Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

ДИПЛОМНА РОБОТА МАГІСТРА

Метод протидії та виявлення в соціальних мережах шкідливої інформації
Назва теми

Галузь знань 12 – Інформаційні технології

Спеціальність 123 –Комп'ютерна інженерія

ДРКІ. 170144.21.01.04 ПЗ

Виконав: студент 2 курсу, група КІ1м-21-1 _____ Зацепіна О.О.
Підпис

Керівник доц., к. т. н, доцент кафедри КБ _____ Тітова В.Ю.
Підпис

Нормоконтролер ст. викладач кафедри КБ _____ Мостовий С.В.
Підпис

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

7 12 2022р.

Хмельницький, 2022

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра КІБЕРБЕЗПЕКИ
Освітній рівень МАГІСТР
Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ
Освітня програма ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ МАГІСТРА

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
к.т.н. доцент Кльоц Ю.П.
"5" 09 2022 року

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ)

Зацепіна Орислава Олександрівна
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Метод протидії та виявлення в соціальних мережах шкідливої інформації
Науковий керівник Тітова Віра Юріївна, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджена наказом №83 ректора університету додаток №25 від 01.07 .2022
2. Строк подання студентом проекту (роботи) на кафедру 05.12.2022.
3. Вихідні дані до проекту (роботи) Провести дослідження сучасного стану протидії та виявлення в соціальних мережах шкідливої інформації з метою визначення та обгрунтування оптимальної структури системи протидії, алгоритмів проведення оцінки в соцмережах джерел інформації. Розробити моделі та алгоритми дослідження соціальних мереж, джерел шкідливої інформації. Розробити метод виявлення та протидії в соцмережах шкідливої інформації. Розробити архітектуру системи виявлення та протидії в соціальних мережах шкідливої інформації.
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Дослідження сучасного стану протидії та виявлення в соціальних мережах шкідливої інформації. Моделі системи протидії: соціальної мережі, джерела та шкідливої інформації в мережі Інтернет. Алгоритми протидії та виявлення в соціальних мережах шкідливої інформації. Метод протидії та виявлення в соціальних мережах поширенню шкідливої інформації.
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень) 1,2.Тема, мета магістерської роботи, об'єкт, предмет, задачі дослідження, наукова новизна, практична цінність, апробація роботи. 3. Моделі комунікації протидії та виявлення в соціальних мережах шкідливої інформації. 4. Алгоритми моніторингу та протидії поширенню шкідливої інформації у процесі обробки мережевого контенту в соцмережах. 5. Концептуальна модель системи виявлення та протидії поширенню шкідливої інформації у соцмережах. 6. Ранжування джерел повідомлень соціальних мережі. 7. Алгоритм ранжування джерел повідомлень за потенціалом. 8. Метод протидії в соціальних мережах поширенню та виявлення шкідливої інформації. 9. Метод протидії в соціальних мережах поширенню та виявлення шкідливої інформації на стадії експлуатації. 10. Архітектура системи протидії
шкідливій інформації в соціальній мережі. 11.Висновки.

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання при
Відповідальний за оформлення ДП	Мостовий С.В., ст. викладач		

7. Дата видачі завдання: «01» лютого 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітк
1	Ґрунтовне ознайомлення та дослідження предметної галузі	21.02.2022	Викон
2	Визначення змісту, структури магістерської роботи	11.03. 2022	Викон
3	Опрацювання першого розділу магістерської роботи	4.04. 2022	Викон
4	Опрацювання статті за результатами дослідження	3.05. 2022	Викон
5	Опрацювання другого розділу магістерської роботи	2.06. 2022	Викон
6	Опрацювання третього розділу магістерської роботи	2.09. 2022	Викон
7	Опрацювання четвертого розділу магістерської роботи	4.10. 2022	Викон
8	Підготовка та опрацювання ілюстративного матеріалу	7.11. 2022	Викон
9	Оформлення магістерської роботи графічної та текстової частини	18.11. 2022	Викон
10	Попередній захист магістерської роботи	25.11. 2022	Викон
11	Захист магістерської роботи на засіданні ЕК	5.12. 2022	Викон

Студент _____ О.О. Зацепіна
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ В.Ю. Тітова
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема дипломної роботи: «Метод протидії та виявлення в соціальних мережах шкідливої інформації».

Автор роботи: студент групи КП1м – 21 – 1 Зацепіна О.О.

Керівник роботи: к.т.н. доц. Тітова В.Ю.

Пояснювальна записка: 76 с., 26 рисунків., 7 таблиць., 31 джерело.

Перелік ключових слів: моделі, алгоритми, соціальні мережі, шкідлива інформація, контрзаходи.

Мета роботи полягає в підвищенні ефективності виявлення та протидії поширення в соціальних мережах шкідливої інформації за рахунок проведення аналізу та дослідження джерел шкідливої інформації в мережі та автоматизації вибору адекватних контрзаходів.

Запропоновані моделі, алгоритми, архітектура системи виявлення та протидії в мережі поширення шкідливої інформації можуть бути використані як окрема складова системи підтримки прийняття рішень на користь протидії шкідливій інформації в соцмережі оператором. Запропонований підхід до вирішення завдач, пов'язаних з аналізом та виявленням в соціальних мережах джерела шкідливої інформації, а також повязаних з протидією інформації та її джерелом, дозволяє формулювати адекватні науково-обгрунтовані вимоги.

29.11.2022р

ANNOTATION

Theme of thesis: "Method of combating and detecting harmful information insocial networks".

The author of the work: a student of the group KI1m - 21 - 1 Zatsepina O.O.

Head of work: candidate of technical Sciences, associate Professor Titova V.Yu.

Explanatory note: 76 p., 26 figures, 7 tables, 31 sources.

List of keywords: models, algorithms, social networks, malicious information,countermeasures.

The purpose of the work is to increase the effectiveness of detecting and countering the spread of malicious information in social networks by analyzing and researching the sources of malicious information in the network and automating the selection of adequate countermeasures.

The proposed models, algorithms, architecture of the system of detection and countermeasures in the network of spreading maliciousinformation can be used as a separate component of the decision-making support system in favor of countering malicious information in the social network by the operator. The proposed approach to solving tasks related to the analysis and identification of the source of harmful information in social networks, as well as relatedto countering information and its source, allows for the formulation of adequate scientifically based requirements.

29.11.2022р

ЗМІСТ

ВСТУП

На сучасному етапі, глибина проникнення у повсякденне життя соціальних мереж є значною, перевагою соціальних мереж є можливість учасників комунікації висловлювати оперативно свою думку значній кількості групі людей, публікувати відео-, медіа файли. На сучасному етапі соціальні мережі є не лише засобом спілкування групи людей, а й також інструментом поширення інформації, в тому числі шкідливої інформації. Таким чином, очевидною проблемою інформаційної безпеки теперішнього суспільства, сьогодення стала шкідлива інформація. Необхідно зазначити, що злочинні та терористичні угрупування беруть на озброєння, дедалі частіше засоби інформаційного впливу, розробляють та пишуть стратегії, спрямовані на залучення нових адептів та розширення сфери впливу через соціальні мережі. Таким чином, однією зі складових надійного забезпечення інформаційної безпеки держави є виявлення, моніторинг, аналіз та активна протидія розповсюдженню шкідливої інформації в соціальних мережах.

На сучасному етапі до шкідливої інформації поширеної в соціальних мережах частіше відносять «фейкові новини». Особливо гостро стоїть необхідність протидії поширенню у соціальних мережах таких новин, що породжують хвилі паніки, що виникають під час пандемії. На теперішній час – війна в Україні. Фейкові новини поширюються у соціальних мережах у шість разів швидше, ніж правдиві дописи. Російська пропаганда стала одним з головних елементів війни в Україні, її якісно закамуфльовано під вигляд матеріалів західних ЗМІ - DW, CNN або BBC.

На теперішній час проблема виявлення та протидії поширенню у соціальних мережах шкідливої інформації, в тому числі «фейкових новин», має недостатньо науково-технічних рішень. Відомі підходи та засоби протидії та виявлення в соцмережах шкідливої інформації не відповідають відповідним вимогам до повноти, швидкості, адекватності та точності прийнятих рішень. Дана ситуація зумовлена кількома причинами: системи розділені на два не пов'язаних модулі –

протидія, моніторинг, між якими знаходиться оператор; соціальні мережі складаються з множини різнорідних повідомлень і мають складну структуру, дана особливість не в повній мірі враховується при виборі мети протидії – джерело, тип повідомлення, а також інші характеристики; необхідно обробляти надвеликі об’єми інформації в реальному масштабі часу і в стислий термін вибирати відповідний інструмент для контрзаходу, оператор системи протидії в ручному режимі не в змозі зупинити поширення шкідливої інформації в соцмережі.

На сьогодні, основна складність виявлення та протидії шкідливої інформації в соцмережах безпосередньо слідує із використанням на даному етапі тенденцій розвитку інформаційно - технологічної сфери, а саме: збільшення швидкості поширення шкідливої інформації в соцмережах; об’єму інформації, що містить шкідливу інформацію; швидкості виникнення нових джерел поширення шкідливої інформації в соцмережах; швидкості тиражування повідомлень в мережі; рівня гетерогенності даних; кількості сценаріїв привернення уваги аудиторії. Таким чином розглянуті тенденції поширення шкідливої інформації зумовлює необхідність підвищення ефективності виявлення та протидії в соціальних мережах шкідливої інформації, враховуючи також обґрунтованість та оперативність.

Проведений аналіз та дослідження оцінювання ефективності інформаційних систем та інформатизації процесів, показали, що проблема виявлення та протидії в соціальних мережах шкідливої інформації не може вважатися вирішеною і вимагає на даному етапі проведення нових досліджень.

Мета магістерської роботи - підвищення ефективності виявлення та протидії поширення в соціальних мережах шкідливої інформації за рахунок проведення аналізу та дослідження джерел шкідливої інформації в мережі та автоматизації вибору адекватних контрзаходів.

Для досягнення поставленої мети в роботі вирішено наступні задачі: аналіз існуючих моделей поширення в мережі шкідливої інформації та інформаційного обміну; аналіз існуючих методик та систем моніторингу виявлення та протидії в

соціальних мережах шкідливої інформації; аналіз алгоритмів проведення оцінки в соцмережах джерел інформації; розробка моделей та алгоритмів аналізу соцмереж, джерела шкідливої інформації; розробка методу виявлення та протидії в соцмережах шкідливої інформації; розробка архітектури системи виявлення та протидії в соціальних мережах шкідливої інформації.

Наукова задача. Розробка моделей, алгоритмів, методу виявлення та протидії в соцмережах поширення шкідливої інформації.

Об'єкт дослідження. Соціальні мережі, у яких можлива наявність поширення інформації із шкідливою інформацією («фейкові новини») та їх джерела.

Предмет дослідження. Моделі, алгоритми, методи виявлення та протидії в соцмережах шкідливої інформації.

Наукова новизна:

1. Моделі шкідливої інформації, джерела повідомлень, соціальної мережі. Враховують в соціальній мережі структуру шкідливої інформації, інформаційних об'єктів та потоку інформаційного обміну на основі використання запропонованої класифікації в соцмережі інформаційних об'єктів. Модель шкідливої інформації в соцмережі, заснована на ознаках шкідливої інформації та взаємопов'язаних об'єктів, результатом якої є шкідливо-інформаційні об'єкти.

2. Метод виявлення та протидії в соціальних мережах шкідливої інформації - орієнтований на автоматизований вибір заходів виявлення та протидії шкідливої інформації в соцмережах зі списку контрзаходів та об'єктів впливу.

Практична цінність роботи. Запропоновані моделі, алгоритми, архітектура системи виявлення та протидії в мережі поширення шкідливої інформації можуть бути використані як окрема складова системи підтримки прийняття рішень на користь протидії шкідливій інформації в соцмережі оператором. Запропонований підхід до вирішення завдач, пов'язаних з аналізом та виявлення в соціальних мережах джерела шкідливої інформації, а також повязаних з протидією інформації та її джерелом, дозволяє формулювати адекватні науково-обґрунтовані вимоги.

Методи дослідження. Для вирішення задач поставлених у магістерській роботі застосовувалися методи дослідження: системний та порівняльний аналіз; аналіз науково-технічної інформації про предметну область та систематизація - дозволили створити відповідні моделі; структурний синтез та об'єктно-орієнтований підхід - для оцінки джерел, проектування та розробки алгоритмів аналізу; експертні оцінки, методи ранжування - запропоновано метод виявлення та протидії поширення в соцмережах шкідливої інформації, архітектуру системи протидії в соцмережах шкідливій інформації.

Положення, що виносяться на захист: моделі шкідливої інформації, джерела та соціальної мережі; алгоритми ранжування контрзаходів та аналізу походження в соцмережах джерел шкідливої інформації; метод виявлення та протидії поширенню в соцмережах шкідливої інформації; архітектура системи виявлення та протидії поширенню шкідливої інформації в мережах.

Обгрунтованість та достовірність результатів дослідження забезпечується ретельним аналізом стану досліджень, коректним використанням математичного апарату, підтверджується, отриманих при експериментальних дослідженнях узгодженістю результатів, апробацією основних положень роботи на наукових конференціях, публікацією основних результатів, у провідних наукових виданнях.

Особистий внесок. Дослідження, викладені в роботі, проведені автором при виконанні магістерської роботи в процесі наукової діяльності. Результати роботи, які виносяться на захист, отримані автором особисто, запозичений матеріал, використаний в роботі, позначений посиланнями.

Апробація роботи. За темою дипломної роботи ОКР «Магістр» опубліковано 1 теза доповідей, 1 фахова стаття.

Структура і обсяг роботи. Дипломна робота ОКР «Магістр» складається зі вступу, основної частини, що містить 4 розділи, висновків і списку використаних джерел. Загальний обсяг роботи - 75 сторінок. Робота містить 26 рисунків та 7 таблиць. Список використаної літератури включає 29 бібліографічних джерела.

1 ДОСЛІДЖЕННЯ СУЧАСНОГО СТАНУ ПРОТИДІЇ ТА ВИЯВЛЕННЯ В СОЦІАЛЬНИХ МЕРЕЖАХ ШКІДЛИВОЇ ІНФОРМАЦІЇ

1.1 Проблеми і задачі протидії та виявлення в соціальних мережах шкідливої інформації

На сучасному етапі залишається відкритим питання, як в інформаційному полі розпізнати шкідливу інформацію, як державі протидіяти окремим соціальним викликам (підлітковий та дитячий суїцид), як захистити суспільство від панічних настроїв у період змін і глобальних катастроф, можливим кольоровим революціям? Удосконалення систем виявлення та протидії поширенню шкідливої інформації в мережах з боку держави, організацій, особистості може дати в даній ситуації дійові результати.

Конфлікти та процеси в інформаційному полі держави - відображення активності суб'єктів діяльності: інституційні, групові актори чи індивідуальні. Таким чином спостерігаємо зворотну тенденцію, коли процеси та конфлікти в інформаційному полі держави можуть породжувати конфлікти та події, що безпосередньо впливають на соціальну активність людей, їх життєвий шлях та захоплення, змінюють, при цьому, суспільство в цілому. Процеси, що породжують зміни стану безпеки суспільства та держави протікають у прихованій формі і результат впливу на інформаційне поле особистості, суспільства, держави виявляємо лише в момент її кульмінації, коли процес чи конфлікт відбивається у економіці держави, політичному дискурсі, здоров'я та життя особистості, суспільства.

Необхідно зазначити, нещодавні соціальні та технічні зміни в галузі інформаційної безпеки суспільства були відносно повільними і держава, шляхом оновлень вимог до гравців ринку послуг контенту та телекомунікацій могла до них пристосовуватися. На теперішній час швидкість змін в інформаційному полі суспільства є досить великою, а уповільнена та невірна реакція з боку органів

безпеки держави може призвести до катастрофи суспільства. Адаптація до змін в інформаційному полі держави, потребує на сучасному етапі значних і швидких коригувань у сфері захисту інформаційного поля держави. Необхідно бути більш здатним краще протидіяти та відновлюватися після кризи, більш обізнаними щодо характеру та потенціалу кризових ситуацій.

Аналіз результатів досліджень робіт в даній області показав, що вони здебільшого спрямовані на аналіз кількісних, якісних характеристик зв'язків пристроїв у соцмережах, систематизацію, кластеризацію отриманих даних, моніторинг інцидентів інформаційної безпеки, на забезпечення інформаційно-технічних, нормативно-правових аспектів інформаційної безпеки в просторі суспільства.

Шкідлива інформація, в сучасному науковому співтоваристві, сприймається як елемент інформаційного впливу (атаки). Інформаційний вплив (information effect IE) - вражаючий основний фактор інформаційної війни, дія інформаційним потоком на об'єкт атаки – компонент, інформаційну систему, з метою викликати в об'єкті, в результаті обробки та прийому інформаційного потоку, задані функціональні та структурні зміни [1, 2].

Формально інформаційний вплив можна визначити наступним чином:

$$R = IW\left(IO\right), \tag{1.1}$$

де IW – інформаційний вплив, IO – інформаційний об'єкт, R – результат. Інформаційний об'єкт – це логічно цілісний блок повідомлення, представлений у певній фіксованій формі, який використовується та створений в ході складової інформаційної діяльності суспільства [3].

Формально зв'язок інформаційного об'єкта з іншими поняттями представляється так: $IO \in I$, інформаційний об'єкт є елементом множини інформації, що аналізується I. Мережа Інтернет (INT) містить «небезпечну» інформацію RI та «безпечну» SI : $Int = RI + SI$. Множина небезпечної інформації

містить шкідливу (*HI*), небажану (*UI*), сумнівну (*DI*) інформацію. На рис. 1.1 представлено модель небезпечної інформації.

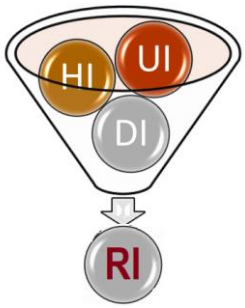


Рисунок 1.1 – Модель небезпечної інформації у мережі Інтернет

Класифікація інформації в Інтернет-мережі заснована на понятті інформаційного об'єкта (*IO*) - логічно цілісний блок повідомлення, представлений у фіксованій формі, використовуваний та створений у ході складової інформаційної діяльності суспільства.

Шкідлива інформація –інформаційний об'єкт (сукупність об'єктів) в Інтернет мережі, що містить обмежену (заборонену) для поширення інформацію. Шкідлива інформація включає множину небезпечної інформації.

Під категорію шкідливої інформації, з погляду забезпечення державної безпеки потрапляють наступні види інформації: інформація, включена до державного списку екстремістських матеріалів [4]; інформація, що ідентифікується як заборонена до поширення в державі [5]; персональні дані; інформація для службового користування; конфіденційна інформація.

Забороняється поширення інформації в Інтернет мережі, спрямованої на пропаганду війни, розпалювання релігійної, національної, расової ненависті та ворожнечі, інформацію, за поширення якої передбачено адміністративну, кримінальну відповідальність [8].

Поширення інформації – дії, створені для передачі та отримання інформації невизначеним колом користувачів. Повідомлення –інформаційний об'єкт, що містить текст, опублікований та створений у процесі інформаційного обміну у

соцмережі Інтернет. Джерело - сторінка в соціальній мережі Інтернет, на якій опублікована та надана інформація доступна невизначеному колу користувачів.

Можна виділити дві основні концепції класифікації шкідливої інформації в соцмережах.

Класифікація за дискретними ознаками інформаційних об'єктів [5,6]: час повідомлень; дата реєстрації у соціальній мережі; частота повідомлень; частота дій; довжина повідомлень; зв'язок з іншими учасниками у соцмережі; зв'язок із спільнотами; географія профілю; унікальність контенту на сторінці профілю у соцмережі Інтернет; географія спільнот, з якими пов'язаний профіль; кількість переглядів; інтереси профілю; ступінь впливу.

Класифікація інформаційних об'єктів за змістом [6,7]: виправдання, пропаганда екстремізму та тероризму; пропаганда, виправдання війни; пропаганда расизму; пропаганда, виправдання правопорушень; пропагування релігійної ненависті; пропаганда національної ненависті; осквернення, образу державних символів; образа, осквернення символів військової слави, історичної пам'яті; виправдання жорстокості, насильства; образу релігійних почуттів віруючих; пропагування нетрадиційних, деструктивних цінностей, установок; свідомо неправдива інформація; виправдання, пропаганда дій небезпечних життю людини; інформація, що містить відомості про виготовлення забороненого; наклеп; сексуально відвертий контент; рекламні оголошення про продаж, купівлю заборонених товарів

Залежно від задачі та мети протидії розробляються, змінюються моделі, методи, алгоритми, використовуються різні архітектури систем виявлення та протидії поширенню шкідливої інформації в соціальних мережах. На сучасному етапі постає питання підвищення ефективність протидії поширенню шкідливої інформації в соцмережах Інтернет.

