Міністерство освіти і науки України

Національний авіаційний університет

На правах рукопису

Гумінський Руслан Вікторович

УДК 004.738.5+004.773.2

МЕТОДИ І ЗАСОБИ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ ВІРТУАЛЬНИХ СПІЛЬНОТ В ІНТЕРНЕТ СЕРЕДОВИЩІ СОЦІАЛЬНИХ МЕРЕЖ

Спеціальність 21.05.01 – інформаційна безпека держави

Дисертація на здобуття наукового ступеня

кандидата технічних наук

Науковий керівник:

Пелещишин Андрій Миколайович

д.т.н., професор

Київ - 2016

Зміст

Вступ

Актуальність теми. У сучасному інформаційному суспільстві відбувається зародження і становлення соціальних формацій – віртуальних спільнот з принципово іншими (порівняно з традиційними формами впливу на соціальні структури в індустріальному суспільстві) можливостями впливу на традиційні громадські та державні структури, поява яких пов’язана з програмами створення оперативного доступу через канали відкритих телекомунікаційних мереж до розподілених інтелектуальних і матеріальних ресурсів у будь-якій точці земної кулі. Багато в чому поява таких віртуальних спільнот пов’язана з проведенням телекомунікаційної глобалізації.

Віртуальні спільноти (англ. virtual communities, e-communities) – новий тип спільнот, які виникають і функціонують в електронному просторі (передусім за допомогою мережі Інтернет) з метою сприяння вирішенню своїх професійних, політичних завдань, задоволення своїх потреб у мистецтві, дозвіллі тощо [39, 67, 150, 153].

Поряд з конструктивними віртуальними спільнотами, які прагнуть активно взаємодіяти з суспільством, маючи на меті поліпшення життя як суспільства загалом, так і окремих соціальних груп та індивідів, соціальні мережі все частіше використовують для створення деструктивних віртуальних спільнот. Проте деструктивні віртуальні спільноти, на відміну від конструктивних, намагаються з цим співтовариством боротися усілякими, не завжди законними, методами. Об'єктом агресії деструктивних віртуальних спільнот є усе суспільство або прихильники тих чи інших соціальних груп, як правило, вороже налаштованих до цієї деструктивної віртуальної спільноти [23, 59, 106, 148].

Крім того, віртуальні спільноти все активніше і масштабніше використовують в інтересах інформаційно-психологічного впливу. Вони надають широкі можливості в плані впливу на формування громадської думки,

прийняття політичних, економічних і військових рішень, впливу на інформаційні ресурси противника і поширення спеціально підготовленої інформації (дезінформації) [15].

Процеси в соціальних мережах викликають підвищений інтерес в науці, однак темпи наукових досліджень істотно відстають від розвитку соціальних мереж [37].

У наукових дослідженнях, пов'язаних з протидією деструктивному інформаційно-психологічному впливу виокремлюють такі напрями:

– дослідження проблем створення систем контент-моніторингу соціальних ресурсів мережі Інтернет з метою розвідки та інформаційного протиборства;

– розроблення методів і алгоритмів проведення інформаційних операцій у відкритих (закритих) ресурсах Інтернету.

Перший напрям об'єднує розроблення та розвиток методів і засобів пошуку, збору та аналізу інформації з різних джерел мережі Інтернет, що дає змогу розглядати її у визначений момент часу (роботи Д. В. Ланде, О. Г. Додонов) [25 – 28, 51 – 55].

Другий напрям об'єднує декілька піднапрямів – розроблення алгоритмів, моделей інформаційних операцій (роботи В. П. Горбулін, О. Г. Додонов, В. М. Фурашев) [12, 24, 97, 98] та моделей інформаційного впливу в соціальних мережах (Д. А. Губанов, А. Г. Чхаршвілі, E. R. Smith) [17, 18, 100, 108, 132, 144, 145] з метою вироблення управлінських рішень щодо інформаційного протиборства в соціальних мережах.

Сьогодні саме об'єднання цих напрямів досліджень з метою створення технічних та програмних засобів для виявлення та протидії деструктивному впливу інформаційного наповнення віртуальних спільнот у соціальних мережах є найактуальнішим. Це зумовлено тим, що деструктивні віртуальні спільноти в соціальних мережах створюють нові загрози, оскільки держава вже не здатна контролювати їх у повному обсязі через особливості їх

функціонування у соціальних мережах [86], що ускладнюється відсутністю типових методик і рішень, неповнотою відповідних технологічних підходів. Дослідження з цих проблем поки що найчастіше є вузькоспеціалізованими [26].

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана у межах пріоритетних наукових напрямів, які охоплюють актуальні проблеми, відповідно до рішення Ради президентів академій наук України від 11 липня 2014 року «Про Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук національних академій наук України на 2014 – 2018 роки», – «Інформатика» за темою: «Розробка обчислювальних алгоритмів і процедур з метою вирішення практичних задач міждисциплінарного характеру для застосувань, що належать до науково-технічної та соціально-економічної сфер діяльності людини», «Наукова інформація» за темою: «Соціальні мережі, формування в Україні інформаційного суспільства».

Дисертаційну роботу виконано у межах зареєстрованої тематики Академії сухопутних військ імені гетьмана Петра Сагайдачного "Основні напрямки роботи засобів масової інформації щодо протидії негативному інформаційному впливу противника", шифр "ЗМІ" (№ державної реєстрації 0101u001889).

Мета і завдання дослідження. Мета дисертаційної роботи – забезпечення інформаційної безпеки держави у соціальних мережах шляхом розроблення методів і засобів виявлення та оцінки інформаційних загроз віртуальних спільнот в інтернет середовищі соціальних мереж.

Мета дисертаційної роботи визначає необхідність розв’язання таких задач:

- Аналіз віртуальних спільнот у соціальних мережах як суб’єктів інформаційної безпеки держави.

- Побудова математичних моделей інформаційного середовища віртуальної спільноти та визначення характеристик віртуальних спільнот у соціальних мережах.
- Формування показника інформаційної загрози віртуальної спільноти на підставі визначених характеристик.
- Розроблення методів і алгоритмів виявлення та оцінки інформаційних загроз віртуальних спільнот у соціальних мережах.
- Розроблення архітектури програмно-алгоритмічного комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах, який вирішуватиме завдання виявлення та оцінки інформаційних загроз віртуальних спільнот у соціальних мережах.

Об'єктом дослідження є процеси функціонування віртуальних спільнот в інтернет середовищі соціальних мереж.

Предметом дослідження методи і засоби виявлення та оцінки інформаційних загроз віртуальних спільнот в інтернет середовищі соціальних мереж.

Методи дослідження. Для вирішення завдань моделювання інформаційного середовища віртуальних спільнот використано теоретико-множинні підходи, теорію відношень, апарат теорії реляційної алгебри, баз даних та контент-аналізу. Для пошуку віртуальних спільнот у соціальних мережах застосовано сучасні засади пошуку інформації в Інтернеті, а також апарат формальних мов для формування параметризованих запитів до глобальних пошукових систем. Для формування інформаційного середовища використано методи автоматичної кластеризації текстів. Для визначення рекомендацій щодо протидії інформаційним загрозам віртуальних спільнот у соціальних мережах застосовано алгоритми теорії графів. Під час проектування програмного комплексу використано апарат розподілених інформаційних систем класу "клієнт – сервер" та технології обміну інформацією у відкритих системах.

Наукова новизна одержаних результатів. Наукова новизна одержаних результатів полягає в обґрунтуванні та виконанні наукового завдання розроблення методів і засобів для організації виявлення та оцінки інформаційних загроз віртуальних спільнот у соціальних мережах. Отримано такі наукові результати:

- удосконалено модель віртуальної спільноти за допомогою розширення її до моделі інформаційного середовища віртуальної спільноти в соціальних мережах, що включає моделі зовнішнього та внутрішнього інформаційного середовища, яка стала основою для розроблення структури бази даних щодо обліку та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах;
- уперше уведено показник інформаційної загрози віртуальної спільноти в соціальних мережах шляхом визначення цінності віртуальної спільноти, що враховує структуру, кількість учасників та якість інформаційного наповнення сторінок дискусій віртуальної спільноти, та став основою для методів щодо прийняття рішення з протидії інформаційним загрозам віртуальних спільнот у соціальних мережах та визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти в соціальних мережах;
- уперше розроблено метод щодо прийняття рішення з протидії інформаційним загрозам віртуальних спільнот у соціальних мережах шляхом об’єднання показників інформаційної загрози, для яких визначення критичних цінностей віртуальної спільноти ґрунтується на встановленні експертами кількості учасників віртуальної спільноти, при якій реалізовується інформаційна загроза, та загальної кількості учасників деструктивної та конкурентної віртуальних спільнот, що дало змогу надати рекомендації щодо прийняття рішення з протидії інформаційним загрозам віртуальних спільнот у соціальних мережах;

- отримали подальший розвиток графові моделі соціальних мереж на основі матричного представлення графів, які, завдяки врахуванню характеристик моделі інформаційного середовища віртуальної спільноти та запропонованого показника інформаційної загрози, стали основою для розробки методу прийняття обґрунтованих рішень щодо вибору дискусій віртуальної спільноти для інформаційного впливу;
- уперше розроблено архітектуру програмно-алгоритмічного комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах, функціональність якого базується на запропонованих у роботі методах та алгоритмах, що дає змогу організувати виявлення та оцінку інформаційних загроз віртуальних спільнот у соціальних мережах.

Практичне значення одержаних результатів. Практичне значення одержаних результатів дисертаційної роботи зумовлено тим, що вони дають змогу організувати виявлення та оцінку інформаційних загроз віртуальних спільнот у соціальних мережах. Зокрема, практично цінними є результати:

- розроблено стратегії протидії інформаційним загрозам віртуальних спільнот у соціальних мережах відповідно до правил протидії держави інформаційним загрозам віртуальних спільнот у соціальних мережах, що дало змогу вибору підходів щодо протидії інформаційним загрозам віртуальних спільнот у соціальних мережах;
- розроблено алгоритми пошуку сторінок дискусій у соціальних мережах з використанням розширених можливостей глобальних пошукових систем та запитів API-методів соціальних мереж, які дають змогу виявити сторінки дискусій у соціальних мережах відповідно їх інформаційного наповнення;
- розроблено алгоритми формування інформаційного середовища віртуальних спільнот у соціальних мережах шляхом застосування алгоритму кластеризації сторінок дискусій у соціальних мережах відповідно до їхнього інформаційного наповнення та алгоритму розподілу сторінок дискусій

залежно від напряму інформаційного наповнення для розподілу сторінок дискусій на деструктивну та конкурентну віртуальні спільноти.

Практичне значення отриманих результатів підтверджено відповідними реалізаціями (акт управління інформаційних технологій Міністерства оборони України від 15.05.2015 року та акт управління Служби безпеки України у Львівській області від 20.05.2015 року).

Особистий внесок здобувача. Усі наукові результати дисертаційної роботи автор отримав самостійно. У друкованих працях, опублікованих у співавторстві, здобувачеві належать: [71] – аналіз віртуальних спільнот у соціальних мережах як суб'єктів інформаційної безпеки держави, визначення основних інформаційних загроз, які можуть виникати під час функціонування віртуальних спільнот у соціальних мережах; [79] – модель інформаційного середовища віртуальної спільноти та методи розрахунку основних характеристик; [72] – алгоритм пошуку віртуальних спільнот за допомогою глобальних пошукових систем та їх особливостей; [75] – визначення складових показника інформаційної загрози віртуальних спільнот у соціальних мережах; [122] – введено поняття показника інформаційної загрози віртуальної спільноти та метод його розрахунку; [80, 123] – метод визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти; [20] – запропоновано структуру системи моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах; [73] – алгоритм моніторингу та аналізу віртуальних спільнот у соціальних мережах; [77] – аналіз стратегій інформаційного впливу на інформаційне середовище віртуальної спільноти; [124] – алгоритм формування інформаційного середовища віртуальних спільнот у соціальних мережах; [81] – архітектура програмного комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах.

Апробація результатів дисертації. Основні результати наукових досліджень неодноразово доповідалися на міжнародних та всеукраїнських наукових конференціях, зокрема:

- міжвідомча науково-технічна конференція «Проблемні питання розвитку озброєння і військової техніки» (Київ, 2012);
- науково-практичний форум «IV Січневі Гіси»: «Інтелектуальна оборона» (Львів, 2013);
- дев'ята наукова конференція Харківського університету Повітряних Сил імені Івана Кожедуба «Новітні технології – для захисту повітряного простору» (Харків, 2013);
- IV науково-технічна конференція «Проблемні питання розвитку озброєння і військової техніки» (Київ, 2013);
- II, III та IV міжнародні наукові конференції «Інформація, комунікація, суспільство» (Львів, 2013 – 2015);
- IV міжнародна науково-технічна конференція «ITSEC-2014»: «Безпека інформаційних технологій» (Київ, 2014);
- міжвідомча науково-практична конференція «Інформаційна безпека у воєнній сфері. Сучасний стан та перспективи розвитку» (Київ, 2015);
- міжнародна науково-практична конференція «Перспективи розвитку озброєння та військової техніки Сухопутних військ» (Львів, 2015).

Результати дисертаційних досліджень регулярно доповідалися на науково-технічній раді Наукового центру Сухопутних військ Академії сухопутних військ імені гетьмана Петра Сагайдачного.

Публікації. За результатами виконаних досліджень опубліковано 18 наукових праць, серед яких 6 статей у фахових наукових виданнях (технічні науки), 2 публікації у закордонних періодичних виданнях та 10 публікацій – у працях наукових конференцій.

Структура та обсяг роботи. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури зі 154 назви та 2 додатків. Загальний обсяг дисертації становить 157 сторінок, з них 108 сторінок основного тексту, який містить 35 рисунків та 7 таблиць.

РОЗДІЛ 1. АНАЛІЗ ВІРТУАЛЬНИХ СПІЛЬНОТ У СОЦІАЛЬНИХ МЕРЕЖАХ ЯК СУБ'ЄКТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Аналіз віртуальних спільнот у World Wide Web

Віртуальні спільноти (англ. virtual communities, e-communities) – новий тип спільнот, які виникають і функціонують в електронному просторі (передусім за допомогою мережі Інтернет) з метою сприяння вирішенню своїх професійних, політичних завдань, задоволення своїх потреб у мистецтві, дозвіллі тощо [39, 67, 150, 153].

Термін «віртуальне співтовариство» (Virtual Community) запропонував Г. Рейнгольд сформулювавши таке визначення: «Віртуальні співтовариства є соціальними об'єднаннями, які виростають з Мережі, коли група людей підтримує відкрите обговорення достатньо довго і людяно, для того, щоб сформувати мережу особистих стосунків в кіберпросторі» [49]. Зауважемо, що сам Г. Рейнгольд був серед засновників одного з перших віртуальних співтовариств «The Whole Earth Lectronic Link» (WELL).

Сучасні віртуальні спільноти дослідники розділяють на декілька основних категорій [3, 56, 90, 129, 136]:

– співтовариства за інтересами, які об'єднують людей з однаковими інтересами (політичними, соціальними, культурними, економічними тощо) або є спеціалізованими (співтовариства молодих батьків, клуби любителів певних марок автівок тощо);

– ігрові співтовариства, які надають користувачам можливості створювати власне середовище, історії та персонажів у вигаданих світах;

– географічні співтовариства, основані на географічному розташуванні або місцевості (часто такі угрупування об'єднуються за допомогою локальних мереж);

– співтовариства взаємин, сформовані навколо певних життєвих ситуацій, в яких люди можуть обмінюватися своїм досвідом і думками;

– комерційні співтовариства, стосунки в яких побудовані на купівлі та продажу онлайнових товарів і послуг;

– віртуальні держави.

За ступенем реалізації віртуальних спільнот в інтернет середовищі [66, 101, 137, 150]:

– соціальна мережа (Social Network) – популярний вид інтернет-спільноти, що відображає соціальну структуру зв’язків між людьми [4] Найпопулярнішими у світі соціальними мережами є «Facebook», «Вконтакте», «MySpace», «LinkedIn»;

– дискусійні листи – це вид віртуальних спільнот, які функціонують поза Вебом (WWW) за допомогою таких засобів, як електронна пошта;

– публічні соціальні мережі, прикладом яких є відомий сьогодні у світі сервіс мікроблогів «Twitter» та популярний на пострадянському просторі «Живий Журнал» (LiveJournal.com);

Відносно суспільства та держави виділяють такі типи віртуальних спільнот [11, 59]:

– індиферентні – налаштовані до суспільства за принципом: «Ми Вас не чіпаємо і Ви нас не чіпайте».

– ізоляціоністські – певною мірою є різновидами індиферентних віртуальних спільнот. Це структури типу закритих клубів за інтересами. Вони намагаються повністю сторонитись від взаємодії з суспільством або обходитися мінімумом контактів.

– конструктивні – навпаки, прагнуть активно взаємодіяти з суспільством, маючи на меті поліпшення життя як усього суспільства, так і окремих соціальних груп та індивідів;

– деструктивні віртуальні спільноти, як і конструктивні, також не ізолюються від суспільства, але, на відміну від останніх, намагаються з цим співтовариством боротися усілякими, не завжди законними, методами. Об'єктом агресії деструктивної віртуальної спільноти є суспільство загалом або прихильники певних соціальних груп, як правило, вороже налаштованих до цієї деструктивної віртуальної спільноти.

1.2. Аналіз соціальних мереж та їх сервісів

Соціальні мережі – один із популярних інтернет сервісів для створення віртуальних спільнот, якими користується 90 % користувачів українського інтернет середовища.

Соціальна мережа (Social service networks) – це інтернет сервіс, сайт, який дає змогу зареєстрованим на ньому користувачам розміщувати інформацію про себе і комунікувати між собою, налагоджуючи соціальні зв'язки. Контент на цьому сервісі створюєть безпосередньо самі користувачі [8].

Повштовхом для розвитку соціальних мереж стали такі можливості [70, 88]:

– спілкування з учасниками мережі в режимі реального часу, зокрема з використанням відео;

– отримання інформації від інших членів соціальної мережі;

– підтвердження ідей через участь в обговоренні з користувачами соціальних мереж.

Ці можливості сприяли зростанню популярності соціальних мереж, завдяки таким чинникам [2, 61, 64, 89]:

– використання соціальних мереж в організаційних цілях для поширення інформації як засобів масових комунікацій;

– використання соціальних мереж у політичній діяльності; сьогодні основними майданчиками для об'єднання протестувальників стали не юридично зареєстровані організації а їхні сторінки в соціальних мережах;

– використання сторінок соціальних мереж для об’єднання користувачів соціальних мереж та їх комунікації;

– інтеграції Інтернет-ЗМІ в соціальні мережі, що трансформує їх у соціальні медіа, що помогає подолати однобічгний, урізаний характер комунікації традиційних медіа, уможливлює відповідь аудиторії;

– зростання рівня довіри до соціальних медіа з боку аудиторії (який в середньому в декілька разів перевищує довіру до традиційних ЗМІ);

– перехід медіа війн у соціальні мережі та розширення їх можливостей, оскільки інформаційне середовище менш контрольоване.

Все вищезазначене приводить до того, що кількість користувачів соціальних мереж зростає з кожним роком. Аудиторія соціальної мережі «Facebook» перевищує мільярда користувачів, «Twitter», «Vk.com» та «Google+» – більше ніж 200 мільйонів, «LinkedIn» та «Odnoklassniki.ru» – понад 100 мільйонів [130].

Серед популярних соціальних мереж в Україні:

– «Facebook» – найпопулярніша соціальна мережа в світі, понад 3 млн українських користувачів.

– «Вконтакте» – популярна соціальна мережа в пострадянських країнах, по суті, є аналогом «Facebook», близько 20 млн. українських користувачів. Найпопулярнішою українською аудиторією є молоде покоління, що зумовлено наявністю великої кількості безкоштовного сервісу, можливістю перегляду неліцензійних фото- та відеоматеріалів.

Крім того більше ніж 80 % компаній в усьому світу використовують соціальні мережі для роботи. Близько 78 % людей довіряють інформації із соціальних мереж.

Розвиток соціальних мереж сприяє задоволенню потреб користувачів, вони пропонують низьку сервісів для їх комунікації:

Публічні сторінки – переважно їх організовують різні організації або окремі особистості, як відкриті джерела для всіх, кого хоч трохи цікавить тема сторінки. Наповнювати контент може тільки адміністрація, учасники соціальної мережі мають змогу лише підписуватися на сторінку і стежити за подіями та коментувати записи.

Групи, в яких люди можуть спілкуватися, ділитися інформацією та взаємодіяти, але тільки в межах заданої теми або ідеї, тобто група має ознаки тематичних дискусій. Можливе гнучке налащтування дій, які будуть доступні користувачам.

Заходи – призначені для анонсування подій.

На підставі аналізу визначення віртуальної спільноти саме групи (далі дискусії) є інструментом для створення віртуальних спільнот у соціальних мережах з метою комунікації їх учасників.

Групи поділяють на закриті та відкриті. У відкритій групі доступ до інформаційного наповнення сторінки мають всі зареєстровані користувачі соціальної мережі. В закритій групі доступ до інформаційного наповнення сторінки мають тільки зареєстровані в групі користувачі. Реєстрацію користувача в групі здійснюється тільки адміністратори групи. Отже, для інформаційного впливу на користувачів соціальної мережі доцільно розглядати відкриті групи, в яких доступ до інформаційного наповнення необмежений.

Зазвичай з однієї тематики створюються велика кількість груп, що крім тематики інформаційного наповнення, можуть відрізнятися:

– віковими ознаками;

– регіональною або територіальною ознакою;

– мовою спілкування;

– прихильністю до політичних партій тощо.

Отже, під структурою віртуальної спільноти в соціальних мережах доцільно розуміти сукупність дискусій, які об’єднані відповідно до їх інформаційного наповнення та тематичної спрямованості повідомлень і дописів.

Відповідно до визначення віртуальної спільноти та сервісів соціальної мережі, за допомогою яких її створюють, її основою є [9, 63, 70]:

– учасники;

– інформаційне наповнення (контент).

Учасники віртуальної спільноти – зареєстровані користувачі соціальної мережі, які беруть участь у спільноті, зареєструвавшись, та взаємодіють, створюючи інформаційне наповнення на сторінці дискусії.

Інформаційне наповнення (контент) – це текстовий, візуальний чи звуковий контент, який створюють учасники спільноти. Може містити: текст, зображення, звук, відео та анімацію

Спостерігаються ознаки децентралізованої ієрархії учасників віртуальної спільноти (принцип багатокерівництва), які розподіляються відповідно до їхньої ролі під час існування спільноти [9, 63]:

– незареєстровані учасники (гості) – можуть лише переглядати (не завжди в повному обсязі) інформаційне наповнення спільноти;

– зареєстровані учасники – можуть переглядати повідомлення, брати участь у дискусіях і опитуваннях та створювати їх, коригувати свої повідомлення;

– модератори – крім можливостей, які мають зареєстровані учасники, модератори виконують функції управління контентом: коригування інформаційного наповнення – видалення некоректних, беззмістовних

повідомлень та таких, що не відповідають чи суперечать ідеології спільноти, залучення нових учасників;

– адміністратори – в ієрархії спільноти мають найвищий статус: окрім функцій модератора, виконують функції реєстрації учасників, блокування порушників, призначення модераторів; основне їх завдання – управління спільнотою та технічна підтримка.

Модераторів спільноти вибирають з-поміж зареєстрованих учасників спільноти, які повністю підтримують її ідеологію та беруть активну участь у її фукціонуванні. Адміністратори спільноти можуть не підтримувати ідеологію, а виконують функції щодо створення спільноти замовниками. В ролі замовника можуть виступати як окремі особи або організації, які зацікавлені в пропагуванні ідеології для досягнення визначеної мети.

Процес функціонування віртуальних спільнот у соціальних мережах має певні особливості:

– сторінки мають низький ранг в алгоритмах ранжування сторінок, що ускладнює пошук цих сторінок;

– велику кількість сторінок спільнот не ранжують глобальні пошукові системи;

– отримати доступ до інформації в дискусіях соціальних мереж може лише зареєстрований користувач соціальних мереж, а в закритих дискусіях – тільки учасник дискусії;

– значна частина відвідувачів потрапляє на сайт за безпосередньою рекомендацією інших користувачів;

– взаємопов’язаність сторінок дискусій;

– збереження дискусій неактуальної тематичної спрямованості.

– анонімність або спотворення даних про себе самими користувачами соціальних мереж.

Враховуючи особливості функціонування віртуальних спільнот у соціальних мережах щодо виявлення інформаційного наповнення та

численність аудиторії, соціальні мережі стають зручним майданчиком для формування віртуальних спільнот деструктивного характеру. Соціальні мережі створюють нові загрози, оскільки держава вже не здатна контролювати їх в повному обсязі [86].

1.3. Аналіз віртуальних спільнот у соціальних мережах як суб'єктів інформаційної безпеки

1.3.1. Властивості віртуальних спільнот у соціальних мережах як суб'єктів інформаційної безпеки

Аналізування процесу функціонування віртуальних спільнот у соціальних мережах показує, що має загальні ознаки суб'єкта інформаційного протиборства (табл. 1.1) [38, 57, 58].

Таблиця 1.1

Аналіз ознак віртуальної спільноти як суб'єкта інформаційного протиборства

№ з/п	Ознаки суб'єктів інформаційного протиборства	Ознаки віртуальної спільноти як суб'єкта інформаційного протиборства
1.	Наявність у суб'єкта в інформаційному просторі власних інтересів.	Тематика інформаційного наповнення сторінок дискусій віртуальної спільноти її поширення серед користувачів соціальної мережі є власним інтересом існування спільноти в інформаційному просторі соціальної мережі.

№ з/п	Ознаки суб’єктів інформаційного протиборства	Ознаки віртуальної спільноти як суб’єкта інформаційного протиборства
2.	Наявність у складі суб'єкта спеціальних сил (структур), функціонально призначених для ведення інформаційного протиборства або уповноважених вести інформаційне протиборство.	Всі зареєстровані учасники віртуальної спільноти мають право генерувати інформаційне наповнення на сторінках дискусій у віртуальній спільноті в соціальній мережі, тобто виконують роль сили, що веде інформаційне протиборство. Модератори та адміністратори сторінок дискусій віртуальної спільноти виступають у ролі спеціальних структур, які стежать за дотриманням правил щодо створення інформаційного наповнення на сторінках дискусій.
3.	Володіння та/або розроблення інформаційної зброї, засобів її доставки і маскування.	Сервіси соціальних мереж використовують як інформаційну зброю, за допомогою якої створюються та функціонують віртуальні спільноти в цих мережах.

№ з/п	Ознаки суб’єктів інформаційного протиборства	Ознаки віртуальної спільноти як суб’єкта інформаційного протиборства
4.	Під контролем суб'єкта перебуває сегмент інформаційного простору, в межах якого він володіє переважним правом встановлювати норми регулювання інформаційно-психологічних відносин (на правах власності, закріплених нормами національного та міжнародного законодавства) або державним суверенітетом (національний сегмент інформаційного простору як частина державної території).	Саме сторінки дискусії є власним сегментом інформаційного простору віртуальної спільноти, в межах якого під час створення інформаційного наповнення зареєстрованими користувачами є певні обмеження на зміст та характер повідомлень. Ці обмеження формують правила. Адміністрування прав доступу до інформаційного наповнення дискусії та контроль за дотриманням правил спілкування у спільноті здійснюють адміністратори та модератори.
5	Існування в офіційній ідеології положень, що допускають участь суб'єкта в інформаційному протиборстві.	Метою створення віртуальних спільнот у соціальних мережах є поширення своїх ідей через інформаційне наповнення сторінок дискусій серед користувачів соціальної мережі.

Визначимо характерні риси віртуальних спільнот у соціальних мережах як суб’єктів інформаційної безпеки [38, 57, 58]:

за метою створення:

– створюються для досягнення визначених цілей із зареєстрованих користувачів соціальних мереж, які підтримують ідеологію інформаційного наповнення сторінок дискусії віртуальної спільноти в соціальній мережі, ці користувачі можуть бути громадянами однієї або групи держав;

за структурою:

– учасниками віртуальної спільноти стають усі охочі, що підтримують ідеологію віртуальної спільноти незалежно від соціальних систем, до яких вони належать в реальному житті;

– спостерігаються ознаки децентралізованої ієрархії (принцип багатокерівництва), учасників спільноти, серед яких окремлюються часткові лідери, що виконують функції модераторів та керівників – адміністраторів спільноти;

– віртуальні спільноти за ідеологією існування можуть брати активну участь у політичній діяльності та впливати на суспільні процеси. Інформаційне наповнення сторінок дискусій віртуальної спільноти може підтримувати національні інтереси держави або групи держав або суперечити, за інформаційним наповненням можуть створювати інформаційну загрозу державі, суспільству;

за проникною та заповнювальною здатністю:

– можуть миттєво збільшувати кількість учасників віртуальної спільноти, використовуючи сторінки лідерів спільноти, політичних партій та інших установ чи інші сервіси соціальної мережі;

– зареєстровані користувачі соціальних мереж можуть бути учасниками різних спільнот та в разі необхідності мобілізувати їх для досягнення своєї мети;

– результат впливу інформаційного наповнення на сторінках дискусій віртуальної спільноти не обмежуються інформаційним простором та можуть бути використані як засоби комунікації, організації масових заворушень, акцій протесту та інших заходів;

за здатністю реорганізації:

– після досягнення визначеної мети існування віртуальної спільноти сторінки дискусії можуть видалити з соціальної мережі адміністратори дискусій;

– у будь-який момент часу можуть створюватися нові дискусії або змінюватися назви та опис дискусій віртуальної спільноти в соціальній мережі;

за вразливістю:

– головна вразливість віртуальних спільнот – ідеологія їх інформаційного наповнення, що об'єднує зареєстрованих користувачів соціальних мереж; якщо не підтримується тематичний напрям інформаційного наповнення дискусій віртуальної спільноти, це призводить до відпливу учасників та руйнування спільноти.

1.3.2. Методи інформаційно-психологічного впливу віртуальних спільнот у соціальних мережах

Сторінки дискусій віртуальних спільнот у соціальних мережах в інтересах інформаційного протиборства можуть використовуватися за такими напрямами:

– як засіб комунікації;

– як засіб для організації мітингів, масових заворушень або акцій протесту;

– для поширення інформації з метою маніпулювання свідомістю.

Яскравим прикладом застосування соціальних мереж як засобів комунікації є події, які сталися під час «Арабської весни». В Ірані в 2009 році «Twitter» став платформою для координації антидержавних демонстрацій. Події 2011 – 2012 рр. в Єгипті показали, что перший етап не координуваля жодна політична організація, акції протесту виникали в соціальних мережах – «Twitter» та «Facebook» їх проводила молодь [11, 85]. Але треба враховувати, що кількість користувачів арабських країн на той час була доволі низькою – в

Єгипті доступ мало 24 % населення, а в Лівії – 6 %. Використання соціальних мереж для комунікації значно прискорило передавання даних та дало змогу забезпечити їх поширення [85].

Засобом для організації заходів протесту стала акція протесту в центрі Києва, а також в інших містах України, яка отримала назву «Євромайдан». Її стартом можна вважати пост відомого блогера Мустафи Найєма, який у «Facebook» закликав вийти на Майдан 21 жовтня 2013 року. Вже через годину після публікації кількість коментарів перевищала 600, а тих хто хотів вийти на Майдан було понад тисячу. Майже всі учасники акції постійно листувалися в соціальних мережах, завантажували фото- і відеофайли, запрошували до акції протесту друзів та знайомих з усієї території України [89].

Іншим прикладом є реакція інтернет – користувачів в 2012 р. на закриття файлообмінника EX.UA. Як акція протестубула запланована в соціальних мережах Dos–атака інтернет – сторінок державних установ та відомств.

З метою маніпулювання свідомістю поширюють інформацію щодо діяльності терористичних організацій, сект, щоб залякувати населення та мобілізувати прихильників до своїх лав, пропагують ідеї, що створюють загрозу державі, суспільству [15]. У Тунісі в 2010 р. соціальні мережі «Facebook» та «Twitter» використовувалися не тільки для координації дій, але і як засіб здобуття міжнародної підтримки для опозиції [134]. В 2011 р. в Сирії головна роль соціальних мереж була пропогандистською, вони стали основним джерелом неправдивої інформації про події, що відбувалися [11]. Яскравим прикладом ведення пропагандистської діяльності є реалізація проекту «Новоросія». Так з травня 2014 р. у «Вконтактах» було створено понад 800 груп що обговорювали відповідну тематику. Необхідно зазначити, що серед зареєстрованих учасників груп були не тільки користувачі соціальних мереж, які вказували своє місце проживання в Донецькій або Луганській областях, а також з інших регіонів України та громадяни Російської Федерації.

Розглядаючи інформаційно-психологічний вплив віртуальних спільнот на національні інтереси держави, суспільства виділяють три етапи формування та інформаційного впливу віртуальних спільнот [86]:

перший етап – створення активного соціального сегмента незадоволеного політичним режимом;

другий етап – інтенсивна інформаційна пропаганда цієї незадоволеності в інформаційному просторі;

третій етап – блокування соціальних груп, які не підтримують ідеологію цього соціального сегмента.

При цьому повинні вирішуватися такі завдання:

– розбудити (підвищити) активність масової свідомості;

– утримати активність (агресивність) на певному рівні, не виходячи за його межі;

– озброїти своїх прихильників аргументацією для бесід з їхніми супротивниками.

Методи для розв’язання цих задач не відрізняються від класичних методів інформаційно-психологічного впливу і починаються з атаки на масову свідомість з використанням класичних методів інформаційних війн [38, 89]:

За цілями:

– методи пропаганди;

– методи контрпропаганди.

Методи пропаганди націлені на те, щоб донести до населення необхідні ідеї, тобто сформувати на певній ділянці інформаційного простору потрібні інформаційні сутності. Відповідно, методи контрпропаганди спрямовані на дискредитацію ворожих ідей, руйнування шкідливих інформаційних сутностей і недопущення їх виникнення надалі.

За характером дії:

– явні методи;

– неявні (приховані) методи.

Явні методи відрізняються від неявних тим, що в них мету і характер впливу не приховують від супротивника.

Серед основних моделей ведення інформаційного противоборства у соціальних мережах варто виділити такі [42]:

- модель мережевих атак;
- модель із залученням користувачів;
- модель тотального блокування.

Модель мережевих атак складна для планування й передбачає створення своєрідної завіси у вигляді оманливих повідомлень чи повідомлень, які провокують конфлікти між учасниками соціальної мережі.

Інша модель полягає у залученні користувачів, які вестимуть запеклі дискусії в обговореннях, писатимуть прихильні коментарі, а також публікуватимуть замітки, повідомлення, які критикуватимуть чи підтримуватимуть певні дії, висвітлюватимуть їх під певним кутом зору.

