення баз даних на основі вмісту онлайн-ресурсів.

6. Запропоновано архітектуру системи моніторингу онлайн-ресурсів, з метою оцінки потенційної загрози онлайн-спільноти.

Об’єктом дослідження є процес впливу онлайн-спільнот соціальних мереж.

Предметом дослідження є методи та інструменти виявлення інформаційних загроз.

Методи дослідження. Для вирішення завдань стосовно розробки інструментів захисту доступу до інформаційних соціальних систем використовуються різноманітні наукові підходи та методології. Зокрема, застосовуються методи математичної логіки для формалізації правил та умов доступу, теорія графів використовується для моделювання зв'язків та взаємодій між елементами системи.

Також методи теорії мультиагентних систем використовуються для аналізу поведінки окремих агентів у соціальних системах та їх взаємодії. Методи аналізу тексту та комп'ютерної лінгвістики використовуються для обробки та розуміння текстової інформації, що може містити елементи доступу або потенційні загрози.

Комп'ютерне моделювання дозволяє провести експерименти та аналіз захисту в умовах віртуального середовища. Також застосовуються методи імітаційного моделювання для відтворення та аналізу різних сценаріїв функціонування систем захисту.

Ці методи взаємодіють для створення комплексних рішень щодо Забезпечення безпеки інформаційних соціальних систем стало предметом наукового дослідження, спрямованого на розробку методу для оцінки інформаційних загроз онлайн-спільнот. Одержані наукові результати включають:

– вдосконалено модель онлайн-спільноти, яка стала основою для розроблення структури бази даних щодо обліку інформаційних загроз;

– розроблено метод виявлення інформаційної загрози за парсингом груп у соціальних інтернет-сервісах, який базується на врахуванні кількості учасників, при якій реалізується інформаційний вплив.

– запропоновано архітектуру системи аналізу інформаційного впливу онлайн-спільноти для більш ефективного виявлення та вирішення цих загроз.

Практичне значення роботи. Були розроблені алгоритми для виявлення загрозливих сторінок обговорень у соцмережах, що базуються на розширених можливостях глобальних пошукових систем та використанні API-методів соціальних мереж. Ці алгоритми дозволяють ідентифікувати сторінки обговорень відповідно до їхнього контенту, що дало можливість реалізації підходів щодо вчасного реагування та протидії.

Теоретичні та практичні результати, доповідалися і обговорювалися у Київському національному університету імені Тараса Шевченка на XIX Міжнародній науково-практичній конференції «Військова освіта і наука: сьогодення та майбутнє»

За матеріалами магістерської роботи опубліковано 1 теза.

1 АНАЛІЗ ФУНКЦІОНУВАННЯ СОЦІАЛЬНИХ МЕРЕЖ

1.1 Аналіз сучасних тенденцій та моніторинг функціонування інтернет-сервісів

Мільярди людей у сучасному світі вже не уявляють свого життя без постійного використання мобільних телефонів і активної участі в соціальних мережах. Від ранку до вечора, вони обов'язково перевіряють свої мобільні пристрої та оглядають стрічки новин на Facebook, Instagram чи X (Twitter). Саме в цифровому просторі вони отримують та публікують новини, знаходять інформацію, обмінюються життєвими історіями, надають рекомендації, діляться проблемами та враженнями, висловлюють емоції, знаходять прихильників та однодумців, відзначають важливі події.

Охоплення цільової аудиторії на широкому рівні є однією з головних переваг соціальних мереж, оскільки вони надають прямий канал для взаємодії з аудиторією. Це не лише дозволяє більше контролювати представлення фактів та аргументів, але й допомагає досягати більшої повноти та швидкості взаємодії з вашою цільовою аудиторією [4].

Соціальні мережі перехопили роль віддачі інформації на користь двосторонньої комунікації, де передбачається взаємодія та залучення членів спільноти до діалогу та збору їхнього відгуку. Можливість надавати безпосередні відповіді на запитання та зауваження аудиторії допомагає уникнути непорозумінь та підвищує достовірність інформації. Таким чином, якщо ваша присутність у соціальних мережах добре організована, це полегшує контакт із громадськістю і робить вашу комунікаційну стратегію набагато більш ефективною. На сьогоднішній день соціальні мережі є, безсумнівно, одними з найефективніших інструментів для реалізації вашої комунікаційної стратегії.

Розвиток інформаційно-телекомунікаційних систем і глобальних мереж одночасно піднімають інформаційну боротьбу на високий рівень, створюючи

важливу складову гібридної війни. Її характерною особливістю є відсутність значних військових конфліктів і агресивних стратегій. Замість цього спостерігаються окремі тактичні операції, короткочасні військові зіткнення, диверсії, деструктивні дії населення та повний контроль над маніпуляціями та впливом на місцевих жителів [5]. Інформаційна агресія, як елемент війни, включає в себе сукупність маніпулятивних впливів та психологічного тиску для досягнення визначених завдань, які поставлені перед ворогом як підконтрольною, так і власною громадою [6].

Постійно виникають труднощі з вибором найкращої соціальної платформи, оскільки це визначає можливості для ефективного інформування громадян про наші послуги, підвищення суспільної довіри та налагодження конструктивного діалогу з громадськістю. При виборі соціальної платформи для вашої організації слід враховувати декілька аспектів. З одного боку, потрібно привертати і взаємодіяти з цільовою аудиторією, а з іншого боку, позитивно представляти діяльність вашої організації та інформувати про надані послуги.

За типом платформи можна виділити наступні підходи:

- соціальні мереж, такі як Facebook, Twitter, LinkedIn;
- форуми та дискусійні групи;
- блоги та мікроблоги, такі як X;
- віртуальні ігри та онлайн-ігрові спільноти;
- месенджери, такі як Viber, WhatsApp, Telegram;
- сервіси відеоконтенту, такі як Youtube, TikTok.

Стратегія роботи в соціальних мережах визначає загальну мету діяльності вашої організації в соціальних мережах і визначає, який контент, для кого і де саме ви будете публікувати. Враховуючи зростання користувачів віртуальних спільнот, виникає потреба у навичках класифікації цих спільнот, які сприятимуть оцінці їх ефективності та розробці плану розвитку [7]. Опис кожного типу віртуальних спільнот відображає їхню специфіку залежно від визначених характеристик, оскільки кожна має свої власні правила для забезпечення якісного

функціонування. Класифікація була створена відповідно до сучасних галузей та технологій використання віртуальних спільнот і представлена на рисунку 1.1

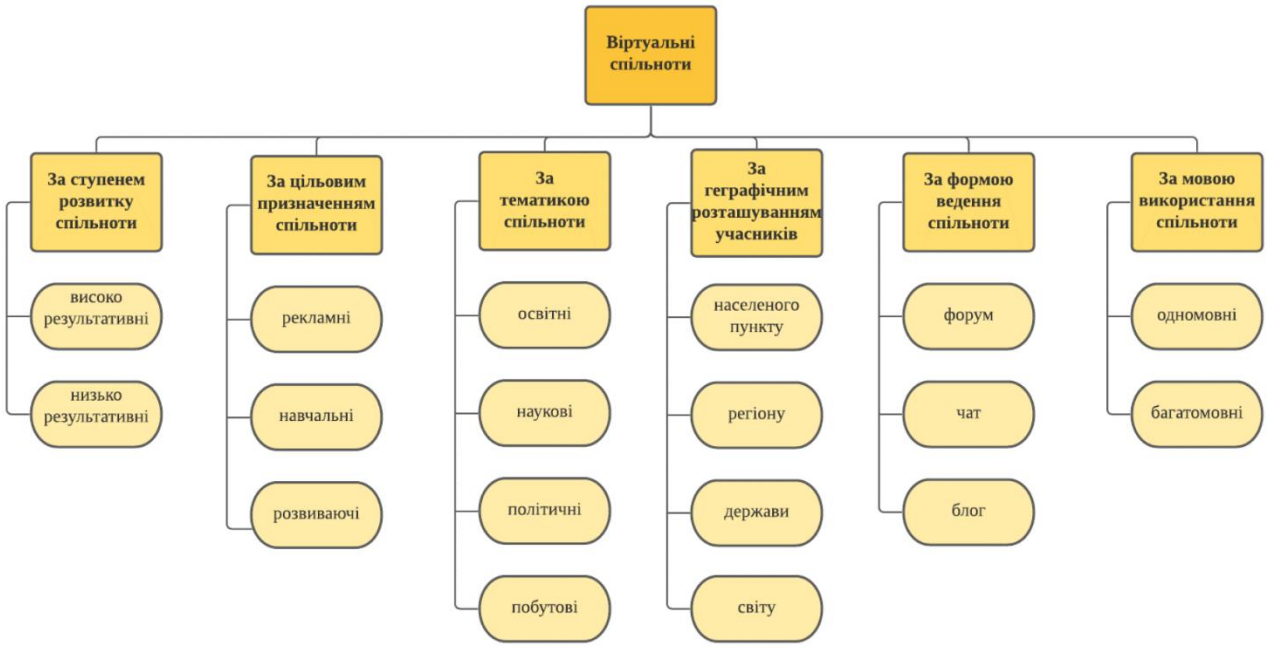


Рисунок 1.1 – Класифікація спільнот в соцмережах

Високоефективна віртуальна група - це спільнота, де учасники взаємодіють і реагують на опубліковану інформацію з високою активністю, що відображається у великій кількості реакцій та впливає на збільшення числа учасників. Група включає як короткотривалі активності (наприклад, одноразові конкурси, події та заходи), так і тривалі теми (які повторюються періодично визначеними інтервалами). Адміністратор спільноти відповідає за контроль активності її учасників, розробляє стратегію розвитку, визначає ролі учасників, контент і програмне забезпечення. Учасники відзначають публікації реакціями, що вказує на корисність інформації. Таким чином, зареєстровані учасники стають активними учасниками спільноти. Інформаційний контент повинен бути якісним, структурованим та цікавим. Окрім того, ефективність спільноти також залежить від оточення, в якому вона діє, оскільки доступність, управління та обмін інформацією грають важливу роль у роботі спільноти. Лише аналізуючи вплив

кожного з цих компонентів віртуальної спільноти, можна зробити її результативною.

Низькоефективна віртуальна група - це спільнота, в якій інформаційний простір завалений безладною інформацією, а активність учасників є низькою або середньою. Вона публікує інформацію з різних сфер, але ця інформація не має структури. У спільноті відсутні чіткі правила та стратегія ведення. Вона може бути створена з певною метою, але через неефективність адміністрування спільнота може втратити свою активність і важливість. Відсутність стратегії розвитку призводить до того, що спільнота не приносить користі учасникам, оскільки вони не працюють для досягнення конкретних результатів, а лише для поширення необробленої інформації. Без структурованості контенту публікацій інформація часто губиться і залишається без уваги. Прогнозувати термін існування такої спільноти неможливо.

Знання різних мов сьогодні відкривають безліч можливостей у використанні інформаційних технологій. Взаємодія з користувачами на їхній рідній мові призводить приблизно до 15% успішності спільноти. Це через те, що багато учасників приєднуються до неї, щоб бути в курсі останніх новин, але понад половину учасників становлять ті, хто вивчає мову та бажає збільшити свої лексичні знання від носіїв мови. З цієї причини важливо класифікувати віртуальні групи в залежності від мови, якою вони користуються: одномовні (пов'язані з конкретною країною або регіоном) і багатомовні (використовують кілька мов в межах однієї країни або регіону) [8].

Більшість користувачів зазвичай взаємодіють з віртуальною групою, яка відповідає їхньому регіону або країні. Порівнюючи цю інформацію з їхнім місцем розташування, можна класифікувати віртуальні групи за населеними пунктами, регіонами, країнами і світовим рівнем. Віртуальні групи населеного пункту мають інформацію про події, які відбуваються в конкретному населеному пункті, і часто їх веде місцева влада. Кількість учасників не змінюється значно, оскільки вони обмежені жителями цього населеного пункту. Вони містять інформацію про місцеву спільноту та інформативний контент. Щодо онлайн-спільнот регіону, тут

кількість учасників трохи більше, але не значно (наприклад, області або райони). Тип інформаційного наповнення не відрізняється від попереднього аналізу. Якщо йдеться про віртуальні спільноти держави або світу, то це масштабні спільноти, які часто займаються розвиваючою та політичною діяльністю. Вони охоплюють велику кількість учасників, проте вимагають уважного відбору та коректності інформації.

З технічної точки зору - соціальна мережа дає можливість користувачам Інтернету об'єднуватися в спеціальних веб-ресурсах для спілкування. Інтерфейс соціальної мережі дозволяє користувачам реєструватися. Математично, соціальну мережу можна розглядати як граф, де користувачі або організації виступають у ролі вузлів, а стосунки між ними відображаються ребрами цього графа [9].

Аналізуючи сферу створення віртуальних спільнот, дослідниками було ідентифіковано ключові складові, які мають велике значення на етапі створення та управління діяльністю спільнот (рис. 1.2). Використовуючи можливості мови UML, було розроблено схематичне зображення взаємодії важливих компонент віртуальної спільноти. Це стало можливим, оскільки UML надає найкращу можливість відобразити взаємозв'язок між сутностями, інтерфейсами та компонентами [10].

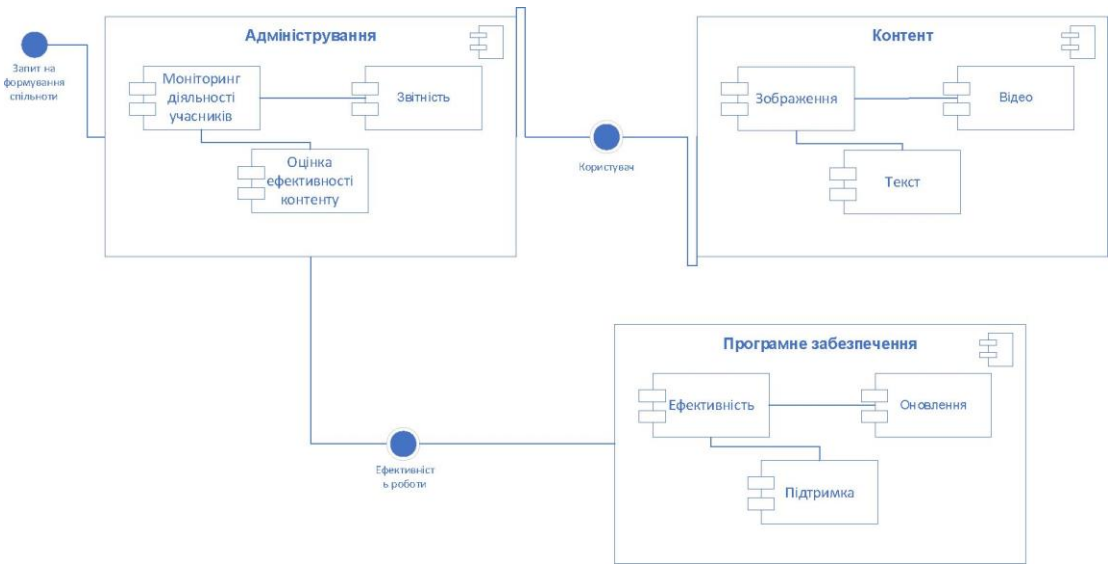


Рисунок 1.2 – Компоненти соціальних груп

Спочатку, слід зазначити клієнта. У соціальних спільнотах він відіграє роль модератора у формуванні потреби віртуальної спільноти. Визначає бюджет, встановлює свої цілі, визначає тематику тощо. Від нього надходить запит на створення спільноти. Клієнтом може бути одна особа або група осіб, які виявляють потребу в створенні віртуального середовища.

Інформаційним наповненням віртуальної групи відповідає адміністратор або менеджер, який розробляє стратегію презентації різних видів контенту (текст, зображення, відео, опитування). Він також готує звіти перед клієнтом згідно з установленими термінами. Адміністратор аналізує активність користувачів та їхні потреби, і може вирішувати, чи необхідно використовувати додаткові методи просування спільноти.

Учасник - це основний споживач контенту в діяльності віртуальних спільнот. Для нього формується наповнення, аналізуються потреби та активність віртуальної спільноти. Критеріями для нього є візуальне представлення, інформативність, програмне забезпечення та можливості, які надає використання віртуальної спільноти.

Щодо наступної складової віртуальної спільноти, контенту, це він формує основний споживацький попит на інформацію, що позиціонується, як вона буде подаватися та наскільки довго вона зможе втримати користувачів. Важливо не боятися експериментів з подачею різних видів інформації: текст, зображення, відео, опитування. Основними вимогами є максимальна інформативність та корисність, можливість висловити свою думку, обговорити та поділитися своїми судженнями.

Пристроєм, який виступає своєрідною оболонкою для роботи з віртуальною спільнотою, є програмне забезпечення. Від нього залежать можливості, ефективність та функціональність проведення різних видів операцій. Також важлива можливість оновлення, швидкого освоєння структури та підтримка розробників. Сьогодні існує безліч технологій для розробки віртуальних спільнот, але важливо вибирати те, яке відповідає запитам користувачів.

Загально об'єднавши найбільш популярні соціальні мережі, можна виділити такі особливості взаємодій між користувачами [11]:

– слідування (фолловінг) - це можливість стежити за оновленнями та новим контентом на сторінці особи, на яку ви підписані (фоловер);

– особисті сторінки - це профілі з відкритою або приватною інформацією про власника сторінки, які містять стрічку постів користувача;

– групи або спільноти - це сторінки в соціальних мережах, які об'єднують специфічну групу людей, зацікавлену в контенті, що генерується цією спільнотою. Зазвичай такі сторінки є публічними.

1.2 Дослідження методів інформаційного впливу в соцмережах в умовах війни

Інформаційний вплив в соціальних мережах включає в себе різноманітні методи та підходи для досягнення певних цілей, таких як розповсюдження інформації, підвищення обізнаності, вплив на громадську думку і багато інших.

Інформаційна боротьба представляє собою важливий компонент гібридної війни, яку російська федерація веде проти України. Ця форма конфлікту включає в себе різні методи та стратегії впливу на сферу інформації: від окремих інформаційно-психологічних чи інформаційно-технічних дій до систематичних і спланованих впливових заходів з метою вплинути на свідомість та поведінку людей, поширюючи передбачену, неповну або недостовірну інформацію для спрямування їх на вигідні для ініціатора інформаційного впливу дії [12]. Головними об'єктами цього деструктивного інформаційного впливу виділяють [13]:

– ідеологічно-психологічне оточення суспільства;

– система розроблення та прийняття політичних рішень;

– система формування громадської свідомості та думки;

– поведінка окремих людей;

– інформаційна інфраструктура та інформаційні ресурси.

Основним об'єктом атак є свідомість окремої особи, прихований вплив на яку реалізується через її психіку та нервову систему, переважно на підсвідомому рівні, "обходячи свідомий контроль, через сферу неусвідомлених, і несвідомих реакцій людської психіки". У зв'язку з особливостями вікового розвитку дитини, частина такого прихованого впливу на неї є значною, ніж на дорослих, і тому становить значну загрозу її безпеці.

Одним із основних видів інформаційно-психологічного впливу є пропаганда. Пропаганда має значний вплив на світогляд людини, оскільки вона створює та поширює ідеї, переконання, а також впливає на спосіб, яким люди сприймають і розуміють світ навколо себе. Вплив пропаганди на світогляд може бути дуже сильним і може призвести до змін у переконаннях та поведінці людей. Пропагандою називається процес поширення та популяризації ідей різного характеру, таких як політичні, філософські, наукові, художні, та інші, в суспільну свідомість [14]. Основна мета пропаганди полягає в маніпулюванні свідомістю людей, спрямованому на досягнення певних цілей через виклик певних емоцій у аудиторії, а її головною функцією є створення уявної, паралельної реальності. Тому для успішної пропаганди використовують різні засоби та техніки для сприйняття аудиторією.

Пропаганда нерідко використовує широкий мас-медійний простір з його технологічними та мультимедійними можливостями для масового, швидкого та ефективного впливу на суспільство.

Досліджуючи соціальні мережі в контексті інформаційних війн, важливо звернути увагу на психологічні явища, які роблять мережі привабливими для здійснення інформаційно-психологічного впливу на користувачів [15]. Зокрема, можна відзначити наступні аспекти: ефект "Спіраль мовчання" (згідно з Е. Ноель-Нойман) [16]; прояв стадного інстинкту в соціальних спільнотах; поширену

довіру до інформації, опублікованої в соціальній мережі; присутність впливових лідерів думок; бажання до самореалізації та прагнення до заміни реальності.

У той же час важливо підкреслити, що соціальні мережі є ідеальним інструментом для здійснення впливу, та для збору необхідної інформації. Фактично, користувач соціальної мережі, навіть не усвідомлюючи цього, стає абсолютно беззахисним перед можливими вторгненнями в його особисте життя. Наприклад, дослідники з Кембриджського університету дослідили, що навіть спосіб, яким користувач ставить "лайки" на Facebook, може розкрити багато інформації про нього [17]. Сучасні комп'ютерні програми надають можливість збирати всю доступну інформацію з соціальних мереж.

У останні роки, соціальні мережі активно використовуються в інформаційних конфліктах більш інтенсивно, ніж традиційні засоби масової інформації, такі як телебачення та газети [18].

У мультиагентній моделі соціальної мережі, ключовими поняттями є агенти, вплив, управління і репутація, та ми використовуємо ці терміни для опису структури, що складається з групи агентів [19]. Початок будь-якого конфлікту супроводжується раптовим збільшенням активності користувачів соціальних мереж, що функціонують в Інтернеті. В цей час створюються спеціальні віртуальні та соціальні групи, головною метою яких є підтримка та консолідація всіх, хто підтримує відповідні політичні погляди. Основним завданням таких груп є ініціювання та координація інформаційної пропаганди та роз'яснювальних заходів. Тому соціальні мережі стали не лише інструментом формування громадської думки, але і засобом впливу на формування переконань. Модель інформаційного впливу надає можливість вивчати, як поведінка суб'єкта залежить від його рівня інформованості, цілей та зовнішніх інформаційних впливів.

У мультиагентних системах кожен вузол представляє окремого актора або агента в цій мережі, а зв'язки відображають взаємовідносини між вузлами [19]. Моделі соціальних мереж можуть бути дуже складними і включати в себе різні рівні зв'язків - від особистих до національних та загальнолюдських.

Розглянемо деякі моделі виявлення інформаціоннного впливу в соціальних мережах: [20]

– моделі порогового впливу, включаючи лінійні моделі, де агенти можуть бути в активному або пасивному стані, і можуть переходити тільки з пасивного стану в активний (зворотний перехід відсутній);

– моделі Ізінга;

– моделі незалежних каскадів;

– моделі поширення та зараження;

– моделі, побудовані на основі ланцюгів Маркова;

– моделі, засновані на клітинних автоматах.

Якщо ефект інформаційного впливу залежить виключно від рівня інформованості та взаємодій між агентами, можна використовувати стандартну теорію ігор. Виграші актора залежать від дій його "друзів". В загальному, до теоретико-ігрових моделей інформаційного впливу включають такі підходи:

– взаємна інформованість;

– моделі комунікації та пошуку мінімально достатньої мережі;

– узгоджені колективні дії;

– стійкості мережі;

– моделі інформаційного протиборства;

– моделі інформаційного впливу та управління.

Інформаційний вплив можна розглядати у двох основних аспектах:

– зміна необхідних даних, які використовує інформаційно-аналітична система об'єкта впливу при ухваленні рішень;

– прямий вплив на процес ухвалення рішень об'єктом впливу, такий як вплив на процедури прийняття рішень або окремі особи, що роблять рішення.