1.2 Дослідження моделей, архітектур систем протидії та виявлення в соціальних мережах шкідливої інформації

Комунікація - навмисна дія джерела, яка виконується для досягнення певного результату. Для визначення ролі та місця системи виявлення та протидії шкідливої інформації в соціальних Інтернет мережах необхідно визначити, що представляє собою джерело в рамках інформаційного обміну в соцмережах, як відбувається, при цьому, інформаційний обмін.

До моделей теорії комунікації можна віднести загальні моделі: Б. Вестлі, М. Макліна інтегральна модель [9, 10], модель Гарольда Дуайта Лассуелл SMCRE [9], модель комунікації Уівера та Шеннона [11]. Моделі поширення інформації в соціальних Інтернет мережах [12]: моделі незалежних каскадів [12], епідемічні моделі: SIR, SIRS, SI, SIS [11].

Модель комунікації SMCRE - є лінійною і може бути представлена графічно (рис. 1.2):

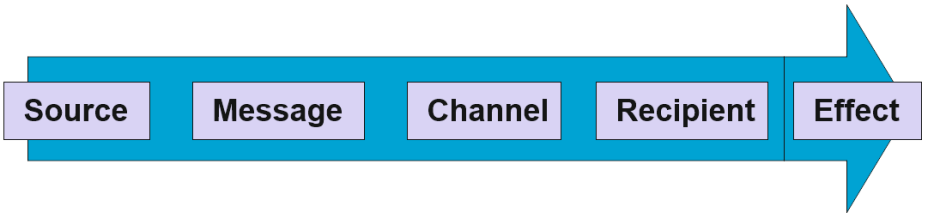


Рисунок 1.2 – Лінійна модель комунікації SMCRE

Елементи моделі SMSRE є складнми конструкціями, представленні відповідними компонентами системи виявлення та протидії поширенню шкідливої інформації в соцмережах: Source -компонент протидії джерелам; Message - компонент протидії повідомленням; Channel - компонент протидії каналам поширення пов'язаних ресурсів; Recipient - компонент протидії поширенню шкідливої інформації на стороні одержувача (користувача); Effect - компонент оцінки ефективності виявлення шкідливої інформації системою протидії. Модель комунікації SMCRE пошуку джерел та шкідливих повідомлень використана в соціальній мережі Twitter.

Лінійна модель Уівера та Шеннона - модель кількісного точного аналізу процесу передачі інформації. У проведених дослідженнях виділено три рівні проблем: технічні проблеми (рівень А); семантичні проблеми (рівень В); проблеми ефективності (рівень С). Модель Шеннона-Уівера представлена на рис. 1.3.

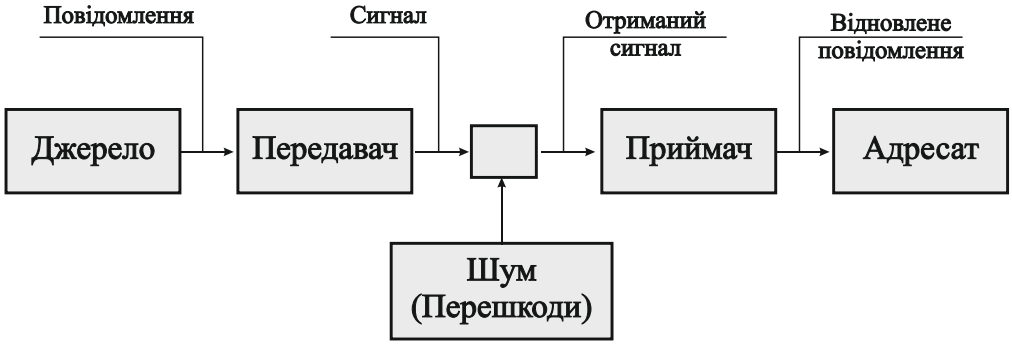


Рисунок 1.3 – Модель комунікації Уівера – Шеннона

Важливим елементом моделі Шенона та Уівера – це шум, запропоновано типологію комунікативних шумів: семантичні шуми – мають нетехнічну природу; механічні шуми – виникають в результаті технічних параметрів каналу - середовища, яким проходить сигнал. Шуми підвищують складність передачі контексту повідомлення через текст. Семантичні шуми поділяються на дві групи: шум за одержувача та шум за джерела. У моделі Уівера - Шеннона виділено окремо елементи - приймач та передавач. В подальшому Д. Файськ обґрунтував необхідність запровадження medium (посередника) [6] – фізичні, технічні засоби перетворення повідомлення в сигнал, для передачі по каналу.

Модель Уінвера- Шенона дозволяє уточнити задачі та компоненти системи протидії поширення шкідливої інформації (компонент протидії каналам може бути доповнений або розширений об'єктом впливу (посередником). Посередник включає пов'язані ресурси в Інтернет мережі, інформаційні відео канали на хостингу, новинні агрегатори, публічні сторінки в соцмережах.

На основі моделі Уівера – Шеннона запропоновано метод вимірювання передбачуваності зв'язків з використанням ентропії Шеннона та локальної інформації, а також метод прогнозування зв'язків.

Модель Теодора Ньюкомба *A-B-X* - пов'язана з такими науками, як журналістика, соціологія, психологія, лінгвістика. Модель *A-B-X* розглядає відношення між об'єктом та учасниками комунікацій, описує, в даній ситуації, вплив цих відношень на результат та характер комунікативної взаємодії. Модель Теодора Ньюкомба дозволяє розширити функціонал системи і спектр задач за рахунок аналізу використання механізмів зворотного зв'язку. Дана модель використовується при проведенні дослідження, яким чином у соцмережах студенти обирають друзів.

Модель *A-B-X* відповідає на ряд питань: як впливають відношення між суб'єктами на комунікацію; що спонукає до вступу в комунікацію суб'єктів; якими будуть соціологічні, психологічні ефекти учасників комунікації.

В моделі Ньюкомб розглядає ситуацію комунікативної взаємодії (діалогу), в якому суб'єкти *A* і *B* вступають у комунікацію з деякого зовнішнього по відношенню до суб'єктів об'єкта *X*, де *X* - будь-яке співтовариство, повідомлення, подія, індивід, інформація, пов'язане із шкідливою інформацією. В якості *A* і *B* можуть виступати соціальні суб'єкти – соціальні організації, групи, індивіди (*A* і *X* поєднує деяка тема, «орієнтація»).

Модель *A-B-X* дозволяє сегментувати одержувачів та джерела на тих, хто підтримує тему *X*, пов'язану із використанням шкідливої інформації та, хто засуджує тему *X*. Модель *A-B-X* представлена на рис. 1.4.

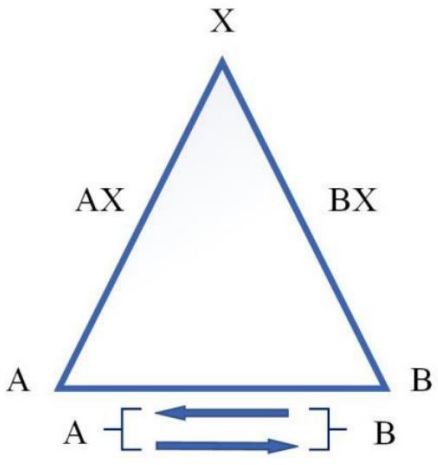


Рисунок 1.4 – Модель *A-B-X* Теодора Ньюкомбу

Модель *A-B-X* Теодора Ньюкомбу: *A, B* – суб'єкти комунікації A, B; *X* – об'єкт комунікації X; *AB* (*BA*) – міжсуб'єктний атітюд комунікації між AB (BA); *AX* (*BX*) - суб'єктно-об'єктний атітюд *AX* (*BX*).

Модель *A-B-X* Теодора Ньюкомбу надає можливість розширити та уточнити набір ознак для алгоритмів оцінки та аналізу джерел, методу виявлення та протидії поширенню шкідливій інформації в соцмережах: спільні інтереси одержувачів та джерел; зв'язки між одержувачами та джерелом; зв'язок між джерелами; зв'язок між одержувачами; загальна інформація між джерелами; загальна інформація між одержувачами; зв'язки між одержувачами та посередниками; загальна інформація між джерелами та одержувачами; зв'язки між посередниками; загальна інформація між одержувачами та посередниками зв'язки між джерелами та посередниками; загальна інформація між джерелами та посередниками; загальна інформація між посередниками.

Епідемічні моделі SIR, SIRS, SI, SIS - представлений підхід напрямів досліджень до систематизації у галузі аналізу соціальних мереж. Задача виявлення шкідливого джерела в соцмережі полягає в тому, щоб знайти вузол або людину, звідки виникли сутності, такі як дезінформація або вірус. Епідемічні моделі пропонують таксономію, яка містить різні чинники (аспекти): оціночні метрики; мережева структура; заходи центральності; моделі поширення.

Епідемічні моделі, для сприйнятливо-інфікованої моделі, вирішують задачу оцінки джерела інфекції, в якій інфіковані не всі вузли. Для соцмереж YouTube, Twitter оцінка вихідного вузла, задається центром Жордана, пов'язаного з найбільш ймовірним шляхом зараження (вузлом з мінімальною відстанню до множини заражених вузлів) [14]. Модель поширення шкідливої інформації SIS (Susceptible-Infected-Susceptible), згідно з якою вузол у соцмережі може бути заражений шкідливою інформацією в процесі її поширення в Інтернет мережі, він далі передає її сусідам, даний вузол, також залишається сприйнятливим до зараження шкідливою інформацією від своїх сусідів. Модель поширення шкідливої інформації SIS та SI, на відміну від SIR (Susceptible-Infected-Removed)

передбачає, що вузол в Інтернет мережі перебувати може у трьох станах: видалений, інфікований, сприйнятливий. Модель SIR пропонує таксономію для класифікації поширення шкідливого інформаційного контенту на стадіях виявлення та локалізації, походження, розповсюдження. Відповідно до моделей SIRS відновлений вузол соціальної мережі, може стати з певною ймовірністю сприйнятливим вузлом.

Моделі впливу в соціальних мережах та незалежних каскадів. Вплив розглядається з боку двох сторін: з впливаючої сторони – цілеспрямований, ненаправлений вплив; з боку реципієнта - вимагає рішення (політичні вибори), не вимагає прийняття рішень (тиражування, поширення шкідливої інформації). Дослідження, які спрямовані на виявлення цілеспрямованого впливу, поділяються на категорії: в яких відбувається вплив, зміни характеристик відношень; в яких автори шукають основні вузли в співтовариствах, співтовариства. Створення інформаційних об'єктів у соціальних мережах - ознака цілеспрямованого впливу.

Розглянемо докладніше моделі впливу. Модель Еверта Роджерса проникнення нововведень. На базі моделі Еверта Роджерса опубліковано та проведено понад 5000 досліджень [15]. Модель Еверта Роджерса використовується у дослідженнях: присвячених виявленню та поширенню шкідливої інформації у соцмережах; спрямованих на виявлення маніпуляцій, управління думкою користувача в соцмережах [14].

Множинна модель Френка Басса проникнення нововведень. Відповідно до моделі Ф. Басса [15] агенти в Інтернет мережі знаходяться в бінарному стані - в не в активному стані так і в активному. Ф. Басс виділяє два типи агентів: імітатори; новатори.

Модель Ф. Басса дифузії інновацій описується наступним чином (1.2):

$$n_t = \left(p + q \times \frac{N_t}{M} \right) \times \left(M - N_t \right), \tag{1.2}$$

де n_t - кількість, в момент часу t, хто прийняв інновацію; N_t - сумарна кількість, в момент часу t, хто прийняв інновацію; M- потенціал ринку; q –

коефіцієнт внутрішнього впливу (рекомендації, міжособистісні комунікації); *p*-коефіцієнт зовнішнього впливу - реклама.

Порогова модель Грановеттера - застосовується дослідниками у різних галузях, формально модель може бути описана наступним чином:

$$F_0\left(r\left(t\right)\right)=\begin{cases} r(t)<0, \textit{ то агент "не діє"} \\ r(t)\geq 0, \textit{ то агент "діє"} \end{cases}, \quad (1.3)$$

де, $F_0\left(r\left(t\right)\right)$ - функція розподілу порогів; *t*:*r*(*t*) - частка агентів, що діють, в момент часу.

Порогова модель (модель масових заворушень Грановеттера) дозволяє спрогнозувати розвиток революційних ситуацій.

Алгоритми виявлення та протидії шкідливій інформації у соцмережах умовно можна розділити за типами моделей: алгоритми, що базуються на моделях інформаційного обміну; алгоритми, що базуються на моделях незалежних каскадів; біоінспіровані підходи та алгоритми до виявлення поширення шкідливої інформації; алгоритми, що базуються на моделях впливу. Алгоритми протидії шкідливій інформації в соцмережах можуть бути сегментовані за місцем та роллю в задачах протидії та моніторингу шкідливої інформації. У [13] пропонується структура аналізу даних соціальних мереж, у якій виділяють наступні основні блоки: вибір метрик оцінювання; збирання даних із соцмереж; вимір соціального впливу; передобробка даних на основі використання BigData; аналіз продуктивності за відповідною моделлю, алгоритмом; розробка алгоритмів максимізації впливу. Блоки - збирання даних із соцмереж та передобробка даних на основі використання BigData відносяться виключно до систем моніторингу.

Ефективність протидії поширенню шкідливої інформації виявлення у соцмережах може бути підвищена штучними користувачами -псевдозахисниками, які поширюють антиінформацію. Роль псевдозахисників полягає у поширенні наклепів, інформації проти вакцинації та ін. Передбачається, що існує «псевдозахисник» та єдине джерело інформації. Для виявлення «псевдозахисника»

та джерела пропонується алгоритм навчання: а) для виявлення «псевозахисника» - аналіз параметрів розподілу відстаней метод максимальної правдоподібності; виявлення джерела інформації - оцінка апостеріорного максимуму на основі вивчених параметрів. Алгоритм динамічного періоду блокування - захід протидії поширенню шкідливої інформації у соцмережах. Дозволяє блокувати та вибирати вузли, які, в даній ситуації, з найбільшою ймовірністю підтримують та поширюють шкідливу інформацію (велику кількість чуток). Запропоноване рішення, на відміну від існуючих методів, не блокує вузли на необмежений термін, термін оцінюється активністю вузла в соціальній мережі. Також, для протидії шкідливій інформації, використовують алгоритми для виявлення кластера ботів у соціальній мережі Twitter, заснованих на моделях інформаційних каскадів. Процес обробки мережевого контенту в соцмережах розділяється на два етапи: моніторинг інформації у соцмережах; протидія поширенню шкідливої інформації у соцмережах. Алгоритми моніторингу та протидії поширенню шкідливої інформації у процесі обробки мережевого контенту в соцмережах представлені на рис. 1.5.

Моніторинг безпеки інформації –постійне спостереження за процесом забезпечення в інформаційній системі безпеки інформації, з метою встановити вимогам безпеки інформації його відповідність. До систем безпеки інформації відносять системи: виявлення вторгнень; моніторингу стану IT-інфраструктури підприємства; системи виявлення аномалій; ситуаційні центри. До систем моніторингу можна віднести пошукові системи: Google, Yandex, які надають відповідні сервіси для аналізу та збирання інформації на запит користувача.

Моніторинг соціальних мереж та мережі Інтернет–збір інформації, збирання всіх деталей та даних, які можна зібрати. Моніторингові системи, на сучасному етапі, дозволяють фіксувати те, що люди пишуть по будь-якій події чи приводу. Таким чином, розвиток сучасної комунікації дозволяє користувачеві залишати фідбек, реагувати на повідомлення, тому також системи можуть бачити статистику зворотного зв'язку користувачів.

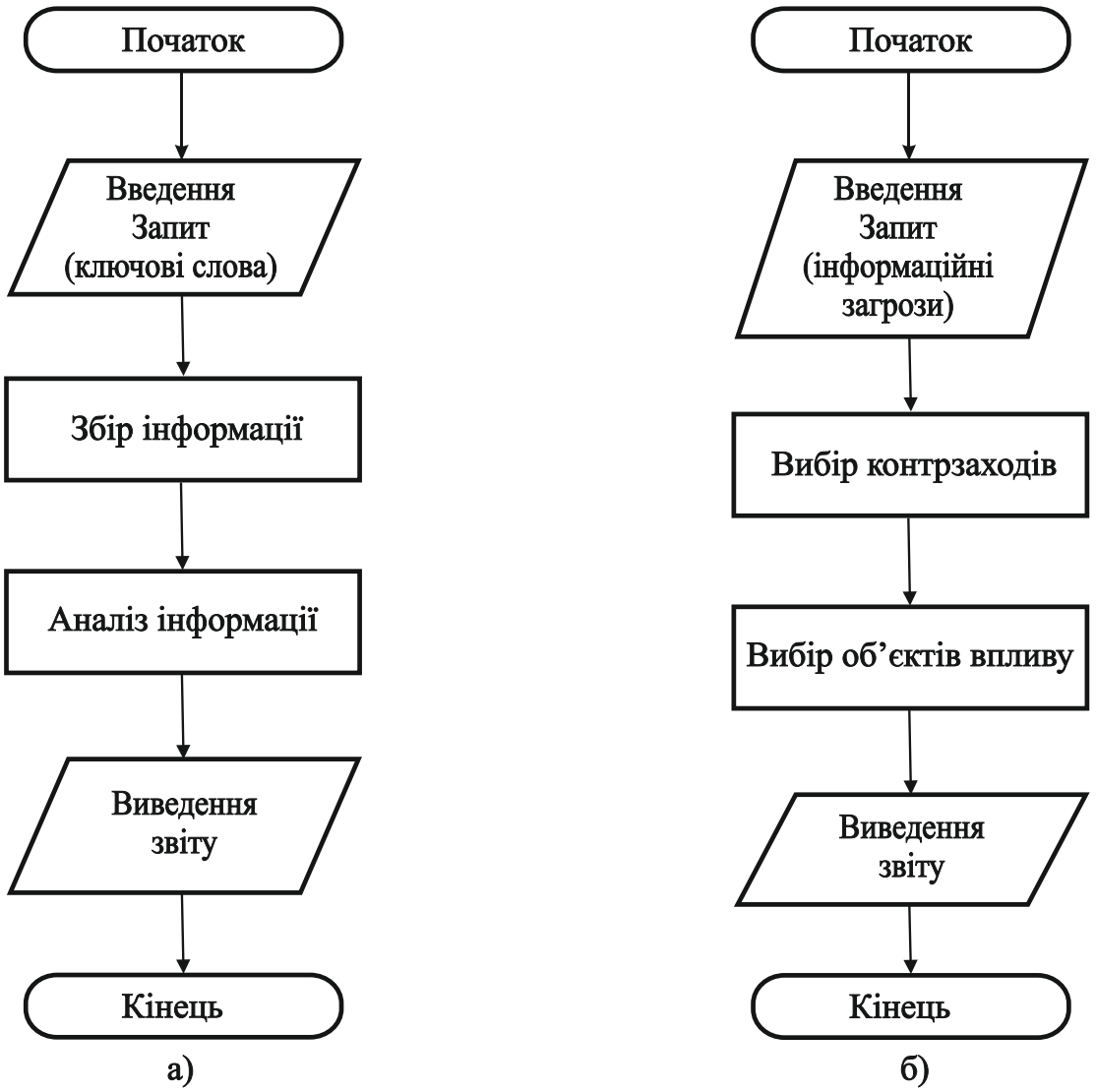


Рисунок 1.5 – Алгоритми моніторингу (*а*) та протидії (*б*) поширенню шкідливої інформації у процесі обробки мережевого контенту в соцмережах

Використання програмних рішень та їх аналогів, в даному контексті, можливе лише на комерційній основі, що, таким чином, ускладнює їхнє застосування в процесі моніторингу в мережі Інтернет шкідливої інформації. Необхідно відзначити той важливий факт, що аналізувати та зібрати сотні тисяч повідомлень із можливою шкідливою інформацією без відповідного програмного забезпечення надто складно. В табл. 1.1 наведена інформація з основними вбудованими можливостями протидії поширенню шкідливої інформації в найпопулярніших браузерах.