Третя модель полягає у тотальному блокуванні. Всі популярні соціальні мережі дають змогу блокувати користувачів, дії яких ображають інших користувачів чи заважають їм. Якщо ж користувач публікує неприйнятну для вас інформацію, можна вирішити проблему, заблокувавши його профіль.

Отже, зважаючи на можливості й властивості притаманні віртуальним спільнотам у соціальних мережах, крім виконання функцій підтримки спілкування, обміну думками, отримання інформації їх членами, організації та ведення бізнесу, останнім часом все частіше вони стають об'єктами і засобами зовнішнього інформаційного управління і ареною інформаційного протиборства на різних рівнях. Вони стали ідеальним інструментом впливу на національні інтереси держави, суспільства в інформаційному просторі.

1.4. Аналіз інформаційних загроз віртуальних спільнот у соціальних мережах

Згідно із законодавством України визначення поняття «інформаційна безпека» таке:

«стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації» [46].

Відповідно до нормативно-законодавчих актів держави [29, 35] та нормативно-правових документів провідних країн світу [30, 110, 111, 125, 126, 142, 149] об’єктами інформаційних загроз є:

– особа;

– суспільство;

– держава.

У відповідності [35] до загроз національним інтересам і національній безпеці в інформаційній сфері відносять наступні:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що е власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Основним інструментом, що використовується у віртуальних спільнотах деструктивного характеру, є інформаційно-психологічний вплив, який передбачає цілеспрямоване розроблення та поширення спеціальної актуальної інформації, здатної справляти безпосередній або непрямий вплив на суспільну свідомість, психологію і поведінку населення [84].

Розглядаючи віртуальні спільноти як суб'єкта інформаційної безпеки та основні інструменти, що використовуються у віртуальних спільнотах деструктивного характеру, доцільно виділити основні реальні та потенційні загрози інформаційної безпеки України [29]:

у зовнішньополітичній сфері:

– поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України, та створює негативний імідж України, як ненадійного партнера для міжнародних відносин;

– зовнішні деструктивні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;

у сфері державної безпеки:

– спроби втручання у внутрішні справи держави з використанням соціальних мереж, поширення у національному сегменті кіберпростору культу насильства, жорстокості, етнічної, релігійної та расової нетерпимості;

– поширення негативного інформаційного впливу на свідомість людини і громадянина, здатного змінювати психічний стан, психологічні та фізіологічні характеристики, керувати свободою вибору;

– деструктивні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України;

– використання засобів масової інформації, а також мережі Інтернет для пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками;

у воєнній сфері:

– здійснення негативного інформаційного впливу на населення України з метою дискредитації воєнно-політичного керівництва держави, підбурювання громадян до перешкоджання діяльності військовим частинам (організаціям, установам, підприємствам), погіршення іміджу військової служби;

– здійснення негативного інформаційного впливу на особовий склад військових частин та підрозділів з метою дискредитації та втрати довіри до військового командування, зниження рівня морально-психологічного стану та готовності військовослужбовців до оборони держави;

– інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;

у внутрішньополітичній сфері:

– поширення суб'єктами інформаційної діяльності недостовірної та упередженої інформації для дискредитації органів державної влади, дестабілізації суспільно-політичної ситуації, що значно ускладнює прийняття політичних рішень;

в економічній сфері:

– поширення у світовому інформаційному просторі недостовірної та упередженої інформації, що знижує інвестиційну привабливість України;

у соціальній та гуманітарній сферах:

– руйнування системи суспільних цінностей, негативні зміни їх цільових настанов, шкідливий вплив інформації на психічне та фізичне здоров'я особи;

– поширення в засобах масової інформації невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської і національної гідності, зневажливе ставлення до гуманітарних надбань Українського народу.

Основні загрози у сфері міжнародної інформаційної безпеки [121]:

– використовуються як інформаційна зброя у військово-політичних цілях, для інформаційного впливу з метою порушення територіальної цілісності держави, що загрожує міжнародному миру, безпеці та стабільності;

– у терористичних цілях, для пропаганди тероризму та долучення до терористичної діяльності нових прихильників;

– для втручання у внутрішні справи суверенних держав, порушення громадського порядку, розпалювання міжнаціональної, міжрасової та міжконфесійної ворожнечі, пропаганди расистських і ксенофобських ідей або теорій, що породжують ненависть і дискримінацію, підбурюють до насильства.

Серед основних завдань, що можна вирішити за допомогою віртуальних спільнот у соціальних мережах виділяють такі [16, 84]:

– створення атмосфери бездуховності та аморальності, негативного ставлення до культурної спадщини;

– маніпулювання суспільною свідомістю і політичною орієнтацією соціальних груп населення країни задля створення політичної напруженості та хаосу;

– дестабілізація політичних відносин між партіями, об'єднаннями і рухами з метою розпалювання недовіри, посилення підозрілості, загострення політичної боротьби, провокування конфліктів, репресій проти опозиції, взаємознищення;

– провокування соціальних, політичних, національних та релігійних зіткнень;

– дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління;

– ініціювання страйків, масових заворушень та інших акцій економічного протесту;

– утруднення прийняття органами управління важливих рішень;

– погіршення міжнародного авторитету держави, її співпраці з іншими країнами;

– створення чи посилення опозиційних угруповань чи рухів;

– підрив морального духу населення і, як наслідок, зниження обороноздатності та бойового потенціалу.

1.5. Правила протидії держави інформаційно-психологічному впливу віртуальних спільнот

Досвід інформаційно-психологічного впливу віртуальних спільнот переконливо свідчить про необхідність посиленої уваги з боку держави до діяльності та розвитку «соціальних мереж». Водночас така увага не повинна порушувати права людини, зафіксовані у законодавстві [34, 46].

Можна виділити такі напрями протидії інформаційно-психологічному впливу віртуальних спільнот:

– силові методи – закриття серверів, обмеження трафіку;

– юридично-правові методи – притягнення до кримінальної відповідальності організаторів та учасників віртуальних спільнот;

– інтернет цензура;

– моніторинг віртуальних спільнот та контент аналіз.

Розглянемо переваги та недоліки кожного із методів.

Перші два методи ефективніші в короткостроковій перспективі. Але їх недоліки щодо недопущення правопорушень в інформаційній сфері зумовлені багатьма об’єктивними причинами, які випливають з характерних властивостей віртуальних спільнот як суб’єктів інформаційної безпеки, серед яких насамперед доцільно виділити (пп. 1.3.1 «Властивості віртуальних спільнот у соціальних мережах як суб’єктів інформаційної безпеки»):

– відсутність географічних кордонів та обмежень для миттєвого поширення, збирання, оброблення та використання інформації, внаслідок чого Інтернет з його глобальними комунікаціями залишається поза сферою

правового регулювання законів будь-якої держави, яка завжди має певну обмежену територію, на яку поширюється її суверенітет (поняття юрисдикції або дії нормативно-правового акта у просторі);

– анонімність, яка підриває традиційне застосування юридичної відповідальності за скоєне правопорушення або злочин в інформаційній сфері, що забезпечує високий рівень латентності та низький рівень розкриття правопорушень;

– легкодоступна змінюваність інформації в електронній формі: на відміну від стабільної, документально оформленої інформації, електронна інформація не має форми, сталої у часі та просторі.

Основна особливість і головна небезпека деструктивних віртуальних спільнот пов'язані з тим, що визнати за законом їхню діяльність деструктивною в умовах дії норм свободи слова, друку, віросповідання можливо тільки після реалізації в реальному світі їх учасниками якихось заходів, здійснених під дією інформаційно-психологічного впливу. Тільки тоді дії та події можна співвіднести з нормами чинного законодавства та відповідно кваліфікувати.

Ще одним із проблемних питань щодо неефективності використання силових методів є те, що українські соціальні мережі дуже сильно інтегровані в російський або світовий Інтернет (з десяти найвідвідуваніших сайтів в Україні – лише два українських).

В Україні згідно чинним законодавством [50] цензурі в інтернет просторі підлягає інформація, яка містить елементи дитячої порнографії, законодавчої бази щодо цензури в інших питаннях (інформаційної безпеки держави, суспільства) немає.

Методи моніторингу та контент аналізу віртуальних спільнот є більш ефективним в довгостроковій, але потребує залучення фахівців різних галузей науки. Виходячи з характерних рис віртуальних спільнот (здатності реорганізації) основною задачею моніторингу та контент аналізу віртуальних

спільнот є не їх знищення, які представляють загрозу для інформаційної безпеки Держави, а управління та контроль діяльністю віртуальних спільнот методами інформаційно-психологічного впливу.

1.6. Моніторинг та контент-аналіз віртуальних спільнот у соціальних мережах

Сьогодні вже розроблена велика кількість спеціального програмного забезпечення щодо моніторингу та контент-аналізу інтернет середовища.

Основні функції цих систем такі:

моніторинг:

– забезпечувати автоматизований пошук інформації в інтернет середовищі;

– визначати та змінювати ключові слова для пошуку інформації використовуючи інформаційно-пошукові мови;

контент-аналіз:

– автоматична обробка інформаційних потоків, виявлення фактів та подій;

– візуалізація аналітичних даних у вигляді дайджестів, схем, графіків та інших видів звітів.

Під моніторингом віртуальних спільнот розуміють процес постійного збирання інформації із соціальних мереж з метою подальшого аналізу.

Основним завданням збирання інформації є виявлення сторінок дискусій соціальних мереж, інформаційне наповнення яких спричиняє інформаційну загрозу національній безпеці держави, суспільству.

Так у наукових дослідженнях проведення пошуку розглядається за допомогою глобальних пошукових систем для віртуальних спільнот, побудованих на платформі форумів [70, 82, 83, 93], та розроблення комерційних пошукових систем для розв’язання спеціальних задач [12, 14, 89], що не враховують особливостей функціонування сторінок дискусій

віртуальних спільнот у соціальних мережах (пп. 1.2 «Аналіз соціальних мереж та їх сервісів»).

Одним із напрямів контент-аналізу є Opinion Mining – технологія інтелектуального виявлення «суб'єктивної» інформації (думок, оцінкових суджень у вигляді відгуків з емоційним забарвленням) із текстової інформації, розміщеної в інтернет ресурсах [131, 135]. Системи та технології видобування оцінкових суджень використовують для автоматизованої оцінки (позитивної, негативної, нейтральної) подій з інтернет ресурсів [151].

Розроблені автоматизовані системи класифікації та аналізу інтернет текстів основані, як правило, на співвіднесенні текстового фрагмента з наперед складеними тональними словниками. За сукупністю виявленої емотивної лексики текст оцінюють як позитивний чи негативний. Однак, інформаційне наповнення сторінок дискусій віртуальних спільнот у соціальних мережах генерується безпосередньо користувачами соціальних мереж з його особливостями:

– неусталений порядок слів у реченні;

– велика кількість розмовної та ненормативної лексики з найнесподіванішими контекстуальними значеннями;

– з двозначності і гумор, зрозумілі з аналізу підтекстів і діалогів, але не з фактичного словникового сенсу сказаного, до якого може звернутися автоматизована система.

Отже можна зробити висновок, що сьогодні доволі адекватної та ефективної автоматизованої системи аналізу інтернет-контенту не існує [115].

Іншим суперечливим питанням щодо аналізу віртуальних спільнот є невизначеність оцінки інформаційної загрози віртуальної спільноти.

У дослідженнях [12] показником інформаційної загрози є кількісна динаміка, що характеризується як кількість подій за одиницю часу або кількість повідомлень пов'язаних з їхнім інформаційним наповненням. Це визначення інформаційної загрози підходить для аналізу інформаційних

новинних інтернет ресурсів як оцінка інтенсивності публікацій за відповідною тематикою.

Водночас аналізуючи інформаційні загрози віртуальних спільнот, які утворюються за допомогою соціальних мереж, необхідно враховувати:

– інформаційне наповнення;

– кількість учасників віртуальної спільноти;

– структуру зв’язків між елементами (дискусіями) у віртуальній спільноті.

Методи моніторингу та контент-аналізу інформаційних потоків в мережі інтернет ускладнюються відсутністю типових методик і рішень, неповнотою відповідних технологічних підходів. Сьогодні дослідження з проблем аналізу інформаційних потоків найчастіше є вузькоспеціалізованими [26].

Вибір методів залежить від моделі за допомогою якої представлені віртуальні спільноти. Так в дослідженнях [68, 69, 82, 83, 94] розроблені формальні моделі віртуальних спільнот побудованих на платформі форумів, але вони не враховують взаємозв’язок між дискусіями у віртуальній спільноті та віртуальними спільнотами в соціальних мережах.

Отже моніторинг та аналіз інформаційних загроз віртуальних спільнот в соціальних мережах повинен забезпечувати такі функції:

– забезпечувати пошук відповідно до ключових слів у інформаційному наповненні сторінок дискусії віртуальної спільноти в соціальних мережах;

– аналіз інформаційного наповнення сторінок дискусії віртуальної спільноти з метою формування віртуальних спільнот (деструктивних, конструктивних) відповідно до їх інформаційного наповнення та його спрямованості;

– аналізування інформаційних ризиків відповідно до інформаційного наповнення, структури зв’язків та кількості учасників віртуальної спільноти;

– надавати рекомендації щодо протидії інформаційно-психологічному впливу віртуальної спільноти;

– візуалізацію структури віртуальної спільноти.

Структурно-логічна схема дослідження для розробки методів і засобів виявлення інформаційних загроз віртуальних спільнот в інтернет середовищі соціальних мереж представлена на рис. 1.1.

Рис. 1.1. Структурно-логічна схема дослідження

Висновки до розділу 1

У першому розділі отримано такі результати.

- Здійснено аналіз віртуальних спільнот в інтернет середовищі та особливостей їх організації в соціальних мережах.
- Розглянуто віртуальні спільноти в соціальних мережах та їхні властивості як суб’єктів інформаційної безпеки держави, суспільства, методи інформаційного впливу віртуальних спільнот у соціальних мережах.
- Розглянуто інформаційні загрози держави, суспільства віртуальних спільнот у соціальних мережах як суб’єктів інформаційної безпеки.
- Проаналізовано правила протидії держави інформаційно-психолігчному впливу віртуальних спільнот у соціальних мережах.

Основні результати розділу автором опублікував у роботах [19, 71, 73].

РОЗДІЛ 2. ФОРМУВАННЯ ПОКАЗНИКА ІНФОРМАЦІЙНОЇ ЗАГРОЗИ ВІРТУАЛЬНИХ СПІЛЬНОТ У СОЦІАЛЬНИХ МЕРЕЖАХ

2.1. Побудова моделі інформаційного середовища віртуальної спільноти

Середовище, в якому функціонують віртуальні спільноти в соціальних мережах, відповідає властивостям та функціям інформаційного середовища, а саме [60, 102, 103, 105]:

1. Властивості:

– інформація має властивість фіксуватись на сторінках соціальних мереж і зберігатися незмінно в такому стані довгий час;

– варіативність, проективна та комунікативна спрямованість, яка визначається тим, що інформаційне наповнення формують користувачі соціальних мереж, які мають особисту думку та створюють його з метою обговорення відповідної тематики з іншими користувачами.

2. Функції: інструменти соціальних мереж забезпечують оперативний обмін інформацією між користувачами та її збереження.

Інформаційне середовище віртуальних спільнот складається із:

– зовнішнього інформаційного середовища, а саме середовища, в якому циркулює інформація, що впливає на функціонування віртуальної спільноти, від елементів соціальної мережі (суб’єктів інформаційного впливу);

– внутрішнього інформаційного середовища, а саме середовища, в якому циркулює інформація всередині віртуальної спільноти між її елементами.

Отже, для формування показника інформаційної загрози процесу функціонування віртуальної спільноти необхідно:

– побудувати загальну модель інформаційного середовища, яка характеризує структуру зовнішнього та внутрішнього інформаційного середовища віртуальної спільноти;

– конкретизувати модель внутрішнього інформаційного середовища для відображення структури інформації (інформаційного наповнення) в елементах віртуальної спільноти;

– побудувати модель інформаційного наповнення віртуальної спільноти та її елементів для його аналізу.

2.1.1. Побудова моделі зовнішнього інформаційного середовища віртуальної спільноти

Для побудови моделі зовнішнього інформаційного середовища віртуальної спільноти в соціальній мережі визначимо формальну модель соціальної мережі.

Відповідно до визначення соціальної мережі, як інтернет сервісу, **соціальна мережа (Social networks service)** – це інтернет сервіс, сайт, який дає змогу зареєстрованим на ньому користувачам розміщувати інформацію про себе і комунікувати між собою, встановлюючи соціальні зв'язки. Контент на цьому сервісі створюють безпосередньо самі користувачі [92, 113].

Тоді, формальна модель соціальної мережі має вигляд:

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

де $Members$ – зареєстровані користувачі соціальної мережі;

$Content$ – інформаційне наповнення (контент);

$Link$ – зв’язки між зареєстрованими користувачами соціальної мережі.

Згідно з визначенням віртуальної спільноти, де в**іртуальна спільнота (англ. virtual communities, e-communities)** – новий тип спільнот, які виникають і функціонують в електронному просторі (насмперед у мережі Інтернет) з метою сприяння вирішенню своїх професійних, політичних завдань, задоволення своїх інтересів у мистецтві, дозвіллі тощо [10, 153].

Отже, формальна модель віртуальної спільноти визначатиметься, як і формальна модель соціальної мережі (2.1), інформаційним наповненням та учасниками:

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

де $Content$ – інформаційне наповнення;

$Member$ – множина учасників.

Розглядаючи інструменти соціальних мереж для започаткування обговорень за визначеною тематикою ($Content$), структуру віртуальної спільноти в соціальних мережах доцільно розглядати як сукупність дискусій, що створили за допомогою інструментів соціальних мереж зареєстровані користувачами, які об'єднуються за ознакою мети, ідеологією спілкування та взаємодіють між собою не тільки в межах окремої дискусії, але і з іншими дискусіями віртуальної спільноти та дискусіями інших віртуальних спільнот.

Отже, **зовнішнє інформаційне середовище віртуальної спільноти** – це сукупність віртуальних спільнот (сторінок дискусій соціальної мережі, об'єднаних за ознаками інформаційного наповнення), агентів зовнішнього впливу (сторінки соціальної мережі, які не є сторінками дискусій) та зв'язками між ними [26, 103, 105].

На рис. 2.1 відображено елементи зовнішнього інформаційного середовища віртуальної спільноти в соціальних мережах.

Розглянемо ці елементи:

Агенти зовнішнього впливу (інтернет-ЗМІ, блоги політиків, відомих людей), які функціонують у соціальних мережах та є суб'єктами управління

віртуальної спільноти, щодо їх інформаційного наповнення та формування ідеології віртуальної спільноти. Агенти зовнішнього впливу характеризуватимутися одностороннім зв'язком інформаційно-психологічного впливу на віртуальну спільноту.

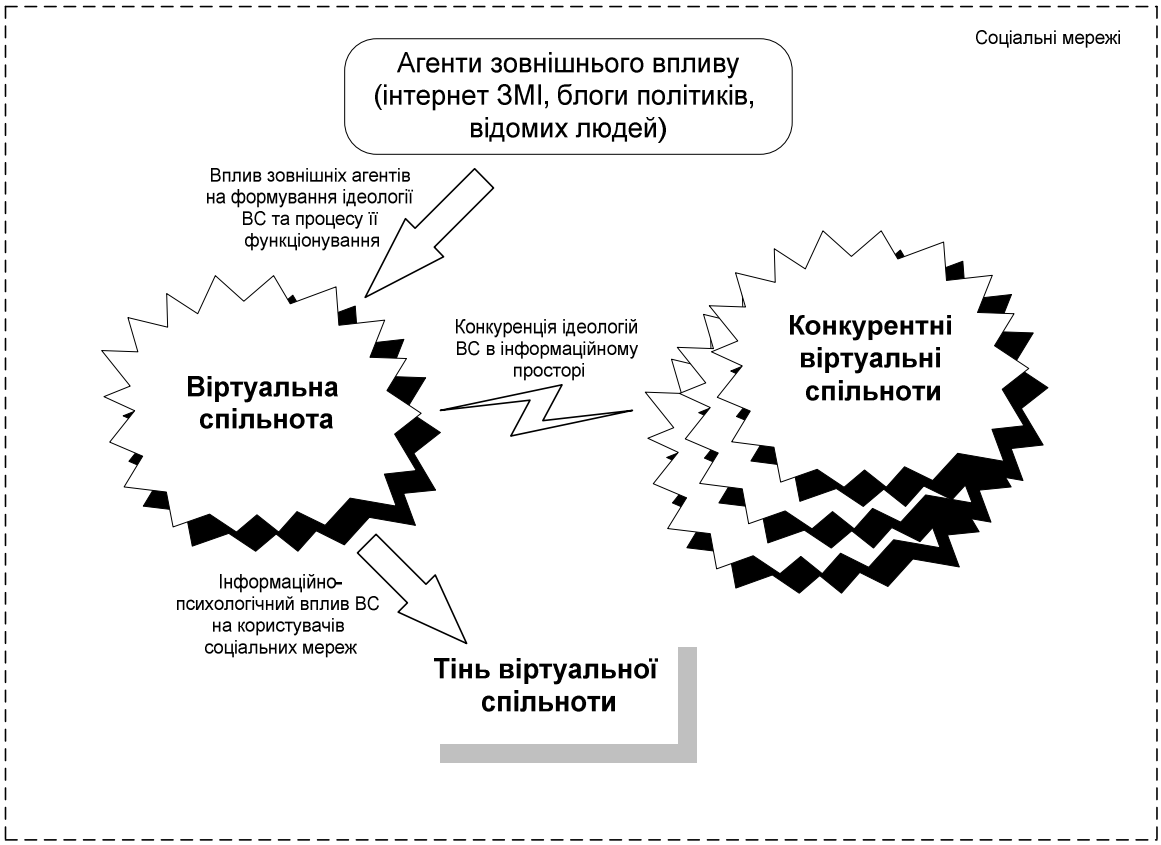

Рис. 2.1. Елементи зовнішнього інформаційного середовища в соціальних мережах

Віртуальні спільноти, які функціонують в інформаційному середовищі соціальних мереж, щоб досягти визначених цілей (деструктивного, конструктивного характеру), характеризуватимуться такими інформаційними зв'язками:

– одностороннім зв'язком з агентами зовнішнього впливу як об'єкт інформаційно-психологічного впливу;

– одностороннім зв'язком з тінню віртуальної спільноти як суб'єкт інформаційно-психологічного впливу;

– двостороннім зв'язком з іншими віртуальними спільнотами з метою конкуренції ідеологій віртуальних спільнот в інформаційному просторі.

Тінь віртуальної спільноти – зареєстровані користувачі соціальних мереж, які не є учасниками дискусій віртуальної спільноти та конкурентних віртуальних спільнот, але цікавляться ідеологією віртуальної спільноти.

Враховуючи визначення зовнішнього інформаційного середовища віртуальної спільноти та елементів, його модель подамо у вигляді:

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

де $VirtualCommunity$ – сукупність віртуальних спільнот в інформаційному середовищі;

$AgentInfl$ – сукупність агентів зовнішнього впливу (інтернет-ЗМІ, блоги політиків, відомих людей);

$LinkExternal(VirtualCommunity)$ – матриця зв'язків між віртуальними спільнотами в інформаційному середовищі;

$LinkExternal(AgentInfl)$ – матриця зв'язків між віртуальними спільнотами та агентами зовнішнього впливу в інформаційному середовищі;

$Shadow(VirtualCommunity)$ – множина зареєстрованих користувачів соціальної мережі, які є тінню віртуальної спільноти.

2.1.2. Побудова моделі внутрішнього інформаційного середовища віртуальної спільноти

Внутрішнє інформаційне середовище віртуальної спільноти – це сукупність дискусій, які створюють зареєстровані учасники соціальної мережі що об'єднуються за ознакою мети та ідеологією існування, а також зв'язками між ними [26, 103, 105].

Варіант структури внутрішнього інформаційного середовища віртуальної спільноти наведено на рис. 2.2.

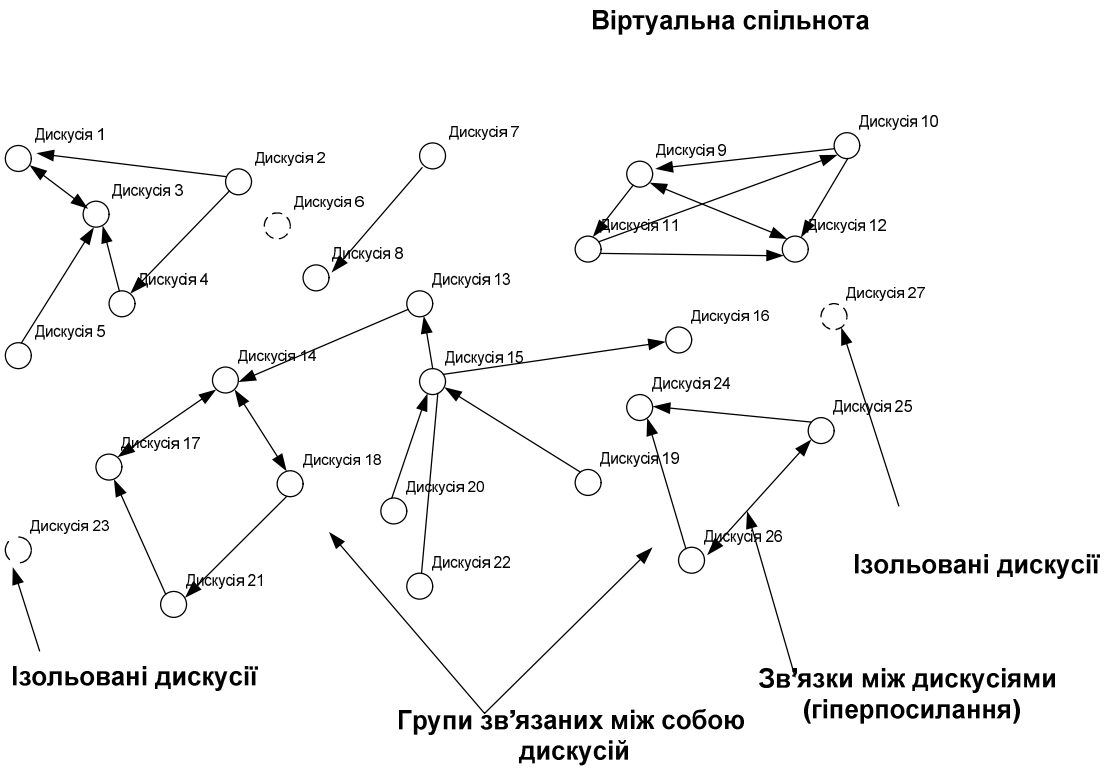

Рис. 2.2. Варіант структури внутрішнього інформаційного середовища віртуальної спільноти

Деталізуємо модель внутрішнього інформаційного середовища віртуальної спільноти відносно моделі віртуальної спільноти (2.2) з урахуванням зовнішнього інформаційного середовища (2.3).

Модель внутрішнього інформаційного середовища віртуальної спільноти має вигляд:

$$InfSpace(VirtualCommunity_i) = \langle Thread(VirtualCommunity_i),\ LinkInternal(Tread),\ Member(VirtualCommunity_i),\ Shadow(VirtualCommunity_i)\rangle, \quad (2.4)$$

де $Thread(VirtualCommunity_i)$ – сукупність дискусій i-ї віртуальної спільноти;

$LinkInternal(Thread)$ – матриця зв'язків між дискусіями i-ї віртуальної спільноти;

$Member(VirtualCommunity_i)$ – множина учасників дискусій *i*-ї віртуальної спільноти, зареєстровані користувачі соціальних мереж;

$$Member(VirtualCommunity_i) = \bigcup_{j=1}^{N_i} Member(Thread_j),$$

де $Member(Thread_j)$ – множина учасників *j*-ї дискусії, зареєстрованих користувачів соціальних мереж;

N_i – кількість дискусій в *i*-й віртуальній спільноті;

$Shadow(VirtualCommunity_i)$ – множина зареєстрованих користувачів соціальних мереж, які зацікавлені ідеологією (тематикою) *i*-ї віртуальної спільноти;

$$Shadow(VirtualCommunity_i) = \bigcup_{j=1}^{N_i} Shadow(Thread_j),$$

де $Shadow(Thread_j)$ – множина зареєстрованих користувачів соціальних мереж, які зацікавлені тематикою *j*-ї дискусії та не є учасниками дискусії;

N_i – кількість дискусій в *i*-й віртуальній спільноті.

При цьому $Member(VirtualCommunity_i) \neq Shadow(VirtualCommunity_i)$.

Отже, (2.3), (2.4) є формальною моделлю структури інформаційного середовища віртуальної спільноти.

2.2. Побудова моделі дискусії віртуальної спільноти

Оскільки інформаційне наповнення дискусій віртуальної спільноти є чинником інформаційної загрози, доцільно глибше дослідити і деталізувати модель дискусії віртуальної спільноти.

Сторінка дискусії має строго структуровану форму (рис. 2.3) та складається з: назви, опису, повідомлень, списку зареєстрованих учасників дискусії та переліку контактів з іншими сторінками соціальної мережі.

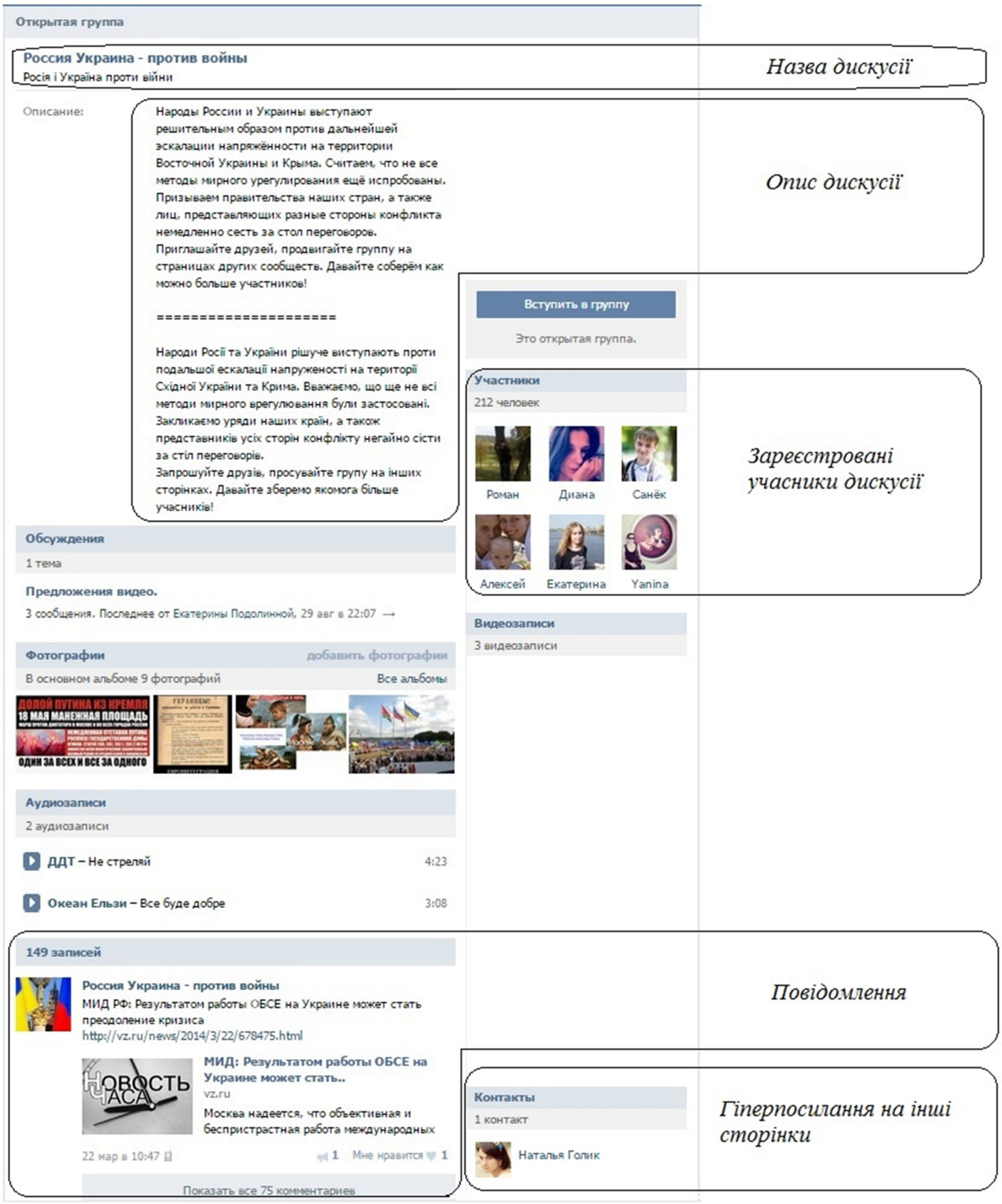

Рис. 2.3. Структура дискусії у соціальних мережах

Повідомлення у дискусіях мають ієрархічну форму. Ієрархічна (деревоподібна) – така структура повідомлень в дискусіях передбачає, що кожний допис є вираженням або відповіддю на відповідне повідомлення в дискусії (рис. 2.4) [70]. Повідомлення створюються послідовно один за одним.

У дискусіях соціальних мереж повідомлення можуть генерувати тільки учасники дискусії, а дописи до них – всі зареєстровані користувачі соціальних мереж.