Моделювання соціальних процесів, включаючи інформаційні впливи, часто потребує проведення обчислювальних експериментів, оскільки зазвичай існують обмеження, які ускладнюють проведення "польових" природних експериментів.

Серед основних моделей інформаційного протистояння в соціальних мережах наступні [21]:

– модель мережевих атак, це складний спосіб планування, який передбачає створення псевдонімів або повідомлень, які можуть викликати конфлікти або вводити в оману учасників соціальної мережі;

– модель із залученням користувачів полягає в привертанні користувачів, які активно обговорюють певну тему, публікують коментарі, створюють записи, висловлюють критику або підтримку з певного кута зору;

– модель тотального блокування передбачає використання можливості блокування користувачів на популярних соціальних мережах.

На сьогодні існує широкий спектр спеціалізованого програмного забезпечення, яке призначене для моніторингу та аналізу контенту у Інтернеті. Віртуальний моніторинг групи передбачає постійний збір інформації з соціальних мереж для подальшого обстеження.

Однією з основних задач цього збору інформації є виявлення сторінок в соціальних мережах, які містять інформаційні матеріали, які можуть становити загрозу для національної безпеки держави та суспільства [21].

Автоматизовані системи аналізу текстів у Інтернеті зазвичай базуються на порівнянні текстових фрагментів з наперед складеними словниками. Вони оцінюють текст, враховуючи наявну емоційну лексику, та визначають, чи є він позитивним чи негативним.

Але важливо зазначити, що вміст сторінок обговорень у онлайн-спільнотах соціальних мереж створюється користувачами самостійно і має свої особливості, які включають:

– непостійний порядок слів у реченнях;

– значну кількість сленгу та ненормативної лексики з непередбачуваними значеннями;

– двозначність, емодзі та гумор, які можуть бути зрозумілі тільки при аналізі підтекстів, а не з фактичного словника, що може бути проблемою для автоматизованих систем.

Таким чином, можна зробити висновок, що на сьогоднішній день не існує відповідної та ефективної автоматизованої системи для аналізу контенту в Інтернеті [22].

Ще однією суперечливою проблемою щодо аналізу онлайн-спільнот є невизначеність оцінки інформаційної загрози, яку представляє віртуальна група.

Отже, аналіз та моніторинг інформаційних загроз у віртуальних групах соціальних інтернет-сервісах повинен виконувати такі завдання:

– проводити пошук в інформаційному вмісті сторінок обговорень онлайн-спільнот у соціальних мережах за ключовими словами;

– визначати інформаційні ризики на основі вмісту, структури зв'язків та кількості учасників спільноти;

– аналізувати інформаційний вміст сторінок обговорень онлайн-спільнот для класифікації їх як деструктивних або конструктивних, враховуючи спрямованість цього вмісту;

– надавати рекомендації щодо протидії загрозливому впливу онлайн-спільнот;

– візуалізувати структуру онлайн-спільнот.

Складність процесів взаємодії інформаційних повідомлень, їх виникнення та організація впливу на суспільство підкреслює необхідність дослідження відповідних механізмів та, відповідно, розробку моделей або повноцінних моделюючих комплексів.

1.4 Постановка задачі

На підставі наведених вище даних, завдання створення та аналізу мультиагентних моделей інформаційного впливу визнається актуальним як з теоретичної, так і з практичної перспективи. На разі не всі існуючі моделі узагальнені та досліджені у повному обсязі, і не відповідають вимогам сучасної інформаційної боротьби. Отже, в рамках магістерської роботи вибрано завдання створення, та дослідження таких моделей. Звертає на себе увагу, що наразі актуальною є задача оперативного виявлення інформаційних загроз завдяки парсингу соцмереж шляхом визначення змін у характеристиках відповідних інформаційних потоків. Таким чином, до завдань магістерського дослідження відноситься:

1. Здійснити аналіз онлайн-спільнот, та розглянути особливості їх організації в соціальних мережах в Інтернеті.
2. Розробити математичні моделі для аналізу інфополя онлайн-спільнот.
3. Створити метод виявлення інформаційного впливу, що базується на аналізі параметрів розподілу характеристик контенту в ресурсах соціальних мереж.
4. Розрахувати показник інформаційної загрози онлайн-спільноти.
5. Розробити технологію для створення баз даних на основі вмісту онлайн-ресурсів.
6. Запропонувати архітектуру системи моніторингу онлайн-ресурсів, з метою оцінки потенційної загрози онлайн-спільноти.

2 МОДЕЛЮВАННЯ ПРОЦЕСУ ФУНКЦІОНУВАННЯ СОЦІАЛЬНОЇ МЕРЕЖІ

2.1 Математичне моделювання онлайн-спільноти

Онлайн-спільноти - це групи людей, які взаємодіють, обмінюються інформацією та взаємодопомагають один одному в інтернеті [23]. Це може бути веб-форум, соціальна мережа, чат, віртуальна група електронної пошти або будь-яке інше онлайн-середовище, де користувачі збираються навколо спільної теми чи інтересу.

Онлайн-спільноти можуть бути спрямовані на різноманітні теми: від обговорення конкретної галузі чи технології до спільнот для людей із спільними хобі чи інтересами. Учасники можуть обговорювати новини, ділитися досвідом, ставити питання та взаємодіяти в інтернет-середовищі.

Онлайн-спільноти можуть мати важливе значення для підтримки, обміну інформацією та створення зв'язків між людьми, які фізично можуть бути далеко один від одного. Вони є важливим елементом цифрової культури і дозволяють людям об'єднуватися навколо спільних інтересів незалежно від географічного розташування.

Інформаційний простір онлайн-спільнот складається із [24]:

– внутрішнього інфополя, яке включає в себе простір, де розповсюджується інформація всередині спільноти між її учасниками;

– зовнішнього інфополя, яке представляє собою середовище, в якому поширюється інформація, що впливає на функціонування спільноти.

Інформація зовнішнього інфополя походить від учасників соціальної мережі, які впливають на неї і є суб'єктами інформаційного впливу.

Отже, для визначення показника загрози функціонуючої онлайн-спільноти необхідно:

– розробити загальну модель інфополя, яка описує структуру зовнішнього та внутрішнього інфополя онлайн-спільноти;

– уточнити модель внутрішнього інфополя для відображення структури інформації (інформаційного наповнення) в елементах онлайн-спільноти;

– розробити модель інформаційного наповнення онлайн-спільноти та її елементів для подальшого аналізу.

Згідно з визначенням соціальної мережі як інтернет-сервісу, це застосунок, який надає можливість зареєстрованим користувачам розміщувати інформацію про себе та взаємодіяти один з одним [25].

Тоді можемо формалізувати модель соціальної мережі:

$$SocialNetworks = \langle Members, Content, Link \rangle \tag{2.1}$$

де $Members$ – це зареєстровані користувачі мережі;

$Link$ – мережа зв'язків між користувачами;

$Content$ - контент (інформаційне наповнення).

Згідно з визначенням онлайн-спільнота (англ. virtual communities,) - тип груп, які виникають і функціонують в електронному з метою сприяння вирішенню різного виду задач, наприклад професійних, політичних, задоволення своїх інтересів у мистецтві, спорті, навчанні, тощо [26].

Технічні характеристики віртуальних спільнот. Технічні показники характеристики віртуальних спільнот описують способи забезпечення її функціонування в мережевому середовищі: засоби хостингу, програмні засоби, мови розмітки, оформлення розміщених матеріалів, доступність зовні спільноти та для автоматизованих сервісів збору даних (таких як глобальні пошукові системи). Зазначимо, що сьогодні існує два головні класи технічної організації спільнот:

– на базі автономних програмно-технічних платформ;

– на базі глобальних соціальних сервісів, зокрема соціальних мереж та

спеціалізованих мультимедійних хостингів.

Із точки зору комунікативних процесів та впливу на інформаційний простір держави обидва підходи до організації спільнот є важливими і певною мірою схожими. На практиці основні відмінності між використанням обох типів середовищ в інформаційній діяльності і в процесах інформаційного протистояння лежать саме в програмно-технічній сфері. Пропонований далі перелік формальних показників є узагальненим для обох підходів, відмінності є лише між алгоритмами, що їх використовують, та ступенем програмної реалізації таких алгоритмів (табл. 2.1).

Таблиця 2.1 – Технічні показники онлайн-спільноти

Показник	Коментар
Тип платформи	(форум, мультимед. хостинг, соцмережа...)
Мережевий ідентифікатор платформи	Мережева адреса сайту, головний URI платформи
Вербальний ідентифікатор платформи	Банер або назва сайту, за яким він знаходиться при зміні адреси
Мережева адреса онлайн-спільноти	Адреса головної сторінки онлайн-спільноти
Вербальна адреса онлайн-спільноти	Банер або назва онлайн-спільноти, де вона знаходиться у разі зміни адреси
Макрокод внутрішнього пошуку	Спооби пошуку в межах онлайн-спільноти
Макрокод зовнішнього пошуку	Способи пошуку в межах онлайн-спільноти

Тоді, формалізована модель онлайн-спільноти визначатиметься, як модель соціальної мережі (2.1), з інформаційним наповненням та її зареєстрованими учасниками:

$$VirtualCommunity = \langle Content, Member \rangle, \quad (2.2)$$

де $Content$ - інформаційний контент;

$Member$ - діапазон учасників.

Розглядаючи можливості використання інструментів соціальних мереж для ініціювання обговорень на визначену тематику (контент), рекомендується розглядати структуру спільноти в соціальних мережах як сукупність обговорень, створених зареєстрованими користувачами за допомогою інструментів соціальних мереж. Ці користувачі об'єднуються за спільною метою, ідеологією спілкування та взаємодіють як в межах конкретної дискусії, так і з іншими обговореннями у віртуальній групі та іншими групами.

Отже, інфополе спільноти визначається як сукупність онлайн-спільнот (сторінок обговорень в соціальних мережах), які об'єднуються за критеріями інформаційного наповнення, а також акторів зовнішнього впливу (сторінки в соціальних мережах, які не є сторінками обговорень), і зв'язками між ними [27].

На рис. 2.1 наведено елементи зовнішнього інфополя онлайн-спільноти в соцмережах.

Рисунок 2.1 - Зовнішнє інфополе соцмереж

У онлайн-спільнотах соціальних мереж значущу роль відіграють агенти (актори) зовнішнього впливу, серед яких особливо варто відзначити Інтернет-ЗМІ, блоги політиків та відомих особистостей. Ці елементи формують інформаційний простір груп, впливаючи на сприйняття та обговорення контенту.

Інтернет-ЗМІ, такі як новинні сайти та онлайн-журнали, є джерелом актуальної інформації, яка стає об'єктом обговорення в онлайн-спільнотах. Їхні публікації можуть визначати теми дискусій та суттєво впливати на динаміку обговорень [28, 29].

Блоги політиків стають платформою для вираження їхніх поглядів та ініціації обговорень. Ці політичні лідери використовують такий інструмент для взаємодії з громадськістю та формування своєї позиції в групових дискусіях.

Відомі особистості, будь то спортсмени, актори чи громадські діячі, також впливають на віртуальні групи через свої блоги. Їхні думки та висловлювання можуть викликати обговорення та впливати на формування групових переконань.

Усі ці актори зовнішнього впливу спільно визначають інфополе спільнот у соціальних мережах, надаючи матеріал для обговорень, визначаючи теми та впливаючи на загальну динаміку в групах. Їхня роль полягає не лише в наданні контексту, а й у формуванні активної взаємодії та різноманітності поглядів серед учасників [30].

Тінь онлайн-спільноти представляє собою аспекти та вплив, які можуть існувати поза видимою поверхнею самої групи в соціальних мережах [31]. Ця "тінь" може включати в себе неформальні зв'язки, неофіційні обговорення, а також впливових осіб, які не є офіційними учасниками групи, але можуть впливати на неї.

Неформальні зв'язки можуть виникнути між учасниками групи поза основними обговореннями. Це може включати приватні повідомлення, особисті думки та відносини, які можуть визначити тон і атмосферу групи. Такі неформальні взаємодії можуть створювати "тінь" або складову, яку не завжди легко виявити на поверхні.

Додатково, впливові особи, які можуть не брати безпосередньо участі в дискусіях, також формують тінь спільноти. Це можуть бути модератори, адміністратори або навіть зовнішні сторони, які мають значущий вплив на обговорення, але можуть залишатися непомітними для більшості учасників.

Крім того, тінь онлайн-спільноти може включати інформацію чи вплив зовні групи, такий як реклама, боти чи фейк-акаунти, які можуть спрямовувати або спотворювати обговорення.

Таким чином, розуміння тіні спільноти є ключовим для повного усвідомлення внутрішньої динаміки групи та її взаємодії з оточуючим середовищем [32].

Зовнішнє інфополе онлайн-спільноти та її елементів, представимо у такій формі:

$$InfSpace = \langle VirtualCommunity, AgentInfl, Shadow(VirtualCommunity), LinkExternal(VirtualCommunity), LinkExternal(AgentInfl) \rangle, \quad (2.3)$$

де $VirtualComumunity$ – це сукупність онлайн-спільнот;

$Shadow(VirtualComumunity)$ – сукупність зареєстрованих користувачів соцмережі, тіньової групи.

$LinkExternal\ (VirtualComumunity)$ – множина зв'язків між онлайн-спільнотами;

$AgentInfl$ – це множина зовнішніх акторів, таких як інтернет-ЗМІ, відомі особистості, блоги політиків;

$Link Ex1ernal(AgentInfl)$ – множина зв'язків між онлайн-спільнотами та зовнішніми акторів, які мають вплив на спільноту.

Розглядаючи внутрішнє інфополе спільноти, можна подивитися на його складові частини. Віртуальна спільнота, що існує в інформаційному просторі, представляє собою збірну онлайн-спільноту, де учасники обмінюються інформацією та взаємодіють один з одним.

Матриці зв'язків розглядають взаємодію спільнот між собою та з акторами, наприклад зовнішнього впливу. Це може включати обмін інформацією, реакції на публікації та вплив на обговорення.

Таким чином, внутрішнє інфополе спільноти включає в себе взаємодію учасників, вплив зовнішніх факторів та неофіційні взаємодії, які формують обговорення та динаміку групи в цілому.

Функціонування онлайн-спільноти - це комплексний процес, що охоплює різноманітні аспекти взаємодії учасників у віртуальному просторі. Учасники приєднуються до спільноти, розділяючи свої інтереси, думки та інформацію через публікації, коментарі та взаємодію з іншими [32].

Спільноти виникають навколо різноманітних тем і можуть мати різний характер - від невеличких груп, що обговорюють конкретні теми, до великих спільнот, що об'єднують людей за різними інтересами чи цілями. Зміст та обговорення, які генеруються учасниками, стають центральною частиною функціонування спільнот.

Взаємодія відбувається через різні форми комунікації, такі як коментарі, особисті повідомлення, обговорення та інші віртуальні інструменти. Це дозволяє учасникам виражати свої думки, обговорювати теми та взаємодіяти з різними точками зору.

Модерація відіграє важливу роль у забезпеченні впорядкування та дотримання правил у групі. Модератори можуть вирішувати конфлікти, визначати тематику групи та впливати на загальну динаміку обговорень [33].

Модерація онлайн-спільноти є важливим аспектом забезпечення здорової та продуктивної взаємодії між учасниками. Модератори виступають в ролі своєрідних кураторів, що визначають та контролюють внутрішні правила, а також сприяють формуванню позитивного середовища в групі.

Однією з ключових функцій модерації є встановлення та виконання правил. Модератори визначають, які види контенту є прийнятними та відповідають меті спільноти, а які можуть бути видалені. Вони надають учасникам чіткі вказівки

щодо стандартів поведінки, що сприяє створенню безпечного та приємного середовища.

Модератори також вирішують конфлікти та виправляють ситуації, що можуть призвести до негативного впливу на атмосферу групи. Вони можуть спрямовувати розмови в конструктивне русло, розвивати дисципліну та вживати заходів для попередження або вирішення конфліктів.

Окрім цього, модератори відіграють роль фасилітаторів обговорень, сприяючи взаємодії та залученню учасників. Вони можуть створювати теми для обговорення, стимулювати активність та сприяти розвитку спільноти.

У цілому, модерація - це комплексний підхід до управління спільнотою, який стежить за дотриманням правил, розвитком позитивного спілкування та забезпеченням комфортного середовища для всіх учасників.

Приклад структури онлайн-спільноти наведено на рис. 2.2.

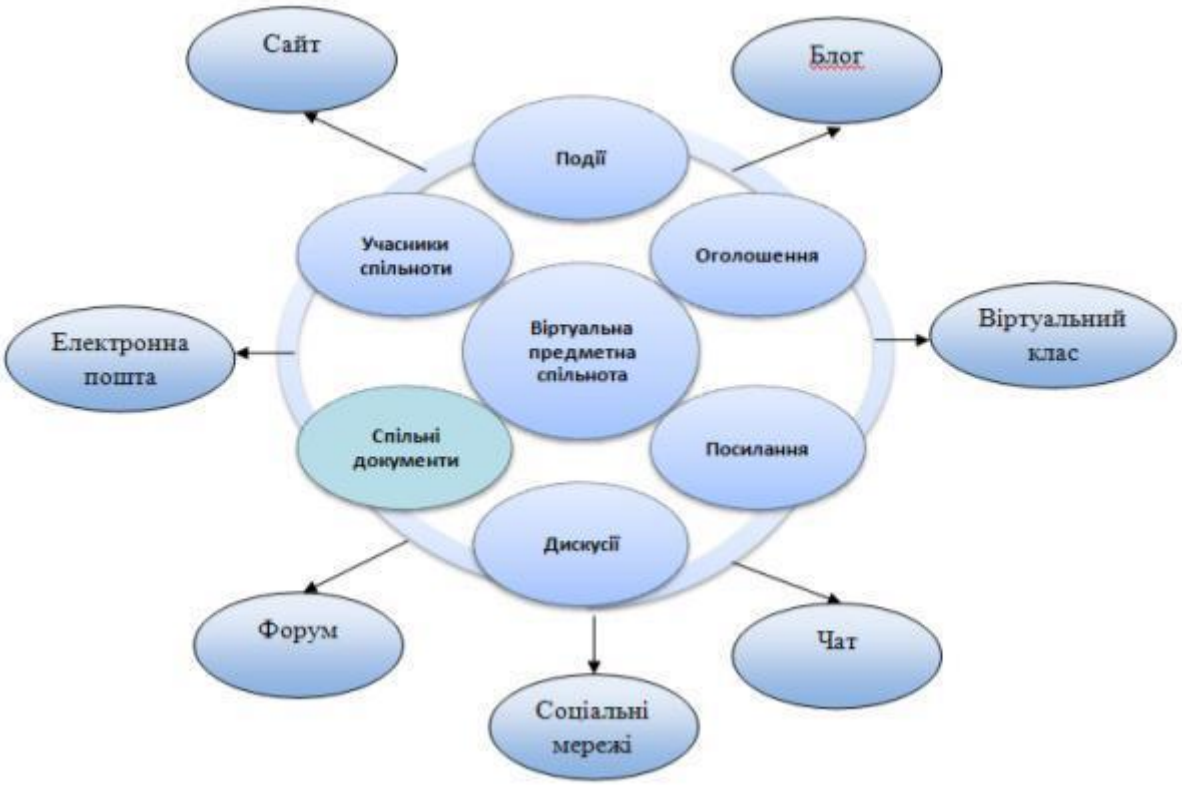


Рисунок 2.2 - Структура онлайн-спільноти

Також спільноти можуть розвиватися та змінюватися з часом. Нові теми можуть з'являтися, коли приєднуються нові учасники, або коли інтереси поточних змінюються. Онлайн-спільнота, таким чином, є динамічним середовищем, що живе та змінюється разом зі своїми учасниками.

Враховуючи (2.3), запропонуємо модель внутрішнього інфопростору онлайн-спільноти відносно моделі (2.2). Тоді ця модель має вигляд:

$$InfSpace(VirtualCommunity_i) = \langle Thread(VirtualCommunity_i), \; LinkInternal(Tread), \; Member(VirtualCommunity_i), \; Shadow(VirtualCommunity_i) \rangle, \tag{2.4}$$

де $Thread(VirtualCommunityi)$ - множина форумів *i*-ї онлайн-спільноти;

$Member(VirtualCommunityi)$ - множина учасників форумів *i*-ї спільноти, зареєстровані користувачі соціальних мереж;

$LinkInternal(Thread)$ - сукупність зв’язків між форумами *i*-ї онлайн-спільноти;

$Shadow(VirtualCommurityi)$ - сукупність зареєстрованих користувачів соцмереж, які проявляють зацікавленість тематикою *i*-ї онлайн-спільноти.

2.2 Просторова модель онлайн-спільноти

Інформаційне наповнення сторінок дискусій в соціальних інтернет-сервісах є важливим елементом взаємодії та обміну ідеями серед учасників. Кожна сторінка дискусії, будучи власною віртуальною ареною, збирає в собі різні форми контенту та вираження поглядів [33].

Зображення та графіка відіграють ключову роль у визначенні візуального аспекту сторінок дискусій. Графічні елементи можуть включати меми,

ілюстрації, фотографії чи інші візуальні матеріали, які допомагають вирізнятися серед інших дискусій та звертати увагу учасників.

Текстовий контент є основною складовою частиною дискусійних сторінок. Учасники розміщують повідомлення, коментарі, аналізуючи та обговорюючи теми, що їх цікавлять. Тексти можуть бути як короткими і ємкими, так і детальною аргументацією, в залежності від характеру дискусії та стилю взаємодії.

Посилання на сторінках обговорень додають додатковий контекст та можливість деталізації інформації. Учасники можуть поділитися посиланнями на статті, новини, відео чи інші ресурси, щоб підкріпити свої аргументи або запропонувати додатковий контент для обговорення.

Крім того, інтерактивні елементи, такі як опитування, голосування, анкети, також можуть збагачувати сторінки дискусій, створюючи можливості для активного участі та висловлення власної думки.

Таким чином, інформаційне наповнення сторінок дискусій у соціальних мережах формується відмінним поєднанням візуального, текстового та інтерактивного контенту, що створює унікальне та захоплююче враження для учасників.

Текстова інформація є головною складовою обсягу інформаційного наповнення, становлячи до 80% від загального обсягу. З цієї причини для аналізу інформаційного наповнення спільноти використовується просторова модель, що базується на векторній моделі опису даних [34]. В рамках цієї моделі обговорення спільноти представлено вектором у евклідовому просторі, де кожному терміну, що використовується в обговоренні, призначений ваговий коефіцієнт. Його значущість визначається на основі статичної інформації про його повторення в конкретному обговоренні та в інших обговореннях спільноти.

Для формалізації обговорення використовується модель, що складається з назви обговорення, його опису та множини повідомлень, що належать до даного обговорення:

$$ThreadTitle_i^{(Term)} = \{Term_j\}_{j=1}^{N_i^{(TT)}},$$

де змінна $Term\ j$ один із термів i-ї дискусії;

$N(TT)$ – їх загальна кількість.

Опис форуму $ThreadTitle$ - це сукупність термів, з яких формується опис обговорення.

Текст повідомлення описується у $PostText$.