Таблиця 1.1 – Вбудовані можливості захисту від поширення шкідливої інформації через браузери

Браузер	Вбудовані можливості захисту від шкідливої сумнівної, та небажаної інформації
Google Chrome	Для фішингових сайтів та ресурсів із вірусними загрозами - система чорних списків. Блокувальник банерів та реклами. Доповнень під різні задачі, зокрема й антивіруси.
Mozilla Firefox	Встановлення розширень від сторонніх виробників (антивірус, батьківський контроль, антиспам).
Яндекс браузер	Блокувальник реклами, здатний закривати банери. Встановлення розширень від сторонніх виробників (антивірус, батьківський контроль, антиспам).
Opera	Сканер фішингових модулів, блокувальник банерів. Блокування підозрілих на веб-сайтах скриптів. Встановлення розширень від сторонніх виробників (антивірус, батьківський контроль, антиспам).

Таким чином, захист від банерів та реклами мають усі браузери, можливе також налаштування захисту функцій батьківського контролю. Жоден браузер не містить функцій аналізу шкідливого контенту, виявлення таких повідомлень та їх протидії.

Незважаючи на безліч розрізнених сервісів, робіт, комплексних методів протидії від поширення шкідливої інформації в соцмережах немає ні з боку користувача, ні з боку платформи соціальної мережі. Відомі підходи до протидії та виявлення шкідливої інформації в соцмережах не відповідають вимогам до повноти, швидкості, адекватності та точності прийнятих рішень. Це зумовлено наступними причинами: системи розділені два незв'язані модулі – протидія, моніторинг; соціальні мережі складаються з множини різнорідних повідомлень і мають складну структуру, що не в повній мірі враховується при виборі мети

протидії – джерело, тип повідомлення; необхідно обробляти в реальному масштабі часу надвеликі потоки повідомлень і в обмежений час для контрзаходу вибирати мету, в ручному режимі система протидії не в змозі адекватно реагувати на поширення шкідливої інформації в мережі.

1.3 Дослідження та аналіз вимог до системи протидії та виявлення в соціальних мережах шкідливої інформації

За своєю архітектурою соцмережі є багатокомпонентними рішеннями, в архітектурі мереж знаходяться компоненти: які здійснюють обробку контенту; компоненти, які забезпечують функції: маркетинг, адміністрування, зберігання даних, розробка. Соціальні мережі не містять окремого компонента протидії поширенню шкідливій інформації. Соціальні мережі контролюють дотримання закону про авторське право (YouTube, Instagram, Facebook) захист від контенту залежно від вікових обмежень.

Вконтакте та Facebook мають загальну логіку графового представлення зв'язків, схожі зовні сторінки. Архітектура соцмережі Вконтакте (рис. 1.6) є кластер серверів: Front-сервер; Content Server, Backend; Sun (розподіл навантаження); pu/pp (photo upload, photo proxy); proxy; Cache; Data Base, engines (система управління) [16].

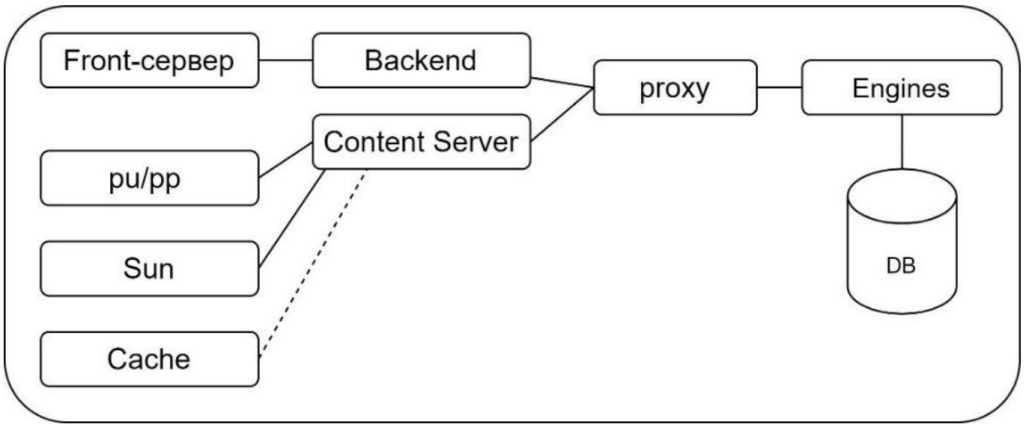


Рисунок 1.6 – Архітектура соціальної мережі Вконтакте

Проведений порівняльний аналіз досліджень у галузі виявлення та протидії шкідливої інформації в соцмережах дозволив визначити загальні вимоги до системи виявлення та протидії, в основу реалізації, покладено модельно-методичний апарат. Розглянемо необхідний фундамент функціональності системи виявлення та протидії шкідливій інформація в соцмережах (рис. 1.7)

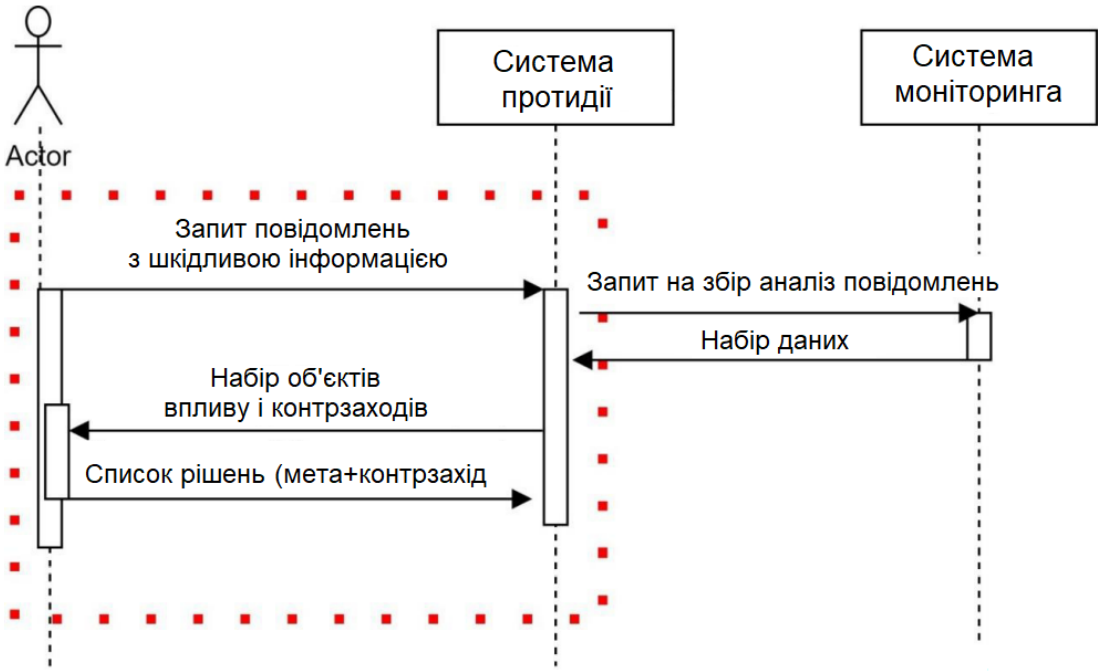


Рисунок 1.7 – Фундамент функціональності системи виявлення та протидії шкідливій інформації у соцмережах

Система виявлення та протидії (рис.1.7) може бути центральним елементом у процесі виявлення шкідливих повідомлень. Процеси у системі виявлення та протидії шкідливих повідомлень можуть бути автоматизовані з використанням запропонованих алгоритмів і відповідних програмних компонентів.

Вимоги до системи виявлення та протидії шкідливих повідомлень розділимо на дві групи: функціональні; не функціональні. Функціональні вимоги можуть бути реалізовані шляхом проектування та розробки компонентів, архітектури, програмних прототипів. Функціональні вимоги - функції, які має виконувати система. Нефункціональні вимоги можуть бути реалізовані шляхом розробки алгоритмів та моделей. Нефункціональні вимоги описують цільові характеристики

системи: оперативність, вимоги щодо обґрунтованості та ресурсоспоживання. Визначимо функціональних вимог до системи виявлення та протидії шкідливої інформації в соціальних мережах: формування задачі на збирання повідомлень, аналіз повідомлень для системи моніторингу; аналіз джерел повідомлень в отриманому наборі даних; налаштування доступних заходів виявлення та протидії у системі; сортування та ранжування об'єктів впливу на отриманому наборі даних; вибір мети впливу для протидії; сортування та ранжування доступних контрзаходів з бази даних контрзаходів для відповідного набору даних; генерація звітів про роботу системи виявлення та протидії в адаптованому вигляді, для адміністратора системи; генерація звітів про отримані результати у адаптованому вигляді, для експерта з інформаційної безпеки закладу.

Три класичні компоненти ефективності - нефункціональні вимоги до системи виявлення та протидії шкідливої інформації:

1. Оперативність – час, необхідний протидії поширенню шкідливої інформації у соцмережах. Вимога до оперативності (1.4):

$$T_m \le T_s, \tag{1.4}$$

де T_m - час, необхідний для протидії поширенню шкідливій інформації у соцмережах з використанням контрзаходів, S – множина систем протидії шкідливої інформації.

Для того, щоб система протидії поширенню шкідливої інформації в соцмережах використовувалася в режимі, близькому до реального часу, система повинна забезпечити протидію шкідливій інформації за час, що не перевищує заданої границі (1.5):

$$P_{operability}\left(T_m \le T^{acceptable}\right) \ge P^{acceptable}_{operability}, \tag{1.5}$$

де $P_{operability}$ – ймовірність протидії поширенню шкідливої інформації за відповідний заданий час, $T^{acceptable}$ – допустимий час протидії поширенню шкідливої інформації, $P^{acceptable}_{operability}$ - допустиме значення ймовірності. Опираючись

на серії проведених досліджень та результатах опитувань експертів $T^{acceptable}$=104 хв.

2. Обґрунтованість – сукупність параметрів для вибраних об'єктів і контрзаходів у процесі виявлення протидії поширенню шкідливої інформації. Вимога до обґрунтованості задається у виді (1.6):

$$\begin{aligned} &N_{param} \to \max, \\ &N_{param} > \max N^{s}_{param}, \end{aligned} \tag{1.6}$$

де N^{s}_{param}- кількість параметрів для системи $s \in S$; N_{param} – кількість параметрів, задіяних при виборі об'єкта впливу та контрзаходів, $\mathcal{S}$ – множина систем протидії.

Система виявлення та протидії шкідливої інформації повинна враховувати більшу кількість параметрів для об'єктів впливу та контрзаходів, ніж існуючі аналоги.

3. Ресурсовживання - характеризує номенклатуру та кількість необхідних та апаратно-програмних засобів, кадрові ресурси, що витрачаються на реалізацію процесу виявлення та протидії поширенню шкідливої інформації. Вимоги до ресурсоспоживання (1.7):

$$P_{res}\left(r \le R^{acceptable}\right) \ge P^{acceptable}_{res}, \tag{1.7}$$

де P_{res} – ймовірність, що ресурси, що витрачаються на протидію поширення шкідливої інформації r не перевищують допустимого значення $R^{acceptable}$, $P^{acceptable}_{res}$- допустиме значення ймовірності.

Цільова функція проектуємої системи - максимізація параметра обґрунтованості з урахуванням вимог до ресурсоспоживання та оперативності.

1.4 Постановка задачі

Протидія поширенню шкідливої інформації у соцмережах є важливим елементом інформаційної безпеки особистості, суспільства, держави, проте більшість систем, на теперішній час не враховує простір функціональності системи виявлення та протидії шкідливій інформації, системи розділені на два модулі: моніторинг; протидія, необхідна автоматизація процесу протидії. Соціальні мережі мають складну структуру, параметри повідомлень та джерел не в повній мірі враховуються під час виборів мети виявлення та протидії шкідливій інформації. При розробці методу протидії поширенню шкідливої інформації, необхідно: в повній мірі, враховувати кількість повідомлень на сторінці, характеристики джерела, зворотний зв'язок від джерела та аудиторії повідомлення; підтримувати дві стадії: експлуатація, налаштування; ранжувати контрзаходи з урахуванням коефіцієнтів складності.

Задача дослідження полягає у розробці: моделей шкідливої інформації, джерела та соціальної мережі; алгоритмів проведення аналізу джерел поширення шкідливої інформації у соціальних мережах та проведення ранжування контрзаходів; методу виявлення та протидії поширенню шкідливої інформації у соціальних мережах з урахуванням вимог до обґрунтованості; архітектури компонентів системи протидії поширеню шкідливої інформації в соцмережах.

Вирішення поставлених задач дозволить: підвищити якість прийнятих рішень у процесі виявлення та протидії шкідливої інформації; сортувати об'єкти впливу для оператора по пріоритету; задати вхідні дані налаштування системи виявлення та протидії поширенню шкідливої інформації.

2 МОДЕЛІ СИСТЕМИ ПРОТИДІЇ: ШКІДЛИВОЇ ІНФОРМАЦІЇ СОЦІАЛЬНОЇ МЕРЕЖІ ТА ДЖЕРЕЛА В МЕРЕЖІ ІНТЕРНЕТ

2.1 Концептуальна модель системи виявлення та протидії поширенню шкідливої інформації у соціальних мережах

Проведений аналіз досліджень показав, що незважаючи на множину робіт, методів, сервісів, в даній області, комплексного підходу до виявлення та протидії поширенню шкідливої інформації немає з боку платформи соціальної мережі, ні з боку користувача. Проблема виявлення та протидії поширенню шкідливої інформації має не достатню кількість науково-технічних рішень. Доступні засоби протидії та виявлення шкідливої інформації в соціальних мережах не відповідають вимогам до адекватності, швидкості, точності та повноти прийнятих рішень. Це обумовлено наступними причинами: системи розділені на два незв'язані модулі – моніторинг, протидія; між якими знаходиться оператор; соціальні мережі мають складну структуру, до складу яких входять різнорідні повідомлення, що недостатньо враховується під час реалізації мети протидії – джерело, тип повідомлення, та інші характеристики; необхідно обробляти у реальному масштабі часу надвеликі потоки повідомлень, в стислий термін реалізувати контрзаходи, в ручному режимі оператор не в змозі зупинити поширення шкідливої інформації в соціальній мережі.

На рис. 2.1 наведено залежність зв'язку між експертом, оператором, який знаходиться між двома роздільними системами протидії та моніторингу, незалежно від того, як реалізується система протидії (чорні списки для операторів зв'язку, батьківського контролю). Основна складність системи виявлення та протидії поширенню шкідливої інформації в соціальних мережах безпосередньо випливає із сучасних тенденцій розвитку інформаційно-технологічної сфери. Сучасний стан систем виявлення та протидії поширенню шкідливої інформації в соцмережах зумовлює необхідність розробки нових моделей, методів, алгоритмів,

архітектури для підвищення ефективності систем виявлення та протидії поширенню шкідливої інформації у соціальних мережах.

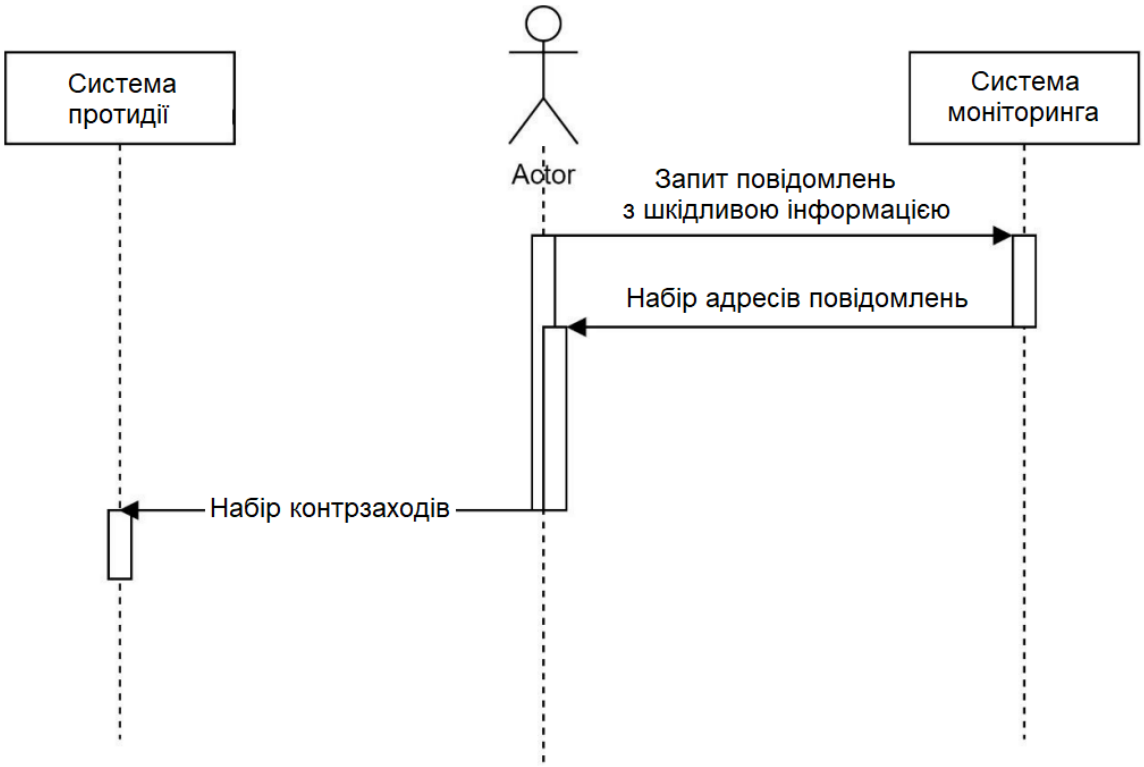


Рисунок 2.1 – Схема протидії поширенню шкідливій інформації в соцмережах

Моделі незалежних каскадів (моделі управління, впливу, протиборства) - описують інформаційний каскад, поширення шкідливої інформації через сусідів. Для блокування поширення каскаду шкідливої інформації між спільнотами вираховується максимальне значення зв'язків агента поза спільнотою (якщо значення менше ніж заданий поріг, каскад не проходить). У моделях незалежних каскадів виділяються незалежні вершини з великим ступенем (хаби), вершини перемикаються, якщо більша кількість їх зв'язків, в каскаді, вже переключено. При перемиканні хаба йде вплив на велику кількість агентів (одиночна зміна стану, при цьому, впливає на невелику кількість). Модель каскадів задається через модель навчання Байєса.

Моделі інформаційного протиборства, поширення інформаційної загрози. Основу моделі інформаційного протиборства (поширення інформаційної загрози) становлять моделі поширення інновацій, поділяють інформаційні канали на

внутрішній та зовнішній - стосовно об'єкту впливу. Швидкість поширення інформаційної загрози у соціальній мережі обмежена ресурсами супротивника.

Аналіз проведених досліджень моделей протидії поширенню шкідливої інформації, інформаційного обміну в соцмережах показав, що кожна з них розроблялася в рамках концепцій, які не враховували виявлення та протидії поширенню шкідливої інформації в мережі. Мета моделей: моделювання зустрічних інформаційних потоків мережі Інтернет, у рамках протидії, виявлення інформаційного каналу у соцмережі, джерела.