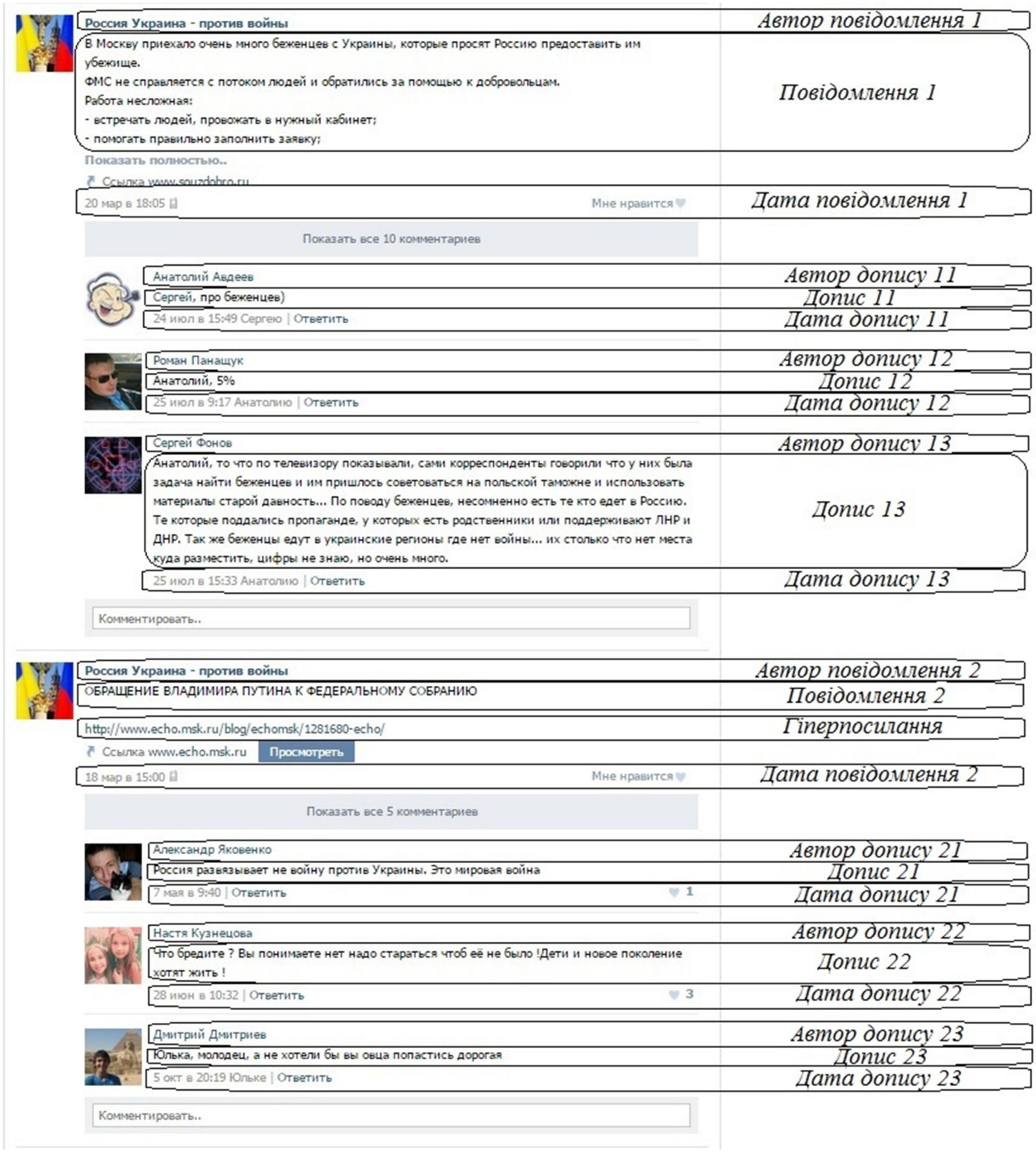

Рис. 2.4. Структура повідомлення дискусії у соціальних мережах

Використовуючи модель дискусії [70, 87, 88], з урахуванням зв'язків між елементами віртуальної спільноти та особливостями побудови сторінок дискусій у соціальних мережах (рис. 2.3, 2.4), подамо її вигляді:

$$Thread_i = \langle ThreadTitle_i, ThreadDescription_i, ThreadMembers_i, Post(Thread_i), Link(Thread_i) \rangle, \quad (2.5)$$

де $ThreadTitle_i$ – назва *i*-ї дискусії;

$ThreadDescription_i$ – опис *i*-ї дискусії;

$ThreadMembers_i$ – множина учасників *i*-ї дискусії;

$Post(Thread_i) = \{Post_{ij}\}_{j=1}^{N^{(PT_i)}}$ – множина повідомлень, що належить до *i*-ї дискусії;

$N^{(PT_i)}$ – кількість повідомлень у дискусії $Thread_i$;

$Link(Thread_i)$ – множина зв'язків у структурі та в інформаційному наповненні *i*-ї дискусії.

Повідомлення – атомарна одиниця інформаційного наповнення дискусії, що складається із тексту, дати створення, автора та дописів до повідомлення:

$$Post_i = \langle PostAuthor_i, PostDate_i, PostText_i, PostReply(Post_i) \rangle, \quad (2.6)$$

де $PostAuthor_i$ – автор *i*-го повідомлення;

$PostDate_i$ – дата *i*-го повідомлення;

$PostText_i$ – текст *i*-го повідомлення;

$PostReply(Post_i) = \{PostReply_{ij}\}_{j=1}^{N^{(PR_i)}}$ – множина дописів до *i*-го повідомлення;

$N^{(PR_i)}$ – кількість дописів до *i*-го повідомлення.

Допис – атомарна одиниця інформаційного наповнення повідомлення, що складається із тексту, дати створення та автора:

$$PostReply_i = \langle PostReplyAuthor_i, PostReplyDate_i, PostReplyText_i \rangle, \quad (2.7)$$

де $PostReplyAuthor_i$ – автор *i*-го допису;

$PostReplyDate_i$ – дата *i*-го допису;

$PostReplyText_i$ – текст *i*-го допису.

Інформаційне наповнення допису характеризує ставлення користувачів до повідомлення. Автором допису може бути і учасник дискусії, і зареєстрований користувач соціальної мережі, якого цікавить інформаційне наповнення дискусії.

Отже, (2.5 – 2.7) є моделлю структури інформаційного наповнення дискусій віртуальної спільноти, з урахуванням зв'язків між елементами віртуальної спільноти.

2.3. Побудова векторно-просторової моделі віртуальної спільноти та дискусії

Проаналізувавши інформаційне наповнення сторінок дискусій, робимо висновок, що основною складовою інформаційного наповнення є текстова інформація (до 80 % обсягу інформаційного наповнення). В зв'язку з цим, для аналізу інформаційного наповнення віртуальної спільноти розроблено векторно-просторову модель віртуальної спільноти, яка ґрунтується на векторній моделі опису даних [107, 146, 147]. У межах цієї моделі дискусія віртуальної спільноти описується вектором у деякому евклідовому просторі, в якому кожному використаному в дискусії терму, увідповіднюється його вага (значущість), яка визначається на підставі статичної інформації про його повторення в окремій дискусії та в дискусіях віртуальної спільноти.

Використаємо формальну модель дискусії (2.5), що складається з назви дискусії, опису дискусії та множини повідомлень, яка належить до дискусії.

Назва дискусії – це множина термів, з яких складається назва дискусії:

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

де $Term_j$ – терм із множини термів у назві *i*-ї дискусії;

$N_i^{(TT)}$ – кількість термів у назві *i*-ї дискусії.

Опис дискусії – це множина термів, з яких складається опис дискусії:

$$ThreadDescription_i^{(Term)} = \{Term_j\}_{j=1}^{N_i^{(TD)}},$$

де $Term_j$ – терм із множини термів у описі *i*-ї дискусії;

$N_i^{(TD)}$ – кількість термів у описі *i*-ї дискусії.

Текст повідомлення – це множина термів, з яких складається текст повідомлення:

$$PostText_{ij}^{(Term)} = \{Term_z\}_{z=1}^{N_{ij}^{(PT)}},$$

де $Term_z$ – терм із множини термів у тексті *j*-го повідомлення *i*-ї дискусії;

$N_{ij}^{(PT)}$ – кількість термів у тексті *j*-го повідомлення *i*-ї дискусії.

Отже, множина термів дискусії складається із множини термів назви дискусії, опису дискусії та текстів повідомлень:

$$Thread_i^{(Term)} = ThreadTitle_i^{(Term)} \bigcup ThreadDiscription_i^{(Term)} \bigcup_{j=1}^{N_i} PostText_{ij}^{(Term)}, \quad (2.8)$$

де $ThreadTitle_i^{(Term)}$ – множина термів, з яких складається тема *i*-ї дискусії;

$ThreadDiscription_i^{(Term)}$ – множина термів, з яких складається опис *i*-ї дискусії;

$PostText_{ij}^{(Term)}$ – множина термів, з яких складається текст *j*-го повідомлення *i*-ї дискусії;

N_i – кількість повідомлень у дискусії.

Множина термів віртуальної спільноти складається із множини термів дискусій (2.8):

$$VirtualCommunity^{(Term)} = \bigcup_{i=1}^{N} Thread_i^{(Term)}, \quad (2.9)$$

де N – кількість дискусій у віртуальній спільноті.

Відповідно до (2.8) векторно-просторова модель дискусії має вигляд:

$$\overline{Thread}^{(Term)} = \langle Term, W \rangle, \tag{2.10}$$

де $Term = \{term_i\}_{i=1}^{N}$ – множина термів дискусії;

$W = \{w_i\}_{i=1}^{N}$ – множина вагових коефіцієнтів термів дискусії;

N – кількість термів у дискусії.

Побудова векторно-просторової моделі дискусії із множини термів дискусії (2.8) поділюється на етапи [96]:

– нормалізація термів (виділення основи термів);

– видалення термів, які не мають смислового навантаження (стоп-слів) та термів, які тільки один раз трапляються у всіх дискусіях;

– побудова частотної матриці використання термів в дискусіях;

– оцінка вагових коефіцієнтів термів.

Для визначення вагових коефіцієнтів термів застосовується *tf***idf* міра оцінки термів як найефективніша для кластеризації інформаційних потоків у мережі Інтернет [44], де *tf* – локальна частота терма (Term Frequency), *idf* – величина, зворотна частоті в усьому потоці документів, що містять цей терм (Inverse Document Frequency).

Для побудови векторів дискусій та розрахунку ваги термів використовують формули [120]:

$$tf = 0{,}5 + 0{,}5 \cdot \frac{TermFrequency(Thread_i)_j}{MaxTermFrequency(Thread_i)}, \tag{2.11}$$

де $TermFrequency(Thread_i)_j$ – частота *j*-го терма в *i*-й дискусії;

$MaxTermFrequency(Thread_i)$ – максимальна частота терма в *i*-й дискусії.

$$idf_{ij} = \log\left(\frac{N}{df^{Term_j}}\right), \tag{2.12}$$

де N – кількість дискусій у віртуальній спільноті;

df^{Term_j} – кількість дискусій віртуальної спільноти в яких трапляється j-й терм.

Отже відповідно до (2.11), (2.12), вагові коефіцієнти j-го терма i-ї дискусії дорівнюють:

$$w_{ij} = tf_{ij} \cdot idf_{ij},$$

де tf_{ij} – локальна частота j-го терма i-ї дискусії;

idf_{ij} – зворотна частота j-го терма i-ї дискусії.

Відповідно до (2.9), векторно-просторова модель віртуальної спільноти має вигляд:

$$\overline{VirtualCommunity}^{(Term)} = \langle Term, W \rangle, \qquad (2.13)$$

де $Term = \{term_i\}_{i=1}^{N}$ – множина термів віртуальної спільноти;

$W = \{w_i\}_{i=1}^{N}$ – множина вагових коефіцієнтів термів віртуальної спільноти;

N – кількість термів у віртуальній спільноті.

Вектор віртуальної спільноти розраховуємо як середній елемент векторного подання дискусій.

2.4. Розрахунок центроїда віртуальної спільноти та дискусій

Центроїд – нормований вектор ключових термів, що характеризує інформаційне наповнення віртуальної спільноти (дискусії) [91].

Для побудови центроїда використовуємо векторно-просторову модель дискусії (2.10) та віртуальної спільноти (2.13).

Нормуємо вектор термів для визначення центроїда віртуальної спільноти:

$$Centroid(VirtualCommunity) = \langle Keyword, W^* \rangle, \qquad (2.14)$$

де $Keyword = \{keyword_i\}_{i=1}^{N}$ – множина ключових термів, що характеризує інформаційне наповнення віртуальної спільноти;

$W_i^* = \{w_i^*\}_{i=1}^N$ – множина вагових коефіцієнтів ключових термів з нормованого вектора вагових коефіцієнтів віртуальної спільноти;

N – кількість ключових термів.

та дискусії:

$$Centroid(Thread) = \langle Keyword, W^* \rangle, \tag{2.15}$$

де $Keyword = \{keyword_i\}_{i=1}^N$ – множина ключових термів дискусії;

$W_i^* = \{w_i^*\}_{i=1}^N$ – множина вагових коефіцієнтів ключових термів з нормованого вектора вагових коефіцієнтів дискусії;

N – кількість ключових термів.

Якщо вважати, що за принципом Парето вісімдесят відсотків загального внеску в формування усього інформаційного наповнення дискусії роблять двадцять відсотків термів, то для визначення ключових термів центроїдів дискусій та віртуальної спільноти вибирають двадцять відсотків термів з найбільшими ваговими коефіцієнтами відповідно з векторно-просторової моделі дискусії (2.10) та віртуальної спільноти (2.13) [54, 65].

2.5. Розрахунок міри відповідності тематичного напряму повідомлень у дискусії

Зважаючи на особливості використовуваної в інформаційному наповненні дискусій віртуальної спільноти мови з її неусталеним порядком слів у реченні, великою кількістю розмовної та ненормативної лексики, з двозначностями і гумором, зрозумілими з аналізу підтекстів і діалогів, повідомлення в інформаційному наповненні дискусій віртуальної спільноти можуть бути оцінені як позитивні чи як негативні [47]. Для цього ввели міру відповідності тематичного напряму повідомлень у дискусії.

Міра відповідності тематичного напряму повідомлень у дискусії – це ознака, яка залежить від позитивного чи негативного напряму повідомлень у дискусії, відповідно до тематичного напряму віртуальної спільноти.

Міру відповідності визначимо як:

$$Sim(Thread_i) = \max\left\{Sim(Thread_i)^{Positive}, Sim(Thread_i)^{Negative}\right\}, \qquad (2.16)$$

де $Sim(Thread_i)^{Positive}$ – міра відповідності позитивних повідомлень в *i*-й дискусії, згідно з тематикою інформаційного наповнення;

$Sim(Thread_i)^{Negative}$ – міра відповідності негативних повідомлень в *i*-й дискусії, згідно з тематикою інформаційного наповнення, що спричиняє інформаційну загрозу.

Міра відповідності позитивних повідомлень в *i*-й дискусії:

$$Sim(Thread_i)^{Positive} = \frac{\sum_{j=1}^{N^{(Thread_i)}} card\left(Post_j^{+}(Thread_i)\right)}{N^{(Thread_i)} - \sum_{j=1}^{N^{(Thread_i)}} card\left(Post_j^{(flood)}(Thread_i)\right)}, \qquad (2.17)$$

де $Post_j^{+}(Thread_i)$ – множина позитивних повідомлень *i*-ї дискусії;

$Post_j^{(flood)}(Thread_i)$ – множина повідомлень *i*-ї дискусії, які не містять ніякої корисної інформації за тематикою віртуальної спільноти;

$N^{(Thread_i)}$ – кількість повідомлень *i*-ї дискусії.

Міра відповідності негативних повідомлень в *i*-й дискусії:

$$Sim(Thread_i)^{Negative} = \frac{\sum_{j=1}^{N^{(Thread_i)}} card\left(Post_j^{-}(Thread_i)\right)}{N^{(Thread_i)} - \sum_{j=1}^{N^{(Thread_i)}} card\left(Post_j^{(flood)}(Thread_i)\right)} \qquad (2.18)$$

де $Post_j^{-}(Thread_i)$ – множина негативних повідомлень *i*-ї дискусії;

$Post_j^{(flood)}(Thread_i)$ – множина повідомлень *i*-ї дискусії, які не містять ніякої корисної інформації відповідно до тематики віртуальної спільноти;

$N^{(Thread_i)}$ – кількість повідомлень *i*-ї дискусії.

У (2.17), (2.18) для визначення міри відповідності тематичного напряму повідомлень у дискусії не враховується вага повідомлень, оскільки за великої кількості повідомлень вона істотно не впливатиме на загальний результат.

Для визначення міри відповідності позитивних чи негативних напрямів повідомлень у дискусії з урахуванням ваги повідомлення використовуємо вираз [53]:

$$Weight\left(Post_j(Thread_i)\right) = \frac{\sum\limits_{w^*_{Centroid(Thread_i)} \in Post_{ij}} w^*_{Centroid(Thread_i)}}{M_{Centroid(Thread_i)}}, \qquad (2.19)$$

де $w^*_{Centroid(Thread_i)}$ – вага ключового терма з центроїда *i*-ї дискусії, яке є в тексті *j*-го повідомлення *i*-ї дискусії;

$M_{Centroid(Thread_i)}$ – кількість ключових термів з центроїда *i*-ї дискусії, які є в *j*-му повідомленні *i*-ї дискусії.

Тоді, використовуючи (2.19), міра відповідності позитивних повідомлень в *i*-й дискусії має вигляд:

$$Sim(Thread_i)^{Positive} = \frac{\sum\limits_{j=1}^{N^{(Thread_i)}} Weight\left(Post_j^+(Thread_i)\right)}{\sum\limits_{j=1}^{N^{(Thread_i)}} Weight\left(Post_j(Thread_i)\right)}, \qquad (2.20)$$

де $Weight\left(Post_j^+(Thread_i)\right)$ – вага позитивних повідомлень *i*-ї дискусії;

$N^{(Thread_i)}$ – кількість повідомлень *i*-ї дискусії.

Та міра відповідності негативних повідомлень в *i*-й дискусії:

$$Sim(Thread_i)^{Negative} = \frac{\sum_{j=1}^{N^{(Thread_i)}} Weight\left(Post_j^{-}(Thread_i)\right)}{\sum_{j=1}^{N^{(Thread_i)}} Weight\left(Post_j(Thread_i)\right)}, \quad (2.21)$$

де $Weight\left(Post_j^{-}(Thread_i)\right)$ – вага негативних повідомлень *i*-ї дискусії;

$N^{(Thread_i)}$ – кількість повідомлень *i*-ї дискусії.

Надалі міри відповідності позитивних та негативних повідомлень використовують для розподілу дискусій у деструктивну та конкурентну віртуальні спільноти.

2.6. Розрахунок матриці зв'язків між дискусіями у віртуальній спільноті

Елементи матриці зв'язків між дискусіями віртуальної спільноти визначаються за умови:

– наявність спільних зареєстрованих учасників у дискусіях віртуальної спільноти.рис. 2.5;

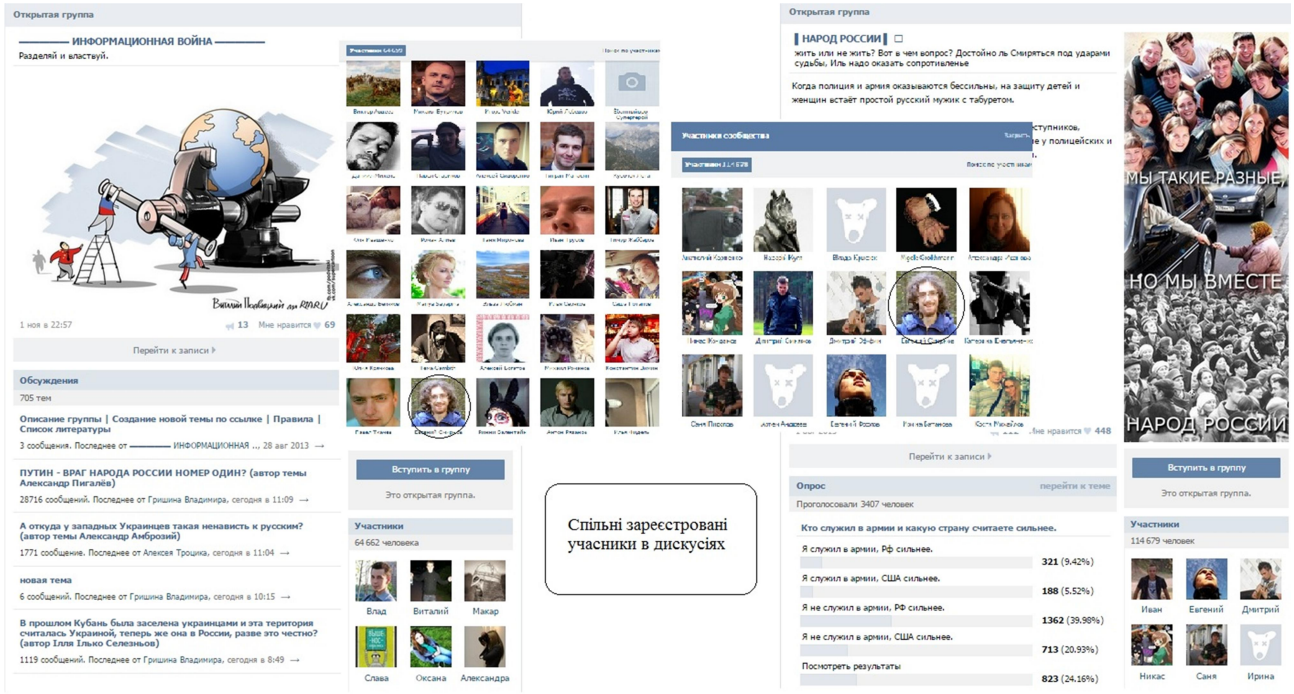

Рис. 2.5. Ознака наявності спільних зареєстрованих учасників у дискусіях

– наявності гіперпосилань у структурі дискусії на сторінки інших дискусій віртуальної спільноти (рис. 2.6);

– наявність гіперпосилань в інформаційному наповненні дискусії на сторінки інших дискусій віртуальної спільноти (рис. 2.7).

Рис. 2.6. Ознака наявності гіперпосилання у структурі дискусії

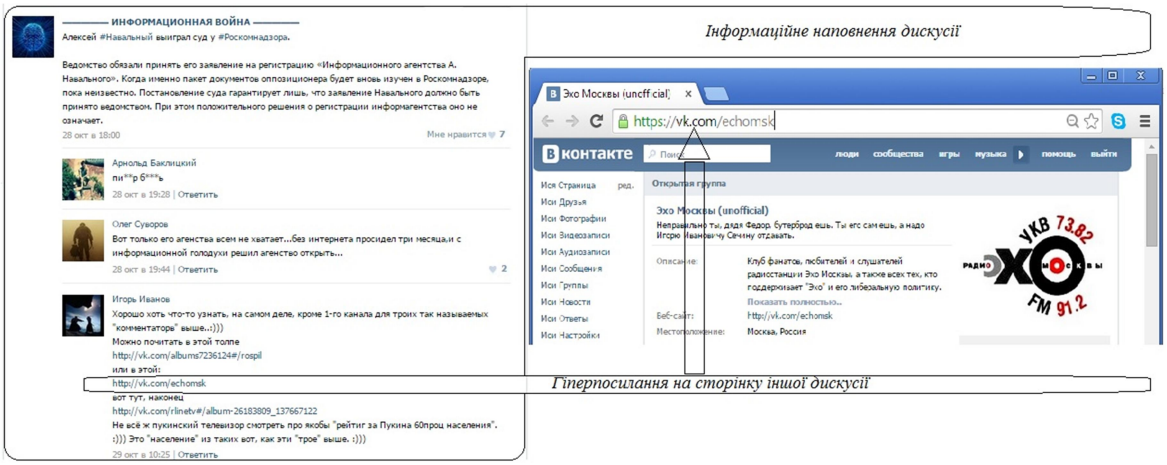

Рис. 2.7. Ознака наявності гіперпосилання в інформаційному наповненні дискусії

Отже, матриця наявності зв'язків між дискусіями у віртуальній спільноті:

$$LinkInternal(Thread) = \left\| link_{ij} \right\|_{n*n}, \quad (2.22)$$

де $link_{ij}$ – ознака наявності зв'язків між i-ю та j-ю дискусією у віртуальній спільноті;

n – кількість дискусій у віртуальній спільноті.

Ознаку наявності гіперпосилань між i-ю та j-ю дискусіями у віртуальній спільноті визначають за формулою:

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

Залежно від спільних зареєстрованих учасників у дискусіях ознака наявності гіперпосилань між i-ю та j-ю дискусією у віртуальній спільноті визначається так:

$$link_{ij} = \begin{cases} 1, якщо\, ThreadMembers_i \cap ThreadMembers_j; \\ 0. \end{cases},$$

де $ThreadMembers_i$ – множина учасників i-ї дискусії.

2.7. Формування показника інформаційної загрози віртуальної спільноти

Відповідно до стандарту інформаційної безпеки NIST 800-30 [140] оцінка ризику визначається як комплексна оцінка двох показників:

- можливості втрат у разі реалізації загрози;
- ймовірності виникнення такої загрози.

Розглядаючи інформаційні загрози для інформаційної безпеки держави в процесі функціонування віртуальних спільнот, основний підхід щодо визначення першого показника реалізується на підставі експертного опитування експертів у сфері інформаційної безпеки, відповідно до нормативно-правових документів, що регламентують інформаційну безпеку держави.

Другий показник залежить від процесу функціонування віртуальної спільноти – показник інформаційної загрози віртуальної спільноти [70].

Показник інформаційної загрози віртуальної спільноти – це кількісна оцінка реалізації інформаційної загрози, яку становить інформаційне наповнення дискусій віртуальної спільноти.

Формуючи показник інформаційної загрози, необхідно враховувати такі складові:

- кількість учасників віртуальної спільноти;
- кількість можливого мобілізаційного ресурсу;
- якість інформаційного наповнення віртуальної спільноти;
- структуру зв'язків дискусій у віртуальній спільноті.

Для визначення показника інформаційної загрози процесу функціонування віртуальної спільноти використовуємо цінність віртуальної спільноти, яка враховує кількість учасників та зв'язки між ними. **Цінність віртуальної спільноти** – це потенційна доступність учасників спільноти, з якими будь-який учасник спільноти може «сконтактуватися» в разі необхідності [7].

Отже, показник інформаційної загрози процесу функціонування віртуальної спільноти в загальному вигляді можна подати так:

$$InfThreat(VirtualCommunity) = \begin{cases} \dfrac{Value(VirtualCommunity)}{Value(VirtualCommunity)^*}, \\ 1, якщо \dfrac{Value(VirtualCommunity)}{Value(VirtualCommunity)^*} > 1 \end{cases}, \quad (2.23)$$

де $Value(VirtualCommunity)$ – цінність віртуальної спільноти;

$Value(VirtualCommunity)^*$ – критична цінність віртуальної спільноти, за якої реалізується інформаційна загроза.

2.7.1. Визначення цінності віртуальної спільноти

Існує декілька підходів до оцінювання цінності мережі [104, 138, 143]. Дослідники критикують ці закони і єдиної думки поки що немає. Один із застосовуваних підходів [17], оснований на законі більш помірнішого зростання цінності мережі порівняно із законом Ципфа.

Використовуючи цей закон, визначимо цінність віртуальної спільноти з урахуванням кількості її учасників:

$$Value(VirtualCommunity) = \sum_{i=1}^{M} card(ThreadMembers_i) \cdot \cdot \ln\left(\sum_{i=1}^{M} card(ThreadMembers_i) \right) - \sum_{i=1}^{M} card(ThreadMembers_i) \quad ,(2.24)$$

де $ThreadMembers_i$ – множина учасників *i*-ї дискусії;

M – кількість дискусій у віртуальній спільноті.

У разі (2.24) визначено максимальну цінність віртуальної спільноти, коли всі дискусії зв’язані між собою та без урахування якості інформаційного наповнення дискусії.

Наступні складові (якість інформаційного наповнення віртуальної спільноти та структура зв’язків дискусій у ній) зменшуватимуть цінність віртуальної спільноти.

Визначемо якість інформаційного наповнення через міру відповідності тематичного напряму повідомлень у дискусії то цінність віртуальної спільноти (2.24) має вигляд:

$$Value(VirtualCommunity) = \sum_{i=1}^{M} \left(Sim(Thread_i) \cdot card(ThreadMembers_i) \right) \cdot \cdot \ln\left(\sum_{i=1}^{M} \left(Sim(Thread_i) \cdot card(ThreadMembers_i) \right) \right) - \quad ,(2.25)$$
$$- \sum_{i=1}^{M} \left(Sim(Thread_i) \cdot card(ThreadMembers_{i)} \right)$$

де $ThreadMembers_i$ – множина учасників *i*-ї дискусії;

$Sim(Thread_i)$ – міра відповідності тематичного напряму *i*-ї дискусії;

M – кількість дискусій у віртуальній спільноті.

Для визначення цінності віртуальної спільноти з урахуванням структури зв'язків дискусій у цій спільноті необхідно розглянути топологію віртуальної спільноти, яка може утворюватися залежно від зв'язків між дискусіями.

Залежно від зв'язків між дискусіями можуть утворюватися такі елементи (рис. 2.2) [118]:

– дискусії, не зв'язані з іншими дискусіями віртуальної спільноти, тобто не мають внутрішніх та зовнішніх гіперпосилань та спільних зареєстрованих учасників між дискусіями віртуальної спільноти;

– сукупність дискусій, які зв'язані між собою гіперпосиланнями або мають спільних зареєстрованих учасників;

– ізольовані сукупності дискусій, не зв'язані з іншими дискусіями віртуальної спільноти.

Отже, залежно від зв'язків між дискусіями утворюємо групи. Група віртуальної спільноти – це сукупність дискусій, взаємозв'язаних між собою та не зв'язаних з іншими дискусіями віртуальної спільноти.

Для утворення груп визначимо правила їх формування:

1. Група не може бути пустою, тобто повинна містити хоча б одну дискусію.

2. У віртуальній спільноті може бути від 1 до *n* груп (*n* – кількість дискусій у віртуальній спільноті), 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.

Згідно з (2.25) визначимо цінність групи віртуальної спільноти:

$$Value(Group_i) = \sum_{j=1}^{M^{(Group_i)}} \left(Sim(Thread_j) \cdot card(ThreadMembers_j)\right) \cdot \ln\left(\sum_{j=1}^{M^{(Group_i)}} \left(Sim(Thread_j) \cdot card(ThreadMembers_j)\right)\right) - \sum_{j=1}^{M^{(Group_i)}} \left(Sim(Thread_j) \cdot card(ThreadMembers_j)\right), \quad (2.26)$$

де $M^{(Group_i)}$ – кількість дискусій в *i*-ій групі.

Для двох ізольованих груп віртуальної спільноти цінність об`єднання цих груп дорівнюватиме сумі цінностей кожної з них, тобто справедливе рівняння [17]:

$$f(m_1 m_2) = f(m_1) + f(m_2),$$

де $f(m_1)$ – цінність *1*-ї групи віртуальної спільноти з m_1 агентами;

$f(m_2)$ – цінність *2*-ї групи віртуальної спільноти з m_2 агентами;

$f(m_1 m_2)$ – цінність об`єднання *1*-ї та *2*-ї груп віртуальної спільноти.

Отже, цінність віртуальної спільноти:

$$Value(VirtualCommunity) = \sum_{i=1}^{N} Value(Group_i), \quad (2.27)$$

де *N* – кількість груп у віртуальній спільноті.

Підставляємо у вираз (2.27) цінність групи віртуальної спільноти (2.26), отримуємо цінність віртуальної спільноти:

$$Value(VirtualCommunity) = \sum_{i=1}^{N} \left(\sum_{j=1}^{M^{(Group_i)}} \left(Sim(Thread_j) \cdot card(ThreadMembers_j)\right) \cdot \ln\left(\sum_{j=1}^{M^{(Group_j)}} \left(Sim(Thread_j) \cdot card(ThreadMembers_j)\right)\right) - \sum_{j=1}^{M^{(Group_j)}} \left(Sim(Thread_j) \cdot card(ThreadMembers_j)\right) \right), \quad (2.28)$$

де N – кількість груп у віртуальній спільноті;

$M^{(Group_i)}$ – кількість дискусій в i-й групі.

Підставляємо (2.28) у вираз (2.23) й отримуємо показник інформаційної загрози віртуальної спільноти з урахуванням кількості учасників віртуальної спільноти, якості інформаційного наповнення віртуальної спільноти та структури зв'язків дискусій у віртуальній спільноті.

Для визначення показника інформаційної загрози з можливим мобілізаційним ресурсом віртуальної спільноти вираз (2.28) подамо у вигляді:

$$Value(VirtualCommunity)^{(Mob)} = \sum_{i=1}^{N}\left(\sum_{j=1}^{M^{(Group_i)}} \left(Sim(Thread_j) \cdot card(ThreadMembers_j) \right) \cdot \right.$$
$$\cdot \ln\left(\sum_{j=1}^{M^{(Group_j)}} \left(Sim(Thread_j) \cdot card(ThreadMembers_j) \right) \right) - \quad ,(2.29)$$
$$\left. - \sum_{j=1}^{M^{(Group_j)}} \left(Sim(Thread_j) \cdot card(ThreadMembers_j) \right) \right) +$$
$$+ card\left(Shadow(VirtualCommunity) \right)$$

де $Shadow(VirtualCommunity)$ – множина зареєстрованих користувачів соціальних мереж, які зацікавлені ідеологією (тематикою) віртуальної спільноти та не є учасниками дискусії.

2.7.2. Підходи щодо визначення критичної цінності віртуальної спільноти

Один із підходів до визначення критичної цінності віртуальної спільноти оснований на тому, що визначають експерти кількість учасників віртуальної спільноти, за якої реалізується i-та інформаційна загроза, без урахування якості інформаційного наповнення віртуальної спільноти, структури зв'язків дискусій у ній.

Одже, згідно з (2.24), критична цінність віртуальної спільноти має вигляд:

$$Value(VirtualCommunity)^* = Members(InfThreat_i) \cdot \ln(Members(InfThreat_i)) - Members(InfThreat_i), \quad (2.30)$$

де $Members(InfThreat_i)$ – критична кількість учасників віртуальної спільноти, що визначили експерти, за якої реалізується *i*-та інформаційна загроза без урахування якості інформаційного наповнення віртуальної спільноти, структури зв'язків дискусій у ній.

Недоліки цього підходу такі:

– не завжди точно можна визначити кількість учасників віртуальної спільноти, за якої реалізується інформаційна загроза;

– не відображає загальної картини щодо інформаційної переваги деструктивної віртуальної спільноти порівняно з до конкурентною віртуальною спільнотою, яка цікавиться цією тематикою.

Перевагою цього підходу є те, що для прийняття рішення щодо протидії інформаційному впливу деструктивної віртуальної спільноти не потрібно враховувати додаткові фактори.

Інший підхід оснований на урахуванні визначення критичної цінності віртуальної спільноти щодо загальної кількості учасників деструктивної та конкурентної віртуальних спільнот, які зацікавлені цією тематикою, з урахуванням якості інформаційного наповнення та структури зв'язків дискусій в цих віртуальних спільнотах.

Отже, критична цінність віртуальної спільноти має вигляд:

$$Value(VirtualCommunity)^* = \sum_{i=1}^{N} Value(VirtualCommunity_i) \quad (2.31)$$

де $Value(VirtualCommunity_i)$ – цінність *i*-ї віртуальної спільноти;

N – кількість віртуальних спільнот, зацікавлених цією тематикою (як правило, деструктивна та конкурентна).

Цінності для деструктивної та конкурентної віртуальних спільнот розраховуємо, використовуючи формулу (2.29).

Недоліки цього підходу такі: в окремих випадках, коли цією тематикою зацікавилась тільки одна деструктивна віртуальна спільнота, до якої входять одна або декілька дискусій, з невеликою кількістю учасників отримуємо максимальне значення показника інформаційної загрози. Отже, приймаючи рішення щодо протидії інформаційному впливу, необхідно враховувати додаткові фактори, а саме:

– загальну кількість учасників віртуальних спільнот, зацікавлених цією тематикою;

– середню інтенсивність публікації повідомлень в інформаційному наповненні дискусій віртуальної спільноти.