Тому, множина обговорення складається із термів назви форуму, його опису та текстів повідомлень:

$$Thread_i^{(Term)} = ThreadTitle_i^{(Term)} \bigcup ThreadDiscription_i^{(Term)} \bigcup_{j=1}^{N_i} PostText_{ij}^{(Term)}, \quad (2.5)$$

Множина термів онлайн-спільноти формується із множини термів обговорень (2.5):

$$VirtualCommunity^{(Term)} = \bigcup_{i=1}^{N} Thread_i^{(Term)}, \quad (2.6)$$

Відповідно до (2.6) запропонована просторова модель дискусії має вигляд:

$$\overline{Thread}^{(Term)} = \langle Term, W \rangle, \quad (2.7)$$

де $Term$ - множина існуючих обговорень;

N – їх кількість;

W - вагові коефіцієнти;

Побудова просторової моделі обговорень із (2.6) поділюється на декілька

етапів:

– виділення основи термів;

– видалення не важливих термів, (стоп-слів) або тих, які тільки обмежену кількість раз раз трапляються в обговорені;

– формування частоти використання термів в обговореннях у вигляді матриці;

– оцінка правильності формування вагових коефіцієнтів термів.

Кластеризація інформаційних потоків є важливим етапом в аналізі великих обсягів даних, призначеним для групування подій, об'єктів або документів з подібними характеристиками чи темами [35, 36]. Цей процес використовує різноманітні методи для виявлення структури та патернів в наборах даних без конкретного перерахування.

Методи машинного навчання, такі як *k*-середні, ієрархічна кластеризація чи агломеративні підходи, можуть автоматично групувати схожі об'єкти в кластери. Також може використовуватися тематичне моделювання, яке дозволяє виявляти теми в текстових документах та групувати їх за спільними концепціями, що спрощує аналіз великих обсягів текстової інформації.

Крім того, аналіз спільнот у графах може використовуватися для виявлення спільнот чи груп взаємозв'язаних об'єктів у мережі, що може включати обговорення спільнот чи взаємодії між користувачами соціальних мереж.

Векторна кластеризація, заснована на векторних моделях, таких як TF-IDF, може визначати ступінь схожості між різними документами та групувати їх відповідно до цієї схожості.

Такий підхід допомагає винятково краще розуміти структуру та властивості великих обсягів інформації, сприяє виявленню ключових тем та забезпечує можливість ефективного подальшого вивчення та аналізу.

У сфері кластеризації інформаційних потоків у мережі Інтернет великою мірою використовується міра оцінки термів, яка виявляється особливо ефективною - TF-IDF (Term Frequency-Inverse Document Frequency) [37].

Ця міра враховує два ключових аспекти для визначення значущості термінів. По-перше, частота терму вказує на те, наскільки часто конкретний термін зустрічається в окремому документі, надаючи йому вагу в контексті цього документа. По-друге, інверсійна частота документа враховує, наскільки часто термін взагалі зустрічається в множині документів. Це дозволяє виділяти терміни, які є важливими для конкретних документів, але рідко зустрічаються в загальному корпусі, надаючи їм великий рейтинг [38].

Такий підхід є ефективним інструментом для кластеризації інформаційних потоків через кілька причин. Вын дозволяє зменшити вагу загальних та часто вживаних термінів, надаючи важливість термінам, які є унікальними для конкретних документів чи кластерів. Крім того, цей підхід підкреслює контекстуальну значущість термінів, адже враховує їх важливість у конкретних документах, а не просто їх частоту в корпусі текстів.

Тому це може стати потужним інструментом для аналізу текстової інформації в Інтернеті, забезпечуючи ефективну кластеризацію та визначення важливих тематичних рис серед інформаційних потоків.

Для ефективного визначення вагових коефіцієнтів термів доцільно запросити експертів, але можна застосовати $if * idf$ як міру оцінки словоформ [39], де if - локальна частота словоформи (Term Frequency), idf - величина, обернена частоті появи в усьому потоці, що містять цю словоформу (Inverse Document Frequency).

Враховуючи це, відповідно до (2.7), просторова модель онлайн-спільноти буде мати вигляд:

$$\overline{VirtualCommunity}^{(Term)} = \langle Term, W \rangle, \qquad (2.8)$$

де $Term = \{term_i\}_{i=1}^{N}$ - множина словоформ обговорення;

$W = \{w_i\}_{i=1}^{N}$ - вагові коефіцієнти словоформ обговорення;

N - кількість словоформ в обговорені.

Зріз онлайн-спільноти розраховуємо як середнє арифмитичне векторного подання обговорень.

Принцип Парето, також відомий як принцип 80/20, розповідає про те, як в багатьох ситуаціях невелика частина входить в силу великої частини. Цей принцип був названий на честь італійського економіста Вільфредо Парето, який вперше описав його, спостерігаючи нерівномірність розподілу багатства в суспільстві [40].

Цей принцип можна застосовувати в різних сферах життя: в економіці, управлінні ресурсами, навчанні та багатьох інших. Він наголошує на тому, що існує концентрація важливості у невеликій частині, і важливо розуміти та використовувати цей принцип при прийнятті рішень та оптимізації ресурсів.

Якщо застосовувати принцип Парето до утворення інформаційного наповнення дискусії, можна стверджувати, що лише двадцять відсотків термінів мають великий внесок у весь контент, а інші вісімдесят відсотків внеску розподіляються на решту термінів. Отже, при визначенні важливих термів для дискусій та спільноти обирають саме ці двадцять відсотків, які володіють найвищими ваговими коефіцієнтами. Цей відбір виконується відповідно до просторової моделі, яка аналізує інформаційні внески та ваги термів у контексті дискусії та спільноти. Цей підхід допомагає визначити ключові аспекти обговорень, спрощуючи подальший аналіз та розуміння важливих тематик.

2.3 Визначення показника загрози онлайн-спільноти

В процесі подальшого вивчення дискусій та їх класифікації на різні типи, метою є використання мір відповідності позитивних та негативних повідомлень. Ці показники служать ключовими факторами при визначенні, наскільки конструктивними чи деструктивними є віртуальні групи.

Класифікація членів віртуальних груп наведено на рис. 2.3.

Рисунок 2.3 - Класифікація членів віртуальних груп соцмереж

Використовуючи ці міри, дослідники можуть ефективно розподілити обговорення між різними категоріями спільнот, розрізняючи ті, де переважають позитивні висловлення, від тих, де спостерігається більше негативних висловлень. Це допомагає виявити та аналізувати динаміку взаємодії між учасниками спільнот та визначити загальний характер обговорення.

Визначення оцінки ризику відповідно до стандарту інформаційної безпеки NIST - це процес, що включає кілька ключових етапів для систематичного аналізу та оцінки потенційних небезпек, вразливостей та можливих наслідків для інформаційних активів [41].

На початковому етапі проводиться ідентифікація активів, тобто визначення інформаційних ресурсів та систем, які мають важливе значення для організації. Це можуть бути бази даних, мережеві елементи, програмне забезпечення тощо.

Далі вивчаються потенційні загрози, які можуть стати причиною виникнення ризиків для інформаційних активів. Це може включати хакерські атаки, природні катастрофи, внутрішні помилки та інші можливі сценарії.

Визначення вразливостей полягає в ідентифікації слабких місць у системі, де можуть виникнути проблеми. Це може бути пов'язано з застарілим

програмним забезпеченням, недоліками в управлінні доступом, слабким паролем і т. д.

Далі проводиться оцінка ймовірності та впливу. Ймовірність визначає частоту можливих подій, а вплив визначає ступінь шкоди, яку може завдати кожна з них. Це допомагає визначити, наскільки часто та як великі можуть бути ризики.

Визначивши ймовірність та вплив, розраховується ризик, який визначається як добуток цих двох показників. Це дозволяє зорієнтуватися в тому, які з них є найбільшими та найбільш значущими.

Останній етап - розробка стратегії управління ризиками. Це включає в себе план дій та заходи для уникнення, зменшення чи передбачення ризиків. Ця стратегія служить як план дій для забезпечення безпеки інформаційних активів.

Оцінка ризику визначається як комплексна оцінка двох компонентів:

– обсяг втрат у випадку реалізації загрози;
– вірогідність її виникнення.

Показник інформаційної загрози спільноти є ключовим елементом для оцінки рівня потенційних ризиків, з якими ця група може стикнутися в онлайн-середовищі. Цей показник визначається комплексnov аналізом різноманітних аспектів, що охоплюють загрози та вразливості віртуального середовища [42].

У визначенні показника інформаційної загрози враховуються потенційні небезпеки, які можуть виникнути внаслідок навмисного втручання, небажаних атак або розповсюдження шкідливого контенту в межах спільноти. Також враховується стійкість та здатність групи витримувати подібні виклики.

Оцінка вразливостей спільноти є важливою складовою визначення показника загрози. Аналізується рівень захищеності від можливих атак, який включає в себе перевірку наявності необхідних заходів безпеки, які можуть запобігти неправомірному доступу або розголошенню конфіденційної інформації.

Крім того, розглядається здатність спільноти виявляти та врегулювати внутрішні конфлікти, які можуть вплинути на загальну стабільність та безпеку. Ефективність механізмів виявлення та вирішення потенційних загроз визначається як важливий фактор у визначенні показника інформаційної загрози.

Таким чином, показник інформаційної загрози спільноти є результатом комплексного аналізу забезпеченості групи та її здатності впоратися з різноманітними потенційними загрозами у віртуальному середовищі.

Тому, множину наявності зв’язків між обговореннями у спільноті представимо у вигляді матриці:

$$LinkInternal(Thread) = \left\| link_{ij} \right\|_{n*n}, \tag{2.9}$$

Щоб виявити зв'язок між спільнотами, дослідимо наявність гіперпосилань між *i*-ю та *j*-ю обговореннями в онлайн-спільноті визначають за формулою:

$$link_{ij} = \begin{cases} 1, якщо\ є\ гіперпосилання\ до\ j\text{ - ї}\ дискусії; \\ 0, відсутнє\ гіперпосилання\ до\ j\text{ - ї}\ дискусії. \end{cases}$$

Тому, показник загрози онлайн-спільноти в можна подати:

$$InfThreat(VirtualCommunity) = \begin{cases} \dfrac{Value(VirtualCommunity)}{Value(VirtualCommunity)^*}, \\ 1, якщо \dfrac{Value(VirtualCommunity)}{Value(VirtualCommunity)^*} > 1 \end{cases} \tag{2.10}$$

де, $Value\ (VirtualComunity)$– важливість онлайн-спільноти;

$Value\ (VirtualComunity)*-$ – критична цінність онлайн-спільноти, яка здатна реалізувати загрозу.

Для визначення цінності спільноти з урахуванням структури зв’язків дискусій у цій спільноті необхідно провести аналіз топології спільноти, що може визначатися через взаємозв'язки між різними дискусіями.

Топологія спільноти визначається розташуванням та організацією її складових частин - дискусій. Зв'язки між дискусіями створюють внутрішню мережу, що визначає структуру спільноти. Важливо враховувати не лише самі дискусії, але й їхні взаємозв'язки та взаємодію.

Серед ключових аспектів, що впливають на цінність спільноти, є густота зв’язків між дискусіями та їхній характер. Щільна та добре впорядкована мережа взаємодій може сприяти ефективній комунікації та обміну інформацією, що підвищує цінність групи.

Додатково, важливо враховувати різноманітність дискусій та їхню відповідність об’єднуючому принципу або цілі спільноти. Це сприяє створенню гармонійного спільнотового середовища.

Таким чином, аналіз топології спільноти, зокрема взаємозв'язків між дискусіями, є важливим етапом для зрозуміння структури та ефективності спільноти, що дозволяє визначити та підвищити її цінність.

Для визначення цінності спільноти важливо глибоко проаналізувати топологію цієї групи, яка формується на основі внутрішніх зв'язків між різними дискусіями. Топологія спільноти представляє собою взаємозв'язки та організацію цих дискусій, створюючи внутрішню мережу спільноти.

Взаємозв'язки між обговореннями визначають структуру та взаємодію спільноти. Одним із ключових аспектів є густота цих зв'язків, яка відображає щільність та активність комунікації між різними частинами групи. Висока густота може сприяти більш ефективній обмін інформацією та сприяти спільній взаємодії.

Додатково, важливо враховувати різноманітність дискусій і їхню відповідність основній меті або принципу спільноти. Збалансована та узгоджена структура групи, де дискусії взаємодіють у напрямку спільної мети, може значно підвищити цінність групи.

Такий аналіз топології спільноти дозволяє отримати глибше розуміння структури та функціональності групи. Враховуючи внутрішні зв'язки між дискусіями, можна ефективно визначити, наскільки група відповідає своїм цілям та вимогам, що визначає її загальну цінність для учасників.

Визначення критичної цінності спільноти вимагає глибокого аналізу різноманітних аспектів, що визначають її суттєвість та важливість для учасників та оточуючого середовища. Критична цінність спільноти визначається не лише її об'ємом чи розміром, але й рядом факторів, що впливають на її стратегічну та функціональну роль.

Один з ключових аспектів - це рівень активності та взаємодії між учасниками. Критична цінність спільноти може виявитися там, де спостерігається висока інтенсивність та продуктивність обміну інформацією, що сприяє досягненню загальних цілей.

Також, важливим є ступінь взаємодії між різними дискусіями та різноманітність їхніх контентів. Коли різні аспекти обговорень взаємодіють, створюючи цілісну та комплексну структуру, це підвищує значущість групи.

Крім того, враховуються такі чинники, як рівень довіри між учасниками, ступінь залученості та відповідність меті групи. Критична цінність визначається там, де існує висока довіра, активна участь та спільна мета, що робить групу стратегічно важливою для своїх членів.

Отже, визначення критичної цінності спільноти - це комплексний підхід, що базується на взаємодії та взаємозв'язках між різними елементами структури та функціонування групи.

Один з методів визначення критичної цінності спільноти полягає у визначенні кількості учасників, при якій реалізується певна інформаційна загроза, як експертами. Однак цей підхід не враховує якість інформаційного наповнення та структуру взаємозв'язків дискусій в групі. Розрахунок показника інформаційної загрози встановлює його значення у межах від 0 до 1, спрощуючи при цьому процес прийняття рішень щодо взаємодії з інформаційним впливом на функціонування онлайн-спільноти.

2.4 Висновки

Отже, у другому розділі запропоновано низку математичні моделі, які дозволяють формалізувати й кількісно оцінити інфополе і процеси у спільнотах соціальних інтернет-сервісах.

Зокрема, побудовано модель структури інфополя спільноти, що враховують як внутрішні, так і зовнішні інформаційні потоки. Також детально формалізовано перебіг обговорень всередині спільноти на рівні окремих повідомлень.

На основі цих моделей розроблено просторове подання онлайн-спільноти та її дискусій, що дає змогу застосовувати автоматизовані методи обробки даних і машинного навчання для аналізу.

В результаті отримано кількісну міру інформаційної загрози для спільноти, яка враховує ключові чинники - кількість учасників, потенціал, якість інформаційного наповнення та топологію зв’язків між дискусіями.

Запропоновані в розділі моделі становлять методологічне підґрунтя для подальшої розробки механізмів виявлення та реагування на інформаційні загрози в соціальних мережах. Вони охоплюють ключові інформаційні характеристики спільнот і дозволяють кількісно оцінювати ризики.

3 МЕТОД ВИЯВЛЕННЯ ІНФОРМАЦІЙНОГО ВПЛИВУ ЗА ПАРСИНГОМ ОНЛАЙН-СПІЛЬНОТ

3.1 Алгоритм тематичного виявлення онлайн-спільнот

В умовах війни з рашистами Україна має контролювати свій інформаційний простір, на виявлення загрозливого інформаційного впливу на громадську думку від окупантів, колаборантів, ботів, тощо.... Ворог цим займається постійно. Недавно (27.11.2023) українські хакери групи “Кібер Спротив” проникли в департамент інформації та масових комунікацій міністерства оборони ворога, та передало в розпорядження OSINT спільноти InformNapalm внутрішню документацію та можливість доступу до програмного забезпечення, яке використовує російські військові пропагандисти [43].

Ворог тотально контролює свій інформаційний простір. Влада вживає вкрай жорстких заходів для контролю внутрішнього інформаційного простору та пропаганди. Це вимагає потужної системи моніторингу ЗМІ та онлайн-ресурсів.

Як видно зі звітів російського військового відомства, обсяги аналізованих даних для виявлення "загроз" є колосальними. Для автоматизації збору та обробки цієї інформації було створено спеціалізовану програмну систему "Катюша".

Вона здійснює моніторинг ЗМІ, соцмереж, блогів та інших онлайн-джерел, аналізує настрої та тенденції за допомогою методів штучного інтелекту. Тобто фактично відбувається тотальна слідкування за громадською думкою та інформаційний контроль у країні-агресорі.

В систему щоденно додаються наклади російських друкованих ЗМІ та закордонних видань, а також проводиться контроль онлайн-спільнот (рис.3.1).

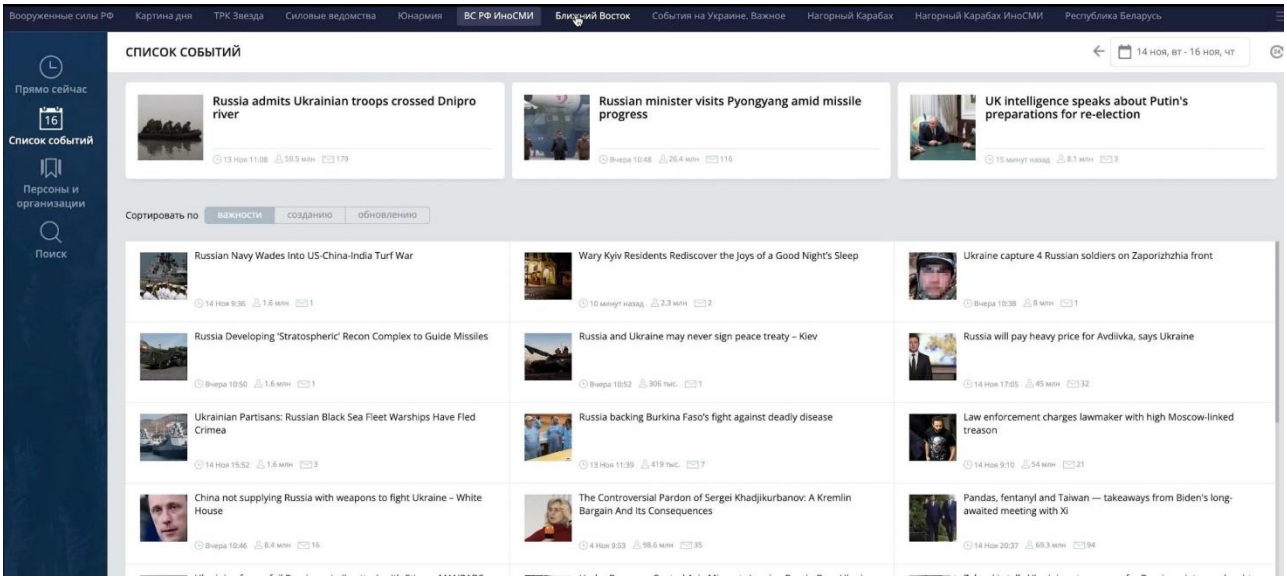


Рисунок 3.1 - Приклад відслідковування іноземних ЗМІ

Влада країни-агресора приділяє виключну увагу моніторингу соціальних мереж та контролю за ними. Це обґрунтовано кількома факторами:

– соціальні мережі є надзвичайно впливовим каналом поширення інформації та формування громадської думки;

– в соцмережах складно контролювати поширення небажаної інформації чи пропагандистських наративів влади, на відміну від традиційних ЗМІ;

– соцмережі є платформою для координації та мобілізації протестних рухів, які російська влада намагається придушити;

– алгоритми рекомендацій в соцмережах можуть посилювати резонанс небажаних тем.

Отже контроль соцмереж є критично важливим елементом російської системи інформаційної безпеки та пропаганди (рис. 3.2).

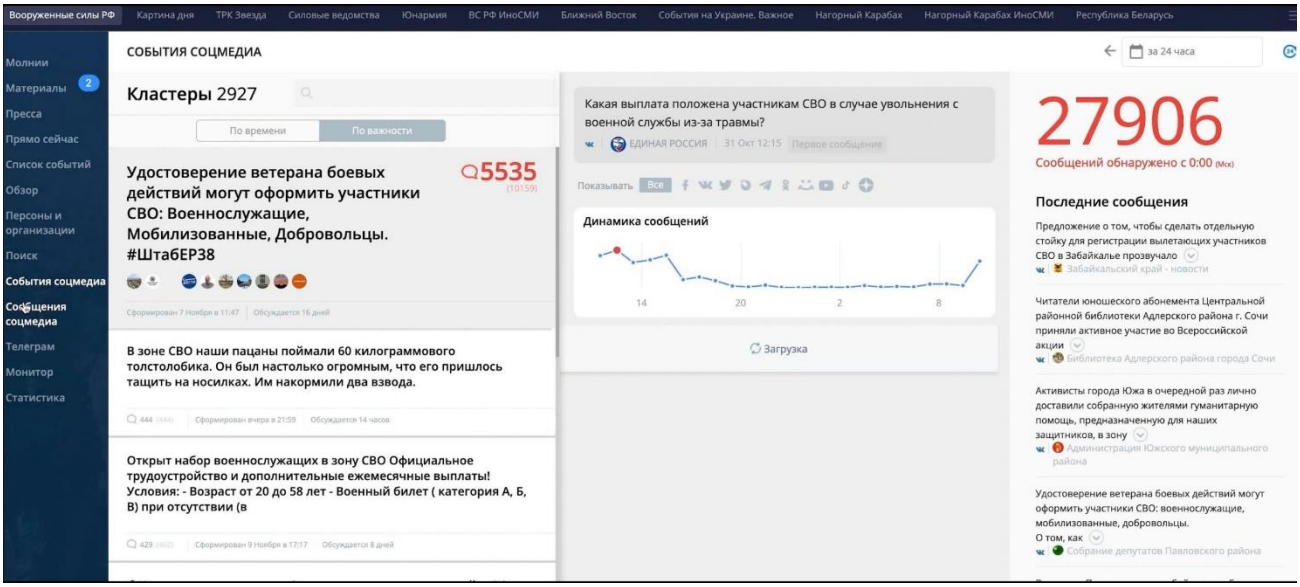


Рисунок 3.2 - Приклад відслідковування віртуальних груп в соцмережах рашистами

Тому тема дослідження є актуальною, і потрібно докласти максимальних зусиль в вдосконалені методів виявлення інформаційного впливу та насаджування наративів кремлівських методичок.

Пошук та ідентифікація сторінок дискусій в соціальних мережах лише за назвами або коротким описом може бути недостатньо ефективним. Це пов'язано з кількома особливостями. По-перше, сторінки дискусій мають низький рівень ранжування в пошукових системах соціальних мереж та не індексуються глобальними пошуковиками. По-друге, існує тісний взаємозв'язок і дублювання інформації між багатьма сторінками дискусій. На сторінках зберігаються застарілі дискусії, що не відповідають актуальним темам і потребам користувачів.

В результаті складно знайти саме ту дискусію чи інформацію, яка цікавить в даний момент, оскільки існуючі пошукові механізми соцмереж не враховують тематичне наповнення та актуальність контенту на сторінках дискусій.

Потрібні нові підходи до пошуку з урахуванням семантичного аналізу змісту дискусій та їх зв'язків між собою за ознакою актуальності.

Комплексний підхід дозволить значно точніше ідентифікувати реальний предмет обговорення на сторінках дискусій соціальних мереж, для цього необхідно:

– провести аналіз змісту останніх публікацій та коментарів на сторінці дискусії за допомогою методів обробки природної мови;

– використати графові алгоритмів аналізу груп для виявлення тематично пов'язаних дискусій, наприклад будувати граф на основі спільних учасників, перетину ключових слів тощо;

– залучити технології машинного навчання, зокрема класифікації текстів, для автоматизованого визначення тематики дискусій по їх контенту;

– провести аналіз переходів між сторінками та активності користувачів, щоб знаходити семантично пов'язані дискусії з подібною аудиторією.