Аналіз проведеного дослідження моделей виявлення та протидії поширенню шкідливої інформації, інформаційного обміну запропоновано концептуальну модель виявлення та протидії поширенню шкідливої інформації та її зв'язок із системою моніторингу (рис. 2.2)

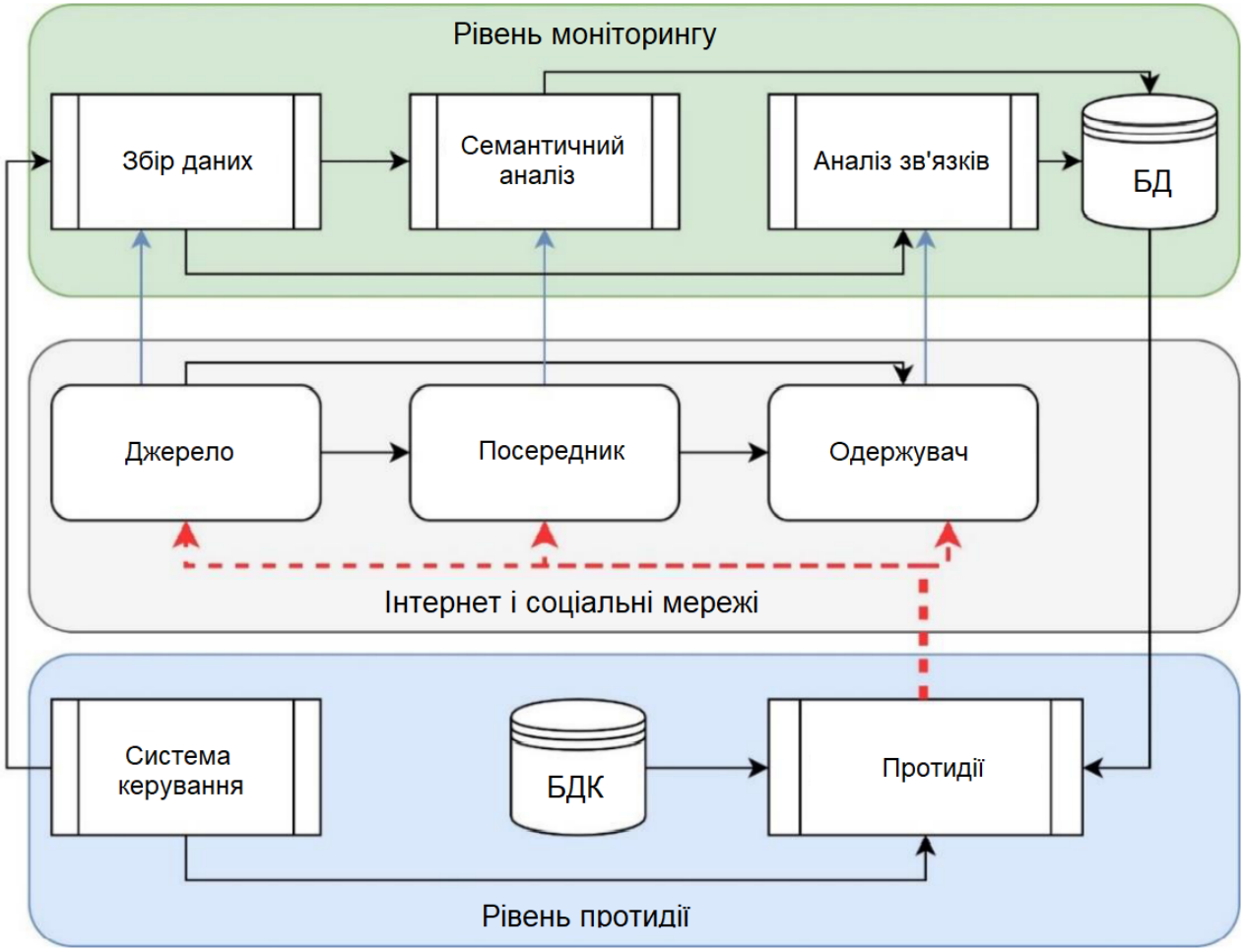


Рисунок 2.2 – Концептуальна модель системи виявлення та протидії поширенню шкідливої інформації у соцмережах

Концептуальна модель (рис. 2.2) включає: рівень моніторингу; рівень протидії. Інформаційний обмін відбувається між рівнями моніторингу та протидії, в інформаційному просторі. На рівні протидії відбувається формування списку інформаційних загроз, що містять шкідливу інформацію в соціальній мережі. На рівні моніторингу відбувається семантичний аналіз текстів, аналіз зв'язків, збір даних.

2.2 Модель соціальної мережі поширення шкідливої інформації

Моделі системи протидії умовно можна розділити на три концепції: моделі інформаційного обміну в соцмережах; моделі представлення даних; моделі поширення інформації в мережі Інтернет. Кожна концепція моделі дозволяє описувати різні характеристики системи протидії. Модель представлення даних найкраще підходить для представлення та розроблення моделі соцмережі.

Моделі представлення даних –сукупність правил взаємозв'язку та створення структур даних соціальних мереж, обмежень, можливих операцій [12]. Модель даних соціальних мереж складається з наступних наборів: правил та операторів виведення; загальних правил цілісності; типів структур даних.

В основі соціальних мереж структуризації даних лежать концепції «узагальнення та «агрегації». Одиницею представлення моделі даних соцмережі є «елемент даних». У моделі даних соцмережі «кортеж» («запис») може мати декілька атрибутів. Наприклад, запис: <user> (користувач) має наступні агрегати: прості - ПІБ, адреса і повторювані – інтереси, та елементи даних (пов'язаний пост, пов'язаний друг, стать). Серед атрибутів моделі даних соціальних мереж виділяються як основний ключ, (одне чи декілька ключових полів), саме вони характеризують домени моделі даних. Для моделей даних соцмережі основними ключами будуть ідентифікатор повідомлення та джерела.

Розглянемо основні структури даних соціальних мереж. Перший тип соціальних мереж –мережі, структура яких представлена повнозв'язним графом

(пов'язані соціальні мережі). До таких соціальних мереж відносяться OK, VK, Facebook (рис. 2.3). Особливістю таких мереж є двоспрямований (односпрямований) зв'язок між ідентифікаторами сторінок (суцільні лінії (рис.2.3)), що дозволяє стороннім сторінкам (групи чи користувача) взаємодіяти з сторінками (повідомленнями), з якими вони не пов'язані (непрямий зв'язок – пунктирні лінії (рис.2.3)).

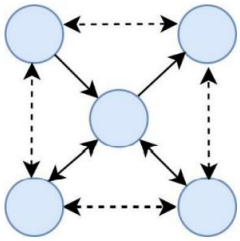


Рисунок 2.3 – Структура даних повнозв'язаних соцмереж

Другий типу соцмереж - структура даних у яких односпрямована від багатьох повідомлень (джерел) до одного реципієнта (рис. 2.4). Особливістю таких соцмереж є те, що набір джерел одержувач інформації вибирає, з якими він пов'язаний, система пропонує одержувачу джерела (повідомлення) на відповідну тему. Джерела зворотнім зв'язком не пов'язані з одержувачами і відповідно не бачать створений ними контент (коментарі знаходяться на сторінці джерела). Прикладами таких соціальних мереж є Youtube та Telegram.

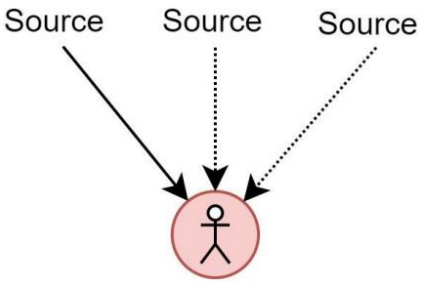


Рисунок 2.4– Структура даних односпрямованих соцмереж

Третій тип – медіа-транслятори інформації (користувач або організація, медіа-транслятори). Структура даних таких соціальних мереж містить зв'язок між ідентифікаторами сторінок, медіа-транслятор - це сторонній інформаційний канал,

формується системою на основі пов'язаних з ними ідентифікаторів та проведення аналізу переваг одержувачів (рис. 2.5). В соціальних мережах даного типу зв'язок встановлюється тільки між користувачами (організаціями), як приклад – мережа Instagram, Tik Tok.

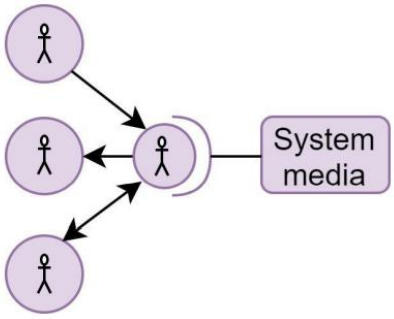


Рисунок 2.5 – Структура даних соцмереж медіа-трансляторів

Усі три типи структур розглянутих соціальний мереж містять загальні атрибути, відмінність структур соцмереж починається на рівні відношень.

Проведений аналіз досліджень основних структур даних соціальних мереж показав, що присутні загальні атрибути, які для опису взаємозв'язку, можуть бути використанні між реципієнтом, джерелом та шкідливою інформацією. Якщо у деякий момент приєднання до соцмережі суб'єкт створює мережевий профіль - account (обліковий запис), проходить процес реєстрації, таким чином його обліковий запис належить множині ACCOUNT. У процесі реєстрації account суб'єкт отримує *id* (унікальний ідентифікатор), який належить множині *ID*. В результаті реєстрації суб'єкт прив'язаний до нього, знаходиться на границі між реальним та віртуальним світом. Суб'єкт, після реєстрації, може не додавати про себе інформації, проте може передавати та створювати інформацію в соцмережі [14]. Суб'єкт шляхом внесення даних у мережному профілі заповнює обліковий запис, таким чином він заповнює свою власну pageac (сторінку). Сторінка облікового запису (account) належить множині PAGEac. Суб'єкт, також може створити спільноту, в результаті спільнота отримує group (профіль) та унікальну адресу. Співтовариства в соцмережі утворюють множину GROUP, таким чином формується pageg (сторінка) спільноти після заповнення профілю. Сторінки груп

утворюють множину PAGEg, таким чином $PAGE = PAGEac \bigcup PAGEg$. У процесі аналізу інформації (повідомлення) можна визначити сторінку (Page) в соціальній мережі, де дана інформація опублікована. Сторінка, на якій опублікована інформація (повідомлення) із шкідливою інформацією – source (джерело). Джерела у соцмережах утворюють множину SOURCE. Поширення шкідливої інформації у соцмережах можливе шляхом публікації message (повідомлення). Повідомлення у соцмережі утворюють множину MESSAGE. Повідомлення – будь-який пост на стіні групи, на стіні акаунта, запис у коментарях. Суб'єкт публікує та створює повідомлення в соцмережі у відкритому доступі від від імені групи, свого облікового запису, в даному випадку суб'єкт є author (автором). Суб'єкти, які публікують повідомлення в соцмережі утворюють множину AUTHOR. Відповідальність за поширення шкідливої інформації в соціальній мережі лежить на джерелі, а не на авторі, в якому інформація опублікована. Множини повідомлень та джерел можуть бути виділено в окремі класи (домени), які утворюють модель соцмережі (рис. 2.6).

Загальні атрибути моделі даних соціальної мережі, які присутні у більшості структур даних наведені в табл. 2.1.

Таблиця 2.1. − Основні атрибути структури даних моделі соціальної мережі

Елемент структури даних	Повнозв'язані соціальні мережі	Однонаправлені соціальні мережі	Медіа-транслятори
id_source	+	+	+
message	+	+	+
url_message	+	+	+
type_message	+	+	+
followers	+	+/-	+
comment	+	+	+
like	+	+	+/-
repost	+/-	-	+/-
views	+	+	+
answer	+	+	+

У моделі даних соціальної мережі інформація представлена у вигляді набору відношщень (таблиць), кожне з яких є підмножиною декартового добутку відповідних множин.

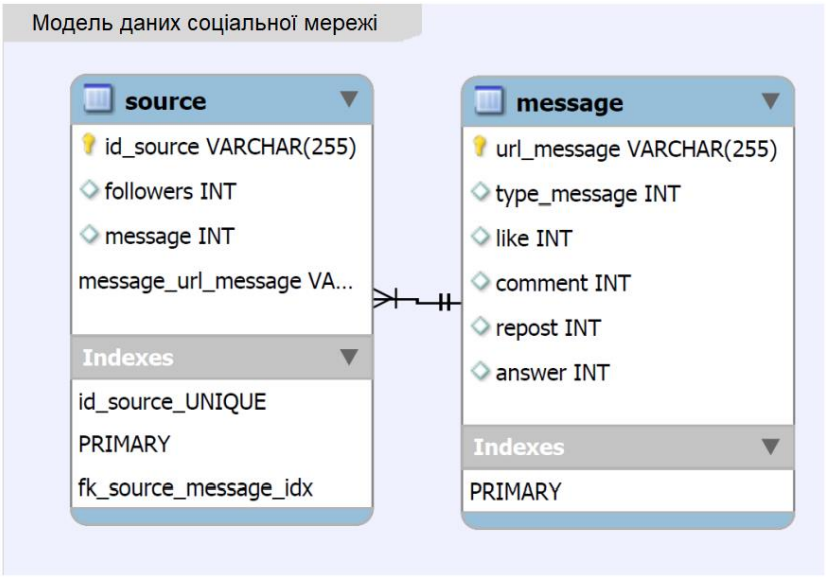


Рисунок 2.6 – Модель даних соціальної мережі

Записи в моделі даних соцмережі називаються "кортежами". Елементи кортежу – поля (атрибути), до яких належать: id_source - адреса веб_сторінки, де публікуються повідомлення; message – кількість повідомлень; followers - кількість передплатників джерела в соціальній мережі; url_message – адреса повідомлення; like – кількість позначок; type_message - тип повідомлення (comment, post, answer); repost – кількість ріпостів; comment – кількість коментарів; views – кількість переглядів; answer – кількість відповідей на коментарі.

Модель даних соціальної мережі містить наступні властивості: $f : MESSAGE \to SOURCE$; соціальна мережа не містить однакові кортежі; порядок кортежів не фіксований; число кортежів відношення $R(SOURCE, MESSAGE)$ - потужність відношення;

Модель даних соціальної мережі містить нові атрибути, класи та відношення між ними.

2.3 Інформаційно-ознакова модель джерела шкідливої інформації в соціальних мережах

Модель даних соціальних мереж, характеризуються, незалежно від їх структури, загальними атрибутами - джерела, повідомлення, ознаки зворотного зв'язку на повідомлення суб’єкта. Наявність ознак зворотного зв'язку в моделі соцмережі дозволяє характеризувати джерело повідомлення. Таким чином -

$$ACTIVITY\ \{countLike, countREpost, countComment, countView\} \qquad (2.1)$$

множина у повідомлення від реципієнтів всіх ознак зворотного зв'язку інформації у соцмережі, де *countLike* – кількість позначок, *countREpost* – кількість копій з посиланням на джерело («репостів»), *countComment* - кількість коментарів *countView* – кількість переглядів.

Виходячи з поставлених задач в магістерській роботі, необхідно визначити атрибути множини *ACTIVITY* , а також відношення $R(SOURCE, MESSAGE)$, які в подальшому дозволять проводити аналіз повідомлення та джерела, що містять шкідливу інформацію та вибирати відповідний об'єкт для протидії. Наприклад, якщо сума елементів активності до повідомлення дає можливість обчислити індекс активності повідомлення, таким чином може бути отриманий, в даній ситуації, інтегральний показник індексу активності, який в свою чергу залежить від кількості повідомлень джерела, очевидно одним із атрибутів моделі даних джерела буде *index_active*. Якщо кількість переглядів повідомлення дозволяє обчислити індекс перегляду, таким чином можемо отримати інтегральний показник індексу перегляду для джерела інформації, отримаємо наступний атрибут моделі даних джерела - *index_viewability*. Функція $f : MESSAGE \to SOURCE$ задає область визначення, вихідні та вхідні значення (аргументи). Функція сюр'єктивна - є відображення множини *MESSAGE* на

множину $SOURCE$, при відображенні кожен елемент множини $SOURCE$ є образом множини $MESSAGE$ (хача б одного елемента). Таким чином, отримаємо:

$$\forall source \in SOURCE \exists message \in MESSAGE : source = f\left(message\right) \quad (2.2)$$

Повідомлення (аргументи) на стіні джерела можуть бути різного типу (відповідь, пост, коментар). Таким чином, для окремих аргументів (повідомлень) може бути заданий числовий коефіцієнт (рейтинг) у дереві повідомлень соціальної мережі (рис. 2.7).

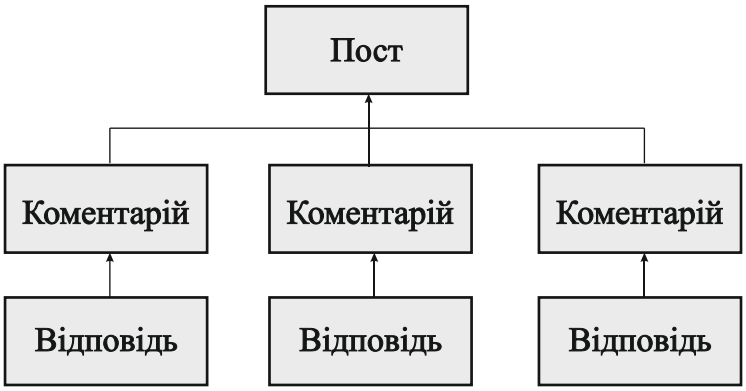


Рисунок 2.7 – Дерево повідомлень соцмережі

В залежності від кількості аргументів джерело повідомлення може оцінити за потенціалом Potential: джерело із низьким потенціалом; джерело із середнім потенціалом; джерело із високим потенціалом. Якщо джерело повідомлень має атрибути: index_active, index_viewability, то можна задати індекс впливу - index_impact, який відображає рівень впливу джерела повідомлення на аудиторію. Модель джерела повідомлень представлена на рис. 2.8.

Виділимо атрибути в кортежі, що характеризує $SOURCE$ через елементи множини $ACTIVITY$ і відношення $R\left(SOURCE, MESSAGE\right)$ - $\left\langle index_{active}, index_{viewabiliy}, potential, index_{impact} \right\rangle$. Також, атрибутами моделі джерел повідомлень є: *social_network_type* – тип даних структури соцмереж; *followers* – кількість пов'язаних користувачів; *registration_time* - час реєстрації в мережі джерела інформації. Модель даних джерела повідомлень відрізняється наявністю нових атрибутів, класів, відношень.

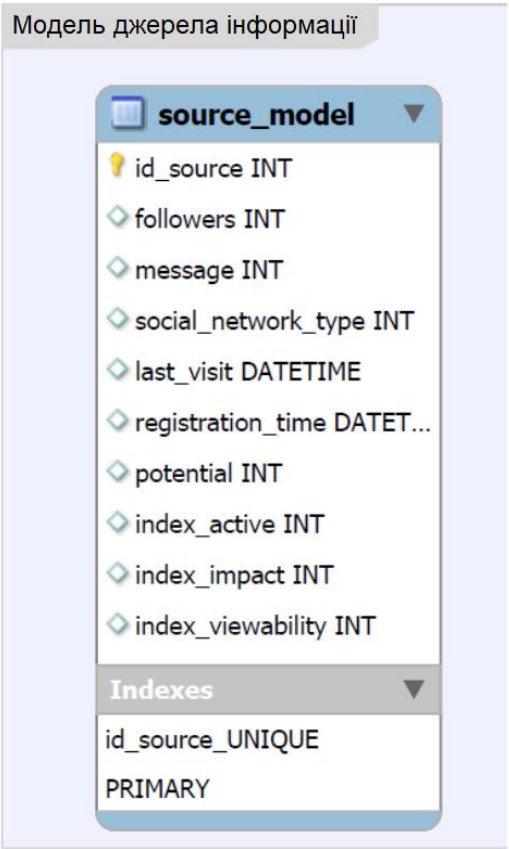


Рисунок 2.8 – Модель джерела повідомлень

Розглянемо модель шкідливої інформації в мережі Інтернет. Основою для формування поняття шкідлива інформація виступають два терміни [8]: I – information (Інформація); IO – information object (Інформаційний об'єкт) –логічно цільний блок відповідної інформації, представлений у фіксованої формі, використовується та створений в ході інформаційної діяльності. Формально терміни пов'язані між собою, так, що $IO \subseteq I$ (рис. 2.9 а) - інформаційний об'єкт є елементом множини всієї інформації, над якою проводиться аналіз. Із терміном «інформація» також пов'язаний термін - IA – information area («інформаційний простір»), а множини I, IO є підмножинами інформаційного простору. Соціальні мережі представляють собою сукупність взаємозалежних вузлів: спільноти, акаунти, сторінки, вкладення, пости; зв'язки між об'єктами – однорівневі відношення (перебувають у співтоваристві, у друзях); відношення вкладеності (сторінка запису містить посилання на пост, стіна містить пост). Соціальні мережі

можуть бути представленні графами: частина об'єктів - інформаційні, вершина графа, а зв'язки між об'єктами - ребра між вершинами. Таким чином, справедливо, що $IO \subseteq I \subseteq IA$, $SN \subseteq I \subseteq IA$, область перетину між SN (соціальна мережа) та IO є предметом дослідження у соціальних мережах розробки моделі шкідливої інформації (рис. 2.9, б).