Перевагою цього підходу є те, що він відображає повну картину інформаційного протиборства між віртуальними спільнотами (деструктивною та конкурентною), зацікавлених цією тематикою.

Отже, використовуючи (2.23 – 2.31), отримуємо кількісний показник інформаційної загрози віртуальної спільноти.

Відповідно до розрахунку показника інформаційної загрози, його значення лежатиме в межах [0,1], що спрощує подальше прийняття рішення щодо протидії інформаційному впливу процесу функціонування віртуальних спільнот.

Висновки до розділу 2

У другому розділі роботи запропоновано моделі, що є основою для подальших досліджень, спрямованих на розроблення методів виявлення та оцінки інформаційних загроз віртуальних спільнот у соціальних мережах. Зокрема, отримано такі результати:

- Формалізовано структуру інформаційного середовища віртуальних спільнот, в яку входять моделі зовнішнього та внутрішнього інформаційних середовищ віртуальної спільноти.

- Деталізовано модель дискусії віртуальної спільноти з урахуванням структури інформаційного наповнення дискусій та зв’язків між ними, у яку входять модель дискусії, модель повідомлення та модель дописів.
- Розроблено векторно-просторову модель віртуальної спільноти та дискусії.
- Розроблено методи визначення основних характеристик віртуальної спільноти: центроїдів віртуальної спільноти та дискусії, міри відповідності тематичного напряму повідомлень у дискусії та матриці зв’язків між дискусіями у віртуальній спільноті.
- Сформовано кількісний показник інформаційної загрози процесу функціонування віртуальних спільнот з урахуванням таких складових: кількості учасників віртуальної спільноти, обсягу можливого мобілізаційного ресурсу, якості інформаційного наповнення віртуальної спільноти та структури зв’язків дискусій у віртуальній спільноті.

Основні результати розділу опубліковано у роботах автора: [22, 74, 75, 78, 79, 122].

РОЗДІЛ 3. МЕТОДИ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ ВІРТУАЛЬНИХ СПІЛЬНОТ У СОЦІАЛЬНИХ МЕРЕЖАХ ТА ОЦІНКА ЇХ

3.1. Алгоритми пошуку сторінок дискусій у соціальних мережах

Пошук сторінок дискусій здійснюється інструментами соціальних мереж за назвами дискусій або за їх коротким змістом, що не завжди відповідає інформаційному наповненню цих сторінок.

Внаслідок цього виникла проблема, пов'язана з пошуком потрібної інформації на сторінках дискусій у соціальних мережах, яка значно ускладнюється необхідністю проведення пошуку відповідно до тематики інформаційного наповнення та актуальності сторінки дискусії з урахуванням особливостей функціонування сторінок дискусій у соціальних мережах, а саме [70]:

– сторінки мають низький ранг в алгоритмах ранжування сторінок;

– велику кількість веб-сторінок дискусій не ранжують глобальні пошукові системи;

– взаємопозв'язаність веб-сторінок дискусій;

– збереження дискусій неактуальної тематичної спрямованості.

У дослідженнях [40, 114] визначено, що найефективнішим та найзручнішим є здійснення пошуку релевантних спільнот та дискусій у глобальній пошуковій системі Google. Для пошуку веб-сторінок спільнот за допомогою Google використовуємо метод формування формалізованих запитів до пошукових систем для виявлення релеватних веб-сторінок спільнот із застосуванням спеціальних операторів пошукової системи [82, 83, 93, 117].

3.1.1. Структура формалізованого запиту

Запит до глобальної пошукової системи на виявлення релевантних дискусій складається із таких операцій:

– операція локалізації пошукового запиту;

– операція виявлення інформаційного наповнення;

– часові обмеження.

Загальну структуру запиту зображено на рис. 3.1

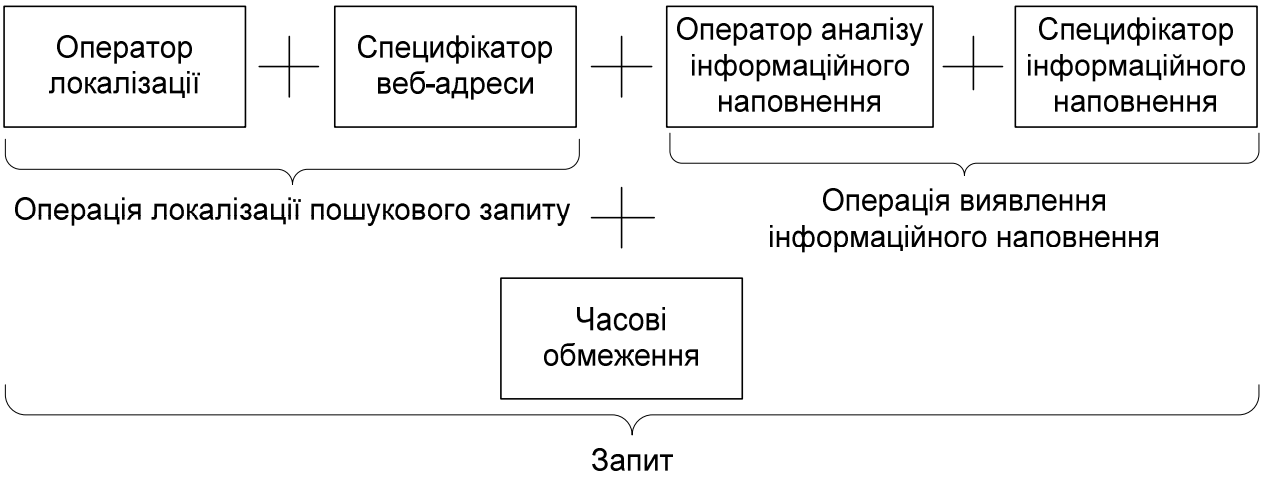

Рис. 3.1. Формалізований запит для виявлення релеватних дискусій веб-сторінок

Операція локалізації пошукового запиту дає змогу обмежити пошук веб-сайтом або доменом. Функціонально ця операція складається з оператора локалізації та специфікатора веб-адреси.

Оператор локалізації – службовий оператор глобальної пошукової системи для обмеження пошуку веб-сайтом або доменом.

Специфікатор веб-адреси – це вказівник на ресурс, на якому здійснюватиметься пошук.

Операція виявлення інформаційного наповнення дає змогу виявити серед веб-сторінок ті, які можуть стосуватися об'єкту пошуку. Ця операція складається з оператора аналізу інформаційного наповнення і специфікатора інформаційного наповнення.

Оператор аналізу інформаційного наповнення – службові оператори глобальної пошукової системи, які аналізують інформаційне наповнення веб-сторінки за заданою тематикою. Інформаційним наповнення сторінки вважатимемо слово або словосполучення, яке міститься у тілі веб-сторінки.

Специфікатор інформаційного наповнення – це ознака, яка характеризує об'єкт пошуку. Ознакою інформаційного наповнення виступає слово або словосполучення у інформаційному наповненні веб-сторінки.

Часові обмеження – під час проведення пошуку необхідне обмеження результатів за визначений діапазон часу, з метою пошуку актуальних веб-сторінок спільнот. Для цього використовуються опції пошуку: за минулий час, за останні 24 години, за минулий тиждень, місяць, рік або інтервал часу, застосовуючи інструменти пошуку.

У зв'язку з особливостями побудови та структури сторінок дискусій у соціальних мережах їх пошук має певні характерні особливості.

3.1.2. Особливості пошуку спільнот та дискусій у «Вконтакті»

Соціальна мережа у «Вконтакті» має багато інструментів для задоволення потреб користувачів. Одним із таких інструментів є створення груп (далі – дискусії), які мають ознаки тематичних дискусій. Отже, для пошуку дискусій спільнот у «Вконтакті» використовуємо формалізований запит (рис. 3.1), поданий на рис. 3.2.

Додатково до формалізованого запиту для виявлення релевантних дискусій у соціальній мережі «Вконтакті» в операції виявлення інформаційного наповнення вводиться специфікатор дискусії «Открытая группа», що дає змогу вести пошук на сторінках дискусій. Пошук здійснюється відповідно до специфікатора інформаційного наповнення (Keywords) – множини ключових слів.

На сторінках дискусій у соціальній мережі у «Вконтакті» можливе створення декількох тематик дискусій. Url-адреси дискусій встановлюємо за

результатами аналізу Html-коду сторінки на наявність ідентифікатора внутрішніх дискусій (рис. 3.3) з визначенням їх адреси.

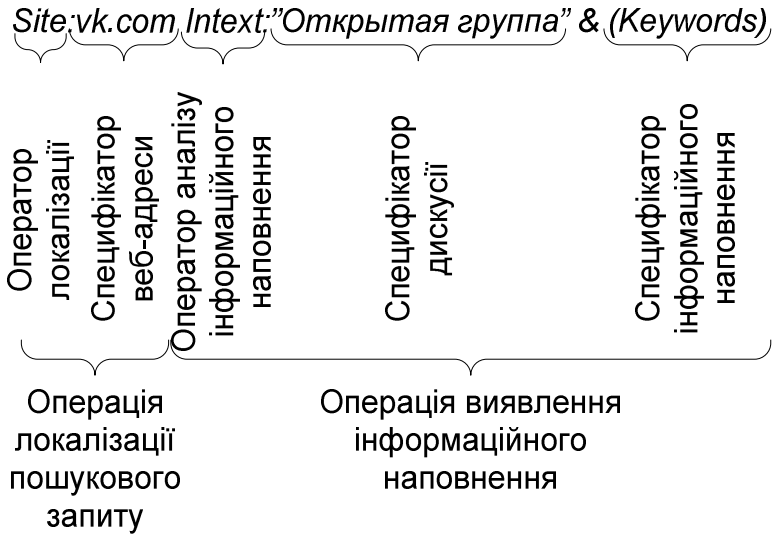

Рис. 3.2. Формалізований запит для виявлення дискусій у соціальній мережі «Вконтакті»

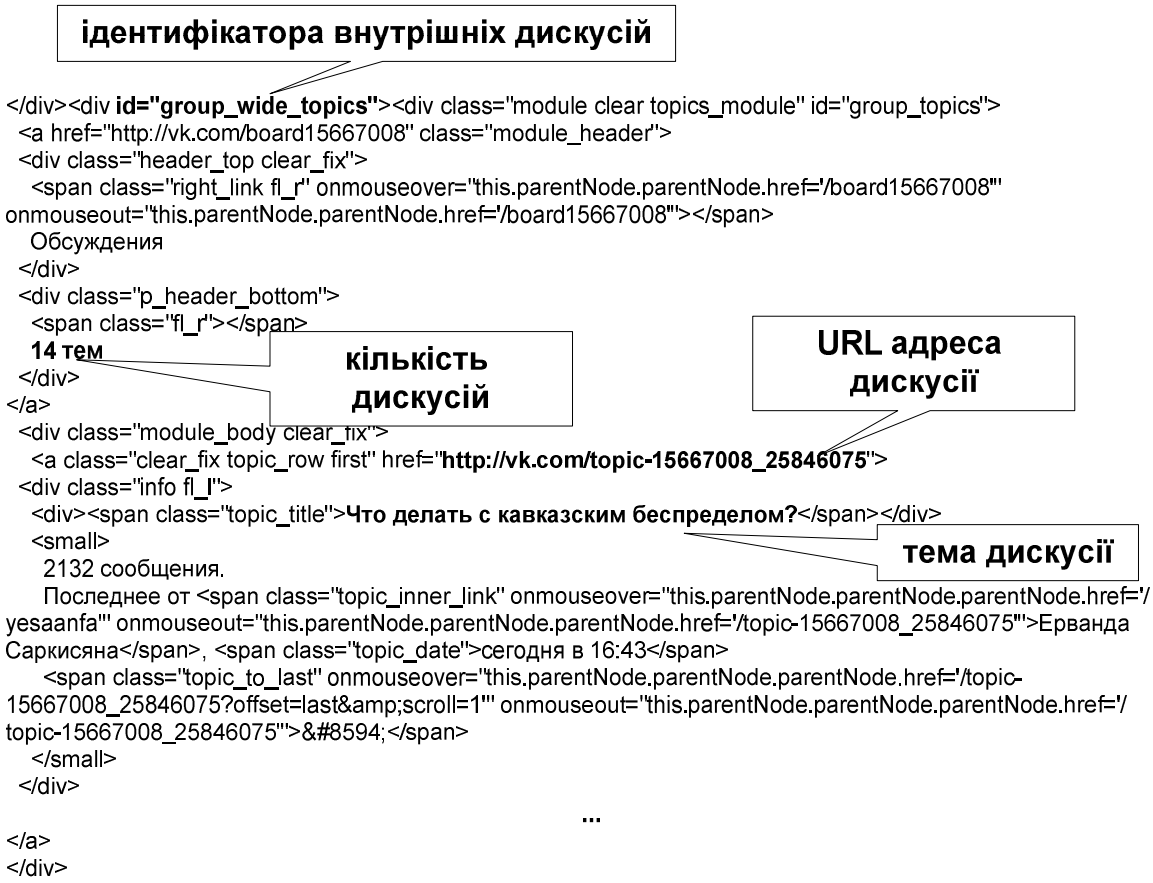

Рис. 3.3. Аналіз Html-коду сторінки дискусії для виявлення Url-адрес внутрішніх дискусій

Результатом пошуку сторінок дискусій у соціальній мережі у «Вконтакті» є адреси сторінок дискусій знайдених, за допомогою формалізованих запитів глобальної пошукової системи, та адреси внутрішніх дискусій. Схематичне зображення алгоритму пошуку відображено на рис. 3.4.

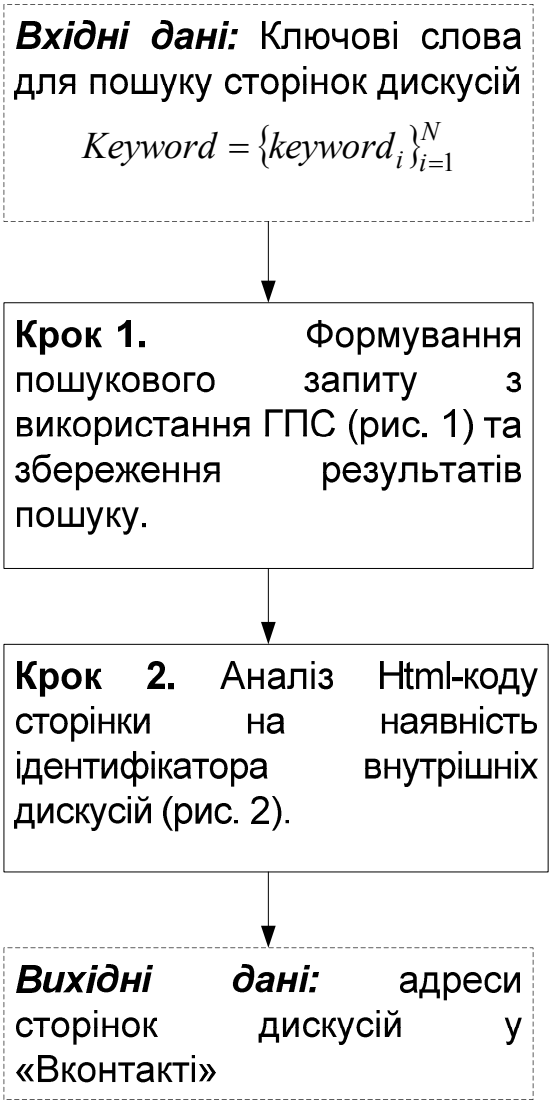

Рис. 3.4. Схематичне зображення алгоритму пошуку дискусій у соціальній мережі «Вконтакті»

3.1.3. Особливості пошуку спільнот та дискусій у «Facebook»

Соціальна мережа «Facebook» надає користувачам змогу створювати свої групи і сторінки спільноти, в яких можна об’єднуватись за інтересами. Група (на далі дискусії) – це спільнота, в якій люди можуть спілкуватися між собою, обмінюватися інформацією та взаємодіяти, але тільки в межах заданої

теми або ідеї, тобто вона має ознаки тематичних дискусій. Однією із основних особливостей дискусій є те, що їх не індексують глобальні пошукові системи. Сторінки переважно сворюють різні організації або окремі особистості як відкриті джерела для всіх, кого хоч якось цікавить тема сторінки, вони, як правило, зв'язані з тематично відповідними дискусіями. На відміну від груп, сторінки індексуються глобальними пошуковими системами.

Отже, пошук дискусій ведемо за допомогою пошуку сторінок у «Facebook», використовуючи формалізований запит (рис. 3.1), наведений на рис. 3.5, з подальшим аналізом Html-коду сторінки.

Рис. 3.5. Формалізований запит для виявлення сторінок у соціальній мережі «Facebook»

Як і під час пошуку в соціальній мережі «Вконтакті», до формалізованого запиту для виявлення сторінок у соціальний мережі «Facebook» в операції пошуку інформаційного наповнення вводиться специфікатор сторінки «сообщество». Пошук здійснюється відповідно до специфікатора інформаційного наповнення (Keywords) – множини ключових слів.

Сторінки в «Facebook» строго структуровані й для визначення наявності зв’язаних дискусій аналізуємо Html-код на наявність пункту меню «группы» (рис. 3.6).

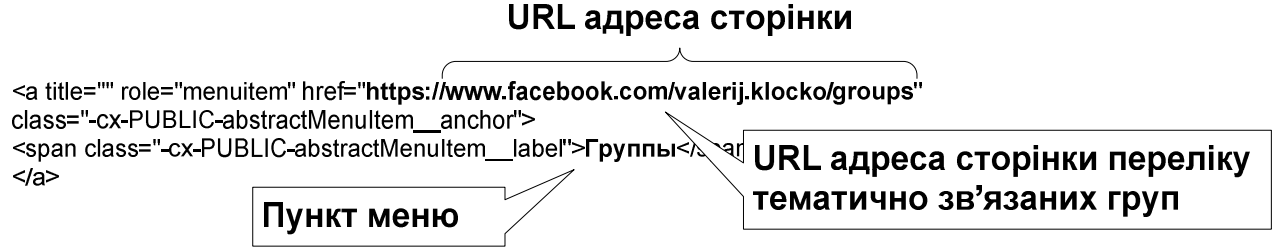

Рис. 3.6. Аналіз Html-коду сторінки для виявлення URL-адреси сторінки переліку тематично зв’язаних груп

Визначаємо частини URL-адреси дискусій, аналізуючи Html-код сторінки переліку тематично зв’язаних дискусій (рис. 3.7).

Рис. 3.7. Аналіз Html-коду сторінки переліку тематично зв’язаних дискусій для виявлення частини URL-адреси дискусій

За результатами виявлених частин URL-адреси формуємо URL-адресу тематично зв’язаних груп. Приклад формування URL-адреси тематично зв’язаних груп наведено в табл. 3.1.

Таблиця 3.1

Формування URL-адреси тематично зв’язаних груп

Адреса сторінки	Частина адреси тематично зв’язаної групи	Адреса тематично зв’язаної групи
www.facebook.com/valerij.klock	/groups/667402756609/	www.facebook.com/groups/667402756609/
www.facebook.com/valerij.klock	/groups/Ivan.SOS/	www.facebook.com/groups/Ivan.SOS/
www.facebook.com/valerij.klock	/groups/180978166552/	www.facebook.com/groups/180978166552/

Схематичне зображення алгоритму пошуку відображено на рис. 3.8.

Рис. 3.8. Схематичне зображення алгоритму пошуку дискусій у соціальній мережі «Facebook»

Проведено експерименти з використанням методу пошуку сторінок дискусій із застосуванням формалізованих запитів глобальної пошукової системи Google та аналізу Html-коду сторінок дискусій у соціальних мережах з різною кількістю ключових слів (Keywords) від 3 до 6, оцінено релевантність пошуку яка становить для «Facebook» 0,6 – 0,8 та «Вконтакті» 0,7 – 0,9. Оцінку виконано за:

$$Relevation = \frac{N_{Keywords \subset D}}{N}$$

де $N_{Keywords \subset D}$ – кількість дискусій в інформаційному наповненні, в яких наявні ключові слова формалізованого запиту;

N – загальна кількість знайдених дискусій.

Отже, запропоновані алгоритми (рис. 3.4, 3.8), які використовують формалізовані запити глобальної пошукової системи Google та аналізу Html-коду сторінок дискусій у соціальних мережах уможливлюють їх пошук відповідно до їх інформаційного наповнення.

3.1.4. Глибинний пошук

Необхідність проведення глибинного пошуку зумовлена причинами як технічного, так і організаційного характеру, а саме: велика кількість сторінок дискусій у соціальних мережах не індексується глобальними пошуковими системами, є певні особливості функціонування сторінок дискусій у соціальних мережах, тобто взаємопов’язаність сторінок дискусій.

Глибинний пошук реалізовується за допомогою розроблення пошукового робота, вхідними даними якого є аналіз списку контактів у структурі сторінки дискусії та гіперпосилань в інформаційному наповненні дискусій, які знайдені за допомогою глобальної пошукової системи Google з використанням запитів API-методів соціальних мереж [62, 99, 119].

Функціонування пошукового робота розподіляється на два блоки:

– визначення id (унікальних ідентифікаторів) сторінок дискусій знайдених глобальною пошуковою системою Google за допомогою запитів API-методів соціальних мереж;

– аналіз списку контактів у структурі сторінки дискусії (рис. 2.6) та гіперпосилань в інформаційному наповненні дискусій (рис. 2.7) за допомогою запитів API-методів соціальних мереж.

Структурна схема фукціонування пошукового робота зображена на рис. 3.9.

Блок 1

Оскільки у разі пошуку сторінок дискусій глобальною пошуковою системою Google отримуємо коротку адресу, яку може змінити адміністратор дискусій, формуємо запит API-методами соціальних мереж для визначення унікального коду дискусії. Унікальний код дискусії – це унікальний ідентифікатор дискусії, який присвоюється під час створення дискусії та не може бути змінений. Перехід до сторінки дискусії може здійснюватися як за короткою адресою дискусії, так і з використанням унікального коду дискусії.

Блок 2

Для аналізу структури дискусії на наявність гіперпосилань використовуємо запит API-методами соціальних мереж, у результаті якого отримуємо унікальний код сторінки та тип сторінки. За типом сторінки здійснюємо розподіл на дискусії та агенти зовнішнього впливу.

Для аналізу інформаційного наповнення завантажуємо сторінку дискусії та проводимо аналіз щодо наявності гіперпосилань у повідомленнях дискусії. Знайшовши гіперпосилання, використовуємо запит API-методами соціальних мереж, у результаті чого отримуємо унікальний код сторінки та тип сторінки. За типом сторінки проводимо розподіл на дискусії та агенти зовнішнього впливу.

Після кожного циклу обробки дискусії уточнюється послідованість обходу дискусій з урахуванням знайдених дискусій.

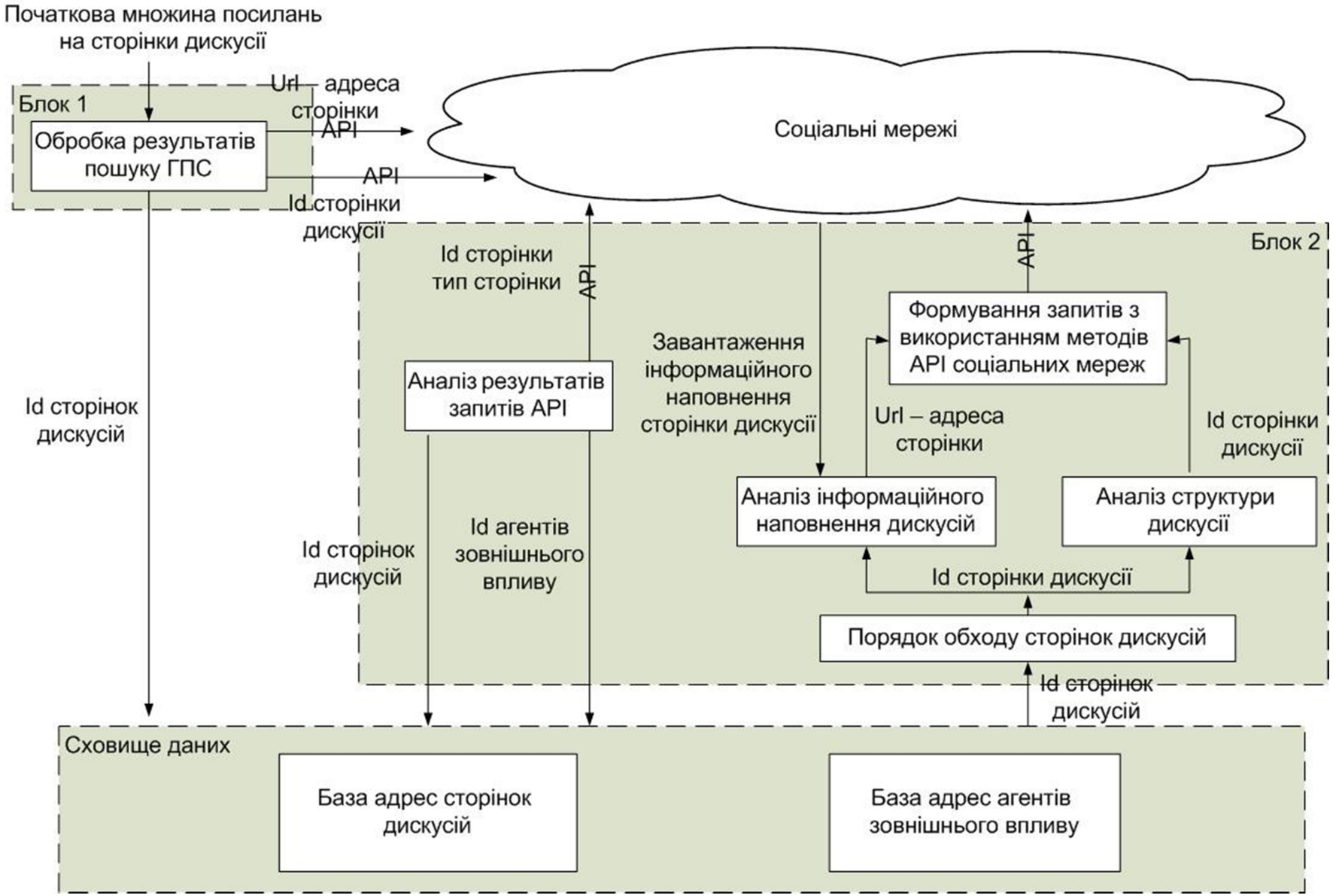

Рис. 3.9. Структурна схема функціонування пошукового робота

Результатами роботи глибинного пошуку є уточнення переліку дискусій, які пов’язані з відповідною тематикою, та формування переліку агентів зовнішнього впливу.

3.2. Формування інформаційного середовища віртуальної спільноти

3.2.1. Кластеризація результатів пошуку

Оскільки під час глибинного пошуку можуть бути знайдені дискусії, які не відповідають тематичному напряму віртуальної спільноти, виникла необхідність в об’єднанні дискусій за ознакою мети та ідеології існування.

Для кластеризації результатів пошуку використаємо векторно-просторову модель дискусії та віртуальної спільноти (2.10), (2.13).

Дискусії обробляються послідовно згідно з підходом Солтона [54, 128].

1. Першій дискусії увідповіднюється 1 кластер, який характеризується центроїдом першої дискусії (2.15).

2. Наступну дискусію порівнюємо з центроїдами наявних кластерів (для цього вводиться міра, яка визначає ступінь близькості). Існують різні варіації мір, що ґрунтуються на векторному поданні документів [109, 139, 141]. Найпоширеніша міра схожості документів, що формулюється як косинус кута між векторами, що представляють документи [43, 112]:

$$\cos\theta = \frac{Centroid(Claster_i) \cdot Centroid(Thread_j)}{\left\|Centroid(Claster_i)\right\| \left\|Centroid(Thread_j)\right\|} \qquad (3.1)$$

де $Centroid(Claster_i)$ – вектор термів центроїда *i*-го кластера;

$Centroid(Thread_j)$ – вектор термів центроїда *j*-ї дискусії;

$Centroid(Claster_i) \cdot Centroid(Thread_j)$ – скалярний добуток центроїдів *i*-го кластера та *j*-ї дискусії;

$\|Centroid(Claster_i)\|$ та $\|Centroid(Thread_j)\|$ – норма центроїдів *i*-го кластера та *j*-ї дискусії.

Визначається порогове значення $\cos\theta$ (3.1). У дослідженні [45] визначено, що для кластеризації інформаційних потоків у мережі Інтернет оптимальне порогове значення вибирають у діапазоні [0,2, 0,3].

3. Дискусії, для яких міра схожості відповідає пороговому значенню, входять у цей кластер. Після цього перераховують центроїд кластера відповідно до пп. 2.4 «Розрахунок центроїда віртуальної спільноти та дискусій», використовуючи векторно-просторові моделі дискусій (2.10), які входять у цей кластер.

4. В іншому випадку створюється новий кластер, для якого визначається його центроїд згідно з кроком 1.

5. Переходять до кроку 2, поки не розглянуті всі дискусії.

В результаті роботи алгоритму кожен кластер містить дискусії, які об'єднуються за ознакою мети та ідеології існування.

3.2.2. Розподіл кластерів дискусій на віртуальні спільноти

За результатами кластеризації дискусії кожного кластера розподіляються на деструктивну та конкурентну віртуальні спільноти.

Розподіл проводять, використовуючи значення позитивних (2.17), (2.20) та негативних (2.18), (2.21) напрямів повідомлень в дискусіях. Дискусія для якої:

$$Sim(Thread_i)^{Negative} \geq Sim(Thread_i)^{Positive},$$

належитиме до деструктивної віртуальної спільноти, в іншому випадку дискусія входить у конкурентну віртуальну спільноту.

Для кожної отриманої віртуальної спільноти розраховуємо її векторно-просторову модель (2.13) та центроїд (2.14) віртуальної спільноти.

Схематичне зображення алгоритму формування інформаційного середовища віртуальної спільноти відображено на рис. 3.10.

Рис. 3.10. Схематичне зображення алгоритму формування інформаційного середовища віртуальної спільноти

3.3. Метод прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот

3.3.1. Формування моделі загроз

Для прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот у соціальних мережах необхідні вивчення та систематизація інформаційних загроз віртуальних спільнот [31, 32, 33]. Для цього формуємо модель загроз (зразок моделі загроз – табл. 3.2), яка складається з:

– об’єкта загрози;

– сфери застосування загрози;

– переліку загроз;

– оцінки ризиків загрози.

Таблиця 3.2.

Модель загроз

Об’єкт	Сфера	Перелік загроз		Оцінка ризиків загроз
		Загрози	Тематика ІН	
1. Держава	1.1. Зовнішньо-політична	1.1.1. Поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України	…	…
			…	…
		1.1.2. Зовнішні деструктивні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет	…	…
			…	…
		1.1.3 …	…	…
	1.2. Державна безпека	1.2.1. Деструктивні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України	…	…
		1.2.2 …	…	…
	1.3 …	1.3.1 …	…	…

Об’єкт	Сфера	Перелік загроз		Оцінка ризиків загроз
		Загрози	Тематика ІН	
2. Суспільство	2.1. Соціальна та гуманітарна	2.1.1. Поширення в засобах масової інформації невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської і національної гідності, зневажливе ставлення до гуманітарних надбань Українського народу	…	…
	2.2 …	2.2.1 …	…	…

Об’єкт, сферу застосування та перелік загроз визначають відповідно до нормативно-правових документів з інформаційної безпеки держави. Загрози процесу функціонування віртуальних спільнот детальніше проаналізовано в пп. 1.4 «Аналіз інформаційних загроз віртуальних спільнот у соціальних мережах ».

Перелік загроз, крім того, розподіляється на відповідні тематики щодо інформаційного наповнення віртуальних спільнот.

Оцінка ризиків, на відміну від технічних систем, визначається не як ймовірність виникнення загрози, а як критична кількість учасників віртуальної спільноти, за якої реалізується ця загроза.

Вихідними даними для експертного визначення інформаційної загрози, яку становить інформаційне наповнення віртуальної спільноти, з моделі загроз є:

– перегляд інформаційного наповнення дискусій віртуальної спільноти;

– оцінювання ключових слів, отриманих центроїдів віртуальних спільнот;

– використання алгоритмів автоматичного реферування [95, 154].

3.3.2. Визначення ступеня інформаційної загрози віртуальної спільноти в соціальних мережах

Для визначення ступеня інформаційної загрози використовуємо показники інформаційної загрози віртуальної спільноти, які розрахуємо відповідно до виразу (2.23) за підходами щодо визначення критичної цінності віртуальної спільноти, розглянутими в пп. 2.7.2 «Підходи щодо визначення критичної цінності віртуальної спільноти», а саме:

– $InfThreat_{CritMembers}(VirtualCommunity)$ – показник інформаційної загрози, для якого визначення критичної цінності віртуальної спільноти основане на встановленні експертами кількості учасників віртуальної спільноти, за якої реалізовується інформаційна загроза, без урахування якості інформаційного наповнення віртуальної спільноти, структури зв'язків дискусій у віртуальній спільноті, а саме – умови виникнення загрози з моделі загроз; розраховується показник відповідно до виразу (2.30);

– $InfThreat_{InfConfr}(VirtualCommunity)$ – показник інформаційної загрози, для якого визначення критичної цінності віртуальної спільноти основане, на загальній кількості учасників деструктивної та конкурентної віртуальних спільнот, які зацікавлені цією тематикою з урахуванням якості інформаційного наповнення та структури зв'язків дискусій у цих віртуальних спільнотах (2.31).

Для визначення рекомендацій щодо прийняття рішення з протидії інформаційним загрозам віртуальних спільнот розглянемо графіки змін показників інформаційної загрози залежно від кількості учасників деструктивної та конкурентної віртуальних спільнот.