Використання глобальної пошукової системи Google [44] для пошуку релевантних груп та дискусій у соціальних мережах дійсно може бути ефективним підходом, проте він має певні недоліки:

– Google не має прямого доступу до всього контенту соціальних мереж, а отже пошук не буде повним, тому він обмежується лише публічними та проіндексованими даними;

– складнощі з точним формулюванням запитів через велику кількість даних та обмежені можливості налаштування пошуку в Google;

– немає гарантій актуальності результатів пошуку, адже процес індексації займає певний час;

– відсутня можливість глибинного аналізу змісту груп та дискусій, Google аналізує лише метадані сторінок.

Тому ефективніше використовувати спеціальні засоби збору та аналізу даних безпосередньо з API соціальних мереж. Це дозволить отримати більш повну та актуальну інформацію, застосувати методи обробки природної мови, машинного навчання для глибинного семантичного аналізу груп та пошуку за релевантністю.

Запит до глобальної пошукової системи на кшталт Google для пошуку релевантних дискусій в соціальних мережах може складатися з таких основних операцій та елементів [44]:

1. Використання операторів:

– site: для обмеження пошуку певним ресурсом (наприклад, facebook.com);

– inurl: для пошуку за ключовими словами у посиланнях;

– intitle: для пошуку у заголовках сторінок;

2. Задання ключових слів або фраз, що описують тематику потрібних дискусій у лапках: "електронне урядування", "цифрова демократія" тощо.

3. Використання логічних операторів AND, OR і NOT для зв'язування ключових слів і фільтрації результатів.

4. Фільтрація за часом, мовою, регіоном, за допомогою відповідних інструментів Google.

5. Сортування видачі за релевантністю, датою, популярністю.

Комбінування цих операцій у запиті дозволяє гнучко налаштувати процес пошуку.

Загальну структуру запиту наведено на рис. 3.3.

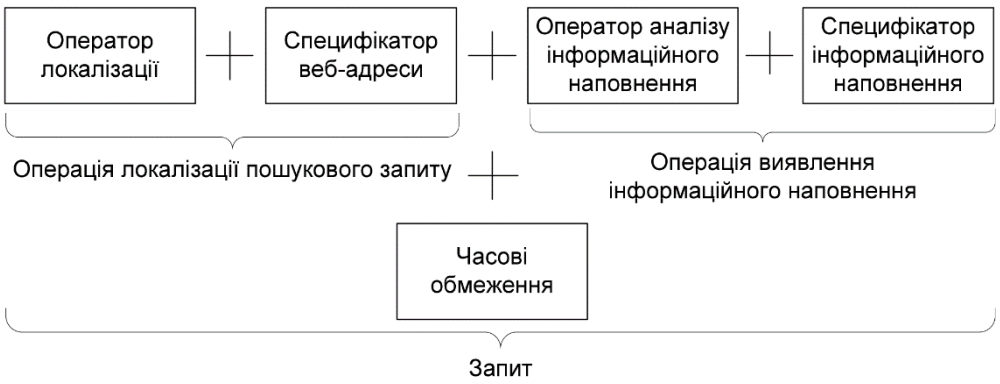


Рисунок 3.3 - Формалізований запит для тематичного виявлення онлайн-спільнот

Операція локалізації дозволяє звузити область пошуку до певного веб-сайту чи домену за допомогою спеціального оператора (site:, domain: тощо) та url адреси ресурсу.

Оператори аналізу контенту (intext:, intitle:) виконують пошук заданих ключових слів та фраз у тексті або заголовках сторінок відповідно.

Специфікатори - це ключові слова або фрази, що зазначають тематику чи інші ознаки потрібного контенту для пошуку.

Часове обмеження дає змогу знайти лише недавній актуальний контент, застосовуючи налаштування періоду публікації результатів пошуку (за останній час, день, тиждень тощо).

Комплексне використання цих операцій дозволяє гнучко налаштувати умови пошуку контенту в мережі за релевантністю запиту.

Сторінки дискусій у Facebook мають певні особливості [45]:

– вони створюються у вигляді публічних або закритих груп, куди додаються учасники, де групи можуть бути різних типів - відкриті, закриті, таємні.

– кожна група має свою сторінку з унікальною адресою та містить стрічку публікацій від учасників у вигляді постів та коментарів до них;

– також налаштовується опис, правила групи, можна створювати окремі альбоми та події;

– є можливості фільтрації та пошуку публікацій за автором, хештегами, датами.

Отже, сторінки груп у Facebook являють собою складні гіпертекстові об'єкти.

Для їх пошуку можна використовувати глобальні пошуковики з обмеженням сайту facebook.com та необхідними ключовими словами. Також Facebook має власний внутрішній пошук груп за тематиками та іменами. Це дає змогу знаходити потрібні сторінки дискусій [46].

Однією з основних особливостей сторінок дискусій у соціальних мережах є те, що їх контент часто не індексується глобальними пошуковими системами на кшталт Google чи Bing на відміну від звичайних веб-сторінок.

Причинами цього є:

– величезні обсяги даних та швидкоплинність дискусій, складно підтримувати актуальність індексу;

– закритий характер багатьох спільнот та обмеження доступу для сторонніх ботів;

– специфічна розмітка сторінок дискусій ускладнює їх аналіз та індексацію традиційними методами.

Натомість сторінки публічні профілі та пости у соцмережах значно краще індексуються глобальними пошуковиками.

Тому потрібні спеціалізовані методи аналізу саме дискусій та пошуку в них потрібної інформації

Соціальна платформа "Facebook" надає можливість користувачам створювати власні групи та сторінки груп, де вони можуть об'єднуватися за спільними інтересами. Група, або дискусія, представляє собою спільноту, де учасники можуть взаємодіяти між собою. Ці дискусії, важливо відзначити, не підлягають індексації глобальними пошуковими системами. На відміну від груп, сторінки піддаються індексації глобальними пошуковими системами.

Ця особливість дискусій забезпечує більш конфіденційне середовище для обміну інформацією та обговорень, оскільки вони залишаються поза обсягом глобального пошуку. З іншого боку, сторінки, які також доступні для створення на платформі, піддаються індексації глобальними пошуковими системами, що робить їх доступними для широкого кола користувачів Інтернету та сприяє їх виявленню та взаємодії з більшою аудиторією.

Тому здійснимо пошук у «Facebook», використовуючи формалізований запит (рис. 3.4), та проведемо подальший аналіз коду HTML-сторінки.

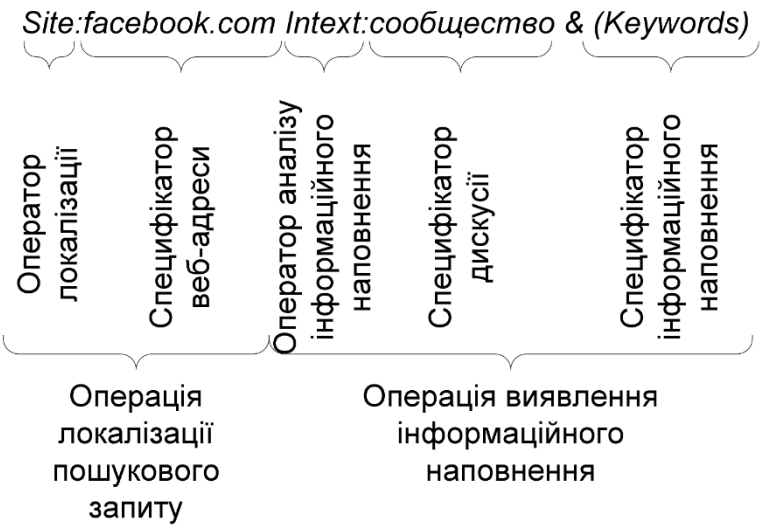


Рисунок 3.4 - Структура запиту для знаходження сторінок у «Facebook»

Для точного пошуку інформаційного контенту на соціальній мережі "Facebook" в формалізованому запиті використовується оператор intext: або intitle: разом зі специфікатором "сообщество", щоб знайти саме публічні спільноти та групи, який допомагає виокремити сторінки згідно з визначеними критеріями. Операція пошуку визначається за ключовими словами (Keywords), які є множиною ключових термінів для точного підбору інформації.

Важливим етапом виявлення зв'язаних дискусій є аналіз HTML-коду сторінок на наявність розділу "группы" (спільнота) в пункті меню. Це дозволяє строго структурувати сторінки та визначати наявність обговорень, пов'язаних із зазначеним специфікатором (рис. 3.5).

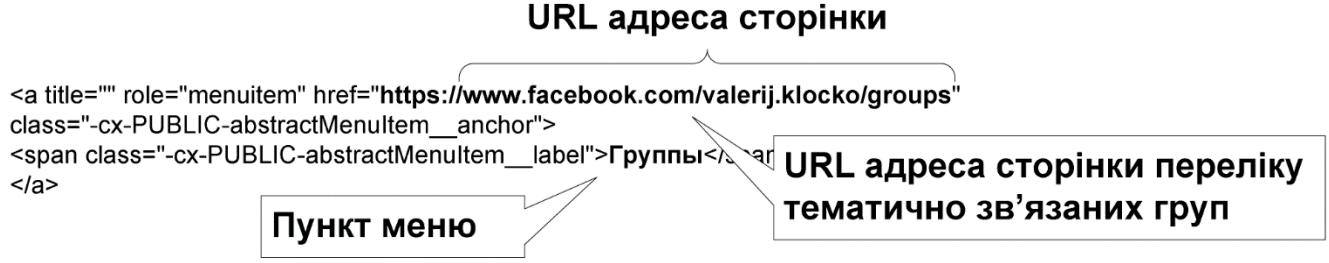


Рисунок 3.5 - Аналіз коду HTML-сторінки для виявлення переліку зв’язаних груп

У процесі формування запиту для пошуку результатів у соціальній мережі "Facebook" за частинами UPL-адрес, важливим етапом є аналіз HTML-відповіді з отриманих сторінок. Це дозволяє отримати інформацію про спільноти, використовуючи програмування та інструменти для виконання HTTP-запитів та обробки отриманих даних.

Рисунок 3.7 - Алгоритми пошуку груп у соціальних інтернет-сервісах

Схематичне зображення алгоритму формування URL-адреси тематичних спільнот наведено на рис. 3.7. Запропонований алгоритм використовує формалізовані запити пошукової системи Google та аналізу коду HTML-сторінок обговорень в групах та дозволяє здійснити їх пошук відповідно до їх інформаційного наповнення.

Після отримання HTML-відповіді від сервера Facebook, використовується парсер HTML, бібліотека BeautifulSoup у Python, для систематизації та аналізу

вмісту сторінок [47]. Під час аналізу визнаються мітки та класи HTML-елементів, які містять необхідну інформацію про спільноти, таку як ім'я групи, опис, кількість учасників тощо. Потрібно зазначити реальний URL групи на Facebook у змінній facebook_url, отриманий за алгоритмом пошуку груп у соціальних мережах (рис. 3.8).

```
import requests
from bs4 import BeautifulSoup

def parse_facebook_page(url):
    # Виконуємо HTTP-запит та отримуємо HTML-відповідь
    response = requests.get(url)

    if response.status_code == 200:
        # Створюємо об'єкт BeautifulSoup для парсингу HTML
        soup = BeautifulSoup(response.text, 'html.parser')

        # Знаходимо HTML-елементи за мітками та класами, які містять необхідну інформацію
        group_name = soup.find('h1', {'class': 'group-name'}).text.strip()
        group_description = soup.find('div', {'class': 'group-description'}).text.strip()
        members_count = soup.find('span', {'class': 'members-count'}).text.strip()

        # Друкуємо отриману інформацію або обробляємо її за потребою
        print(f"Назва групи: {group_name}")
        print(f"Опис групи: {group_description}")
        print(f"Кількість учасників: {members_count}")
    else:
        print(f"Помилка при отриманні сторінки. HTTP-код: {response.status_code}")

# Приклад використання
facebook_url = 'https://www.facebook.com/groups/example_group'
parse_facebook_page(facebook_url)
```

Рисунок 3.8 – Фрагмент парсера для автоматизації аналізу змісту публікацій

За допомогою цих інструментів здійснюється пошук, виділення та збереження необхідних даних про спільноти, які містяться у HTML-коді сторінок. Цей процес повторюється для інших сторінок, якщо результати розділені між кількома сторінками. Такий підхід дозволяє ефективно автоматизувати збір інформації про спільноти на основі аналізу HTML-коду.

Для автоматизації аналізу змісту публікацій та коментарів на сторінках дискусій за допомогою методів обробки природної мови можна використати такий метод:

1. Створити парсер на мові програмування Python для збору контенту - текстів постів, коментарів з відповідних сторінок соцмережі.

2. Виконати передобробку текстів - токенізацію, видалення стоп-слів, стемінг для приведення слів до базової форми.

3. Застосувати метод мішок слів (bag-of-words) або TF-IDF для векторного представлення текстів [37].

4. Кластеризувати тексти методами K-means чи ієрархічної кластеризації для групування за тематикою.

5. Проаналізувати отримані кластери текстів, визначити домінуючі у кожному слова-маркери тем.

6. Тренувати модель класифікації текстів (Naive Bayes) на розмічених даних для автоматичного визначення тем нових текстів [48].

7. Інтегрувати модель класифікації в веб-застосунок для автоматичного аналізу нового контенту на сторінках дискусій.

Така система дозволить масштабно аналізувати зміст обговорень в соцмережах для виявлення реальних тем дискусій.

3.2 Використання алгоритмів глибокого пошуку

Необхідність глибокого пошуку обумовлена рядом технічних та організаційних факторів. Основні причини включають велику кількість дискусійних сторінок у соціальних. Глибокий пошук реалізовується через створення пошукового робота, який використовує аналіз структури сторінок дискусій, що базується на списку контактів, а також гіперпосилань в інформаційному наповненні дискусій. Ці дані отримані за допомогою API-методів соціальних мереж та глобальної пошукової системи Google (рис.3.8).

Для реалізації глибокого пошуку у соціальних мережах, зокрема на дискусійних сторінках, можна створити власний пошуковий робот, використовуючи мову програмування Python та бібліотеки, такі як requests і beautifulsoup.

Пошук може бути розпочатий із отримання списку дискусійних сторінок. Далі, для кожної сторінки проводиться аналіз HTML-коду з метою визначення структури та взаємопов'язаності сторінок

Додатково можна використовувати гіперпосилання в інформаційному наповненні сторінок для глибшого пошуку та розширення обсягу контактів. Взаємодія з Google API може надати можливість перевірки та додаткового пошуку інформації, що допомагає визначити зв'язки між сторінками.

Цей підхід дозволяє створити гнучкий та налаштований пошуковий інструмент для виявлення сторінок дискусій та детального аналізу їх змісту та взаємодії.

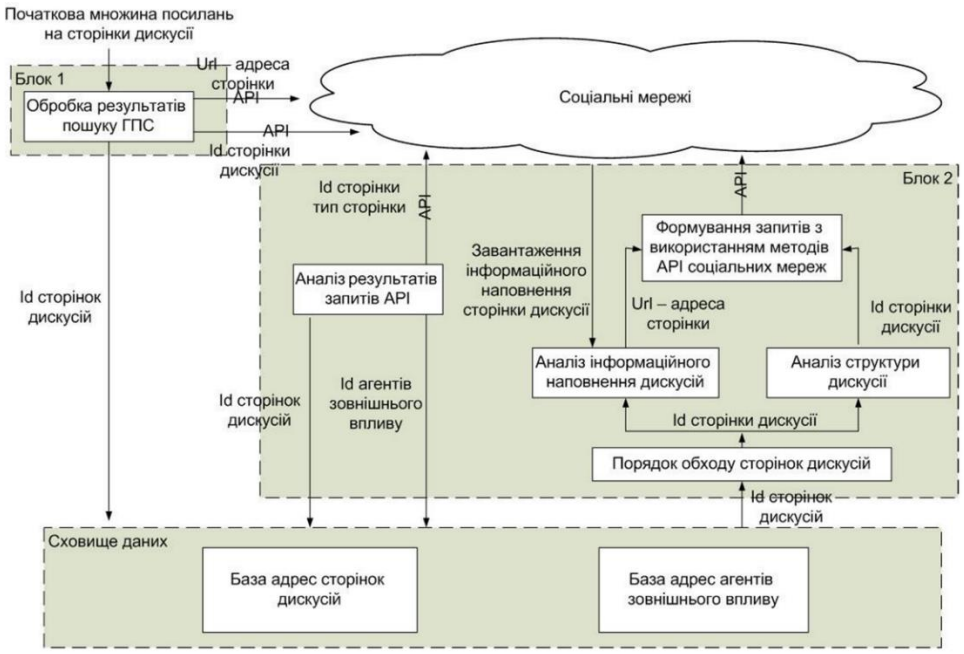


Рисунок 3.9 - Функціонування пошукового робота

Розуміючи, що глибокий пошук в соціальних мережах має визначені складнощі, наш пошуковий робот використовує два основні кроки для ефективного аналізу сторінок дискусій. Спочатку за допомогою глобальної пошукової системи Google формуються відповідні запити і знаходяться URL сторінок дискусій у межах цільової соціальної мережі.

Отже, поєднання можливостей зовнішнього пошуку та внутрішнього API дозволяє ефективно виявляти й аналізувати відповідні дискусії у соціальних мережах.

Перший блок націлений на визначення унікальних ідентифікаторів (ID) сторінок дискусій. Для цього ми взаємодіємо з глобальною пошуковою системою Google через API-методи соціальних мереж. Це надає дані про топологію мережі дискусій та інформаційні зв'язки. Отримавши список URL-адрес, які вказують на сторінки дискусій, ми визначаємо їхні унікальні ID для подальшого аналізу.

Другий блок зосереджений на докладному аналізі структури сторінок дискусій. Це включає використання API-методів соціальних мереж для збору деталей сторінок. Ми аналізуємо HTML-код сторінок, витягуємо дані про контакти та гіперпосилання з інформаційного наповнення сторінок для отримання повного зображення взаємодії та спільноти на даних сторінках.

Такий підхід дозволяє нашому пошуковому роботу ефективно визначати та аналізувати сторінки дискусій, використовуючи інформацію від глобальних пошукових систем та соціальних мереж.

Блок 1. У першому блоку нашого пошукового робота, коли ми отримуємо коротку адресу сторінки дискусії в результатах пошуку Google, усвідомлюючи її нестабільність через можливі зміни від адміністратора дискусії, ми використовуємо API-методи соціальних мереж для формування запиту для визначення унікального коду цієї дискусії.

Такий унікальний код дискусії представляє собою унікальний ідентифікатор, який присвоюється при створенні самої дискусії і залишається незмінним протягом її існування. Цей код може бути використаний для переходу на сторінку дискусії як за короткою адресою, так і через використання унікального ідентифікатора, надаючи стабільний доступ до конкретної дискусії, незалежно від можливих змін короткої адреси.

Блок 2. У другому блоку нашого пошукового робота ми використовуємо запит API-методами соціальних мереж для аналізу структури дискусії та визначення наявності гіперпосилань. Отримуючи унікальний код сторінки та тип

сторінки, ми класифікуємо її як частину дискусії або актора зовнішнього впливу відповідно до типу.

Цей аналіз дозволяє нам розподілити вміст за наявністю гіперпосилань та поділити сторінки на дискусії та агентів зовнішнього впливу в залежності від їх призначення та ідеології. Звертаючи увагу на тип сторінки, ми можемо визначити, чи відповідає вона тематичному напряму спільноти.

Враховуючи можливість знаходження дискусій, які не відповідають тематиці онлайн-спільноти, ми об'єднуємо дискусії за ознакою мети.

Для кластеризації результатів пошуку використаємо метематичну модель, а саме, просторову модель онлайн-спільноти (2.8).

Для аналізу вмісту сторінок дискусій наш пошуковий робот завантажує сторінку дискусії та проводить аналіз, спрямований на виявлення наявності гіперпосилань у повідомленнях дискусії. По виявленні гіперпосилань ми використовуємо API-методи соціальних мереж для отримання унікального коду сторінки та її типу. За типом сторінки ми проводимо розподіл між дискусіями та агентами зовнішнього впливу. Враховуючи можливість знаходження дискусій, які не відповідають тематиці спільноти, ми об'єднуємо їх за метою та ідеологією існування, щоб забезпечити точність і конкретність результатів глибинного пошуку.

Після завершення кожного циклу обробки дискусії, ми уточнюємо порядок обходу дискусій з урахуванням вже знайдених дискусій. Результатами глибокого пошуку є вдосконалення переліку дискусій, що пов’язані з відповідною тематикою, та створення переліку агентів зовнішнього впливу. Після кожного циклу обробки дискусії ми не лише уточнюємо порядок обходу дискусій з урахуванням знайдених, але і оновлюємо дані про кожну дискусію, зокрема, розширюємо перелік гіперпосилань та оновлюємо інформацію про тип сторінки. Це допомагає нам уникнути втрати корисної інформації та дозволяє точніше класифікувати дискусії.

Окрім того, через можливість знаходження дискусій, що не відповідають тематиці спільноти, ми використовуємо об'єднання дискусій за ознаками мети та

ідеології існування, щоб уникнути розкидання уваги на неспродуктивні або невідповідні результати глибинного пошуку. Результатами глибокого пошуку є вдосконалення та розширення переліку дискусій, які пов'язані із відповідною тематикою. Також формується перелік агентів зовнішнього впливу, які можуть бути асоційовані з цими дискусіями (рис 3.10).

Рисунок 3.10 - Узагальнений алгоритм формування інформаційного простору віртуальної групи

3.3 Метод протидії інформаційним загрозам онлайн-спільнот

Для вивчення та систематизації інформаційних загроз онлайн-спільнот у соціальних мережах слід розглядати різні аспекти, які можуть впливати на безпеку та стабільність спільнот. Зокрема, розглядаються загрози розповсюдження дезінформації, такі як фейкові новини, маніпуляції та штучне розбурювання з метою спровокувати конфлікти та розкол у спільноті.

Крім того, розглядаються загрози кібербезпеки, такі як хакерські атаки на інфраструктуру соціальної мережі, фішингові атаки та інші форми кіберзлочинності. Зокрема, увага приділяється втручанню в облікові записи членів спільноти та намаганню використати їхні дані.

Паралельно вивчається проблема кібербулінгу та негативної поведінки в мережі, така як образа, шкідливі коментарі та сприяння онлайн-ненависті. Досліджуються інциденти, пов'язані з порушенням приватності, такі як незаконний збір та використання особистої інформації членів спільноти.

Окрему увагу приділяємо загрозам соціальної інженерії, таким як вплив на виборчі процеси через маніпуляції та фейкові повідомлення. У цілому, аналіз інформаційних загроз відображає потребу в створенні докладної моделі, яка враховуватиме конкретний контекст та особливості кожної онлайн-спільноти.

Елементи аналізу інформаційної безпеки онлайн-спільнот визначаються відповідно до законодавчих актів, що регулюють інформаційну безпеку національної системи. До таких елементів відносять об'єкт, сферу застосування та конкретний перелік інформаційних загроз.

При розподілі переліку загроз враховується специфіка інформаційного наповнення онлайн-спільнот, і цей перелік поділяється на тематичні категорії.