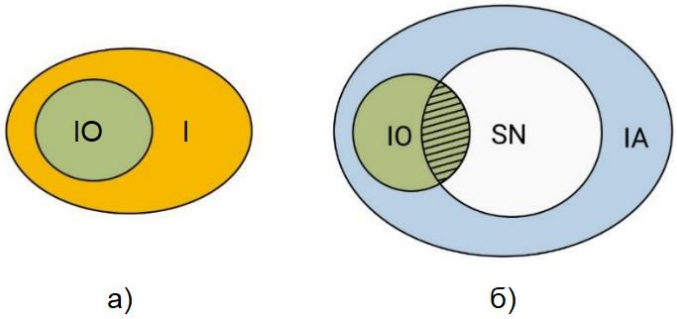


Рисунок 2.9 – Графічне представлення відношень множини інформаційного простору

Інформаційний об'єкт - MIO (шкідливий інформаційний об'єкт), містить відповідні ознаки, які дозволяють прийняти рішення, що інформація завдає шкоди державі, суспільству, бізнесу особистості. В залежності від умови експерт встановлює ознаки ознаки $Token$ інформаційної загрози T. Наприклад, батько сам вибирає обмеження для дитини, у випадку використання система батьківського контролю. Якщо представник бізнес - компанії зацікавлений у захисті конфіденційного інформації бізнеса, в даній ситуації він їх сам задає. Таким чином, у соціальній мережі, теоретико-множинна модель шкідливої інформації, включає наступні базові елементи: IO - інформаційний об'єкт (Information Object); T - інформаційна загроза (Threat); MIO – шкідливий інформаційний об'єкт; $Token$ – ознака інформаційної загрози, що знаходиться у шкідливому інформаційному об'єкті; $Feature$ – ознака наявності інформаційного об'єкта [0,1]; зв'язок між інформаційними об'єктами.

Теоретико-множинна модель шкідливої інформації (2.2) формально представлена наступним чином:

$$
\begin{aligned}
&IO = \{io\}; MIO = \{io\}; MIO_i = \{io\} \\
&MIO \subset IO; \forall io \in MIO : io \in IO \\
&MIO_i \subseteq MIO; \forall io \in MIO_i : io \in MIO \\
&Token_{mio_i} \subset T; Token_{mio_i} = \{t\} \\
&CheckFeature(io,t) = \{True; False\} \\
&io \in MIO_i \Leftrightarrow \exists Token_{mio_i} : checkFeature(io,t) = True
\end{aligned}
, \qquad (2.2)
$$

де IO – множина інформаційних об'єктів, io – інформаційний об'єкт, T - множина ознак інформаційної загрози, t_i –*i -а* ознака інформаційної загрози, MIO – множина шкідливих інформаційних об'єктів мережі, MIO_i - *і-й* клас шкідливої інформації, $Token_{mio_i}$ - множина ознак загрози, що характеризують MIO.

Таким чином, для виявлення та протидії поширенню шкідливій інформації в мережі необхідно задати набір ознак, характерних для інформаційної загрози в соцмережі.

Особливістю моделі шкідливої інформації соцмережі є те, що модель допускає наявність дискретних ознак у множині ознак: зв'язок інформаційного об'єкта з іншими інформаційними об'єктами у соцмережі; частота повторення ознаки; дата створення інформаційного об'єкта.

Протидія поширенню шкідливого інформаційного об'єкта в соціальній мережі може здійснюватися лише на рівні джерел чи повідомлень. Таким чином, необхідно виділити такі інформаційні загрози та відповідні інформаційні ознаки повідомлення у соцмережі, що характеризують його як шкідливий об'єкт.

Інформаційно-ознакова модель (табл.2.2.) - впорядкована сукупність інформації про зв'язки повідомлень та їх ознак зі змістом повідомлень. Інформаційні ознаки повідомлень - окремі властивості повідомлень, їх зміст. Інформаційна загроза – задається оператором системи. Шкідлива інформація в соціальній мережі – задається оператором шляхом формування набору відповідних ключових слів. Інформаційні ознаки - формують множину усіх можливих інформаційних ознак *t*. На рис. 2.10 наведено співвідношення, взаємозв’язок різних рівнів інформаційно-

ознакової моделі шкідливої інформації Показано, що формується повідомлення, розміщується повідомлення в джерелі розповсюдження, на сторінці групи, облікового запису. Повідомлення можуть містити ознаки шкідливої, а також не містити ознаки шкідливої інформації.

Таблиця 2.2. – Інформаційно-ознакова модель шкідливої інформаціїсоціальної мережі

Інформаційні загрози	Шкідлива інформація у соцмережах	Інформаційні ознаки
Приклад Самогубство	Приклад Повідомлення, що містить прохання, пропозицію, наказ зробити самогубство, описує самогубство як спосіб вирішення проблем	t_1
	Приклад Повідомлення, що містить позитивну оцінку схвалення вчинення самогубства, дій, спрямованих на самогубство	t_2

Інформаційні ознаки (табл. 2.2) формують рівень інформаційних загроз в соціальній мережі.

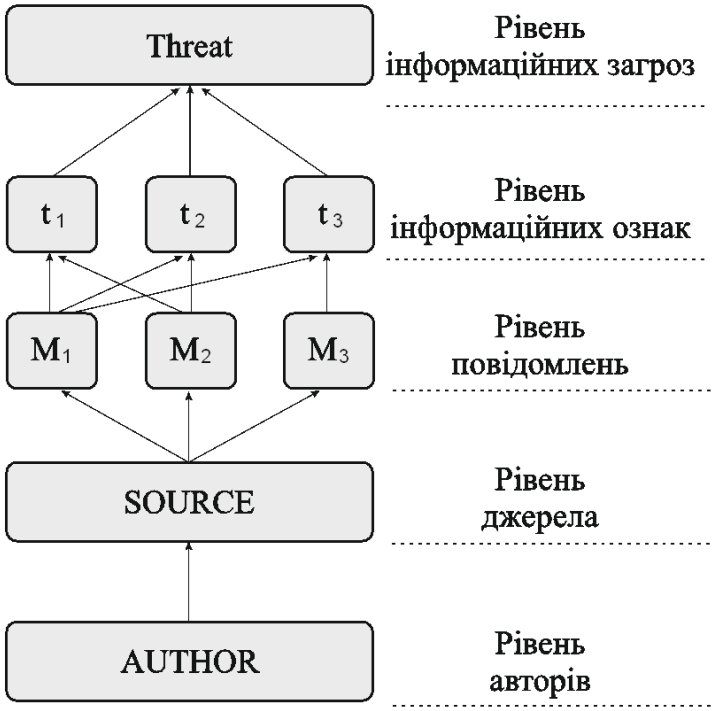


Рисунок 2.10 – Інформаційно-ознакова модель шкідливої інформації

Таким чином, зібравши відповідну інформацію на сторінці джерела можливо визначити, які з цих повідомлень інформаційної мережі належать до шкідливих повідомлень. Результатом виявлених загроз та їх кількості буде прийняте відповідне рішення про протидію джерелу, повідомленню.

Запропонована інформаційно-ознакова модель шкідливої інформації в соціальних мережах, дозволяє сформувати дані для виявлення та протидії поширенню шкідливої інформації в мережі. Комплекс моделей складається з моделі шкідливої інформації, інформаційно-ознакової моделі шкідливої інформації, моделі джерела інформації, моделі соціальної мережі. Кожна з моделей містить унікальні атрибути та відношення між інформаційними об’єктами, також комплекс моделей дозволяє сформувати відповідні вимоги до алгоритмів оцінки та аналізу джерел повідомлень та забезпечує вибір контрзаходів.

2.4 Висновки

Запропонована модель соціальної мережі, що включає джерела, повідомлення, зв'язки (відношення) між інформаційними об’єктами, відрізняється наявністю нових рв'язків та структурних елементів. Розроблено модель джерела, в якій враховуються наступні параметри: індекс впливу, індекс активності, індекс перегляду, потенціал. Запропонована теоретико-множинна модель шкідливої інформації в соціальній мережі, складається з ознак шкідливої інформації та взаємопов'язаних об'єктів, що в сукупності формують шкідливо-інформаційні об'єкти в мережі Інтернет. Також розроблена інформаційно-ознакова модель шкідливої інформації в соціальних мережах, дозволяє сформувати дані для виявлення та протидії поширенню шкідливої інформації в мережі.

3 АЛГОРИТМИ ПРОТИДІЇ ТА ВИЯВЛЕННЯ В СОЦІАЛЬНИХ МЕРЕЖАХ ШКІДЛИВОЇ ІНФОРМАЦІЇ

3.1 Алгоритм ранжирування джерел повідомлень соціальної мережі по потенціалу

Аналіз проведених досліджень показав, що більшість існуючих алгоритмів використовує аналіз контент у своїй основі. Запропонований алгоритм ранжування джерел опирається на залежність від кількості повідомлень. У більшості DATASET сукупність повідомлень соцмережі може бути розділена відповідно множині SOURCES, яким належать різна кількість повідомлень мережі з множини MESSAGES. Таким чином, список повідомлень від окремих джерел можна представити ієрархічним графом (рис. 3.1).

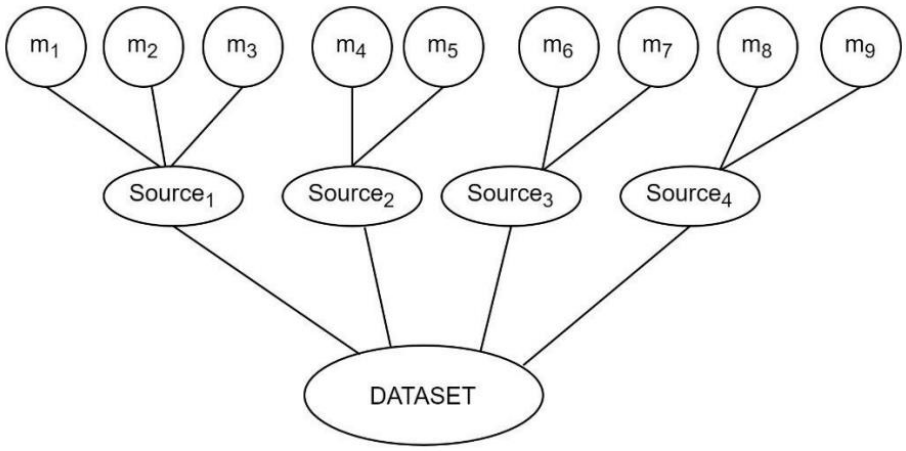


Рисунок 3.1 – Ієрархічний граф ранжування джерел повідомлень соцмережі

Таким чином, кожне повідомлення мережі знаходиться на відповідному рівні глибини дерева повідомлень на стіні джерела, пост – є коренем дерева, коментар на пост - повідомлення розміщується на другому рівні дерева, відповідь на коментар - третій рівень. Кожному повідомленню присвоюється числовий коефіцієнт (табл. 3.1). Залежно від кількості повідомлень на стіні, джерела соцмережі можуть бути розділені потенціалами:

1. Потенціал джерела низький (low index) - $P_{LI} = 0,$ відповідає нерівності (3.1):

$$f_1\left(S_p\right) \le \overline{X_1} = \frac{\sum_{i=1}^{n} x_i}{n}, \tag{3.1}$$

де $\sum_{i=1}^{n} x_i$ – сума числових коефіцієнтів повідомлень соцмережі на стіні джерела, $\overline{X_1}$ - середньоарифметичне у наборі даних для DATASET, n – кількість повідомлень джерела.

2. Потенціал джерела середній (medium index) - $P_{MI} = 1,$ відповідає нерівності (3.2):

$$f_2\left(S_p\right) \le \overline{X_2} = \frac{\sum_{i=1}^{n} x_i}{n}, \tag{3.2}$$

де $\overline{X_2}$ - середньоарифметичне значення у наборі даних для DATASET, отримане після видалення джерел із низьким потенціалом P_{LI}.

3. Потенціал джерела високий (high index) - $P_{HI} = 2,$ відповідає нерівності (3.3):

$$f_3\left(S_p\right) > \overline{X_2} = \frac{\sum_{i=1}^{n} x_i}{n}, \tag{3.3}$$

Таблиця 3.1 − Числові коефіцієнти повідомлень соцмережі на стіні джерела

№	Тип повідомлення	Коефіцієнт
1	Пост	1
2	Коментар	0,5
3	Відповідь на коментар	0,25

Всі джерела повідомлень в наборі даних DATASET можуть бути ранжовані за потенціалом в залежності від глибини та кількості на стіні джерела повідомлень. Алгоритм ранжування джерел повідомлень за потенціалом наведений на рис. 3.2.

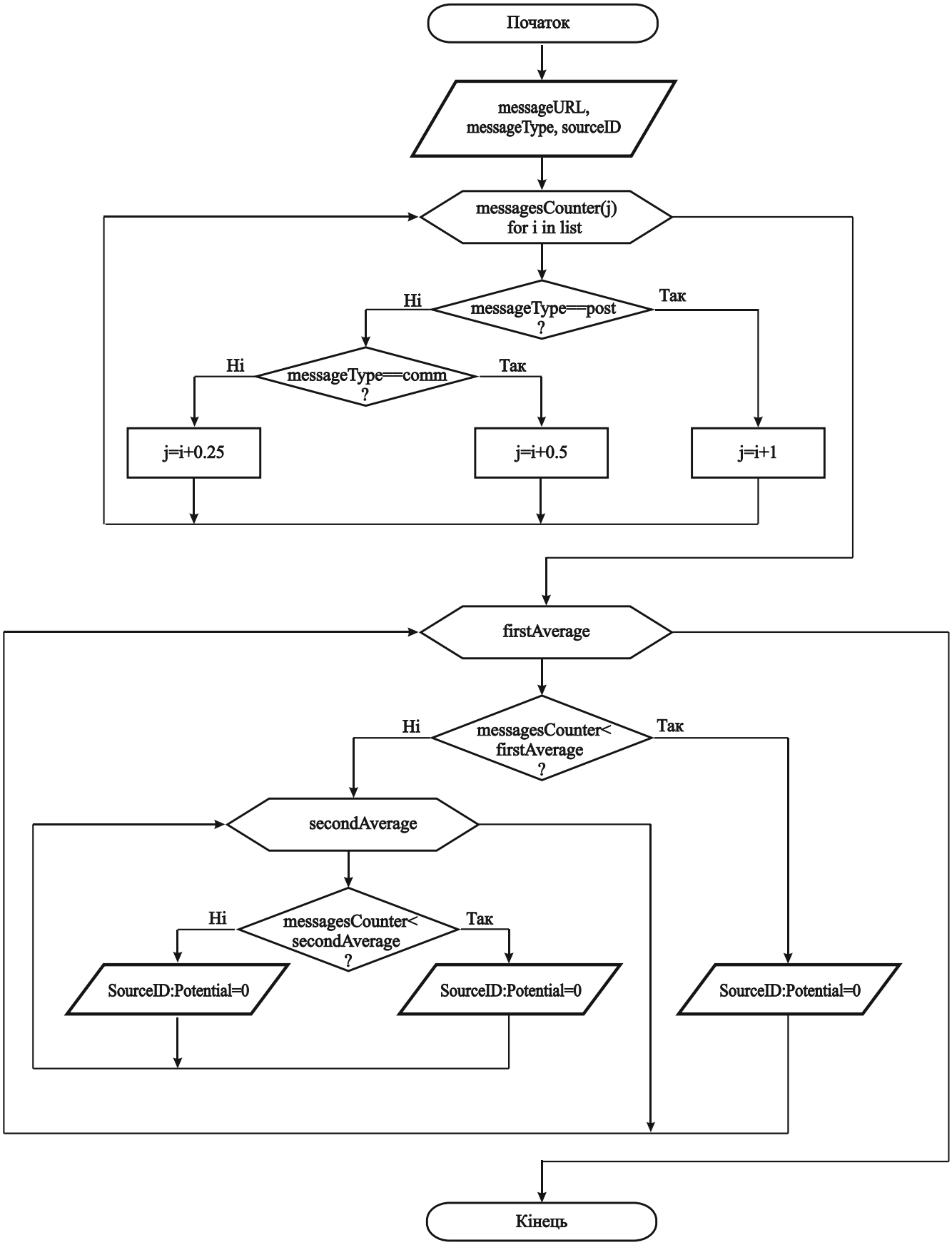


Рисунок 3.2 –Алгоритм ранжування джерел повідомлень за потенціалом

Таким чином, на вхід алгоритму (рис. 3.2) набір записів <messageURL, messageType, sourceID>, обробка інформації відбувається наступним чином:

1. Кожному повідомленню задається значення числового коефіцієнта, взалежності від типу повідомлення (атрибут messageType), сумуються числові коефіцієнти повідомлень відповідного джерела. На виході отримаємо кортеж <sourceID, message_Count>.

2. Розрахунок середньоарифметичного значення кількісті повідомлень, відповідних джерел. Для джерел з меншим message_Count значенням, ніж перший присвоюється відповідний показник низького потенціалу - 0. Джерела з низьким потенціалом формують новий кортеж <sourceID, message_Count>.

3. Розрахунок наступного середньоарифметичного значення кількісті повідомлень, відповідних джерел. Для джерел з значенням меншим або рівним другому середньоарифметичному message_Count присвоюється відповідний показник потенціалу - 1. Для джерел із значенням кількісті повідомлень message_Count більшим середньоарифметичного – показник потенціалу -2.

На виході алгоритму (рис. 3.2) формується кортеж <sourceID, potentialIndex>. Алгоритм ранжування за потенціалом джерел повідомлень враховує: глибину розташування на сторінці в соцмережі повідомлень, кількість опублікованих повідомлень.

3.2 Алгоритм оцінки джерел повідомлень соціальної мережі та сортування об'єктів впливу

Протидія поширенню шкідливої інформації може здійснюватися на основі дослідження та аналізу джерел повідомлень. Об'єктом, є користувачі соцмережі, деструктивного впливу шкідливою інформацією [14]. Кожен користувач залишає відповідний слід під час перегляду повідомлення в мережі, і може залишити відповідну реакцію. Таким чином, алгоритм оцінки джерел повідомлень, повинен враховувати зворотній зв'язок від користувачів шкідливої інформації в соцмережі,

у процесі інформаційного обміну. Множина *ACTIVITY* (3.4) включає всі ознаки зворотнього зв'язок від користувачів шкідливої інформації соцмережі,

$$ACTIVITY\{countrepost, countLike, countComment, countView\}, \quad (3.4)$$

де *countrepost* – кількість посилань на джерело («репостів»), *countLike* - кількість позначок, *countComment* – кількість коментарів, *countView* – кількість переглядів. До множини $SOURCE\{sourceID, messageURL\}$ входить ідентифікатор джерела, адреса повідомлень у соцмережі.

Таким чином, необхідно знайти кортеж атрибутів, на основі елементів множини *ACTIVITY* і відношення *R* (3.5), які характеризуть *SOURCE*.

$$R(SOURCE, MESSAGE) - < index_{active}, index_{viewability}, index_{impact} >, \quad (3.5)$$

де $index_{active}$ - індекс активності, $index_{viewability}$ - індекс перегляду, $index_{impact}$ - індекс впливу джерела повідомлень.

Значення індексів перегляду, активності, пливовості джерела повідомлень знаходиться в діапазоні 0 - 2, до значень індексів застосовується нормування– порівняльна нормалізація, ідеальне значення є максимум.

Розглянемо алгоритм оцінки джерел повідомлень соцмережі:

1. На вхід алгоритму подається кортеж:

$< sourceID, messageURL, repostCount, likesCount, commentCount, viewCount >$

<messageURL,

2. Обчислення індексу активності джерел повідомлень соцмережі: формуються хеш-таблиці (key-value), <sourceID, urlCOUNTER>, <messageURL, likesCount>, <messageURL, commentCount>, <messageURL, repostCount>; в наступній хеш-таблиці сумуються показники commentCount, repostCount likesCount для messageURL, формується, в даному випадку кортеж $< message.SourceID, activityIndex >$; значення з кортежу $< message.SourceID, activityIndex >$ сумуються, результат ділиться на показник

urlCOUNTER з першої хеш-таблиці, таким чином формується набір індексів активності джерела повідомлень, до яких застосовується нормування.

3. Обчислення індексу перегляду джерел повідомлень соцмережі: формуються хеш-таблиці (key-value), $\{SourceID : urlCOUNTER,\ messageURL : viewCount\}$. Значення viewCount всіх *messageURL* сумуються і отриманий результат ділиться на *urlCOUNTER*. В результаті формується кортеж $< SourceID,\ viewIndex >$. Індекси переглядів нормуються.

4. Обчислення індексу впливу джерела повідомлень соцмереж: для кожного джерела повідемлень перемножуються індекс переглядів та активності, в результаті отримаємо значення індексу впливовості, також для нього використаємо порівняльне нормування. На виході алгоритму оцінки джерел повідомлень соцмережі формується кортеж $< sourceID,\ activityIndex, viewIndex, impactIndex >$.

Алгоритм оцінки джерел повідомлень соцмережі в процесі інформаційного обміну враховує зворотній зв'язок, його кількісні характеристики від аудиторії поширення шкідливої інформації, перетворює їх у якісні індекси.