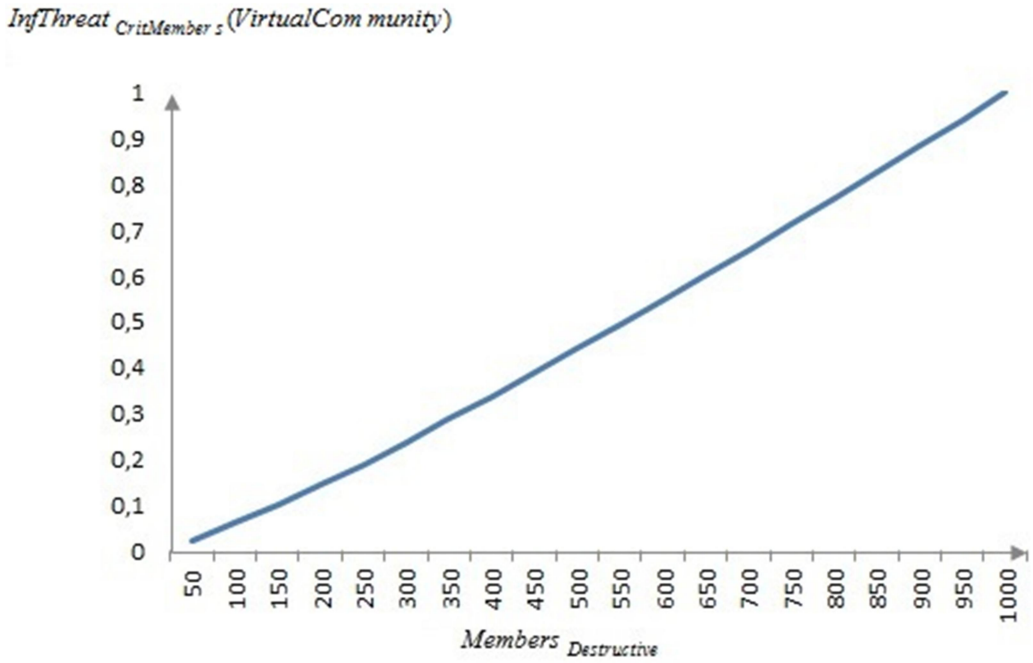

Рис. 3.11. Зміна $InfThreat_{CritMembers}(VirtualCommunity)$ залежно від кількості учасників деструктивної віртуальної спільноти

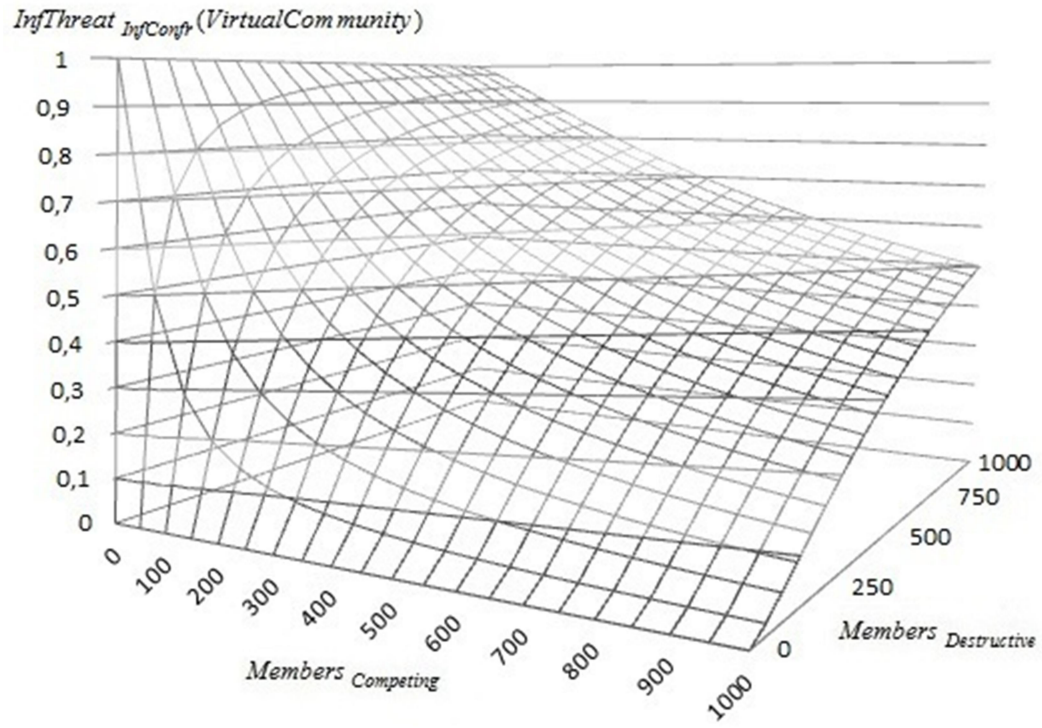

Рис. 3.12. Зміна $InfThreat_{InfConfr}(VirtualCommunity)$ залежно від кількості учасників деструктивної та конкурентної віртуальних спільнот

На рис. 3.11 видно, що в разі збільшенні кількості учасників деструктивної віртуальної спільноти збільшується показник $InfThreat_{CritMembers}(VirtualCommunity)$.

Якщо відсутня конкурентна віртуальна спільнота (рис. 3.12), то за малої кількості учасників деструктивної віртуальної спільноти $InfThreat_{InfConfr}(VirtualCommunity) = 1$, що необхідно врахувати, приймаючи рішення щодо протидії інформаційним загрозам віртуальних спільнот.

Таким чином, ступень інформаційної загрози залежить від $InfThreat_{CritMembers}(VirtualCommunity)$ та $InfThreat_{InfConfr}(VirtualCommunity)$:

$$InfThreat = 1 - f(InfThreat_{CritMembers}(VirtualCommunity), InfThreat_{InfConfr}(VirtualCommunity))$$

Враховуючи, що показники $InfThreat_{CritMembers}(VirtualCommunity)$ та $InfThreat_{InfConfr}(VirtualCommunity)$ мають значення в межах [0, 1] тобто не потребують нормування, мають однакову важність використовуючи метод адитивного згортання критеріїв [6, 13] ступень інформаційної загрози з урахуванням цих показників визначемо за виразом:

$$InfThreat = 1 - (InfThreat_{InfConfr}(VirtualCommunity) + InfThreat_{CritMembers}(VirtualCommunity)), \quad (3.2)$$

Враховуючи визначення ступеня інформаційної загрози (3.2) він буде приймати значення в межах [1,-1]. Зміни значення ступеня інформаційної загрози віртуальної спільноти в залежності від кількості учасників деструктивної та конкуруючої віртуальної спільноти зображено на рис. 3.13.

При значенні $InfThreat \le 0$ приймається рішення щодо протидії інформаційним загрозам віртуальної спільноти.

Схематичне зображення методу прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот відображено на рис. 3.14

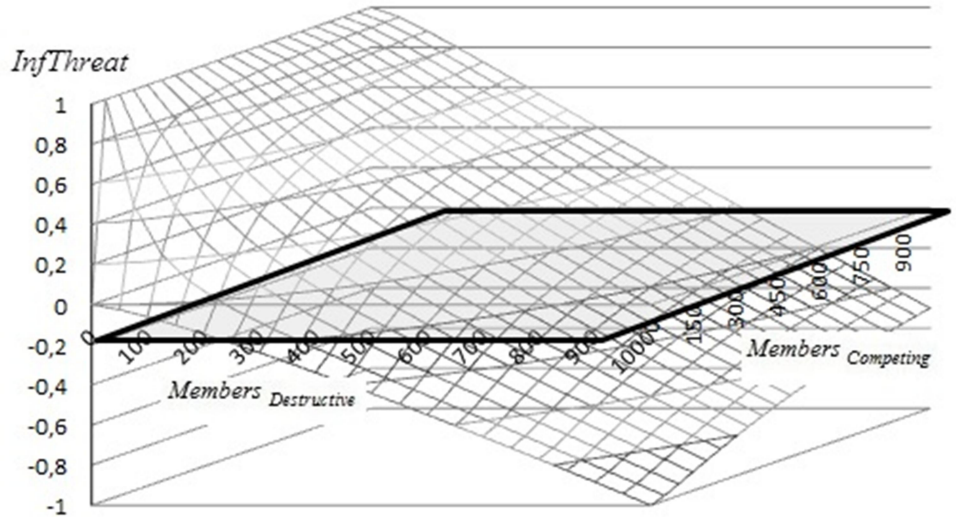

Рис. 3.13. Зміна *InfThreat* залежно від кількості учасників деструктивної та конкурентної віртуальних спільнот

Рис. 3.14. Схематичне зображення методу прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот

Більш детально з урахуванням значенням показників $InfThreat_{CritMembers}(VirtualCommunity)$ та $InfThreat_{InfConfr}(VirtualCommunity)$ рішення щодо протидії інформаційним загрозам віртуальної спільноти, наведені у табл. 3.3.

Таблиця 3.3

Значення показників інформаційної загрози

Значення *InfThreat*	Опис	Результат
$InfThreat \le 0$	Деструктивна віртуальна спільнота має достатню кількість учасників для реалізації інформаційної загрози та перевагу в інформаційному протиборстві з конкурентною віртуальною спільнотою.	Необхідно протидіяти інформаційній загрозі.
	Значення показника $InfThreat_{InfConfr}(VirtualCommunity) \to 1$ свідчить про відсутність конкурентної віртуальної спільноти щодо тематики інформаційного наповнення деструктивної віртуальної спільноти.	Необхідно здійснювати вплив на інформаційне наповнення деструктивної віртуальної спільноти та проводити заходи щодо створення конкурентної.
	Якщо значення показника $InfThreat_{InfConfr}(VirtualCommunity) \to 0$ це вказує на відсутність деструктивної віртуальної спільноти.	Ведення постійного моніторингу.
$InfThreat \approx 0$	$InfThreat_{CritMembers}(VirtualCommunity) \to 1$ та $InfThreat_{InfConfr}(VirtualCommunity) \to 1$ кількість учасників деструктивної віртуальної спільноти достатня для реалізації інформаційної загрози та спільнота має рівну перевагу в інформаційному протиборстві.	Необхідно протидіяти інформаційній загрозі.

Значення *InfThreat*	Опис	Результат
$InfThreat > 0$	Кількість учасників деструктивної віртуальної спільноти не достатня для реалізації інформаційної загрози, але спільнота має значну перевагу в інформаційному протиборстві з конкурентною віртуальної спільнотою.	Ведення постійного моніторингу щодо збільшення кількості учасників деструктивної віртуальної спільноти.
	Якщо значення показника $InfThreat_{CritMembers}(VirtualCommunity) \approx 0{,}5$	Ведення постійного моніторингу щодо збільшення кількості учасників деструктивної віртуальної спільноти.
	Якщо значення показника $InfThreat_{InfConfr}(VirtualCommunity) \to 1$, це вказує на відсутність конкурентної віртуальної спільноти відносно тематики інформаційного наповнення деструктивної віртуальної спільноти.	Ведення постійного моніторингу щодо збільшення кількості учасників та вживання заходів для створення конкурентної віртуальної спільноти.
	Якщо значення показників $InfThreat_{CritMembers}(VirtualCommunity) \to 0$ та $InfThreat_{InfConfr}(VirtualCommunity) \to 1$, це свідчить про створення нової або руйнування існуючої деструктивної віртуальної спільноти.	Ведення постійного моніторингу щодо сценарію розвитку деструктивної віртуальної спільноти.

3.4. Стратегії інформаційного впливу на структуру віртуальної спільноти

Стратегії впливу на структуру внутрішнього інформаційного середовища розроблено залежно від правил протидії держави інформаційному впливу віртуальних спільнот – пп. 1.5 «Правила протидії держави інформаційно-психологічному впливу віртуальних спільнот», а саме:

Стратегія 1

Блокування дискусій або інформаційно-психологічний вплив на них з метою зміни тематичної спрямованості дискусій та їх переміщення до конкуретної віртуальної спільноти, що пов'язано зі зменшенням кількості дискусій та учасників у віртуальній спільноті.

Стратегія 2

Руйнування зв'язків окремої дискусії, щоб зробити її ізольованою дискусією без зменшення загальної кількості дискусій та учасників у віртуальній спільноті.

Стратегія 3

Руйнування зв'язків окремої дискусії задля формування окремих груп дискусій без зменшення загальної кількості дискусій та учасників у віртуальній спільноті.

Проведено дослідження з метою аналізу використання стратегій впливу на внутрішнє інформаційне середовище.

Умови дослідження:

Початкова структура внутрішнього інформаційного середовища така:

кількість дискусій – 100;

кількість учасників дискусій $ThreadMembers_i = 100$;

всі дискусії між собою взаємозв'язані гіперпосиланнями, тобто віртуальна спільнота становить одну групу.

Обмеження експерименту:

для вибору стратегії не враховується якість інформаційного наповнення віртуальної спільноти, тобто $Sim(Thread_i) = 1$.

Критична кількість учасників віртуальної спільноти дорівнює загальній кількості учасників дискусій у віртуальній спільноті $Members(InfThreat_i) = 10000$.

Для визначення інформаційної загрози віртуальної спільноти використовуємо показник інформаційної загрози (2.23).

Результати розрахунків вибіркових точок наведено в табл. 3.4.

Таблиця 3.4.

Результати вибіркових точок

№ розрахунку	Стратегія 1			Стратегія 2			Стратегія 3		
	К-ть дискусій у групі	К-ть блокованих дискусій	Показник інформаційної загрози	К-ть дискусій у групі	К-ть ізольованих дискусій	Показник інформаційної загрози	К-ть груп	К-ть дискусій у групі	Показник інформаційної загрози
1	100	0	1	100	0	1	1	100	1
2	99	1	0,99	99	1	0,99	2	50	0,92
4	97	3	0,97	97	3	0,98	4	25	0,83
5	96	4	0,96	96	4	0,97	5	20	0,80
10	91	9	0,9	91	9	0,94	10	10	0,72
20	81	19	0,79	81	19	0,87	20	5	0,64
25	76	24	0,73	76	24	0,84	25	4	0,61
50	51	49	0,47	51	49	0,68	50	2	0,52
100	1	99	0	1	99	0,44	100	1	0,44

Графіки зміни показника інформаційної загрози процесу функціонування віртуальної спільноти залежно від стратегії впливу на структуру внутрішнього інформаційного середовища наведено на рис. 3.15.

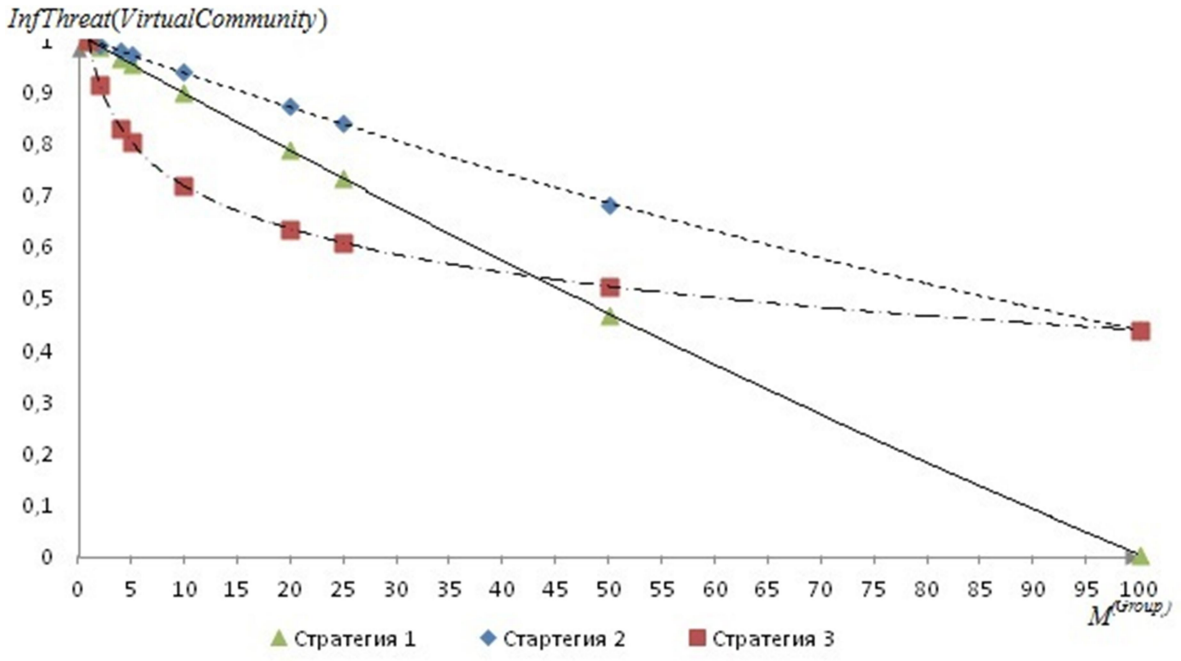

Рис. 3.15. Зміна показника інформаційної загрози в разі використання Стратегій 1, 2 та 3

Результати використання стратегій:

Стратегія 1

Планомірне зменшення показника інформаційної загрози до нульової позначки, що характеризується не зміною структури внутрішнього інформаційного середовища віртуальної спільноти, а зменшенням кількості дискусій та учасників у віртуальній спільноті.

Недоліками цієї стратегії є те, що не завжди існують інструменти впливу щодо блокування сторінок дискусій у соціальних мережах, що пов’язано з багатьма об’єктивними причинами та особливостями віртуальних спільнот у разі виявлення небезпеки їх функціонування, які розглянуті в пп. 1.3.1 «Властивості віртуальних спільнот у соціальних мережах як суб’єктів інформаційної безпеки».

Стратегія 2

Планомірне зменшення показника інформаційної загрози до граничного мінімального значення. Зменшення показника залежить від кількості ізольованих дискусій, які утворилися в результаті інформаційно-психологічного впливу на структуру віртуальної спільноти.

Недоліки цієї стратегії такі:

– практично неможливо за великої кількості дискусій здіснювати інформаційно-психологічний вплив на всі дискусії для зміни структури внутрішнього інформаційного середовища;

– обмеженість граничним мінімальним значенням показника інформаційної загрози.

Стратегія 3

Характеризується на перших етапах різким зменшенням показника інформаційної загрози з подальшим планомірним зниженням до граничного мінімального значення.

Недоліки цієї стратегії такі:

– у загальному випадку, для формування окремих груп дискусій необхідно здійснювати інформаційно-психологічний вплив більш ніж на одну дискусію;

– обмеженість граничним мінімальним значенням показника інформаційної загрози.

Загальним недоліком стратегій 2 та 3 є те, що практично неможливо методами інформаційно-психологічного впливу руйнувати зв’язки між дискусіями у віртуальній спільноті.

Отже, ефективними стратегіями впливу є змішані стратегії 1&2 та 1&3, у разі використання яких можливі такі варіанти впливу:

– руйнування зв’язків між дискусіями групи за допомогою блокування дискусій (силовий метод);

– інформаційно-психологічний вплив на дискусії з метою зменшення ступеня відповідності тематичного напряму повідомлень у дискусії та переходу дискусії до конкурентної віртуальної спільноти (моніторинг віртуальних спільнот та протидія методами інформаційно-психологічного впливу).

3.5. Метод визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти

Щоб сформувати рекомендації щодо впливу на структуру віртуальної спільноти, використовуючи модель внутрішнього інформаційного середовища (2.4), віртуальну спільноту подамо у вигляді незв'язного, неорієнтованого графа матричним способом [127, 152]:

$$G = (V, A), \tag{3.3}$$

де V – множина вершин, яка складається із сукупностей дискусій *i*-ї віртуальної спільноти $Thread(VirtualCommunity_i)$;

A – матриця суміжності графа G.

Елементи матриці суміжності A визначаються з матриці зв'язків між дискусіями віртуальної спільноти (2.22):

$$a_{ij} = link_{ij}.$$

На основі характеристик дискусій $Sim(Thread_i)$ (2.16) та моделі дискусії (2.5) визначимо вагові показники вершин графа:

$$V = \left\| Sim(Thread_i), card(ThreadMembers_i) \right\|_{i=\overline{1,n}}, \tag{3.4}$$

де $Sim(Thread_i)$ – міра відповідності тематичного напряму дописів *i*-ї дискусії;

$card(ThreadMembers_i)$ – кількість учасників дискусії.

Отже, (3.3), (3.4) – це модель внутрішнього інформаційного середовища віртуальної спільноти у вигляді незв'язного, неорієнтованого графа матричним способом.

Використовуючи алгоритми теорії графів, розв'язано задачу щодо визначення мінімального переліку дискусій $Thread$ віртуальної спільноти $VirtualCommunity$, після видалення яких показник інформаційної загрози

отриманої віртуальної спільноти зменшився до порогового значення $InfThreat(VirtualCommunity) \le \varepsilon$.

3.5.1. Алгоритм вибору дискусій віртуальної спільноти для інформаційного впливу на внутрішнє інформаційне середовище

Результатом роботи алгоритму є визначення мінімальної кількості дискусій віртуальної спільноти для інформаційного впливу, щоб зменшити показник інформаційної загрози до порогового значення.

Крім того, виконано такі часткові завдання:

– сформовані групи дискусій;

– під час повторного використання алгоритму враховано зворотний зв’язок за результатами інформаційного впливу на віртуальну спільноту.

Метод визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти включає наступні блоки:

Блок 1.

Формуємо групи дискусій віртуальної спільноти відповідно до розроблених правил (пп. 2.7.1 «Визначення цінності віртуальної спільноти»). Для створених груп визначаємо їхні цінності згідно з формулою (2.24). Вибираємо групу, для якої цінність (2.29) максимальна та кількість елементів більша за два.

Блок 2.

Для вибраної групи визначаємо дискусію або перелік дискусій для інформаційного впливу.

Потім цю дискусію вилучаємо з віртуальної спільноти за допомогою дії силового (блокування дискусії) або інформаційного впливу (зміна тематичного напряму дискусії та її переміщення у конкурентну віртуальну спільноту).

Блок 3.

Для отриманої віртуальної спільноти розраховуємо показник інформаційної загрози відповідно до виразу (2.23).

Якщо показник інформаційної загрози більший від порогового значення, переходимо до блока 1.

Блок 4.

Надання рекомендацій щодо переліку дискусій для впливу на внутрішнє інформаційне середовище та формування прогнозованої структури внутрішнього інформаційного середовища віртуальної спільноти.

3.5.2. Формування груп дискусій

У зв'язку з тим, що віртуальну спільноту подано матричним способом (3.3), для формування груп дискусій застосовуємо алгоритм матричного розбивання графу на максимальні сильно зв'язані підграфи [5, 36].

Для цього використовуємо матрицю суміжності A. Крім того, всі діагональні елементи матриці дорівнюють одиниці, оскільки кожна вершина досяжна сама для себе.

Розраховуємо матрицю досяжності R, використовуючи паралельний алгоритм знаходження матриці досяжності у графі [41].

Розглянемо суть паралельного алгоритму формування матриці досяжності:

1. Визначаємо матрицю досяжності $R^0 = A$.

2. Розраховуємо матрицю досяжності для наступних ітерацій *k*, відповідно до загальної формули перетворення:

$$\forall R_i^k = R_{i1}^{k-1} \times (R_{11}^{k-1}, R_{12}^{k-1}, R_{13}^{k-1}, ..., R_{1n}^{k-1}) \vee R_{i2}^{k-1} \times (R_{21}^{k-1}, R_{22}^{k-1}, R_{23}^{k-1}, ..., R_{2n}^{k-1}) \vee ... \vee \vee R_{in}^{k-1} \times (R_{n1}^{k-1}, R_{n2}^{k-1}, R_{n3}^{k-1}, ..., R_{nn}^{k-1}).$$

3. Далі крок 2 повторюється, поки не виконається умова:

$$R^k = R^{k-1}.$$

За результатами роботи паралельного алгоритму отримуємо матрицю, в якій $r_{ij} = 1$, якщо існує шлях від *i*-ї до *j*-ї вершини.

Елементи, що мають однакові рядки і стовпці в матриці R, групуємо, переставляючи рядки і стовпці, отримуємо блочно-діагональну матрицю R_B, кожна група елементів якої є групою дискусій віртуальної спільноти.

Якщо всі елементи матриці R дорівнюють одиниці, то віртуальна спільнота представлена однією групою.

Ізольовані дискусії створюються тоді, коли в матриці R_B для вершини тільки діагональний елемент дорівнює одиниці.

3.5.3. Визначення дискусій для впливу на внутрішнє інформаційне середовище

Для визначення дискусії використовуємо властивості матриці суміжності, піднесеної до степеня [5, 36]. Оскільки необхідно визначити тільки наявність шляху між вершинами в алгоритмі з піднесенням матриці суміжності до степеня, алгоритмічні дії між її елементами замінюємо на логічні (суму замінюємо на диз'юнкцію, а добуток на кон'юнкцію).

Зміст алгоритму такий:

1. Визначаємо матрицю досяжності $R^1 = A$.

2. Розраховуємо матрицю досяжності для наступних ітерацій k, відповідно до загальної формули перетворення:

$$\forall R_i^k = R_{i1}^{k-1} \times (R_{11}^1, R_{12}^1, R_{13}^1, ..., R_{1n}^1) \vee R_{i2}^{k-1} \times (R_{21}^1, R_{22}^1, R_{23}^1, ..., R_{2n}^1) \vee ... \vee \\ \vee R_{in}^{k-1} \times (R_{n1}^1, R_{n2}^1, R_{n3}^1, ..., R_{nn}^1)$$

3. Далі крок 2 повторюється, поки не буде виконана умова: сума всіх елементів для одного із рядків матриці R^k не дорівнюватиме кількості дискусій у групі.

За результатами роботи алгоритму отримуємо від однієї до декількох дискусій, з найкоротшим шляхом до всіх дискусій групи віртуальної спільноти.

3.5.4. Вибір дискусій для впливу на внутрішнє інформаційне середовище

Вибираючи дискусії, необхідно враховувати, що під час повторного моніторингу та визначення стратегії впливу на внутрішнє інформаційне середовище створюється перелік заборонених дискусій, на які неможливий подальший інформаційно-психологічний вплив, оскільки:

– дискусія сильно модерована, адміністратори та модератори дискусії постійно видаляють небажане інформаційне наповнення;

– інформаційно-психологічний вплив призвів до негативного результату для учасників дискусії.

Отже, для вибору дискусії з переліку визначених видаляємо із переліку дискусії, які входять до переліку заборонених, та надалі дотримуємось таких правил:

– якщо перелік дискусій не містить жодної дискусії, то виконуємо алгоритм визначення дискусій для $k+1$ ітерації, щоб отримати додатковий перелік дискусій;

– якщо в переліку дискусій одна дискусія, вибираємо її як об’єкт інформаційного впливу.

За наявності декількох дискусій вибираємо ту дискусію, у разі видалення якої показник інформаційної загрози зменшується найбільше. Якщо таких дискусій декілька, вибираємо ту, в якій значення тематичного напряму дискусії найменше.

3.5.5. Визначення рекомендацій щодо впливу на внутрішнє інформаційне середовище

Рекомендації формулюють після того, як сформовано повний перелік дискусій, видалення яких з віртуальної спільноти забезпечує зменшення показника інформаційної загрози до порогового значення.

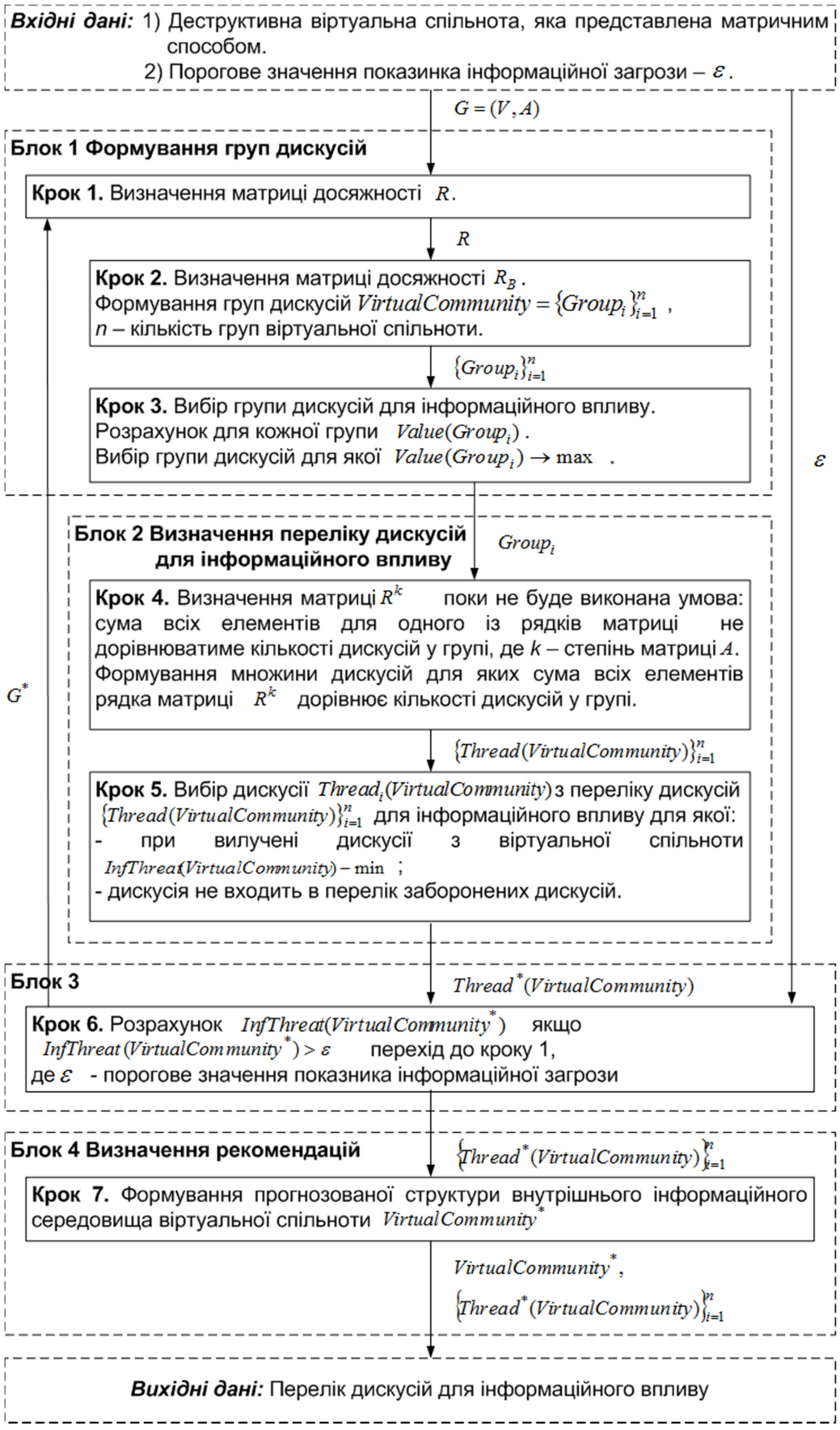

Рис. 3.16. Схематичне зображення методу визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти

Крім переліку дискусій, формується прогнозована структура внутрішнього та зовнішнього інформаційних середовищ віртуальної спільноти після інформаційного впливу.

Для подальшого моніторингу віртуальної спільноти визначають вікно спостереження, яке забезпечить очікування результатів після виконання дій щодо інформаційно-психологічного впливу.

Під час повторного моніторингу соціальної мережі здійснюють всі заходи для виявлення та формування віртуальної спільноти за визначеною тематикою інформаційного наповнення.

Перед повторним моніторингом соціальної мережі формується перелік заборонених дискусій.

Схематичне зображення методу визначення рекомендацій щодо впливу на структуру віртуальної спільноти відображено на рис. 3.16.

3.5.6. Експериментальна частина

Виконано розрахунки для змодельованої віртуальної спільноти з характеристиками, наведеними в табл. 3.5.

Таблиця 3.5

Характеристики графу змодельованої віртуальної спільноти

№ з/п	Метрики графу	Значення
1	Вершини графа (дискусії)	500
2	Ребра графу	737
3	Зв’язні компоненти	1
4	Максимальна кількість вершин у зв’язному компоненті	500
5	Максимальний діаметр графу	500
6	Середній діаметр графу	12
7	Щільність графу	5,72

Ці характеристики графу змодельованої віртуальної спільноти відповідають попереднім дослідженням структури соціальних мереж [1, 36, 41, 116, 133].

Додаткові характеристики для дискусій віртуальної спільноти подано в табл. 3.6.

Таблиця 3.6

Характеристики дискусій віртуальної спільноти

№ з/п	Характеристики дискусій	Значення
1	Мінімальна кількість учасників	100
2	Максимальна кількість учасників	1000
3	Мінімальна міра відповідності тематичного напряму дописів у дискусії	0,5
4	Максимальна міра відповідності тематичного напряму дописів у дискусії	1

Розрахунки виконано для двох варіантів:

Варіант 1: для віртуальної спільноти, в якій не визначено перелік заборонених дискусій, на які неможливий подальший інформаційно-психологічний вплив.

Варіант 2: для віртуальної спільноти, у якій визначено перелік заборонених дискусій, на які неможливий подальший інформаційно-психологічний вплив за результатами розрахунків за варіантом 1 (дискусії – 1, 101, 105, 128).

Розрахунок для обох варіантів виконують до зменшення показника інформаційної загрози до порогового значення – 0,5.

Структуру графу зображено на рис. 3.17, 3.18 для першого та другого варіантів розрахунків.