Оцінка ризиків, в контексті онлайн-спільнот, не визначається як ймовірність виникнення загрози, а розглядає критичну кількість учасників, при якій ризик вважається значущим.

Для експертного визначення інформаційної загрози використовуються вихідні дані, отримані з моделі загроз:

- аналіз інформаційного наповнення дискусій у спільноті;
- оцінювання ключових слів, отриманих центроїдами онлайн-спільноти;
- використання алгоритмів автоматичного реферування.

Ці етапи визначають ступінь інформаційної загрози для спільноти в соціальних мережах. Визначення елементів аналізу інформаційної безпеки онлайн-спільнот здійснюється відповідно до вимог законодавства, що регулює інформаційну безпеку національної системи [49]. Серед цих елементів важливі об'єкт, область застосування та конкретний перелік інформаційних загроз.

При розподілі переліку загроз враховується специфіка інформаційного наповнення онлайн-спільнот, і такий перелік розділяється на різні тематичні категорії.

Оцінка ризиків в контексті онлайн-спільнот відрізняється від традиційних підходів. Тут ризик не визначається як ймовірність виникнення загрози, а розглядається як критична кількість учасників, при якій реалізується ця загроза.

Для експертного визначення інформаційної загрози використовуються вхідні дані, отримані з моделі загроз. Аналіз інформаційного наповнення дискусій у спільноті, оцінка ключових слів від центроїдів онлайн-спільноти та застосування алгоритмів автоматичного реферування – це етапи, які визначають ступінь інформаційної загрози для спільнот в соціальних мережах.

Показник загрози, яку несе функціонування онлайн-спільноти $InfThreat$ визначимо за формулою (2.8):

– $InfThreatCritMembers(VirtualCommunity)$ визначає критичну цінність онлайн-спільноти шляхом встановлення експертами того числа учасників, при якому реалізується інформаційна загроза, при цьому не враховується якість інформаційного наповнення спільноти та структура зв'язків дискусій у віртуальній спільноті, тобто умови виникнення загрози;

– $InfThreatInfConfr(VirtualCommunity)$ визначає критичну цінність онлайн-спільноти на основі загальної кількості учасників конкурентних а деструктивних онлайн-спільнот, які зацікавлені в даній тематиці і при цьому

враховується якість інформаційного наповнення та граф зв'язків дискусій у цих онлайн-спільнотах.

Міру інформаційної загрози з урахуванням зазначених показників розрахуємо за формулами:

$$InfThreat = 1 - (InfThreat_{InfConfr}(VirtualCommunity) + \\ + InfThreat_{CritMembers}(VirtualCommunity))^{'} \quad (3.1)$$

Так як ступінь інформаційної загрози може приймати значення в діапазоні [1,-1], то її значення залежить від кількості учасників деструктивної та конкуруючої онлайн-спільнот (рис. 3.10).

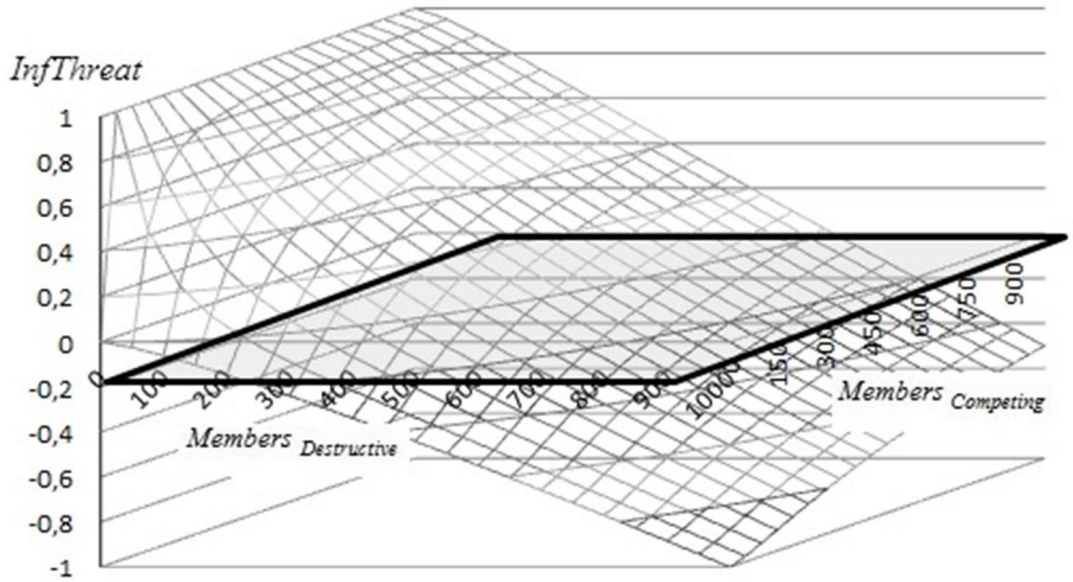


Рисунок 3.11 – Вплив деструктивної та конкурентної онлайн-спільнот на загрозу функціонування спільноти залежно від кількості учасників

Для відємних значень $InfThreat$ необхідно прийняти рішення щодо протидії інформаційним загрозам віртуальної групи. Це включає наступні кроки:

– проведення постійного моніторингу інформаційної обстановки;

– здійснення впливу на інформаційне наповнення деструктивної спільноти;

– проведення заходів щодо створення конкурентоспроможної групи;

– вживання заходів для протидії інформаційним загрозам.

На рисунку 3.12 схематично зображений метод прийняття рішення щодо заходів із протидії інформаційним загрозам онлайн-спільноти.

Рисунок 3.12 - Метод протидії інформаційним загрозам онлайн-спільнот

У процесі прийняття рішень щодо протидії інформаційним загрозам онлайн-спільнот використовується система показників, яка оцінює рівень інформаційної загрози для кожної віртуальної спільноти. Два ключові показники, визначають критичні значення для учасників та взаємодій деструктивних та конкурентних груп відповідно.

Якщо значення показників інформаційної загрози виявляються меншими за нуль, це свідчить про наявність критичної інформаційної загрози, і вживаються відповідні заходи. Такі заходи включають постійний моніторинг, вплив на

інформаційне наповнення деструктивних спільнот, створення конкурентноспроможних груп та загальний протидійний вплив на інформаційні загрози.

Процес виявлення критичних значень показників визначає потребу у вжитті заходів і дозволяє вчасно та ефективно реагувати на потенційні ризики.

Запропонований підхід до оцінювання рівня інформаційних загроз онлайн-спільнот має такі переваги:

1. Дає кількісну міру загрози на основі урахування ключових чинників - розміру і активності спільноти, якості контенту, топології зв'язків.

2. Дозволяє відстежувати динаміку загрози у часі шляхом моніторингу запропонованих показників.

3. Надає обґрунтовані критерії для систематизації спільнот за рівнями загрози та формування відповідних стратегій реагування і протидії деструктивним впливам.

4. Може бути основою для створення автоматизованих систем підтримки прийняття рішень у сфері забезпечення інформаційної безпеки.

Такий підхід дозволяє забезпечити стійкість та безпеку онлайн-спільнот в умовах інформаційних загроз.

3.3 Висновки

В третьому розділі розроблено метод та алгоритмів для ефективного виявлення та оцінки інформаційних загроз онлайн-спільнот у соціальних мережах. Отримані результати можна узагальнити наступним чином:

1. Розроблено ефективні методи та алгоритми для пошуку онлайн-спільнот за допомогою глобальної пошукової системи Google. Застосування формалізованих запитів та пошукового робота з використанням API-методів соціальних мереж дозволило здійснювати точний та цільовий пошук, а також отримувати необхідну інформацію про дискусії.

2. Вдосконалено алгоритми формування інфополя онлайн-спільнот враховуючи їх мету, ідеологію та ступінь відповідності тематичному напряму повідомлень. Це дозволяє отримувати комплексну картину спільноти та її спрямованість.

3. Вдосконалено метод прийняття рішень з протидії інформаційним загрозам онлайн-спільнот. Визначено два ключові показники, які служать критеріями для вжиття відповідних заходів при виявленні критичних значень. Цей метод дозволяє систематизувати та ефективно реагувати на інформаційні загрози онлайн- спільнот.

Отже, отримані результати роблять важливий внесок у розробку системи безпеки соціальних мереж, забезпечуючи ефективний моніторинг та протидію інформаційним загрозам онлайн-спільнот.

4 ЗАСОБИ КОМПЛЕКСУ МОНІТОРИНГУ ІНФОРМАЦІЙНИХ ЗАГРОЗ ОНЛАЙН-СПІЛЬНОТ

4.1 Архітектура програмного комплексу аналізу інформаційних загроз

Підхід до побудови архітектури програмного комплексу аналізу інформаційних загроз передбачає ретельне проектування та імплементацію системи, яка здатна ефективно виявляти та оцінювати потенційні загрози у віртуальних спільнотах соціальних мереж. Вважливо ретельно врахувати різноманітні аспекти та етапи, які спрямовані на створення ефективного та функціонального рішення [50].

На самому початку стоїть аналіз вимог, де здійснюється детальне вивчення потреб користувачів та особливостей соціальних мереж. Цей етап дозволяє зрозуміти, які функціональність та характеристики повинні бути вбудовані в систему.

Після аналізу вимог наступає архітектурне проектування, де визначається структура програмного комплексу та його основні компоненти. Важливо забезпечити ефективність та гнучкість архітектури, щоб вона відповідала усім вимогам.

На етапі вибору технологій обираються мови програмування, фреймворки та інші технічні рішення, що оптимально взаємодіють із завданням та забезпечують ефективну реалізацію.

Після визначення технічних аспектів слід етап імплементації та інтеграції, де створюється сам програмний продукт та відбувається його взаємодія з іншими системами.

На етапі аналізу та валідації проводиться тестування та перевірка на відповідність вимогам. Це дозволяє упевнитися в правильності функціонування та ефективності системи.

Після впровадження системи в експлуатацію настає етап оптимізації та підтримки, де забезпечується стабільна робота та розгортання оновлень для підтримки актуальності продукту.

Такий комплексний підхід забезпечує розроблення високоефективного та надійного програмного продукту, який успішно впроваджується в сферу аналізу інформаційних загроз у соціальних мережах.

Використання модулів у складі програмного комплексу аналізу інформаційних загроз є доцільним, оскільки дозволяє реалізувати увесь необхідний функціонал:

Модуль збору даних забезпечує отримання повних та актуальних вхідних даних з різних соцмереж для подальшого аналізу. Кожна платформа має свою специфіку, яка враховується індивідуальним підмодулем інтеграції.

Модуль підготовки даних реалізує всі необхідні кроки - очищення, стандартизацію, зберігання у зручній формі для опрацювання іншими модулями комплексу.

Модулі графового аналізу застосовують сучасні аналітичні методи для глибокого аналізу даних та виявлення прихованих закономірностей і загроз.

Модуль візуалізації та звітності робить аналітику зручною та зрозумілою для кінцевих користувачів системи.

Таке комплексне поєднання компонент дозволяє реалізувати повноцінну платформу аналізу інформаційних ризиків у соціальних мережах.

Процес моніторингу та аналізу інформаційних загроз онлайн-спільнот у соціальних мережах може включати такі основні етапи:

– збір даних, збирання і накопичення даних з соціальних мереж щодо цільових спільнот і дискусій за допомогою відповідних API;

– попередня обробка, структурування, очищення, стандартизація даних для аналізу; фільтрація за параметрами;

– лінгвістичний та семантичний аналіз текстів дискусій, ідентифікація маніпуляцій, прихованої пропаганди;

– соціальний аналіз, побудова соціальних графів, виявлення груп і спільнот, аномальної поведінки учасників;

– розрахунок показників, що характеризують рівень інформаційних ризиків та загроз в дискусіях спільнот;

– візуалізація та звітність для прийняття рішень щодо реагування на виявлені загрози.

Архітектура програмного комплексу для виявлення та протидії інформаційним загрозам онлайн-спільнот, складається з трьох модулів (рис. 4.1):

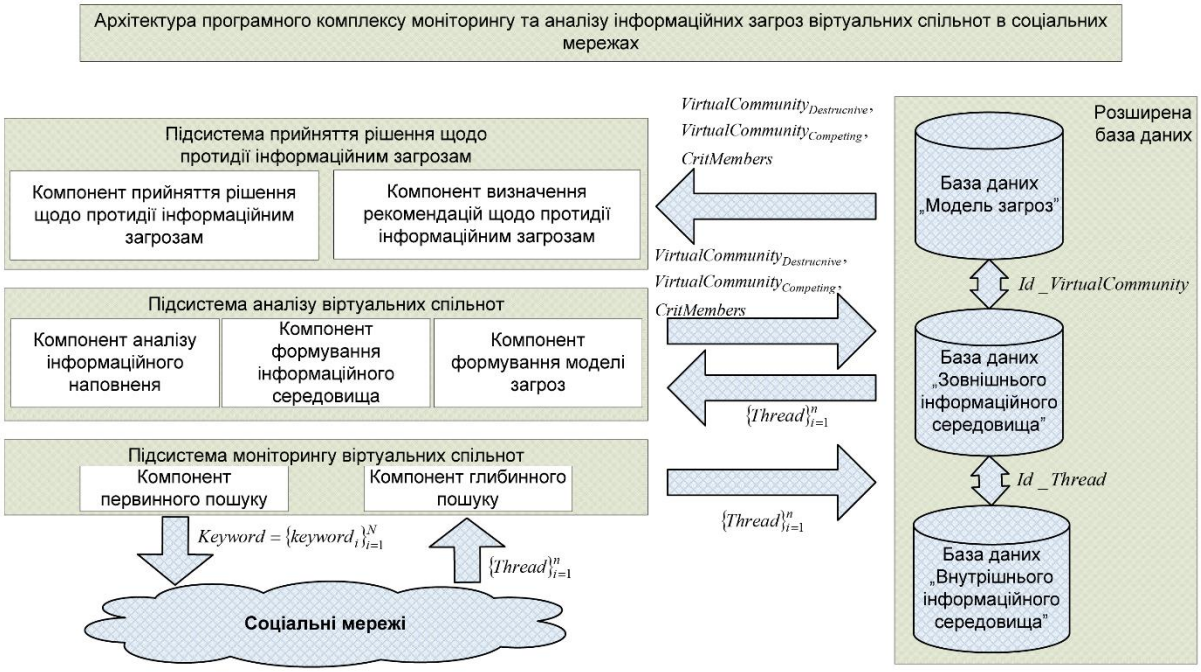


Рисунок 4.1 - Архітектура програмного комплексу аналізу інформаційних загроз

Система моніторингу онлайн-спільнот розроблена для здійснення пошуку дискусій в соціальних мережах відповідно до їх інформаційного наповнення. Ця підсистема спрямована на забезпечення комплексного аналізу активності та обговорень в онлайн-спільнотах.

```
def get_page(url):
    r = requests.get(url)
    return r.text
def parse_page(html):
    soup = BeautifulSoup(html, 'lxml')
    # аналіз заголовку
    title = soup.title.text
    # пошук останніх постів
    posts = soup.find_all('div', class_='post')[-5:]

    for post in posts:
        # аналіз тексту поста
        print(post.text)
        # пошук ключових слів
        if 'Базування ППО' in post.text.lower():
            print('Знайдено ключове слово')

    # інша логіка аналізу сторінки та контенту
```

Рисунок 4.2 - Фрагмент програмного коду, який здійснює глибокого аналізу інформаційного наповнення

URL адресу онлайн-спільноти визначимо згідно алгоритму, запропонованого в пункті 3.1

```
<a titile=""role="menuitem" href="https://www.facebook.com/Matviichuk.Andrii/groups"
```

Рисунок 4.3 – Визначення URL онлайн-спільноти

Підсистема аналізу онлайн-спільнот використовується для глибокого аналізу інформаційного наповнення з метою формування структурованого інформаційного простору спільноти. Цей модуль сприяє розумінню та класифікації вмісту дискусій, сприяючи створенню точного образу спільноти в соціальних мережах.

```
url = "https://www.facebook.com/Matviichuk.Andrii/groups"
html = get_page(url)
parse_page(html)
```

Рисунок 4.4 – Фрагмент програмного коду, для виклику глибокого пошуку

Підсистема прийняття рішення щодо протидії інформаційним загрозам онлайн-спільнот спроектована для оцінювання інформаційних загроз та формування рекомендацій з метою контролю інформаційного впливу на структуру спільнот в соціальних мережах. Ця підсистема дозволяє аналізувати потенційні загрози та розробляти стратегії взаємодії для забезпечення стійкості та безпеки онлайн-спільнот.

4.2 Проектування бази даних загроз онлайн-спільнот

Повноцінний моніторинг та аналіз інформаційних загроз онлайн-спільнот у соціальних мережах ґрунтується на використанні розширеної бази даних, яка включає декілька ключових компонентів.

На першому етапі, база даних зберігає інформацію, зібрану в ході пошукових операцій. Це може включати у себе дані про спільноти, їхні учасники, ключові теми обговорень, та інше. Для кожного виявленого елемента в соціальних мережах, база даних фіксує докладні деталі, такі як динаміка активності, рейтинги популярності, та інші параметри.

Другий компонент бази даних відноситься до аналізу інформаційного наповнення спільнот. Цей блок зберігає в собі оброблені дані щодо змісту повідомлень, гіперпосилань, та обговорень. Інструменти аналізу тексту використовуються для визначення ключових слів, емоційного забарвлення, а також виявлення можливих загроз.

Третій компонент визначається базою даних експертної інформації, де зберігаються дані про існуючі інформаційні загрози та попередні випадки впливу

на спільноти в соціальних мережах. Ця база даних допомагає визначити контекст і важливість конкретних подій.

В цілому, ці компоненти утворюють інтегровану систему, що забезпечує доступ до зібраної, обробленої та відфільтрованої інформації, необхідної для вдосконалення стратегій моніторингу та прийняття рішень в сфері інформаційної безпеки онлайн-спільнот.

При проектуванні ї бази даних для повноцінного моніторингу та аналізу інформаційних загроз онлайн-спільнот у соціальних мережах, слід враховувати кілька ключових етапів [52].

На початковому етапі необхідно визначити структуру бази даних, визначити основні сутності та взаємозв'язки між ними. Наприклад, можливі сутності включають дані про спільноти, їхніх учасників, повідомлення, ключові теми обговорень та інші аспекти, які можуть бути важливими для аналізу.

Другий етап включає розробку механізмів для зберігання та оновлення інформації в базі даних. Необхідно розробити ефективні схеми для зберігання даних, зокрема враховуючи можливість масштабування обсягів інформації з часом.

Третій етап передбачає введення механізмів для обробки та аналізу текстового контенту. Це включає в себе використання алгоритмів аналізу тексту для визначення ключових слів, емоційного забарвлення, та інших параметрів, які можуть бути важливими для оцінки загроз.

Крім того, слід розглядати можливість створення бази даних експертної інформації, яка буде включати в себе дані про існуючі інформаційні загрози та випадки впливу на спільноти в соціальних мережах.

Нарешті, важливим етапом є розробка інтерфейсів для доступу до бази даних, які дозволять ефективно взаємодіяти зі зібраною, обробленою та відфільтрованою інформацією. Це може включати в себе створення зручного веб-інтерфейсу або API для інтеграції із зовнішніми інструментами.

Такий комплексний підхід дозволяє створити ефективну та гнучку базу даних для аналізу інформаційних загроз у соціальних мережах.

Для забезпечення ефективного зберігання даних та аналізу інформаційних загроз онлайн-спільнот пропоную спроектувати базу даних з такими основними сутностями [53]:

– користувачі, ідентифікатори, профілі учасників, демографічні та поведінкові характеристики;

– повідомлення, зміст, метадані постів, коментарів у соцмережах;

– спільноти, характеристики онлайн-груп та сторінок дискусій;

– зв'язки, це соціальні ребра між користувачами, спільнотами на основі перетинів активності,

– аналітика, а саме результати лінгвістичного аналізу текстів, виявлені ознаки загроз, розрахункові показники ризиків,

– моделі, перелік збережених моделей машинного навчання для класифікації текстів, користувачів тощо.

Така структура дозволить накопичувати увесь спектр необхідних даних та ефективно їх аналізувати для виявлення інформаційних загроз.

Повноцінний моніторинг інформаційних загроз онлайн-спільнот забезпечує використання розширеної бази даних, яка включає в себе не лише основні дані про спільноти і користувачів, але й розширену інформацію про динаміку змін у популяції, структуру спілкування та сутність дискусій.

Така база даних повинна враховувати різноманіття форматів інформаційних матеріалів, включаючи текстові повідомлення, графічний та відеоконтент. Такий підхід дозволить більш точно аналізувати вплив загроз на різні аспекти життя спільнот та їхніх учасників.

Для ефективного моніторингу, база даних має включати систему сповіщень та автоматичного оновлення, щоб оперативно реагувати на зміни в інформаційному просторі соціальних мереж.

Забезпечення гнучкості та масштабованості бази даних є ключовим елементом, щоб вона могла ефективно працювати в умовах зростаючого обсягу інформації та потреб користувачів (рис. 4.5).

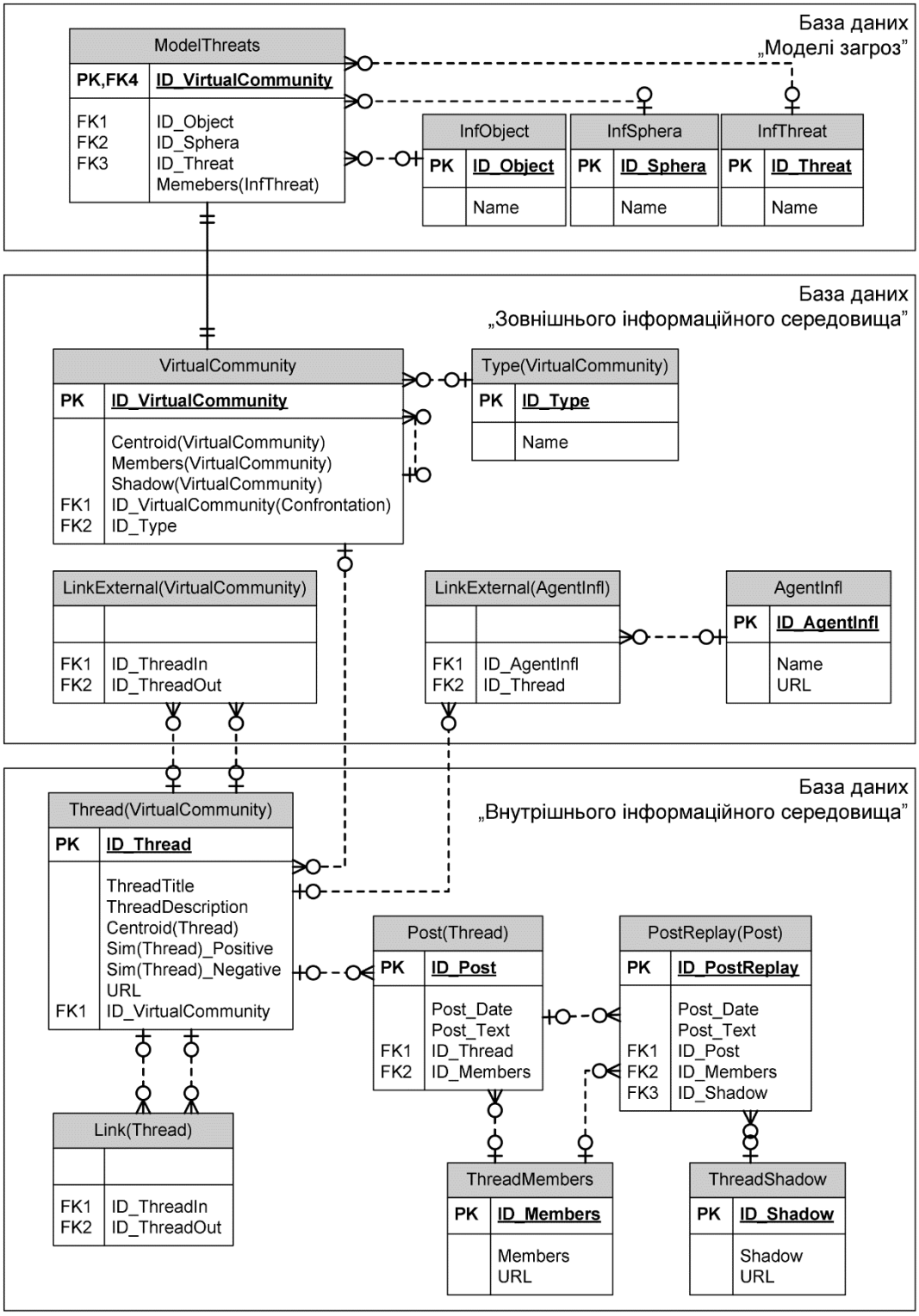


Рисунок 4.5 - Структура бази даних загроз онлайн-спільнот

Потрібно також передбачити механізми забезпечення безпеки для захисту конфіденційної інформації та унеможливлення неправомірного доступу до даних.