Алгоритм сортування об'єктів впливу соціальної мережі (рис. 3.3). В основі існуючих рішень, методів поширення та протидії шкідливої інформації в соцмережах лежать підходи виявлення із шкідливою інформацією інформаційних об'єктів. Розглянуті підходи опираються на концепцію - «виявлення-протидія» інформаційних об'єктів. Інформаційні об'єкти, які містять джерела шкідливої інформації в соціальних мережах - мільйони. Інформаційні об'єкти можливо розділити між собою за індексами активності та потенціалом джерела, таким чином, можна застосувати фільтр у процесі вибору інформаційного об'єкта протидії та задати пріоритет. Алгоритм сортування інформаційних об'єктів впливу соцмережі пов'язаний із алгоритмами оцінкою джерел та ранжування за потенціалом, отримує вхідні дані з них, сортує інформаційні об'єкти впливу

пріоритету на виході. Цільова функція об'єктів впливу пріоритету (3.6) задається наступною формулою:

$$f(S) \to l_{pr}^{s} = l_{p}^{s} + l_{i}^{s} = [0,4], \tag{3.6}$$

де S – джерело повідомлень, l_{pr}^{s} - пріоритет джерела повідомлень, l_{p}^{s} - потенціал, l_{i}^{s} - індекс впливовості.

Правила вибору об'єкта впливу *Target:* $\left\{source \in TARGET \mid I_{pr}^{s} \cong \max\right\}$; $\left\{message \in TARGET \mid I_{pr}^{s} \cong \min\right\}$, де $TARGET$ - множина інформаційних об'єктів впливу. Алгоритм сортування об'єктів впливу соцмережі наведено на рис. 3.3.

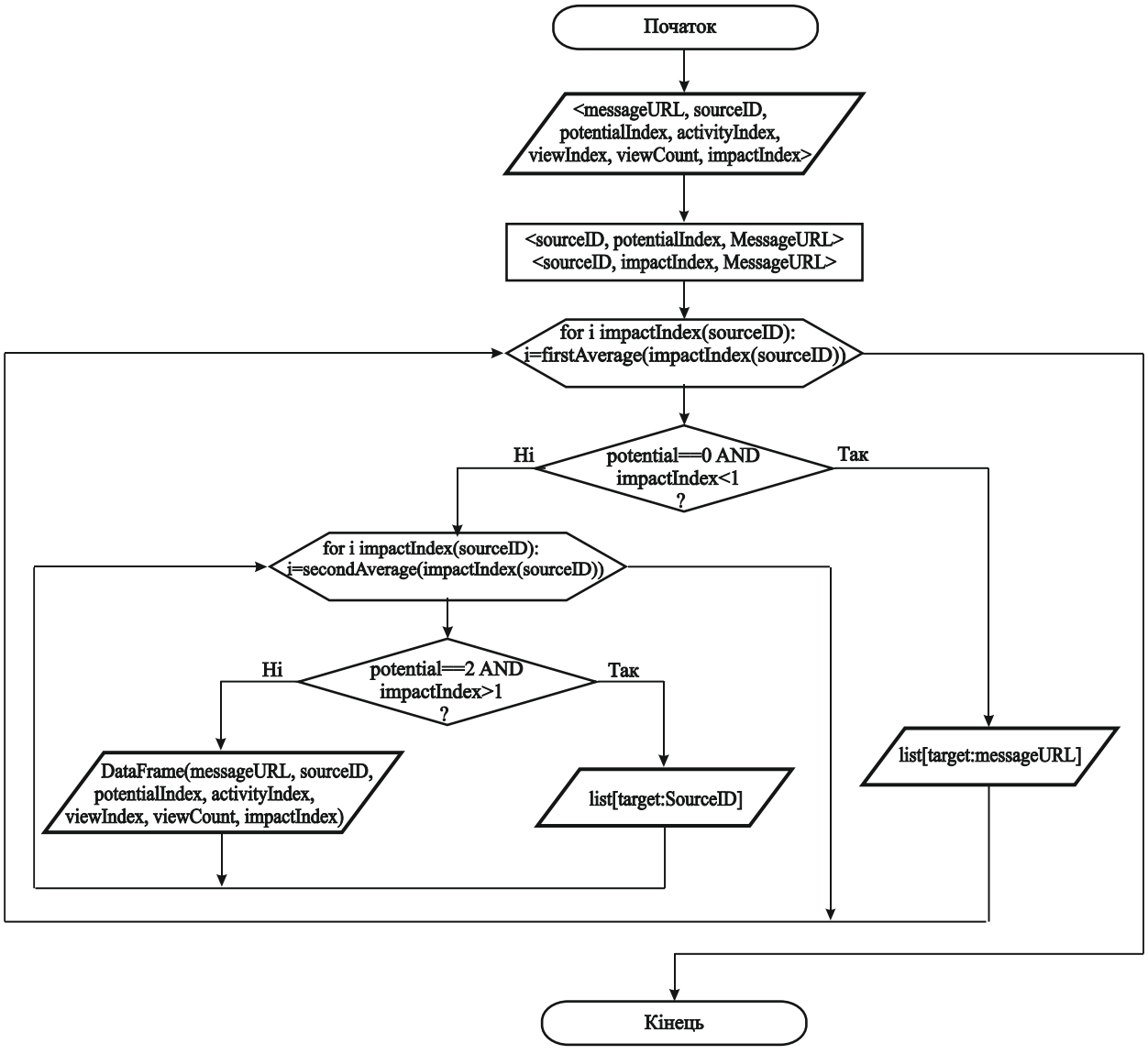


Рисунок 3.3 – Алгоритм сортування об'єктів впливу соціальної мережі

На вхід алгоритму сортування об'єктів (рис.3.3) передається набір кортежів $< messageURL, sourceID, potentialIndex, activityIndex, viewIndex, impactIndex >$. На першому етапі роботи алгоритму обчислюється середнє арифметичне індексу об’єктів впливу всіх джерел повідомлень, виділяються об'єкти з низьким та високим пріоритетом. Формуються кортежі з індексом пріоритету $1 \le l_{pr}^{s} \le 3$

$< messageURL, sourceID, potentialIndex, activityIndex, viewIndex, impactIndex >$.

Результат роботи алгоритму- набір кортежів та два списки: набір кортежів Priority_Medium, передається оператору для вибору та додаткової оцінки інформаційного об'єкта впливу між адресою сторінки в соцмережі та адресою повідомлення; Priority_High – цілі Target, sourceID є інформаційним об'єктом впливу, для прийняття заходів протидії мають високий пріоритет; Priority_Low – цілі Target, messageURL є інформаційним об'єктом впливу, для прийняття заходів протидії мають низький пріоритет.

Алгоритм сортування інформаційних об'єктів впливу соціальної мережі формує пріоритетні списки для протидії поширенню шкідливої інформації.

3.3 Алгоритм протидії та виявлення в соціальних мережах поширення шкідливої інформації

Для ранжування заходів протидії поширення шкідливої інформації в соцмережах використовується оцінка складності, визначається експертами, на основі особливостей заходів протидії та доступних ресурсів. Результатом є список цілей заходів протидії поширення шкідливої інформації, який на основі метрики ранжований, враховує властивості інформаційного об'єкта впливу, складність міри протидії [13]. Для розробки алгоритму ранжування контрзаходів протидії використовується відповідно діаграма протидії (рис. 3.4). Узагальнюючим класом виступає клас контрзаходів протидії, для всіх класів забезпечення інформаційної безпеки: управлінські заходи; технічні заходи; організаційні заходи. Клас

контрзаходів протидії пов'язаний із класами: метод впливу; мета дії; тип дії. Клас протидії пов'язаний наступним чином – зміна в операціях, в атрибутах у цих класів приводить до необхідності змін в класі контрзаходу протидії.

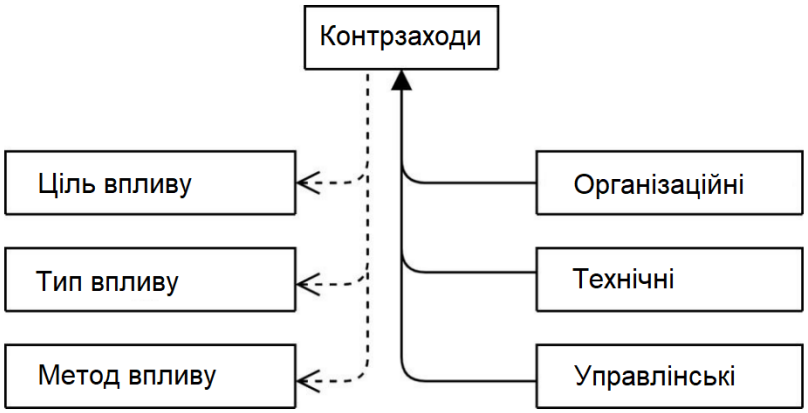


Рисунок 3.4 – Діаграма класів вибору контрзаходів протидії

Проведений аналіз досліджень заходів протидії показав - при виборі контрзаходів протидії необхідно враховувати параметри: доступні ресурси (відсутність або наявність подання скарги у суд); складність реалізації заходів протидії (автоматичний значно простіший, ніж ручний).

Алгоритм контрзаходів протидії складається з наступних станів інформаційних об'єктів, які є складовими суперкласу {контрзаходи}, задача – вибрати налаштування контрзаходів протидії:

1. Формування списків - списку контрзаходів. Список контрзаходів задається оператором: обраний зі списку, представлених у базі даних; створений з нуля.

2. Класифікація контрзаходів протидії. Виділимо властивостей, задамо пов'язані з контрзаходами, класи та їх атрибути [14]: метод впливу: ручний – необхідне втручання оператора для розробки унікального сценарію, автоматизований – необхідне підтвердження від оператора, автоматичний - спеціальні сценарії системою застосовуються без участі; тип впливу: шум (нейтральний) - протидія передбачає в інформаційному просторі зниження популярності шкідливої інформації, розмиття уваги, поширенням альтернативної точки зору, заміщення (позитивний) - протидія передбачає наповнення соцмереж

інформаційного простору позитивною інформацією, не пов'язаною з шкідливою інформацією, блокування (негативний) - протидія передбачає в інформаційному просторі соцмереж зниження об’єму поширення шкідливої інформації, спрямований на блокування в мережі джерел повідомлень.

3. Формування властивостей контрзаходів протидії. Для контрзаходів протидії визначено ряд класів властивостей (3.7):

$$KC_i \in KC, \tag{3.7}$$

де KC – множина класів властивостей контрзаходів протидії поширенню шкідливої інформації в соцмережах, KC_i – i-й клас властивостей контрзаходів протидії. Для кожного i-го класу задана вага w_i - визначає внесок у складність контрзаходу від i-го. Кожен KC_i містить набір екземплярів - визначають значення даної властивості (3.8):

$$kc_{ij} \in KC_i, \tag{3.8}$$

де kc_{ij} – екземпляри i-го класу властивостей контрзаходів протидії. Для кожного екземпляра i-го класу властивостей контрзаходів протидії задається рівень складності lc_{ij} - визначає внесок у складність контрзаходу протидії екземпляра класу. Кожен з контрзаходів протидії визначає свою початкову складність - cw_x. Контрзахід протидії визначається як вибір з доступних екземплярів одного екзампляра для i-го класу властивостей контрзаходів протидії $c_x \in C$, значення властивості cp_{xij}, визначеного i-м класом властивостей контрзаходів протидії. KC_i – приймає значення $\{1,0\}$, взалежності чи належить контрзахід протидії до екземпляра i-го класу властивостей kc_{ij}. Таким чином:

$$\forall c_x, \forall KC_i, \sum_{j=1}^{|KC_i|} cp_{xij} = 1, \tag{3.9}$$

конкретний захід може мати одне значення, визначається конкретним класом властивостей контрзаходів протидії. Множина контрзаходів - набір комбінацій

властивостей заходів протидії. Повний список контрзаходів протидії поширенню шкідливої інформації в соцмережах представлений у табл. 3.1.

Таблиця 3.1 −Список контрзаходів протидії поширенню шкідливої інформації

C	W	KC								
		KC_1			…			KC_p		
		w_1			…			$w_{\|KC\|}$		
		$kc_{1,1}$	…	$kc_{1,\|KC_1\|}$	…	…	…	$kc_{\|KC\|,1}$	…	$kc_{\|KC\|,\|KC_p\|}$
		$lc_{1,1}$	…	$lc_{1,\|KC_1\|}$	…	…	…	$lc_{\|KC\|,1}$	…	$lc_{\|KC\|,\|KC_p\|}$
c_1	cw_1	$cp_{1,1,1}$	…	$cp_{1,1,\|KC_1\|}$	…	…	…	$cp_{1,\|KC\|,1}$	…	$cp_{1,\|KC\|,\|KC_p\|}$
…	…	…	…	…	…	…	…	…	…	…
c_n	c_{wn}	$cp_{n,1,1}$	…	$cp_{n,1,\|KC_1\|}$	…	…	…	$cp_{n,\|KC\|,1}$	…	$cp_{n,\|KC\|,\|KC_p\|}$

4. Оцінка складності реалізації контрзаходу протидії поширенню шкідливої інформації. Метрика складності реалізації контрзаходу протидії $c_x \in C$, задана функцією (3.10):

$$complexity(c_x) = cw_x \cdot \sum_{i=1}^{|KC|} w_i \cdot \left(\sum_{j=1}^{|KC_i|} \left(cp_{x,i,j} \cdot lc_{x,i,j} \right) \right) \quad (3.10)$$

Результат роботи алгоритму - набір кортежів з оцінками складності для контрзаходу протидії поширенню шкідливої інформації в соцмережах $< c_x, complexity(c_x) >$. Таким чином, кожен контрзахід протидії c_x має власну метрику складності і можливо провести ранжування в системі.

Представимо у вигляді атрибутів, аналіз джерел повідомлень та ранжирування контрзаходів протидії з метою вибору інформаційного об'єкта впливу на поширення шкідливої інформації у соцмережах:

1. $Sources =< messageURL, messageType, sourceID >$. Кортеж $Sources$ містить наступні поля: $messageURL, messageType, sourceID$.

2. $Messages =< messageURL, sourceID, likesCount, commentCount,$
$repostCount, viewCount, subscriberCount >$

Кортеж *Messages* містить наступні поля: *sourceID* – ідентифікатор джерела повідомлення, де повідомлення опубліковано, *messageURL* – адреса повідомлення в Інтернет та соціальній мережі, *likesCount* – кількість лайків «мені модобається», *commentCount* –кількість коментарів, *subscriberCount* –кількість передплатників, *repostCount* – кількість репостів, *viewCount* – кількість переглядів.

3. $\Pr iorities =< messageURL, sourceID, potentialIndex, activityIndex, viewIndex, impactIndex >$

Кортеж $\Pr iorities$ містить наступні поля: $messageURL, sourceID$, *activityIndex* – індекс активності джерела соцмережі, *potentialIndex* – потенціал джерела повідомлення, *impactIndex* - індекс впливу, *viewIndex* - індекс перегляду.

4. $Countermeasures =< type_{action}, method_{action}, level_{complexity}, class_{weight}, applicability_{factor}, cw, complexity >$

Кортеж *Countermeasures* містить наступні поля: $type_{action}$ -тип впливу, впливу, $method_{action}$ – метод впливу, $class_{weight}$ – вага класу контрзаходів протидії, $level_{complexity}$ - рівень складності реалізації контрзаходів протидії, $applicability_{factor}$ – застосовність контрзаходів протидії, *cw* – початкова складність контрзаходу протидії, *complexity* - складність реалізації конкретної контрзаходу.

Діаграма комплексу алгоритмів проведення аналізу джерел повідомлень соціальної мережі та ранжування контрзаходів протидії поширенню шкідливої інформації в мережах представлена на рис. 3.5.

Запропонований комплекс алгоритмів проведення аналізу джерел повідомлень соціальної мережі та ранжування контрзаходів протидії поширенню шкідливої інформації в мережах відрізняється від аналогів, з урахуванням атрибутів: активність користувачів на сторінці джерела повідомлень, потенціал джерела, кількість переглядів повідомленнь з вмістом шкідливої інформації, кількість передплатників джерела та друзів.

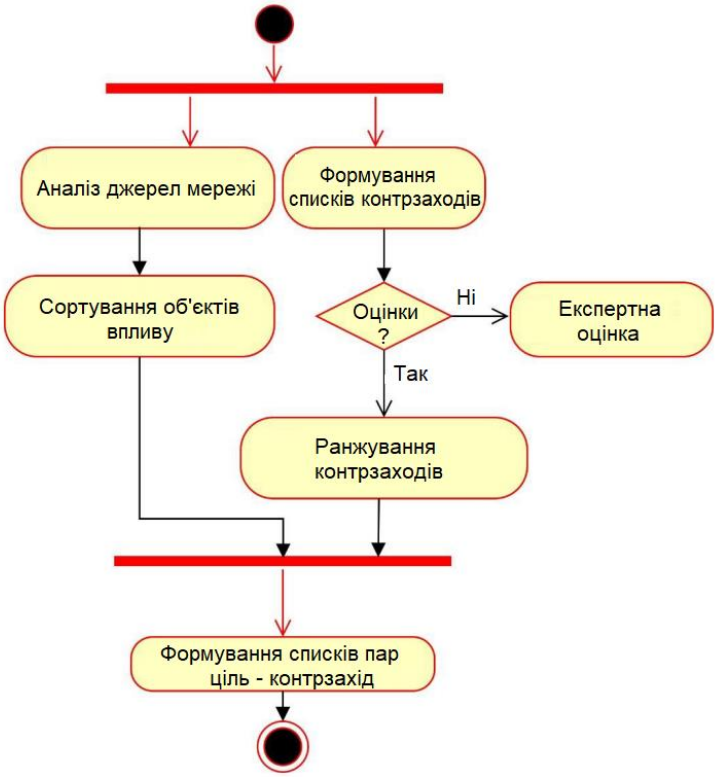


Рисунок 3.5 – Діаграма алгоритмів аналізу джерел повідомлень та ранжування контрзаходів

3.4 Висновки

Розроблено комплекс алгоритмів ранжирування контрзаходів протидії, аналізу джерел поширення шкідливої інформації в соцмережі; враховуються наступні атрибути: активність аудиторії на сторінці джерела, кількість друзів та передплатників джерела, потенціал джерела, кількість переглядів зі шкідливою інформацією повідомлення. Запропонований комплекс алгоритмів дозволяє сформувати вимоги до методу протидії поширенню шкідливої інформації в сошмережах і є основою системи прийняття рішень. Представлені результати розробки алгоритмів та діаграм, дозволяють ранжувати об'єкти впливу та оцінювати джерело повідомлень, задіяти контрзаходи для реалізації заходів протидії поширенню шкідливої інформації у соцмережах, як результат, підвищення ефективність протидії поширенню шкідливої інформації за рахунок застосування цільових заходів.

4 МЕТОД ПРОТИДІЇ ТА ВИЯВЛЕННЯ В СОЦІАЛЬНИХ МЕРЕЖАХ ПОШИРЕННЮ ШКІДЛИВОЇ ІНФОРМАЦІЇ

4.1 Метод протидії в соціальних мережах поширенню та виявлення шкідливої інформації

Метод протидії в соціальних мережах шкідливої інформації вирішує задачу інформаційної підтримки процесу ухвалення рішень, включає: проведення аналізу обробленої та зібраної інформації; вироблення на основі проведеного аналізу варіантів рішень; проведення оцінки варіантів, вибір найкращого; надання обраного та альтернативних варіантів, особі, яка приймає рішення, з обґрунтуванням вибору.

Метод протидії, відповідно до життєвого циклу інформаційних систем, подіфляєлься на два етапи: налаштування та експлуатації. На стадії формування вхідних даних та налаштування протидії задаються: списки доступних у системі контрзаходів, їх коефіцієнти; списки інформаційних загроз; списки доступних агентів реалізації; формується список ранжированих контрзаходів. Стадія експлуатації включає: аналіз об'єктів впливу та сортування; отримання інформації від системи моніторингу; формування пар ціль-контрзахід; запуск протидії.

На рисунках 4.1 та 4.2 наведено загальне представлення методу протидії в соціальних мережах поширенню та виявлення шкідливої інформації.

Стадія налаштування методу протидії та формування вихідних даних включає:

1. Налаштування системи запитів. Оператор, відповідно до інформаційно-ознакової моделі загроз, формує список інформаційних загроз та їх ознак. Після отримання від оператора, інформаційних загроз та їх ознак, формується перелік загроз та ознак (табл. 4.1). Списки загроз та їх ознак отриманих в результаті виконання налаштування системи запитів зберігаються у загальне сховище даних.