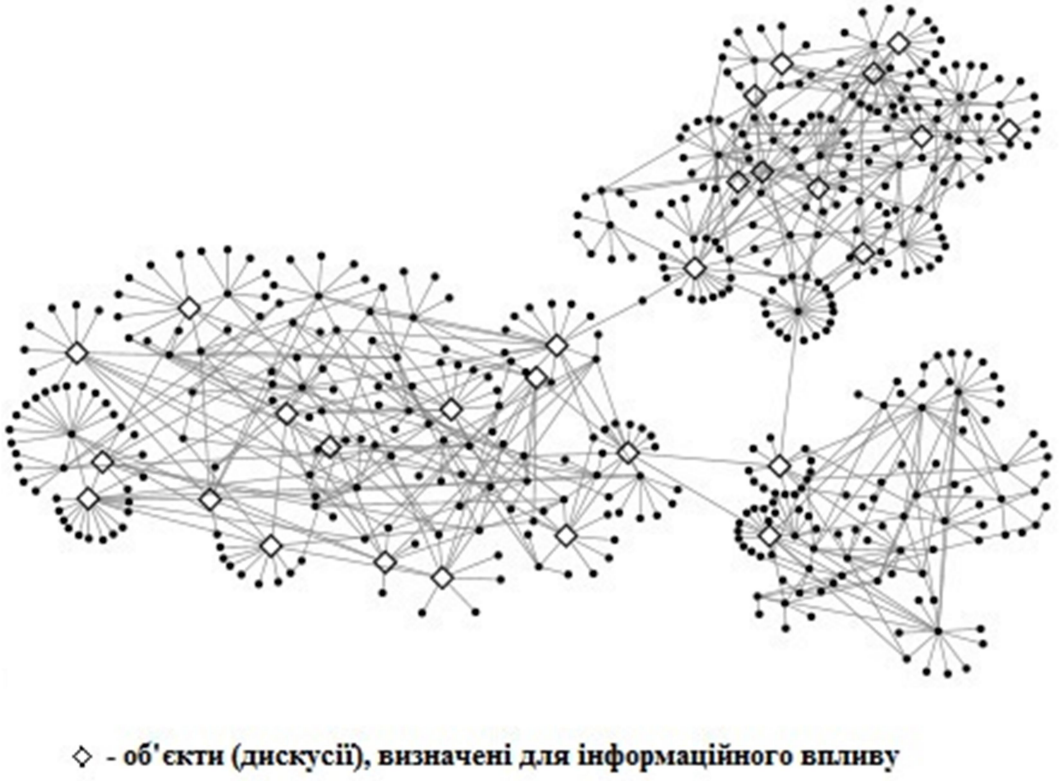

Рис. 3.17. Структура віртуальної спільноти (варіант 1)

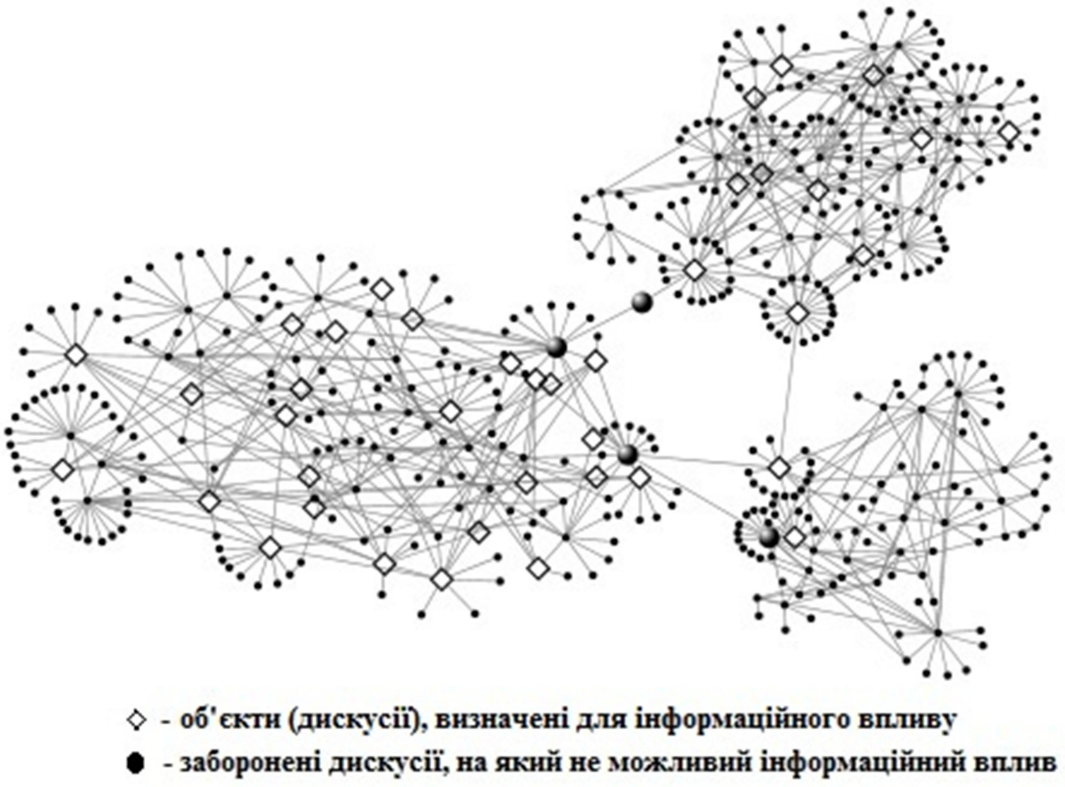

Рис. 3.18. Структура віртуальної спільноти (варіант 2)

Результати виконаних розрахунків подано в табл. А.1, А.2 для першого та другого варіантів.

Графіки змін показника інформаційної загрози для першого та другого варіантів подано на рис. 3.19.

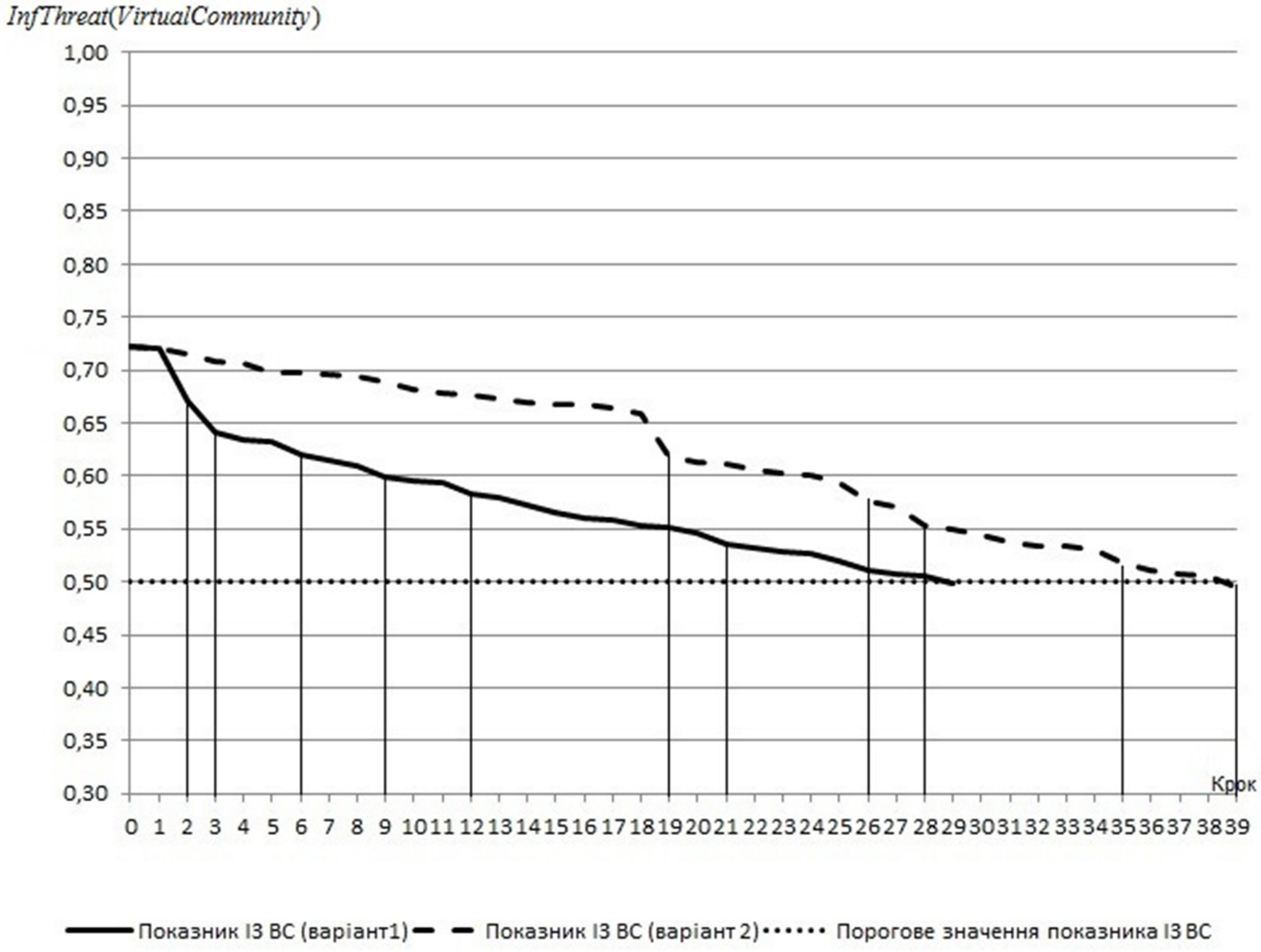

Рис. 3.19. Графіки змін показника інформаційної загрози

Прогнозовані структури віртуальної спільноти після інформаційного впливу для варіантів 1 та 2 зображено на рис. 3.20, 3.21.

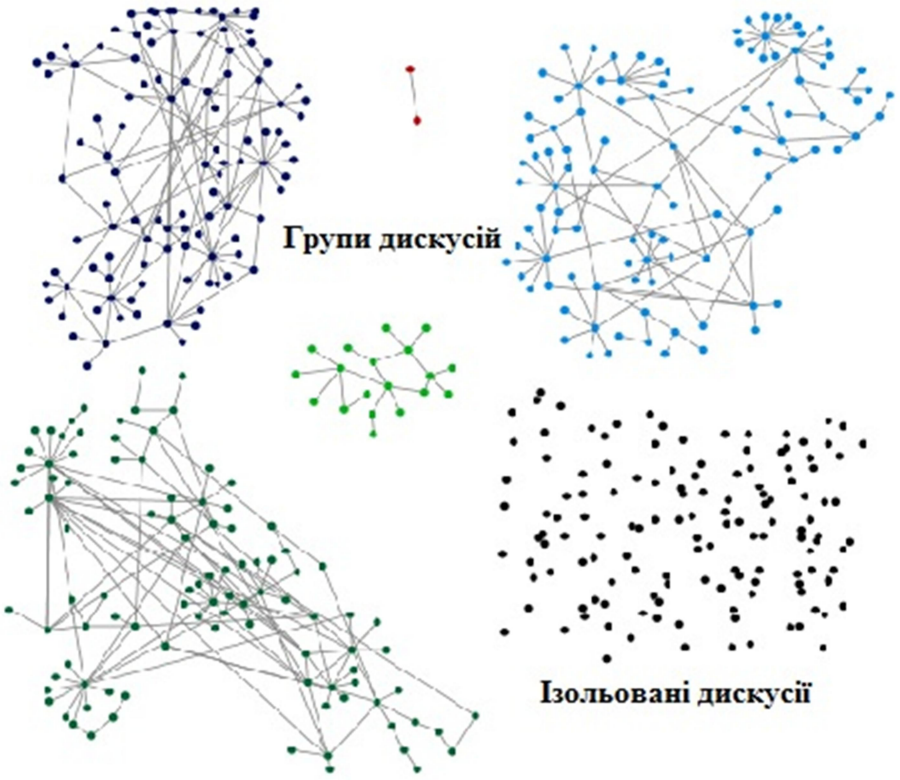

Рис. 3.20. Прогнозована структура віртуальної спільноти (варіант 1)

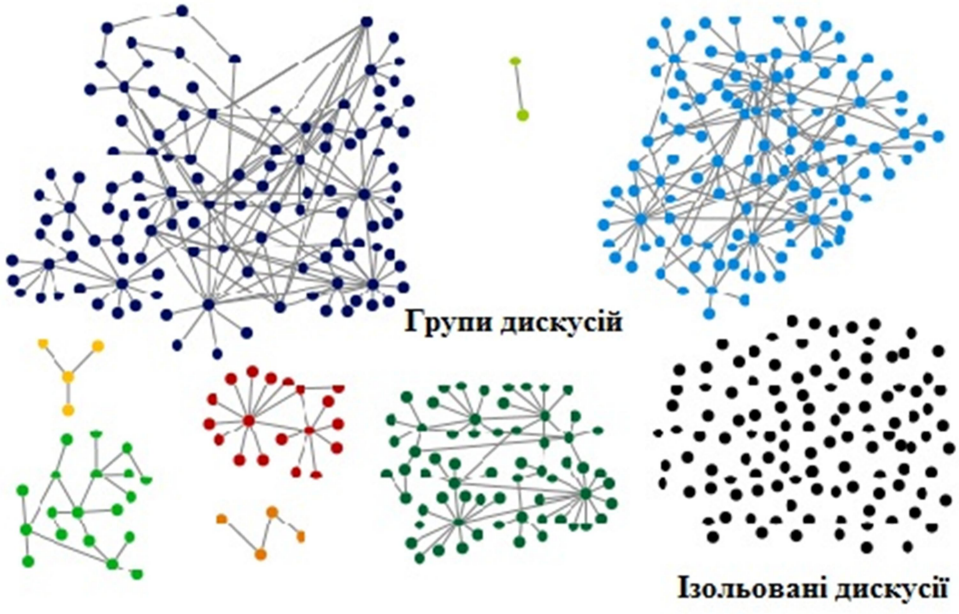

Рис. 3.21. Прогнозована структура віртуальної спільноти (варіант 2)

Найбільше зменшення показника інформаційної загрози досягається у разі використання змішаних стратегій впливу з формуванням окремих груп на кроках для варіанта 1 – (2, 3, 6, 21) та для варіанта 2 – (19, 28, 35), а також

створення великої кількості ізольованих дискусій унаслідок впливу на одну дискусію на кроках для варіанта 1 – (9, 12) та для варіанта 2 – (26, 39).

Результати експерименту підтвердили, що показник інформаційної загрози знижується за рахунок руйнування структури віртуальної спільноти, а не внаслідок зменшення кількості дискусій у віртуальній спільноті (табл. А.1, А.2).

Для визначення аддекватності методу був проведений експеримент за варіантом 3 з модельованою віртуальною спільнотою з визначеними характеристиками табл. 3.5, 3.6 відповідно до стратегії 1, що пов’язано зі зменшенням кількості дискусій, учасників у віртуальній спільноті та випадковим руйнуванням структури віртуальної спільноти. Відповідно до цього для впливу вибираються дискусії в яких максимальна кількість учасників. Результати виконаних розрахунків подано в табл. А.3.

Зміни показника інформаційної загрози за варіантами 1, 2 та 3 зображено на рис. 3.22. Відповідно до графіку

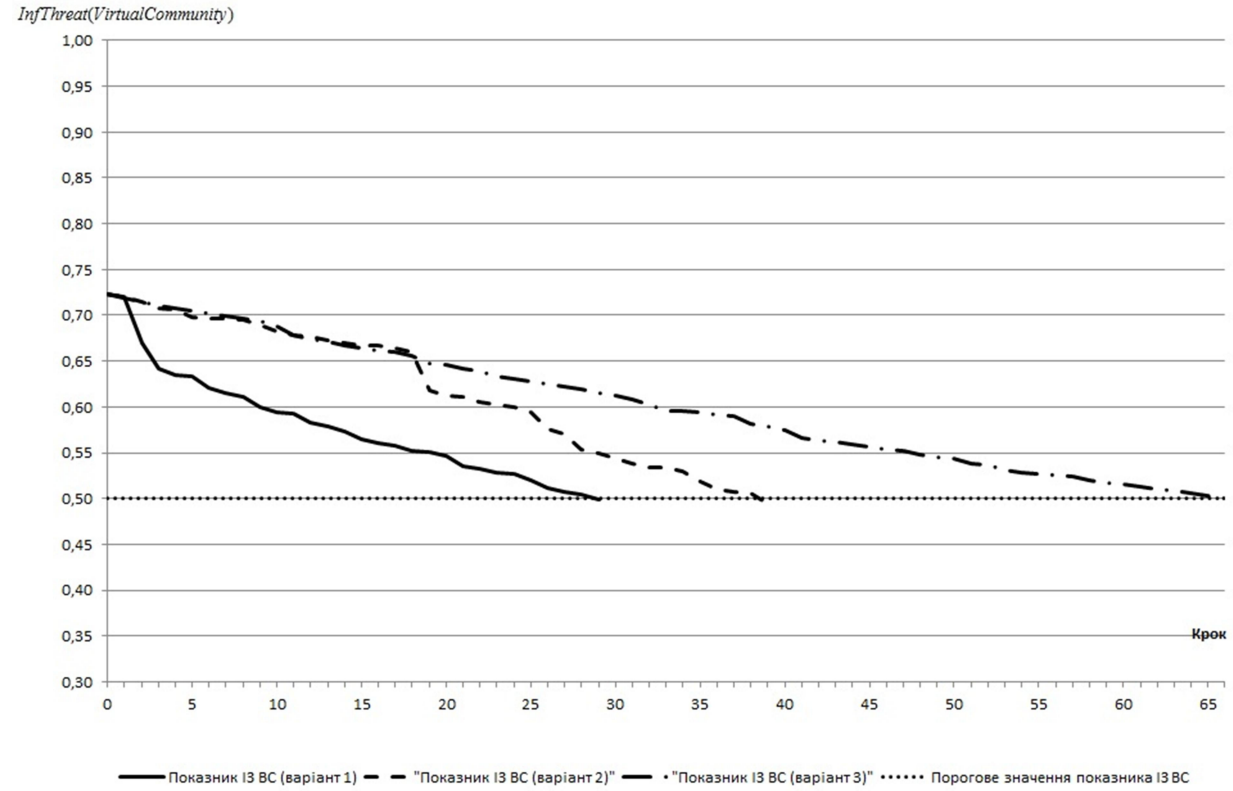

Рис. 3.22. Графіки змін показника інформаційної загрози для 1, 2 та 3 варіантів

Відповідно до результатів експериментів визначено, що при використанні методу визначення рекомендацій щодо впливу на структуру внутрішнього інформаційного середовища віртуальної спільноти для зменьшення показника інформаційної загрози до порогового значення необхідно проводити вплив на меньшу кількість дискусій віртуальної спільноти ніж при впливі на дискусії з максимальною кількістю учасників.

Висновки до розділу 3

У третьому розділі розроблено методи та алгоритми виявлення інформаційних загроз віртуальних спільнот у соціальних мережах та оцінка їх. Зокрема, отримано такі результати:

- Розроблено методи та алгоритми пошуку дискусій за допомогою глобальної пошукової системи Google з використанням формалізованих запитів та пошукового робота із застосуванням запитів API-методами соціальних мереж.
- Запропоновано методи та алгоритми формування інформаційного середовища віртуальних спільнот згідно з ознакою мети, ідеології існування та міри відповідності тематичного напряму повідомлень у дискусіях.
- Розроблено метод прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот.
- Розроблено стратегії інформаційного впливу на структуру віртуальної спільноти.
- Розроблено метод визначення рекомендацій щодо інформаційного впливу на структуру внутрішнього інформаційного середовища віртуальної спільноти.

Основні результати розділу автор опублікував у роботах: [21, 72, 76, 77, 80, 123, 124].

РОЗДІЛ 4. ПОБУДОВА АРХІТЕКТУРИ КОМПЛЕКСУ МОНІТОРИНГУ ТА АНАЛІЗУ ІНФОРМАЦІЙНИХ ЗАГРОЗ ВІРТУАЛЬНИХ СПІЛЬНОТ У СОЦІАЛЬНИХ МЕРЕЖАХ

4.1. Архітектура програмного комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах

Запропоновані у попередніх розділах методи та алгоритми виявлення та оцінки інформаційних загроз віртуальних спільнот в соціальних мережах є основою архітектури програмно-алгоритмічного комплексу автоматизації моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах. Процес моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах складається з таких етапів життєвого циклу (рис. 4.1):

Пошук – визначення ключових слів відповідно до тематики інформаційної загрози та виявлення релевантних сторінок дискусій віртуальних спільнот у соціальних мережах.

Аналіз – аналіз інформаційного наповнення з метою формування інформаційного середовища віртуальної спільноти та моделі загроз.

Рекомендації – оцінка ступеня інформаційної загрози віртуальної спільноти та визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти в соціальних мережах.

Вплив – інформаційний вплив на інформаційне наповнення сторінок дискусій віртуальної спільноти в соціальних мережах.

Прийняття рішення – підтвердження результатів на всіх етапах роботи.

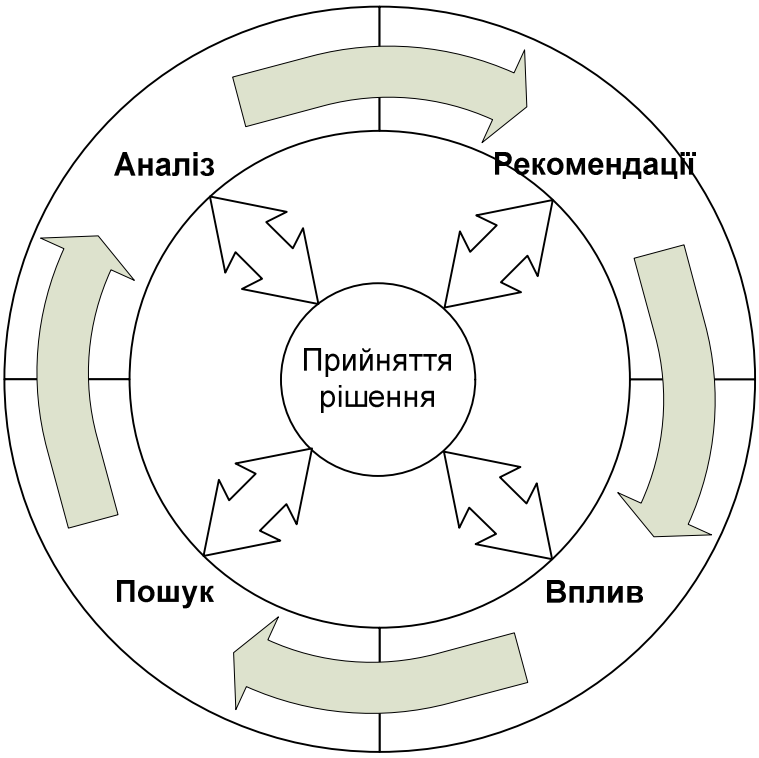

Рис. 4.1. Цикл моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах

Відповідно до циклу моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах архітектура комплексу складається з основних компонентів, наведених на рис. 4.2.

Програмний комплекс відповідно до завдань, які виникають у процесі виявлення та протидії інформаційним загрозам віртуальної спільноти в соціальних мережах, складається з трьох підсистем:

– підсистема моніторингу віртуальних спільнот, призначена для пошуку дискусій в соціальних мережах відповідно до їх інформаційного наповнення;

– підсистема аналізу віртуальних спільнот, що слугує для аналізу інформаційного наповнення з метою формування інформаційного середовища віртуальної спільноти;

– підсистема прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот у соціальних мережах, призначена для оцінювання інформаційних загроз та визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти в соціальних мережах.

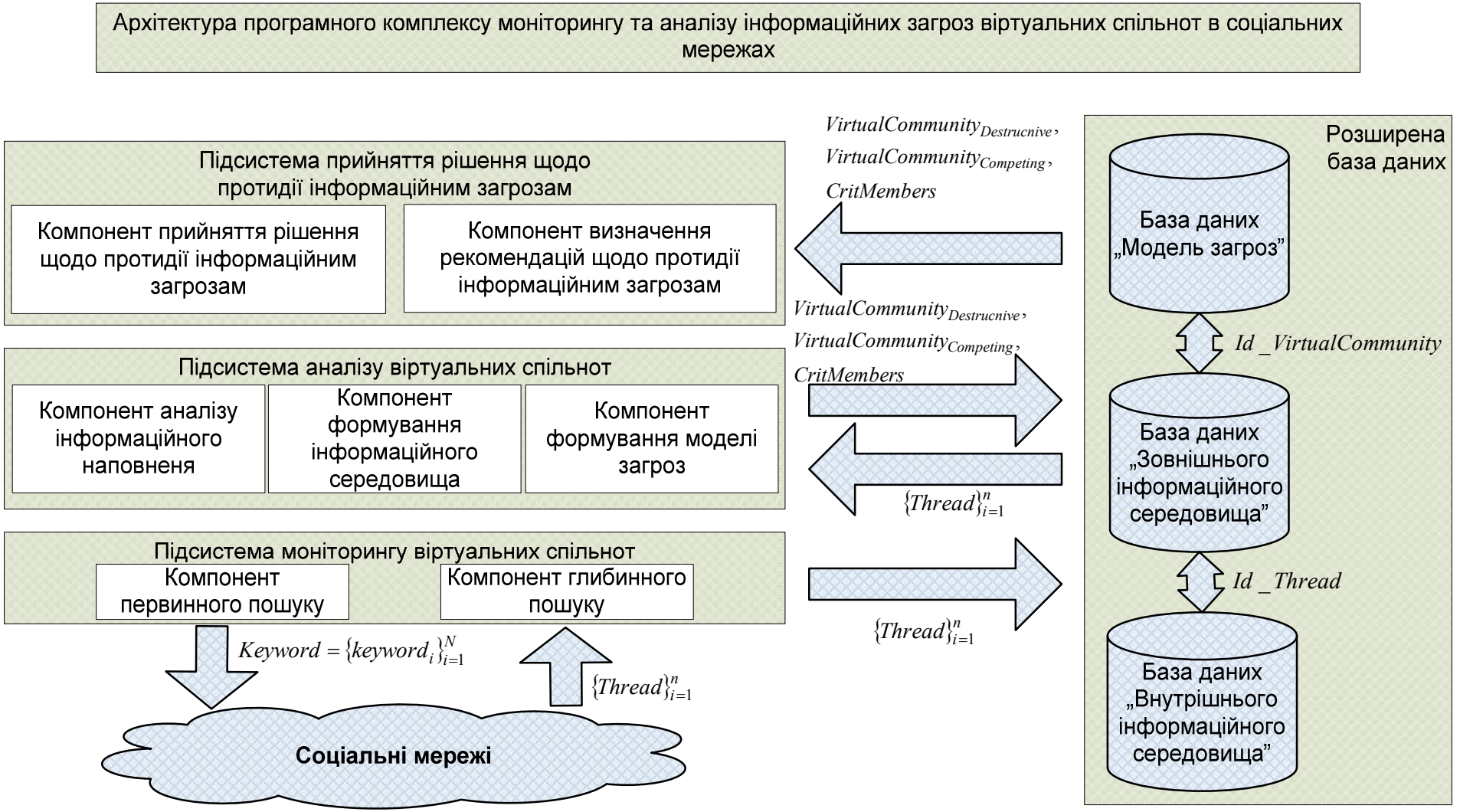

Рис. 4.2. Архітектура програмного комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах

Своєю чергою, кожна з цих підсистем складається з програмних компонент.

Підсистема моніторингу віртуальних спільнот:

– компонент первинного пошуку за допомогою формалізованих запитів глобальної пошукової системи Google відповідно до ключових слів (пп. 3.1.1 «Структура формалізованого запиту», пп. 3.1.2 «Особливості пошуку спільнот та дискусій у «Вконтакті», пп. 3.1.3 «Особливості пошуку спільнот та дискусій у «Facebook»);

– компонент глибинного пошуку за допомогою пошукового робота з використанням запитів API-методів соціальних мереж та аналізу Html-коду сторінок, які знайдені під час первинного пошуку (пп. 3.1.4 «Глибинний пошук»).

Підсистема аналізу віртуальних спільнот:

– компонент кластеризації результатів пошуку відповідно до інформаційного наповнення дискусій (пп. 3.2.1 «Кластеризація результатів пошуку»);

– компонент формування інформаційного середовища віртуальної спільноти в соціальних мережах з метою визначення деструктивної та конкурентної віртуальних спільнот (пп. 3.2.2 «Розподіл кластерів дискусій на віртуальні спільноти»);

– компонент формування моделі загроз (пп. 3.3.1 «Формування моделі загроз»).

Підсистема прийняття рішення щодо протидії інформаційним загрозам:

– компонент прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот у соціальних мережах (пп. 3.3.2 «Визначення ступеня інформаційної загрози віртуальної спільноти в соціальних мережах»);

– компонент визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти в соціальних мережах (пп. 3.5 «Метод

визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти»).

4.2. База даних комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах

Повноцінний моніторинг та аналіз інформаційних загроз віртуальних спільнот у соціальних мережах забезпечує використання розширеної бази даних, яка складається із таких компонент (рис. 4.3):

– база даних «Зовнішнього інформаційного середовища»;

– база даних «Внутрішнього інформаційного середовища»;

– база даних «Моделі загроз».

Наповнення та підтримку актуальності бази даних здійснюють фахівці на різних робочих місцях системного комплексу, залежно від функціональних обов’язків та сфери відповідальності.

Далі розглянемо структуру кожної компоненти розширеної бази даних.

4.2.1. База даних «Зовнішнього інформаційного середовища»

Для обліку елементів зовнішнього інформаційного середовища віртуальної спільноти в соціальних мережах, їхніх технічних і семантичних характеристик використовується база даних «Зовнішнього інформаційного середовища». Наповнення бази даних здійснюється у процесі виконання завдань:

– пошуку та обліку віртуальних спільнот залежно від інформаційного наповнення їх дискусій;

– обліку та аналізу статистичних та семантичних характеристик віртуальних спільнот, підтримання актуальності цих даних;

– алгоритмів формування зовнішнього інформаційного середовища.

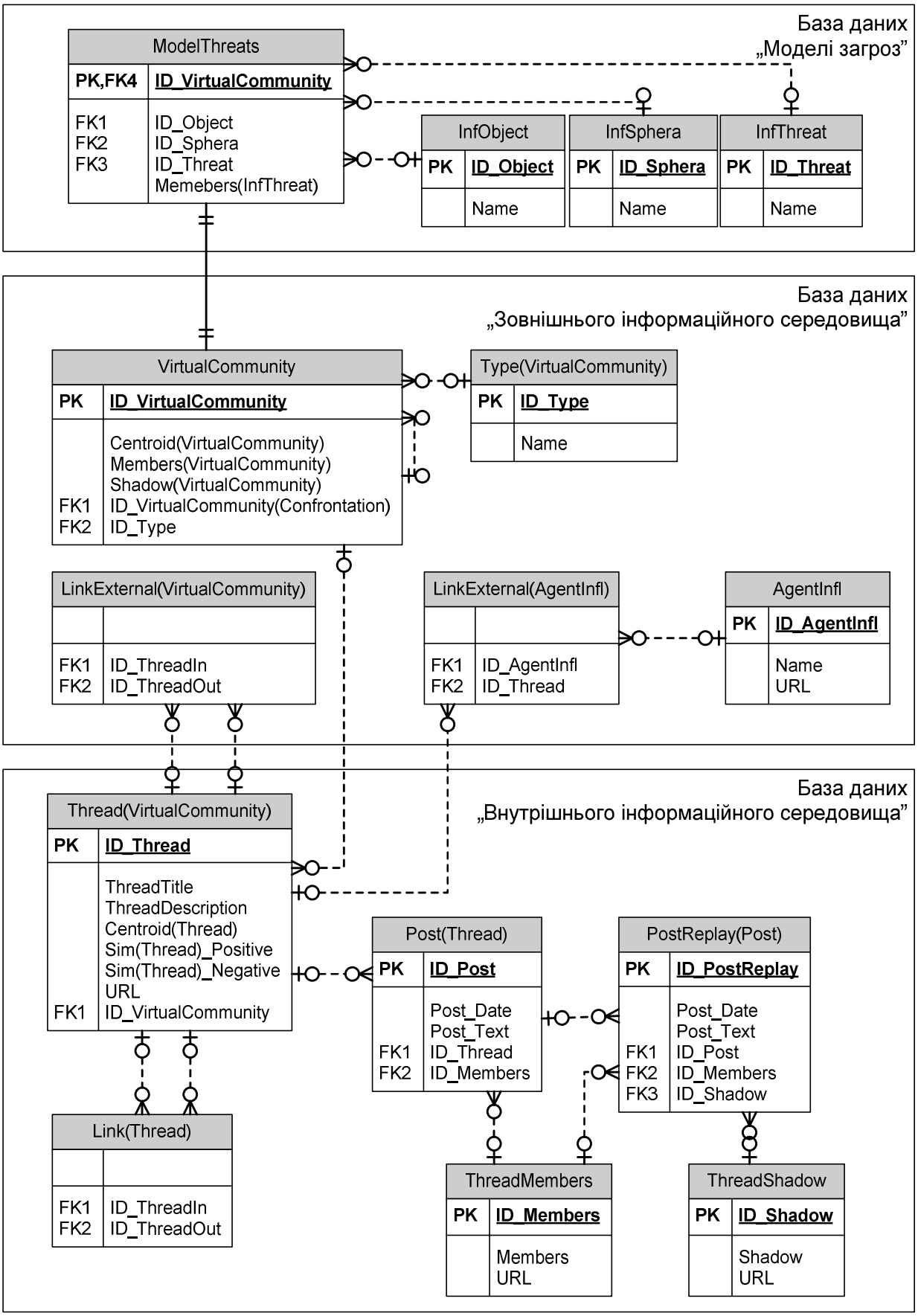

Рис. 4.3. ER-діаграма розширеної бази даних

База даних «Зовнішнього інформаційного середовища» складається з таких частин:

– таблиця *VirtualCommunity* – описує віртуальні спільноти в інформаційному середовищі, їхні статистичні та семантичні характеристики;

– таблиця *AgentInfl* – описує агентів зовнішнього впливу (інтернет-ЗМІ, блоги політиків, відомих людей);

– таблиця *LinkExternal(VirtualCommunity)* – містить інформацію про зв'язки між дискусіями різних віртуальних спільнот;

– таблиця *LinkExternal(AgentInfl)* – містить інформацію про зв'язки між дискусіями віртуальних спільнот та агентів зовнішнього впливу;

– таблиця *Type(VirtualCommunity)* описує тип віртуальної спільноти (конструктивна – деструктивна).

Математичною основою бази даних «Зовнішнього інформаційного середовища» є формальна модель, побудована у пп. 2.1.1 «Побудова моделі зовнішнього інформаційного середовища віртуальної спільноти».

4.2.2. База даних «Внутрішнього інформаційного середовища»

Для опису внутрішнього інформаційного середовища обліку підлягають елементи віртуальної спільноти – дискусії та їхні статистичні й семантичні характеристики. Дані отримують у результаті:

– пошуку та обліку дискусій залежно від їхнього інформаційного наповнення;

– обліку технічних та семантичних характеристик цих дискусій;

– алгоритмів формування внутрішнього інформаційного середовища.

База даних «Внутрішнього інформаційного середовища» складається з таких частин:

– таблиця *Thread(VirtualCommunity)* – описує дискусії віртуальної спільноти, їхні статистичні та семантичні характеристики;

– таблиця *PostThread* – описує повідомлення у дискусії віртуальної спільноти, її статистичні та семантичні характеристики;

– таблиця *PostReplay(Post)* – описує дописи до повідомлень у дискусії віртуальної спільноти;

– таблиця *Link (Thread)* – містить інформацію про зв'язки між дискусіями в межах віртуальної спільноти;

– таблиця *ThreadMembers* – описує учасників дискусії віртуальної спільноти;

– таблиця *ThreadShadow* – описує зареєстрованих користувачів соціальних мереж, які цікавляться ідеологією (тематикою) віртуальної спільноти, але не є учасниками дискусії.

Математичною основою бази даних «Внутрішнього інформаційного середовища» є формальна модель, побудована у пп. 2.1.2 «Побудова моделі внутрішнього інформаційного середовища віртуальної спільноти».

4.2.3. База даних «Моделі загроз»

Для прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот у соціальних мережах формується база даних «Моделі загроз». Даними для бази даних є результати експертного визначення інформаційної загрози, яку становить інформаційне наповнення віртуальної спільноти.

База даних «Внутрішнього інформаційного середовища» складається з таких частин:

– таблиця *ModelThreats* – описує модель загроз відповідно до табл. **Ошибка! Источник ссылки не найден.**;

– таблиця *InfObject* – службова таблиця, що описує об'єкт інформаційної загрози;

– таблиця *InfSphera* – службова таблиця, що визначає сферу інформаційної загрози;

– таблиця *InfThreat* – службова таблиця, що описує інформаційну загрозу.

Дані для службових таблиць бази даних «Моделі загроз» визначаються відповідно до нормативно-правових документів з інформаційної безпеки держави. Загроз процесу функціонування віртуальних спільнот детальніше проаналізовано в пп. 1.4 «Аналіз інформаційних загроз віртуальних спільнот у соціальних мережах ».