Для ефективного реагування на інформаційні загрози віртуальних спільнот формується спеціалізована база даних аналітичних моделей. Вона містить результати комплексного аналізу контенту, комунікацій та ризиків конкретних онлайн-груп.

Зокрема, тут зберігаються висновки експертів щодо характеру загроз, які несе інформаційне наповнення цих спільнот, з урахуванням особливостей їх функціонування.

Також база даних містить довідкові та службові дані для визначення рівнів загроз, стратегій протидії та реагування - згідно чинних нормативних документів у сфері інфо безпеки.

Комплексне використання накопичених в базі аналітичних моделей і довідкових даних дозволяє приймати обґрунтовані рішення для нейтралізації інформаційних загроз.

В подальшому її можна розширити за рахунок використання таких компонентів:

– моделі користувачів-центроїдів, яка буде визначати соціально-демографічні характеристика профілів ключових учасників, а саме історія активності, демографія, геолокація, приналежність до різних груп тощо;

– моделі контенту, результати аналізу текстів публікацій в спільнотах - тематика, тональність, маніпулятивні техніки, ознаки пропаганди тощо;

– моделі комунікацій, тобто графи зв'язків між учасниками та публікаціями в спільноті: щільність, центральність, наявність аномалій.

– моделі ризиків, де можна враховувати показники ймовірності та рівня конкретних типів інформаційних загроз для окремих спільнот;

– моделі прогнозування, які будуть використовувати методи машинного навчання та засоби екстраполяції динаміки зміни показників загроз для оцінки майбутніх тенденцій розвитку ризиків.

Основними завданнями бази даних зовнішнього інфополя онлайн-спільнот є:

– облік та акумулювання даних про зовнішні інформаційні джерела, профілі користувачів, які взаємодіють з цільовою спільнотою, але не є її безпосередніми учасниками;

– збір технічних характеристик зовнішніх об'єктів, кількість друзів, підписників, рівень активності, належність до інших спільнот тощо;

– аналіз семантичних характеристик, тематика публікацій зовнішніх джерел, ключові слова, емоційне забарвлення, зв'язок з тематикою внутрішнього контенту цільової спільноти;

– виявлення закономірностей і аномалій у даних зовнішньої периферії, які можуть свідчити про існуючі інформаційні загрози для конкретної спільноти.

Уточнимо структуру бази даних зовнішнього інфополя онлайн-спільнот:

– таблиця характеристики цільових онлайн-груп, профілі, статистики, тематика.

– таблиця зовнішніх джерел впливу, дані про ресурси, не пов'язані безпосередньо з конкретною спільнотою, але які можуть мати на неї вплив.

– таблиці зв'язків між спільнотами містить дані про спільних учасників, перетин тематик, взаємодію між різними онлайн-групами.

– таблиці зв'язків онлайн-спільнот і зовнішніх джерел, інтенсивності і тематики комунікацій цільових груп і зовнішніх каналів.

– таблиця типів (конструктивна - деструктивна), яка класифікує за рівнем потенційної небезпеки чи конструктивності на основі аналізу.

Така структура дозволяє акумулювати увесь спектр даних про зовнішнє інфополе цільових онлайн-спільнот.

Уточнимо процес формування даних для опису внутрішнього інфополя онлайн-спільнот:

– здійснюється пошук та ідентифікація конкретних сторінок та потоків дискусій в межах цільової онлайн-групи на основі аналізу їх інформаційного наповнення - текстів постів і коментарів;

– проводиться збір технічних характеристик виявлених дискусій, а саме кількість учасників, динаміка публікацій, час активності тощо;

– здійснюється семантичний аналіз, тобто визначення тематики, тональності, маніпулятивного потенціалу контенту дискусій з використанням методів обробки природної мови;

– формується узагальнена модель внутрішнього інфополя цільової спільноти на основі даних про окремі дискусії та їх взаємозв'язки.

Така послідовність дозволяє комплексно описати і проаналізувати інформаційне середовище всередині онлайн-спільноти.

Для модернізації та розширення функціональності бази даних внутрішнього інформаційного середовища віртуальних спільнот можна додати такі елементи:

– розширені профілі користувачів, використовуючи методи OSINT для основі аналізу всієї їх активності у соцмережі за межами конкретної цільової спільноти [54];

– моделі соціальних графів, що описують зв'язки між учасниками та їх ролі у комунікаціях всередині спільноти;

– таблиці зі стратегіями реагування на потенційні загрози відповідно до їх типів та рівнів.

Така розширена структура підвищить якість аналізу та можливості оперативного реагування на інформаційні ризики соціальних мереж.

Для деанону користувачів-центроїдів, які здійснюють найбільший вплив на соціальну спільноту потрібно використати засоби OSINT та алгоритму формування соціального портрету учасника онлайн-спільноти, що дасть змогу ефективніше реагувати на його дії експертам [55].

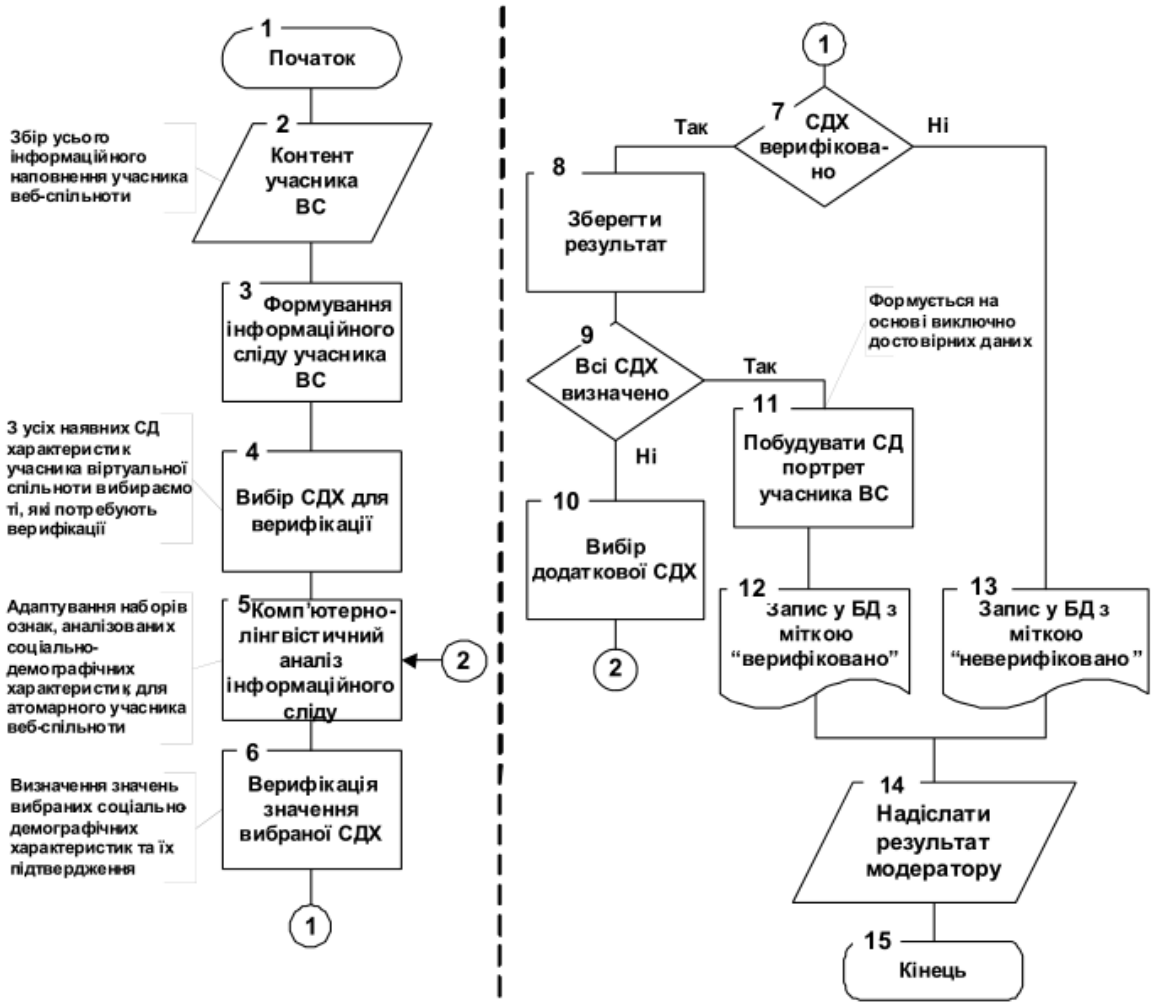


Рисунок 4.6 - Блок-схема алгоритму формування портрету учасника онлайн-спільноти

Учасники онлайн-спільнот в соціальних мережах залишають певний інформаційний слід своєї діяльності, який дає уявлення про їх інтереси, переконання, наміри. Цей слід можна відстежити та проаналізувати такими способами:

1. Аналіз профілю користувача в соціальній мережі - його постів, коментарів, вподобаного контенту, груп, сторінок і спільнот, на які він підписаний.

2. Виявлення інших профілів та облікових записів користувача в інших соціальних мережах чи на інших сайтах за допомогою пошуку за іменем, email, нікнеймом тощо.

3. Аналіз кола друзів і підписок користувача - часто це люди зі спільними інтересами чи переконаннями.

4. Пошук коментарів користувача на різних платформах за ключовими словами чи фразами, що вказують на його належність чи погляди.

Комплексно дослідивши увесь можливий інформаційний слід учасників, можна скласти більш повне уявлення про їх роль у віртуальних спільнотах

4.3 Експериментальне дослідження розробленого методу

Уточнимо етапи процесу аналізу дискусій віртуальних спільнот:

– формується розширена база даних та визначається перелік ключових слів для пошуку згідно тематики потенційних інформаційних загроз;

– за допомогою формалізованих запитів до пошукової системи Google та аналізу HTML-коду сторінок знаходяться релевантні дискусії у соціальних мережах;

– використовуються пошуковий робот, що працює з API соціальних мереж;

– виявлені сторінки дискусій кластеризуються за тематикою їх інформаційного наповнення для подальшої класифікації на конструктивні та деструктивні.

– експерти вручну аналізують вибіркові дискусії для уточнення їх тематичного спрямування та рівня відповідності потенційним загрозам.

Такий комбінований людино-машинний підхід дозволяє ефективно шукати та класифікувати дискусії для подальшого моніторингу загроз.

Далі формуємо сценарій інформаційного впливу на загрозливі онлайн-спільноти:

– на основі автоматичного аналізу та розрахунку показників інформаційних загроз оцінюється рівень ризиків конкретної онлайн-спільноти;

– за результатами аналізу алгоритмічно вибираються оптимальні дискусії для блокування чи видалення, що забезпечить максимальне зниження загроз.

– експерти формують комплексний сценарій інформаційного впливу, що включає як обмежувальні заходи щодо шкідливих дискусій, так і стимулювання позитивного контенту;

– після реалізації сценарію проводиться повторний моніторинг онлайн-спільноти і аналіз ефективності інформаційного впливу для подальшої оптимізації стратегії.

Такий підхід поєднує автоматизований аналіз даних та експертні знання для мінімізації загроз онлайн-спільнот.

Пропонується три стратегії впливу на структуру внутрішнього інфополя.

Стратегія 1. Блокування. Здійснюється шляхом активного втручання у хід обговорень з метою зміни їх тематичної спрямованості та виведення їх за межі загальної тематики спільноти, або подальшого блокування дискусії.

Спрямована на зменшення кількості дискусій та залучених учасників, спрямованих на конкретні теми, тим самим створюючи перепони для розгортання великих обговорень.

Стратегія 2. Знищення зв’язків окремого обговорення, направлена на створення ізольованих дискусій, розірваних з загальною структурою спільноти. Має на меті не зменшувати загальну кількість дискусій або учасників, але розділяє обговорення на більше специфічні групи.

Стратегія 3. Знищення зв’язків окремого обговорення задля створення окремих груп обговорень, але без зменшення загальної кількості дискусій та учасників онлайн-спільноти. Здійснюється для того, щоб сприяти більш деталізованим тематичним обговоренням без впливу на загальну динаміку віртуальної спільноти.

Проведено експеримент з метою дослідження впливу запропонованих стратегій на внутрішнє інфополе онлайн-спільноти. Досліджувалася віртуальна спільнота на 10000 учасників які могли організувати 100 обговорень, по 100

учасників.

Для визначення потенціної загрози використовуємо показник загрози онлайн-спільноти (2.10).

Графіки зміни показника загрози онлайн-спільноти в залежності від стратегії впливу на внутрішнє інфополе наведено на рис. 4.7.

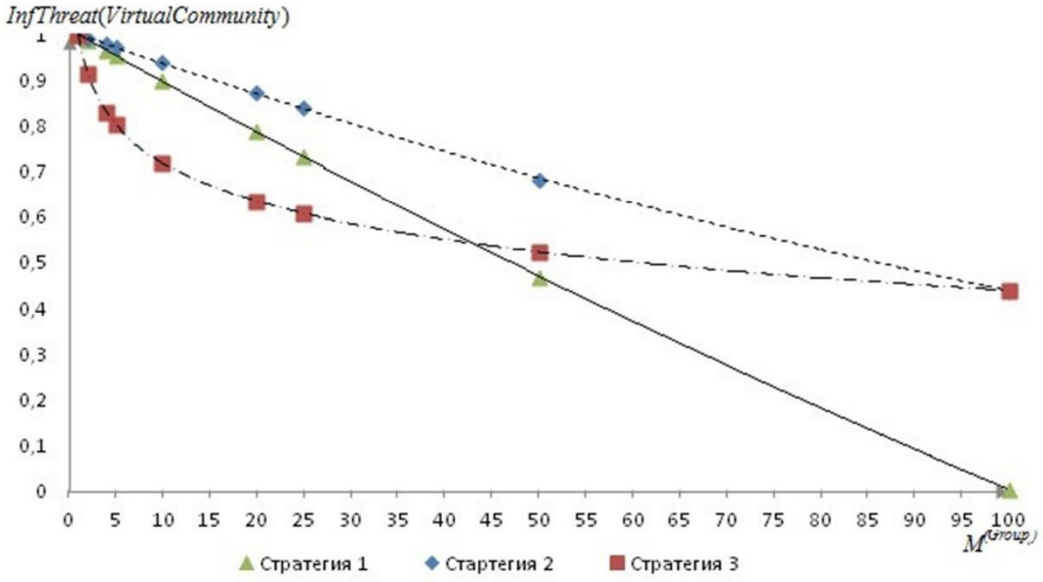


Рисунок 4.7 - Зміна показника загрози онлайн-спільноти в залежності від стратегії впливу на внутрішнє інфополе

В результаті проведеного дослідження пропонується застосувати комплексну стратегію:

1. Часткове блокування окремих дискусій для порушення комунікаційних зв'язків всередині спільноти.

2. Поширення альтернативної інформації та точок зору з метою трансформації тематичного напрямку обговорень у потрібне русло.

3. Стимулювання конструктивної дискусії та перенесення її у спеціально створені майданчики під контролем модераторів.

4. Виявлення лідерів думок спільноти та інформаційно-психологічний вплив на них задля зміни тональності наративу.

Такий комплексний підхід дасть змогу ефективно нейтралізувати деструктивний потенціал віртуальних спільнот у соціальних мережах.

4.3 Висновки

У четвертому розділі було розроблено архітектуру програмного комплексу для моніторингу та аналізу інформаційних загроз онлайн-спільнот у соціальних мережах. Детально описано ключові компоненти системи, їх функціональне призначення та технічні аспекти реалізації.

Для накопичення даних про інформаційний простір онлайн-спільнот використовується база даних. Її структура ґрунтується на формальній моделі інформаційного простору спільноти, розробленій у попередньому розділі.

Функціональні можливості програмно-алгоритмічного комплексу охоплюють виконання таких основних завдань:

– автоматизований пошук та моніторинг онлайн-спільнот у популярних соціальних мережах;

– збір та аналіз інформаційного наповнення сторінок дискусій цих спільнот;

– кількісна оцінка рівня інформаційних загроз та формування рекомендацій щодо протидії цим загрозам.

Таким чином, розроблений функціонал дозволяє комплексно аналізувати інформаційний простір та ризики для онлайн-спільнот у соціальних мережах.

ВИСНОВКИ

У магістерському досліджені розв’язано актуальне науково-прикладне завдання, а саме розроблено метод та інструментарій для аналізу та виявлення впливу загрозливої інформації в соціальних інтернет-сервісах, спрямованого на оптимізацію часових витрат на збір та обробку даних щодо поширення та характеристик повідомлень.

Запропоновано використання методів машинного навчання для класифікації контенту в соцмережах за рівнем потенційного впливу. Розроблено алгоритми інтелектуального пошуку та моніторингу інформаційних кампаній на основі графових моделей. Створено інструментарій автоматизованого збору статистики поширення повідомлень з використанням API соціальних мереж.

Отримано вагомі результати:

1. Проведено ґрунтовний аналіз проблем захисту даних у соціальних інтернет-сервісах. Сформульовано завдання адаптивного захисту доступу з урахуванням повноважень користувачів і типів даних.

2. Досліджено існуючі підходи до протидії інформаційним загрозам в соцмережах. Виявлено відсутність на сьогоднішній момент ефективного інструментарію оцінки таких загроз відносно онлайн-спільнот.

3. Вдосконалено модель інформаційного простору онлайн-спільноти, що стала базисом для аналізу загроз її безпеці.

4. Розраховано кількісний показник рівня інформаційної загрози з урахуванням цінності онлайн-спільноти.

5. Розроблено ефективні алгоритми пошуку уразливих об’єктів у соцмережах за допомогою API. Створено інструментарій автоматизованого збору статистики поширення повідомлень з використанням API соціальних мереж.

6. Розроблено метод виявлення інформаційної загрози за парсингом груп у соціальних інтернет-сервісах, який базується на врахуванні кількості учасників, при якій реалізується інформаційний вплив

7. Розроблено архітектуру програмного комплексу моніторингу та захисту онлайн-спільнот. Проведено успішну експериментальну перевірку запропонованого функціоналу.

Застосування даних методів та підходів дозволяє суттєво прискорити аналіз інформаційних операцій та оцінку їх впливу на користувачів соцмереж. Це сприяє підвищенню ефективності моніторингу, прогнозування та реагування на інформаційні загрози в соціальних медіа.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Комплексна інформаційна безпека соціотехнічних систем: моделі впливу та захисту: монографія/ А. В. Дудатьєв. – Вінниця : ВНТУ, 2017. – 128 с.

2. Горбулін В.П., Качинський А.Б. Методологічні засади розробки стратегії національної безпеки // Стратегічна панорама. — 2018. — № 3. — С. 15 - 24.

3. Molodetska, Kateryna, Yuriy Tymonin, and Ihor Melnychuk. "The conceptual model of information confrontation of virtual communities in social networking services." International Journal of Electrical and Computer Engineering 10.1 (2020): 1043.

4. Jones S. Cybersociety: Computer-mediated communication and community / S. Jones. - Thousand Oaks, CA : Sage, 1995. - P. 1-34.

5. Жарков Я. та ін. Інформаційно-психологічне протиборство (еволюція та сучасність) : [Монографія] / Я. Жарков, В. Петрик, М. Присяжнюкта ін. - К.: ПТ «Віпол», 2013. -248 с.

6. Прибутько П. Інформаційні впливи : роль у суспільстві та сучасних воєнних конфліктах / П. Прибутько, І. Лук'янець. - К. : Вид. ПАЛИВОДА А.В., 2007. - 252 с.

7. Сучасні інформаційні системи і технології: управління знаннями: навчальний посібник/ В. М. Антоненко, С. Д. Мамченко, Ю. В. Рогушина. – Ірпінь: Національний університет ДПС України, 2016. – 212 с.

8. Axelrod R. Modeling Security Issues of Central Asia // Gerald R. Ford School of Public Policy University of Michigan (Project on "Security in Central Asia" June 2014. US Govt. Contract № 2003*H513400*000)

9. Simulation Modeling and Arena / Manuel D. Rossetti. – 2nd ed. – Hoboken: John Wiley & Sons, Inc., 2016. – 744 p.

10. Моделювання систем: конспект лекцій / В. М. Задачин, І. Г. Конюшенко. – Харків : Вид. ХНЕУ, 2012. – 268 с.

11. Соціальна мережа. Вікіпедія [Електронний ресурс] – Режим доступу:

https://uk.wikipedia.org/wiki/Соціальна_мережа/ – (дата звернення 18.10.2023) – Назва з екрана.

12. Почепцов Г. Інформаційна війна як інтелектуальна війна [Електронний ресурс] / Г. Почепцов. – Режим доступу: http://osvita.mediasapiens.ua/material/13303. – (дата звернення 28.9.2023) – Назва з екрана.

13. Пелещишин А.М., Гумінський Р.В. «Загрози інформаційної безпеки держави в соціальних мережах». Наука і техніка Повітряних Сил Збройних Сил України. 2(11). 2013. С. 192-199.

14. Муляр І.В. Виявлення інформаційного впливу на основі аналізу контенту ресурсів соціальних мереж / І.В. Муляр, В.О., А.А. Берназ // Тези доповідей XV Міжнародної науково-практичної конференції "Військова освіта і наука: сьогодення та майбутнє" / за заг. редакцією Ігоря Толока. – К. : ВІКНУ, 2019. – С. 60

15. Інформаційна безпека. Практикум/ В.М. Ахрамович, В.М. Чегренець.- К.: ДУТ, 2017. - 396с

16. Спіраль мовчання. Вікіпедія [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Спіраль мовчання/ – (дата звернення 21.10.2023) – Назва з екрана.

17. Тимовчак-Максимець О.Ю. «Аналіз комунікативної взаємодії на веб-форумах: інформаційна поведінка таучасники». Інформаційні системита мережі. № 699, 2011. С. 352-362.

18. Cyber Bullying Law and Legal Definition [Електронний ресурс]. — Режим доступу: https://definitions.uslegal.eom/c/cyber-bullying/ – (дата звернення 16.09.2023) — Назва з екрана.