Таблиця 4.1 − Список загроз та їх ознак

Загроза	Шкідлива інформація у соцмережах	Інформаційні ознаки
T_1	Наркотики купити	a_1
	Наркотики рецепт виготовлення	a_2
T_2	Вибуховий пристрій набір для збирання з інструкцією	b_1
T_3	Секретний алгоритм захисту телефонних дзвінків	c_1

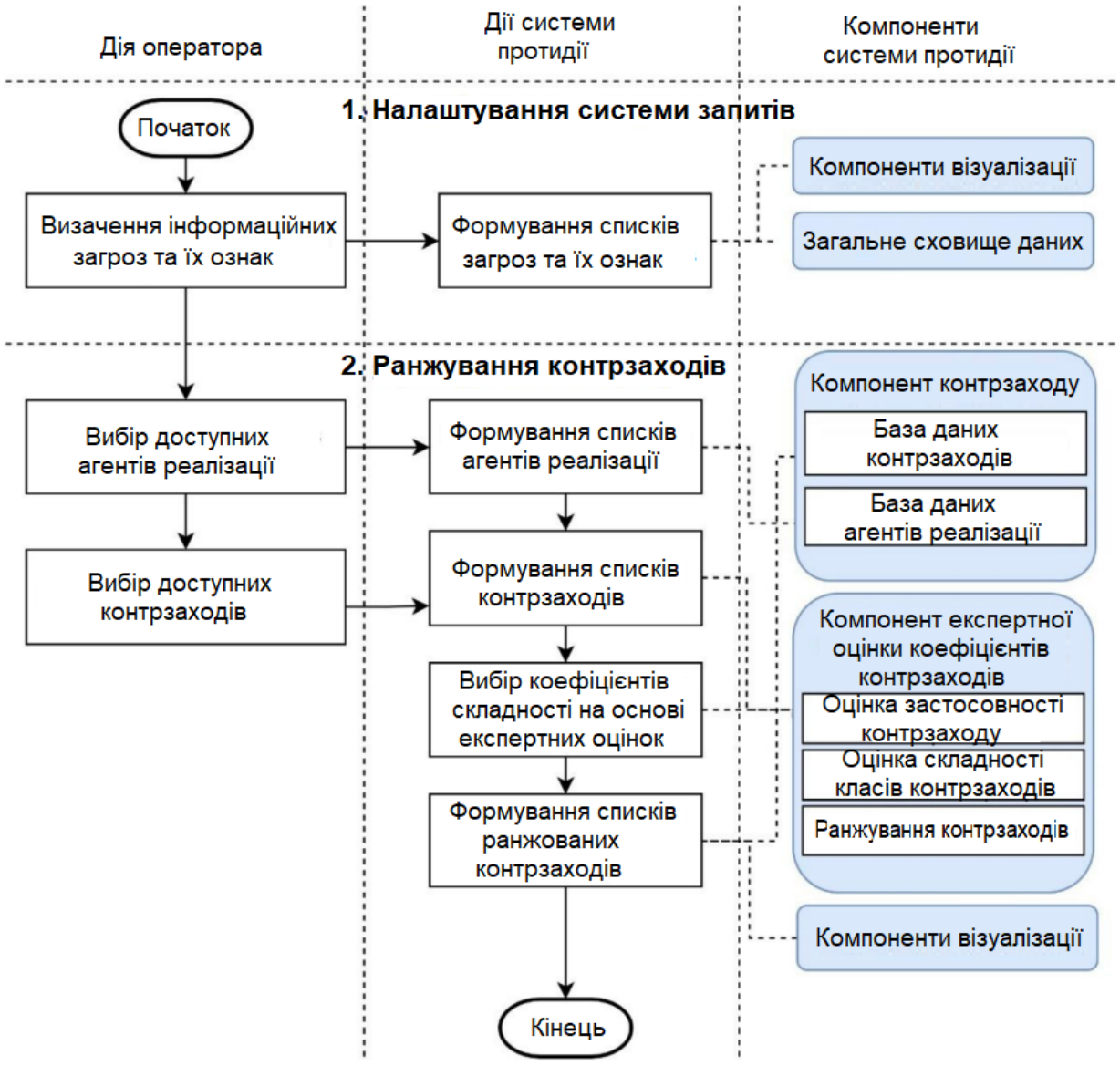


Рисунок 4.1 – Метод протидії в соціальних мережах поширенню та виявлення шкідливої інформації

2. Ранжування контрзаходів. Оператор вибирає доступні агенти реалізації: браузер; оператор зв'язку; black_list; антивірус; система батьківського контролю; операційна система. Формується та зберігається список доступних агентів реалізації. Оператор вибирає доступні контрзаходи: блокування через соцмережу; блокування через оператора зв'язку; блокування через спеціальне програмне забезпечення; блокування через black_list; фільтрація через систему батьківського контролю; фільтрація через антивірус. Формується список контрзаходів протидії, на основі експертних оцінок формуються коефіцієнти складності, згідно до алгоритму вибору коефіцієнтів складності. Алгоритм вибору коефіцієнтів складності використовує наступні величини: вага w_i, визначає внесок у складність контрзаходу класу KC_i; рівень складності $lc_{i,j}$, визначає внесок у складність контрзаходу екземпляра класу $kc_{i,j}$; початкова складність cw_x заходу протидії. Величини залежать від кваліфікації співробітників, доступних ресурсів та задаються експертним шляхом. Для вибору значень пропонується використовувати Дельфі-метод експертних оцінок, в результаті серії дій експертів формується узагальнений результат, який дозволяє уникнути суб'єктивних оцінок.

Алгоритм вибору коефіцієнтів складності включає наступні кроки:

1. Вибір експертів. Групі експертів надаються відомості про можливі заходи протидії.

2. Голосування. Визначаються властивості які застосовуються до заходів протидії. Для кожної величини $cp_{x,i,j}$ експерти виставляють оцінки застосовності від одиниці до десяти.

3. Опрацювання результатів. Виконується усереднення отриманих значень (4.1):

$$cp_{x,i,j} = \frac{\sum_{l=1}^{N} cp_{x,i,j,l}}{10 \cdot N} \tag{4.1}$$

Отримане значення округляється до 0 чи 1, і визначається, чи застосовний даний екземпляр $kc_{i,j}$ класу властивостей заходів протидії для даного контрзаходу.

4. Голосування. Для уточнюючих величин $\left(w_i, lc_{i,j}\right)$ експерти виставляють оцінки складності від 1 до 10.

5. Опрацювання результатів. Виконується усереднення отриманих значень (4.2):

$$\begin{aligned} w_i &= \frac{\sum_{l=1}^{N} w_{i,l}}{N} \\ lc_{i,j} &= \frac{\sum_{l=1}^{N} lc_{i,l}}{N} \end{aligned} \tag{4.2}$$

6. Голосування. Експерти для заходів протидії виставляють оцінки початкової складності cw_x від 1 до 10.

7. Опрацювання результатів. Виконується усереднення для початкової складності отриманих значень (4.3).

$$coefficient\left(cw_i\right) = \frac{\sum_{l=1}^{N} cw_{x,l}}{N} \tag{4.3}$$

Результатом роботи алгоритму є отримані показники визначення складності застосування заходів протидії.

Розглянемо метод протидії в соціальних мережах поширенню та виявлення шкідливої інформації на стадії експлуатації. Етап експлуатації аналізу об'єктів впливу та запиту інформації містить наступні кроки:

1. Запит на збирання інформації (даних). Оператор із збереженого списку вибирає інформаційні загрози, задає нові інформаційні ознаки, у випадку необхідності. Оператор запускає процес збирання інформації, система протидії поширенню та виявлення шкідливої інформації надсилає запит до моніторингу зовнішніх систем та отримує, як результат, набір даних із повідомленнями, джерелами та параметрами, що містять шкідливу інформацію, необхідними для подальшого аналізу.

2. Сортування та ранжування об'єктів впливу: джерела ранжуються за потенціалом та оцінюються, формуються кортежі $< messageURL, sourceID, potentialIndex, activityIndex, viewIndex, impactIndex >$. Далі

сортуються інформаційні об'єкти впливу за пріоритетом, формуються списки, які в результаті передаються оператору.

3. Протидія поширенню шкідливої інформації в соцмережах. Оператор системи отримує інформацію про потенціал джерела мережі, на яке, опублікованих на його сторінці у соцмережі, впливає кількість повідомлень, інформацію про пріоритет впливу, на який впливає кількість переглядів, рівень активності користувачів джерела. Оператор коригує списки об'єктів впливу, формуються пари ціль-контрзахід, перевірка відповідних пар оператором та запуск системи протидії поширенню шкідливої інформації в соцмережах.

Оператор передає команду на запуск системи протидії поширенню шкідливої інформації в соцмережах, запускається через агентів реалізації, демонструє проміжні результати процесу проведення протидії оператору системи. Формується звіт про результати роботи системи протидії, інформаційній загрозі та визначеними у ході експлуатації системи об'єктів впливу протидію.

Вхідними даними методу протидії поширенню шкідливої інформації в соцмережах є: параметри об'єктів впливу, відповідно до яких оператор розподіляє про протидію черговість прийняття рішення; сформовані пари ціль-контрзахід для протидії поширенню шкідливої інформації у соцмережах через доступні агенти реалізації; контрзаходи та їх коефіцієнти, інформаційні загрози, доступні агенти реалізації заходів протидії, ознаки.

Запропонований метод протидії виявлення та поширенню шкідливій інформації в соцмережах, з урахуванням вимог до обґрунтованості, на різних етапах життєвого циклу дозволяє: визначити потенціал джерела повідомлень, значення якого залежить від кількості повідомлень на сторінці; оцінити індекс активності джерела повідомлень мережі, на значення впливає рівень активності користувачів повідомлень із вмістом шкідливої інформації; оцінити індекси перегляду повідомлень мережі, також джерела; визначити індекс впливу джерела повідомлень, значення залежить від активності та перегляданості інформації в цілому.

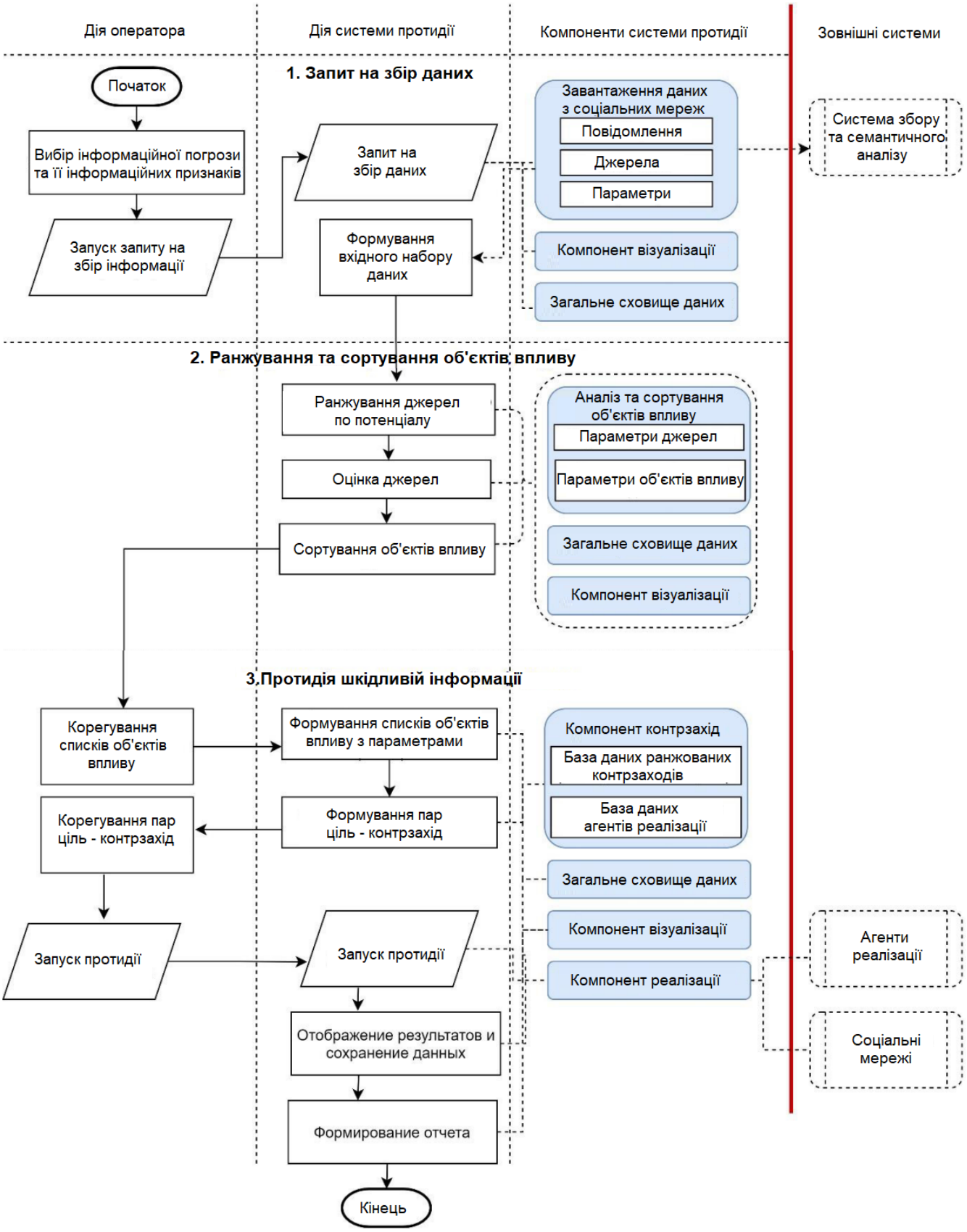


Рисунок 4.2 – Метод протидії в соціальних мережах поширенню та виявлення шкідливої інформації на стадії експлуатації

Метод протидії, також дозволяє: визначити пріоритет об'єкта впливу протидії, на об'єкт впливу впливають індекс впливовості та потенціал джерела; для підтримки прийняття рішення оператором, сортувати об'єкти впливу протидії за пріоритетом вибору об'єкта; сформувати відповідні пари ціль-контрзахід, для підтримки прийняття відповідного рішення про протидію поширення шкідливої інформації в соціальній мережі.

Розроблений метод протидії виявлення та поширенню шкідливій інформації в соцмережах відрізняється від існуючих, використанням алгоритмів оцінки джерел, ранжирування та аналізу контрзаходів, в результаті підвищується обґрунтованість прийняття рішення про протидію поширенню шкідливій інформації цілі та вибору контрзаходу, відповідним чином скорочується час роботи оператора системи у процесі протидії поширенню шкідливої інформації у соцмережах.

4.2 Архітектура компонентів системи протидії в соціальних мережах поширенню та виявлення шкідливої інформації

Аналіз проведених досліджень показав, що лідери у розробці архітектур та систем моніторингу та протидії поширенню та виявлення шкідливої інформації в соцмережах – це великі корпорації. Creopoint Inc - займається блокуванням інформації для відомих мільярдерів та великих брендів, фільтром фальшивих новин. Зареєструвала патент на «Стримування поширення повыдемлень дезінформації з використанням каналів розвідки». Zerofox Inc –на ринку систем протидії поширенню шкідливої інформації та моніторингу, збирає та обробляє дані з Facebook, Instagram, YouTube, Twitter, з сайтів магазинів мобільних додатків. Належить патент на інформаційну систему захисту від підозрілих соціальних суб'єктів мережі[12]. International Business Machines Corp - розробляє продукти в галузі інформаційної безпеки, отримано патент на систему аналітики з боку інтернет-тролів для пом'якшення зловживань в соцмережах[12]. Аналіз проведеного дослідження рішень у галузі розробок систем протидії поширенню

шкідливій інформації, світових виробників, у соцмережах, надав можливість сформувати специфічні та загальні вимоги для систем протидії та поширенню шкідливої інформації: специфічні вимоги - підтримка процесів на запит оператора збору інформації, підтримка процесів сортування об'єктів дії, аналізу джерел повідомлень, підтримка процесів протидії поширенню шкідливої інформації в соцмережах, підтримка процесів ранжирування контрзаходів, формування вихідних даних; загальні вимоги - розділеність на компоненти, розділеність на рівні, взаємодія із зовнішніми системами та сервісами.

Запропоновані алгоритми та метод реалізовані в рамках системи протидії та поширенню шкідливого впливу у соцмережах. Архітектура системи протидії поширенню шкідливої інформації у соцмережах включає вісім компонентів та три рівні (рис. 4.3) - рівень управління: компонент візуалізації, компонент менеджменту; рівень оцінки змісту: компонент оцінки та аналізу джерел повідомлень, база даних, SQL сервер; рівень реалізації контрзаходів: компонент вибору контрзаходів, компонент реалізації контрзаходів. Для визначення функцій системи протидії поширенню шкідливої інформації у СМ, що виконуються компонентами, розглянемо функціональну структуру системи (рис.4.4).

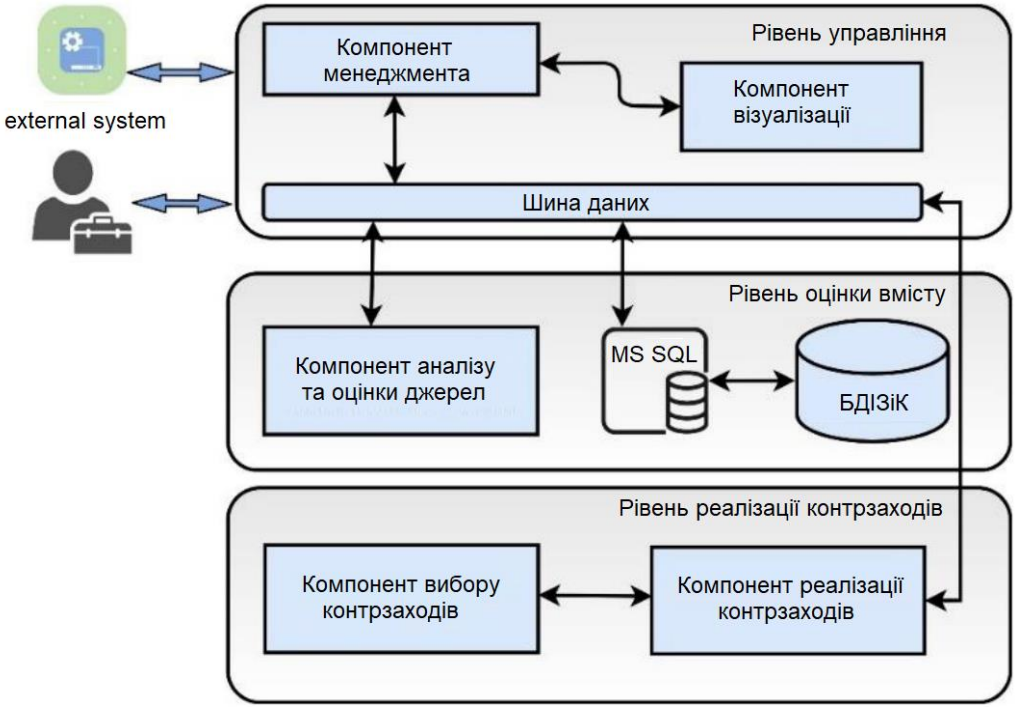


Рисунок 4.3 – Архітектура системи протидії шкідливій інформації в СМ

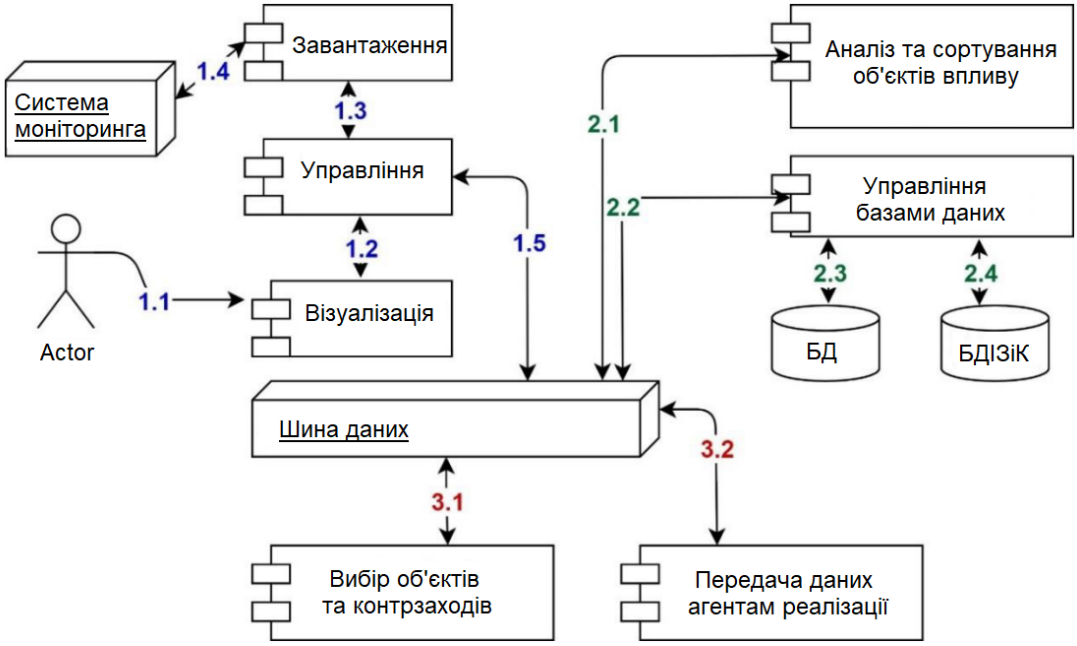


Рисунок 4.4 – Функціональна структура системи протидії поширенню шкідливій інформації у СМ.