4.3. Структурна схема програмного комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах

Програмний комплекс моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах містить робочі місця (РМ) таких видів:

– «Керівник» – для здійснення стратегічного планування та загального контролю за процесом;

– «Аналітик» – для аналізу інформаційного наповнення дискусій віртуальних спільнот у соціальних мережах;

– «Координатор» – для організації та координації «Агентів впливу» у віртуальних спільнотах;

– «Агент впливу» – для інформаційного впливу на інформаційне наповнення дискусій віртуальних спільнот у соціальних мережах;

– «Пошуковець» – для пошуку та моніторингу віртуальних спільнот у соціальних мережах.

Наведена на рис. 4.4 схема програмного комплексу відображає функціональність робочих місць та основні інформаційні потоки системи.

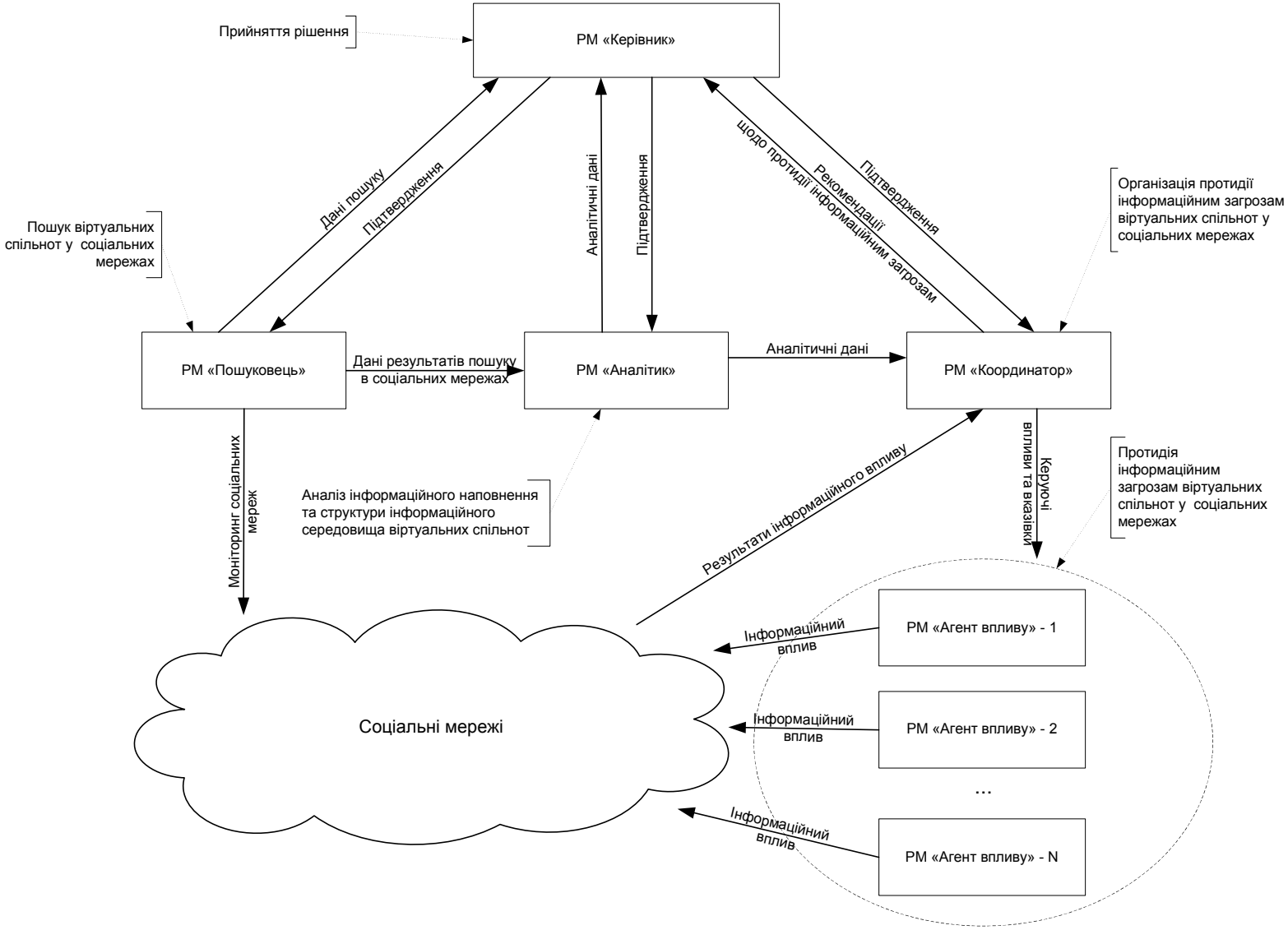

Рис. 4.4. Структурна схема програмного комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах

Основне завдання фахівців на робочому місці «Пошуковець» – початковий етап формування розширеної бази даних, під час якого визначаються ключові слова згідно з тематикою інформаційної загрози. Відповідно до визначених ключових слів здійснюється пошук релевантних сторінок дискусій у соціальних мережах з використанням автоматичних алгоритмів:

– формалізованих запитів глобальної пошукової системи Google та аналізу Html-коду;

– пошукового роботу з використанням запитів API-методів соціальних мереж.

Результатами роботи фахівців на робочому місці «Аналітик» є завершення формування розширеної бази даних. Під час роботи здійснюється кластеризація знайдених сторінок дискусій відповідно до їх інформаційного наповнення з використанням автоматичного алгоритму. Розподіл сторінок дискусій між конкурентною та деструктивною віртуальними спільнотами здійснюється автоматично в залежно від значення міри відповідності тематичного напряму дописів у дискусії. Розрахунок міри відповідності тематичного напряму дописів у дискусії виконують безпосередньо фахівці в ручному режимі, переглядаючи інформаційне наповнення сторінок дискусій, що пов’язано з особливостями формування повідомлень та дописів на сторінках дискусії (пп. 1.6 «Моніторинг та контент-аналіз віртуальних спільнот у соціальних мережах»). Щоб прийняти рішення, надалі фахівці на робочому місці «Аналітик» з використовуючи отримані результати, формують вихідні дані для проведення експертного опитування для створення формування моделі загроз, а саме: об’єкт загрози; сфера застосування загрози; інформаційна загроза; тематика інформаційного наповнення віртуальної спільноти.

Експертне оцінювання проводиться, щоб визначити критичну кількість учасників віртуальної спільноти, за якої реалізується інформаційна загроза.

Основне завдання фахівців на робочому місці «Координатор» – на підставі автоматичних алгоритмів оцінки ступеня інформаційної загрози та визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти в соціальних мережах розробити сценарій інформаційного впливу. Використовуючи сценарій, розробити керуючі впливи та вказівки для «агентів впливу».

Отримані результати інформаційного впливу на віртуальну спільноту необхідно проаналізувати та надати пропозиції щодо подальшого моніторингу віртуальної спільноти.

Основні завдання фахівців на робочому місці «Агент впливу» такі:

– формування та розміщення на сторінках дискусій віртуальної спільноти нових повідомлень, коментарів та відповідей відповідно до сценарію інформаційного впливу;

– моніторинг сторінок дискусій віртуальних спільнот;

– аналізу реакції інших учасників віртуальної спільноти на інформаційний вплив.

«Керівник» здійснює загальне керівництво та організує роботу фахівців на робочих місцях. Основні завдання:

– визначення тематики інформаційної загрози;

– прийняття рішення щодо протидії інформаційним загрозам віртуальної спільноти на підставі ступеня інформаційної загрози;

– затвердження сценарію інформаційного впливу та контроль за його виконанням.

На робочому місці «Керівник» фахівець має змогу аналізувати зведену інформацію щодо процесу виявлення та протидії інформаційним загрозам віртуальних спільнот у соціальних мережах.

На рис. 4.5 наведено схему взаємодії фахівців на різних робочих місцях у процесі виявлення та протидії інформаційним загрозам віртуальних спільнот у соціальних мережах.

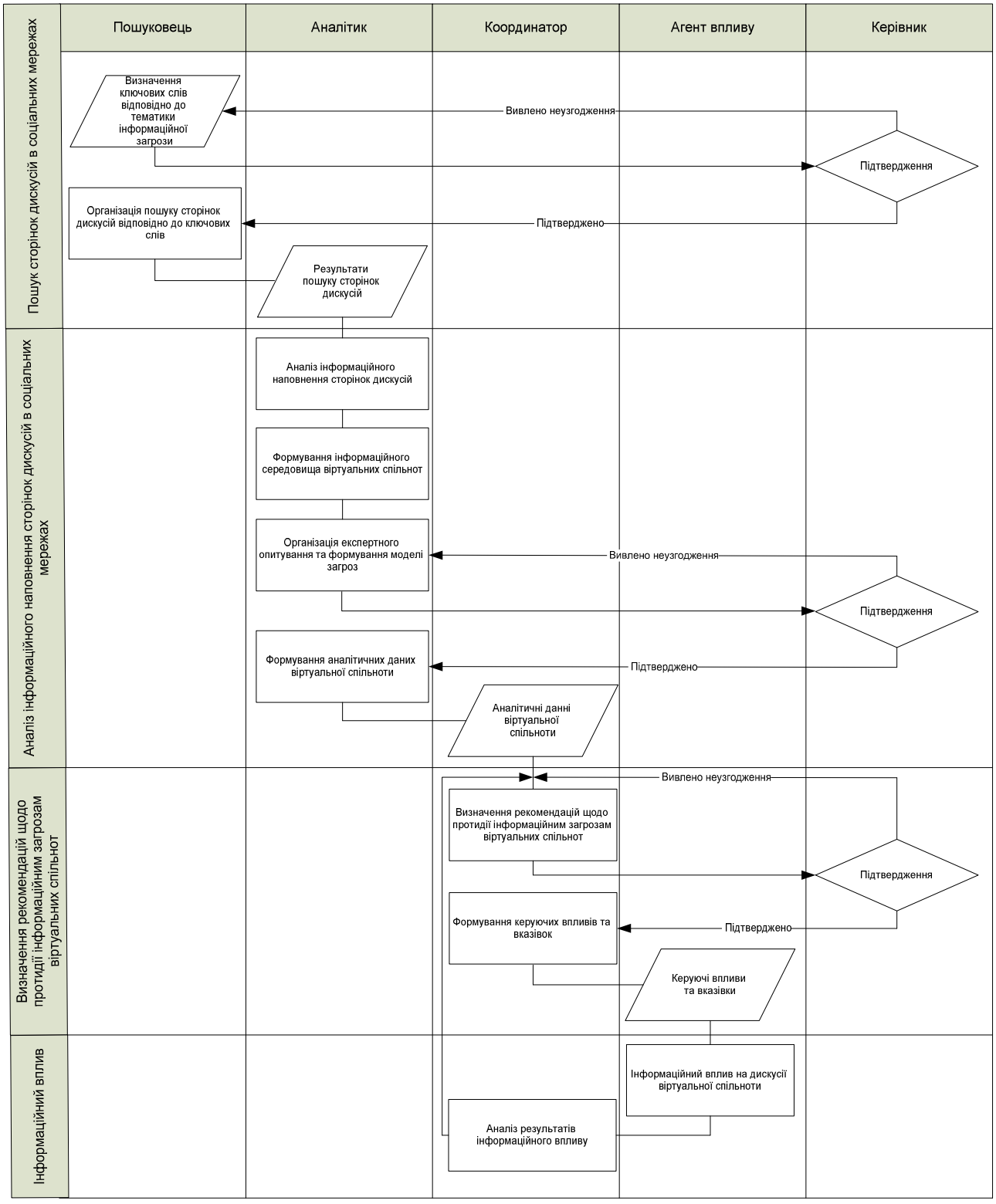

Рис. 4.5. Схема взаємодії фахівців на різних робочих місцях у процесі організації виявлення та протидії інформаційним загрозам віртуальних спільнот у соціальних мережах

4.4. Використання результатів результатів дисертаційних досліджень під час реалізації державної інформаційної політики

У відповідності до [48] одними з основних суб'єктів реалізації державної політики в сфері інформаційної безпеки є:

Служба безпеки України;

Міністерство оборони України.

При цьому одним із завданням у сфері інформаційної безпеки в [6] визначено: здійснення постійного моніторингу впливу на національну безпеку процесів, що відбуваються в інформаційній сфері.

Основними напрямами застосування результатів дисертаційних досліджень під час реалізації державної інформаційної політики є здійснення моніторингу та аналізу інформаційних загроз віртуальних спільнот в інтернет середовищі соціальних мереж, а саме:

– моніторинг соціальних мереж в інтернет середовищі з метою виявлення потенційних та реальних загроз інформаційній безпеці держави;

– визначення та організації інформаційних дій з метою реалізації державної інформаційної політики.

Для виконання наведених вище завдань використано такі результати дисертаційних досліджень:

– алгоритми пошуку сторінок дискусій в соціальних мережах з використанням розширених можливостей глобальних пошукових систем та API – запитів соціальних мереж;

– алгоритми формування інформаційного середовища віртуальних спільнот в соціальних мережах;

– визначення рекомендацій щодо прийняття рішення з протидії інформаційним загрозам віртуальних спільнот в соціальних мережах;

– алгоритм визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти в соціальних мережах;

– архітектура програмно-алгоритмічного комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот в соціальних мережах, функціональність якого основана на запропонованих у роботі методах та алгоритмах виявлення та протидії інформаційних загроз віртуальних спільнот в соціальних мережах.

Впровадження указаних результатів дисертаційної роботи дозволило підвищити ефективність процесів по виявленню та оцінки інформаційних загроз віртуальних спільнот в інтернет середовищі соціальних мереж, а саме:

– підвищення ефективності пошуку та формування інформаційного середовища віртуальних спільнот в соціальних мережах відповідно до їх інформаційного наповнення та напрямку тематики інформаційного наповнення;

формування обґрунтованих рекомендацій щодо прийняття рішення з протидії інформаційним загрозам та стратегій інформаційного впливу на структуру віртуальної спільноти в соціальних мережах.

Зазначені результати впроваджені у діяльність управління інформаційних технологій Міністерства оборони України та управління Служби безпеки України у Львівський області, що підтверджено відповідними актами впровадження (Додаток Б).

Висновки до розділу 4

У четвертому розділі розроблено архітектуру програмного комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах, описано основні складові системи, їхні функції та технічні аспекти реалізації. Для обліку даних інформаційного середовища віртуальних спільнот використано розширену базу даних, структура якої

ґрунтується на побудованій у другому розділі формальній моделі інформаційного середовища віртуальної спільноти.

Функціональність програмно-алгоритмічного комплексу підтримує виконання таких завдань:

- Пошук та облік віртуальних спільнот у соціальних мережах.
- Аналіз інформаційного наповнення сторінок дискусій віртуальних спільнот у соціальних мережах.
- Оцінка ступеня інформаційної загрози та визначення рекомендацій щодо протидії інформаційним загрозам віртуальних спільнот у соціальних мережах.

Основні результати розділу автором опублікував у роботах [20, 73, 81].

Висновки

У дисертаційній роботі розв’язано актуальну наукову задачу розроблення методів і засобів виявлення та оцінки інформаційних загроз віртуальних спільнот у соціальних мережах.

У роботі отримано такі основні наукові та практичні результати.

1. В результаті аналізу віртуальних спільнот в інтернет середовищі встановлено, що вони створюють нові загрози інформаційній безпеці держави. Дослідження сучасної теоретичної та практичної бази, систем та методів протидії деструктивному впливу в соціальних мережах показали неможливість виявлення та оцінки інформаційних загроз віртуальних спільнот в інтернет середовищі соціальних мереж. Таким чином, виникла необхідність щодо розробки методів і засобів виявлення та оцінки інформаційних загроз віртуальних спільнот в інтернет середовищі соціальних мереж.
2. Удосконалено модель віртуальної спільноти за допомогою розширення її до моделі інформаційного середовища віртуальної спільноти в соціальних мережах, що включає моделі зовнішнього та внутрішнього інформаційного середовища, яка стала основою для розроблення структури бази даних щодо обліку та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах.
3. Уведено показник інформаційної загрози віртуальної спільноти в соціальних мережах, шляхом визначення цінності віртуальної спільноти, що враховує структуру, кількість учасників та якість інформаційного наповнення сторінок дискусій віртуальної спільноти та став основої для методів щодо прийняття рішення з протидії інформаційним загрозам віртуальних спільнот у соціальних мережах та визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти в соціальних мережах.

4. Розроблено метод щодо прийняття рішення з протидії інформаційним загрозам віртуальних спільнот у соціальних мережах шляхом об’єднання показників інформаційної загрози, для яких визначення критичних цінностей віртуальної спільноти грунтується на встановленні експертами кількості учасників віртуальної спільноти, при якій реалізовується інформаційна загроза, та загальній кількості учасників деструктивної та конкурентної віртуальних спільнот, що дало змогу надати рекомендації щодо прийняття рішення з протидії інформаційним загрозам віртуальних спільнот у соціальних мережах.
5. Отримали подальший розвиток графові моделі соціальних мереж на основі матричного представлення графів, які завдяки врахуванню характеристик моделі інформаційного середовища віртуальної спільноти та запропонованого показника інформаційної загрози, що стали основою для розробки методу прийняття обґрунтованих рішень щодо вибору дискусій віртуальної спільноти для інформаційного впливу.
6. Розроблено архітектуру програмно-алгоритмічного комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот у соціальних мережах, функціональність якого грунтується на запропонованих у роботі методах та алгоритмах, що дає змогу організувати виявлення та оцінку інформаційних загроз віртуальних спільнот у соціальних мережах.
7. Розроблено стратегії протидії інформаційним загрозам віртуальних спільнот у соціальних мережах відповідно до правил протидії держави інформаційним загрозам віртуальних спільнот в соціальних мережах, що дало змогу вибору підходів щодо протидії інформаційним загрозам віртуальних спільнот у соціальних мережах.
8. Розроблено алгоритми пошуку сторінок дискусій у соціальних мережах з використанням розширених можливостей глобальних

пошукових систем та запитів API-методів соціальних мереж, які дають змогу виявити сторінки дискусій у соціальних мережах відповідно їх інформаційного наповнення.

9. Розроблено алгоритм формування інформаційного середовища віртуальних спільнот у соціальних мережах, шляхом застосування кластеризації сторінок дискусій у соціальних мережах відповідно до їх інформаційного наповнення та розподілу сторінок дискусій в залежності від напряму інформаційного наповнення для розподілу сторінок дискусій на деструктивну та конкурентну віртуальні спільноти.
10. Проведені експериментальні дослідження запропонованих методів і засобів, які підтвердили достовірність теоретичних і практичних результатів дисертаційної роботи щодо можливості виявляти та оцінювати інформаційні загрози віртуальних спільнот в інтернет середовищі соціальних мереж. Зазначені результати впроваджені у діяльність управління інформаційних технологій Міністерства оборони України та управління Служби безпеки України у Львівський області, що підтверджено відповідними актами впровадження.

Список літератури

1. Абрамов К. Г. К вопросу моделирования топологии социальной сети / К. Г. Абрамов, Ю. М. Монахов, И. Ю. Бодров // Труды V Всероссийской научн.-практ. конференции «Имитационное моделирование. Теория и практика» (ИММОД-2011), Санкт-Петербург (Россия), 19-21 окт. 2011 г. / ЮФУ. – Санкт-Петербург, 2011 – С. 11 – 14.
2. Адаськов О. І. Рекомендації щодо проведення інформаційних заходів в мережі Інтернет в інтересах виконання завдань інформаційно-психологічних операцій / О. І. Адаськов // збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2014. – Вип. 45. – С. 57 – 67.
3. Аксак В. А. Общение в сети Интернет. Просто как дважды два / В. А. Аксак. – М. : Эксмо, 2006. – 256 с.
4. Березко О. Л. WWW як соціальна мережа / О. Л. Березко, А. М. Пелещишин // Proc. of the Second Intern. Conf. on Computer Science and Engineering (CSE’2007). – Lviv, 2007. – P. 29–30.
5. Берж К. Теория графов и ее применение / пер. с фр. А. А. Зыкова под ред. И. А. Вайнштейна. – М.: Изд. иностр. литературы, 1962. – 319 с.
6. Брахман Т.Р. Многокритериальность и выбор альтернативы в технике. – М.: Радио и связь, 1984. – 288 с.
7. Бреер В. В. Стохастические модели социальных сетей / В. В. Бреер // Управление большими системами. Вып. 27. – М.: ИПУ РАН. – 2009. – С.169 – 204.
8. Вебер К. С. Сравнительный анализ социальных сетей / К. С. Вебер, А. А. Пименова // Вестник Тамбовского университета. Серия: естественные и технические науки. – 2014. – № 2 (19). – С. 634 – 636.
9. Висоцька В. А. Моделювання етапів життєвого циклу комерційного web-контенту / В. А. Висоцька, Л. Б. Чирун, Л. В. Чирун // Вісник

Національного університету "Львівська політехніка". – 2011. – № 715 : Інформаційні системи та мережі. – С. 69 – 87.

10. Віртуальні спільноти [Електронний ресурс]. – Режим доступу: WWW/URL: http://uk.wikipedia.org/wiki/Віртуальні_спільноти. – Назва з екрана.
11. Гнедаш А. А. Конструктивные и деструктивные социально-политические практики в online-пространстве современной России: «фейлы», «кейсы», «механики» / А. А. Гнедаш, Н. А. Рябченко // Человек. Сообщество. Управление. – 2014. – № 2. – С. 40 – 54.
12. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.
13. Григорук П.М. Метод побудови інтегрального показника / П.М. Григорук, Ткаченко І.С. // Бізнес Інформ. – 2012. – № 4. – С. 34 – 38.
14. Григорьев А. Н. InfoStream. Мониторинг новостей из Интернет: технология, система, сервис / А. Н. Григорьев, Д. В. Ландэ, С. А. Бороденков, Р. В. Мазуркевич, В. Н. Пацьора. – К.: ООО “Старт-98”, 2007. – 40 с.
15. Гриненко І. Вплив віртуальних спільнот на інформаційну безпеку: сучасний стан та тенденції розвитку / І. Гриненко, Д. Прокофьєва – Янчиленко // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – 2012. – № 1 (23). – С. 18 – 23.
16. Гриняев С. Н. Проблемы внутренней безопасности России в XXI веке / С. Н. Гриняев [Электронный ресурс]. – Режим доступу: http://www.agentura.ru/equipment/psih/info/inter/. – Загл. с экрана.
17. Губанов Д. А. Социальные сети: модели информационного влияния, управления и противоборства / Д. А. Губанов, Д. А. Новиков, А. Г. Чхартишвили; под ред. чл.-кор. РАН Д. А. Новикова. – М.: Издательство физико-математической литературы, 2010. – 228 с.

18. Губанов Д. А. Формальные и неформальные связи пользователей социальной сети facebook / Д. А. Губанов, А. Г. Чхартишвили // Материалы XII Всероссийского совещания по проблемам управления ВСПУ-2014, Москва, 16 – 19 июня 2014 г. / ВСПУ. – М, 2014 – С. 6301 – 6309.
19. Гумінський Р. В. Віртуальні спільноти, як суб'єкт інформаційної безпеки держави / Р. В. Гумінський // Захист інформації. – 2012. – № 3 (56). – С. 18 – 25.
20. Гумінський Р. В. Система розвідки та моніторингу інтернет середовища / Гумінський Р. В. / Проблемні питання розвитку озброєння і військової техніки: матеріали міжвідомчої наук.-техн. конференції, Київ, 17-20 груд. 2012 р. / ЦНДІ ОВТ. – Київ, 2012. – С. 217 – 218.
21. Гумінський Р. В. Методика прийняття рішення щодо протидії інформаційним загрозам віртуальних спільнот / Р. В. Гумінський // Східно-Європейський журнал передових технологій. – 2015. – № 2/2 (74). – С. 4 – 8.
22. 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.
23. Дзюндзюк В. Б. Віртуальні співтовариства: потенційна загроза для національної безпеки / В. Б. Дзюндзюк // Державне будівництво [Електронне видання]. – 2011. – № 1. – Режим доступу до журн. : http:// www.kbuapa.kharkov.ua. – Назва з екрана.
24. Додонов О. Г. Інформаційне суспільство: технології та безпека / О. Г. Додонов, О. С. Горбачик, М. Г. Кузнєцова // інформація та відкритість влади як засоби демократизації суспільства: зб. матеріалів «круглого столу». – К.: Альтпрес, 2003. – С. 119 – 124.

25. Додонов О. Г. Інформаційні потоки в глобальних комп'ютерних мережах / О. Г. Додонов, Д. В. Ланде, В. Г. Путятін. – К.: Наукова думка, 2009. – 295 с.
26. Додонов А. Г. Живучесть информационных систем / А. Г. Додонов, Д. В. Ландэ. – К.: Наукова думка, 2011. – 256 с.
27. Додонов А.Г. Конкурентная разведка в компьютерных сетях / А. Г. Додонов, Д. В. Ландэ, В. В. Прищепа, В. Г. Путятин. – К.: ИПРИ НАН Украины, 2013. – 248 с.
28. Додонов А. Г. Компьютерные сети и аналитические исследования / А. Г. Додонов, Д. В. Ландэ, В. Г. Путятин. – К.: ИПРИ НАН Украины, 2014. – 486 с.
29. Доктрина інформаційної безпеки України: проект: за станом на 1 квітня 2015 р. / [Електронний ресурс]. – Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025. – Назва з екрана.
30. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] / Совет Безопасности Российской Федерации. – 2000. – Режим доступа: http://www.scrf.gov.ru/documents/6/5.html. – Загл. с экрана.
31. Домарев В. В. Защита информации и безопасность компьютерных систем. – К.: ДиаСофт, 1999. – 480 с.
32. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. – К.: Диа Софт, 2002. – 688 с.
33. Домарева В. В. Безопасность информационных технологий. Системный поход. – К.: Диасофт, 2004. – 992 с.
34. Закон України «Про інформацію» від 2 жовтня 1992 р.: із змінами, внесеними Законом України від 2 грудня 2010 р. : за станом на 1 березня 2015 р. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2657-12/ed20110113. – Назва з екрана.

35. 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. – Назва з екрана.
36. Зыков А. А. Основы теории графов. – М.: Наука, Главная ред. физ.-мат. лит, 1987. – 384 с.
37. Ефимов Е. Г. Социальные интернет-сети (методология и практика исследования): монография / Е. Г. Ефимов / Волгоградский гос. тех. ун-т. – Волгоград, 2015. – 169 с.
38. Жарков Я.М. Інформаційна безпека особистості, суспільства, держави / Я. М. Жарков, М. Т. Дзюба, І. В. Замаруєв. – К. : Видавничо-поліграфічний центр «Київський університет», 2008. – 274 с.
39. Иванов Д. В. Виртуализация общества. Версия 2.0 / Д. В. Иванов. – С-Пб.: Петербургское востоковедение, 2002. – 224 с.
40. Интегральный показатель качества поиска [Электронный ресурс]. – Режим доступа: http://analyzethis.ru/?analyzer=summary&interval=year&lang=ru&location=en. – Загл. с экрана.
41. Князькова А. В. Параллельный алгоритм нахождения достижимостей в графе / А. В. Князькова, Т. В. Волченская, В. С. Князьков // Фундаментальные исследования. – 2014. – № 5 (часть 1). – С. 34 – 38. [Электронный ресурс]. – Режим доступа: URL: www.rae.ru/fs/?section=content&op=show_article&article_id =10003049. – Загл. с экрана.
42. Ковалевич Б. В. Соціальні мережі як новий інструмент ведення інформаційних війн у сучасному світі / Б. В. Ковалевич // Грані : наук.-теорет. і громад.-політ. альм. – 2014. – № 4 (108). – С. 118 – 121.
43. Коляда А. С. Достоверность идентификации авторства научных публикаций на основе латентно-семантического анализа / А. С. Коляда,

В. Д. Гогунский // Восточно-Европейский журнал передовых технологий. – Харків, 2014. – № 3/2 (69). – С. 36 – 40.

44. Кондратьев М. Е. Двухуровненвая иерархическая кластеризация новостного потока в РОМИП 2006 [Электронный ресурс] / М. Е. Кондратьев // Труди РОМИП. – 2006. – Режим доступа: http://romip.narod.ru. – Загл. с экрана.
45. Кондратьев М. Е. Анализ методов кластеризации новостного потока [Электронный ресурс] / М. Е. Кондратьев // Санкт-Петербургский государственный университет. – 2006. – Режим доступа: http://www.rcdl2006.uniyar.ac.ru/papers/paper_92_v1.pdf. – Загл. с экрана.
46. Конституція України : прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р. із змінами, внесеними Законом України від 21 лютого 2014 р. : за станом на 1 березня 2015 р. / [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/254к/96-вр. – Назва з екрана.
47. Конторович С. Д. Методика мониторинга и моделирования структуры политически активного сегмента социальных сетей [Электронный ресурс]. / С. Д. Конторович, С. В. Литвинов, В.И. Носко // Инженерный вестник Дона: электронный научный журнал «». – 2011. – № 4. – Режим доступа: URL: http://ivdon.ru/magazine/archive/n4y2011/642. – Загл. с экрана.
48. Концепція інформаційної безпеки України: проект: за станом на 8 червня 2015 р. / [Електронний ресурс]. – Режим доступу: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf. – Назва з екрана.
49. Кремлева С. О. Сетевые сообщества / С. О. Кремлева. [Электронный ресурс]. – Режим доступа: http://www.follow.ru/print.php?id=116&page=1. – Загл. с экрана.
50. Кримінально-процесуальний кодекс України : за станом на 1 грудня 2005 р. / Верховна Рада України. – Офіц. вид. – К. : Парлам. вид-во, 2006. – 207 с. – (Бібліотека офіційних видань).

51. Ландэ Д. В. Поиск знаний в Internet. Профессиональная работа. – М.: Диалектика, 2005. – 272 с.
52. Ландэ Д. В. Основы моделирования и оценки электронных информационных потоков: монографія / Д. В. Ландэ, В. Н. Фурашев, С. М. Брайчевский, А. Н. Григорьев. – К.: Инжиниринг, 2006. – 176 с.
53. Ландэ Д. В. Основы интеграции информационных потоков: монография. – К.: Инжиниринг, 2006. – 240 с.
54. Ландэ Д. В. Интернетика: Навигация в сложных сетях: модели и алгоритмы / Д. В. Ландэ, А. А. Снарский, И. В. Безсуднов. – М.: Книжный дом «ЛИБРИКОМ», 2009. – 264 с.
55. Ланде Д. В. Елементи комп'ютерної лінгвістики в правовій інформатиці / Д. В. Ланде. – К.: НДІІП НАПрН України, 2014. – 168 с.
56. Литвинова С. Г. Віртуальні спільноти у дослідженнях зарубіжних вчених / С. Г. Литвинова // Інформаційні технології і засоби навчання. – 2012. – № 5 (31). [Електронний ресурс]. – Режим доступу до журналу: http://www.journal.iitta.gov.ua. – Назва з екрана.
57. Манойло А. В. Государственная информационная политика в особых условиях: монография / А. В. Манойло. – М.: Изд. МИФИ, 2003. – 388 с.
58. Манойло А. В. Государственная информационная политика в условиях информационно-психологической войны: монография / А. В. Манойло, А. И. Петренко, Д. Б. Фролов. – М.: Горячая линия – Телеком, 2003. – 541 с.
59. Матвиенко Ю. А. Деструктивные сетевые социальные структуры как средство информационной войны и угроза безопасности России / Ю. А. Матвиенко // Информационно-аналитеческий портал «Геополитика» [Электронный ресурс]. – 2011. – Режим доступу до журн.: http://old.geopolitica.ru/Articles/1218. – Загл. с экрана.

60. Мелюхин И. С. Концепция управления деятельностью по формированию, использованию, ведению и защите информационной среды / И. С. Мелюхин; ВИНИТИ. – 1999. – 150 с.
61. Муратова Н. Ф. Интернет-СМИ как отдельный вид в системе средств массовой информации: лексическое и этимологическое обозначения понятия // Филологические науки. Вопросы теории и практики, – № 2 (6). – С. 118-120.
62. Описание методов API [Электронный ресурс]. Режим доступа: https://vk.com/dev/methods. – Загл. с экрана.
63. Орлов А. Ю. Организация виртуального сообщества в сети Интернет / А. Ю. Орлов // Информационные технологии. – 2008. – № 8. – С. 15 – 19.
64. Панченко Е. Интеграция Интернет-СМИ и социальных сетей в Рунете: Новая публичная сфера или пространство контроля? / Е. Панченко // Digital Icons: Studies in Russian, Eurasian and Central European New Media – 2011. – № 5. – С. 87 – 118.
65. Парето принцип [Електронний ресурс]. – Режим доступу: WWW/URL: http://uk.wikipedia.org/wiki/Принцип_Парето – Назва з екрана.
66. 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.
67. Пелещишин А. М. Веб 2.0 – другий шанс для Уанету [Електронний ресурс] / А. М. Пелещишин // Онлайн-журнал Наукового товариства ім. Т. Шевченка. – 2006. – Режим доступу: WWW/URL: http://ntsh.org/uaweb2 07.06.2007. – Назва з екрана.
68. Пелещишин А. М. Структурування інформаційного наповнення для покращення рангу веб-форуму / А. М. Пелещишин, Ю. О. Сєров // Східно-Європейський журнал передових технологій. – 2010. – № 68 (48). – С. 37 – 39.

69. 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. – 2011. – С. 212 – 221.
70. Пелещишин А. М. Процеси управління інтерактивними соціальними комунікаціями в умовах розвитку інформаційного суспільства: монографія / А. М. Пелещишин, Ю. О. Сєров, О. Л. Березко, О. П. Пелещишин, О. Ю. Тимовчак-Максимець, О. В. Марковець; за заг. ред. А. М. Пелещишина. – Львів: Видавництво Львівської політехніки, 2012. – 368 с.
71. Пелещишин А. М. Загрози інформаційної безпеки держави в соціальних мережах / А. М. Пелещишин, Р. В. Гумінський // Наука і техніка Повітряних Сил Збройних Сил України. – 2013. – 2(11). – С.192 – 199.
72. Пелещишин А. М. Пошук сторінок дискусій в соціальних мережах глобальними пошуковими системами / А. М. Пелещишин, Р. В. Гумінський, О. Ю. Тимовчак-Максимець // Безпека інформації. – 2013. – № 3 (19). – С. 181 – 187.
73. Пелещишин А. М. Системи моніторингу та протидії інформаційним загрозам у віртуальних спільнотах / А. М. Пелещишин, Р. В. Гумінський // «IV Січневі Гіси»: інтелектуальна оборона: зб. праць наук.-практ. форуму, Львів, 22-24 січ. 2013 р. / Академія Сухопутних військ. – Львів: АСВ, 2013. – С. 45 – 47.
74. Пелещишин А. М. Визначення інформаційної загрози процесу функціонування віртуальних спільнот / А. М. Пелещишин, Р. В. Гумінський // Новітні технології – для захисту повітряного простору: тези доповідей Дев'ятої наукової конференції Харківського університету Повітряних Сил імені Івана Кожедуба, Харків, 17-18 квіт. 2013 р. / Міністерство оборони України, Харківський університет Повітряних Сил. – Харків: ХУ ПС, 2013. – С.176.