19. Грайворонська А.М., Ланде Д.В. Дослідження інформаційних потоків, як динамічних мультиагентних систем // Системный анализ и информационные технологии: материалы 17-й Международной научнотехнической конференции SAIT 2015, Киев, 22 -25 июня 2015 г. / - К.: УНК "ИПСА" НТУУ "КПИ", 2015. - С. 62-63.

20. A Data Model of the Internet Social Environment Peleshchyshyn, A., Mastykash, O. Advances in Intelligent Systems and Computing, 2020, 902, pp. 439-448.

21. Пелещишин А.М., Гумінський Р.В. «Загрози інформаційної безпеки держави в соціальних мережах». Наука і техніка Повітряних Сил Збройних Сил України. 2(11). 2013. С. 192-199.

22. Інформаційно-ознакова модель джерела шкідливої інформації в соціальних мережах / В.М.Джулій, І. В. Муляр, О.О Зацепіна, В.О. Пічура // Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». 2022. № 3. С. 73–78.

23. Jones S. Cybersociety: Computer-mediated communication and community / S. Jones. - Thousand Oaks, CA : Sage, 1995. - P. 1-34.

24. Peleshchyshyn, A., Bandrovskyi, H. “Informational influence in social networks: Dynamics modeling based on the system of linear equations”. IEEE 2019 14th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2019 - Proceedings, 2019, 1, pp. 165-168, 8929819.

25. Peleshchyshyn, A., Mastykash, O. A “Data Model of the Internet Social Environment.” Advances in Intelligent Systems and Computing, 2020, 902, pp. 439-448.

26. Малихін О. В. Професійний розвиток учителів закладів загальної середньої освіти: віртуальні педагогічні спільноти / О. В. Малихін, Н. О. Арістова // The 8 th International scientific and practical conference: Eurasian scientific congress!. - August 9-11, 2020. - Barca Academy Publishing, Barcelona, Spain. 2020. - 370 p.

27. Tatnall A. Actor-Network Theory and Technology Innovation : Advancements and New Concepts. Information Science Reference / A. Tatnall. - New York, 2010. - 328 p.

28. Epstein J. M., Axtell R. Artificial societies and generative social science // Artificial Life and Robotics. - Vol., № 1 / March, 2017. - pp. 33-34].

29. Epstein J. M. Generative Social Science : Studies in Agent-Based

Computational Modeling / Joshua M. Epstein. - Princeton : Princeton University Press, 2016. - 384 p.

30. Trach, Olha, and Andriy Peleshchyshyn. "Development of directions tasks indicators of virtual community life cycle organization." 2017 12th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT). Vol. 1. IEEE, 2017.

31. Гришук Р В. Стартап віртуальних спільнот у соціальних мережах за принципом критичної маси / Р В. Гришук // Захист інформації. - Луганськ : СНУ. - 2015. - Спеціальний випуск. - С. 19-25.

32. Peleshchyshyn, Andriy, et al. "Identifying specific roles of users of social networks and their influence methods." 2018 IEEE 13th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT). Vol. 2. IEEE, 2018.

33. Даник Ю. Г. Сучасні мобільні соціальні інтернет сервіси як один з перспективних засобів масової комунікації / Ю. Г. Да- ник, Р В. Гришук, О. В. Самчишин // Наук.-практ. конф. [«Актуальні проблеми управління інформаційною безпекою держави»] (Київ, 19 берез. 2015 р.). - К. : Центр. навч., наук. та період. видань НА СБ України, 2015. - С. 232-235

34. Гумінський Р. В. Підходи щодо визначення критичної цінності віртуальної спільноти в соціальних мережах / Р. В. Гумінський // Інформаційна безпека у воєнній сфері. Сучасний стан та перспективи розвитку: матеріали міжвідомчої наук.-практ. конференції, Київ, 31 берез. 2015 р. / НУОУ. - Київ, 2015. - С. 104 - 107.

35. Пасічник В. В. Глобальні інформаційні системи та технології (моделі ефективного аналізу, опрацювання та захисту даних) / В. В. Пасічник, П. І. Жежнич, Р. Б. Кравець та ін. - Львів : Вид-во Національного університету “Львівська політехніка”, 2006. - 350 с.

36. Фурашев В. М. Інформаційні операції крізь призму системи моніторингу та інтеграції Інтернет-ресурсів / В. М. Фурашев, Д. В. Ланде // Правова інформатика. - 2009. - № 2(22). - С. 49 - 57.

37. Term Frequency-Inverse Document Frequency. Вікіпедія [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/TF-IDF – (дата звернення 26.10.2023) – Назва з екрана.

38. Гришук Р. В. Мобільні соціальні інтернет-сервіси як один із різновидів масової комунікації на сучасному етапі / Р В. Гришук, Ю. Г. Даник, О. В. Самчишин // Безпека інформації : НАУ. - 2015. - Т. 21. - № 1. - С. 16-20.

39. Axelrod R., Hammond R.A. The Evolution of Ethnocentric Behavior // Paper presented at the annual meeting of the Midwest Political Science Convention, Chicago, IL, April 2016.

40. Принцип Парето [Електронний ресурс] – Режим доступу: https://happymonday.ua/shho-take-pryntsyp-pareto – (дата звернення 26.10.2023) – Назва з екрана.

41. Що таке NIST [Електронний ресурс] – Режим доступу: https://getpci.com/what-is-the-nist-standart – (дата звернення 27.10.2023) – Назва з екрана.

42. Пелещишин, А. М. Аналіз існуючих типів віртуальних спільнот у мережі інтернет та побудова моделі віртуальної спільноти на основі веб-форуму / А. М. Пелещишин, Р. Б. Кравець, Ю.О. Сєров // Інформаційні системи та мережі: Вісник Національного університету “Львівська політехніка”. - 2011. - № 699. - С. 212-221.

43. Злам Департаменту інфокомунікацій МО РФ. Секрети генерала Конашенкова і “Катюші” [Електронний ресурс] – Режим доступу: https://informnapalm.org/ua/zlam-departamentu-informatsii-rf/#google_vignette – (дата звернення 27.11.2023) – Назва з екрана.

44. Пошук через інтернет [Електронний ресурс] – Режим доступу: https://sites.google.com/view/bezpecnyj-internet – (дата звернення 17.09.2023) – Назва з екрана.

45. Що вибрати: сторінку чи групу на Facebook? [Електронний ресурс] – Режим доступу: https://crespo.com.ua/shho-krashhe-i-shho-pravilno-storinka-chi-grupa/ – (дата звернення 19.09.2023) – Назва з екрана.

46. Rakesh V., Singh D., Vinzamuri B., Reddy C.K. Personalized Recommendation of Facebook Lists Using Content and Network Information // Association for the Advancement of Artificial Intelligence (Proceedings of the Eighth International AAAI Conference on Weblogs and Social Media, 2014.

47. Beautifulsoup4 [Електронний ресурс] – Режим доступу: https://pypi.org/project/beautifulsoup4/ – (дата звернення 29.09.2023) – Назва з екрана.

48. Naive Bayes [Електронний ресурс] – Режим доступу: https://scikit-learn.org/stable/modules/naive_bayes.html – (дата звернення 1.10.2023) – Назва з екрана.

49. Закон України «Про основи національної безпеки України» від 19 червня 2003 року: із змінами, внесеними Законом України від 12 лютого 2015 р.: за станом на 1 березня 2015 р. / [Електронний ресурс]. - Режим доступу: http://zakon4.rada.gov.ua/laws/show/964-15. – (дата звернення 1.10.2023) – Назва з екрана.

50. Пелещишин А. М. Архітектура програмного комплексу моніторингу та аналізу інформаційних загроз у віртуальних спільнотах / А. М. Пелещишин, Р. В. Гумінський // 4th International academic conference «Information, Communication, Society» ICS-2015, Львів, Славське, 20-23 трав. 2015 р. / Національний університет "Львівська політехніка". - Львів : Видавництво Львівської політехніки, 2015. - С. 20 - 21.

51. Stohl C., Stohl M. Networks of Terror: Theoretical Assumptions and Pragmatic Consequences // Communication Theory, 2007. - Vol. 17. - P. 93 - 124.

52. Optimization Concepts and Applications in Engineering. 3rd Edition/ A.D. Belegundu, T.R. Chandrupatla. – Cambridge University Press, 2019. – 465 p.

53. Гумінський Р. В. Методика прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот / Р. В. Гумінський // Східно-Європейський журнал передових технологій. - 2015. - № 2/2 (74).

54. Розвідка з відкритих джерел (Open-source intelligence - OSINT) [Електронний ресурс] – Режим доступу: https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/ – (дата звернення 9.11.2023) – Назва з екрана.

55. Determination of the account personal data adequacy of webcommunity member / Fedushko S., Syerov Yu., Peleschyshyn A., Korzh R. // Intern. Journal of Computer Science and Business Informatics. - Vol. 15 (1). - 2015. - P. 1-12.

ДОДАТОК А

Копії наукових публікацій

к.т.н., доц. Муляр І.В. (ХмНУ)
Матвійчук А.В. (ХмНУ)

ОЦІНКА ІНФОРМАЦІЙНОЇ ЗАГРОЗИ ТА УПРАВЛІННЯ ПРОСТОРОМ ВІРТУАЛЬНИХ ГРУП

У соціальних мережах часто з'являються фейкові новини та дезінформація, які можуть вплинути на групове сприйняття інформації та призвести до неправильних рішень. Моніторинг допомагає вчасно виявляти такі випадки та приймати відповідні заходи.

Віртуальні групи - це складне і різноманітне середовище, яке включає в себе всі дані, які стосуються взаємодії і комунікації між учасниками таких груп в інтернеті. Це інформаційний простір складається з двох основних компонентів:

– зовнішнього інформаційного простору, а саме інформація та дані, яка обробляє зовнішню віртуальну групу та впливає на її діяльність, наприклад повідомлення від інших користувачів соціальних мереж, новини, ресурси, які група використовує або спільно обговорює;

– внутрішній інформаційний прості, а саме інформація та дані, якою обмінюються члени самої віртуальної групи всередині групи ,наприклад текстові

повідомлення, сумісні документи, обговорення, рішення та інші дані, що виникають у внутрішньому спілкуванні та групі співпраці.

Оцінка та управління інформаційним простором віртуальних груп важлива для забезпечення їх продуктивності та безпеки. Неграмотне використання або небажане втручання в цьому просторі може створити загрозу для конфіденційності та безпеки даних, а також пов'язати взаємодію та спільну роботу групи. Тому розуміння та управління інформаційним простором віртуальних груп є важливим аспектом у сучасному цифровому світі.

Отже, для оцінки показника інформаційної загрози процесу функціонування віртуальної групи необхідно виконати такі кроки:

- спроектувати загальну модель інформаційного простору, яка дозволить визначити структуру і взаємозв'язок між зовнішнім і внутрішнім інформаційним простором віртуальної групи;
- конкретизувати модель внутрішнього інформаційного простору для відображення структури та змісту інформації, що обмінюється між елементами віртуальної групи;
- розробити модель інформаційного наповнення віртуальної групи та її складових для проведення подальшого аналізу цієї інформації.

Ці кроки допоможуть зрозуміти структуру і динаміку інформаційного середовища віртуальної групи та виявити можливі загрози для її функціонування.

ДОДАТОК Б

Презентація кваліфікаційної роботи

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
кафедра кібербезпеки

Андрій МАТВІЙЧУК

Метод виявлення інформаційної загрози за парсингом спільнот у соціальних інтернет-сервісах

Науковий керівник
ст. викладач, к.т.н., доцент Муляр І.В.

Загальна характеристика магістерської роботи

Мета роботи: Розробка методу та інструментів для аналізу та виявлення впливу інформації в соціальних мережах, спрямованого на оптимізацію часових витрат на збір та обробку даних щодо поширення та характеристик повідомлень.
Об'єктом дослідження процес впливу онлайн-спільнот соціальних мереж.
Предметом дослідження методи та інструменти виявлення інформаційних загроз.
Задачі досліджень у роботі формулюються наступним чином:

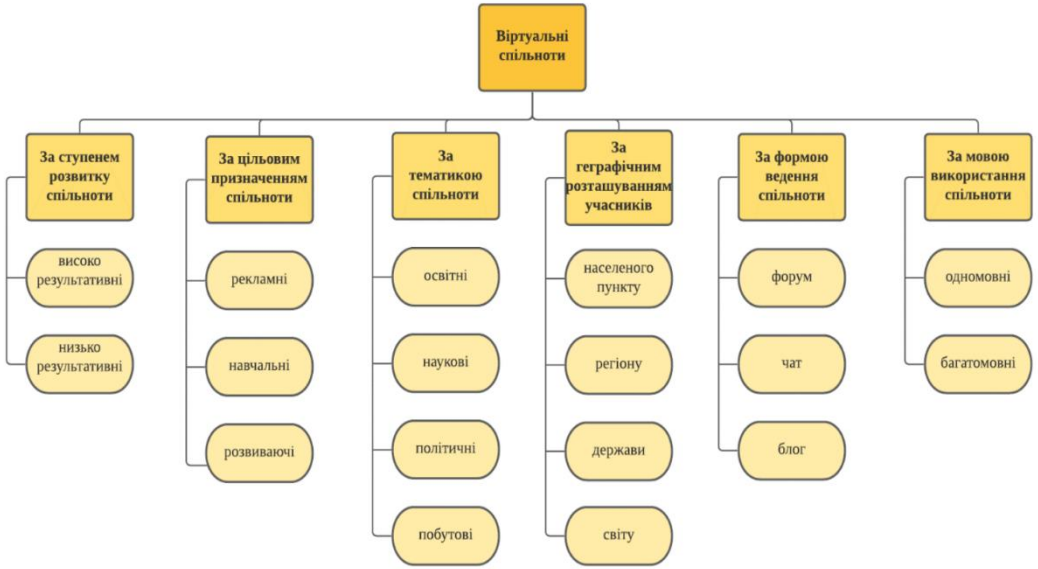
- Здійснити аналіз онлайн-спільнот, та розглянути особливості їх організації в соціальних мережах в Інтернеті.
- Розробити математичні моделі для аналізу інфополя онлайн-спільнот.
- Створити метод виявлення інформаційного впливу, що базується на аналізі параметрів розподілу характеристик контенту в ресурсах соціальних мереж.
- Розрахувати показник інформаційної загрози онлайн-спільноти.
- Розробити технологію для створення баз даних на основі вмісту онлайн-ресурсів.
- Запропонувати архітектуру системи моніторингу онлайн-ресурсів, з метою оцінки потенційної загрози онлайн-спільноти.

Наукова новизна одержаних результатів

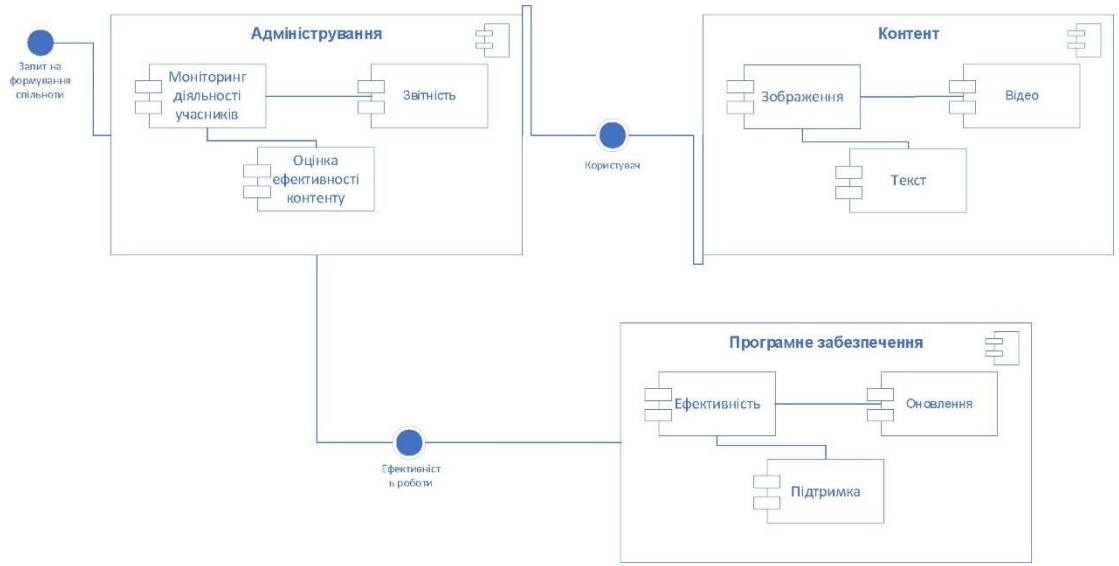
- вдосконалено модель онлайн-спільноти, яка стала основою для розроблення структури бази даних щодо обліку інформаційних загроз;
- розроблено метод виявлення інформаційної загрози за парсингом груп у соціальних інтернет-сервісах, який базується на врахуванні кількості учасників, при якій реалізується інформаційний вплив.
- запропоновано архітектуру системи аналізу інформаційного впливу онлайн-спільноти для більш ефективного виявлення та вирішення цих загроз.

Практична значимість:
розроблені алгоритми для виявлення загрозливих сторінок обговорень у соцмережах, що базуються на розширених можливостях глобальних пошукових систем та використанні API-методів соціальних мереж. Ці алгоритми дозволяють ідентифікувати сторінки обговорень відповідно до їхнього контенту, що дало можливість реалізації підходів щодо вчасного реагування та протидії.

Класифікація спільнот в соцмережах



Компоненти соціальних груп



Моделювання інфополя віртуальних груп

Формальна модель соціальної мережі

$$SocialNetworks = \langle Members, Content, Link \rangle$$

де *Members* - зареєстровані користувачі соціальної мережі;
Content - інформаційне наповнення (контент);
Link - зв'язки між зареєстрованими користувачами соціальної мережі.

Формальна модель онлайн-спільноти

$$VirtualCommunity = \langle Content, Member \rangle$$

Зовнішнє інфополе

Формальна модель зовнішнього інфополя онлайн-спільноти

$$InfSpace = \langle VirtualCommunity, AgentInfl, Shadow(VirtualCommunity), LinkExternal(VirtualCommunity), LinkExternal(AgentInfl) \rangle ,$$

де *VirtualComumunity* - сукупність онлайн-спільнот в інформаційному просторі;
AgentInfl - сукупність агентів зовнішнього інфополя;
LinkExternal (VirtualComumunity) - матриця зв'язків між онлайн-спільнот в інформаційному просторі;
LinкEx1eгnal(AgentInfl) - матриця зв'язків між онлайн-спільнот та агентами зовнішнього впливу;
Shadow(VirtualComumunity) - множина зареєстрованих користувачів соціальної мережі, які є тінню онлайн-спільноти.

Формальна модель внутрішнього інфополя онлайн-спільноти

$$InfSpace(VirtualCommunity_i) = \langle Thread(VirtualCommunity_i), LinkInternal(Tread), Member(VirtualCommunity_i), Shadow(VirtualCommunity_i) \rangle ,$$

ле *Thread(VirtualCommunity$_i$)* - сукупність дискусій *i*-ї онлайн-спільнот;
LinkInternal(Thread) - матриця зв'язків між дискусіями і-ї онлайн-спільнотою;
Member(VirtualCommunity$_i$) - множина учасників дискусій *i*-ї онлайн-спільноти, зареєстровані користувачі соціальних мереж;
Shadow(VirtualCommurity$_i$) - множина зареєстрованих користувачів соціальних мереж, які зацікавлені ідеологією (тематикою) *i*-ї онлайн-спільноти.

Перший науковий результат

Модель дискусії

$$ThreadTitle_i^{(Term)} = \{Term_j\}_{j=1}^{N_i^{(TT)}},$$

де $Term_j$ – терм із множини термів у назві *i*-ї дискусії;
$N^{(TT)}$ – кількість термів у назві *i*-ї дискусії.

Модель множини термів дискусії

$$Thread_i^{(Term)} = ThreadTitle_i^{(Term)} \bigcup ThreadDiscription_i^{(Term)} \bigcup_{j=1}^{N_i} PostText_{ij}^{(Term)},$$

Опис дискусії *ThreadTitle* - це множина термів, з яких складається опис дискусії.
Текст повідомлення *PostText* - це множина термів, з яких складається текст повідомлення.