75. Пелещишин А. Вибір складових показника інформаційної загрози процесу функціонування віртуальних спільнот / А. Пелещишин, Р. Гумінський // Інформація, комунікація, суспільство 2013 : матеріали 2-ї Міжнародної наукової конференції ІКС-2013, Львів, Славське, 16-19 трав. 2013 р. / Міністерство освіти і науки України, Національний університет "Львівська політехніка". – Львів : Видавництво Львівської політехніки, 2013. – С. 100 – 101.

76. Пелещишин А. М. Алгоритми пошуку сторінок дискусій в соціальних мережах глобальними пошуковими системами / А. М. Пелещишин, О. Ю. Тимовчак-Максимець, Р. В. Гумінський // Проблемні питання розвитку озброєння і військової техніки: матеріали IV наук.-техн. конференції, Київ, 16-20 груд. 2013 р. / ЦНДІ ОВТ. – Київ, 2013. – С. 184 – 185.

77. Пелещишин А. М. Вибір стратегії інформаційного впливу на інформаційне середовище віртуальної спільноти / А. М. Пелещишин, Р. В. Гумінський // 3rd International academic conference «Information, Communication, Society» ICS-2014, Львів, Славське, 19-21 трав. 2014 р. / Національний університет "Львівська політехніка". – Львів : Видавництво Львівської політехніки, 2014. – С. 30 – 31.

78. Пелещишин А. М. Оцінка інформаційних загроз процесу функціонування віртуальних спільнот / А. М. Пелещишин, Р. В. Гумінський // Безпека інформаційних технологій «ITSEC-2014»: матеріали IV міжнар. наук.-техн. конференції, Київ, 21-24 трав. 2014 р. / НАУ. – Київ, 2014. – С. 26 – 27.

79. Пелещишин А. М. Модель інформаційного середовища віртуальної спільноти / А. М. Пелещишин, Р. В. Гумінський // Східно-Європейський журнал передових технологій. – 2014. – № 2/2 (68). – С. 10 – 16.

80. Пелещишин А. М. Визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти / А. М. Пелещишин, Р. О. Корж, Гумінський Р. В. // Безпека інформації. – 2014. – № 3 (20). – С. 264 – 273.

81. 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.
82. Пелещишин О. П. Інформаційні технології обліку та пошуку онлайн-спільнот у задачі соціального маркетингу / О. П. Пелещишин // Вісник Національного університету “Львівська політехніка”. Серія економічна. – 2010. – № 44. – С. 50 – 59.
83. Пелещишин О. П. Аналіз та протидія загрозам маркетинговій позиції підприємства в онлайн-спільнотах / О. П. Пелещишин // Захист інформації. – 2013. – № 3 (15). – С. 217 – 224.
84. Петрик В. М. Сутність інформаційної безпеки держави, суспільства та особи / В. М. Петрик // Юридичний журнал. – 2009. – № 5. [Електронний ресурс]. – Режим доступу до журналу: http://www.journal.iitta.gov.ua. – Назва з екрана.
85. Подцероб А. Б. Арабская смута: роль пропаганды и современных информационных технологий / А. Б. Подцероб // Институт Ближнего Востока [Електронне видання]. – 2012. – Режим доступу до журн.: http://www.iimes.ru/?p=15619. – Загл. с экрана.
86. Почепцов Г. Контроль над разумом / Г. Почепцов. – К: ВД Києво-Могилянська академія, 2012. – 350 с.
87. Сєров Ю. О. Методи аналізу ефективності Веб-форумів / Ю. О. Сєров, Р. Б. Кравець, А. М. Пелещишин // Інформаційні системи та мережі : Вісник Національного університету «Львівська політехніка». – 2009. – № 653. – С.197 – 206.
88. Сєров Ю. О. Аналіз комунікативних процесів у Веб-спільнотах середовища Веб 2.0 / Ю. О. Сєров, А. М. Пелещишин, К. О. Слобода //

Східно-Європейський журнал передових технологій. – 2009. – № 1/2 (37). – С. 38 – 41.

89. Смирнов А. И. Глобальная безопасность в цифровую эпоху: стратагемы для России / А. И. Смирнов, В. Р. Григорьев, И. Н. Кохтюлин, Б. В. Куроедов, О. В. Сандаров. – М. : ВНИИ геосистем, 2014. – 394 с.
90. Смирнов Ф. О. Искусство общения в Интернет: краткое руководство / Ф. О. Смирнов. – М.: Вильямс, 2006. – 240 с.
91. Солтон Дж. Динамические библиотечно-информационные системы / пер. с англ. под ред. В. Р. Хисамутдинова. – М.: Мир, 1979. – 558 с.
92. Социальная сеть [Электронный ресурс]. – Режим доступа: WWW/URL: http://seopult.ru/library/Социальная_сеть. – Загл. с экрана.
93. Тимовчак-Максимець О. Ю. Методи використання розширених можливостей глобальних пошукових систем в задачі пошуку споживацького досвіду в онлайн середовищах / О. Ю. Тимовчак-Максимець // Вісник Національного університету “Львівська політехніка”: Інформаційні системи та мережі. – 2010. – № 689. – С. 323 – 331.
94. Тимовчак-Максимець О. Ю. Моделювання процесу обміну досвідом на веб-форумах шляхом аналізу розгортання дискусій / О. Ю. Тимовчак-Максимець // Вісник Національного університету "Львівська політехніка" : Інформаційні системи та мережі. – № 689. – 2010. – С. 323–331.
95. Тичер С. Методы анализа текста и дискурса / С. Тичер, М. Мейер, Р. Водак, Е. Веттер пер. с англ. – Х.: Гуманитарный Центр, 2009. – 356 с.
96. Филиппович Ю. Н. Семантика информационных технологий: опыты словарно-тезаурусного описания. / Ю. Н. Филиппович, А. В. Прохоров с пред. А. И. Новикова. – М.: Изд-во МГУП, 2002. – 368 с.
97. Фурашев В. Н. Моделирование информационно-электоральных процессов: монография / В. Н. Фурашев, Д. В. Ландэ, С. М. Брайчевский. – К.: НИЦПИ АпрН Украины, 2007. – 182 с.

98. 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.
99. Чекмышев О. А. Извлечение и использование данных из электронных социальных сетей / О. А. Чекмышев, А. Д. Яшунский. – М.: Институт прикладной математики им. М. В. Келдыша РАН, 2014. – 16 с.
100. Чхартишвили А. Г. Теоретико-игровые модели информационного управления / А. Г. Чхартишвили. – М. : ЗАО «ПМСОФТ», 2004. – 227 с.
101. Шарков Ф. И. Интерактивные электронные коммуникации / Ф. И. Шарков. – М.: Дашков и Ко, 2009. – 260 с.
102. Шрейдер Ю. А. Информационные процессы и информационная среда / Ю. А. Шрейдер. – С-Пб.: Символ-Плюс, 2000. –169 с.
103. Ярох А. І. Інформаційний простір та засоби масової інформації: концептуальна модель / А. І. Ярох // Вісник Харківського національного університету ім. В. Н. Каразіна. – 2011. – № 968. Сер.: Соціальні комунікації. – Вип. 3. – С. 30 – 34.
104. Briscoe B., Odlyzko A., Tilly B. Metcalfe's Law is Wrong [Electronic resourse]. – 2006. – Mode of access: http://spectrum.ieee.org/computing/networks/metcalfes-law-is-wrong. – Title from the screen.
105. Burnett G. Information exchange in virtual communities: a typology [Electronic resourse] // Information Research, Vol. 5 No. 4, – 2000. – Mode of access: http://www.informationr.net/ir/5-4/paper82.html. – Title from the screen.
106. Carley K., Lee J., Krackhardt D. Destabilizing networks // Connections, 2002. – Vol. 24. – №. 3. – P. 79 – 92.
107. Chakrabarti S. Mining the web. Discovery knowledge from hypertext data. – Publisher: Morgan Kaufmann. – 2002. – 344 p.
108. Collins, E. C., Percy, E. J., Smith, E. R., & Kruschke, J. K. Integrating advice and experience: Learning and decision making with social and non-social

cues // Journal of Personality and Social Psychology, 2011. – Vol. 100. – P. 967 – 982.

109. Connel M., Feng A., Kumar G., Raghavan H., Shah C. and Allan J., Umass at TDT2004. Proc. DARPA Topic Detection and Tracking Workshop, Gaithersburg, December 2004.
110. Cyber Security Strategy for Germany [Electronic resourse] / Federal Ministry of the interior. – 2011. – Mode of access: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile. – Last access: 2013. – Title from the screen.
111. Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space [Electronic resourse] // UK Cyber Security Operations Centre . – 2009. – Mode of access: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf . – Title from the screen.
112. Deerwester S., Dumais S. T., Furnas G. W., Landauer T. K., Harshman R. Indexing by Latent Semantic Analysis // Journal of the American society for information science. – 1990. – № 41(6). – P. 391 – 407.
113. Dinerman B. Social networking and security risks [Electronic resourse]. GFI White Paper – 2011. – Mode of access: www.gfi.com/whitepapers/Social_Networking_and_Security_Risks.pdf Last access: 2013.
114. Edosomwan J., Edosomwan T. Comparative analysis of some search engines [Electronic resourse] // South African Journal of Science. – 2010 Vol. 106 No. 11/12. – Mode of access: http://www.sajs.co.za/sites/default/files/publications/pdf/169-2706-8-PB.pdf. – Title from the screen.
115. Falls J. Why You Shouldn’t Trust Automated Sentiment Scoring [Electronic resourse]. – 2011. – Mode of access:

http://www.socialmediaexplorer.com/social-media-monitoring/trusting-automated-sentiment-scoring. – Title from the screen.

116. Finin T. Social networking on the semantic web / T. Finin, L. Ding, L. Zhou and A. Joshi // The Learning Organization Vol. 12 No. 5. – 2005 – P. 418 – 435.
117. Google Guide Quick Reference: Google Advanced Operators [Electronic resourse]. – Mode of access: http://www.googleguide.com/using_advanced_operators.html. – Title from the screen.
118. Gotta M. Risks & Benefits of More Open Social Networking [Electronic resourse] // Environmental Information Symposium "Enabling Environmental Protection through Transparency and Open Government", May 10 – 13, 2010 / United States Environmental Protection Agency. – 2010. – Mode of access: http://www.epa.gov/oei/symposium/2010/gotta.pdf. – Title from the screen.
119. Graph API Facebook [Electronic resourse]. – Mode of access: https://developers.facebook.com/docs/reference/api/. Last access: 2013. – Title from the screen.
120. Greengrass E., Information retrieval: A survey // DOD Technical Report TR-R52-008-001. – 2001. – p. 20.
121. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security United Nations General Assembly 24 June 2013 [Electronic resourse]. – Mode of access: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98. – Title from the screen.
122. Huminskyi R., Peleshchyshyn A. An assessment of informational threat in the functioning process of virtual community [Electronic resourse] // Cybernetic Letters, 2014. – Mode of access: http://www.cybletter.com. – Title from the screen.

123. Huminskyi R.V., Peleshchyshyn A.M. and Holub Z. Suggestions for Informational Influence on a Virtual Community // International Journal of Computer Science and Business Informatics, 2015. – Vol. 15. – No. 1, pp. 47 – 65.
124. Huminskyi R.V. Algorithm of search results clusterization / R. V. Huminskyi, O. M. Sovhar // Перспективи розвитку озброєння та військової техніки Сухопутних військ: матеріали міжнар. наук.-техн. конференції, Львів, 14-15 трав. 2015 р. / АСВ. – Львів, 2015. – С. 175 – 176.
125. Internet social networking risks [Electronic resourse] / U.S. Department of Justice Federal Bureau of Investigation. – Mode of access: http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1. – Title from the screen.
126. International strategy for cyberspace: Prosperity, Security, and Openness in a Networked World [Electronic resourse] // THE WHITE HOUSE WASHINGTON. – 2011. – Mode of access: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. – Title from the screen.
127. Koçak N. G. Social Networks and Social Network Analysis // International Journal of Business and Social Science. – 2014. – P. 126 – 135.
128. Kurt H. On-line new event detection and tracking in a multi-resource environment, MS. Thesis, Bilkent University, 2001.
129. Lawrence K. F., Schraefel M. C. Bringing Communities to the Semantic Web and the Semantic Web to Communities [Electronic resourse]. – 2006. – Mode of access: WWW/URL: http://www2006.org/programme/files/pdf/1083.pdf. – Title from the screen.
130. List of virtual communities with more than 100 million active users [Electronic resourse]. – Mode of access: http://en.wikipedia.org/wiki/List_of_virtual_communities_with_more_than_100_million_active_users. – Title from the screen.

131. Liu B. Web Data Mining: Exploring Hyperlinks, Contents, and Usage Data // Springer – 2011. – 622 c.
132. Mason W. A., Conrey F. R., & Smith E. R. Situating social influence processes: Dynamic, multidirectional flows of influence within social networks // Personality and Social Psychology Review. – 2007. – Vol. 11. – P. 279 – 300.
133. Newman M. E. J., Watts D. J., and Strogatz S. H. Random graph models of social networks [Electronic resourse]. PNAS. – 2002. – vol. 99. – Mode of access: www.pnas.org/content/99/suppl_1/2566.full.pdf. – Title from the screen.
134. Niekerk B., Pillay K., Mahara M. Analyzing the Role of ICTs in the Tunisian and Egyptian Unrest from an Information Warfare Perspective // International Journal of Communication. – 2011. – 5. – P. 1406 –1416.
135. Pang B., Lee L. Opinion Mining and Sentiment Analysis // Foundations and Trends in Information Retrieval. – //Now Publishers Inc. – 2008. – Vol. 2: No 1-2. – P. 1-135.
136. Powazek D. M. Design for community: the art of connecting real people in virtual places. – 2002. – 307 p.
137. Preece J. Online Communities: Designing Usability and Supporting Sociability. – Wiley. – 2000. – 464 p.
138. Reed D. P. That Sneaky Exponential: Beyond Metcalfe's Law to the Power of Community Building [Electronic resourse]. – 1999. – Mode of access: URL: http:/www. reed.com/gfn/docs/reedslaw.html. – Title from the screen.
139. Rijsbergen C. J. "Information Retrieval", Dept. of Computer Science, University of Glasgow. – 1979. – p. 224.
140. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. NIST, Special Publication 800 – 30 [Electronic resourse]. – Mode of access: http://csrc.nist.gov/publications/nistpubs/800. – Title from the screen.

141. Schultz J. M. and Liberman M., Topic Detection and Tracking using idf Weighted Cosine Coefficient. Proceedings of the DARPA Broadcast News Workshop, 189-192, 1999.
142. Security Tips for the Use of Social Media Websites [Electronic resourse] // Australian Government Department of defence. – Mode of access: http://www.asd.gov.au/publications/csocprotect/security_tips_for_using_social_media_websites.htm. – Title from the screen.
143. Simeonov S. Metcalfe's Law: more misunderstood than wrong? [Electronic resourse]. – 2006. – Mode of access: URL: http://blog.simeonov.com/2006/07/26/metcalfes-law-more-misunderstood-than-wrong/. – Title from the screen.
144. Smith, E. R. & Conrey F. R. Agent-based modeling: A new approach for theory-building in social psychology // Personality and Social Psychology Review. – 2007. – Vol. 11. – P. 87 – 104.
145. Smith, E. R. & Semin G. R. Situated social cognition // Current Directions in Psychological Science. – 2007. – Vol. 16. – P. 132 – 135.
146. Solton G., Wong A. and Yang C. S. A vector space model for automatic indexing. Com. Of the ACM. – 1975 – 18, №11. – P. 13 – 14.
147. Solton G., Allan J. and Buckley C. Approaches to passage retrieval in full text information systems. In ACM SIGIR conference on R&D in information Retrieval. – 1993. P. 49 – 58.
148. Stohl C., Stohl M. Networks of Terror: Theoretical Assumptions and Pragmatic Consequences // Communication Theory, 2007. – Vol. 17. – P. 93 – 124.
149. Timothy L. T. Information Security Thinking: A Comparison Of U.S., Russian, And Chinese Concepts // The Science and culture Series Nuclear Strategy and Peace Technology International Seminar on Nuclear War and Planetary Emergencies August 2001. – 2001. – pp. 344 – 358.
150. Toyoda M., Kitsuregawa M. Observing Evolution of Web Communities [Electronic resourse] // Proceedings of the 11th International World Wide Web

Conference. – 2002. – 4.C. – Mode of access: URL: http://www2002.org/CDROM/poster/161.pdf. – Title from the screen.

151. Turney P. Thumps up or thumbs down? Semantic orientation applied to unsupervised classification of reviews [Electronic resourse] // Proceedings of the 40th Annual Meeting of the Association for Computational Linguistics. – Philadelphia, 2002. – P. 417-424. – Mode of access : WWW/URL : http://www.aclweb.org/anthology-new/P/P02/P02-1053.pdf. – Title from the screen.
152. Wasserman S. and Faust K. Social Network Analysis: Methods and application. Cambridge University. – 1994. – p. 827.
153. Web community [Electronic resourse]. – Mode of access: URL:http://en.wikipedia.org/wiki/Web_community. – Title from the screen.
154. Yatsko V. A., Starikov M. S., Butakov A. V. Automatic genre recognition and adaptive text summarization // Automatic Documentation and Mathematical Linguistics. – 2010. – V44, №3. – P. 111–120.

Додатки

Додаток А. Результати розрахунків

Таблиця А.1.

Результати розрахунків для варіанта 1

Крок	Об'єкт ІВ	Кількість груп	Кількість ізольованих дискусій	Показник інформаційної загрози ВС	Зменшення показника інформаційної загрози:		
					разом	за рахунок руйнування структури ВС	за рахунок вилучення елементів ВС
0		1		0,723			
1	5	1	2	0,721	0,002	0,002	0,000
2	128	1	9	0,670	0,052	0,051	0,001
3	1	2	13	0,642	0,081	0,079	0,002
4	224	3	20	0,634	0,088	0,086	0,002
5	311	3	20	0,633	0,089	0,087	0,002
6	428	4	32	0,621	0,102	0,099	0,003
7	101	4	38	0,615	0,108	0,105	0,003
8	196	4	42	0,610	0,112	0,109	0,004
9	435	4	53	0,599	0,123	0,118	0,005
10	201	4	57	0,595	0,128	0,122	0,005
11	253	4	59	0,593	0,129	0,124	0,006
12	135	4	70	0,583	0,140	0,133	0,007
13	401	4	75	0,579	0,143	0,136	0,007
14	470	4	79	0,573	0,150	0,141	0,008
15	132	4	85	0,565	0,158	0,148	0,010
16	496	4	89	0,560	0,163	0,153	0,010
17	487	4	90	0,558	0,165	0,154	0,011
18	265	4	96	0,552	0,170	0,159	0,011
19	336	4	96	0,551	0,172	0,160	0,012
20	345	4	99	0,547	0,176	0,164	0,012
21	459	5	102	0,536	0,187	0,174	0,013
22	293	5	105	0,532	0,190	0,177	0,013
23	300	5	106	0,528	0,194	0,181	0,013
24	165	5	107	0,527	0,196	0,182	0,014
25	209	5	115	0,521	0,202	0,188	0,014
26	129	5	122	0,512	0,211	0,195	0,016

Крок	Об'єкт ІВ	Кількість груп	Кількість ізольованих дискусій	Показник інформаційної загрози ВС	Зменшення показника інформаційної загрози:		
					разом	за рахунок руйнування структури ВС	за рахунок вилучення елементів ВС
27	429	5	127	0,508	0,215	0,198	0,016
28	121	5	129	0,505	0,218	0,200	0,017
29	**398**	**5**	**136**	**0,498**	**0,224**	**0,206**	**0,018**

Таблиця А.2.

Результати розрахунків для варіанта 2

Крок	Об'єкт ІВ	Кількість груп	Кількість ізольованих дискусій	Показник інформаційної загрози ВС	Зменшення показника інформаційної загрози:		
					разом	за рахунок руйнування структури ВС	за рахунок вилучення елементів ВС
0		1		0,723			
1	5	1	2	0,721	0,002	0,002	0,000
2	230	1	7	0,714	0,008	0,007	0,001
3	278	1	11	0,708	0,016	0,014	0,002
4	218	1	12	0,707	0,028	0,014	0,002
5	152	1	12	0,695	0,026	0,014	0,004
6	187	1	12	0,696	0,026	0,014	0,005
7	204	1	12	0,697	0,025	0,014	0,006
8	227	1	12	0,698	0,025	0,014	0,006
9	224	2	18	0,689	0,034	0,023	0,011
10	209	2	25	0,682	0,040	0,029	0,011
11	144	2	28	0,678	0,044	0,032	0,012
12	253	2	30	0,677	0,046	0,034	0,012
13	300	2	32	0,672	0,050	0,037	0,013
14	165	2	34	0,670	0,053	0,039	0,014
15	270	2	35	0,668	0,055	0,041	0,014
16	176	2	35	0,668	0,055	0,041	0,014
17	170	2	39	0,664	0,059	0,045	0,014
18	181	2	41	0,660	0,063	0,048	0,015
19	214	3	41	0,618	0,105	0,089	0,016
20	196	3	45	0,613	0,110	0,093	0,017
21	246	3	47	0,611	0,111	0,094	0,017

Крок	Об'єкт ІВ	Кількість груп	Кількість ізольованих дискусій	Показник інформаційної загрози ВС	Зменшення показника інформаційної загрози:		
					разом	за рахунок руйнування структури ВС	за рахунок вилучення елементів ВС
22	139	4	48	0,605	0,117	0,099	0,018
23	293	4	48	0,602	0,120	0,102	0,019
24	173	4	51	0,600	0,122	0,103	0,019
25	265	4	58	0,594	0,128	0,109	0,019
26	435	4	68	0,576	0,147	0,126	0,021
27	249	5	70	0,571	0,152	0,131	0,021
28	110	6	70	0,553	0,170	0,148	0,022
29	401	6	75	0,550	0,173	0,151	0,022
30	496	6	80	0,544	0,178	0,156	0,023
31	470	6	83	0,538	0,185	0,162	0,023
32	487	6	84	0,534	0,189	0,166	0,023
33	336	6	84	0,534	0,188	0,164	0,024
34	345	6	87	0,530	0,192	0,168	0,024
35	459	7	90	0,519	0,204	0,179	0,025
36	82	8	95	0,510	0,212	0,187	0,025
37	429	8	101	0,507	0,216	0,190	0,026
38	311	8	102	0,506	0,217	0,191	0,026
39	428	8	114	0,494	0,228	0,202	0,026

Таблиця А.3.

Результати розрахунків для варіанта 3

Крок	Об'єкт ІВ	Кількість груп	Кількість ізольованих дискусій	Показник інформаційної загрози ВС	Зменшення показника інформаційної загрози:		
					разом	за рахунок руйнування структури ВС	за рахунок вилучення елементів ВС
0		1		0,723			
1	71	1	0	0,719	0,004	0	0,004
2	9	1	0	0,715	0,008	0	0,008
3	23	1	1	0,711	0,012	0,001	0,011
4	320	1	1	0,708	0,015	0,001	0,014
5	254	1	1	0,705	0,018	0,001	0,017

Крок	Об'єкт ІВ	Кількість груп	Кількість ізольованих дискусій	Показник інформаційної загрози ВС	Зменшення показника інформаційної загрози:		
					разом	за рахунок руйнування структури ВС	за рахунок вилучення елементів ВС
6	407	1	1	0,702	0,021	0,001	0,020
7	186	1	1	0,699	0,024	0,001	0,023
8	158	1	1	0,697	0,026	0,001	0,025
9	364	1	2	0,693	0,030	0,002	0,028
10	249	1	3	0,688	0,035	0,003	0,032
11	435	1	12	0,678	0,045	0,012	0,033
12	478	1	12	0,675	0,048	0,012	0,036
13	371	1	12	0,671	0,052	0,012	0,040
14	343	1	13	0,668	0,055	0,013	0,042
15	448	1	13	0,665	0,058	0,013	0,045
16	147	1	13	0,662	0,061	0,013	0,048
17	334	1	13	0,660	0,063	0,013	0,050
18	256	1	13	0,656	0,067	0,013	0,054
19	129	1	18	0,648	0,075	0,018	0,057
20	56	1	18	0,645	0,078	0,018	0,060
21	116	1	18	0,642	0,081	0,018	0,063
22	383	1	18	0,639	0,084	0,018	0,066
23	305	1	21	0,633	0,090	0,021	0,069
24	123	1	21	0,631	0,092	0,021	0,071
25	40	1	21	0,627	0,096	0,021	0,075
26	57	1	21	0,625	0,098	0,021	0,077
27	164	1	21	0,622	0,101	0,021	0,080
28	259	1	21	0,619	0,104	0,021	0,083
29	406	1	21	0,615	0,108	0,021	0,087
30	454	1	21	0,613	0,110	0,021	0,089
31	300	1	23	0,608	0,115	0,023	0,092
32	128	1	31	0,602	0,121	0,031	0,090
33	329	1	31	0,596	0,127	0,031	0,096
34	289	1	30	0,595	0,128	0,03	0,098
35	441	1	29	0,594	0,129	0,029	0,100
36	420	1	29	0,592	0,131	0,029	0,102
37	361	1	29	0,590	0,133	0,029	0,104
38	100	1	35	0,581	0,142	0,035	0,107
39	341	1	35	0,579	0,144	0,035	0,109
40	25	1	36	0,574	0,149	0,036	0,113

Крок	Об'єкт ІВ	Кількість груп	Кількість ізольованих дискусій	Показник інформаційної загрози ВС	Зменшення показника інформаційної загрози:		
					разом	за рахунок руйнування структури ВС	за рахунок вилучення елементів ВС
41	473	1	41	0,567	0,156	0,041	0,115
42	161	1	41	0,564	0,159	0,041	0,118
43	78	1	40	0,563	0,160	0,04	0,120
44	486	1	40	0,559	0,164	0,04	0,124
45	146	1	40	0,557	0,166	0,04	0,126
46	477	1	40	0,554	0,169	0,04	0,129
47	487	1	41	0,552	0,171	0,041	0,130
48	252	1	41	0,548	0,175	0,041	0,134
49	199	1	41	0,545	0,178	0,041	0,137
50	204	1	41	0,543	0,180	0,041	0,139
51	45	1	45	0,539	0,184	0,045	0,139
52	229	1	45	0,536	0,187	0,045	0,142
53	98	1	49	0,531	0,192	0,049	0,143
54	436	1	49	0,528	0,195	0,049	0,146
55	257	1	48	0,527	0,196	0,048	0,148
56	438	1	48	0,525	0,198	0,048	0,150
57	316	1	48	0,523	0,200	0,048	0,152
58	433	1	48	0,520	0,203	0,048	0,155
59	327	1	48	0,517	0,206	0,048	0,158
60	167	1	48	0,515	0,208	0,048	0,160
61	84	1	48	0,513	0,210	0,048	0,162
62	174	1	48	0,511	0,212	0,048	0,164
63	424	1	48	0,508	0,215	0,048	0,167
64	157	1	48	0,506	0,217	0,048	0,169
65	187	1	48	0,503	0,220	0,048	0,172
66	285	1	48	0,500	0,223	0,048	0,175

Додаток Б. Акти впровадження дисертаційних досліджень

«ЗАТВЕРДЖУЮ»
Начальник Академії сухопутних військ
імені гетьмана Петра Сагайдачного
доктор історичних наук, професор
генерал-лейтенант
П.П. ТКАЧУК
“ ” 2015р.

АКТ

реалізації результатів наукових досліджень старшого наукового співробітника науково-дослідного відділу (моделювання бойових дій) Наукового центру Сухопутних військ Академії сухопутних військ імені гетьмана Петра Сагайдачного підполковника Гумінського Руслана Вікторовича

Комісія у складі:

голови – заступника начальника Академії з наукової роботи кандидата історичних наук, доцента, полковника СЛЮСАРЕНКА А.В.

членів комісії – завідувача кафедри гуманітарних наук загальновійськового факультету доктора історичних наук, професора, працівника ЗС України ХАРУКА А.І., начальника науково-дослідної лабораторії (проблем інформаційно-психологічного протиборства) загальновійськового факультету підполковника ПАЗИНИ В.І., провідного наукового співробітника науково-дослідної лабораторії (проблем інформаційно-психологічного протиборства) загальновійськового факультету підполковника РУДКОВСЬКОГО В.Б.

ВСТАНОВИЛА: що результати дисертаційної роботи підполковника ГУМІНСЬКОГО Р.В. «Методи і засоби виявлення інформаційних загроз віртуальних спільнот в Інтернет середовищі соціальних мереж» використані при підготовці матеріалів до виконання науково-дослідної роботи "Основні напрямки роботи засобів масової інформації щодо протидії негативному

інформаційному впливу противника", шифр "ЗМІ" (№ державної реєстрації 0101u001889) в Академії сухопутних військ імені гетьмана Петра Сагайдачного.

Голова комісії:
Заступник начальника Академії з наукової роботи
кандидат історичних наук, доцент
полковник А.В. СЛЮСАРЕНКО

Члени комісії:
Завідувач кафедри гуманітарних наук
загальновійськового факультету
доктор історичних наук, професор,
працівник ЗС України А.І. ХАРУК

Начальник науково-дослідної лабораторії
(проблем інформаційно-психологічного
протиборства) загальновійськового факультету
підполковник В.І. ПАЗИНА

Провідний науковий співробітник науково-
дослідної лабораторії (проблем інформаційно-
психологічного протиборства)
загальновійськового факультету
підполковник В.Б. РУДКОВСЬКИЙ

«ЗАТВЕРДЖУЮ»
Начальник Управління СБУ
у Львівській області
генерал-майор
Андрейчук В. Г.

«22» травня 2015 р.

АКТ
про впровадження результатів дисертаційних досліджень
Гумінського Руслана Вікторовича

Комісія у складі:

голова комісії:	Кобилінський Володимир Михайлович
члени комісії:	Івануса Олександр Володимирович
	Мартинюк Роман Вікторович
	Овчаренко Антон Валерійович
секретар комісії:	Колупаєва Антоніна Альбертівна

склала цей акт про розгляд результатів дисертаційних досліджень Гумінського Р.В., а саме:

- формальна модель віртуальної спільноти за допомогою розширення її до моделі інформаційного середовища віртуальної спільноти в соціальних мережах;
- метод оцінки інформаційної загрози віртуальної спільноти в соціальних мережах;
- метод прийняття рішення по протидії інформаційним загрозам віртуальних спільнот в соціальних мережах;
- метод визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти в соціальних мережах;

є використаними для:

- побудови алгоритмів пошуку сторінок дискусій в соціальних мережах з використанням розширених можливостей глобальних пошукових систем та API – запитів соціальних мереж;
- побудови алгоритму формування інформаційного середовища віртуальних спільнот в соціальних мережах;
- визначення рекомендацій щодо прийняття рішення по протидії інформаційним загрозам віртуальних спільнот в соціальних мережах;
- побудови алгоритму визначення рекомендацій щодо інформаційного впливу на структуру віртуальної спільноти в соціальних мережах;
- побудови архітектури програмно-алгоритмічного комплексу моніторингу та аналізу інформаційних загроз віртуальних спільнот в

соціальних мережах, функціональність якого основана на запропонованих у роботі методах та алгоритмах виявлення та протидії інформаційних загроз віртуальних спільнот в соціальних мережах.

Впровадження указаних результатів дисертаційної роботи Гумінського Р.В. дозволило підвищити ефективність процесів по виявленню та протидії інформаційним загрозам віртуальних спільнот в Інтернет-середовищі соціальних мереж, а саме:

- підвищення ефективності пошуку та формування інформаційного середовища віртуальних спільнот в соціальних мережах відповідно до їх інформаційного наповнення та напрямку тематики інформаційного наповнення;
- формування обґрунтованих рекомендацій щодо прийняття рішення по протидії інформаційним загрозам та стратегій інформаційного впливу на структуру віртуальної спільноти в соціальних мережах.

голова комісії: _____ Кобилінський В. М.

члени комісії: _____ Івануса О. В.

_____ Мартинюк Р. В.

_____ Овчаренко А. В.

секретар комісії: _____ Колупаєва А. А.

№ 62/30-1269

ЗАТВЕРДЖУЮ
Начальник Управління інформаційних технологій Міністерства оборони України
полковник К.О. СОКОЛОВ
“ 15 ” 05 2015 року

А К Т
про реалізацію результатів наукових досліджень старшого наукового співробітника Наукового центру Сухопутних військ Академії Сухопутних військ ім. П.Сагайдачного
підполковника ГУМІНСЬКОГО Руслана Вікторовича

Комісією Управління інформаційних технологій Міністерства оборони України у складі: голови комісії – заступника начальника Управління інформаційних технологій Міністерства оборони України кандидата технічних наук, доцента полковника Крижанівського О.А. та членів комісії: начальника відділу інформаційних ресурсів Управління інформаційних технологій Міністерства оборони України кандидата технічних наук, старшого наукового співробітника полковника Гудима О.П., старшого офіцера відділу інформаційної політики Управління інформаційних технологій Міністерства оборони України кандидата технічних наук, доцента полковника Раєвського В.М. проведено вивчення результатів дисертаційної роботи за темою “Методи і засоби протидії інформаційним загрозам віртуальних спільнот в соціальних мережах”.

За результатами розгляду та вивчення наданих матеріалів комісія встановила:

Основними науковими та практичними результатами роботи, отриманими підполковником Гумінським Р.В. є:

аналіз віртуальних спільнот в соціальних мережах, як суб’єктів інформаційної загрози держави;

побудова математичних моделей інформаційного середовища віртуальної спільноти та визначення характеристик віртуальних спільнот в соціальних мережах;

формування показника інформаційної загрози віртуальної спільноти на підставі визначених характеристик;

розроблення методів та алгоритмів виявлення та протидії інформаційним загрозам віртуальних спільнот в соціальних мережах.

ВИСНОВОК:

Результати наукових досліджень використані в процесі реалізації Концепції забезпечення інформаційної безпеки Міністерства оборони України та Збройних Сил України; для моніторингу інформаційного простору з метою виявлення потенційних та реальних загроз інформаційній безпеці держави у воєнній сфері та прогнозування наслідків їхньої реалізації; при підготовці та проведенні службових нарад в Міністерстві оборони України з питань оцінювання стану інформаційної безпеки держави в умовах протидії інформаційній кампанії Російської Федерації проти України, визначення та організації інформаційних дій Міністерства оборони України та Збройних Сил України з метою реалізації державної інформаційної політики у воєнній сфері, інформаційної підтримки дій військ (сил) Збройних Сил України в антитерористичній операції.

Голова комісії:

к.т.н., доцент полковник О.А. КРИЖАНІВСЬКИЙ

Члени комісії:

к.т.н., с.н.с. полковник О.П.ГУДИМА

к.т.н., доцент полковник В.М. РАЄВСЬКИЙ