Просторова модель онлайн-спільноти

$$\overline{VirtualCommunity}^{(Term)} = \langle Term, W \rangle,$$

де *Term* - множина термів дискусії;
W - множина вагових коефіцієнтів термів дискусії;
N - кількість термів у дискусії

Формування показника інформаційної загрози

$$InfThreat(VirtualCommunity) = \begin{cases} \dfrac{Value(VirtualCommunity)}{Value(VirtualCommunity)^*}, \\ 1, якщо \dfrac{Value(VirtualCommunity)}{Value(VirtualCommunity)^*} > 1 \end{cases}$$

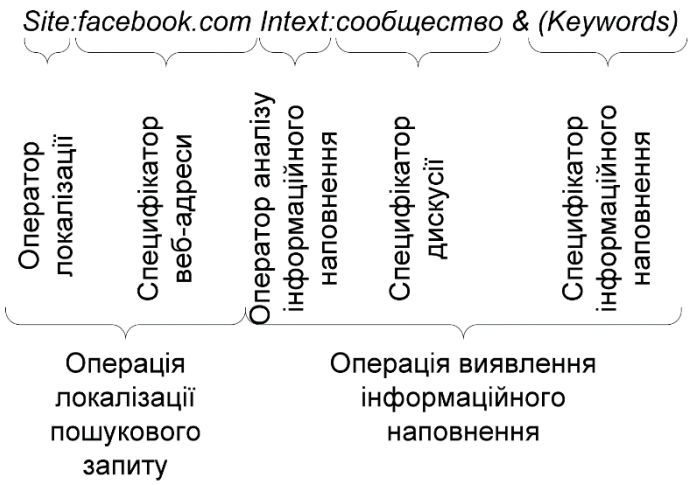
де *Value* (*VirtualCom munity)*– цінність онлайн-спільноти;
Value(*VirtualCommunity)**– критична цінність онлайн-спільнот, за якої реалізується інформаційна загроза

Правила формування груп

1. Група не може бути пустою, тобто повинна містити хоча б одну дискусію.
2. У онлайн-спільнот іможе бути від 1 до n груп (n - кількість дискусій), тобто в групі може бути від 1 до n дискусій.
3. Всі дискусії в групі взаємозв'язані внутрішніми та зовнішніми гіперпосиланнями або спільними зареєстрованими учасниками. Дискусії, які не зв'язані з дискусіями групи, утворюють нову групу.
4. Всі дискусії групи не можуть мати внутрішніх та зовнішніх гіперпосилань або спільних зареєстрованих учасників з дискусіями інших груп. У разі наявності цих зв'язків групи об'єднуються в одну групу

Алгоритми пошуку дискусій у соціальних мережах

Формалізований запит для виявлення сторінок у соціальній мережі «Facebook»



Аналіз HTML-коду сторінки для виявлення URL-адреси сторінки переліку тематично зв'язаних груп

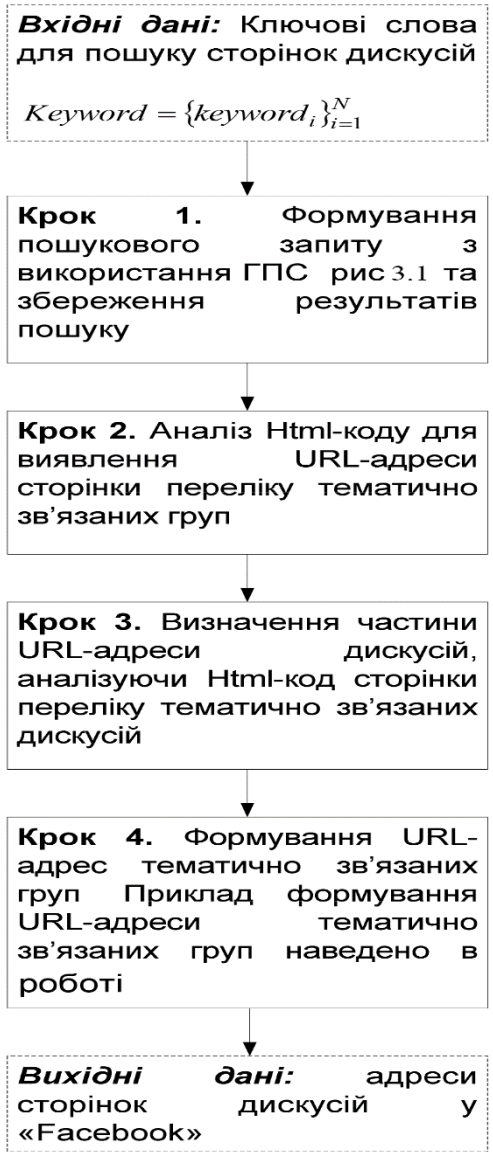
URL адреса сторінки

```
<a title="" role="menuitem" href="https://www.facebook.com/valerij.klocko/groups"
class="-cx-PUBLIC-abstractMenuItem__anchor">
<span class="-cx-PUBLIC-abstractMenuItem__label">Группы</span>
</a>
```

Пункт меню

URL адреса сторінки переліку тематично зв'язаних груп

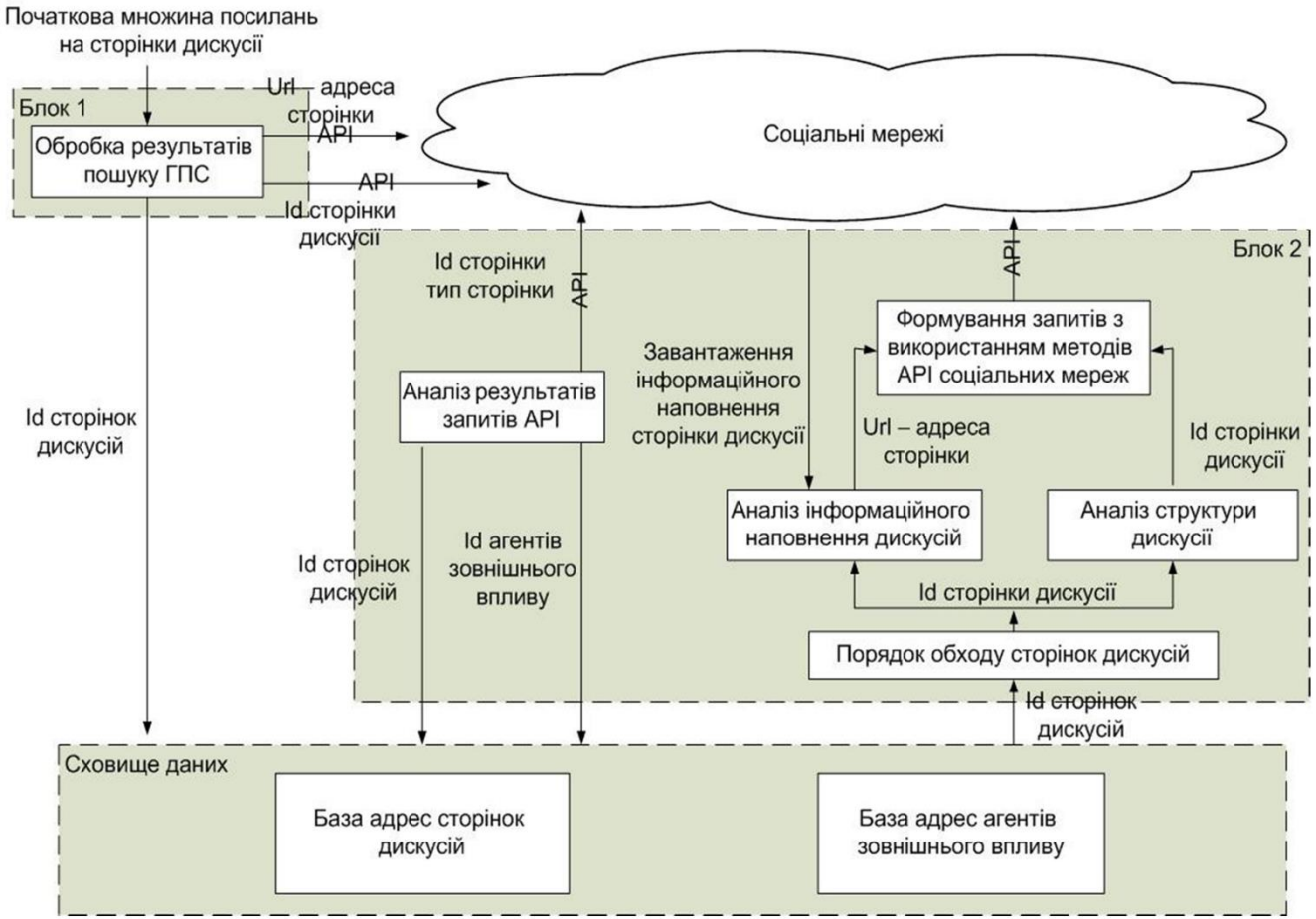
Схематичне зображення алгоритму пошуку



Другий науковий результат

Алгоритм глибокого пошуку

Структурна схема функціонування пошукового робота



Схематичне зображення алгоритму формування інформаційного простору онлайн-спільноти

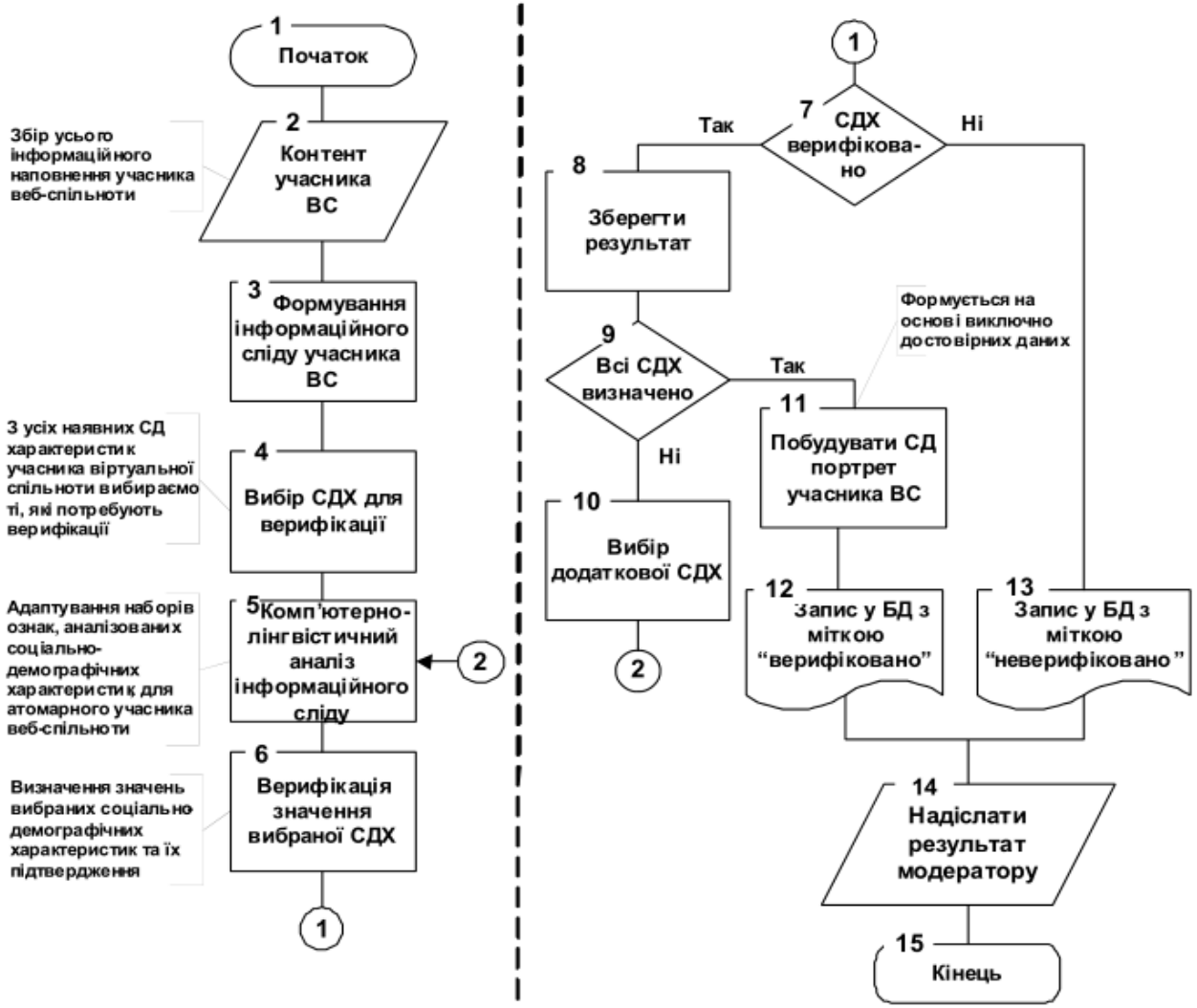
Вхідні дані: 1) Результати пошуку сторінок дискусії;
2) Векторно-просторова модель дискусії.

Крок 1. Кластеризації результатів пошуку з використанням векторно-просторової моделі дискусії $\overline{Thread}^{(Term)} = \langle Term, W \rangle$ та віртуальної спільноти $\overline{VirtualCommunity}^{(Term)} = \langle Term, W \rangle$.
Дискусії обробляються послідовно згідно з підходом Солтона.

Крок 2. Розподіл на деструктивну та конкурентну ВС. Розподіл проводиться, використовуючи значення позитивних та негативних напрямів дописів в дискусіях (2.17, 2.18, 2.20, 2.21).
Дискусія для якої: $Sim(Thread_i)^{Negative} \geq Sim(Thread_i)^{Positive}$ належатиме до деструктивної ВС, в іншому випадку дискусія входить у конкурентну ВС.

Вихідні дані: 1) Віртуальні спільноти;
2) Векторно-просторова модель дискусії та віртуальної спільноти.

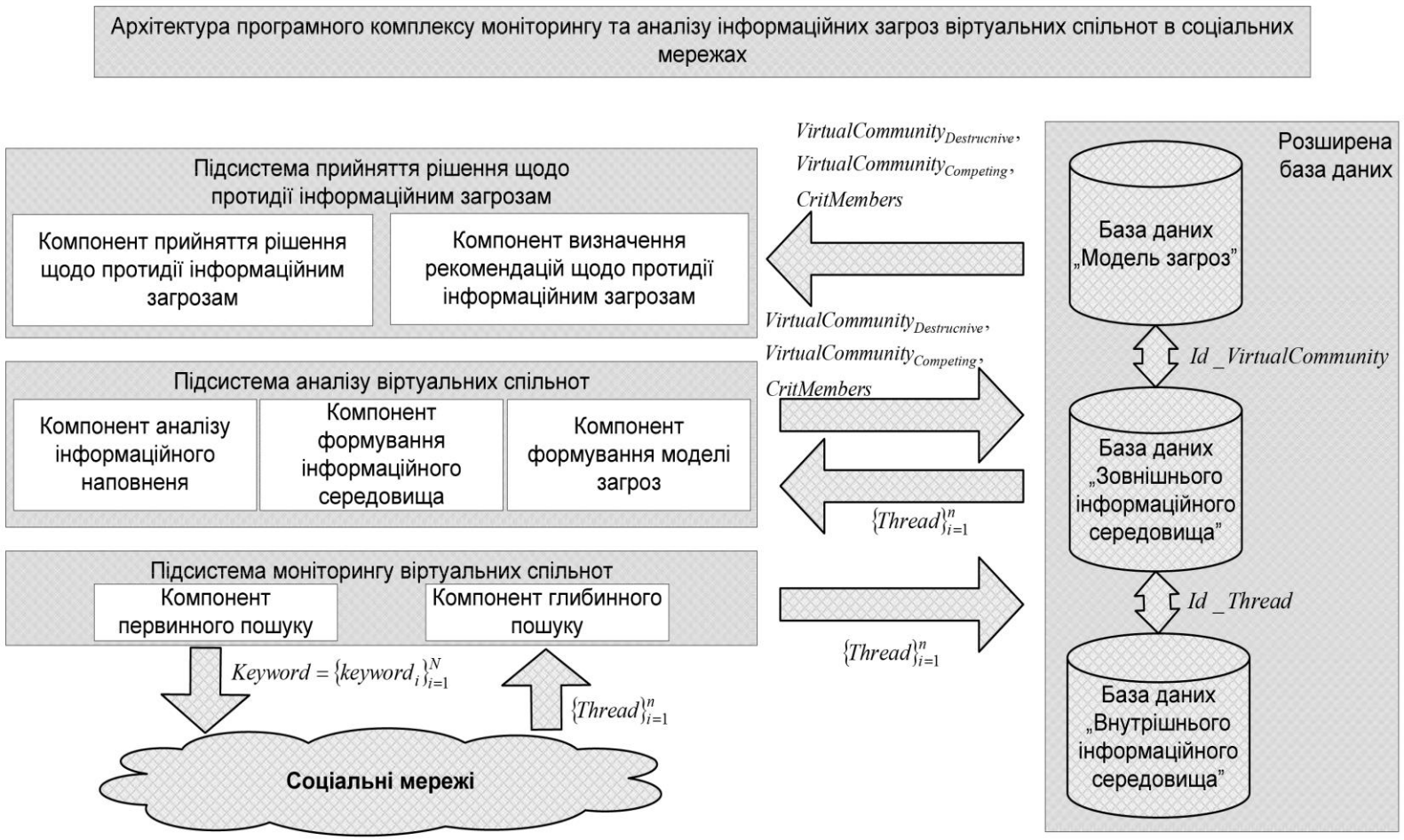
Блок-схема алгоритму формування портрету учасника онлайн-спільноти



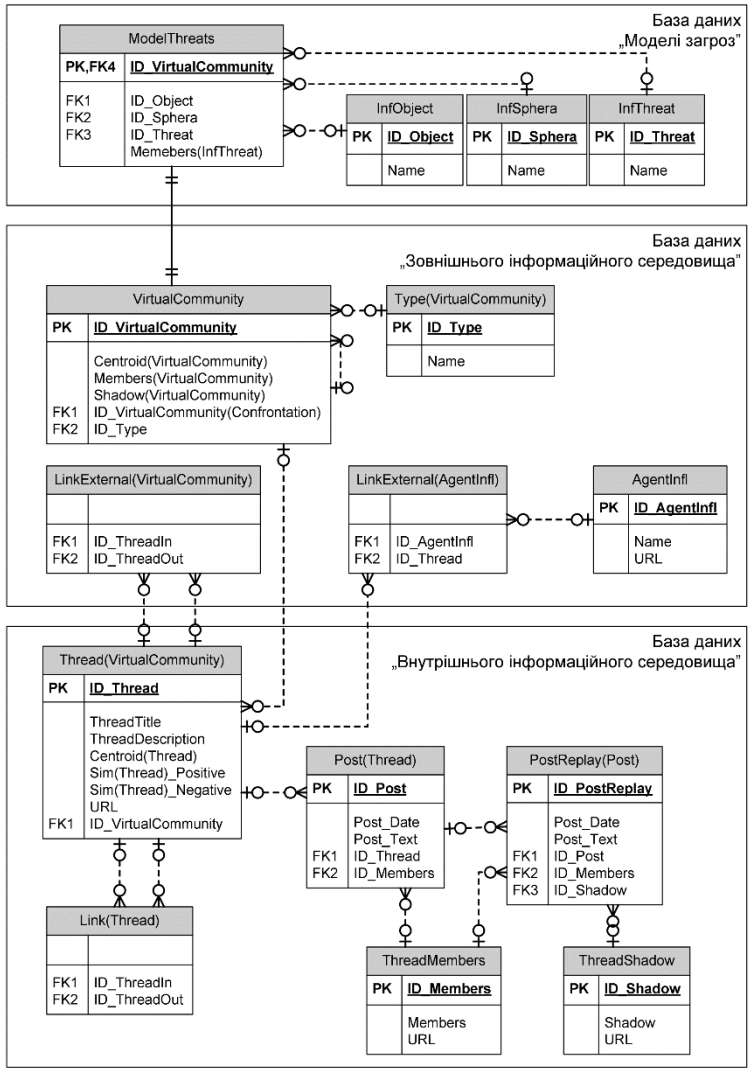
Третій науковий результат

Архітектура системи моніторингу інформаційних загроз

Архітектура програмного комплексу моніторингу та аналізу інформаційних загроз



ER-діаграма бази даних



Висновки

У магістерському досліджені розв’язано актуальне науково-прикладне завдання, а саме розроблено метод та інструментарій для аналізу та виявлення впливу загрозливої інформації в соціальних інтернет-сервісах, спрямованого на оптимізацію часових витрат на збір та обробку даних щодо поширення та характеристик повідомлень.

Запропоновано використання методів машинного навчання для класифікації контенту в соцмережах за рівнем потенційного впливу. Розроблено алгоритми інтелектуального пошуку та моніторингу інформаційних кампаній на основі графових моделей. Створено інструментарій автоматизованого збору статистики поширення повідомлень з використанням API соціальних мереж.

Отримано вагомі результати:

- Проведено ґрунтовний аналіз проблем захисту даних у соціальних інтернет-сервісах. Сформульовано завдання адаптивного захисту доступу з урахуванням повноважень користувачів і типів даних.
- Досліджено існуючі підходи до протидії інформаційним загрозам в соцмережах. Виявлено відсутність на сьогоднішній момент ефективного інструментарію оцінки таких загроз відносно онлайн-спільнот.
- Вдосконалено модель інформаційного простору онлайн-спільноти, що стала базисом для аналізу загроз її безпеці.
- Розраховано кількісний показник рівня інформаційної загрози з урахуванням цінності онлайн-спільноти.
- Розроблено ефективні алгоритми пошуку уразливих об’єктів у соцмережах за допомогою API. Створено інструментарій автоматизованого збору статистики поширення повідомлень з використанням API соціальних мереж.
- Розроблено метод виявлення інформаційної загрози за парсингом груп у соціальних інтернет-сервісах, який базується на врахуванні кількості учасників, при якій реалізується інформаційний вплив
- Розроблено архітектуру програмного комплексу моніторингу та захисту онлайн-спільнот. Проведено успішну експериментальну перевірку запропонованого функціоналу.
- Застосування даних методів та підходів дозволяє суттєво прискорити аналіз інформаційних операцій та оцінку їх впливу на користувачів соцмереж. Це сприяє підвищенню ефективності моніторингу, прогнозування та реагування на інформаційні загрози в соціальних медіа.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА ДИПЛОМНУ РОБОТУ

ОПП «магістр»

Магістр Матвійчук А.В.

Тема Метод виявлення інформаційної загрози за парсингом спільнот у соціальних інтернет-сервісах

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Обсяг дипломної роботи ОПП «магістр»:

кількість листів креслень ; кількість сторінок записки 87

1. Короткий зміст ДР та прийнятих рішень В рамках магістерської роботи проведено ґрунтовний аналіз особливостей інформаційного наповнення та взаємодії користувачів у соціальних мережах. Розроблено формалізовану математичну модель для опису процесів функціонування та поширення інформації у соціальних мережах з урахуванням їх топології, цільової аудиторії та інших ключових параметрів.
Запропоновано удосконалений метод виявлення інформаційних загроз в соціальних мережах на основі інтелектуального аналізу контенту, динаміки його поширення та сентимент-аналізу реакцій користувачів. Метод дозволяє з високою ймовірністю ідентифікувати потенційно небезпечну та деструктивну інформацію на ранніх етапах її появи в соцмережі.

2. Висновок про відповідність ДР дипломному завданню Дипломна робота ОП «магістр» у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині дипломної роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовано актуальність дослідження проблеми забезпечення інформаційної безпеки соціальних мереж. Проведено аналіз існуючих підходів у цій сфері та окреслено напрямки удосконалення методів моніторингу й виявлення загроз. Сформульовано мету та конкретні завдання роботи. У першому розділі досліджено основні вимоги до систем моніторингу соціальних мереж та проаналізовано чинники, що впливають на їх ефективність. Наступні розділи присвячені безпосередньо розробці математичної моделі поширення інформації у соцмережах з урахуванням топології зв’язків та інтелектуального методу виявлення деструктивного контенту. Також розглянуті питання практичного застосування отриманих результатів.

4. Позитивні сторони проекту У роботі запропоновано низку інноваційних підходів у сфері кібербезпеки соціальних мереж. Зокрема, розроблено метод розрахунку показника рівня інформаційної загрози для віртуальних спільнот Це дозволяє здійснювати кількісну оцінку потенційної небезпеки онлайн-груп та прогнозувати ескалацію інформаційних загроз в соціальних мережах.

5. Негативні сторони проект.у Ефективний моніторинг віртуальних спільнот та протидія інформаційно-психологічним впливам в мережі потребують залучення вузькопрофільних фахівців. Зокрема, необхідна наявність команди кваліфікованих аналітиків соціальних мереж, експертів з кібербезпеки, які володіють методиками виявлення ознак радикалізації в інтернет-просторі та технологіями інформаційного впливу для запобігання поширення деструктивних ідей.

6. Оцінка графічного оформлення та пояснювальної записки роботи Пояснювальна записка відповідає нормам для її оформлення.

7. Відгук про роботу в цілому В загальному дипломна робота заслуговує позитивної оцінки. Весь матеріал дипломної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики дипломної роботи.

8. Інші зауваження

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої дипломної роботи, можна зробити висновок, що вона заслуговує оцінку «добре». В

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
д.т.н, проф. кафедри ТМІТ, Підченко С.К.

« 12 » 12 2023 . (підпис)

ХНУ. Зам. 54, тир. 6000, 2007.

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 6%**

	Документ		Сумарний збіг по Базі Даних	
ID: 122497 Назва: Метод виявлення інформаційної загрози за парсингом спільнот у соціальних інтернет-сервісах Додано в БД: 2023-12-11 Автора: Матвійчук А.В. Керівники: Муляр І.В. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	95203	1463	457 (0%)	7 (0%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015992646

Дата перевірки:
11.12.2023 14:06:09 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
11.12.2023 14:48:14 EET

ID користувача:
100008300

Назва документа: **Матвійчук_на плагіат**

Кількість сторінок: **80** Кількість слів: **13543** Кількість символів: **111408** Розмір файлу: **2.82 MB** ID файлу: **1015675274**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

2.7%
Схожість

Найбільша схожість: **0.92%** з Інтернет-джерелом (http://ena.lp.edu.ua:8080/bitstream/ntb/45593/3/dys_vus_v.a.pdf)

2.34% Джерела з Інтернету	249	Сторінка 82
0.56% Джерела з Бібліотеки	46	Сторінка 82

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	4
Підозріле форматування	13 сторінок

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод виявлення інформаційної загрози за парсингом спільнот у соціальних інтернет-сервісах

Автор: Матвійчук Андрій Вікторович

Науковий керівник: Муляр Ігор Володимирович, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 97.3%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 100%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ І.В. Муляр

Гарант ОП _____ В.Ю. Тітова

Завідувач кафедри кібербезпеки _____ Ю.П. Кльоц