Функціональна структура системи протидії поділяється відповідно до рівнів архітектури системи: рівень управління - функції компонента менеджера включають завданнями всередині системи та керування навантаженнями, функції компонента візуалізації із оператором системи протидії забезпечують зв'язок, шина даних призначена для передачі даних між компонентами системи протидії поширенню шкідливій інформації; рівень оцінки змісту - компонент оцінки та аналізу джерел повідомлень включає функції оцінку параметрів об'єктів впливу, ранжування за потенціалом, пріоритезацію, знаходиться компонент для управління базами (SQL Server), керує базою даних контрзаходів та інформаційних загроз; рівень реалізаціїіі контрзаходів – компонент вибору контрзаходів входять функції завдання системи формування списків контрзаходів та цілей підтримки прийняття рішення, а компонент реалізації контрзаходів підтримує зв'язок із системами реалізації, зовнішніми агентами.

Елементи архітектури реалізовані у вигляді програмних прототипів: програмний компонент оцінки та аналізу джерел повідомлень у соцмережах включає алгоритм оцінки джерел повідомлень, алгоритм ранжування джерел,

алгоритм сортування об'єктів впливу; програмний компонент вибору контрзаходів, включає алгоритм експертних оцінок для формування відповідних коефіцієнтів, алгоритм ранжування контрзаходів; прототип бази даних контрзаходів та інформаційних загроз мережі, який містить інформацію про - заходи протидії поширенню шкідливої інформації у соцмережах, про агентів реалізації, типи об'єктів, до яких відповідні контрзаходи можуть бути застосовні та з використанням яких можуть бути реалізовані контрзаходи.

Прототип бази даних контрзаходів та інформаційних загроз є частиною архітектури системи протидії у соцмережах. Формальний вид контрзаходу $Measure$ представлений наступним чином: $Measure = \langle Threat, Countermep \rangle$, де $Threat$ - загроза в соцмережі, $Countermep$ - контрзахід, відповідно до загрози, враховує тип відповідного інформаційного об'єкта, атрибути його реалізації.

Загроза ($Threat$) в соцмережі описується наступними атрибутами:

$$Threat = \langle Definition, Toke, Keys\_words \rangle, \quad (4.4)$$

де, $Definition$ - опис загрози; $Toke$ –ознаки загрози інформаційній безпеці, що дозволяють комусь оператору, однозначно класифікувати загрозу; $Keys\_words$ – семантичні ознаки загрози.

$Countermep$ (контрзахід) в соцмережі описується наступними атрибутами:

$$Countermep = \langle Object, Agent, \mathrm{Im}\, plementation_{type}, Phase \rangle, \quad (4.5)$$

де, $Object$ - інформаційний об'єкт мережі, до якого застосовується контрзахід; $Agent$ - агент реалізації, з використанням якого, реалізований контрзахід; $\mathrm{Im}\, plementation_{type}$ - тип реалізації контрзаходу (авто, ручний); $Phase = Static \vee Dynamic$ – відповідний етап реалізації контрзаходу: на етапі реагування на поширення шкідливої інформації ($Dynamic$ - динамічні контрзаходи) і на етапі запобігання поширення шкідливої інформації($Static$ – статичні контрзаходи).

Програмний компонент оцінки та аналізу джерел у соцмережах складається з пов'язаних у комплекс наступних алгоритмів: алгоритм ранжирування джерел повідомлень по потенціалу; алгоритм оцінки джерел мережі по активності; алгоритм сортування інформаційних об'єктів впливу. На вхід алгоритму ранжування джерел повідомлень мережі по потенціалу подаються кортежі $\langle messageURL, messageType, sourceID \rangle$, на виході – набір $\langle sourceID, potentialIndex \rangle$. кортежів <sourceID, potentialIndex>. На вхід алгоритму оцінки джерел повідомлень мережі по активності подаються кортежі $\langle messageURL, sourceID, likesCount, commentCount, repostCount, viewCount, subscriberCount \rangle$, на виході – набір кортежів $\langle sourceID, activityIndex, viewIndex, impactIndex \rangle$.

4.3 Оцінка методу протидії в соціальних мережах поширенню та виявлення шкідливої інформації

Основні вимоги до методу протидії в соціальних мережах поширенню та виявлення шкідливої інформації, поділені на групи: оперативність; обґрунтованість; ресурсоспоживання.

Оцінка оперативності відповідає наступним крокам: на стадії налаштування системи протидії поширенню шкідливій інформації - ранжування контрзаходів, налаштування системи запитів; на стадії експлуатації системи протидії поширенню шкідливій інформації - запит на збирання даних, сортування та ранжування інформаційних об'єктів дії, протидія поширенню шкідливої інформації. Час виконання процесу протидії поширенню шкідливої інформації в соцмережах буде складатися з тривалості операцій проведення аналізу наступних кроків (4.6):

$$T^M = T_1^{HC} + T_2^{HC} + T_1^{EC} + T_2^{EC} + T_3^{EC}, \quad (4.6)$$

де T_i - час виконання і-го кроку.

Час виконання кроків процесу протидії поширенню шкідливої інформації в соцмережах розглядається як випадкова величина, ймовірність підпорядковується закону нормального розподілу. Очікуваний час процесу протидії поширенню шкідливої інформації в соцмережах та його дисперсія розраховується з використанням двооцінної методики [12]. Імовірність, що час виконання *i*-го кроку не буде перевищувати допустимого значення $T^{additional}$, обчислюється за наступною формулою (4.7):

$$P_{op}\left(T \le T^{additional}\right) = \Phi\left(Z\right), \tag{4.7}$$

де $\Phi\left(Z\right)$ –функція Лапласа для (4.8):

$$Z = \frac{T^{additional} - \sum_{i=1}^{n} T_i}{\sqrt{\sum_{i=1}^{n} \sigma_i^2\left(T_i\right)}} \tag{4.8}$$

Найвитратнішим процесом протидії поширенню шкідливої інформації в соцмережах з погляду оперативності є час роботи оператора відповідно на кроках 1,2 на стадії налаштування системи та на стадії експлуатації на кроках 1, 3.

Експертами проведено оцінку наступних задач: час, необхідний оператору для визначення інформаційних загроз, їх ознак (експерт заповнює таблицю з трьома загрозами та їх ознаками; час, який оператор витрачає на вибір відповідних доступних агентів реалізації та контрзаходів (експерт заповнює таблицю з доступними агентами реалізації та контрзаходами; час, необхідний оператору для виконання запиту на збір, аналіз інформації; час, який оператором витрачається на вибір інформаційних об'єктів впливу та коригування відповідних пар, ціль-контрзахід. Таким чином на основі проведених досліджень отримані часові характеристики роботи оператора на стадії налаштування системи та на стадії експлуатації системи протидії в соціальних мережах поширенню та виявлення шкідливої інформації. Отримані значення наведено у табл. 4.2.

Для порівняння часових характеристик пропонованого методу з процесом протидії в соцмережах поширенню та виявлення шкідливої інформації без

використання запропонованого підходу було також проведено дослідження. Експертам запропоновано оцінити час на формування відповідного запиту до системи моніторингу, час прийняття рішення про вибір інформаційного об'єкта впливу на загрозу, час прийняття адекватного рішення на вибір контрзаходів протидії.

Таблиця 4.2 − Часові характеристики роботи оператора з використанням системи протидії в соцмережах поширенню та виявлення шкідливої інформації

Крок	$t_i^{\min}, хв.$	$t_i^{\max}, хв.$	$T_i = \frac{3 \cdot T_i^{\min} + 2 \cdot T_i^{\max}}{5}$	$\sigma^2(T_i) = 0.4\left(T_i^{\max} - T_i^{\min}\right)^2$
T_1^{HC}	46.00	64.10	52.44	102.685
T_2^{HC}	11.20	13.50	15.00	8.396
T_1^{EC}	1.08	1.26	1.24	2.046
T_3^{EC}	1.50	7.01	3.16	15.547
Разом, хв			71.84	128.674

В результаті отриманні наступні експериментальні значення для $T^{additional}$ = 98 хв. Таким чином, значення функції Лапласа $\Phi(Z)$ для $T^{additional}$ = 98 хв. для системи протидії в соцмережах поширенню та виявлення шкідливої інформації, отримаємо (4.9):

$$\left(Z = \frac{T^{additional} - \sum_{i=1}^{n} T_i}{\sqrt{\sum_{i=1}^{n} \sigma_i^2(T_i)}}\right) = \left(\frac{98 - 71.84}{\sqrt{128.674}}\right) \approx 2.69 \qquad (4.9)$$

За отриманими значеннями функції Лапласа, заданих у відповідних таблицях, ймовірність виконання системи протидії в соцмережах поширенню та виявлення шкідливої інформації за заданий час складає $P_{op}\left(T_m \le T^{additional}\right) = 0.9924$, що відповідає вимогам пред'явленим до системи протидії до оперативності

$\left(P_{op}^{additional}=0.99\right)$. Водночас, скоротився загальний час роботи оператора системи протидії поширенню шкідливій інформації в соцмережі з 98 хв. до 71.84.

Оцінка ресурсоспоживання проводилася по ряду показників, характерних, в даній ситуації для другого кроку стадії експлуатації системи протидії в соцмережах поширенню та виявлення шкідливої інформації:

1. Використання часу зайнятості центрального процесорного пристрою (4.10):

$$R_{CP}=\frac{Q_{CP}^{M}}{Q_{CP}^{GEN}}, \tag{4.10}$$

де Q_{CP}^{M} - час, витрачений центральним процесором на виконання системи протидії, Q_{CP}^{GEN} - загальний доступний час центрального процесора.

2. Використання оперативної пам'яті системою протидії (4.11):

$$R_{DDR}=\frac{Q_{DDR}^{M}}{Q_{DDR}^{GEN}}, \tag{4.11}$$

де Q_{DDR}^{M} - об'єм оперативної пам'яті, який використовується у процесі виконання системи протидії, Q_{DDR}^{GEN} – загальний об'єм оперативної пам'яті.

3. Час роботи оператора (4.12):

$$R_{\exp ert}=\frac{Q_{\exp ert}^{M}}{Q_{\exp ert}^{GEN}}, \tag{4.12}$$

де $Q_{\exp ert}^{M}$ – час роботи оператора, витрачений на процес протидії поширенню шкідливої інформації в соцмережах, $Q_{\exp ert}^{GEN}$ – загальний час роботи оператора системи протидії.

Для вхідних даних $R_{DDR}=\frac{Q_{DDR}^{M}}{Q_{DDR}^{GEN}}, R_{CP}=\frac{Q_{CP}^{M}}{Q_{CP}^{GEN}}$ значення отримуються з вимірювань часу роботи алгоритму сортування інформаційних об'єктів впливу та ранжування джерел повідомлень соціальної мережі. Отриманна оцінка

ресурсоспоживання відповідає заданим у вимогах до системи протидії, якщо відповідні показники відповідають умові $r \le R^{additional}$.

Запропоновані моделі, алгоритми роботи системи, метод та архітектура системи протидії можуть бути використані для вирішення наступних задач:

1. Для підвищення інформаційної безпеки суспільства та особистості у соцмережах за рахунок використання обґрунтованого вибору інформаційних об'єктів впливу на контрзаходи. Якщо оператор системи протидії поширенню шкідливої інформації отримуватиме інформацію про інформаційні об'єкти впливу з високим пріоритетом, на формування якого впливає активність аудиторії, кількість переглядів, кількість повідомлень із шкідливою інформацією на відповідній сторінці в соцмережі, оператор зможе приймати адекватні рішення щодо протидії поширенню об'єктів своєчасно, протидія повідомленням мережі, які ніхто не читає та не бачить в соцмережах буде здійснюватиметься в останню чергу. Таким чином, дозволить підвищить якість рішень оператором, перерозподілити роботу оператора. В екстрених ситуаціях, які пов'язані з протидією тероризму, екстремізму, система налаштовується відповідним чином, щоб система протидії запускалася в автоматичному режимі. Перспективним напрямом використання результатів роботи - аналіз джерел мережі шкідливих повідомлень у соцмережах, що містять заклики до суїциду підлітків та дітей, дозволить на рівні міських та муніципальних адміністрацій виявляти найактивніші сторінки у соцмережах, зосереджуватись на захисті передплатників та учасників таких об’єднань від необдуманих вчинків, також даний підхід можна використовувати на рівні адміністрації районів, міста для пошуку активних джерел мережі поширення наркотиків через соцмережі.

2. Запропоновані моделі, алгоритми роботи системи, метод та архітектура системи протидії можуть бути використанні в комерційних організаціях, державних корпораціях для захисту бренду та репутації. Список інформаційних загроз для даної задачі може включати негативні відгуки про компанію, а подальший аналіз джерел повідомлень мережі, їх сортування дозволять

сфокусувати зусилля відповідної компанії на нівелювання нею негативного іміджу. Даний підхід може бути використаний організаціями для захисту від поширення закритої інформації із порушенням авторського права, від витоку конфіденційної інформації у соцмережах.

3. Запропоновані метод, алгоритми роботи ситеми протидії поширенню та виявлення шкідливої інформації в соцмережах можуть використуватися для вдосконалення наступних відповідних рішень: антивірусів, систем батьківського контролю. Аналіз джерел повідомленьмережі, сортування інформаційних об'єктів впливу дозволить виділяти об'єкти соцмереж впливу, зберігати відомості про них для подальшої перевірки новихт інформаційних об'єктів щодо зв'язку з ними. Таким чином, це дозволить приймати адекватні рішення про обмеження доступу користувачів до інформаційного об'єкта без проведення аналізу відповідного контенту. Запропоновані в роботі алгоритми можуть стати частиною SIEM (Security information and event management) - системи, яка проводить аналіз джерел повідомлень у соціальних мережах та формує відповідні обмежувальні списки працівників організації, на підставі отриманих даних в Інтернет – мережі.

4.4 Висновки

1. Запропоновано метод протидії та виявлення в соціальних мережах поширенню шкідливої інформації, ґрунтується на використанні алгоритмів, моделей, забезпечує, на відміну від аналогів, аналіз інформації соцільних мереж; формування списків інформаційних об'єктів впливу для проведення протидії об'єктам, сортування інформаційних об'єктів; надання оператору системи протидії альтернативних варіантів та пропонованого з обґрунтуванням вибору. Система протидії загрозам соцмереж забезпечує ранжування відповідних контрзаходів доступних у системі для протидії поширенню та виявлення шкідливої інформації у Інтернет - мережі.

2. Запропоновано архітектуру системи протидії та виявлення в соціальних мережах поширенню шкідливої інформації та прототипи компонентів системи, відрізняються від аналогів тим, що орієнтовані вибір доступних в системі контрзаходів на їх ранжування. Архітектура системи містить оригінальні компоненти проведення аналізу та оцінки джерела повідомлень мережі шкідливої інформації, базу даних з інформацією про контрзаходи протидії поширенню шкідливої інформації в соцмережах, також містить інформацію про агентів реалізації, з використанням яких будуть реалізовані контрзаходи. Запропонована архітектура системи протидії дозволяє формувати вхідні дані для проведення розробок та досліджень в області протидії поширенню шкідливої інформації в соцмережах, а також проведення розробок рішень, досліджень для систем підтримки та прийняття адекватних рішень.

3. Проведено експериментальну оцінку запропонованого підходу та прототипів. Обрані критерії для досягнення мети дослідження - обґрунтованість ресурсоспоживання, оперативність. Запропоновано варіанти використання, розроблених у процесі проведених досліджень моделей, алгоритмів, архітектури системи протидії поширенню та виявлення шкідливої інформації у соціальних мережах.

ВИСНОВКИ

У магістерській роботі з метою підвищення ефективності системи протидії у Інтернет - мережах вирішена задача розробки відповідного підходу підвищення обґрунтованості прийнятого рішення на протидію поширенню та виявлення шкідливої інформації за рахунок збільшення числа параметрів, що враховуються при виборі інформаційного об'єкта впливу та дійових контрзаходів. Вирішення поставленої задачі, досягається за рахунок проведення ранжування контрзаходів та аналізу джерел мережі шкідливої інформації. В результаті виконання магістерської роботи отримані наступні результати:

1. Проведено аналіз дослідження існуючих моделей шкідливої інформації та інформаційного обміну в соціальних мережах.

2. Проведено аналіз дослідження існуючих систем моніторингу та методів протидії поширенню та виявлення шкідливої інформації у Інтернет – мережах, алгоритмів оцінки джерел повідомлень у соціальних мережах.

3. Запропоновані моделі джерела поширення шкідливої інформації, соціальної мережі та шкідливої інформації.

4. Запропоновані алгоритми проведення аналізу джерел поширення шкідливої інформації, ранжування контрзаходів протидії.

5. Розроблено метод протидії та виявлення в соціальних мережах поширення шкідливої інформації.

6. Розроблена архітектура та програмні прототипи компонентів системи протидії та виявлення в соціальних мережах поширення шкідливої інформації. Проведено експериментальна оцінка запропонованих в магістерській роботі моделей, алгоритмів, архітектури системи.

Розроблені моделі шкідливої інформації, соціальної мережі, джерела повідомлень, відрізняється від аналогів, доданих нових атрибутів, елементів, зв'язків між ними, які більш детально характеризують інформаційні об'єкти в соціальних мережах. Запропоновані алгоритми проведення аналізу джерел

поширенню шкідливої інформації та проведення ранжування контрзаходів, відрізняється від наявних, врахуванням залежних атрибутів інформаційних об'єктів та зв'язків у соцмережі. Як результат роботи алгоритму проведення аналізу джерел поширення шкідливої інформації формується відсортований список інформаційних об'єктів впливу. Алгоритм проведення ранжування контрзаходів протидії, враховує рівні складності та коефіцієнти для проведення кожного контрзаходу. Метод протидії та виявлення в соціальних мережах поширення шкідливої інформації, орієнтований на автоматизований та автоматичний вибір інформаційних об'єктів впливу та контрзаходів протидії поширенню в мережах шкідливої інформації зі списку контрзаходів та підтримку прийняття рішення про обрану протидію загрозам. Запропоновано архітектуру системи протидії та програмні компоненти системи протидії поширенню шкідливої інформації, яка містить оригінальні компоненти проведення оцінки та аналізу джерела поширення шкідливої інформації, ранжує контрзаходи протидії, базу даних – містить інформацію про контрзаходи протидії, інформацію про агентів реалізації, з використанням яких будуть реалізовані контрзаходи.

Сформульовано відповідні рекомендації щодо використання результатів роботи для захисту інтересів організації, забезпечення інформаційної безпеки суспільства та особистості у соцмережах. Запропоновані підходи в магістерській роботі можуть бути використанні в міських та державних ситуаційних центрах для протидії тероризму та екстремізму, запобіганню розповсюдженню в мережах фейкових новин, інформації суїцид чи закликів до нього. Результати роботи можуть бути використані для систем керування репутацією бренду, вдосконалення систем батьківського контролю.

За темою роботи опубліковано 1 теза та 1 наукова стаття.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Гошубєв, О.В. Програмно-технічні засоби захисту даних від комп'ютерних злочинів / О. В. Гошубєв– Запоріжжя : «Павел», 2018. – 145

2. Гошубєв, О.В. Розслідування комп'ютерних злочинів / О.В. Гошубєв – «Запоріз. ін-т муніцип. упр. і держ.», 2016. – 297 с.

3. Горбулін, П.В. Проблеми захисту інформаційного простору України / М.М. Баченок, П.В. Горбулін – К.: Інтертехнологія, 2019. – 138 с.

4. Джулій, В.М. Інформаційно-ознакова модель шкідливої інформації в соціальних мережах/ І.В. Муляр, В.М. Джулій, В. М. Пічура, О.О Зацепіна – Вимірювальна та обчислювальна техніка в технологічних процесах № 3 (2022)-73–78с.

5. Джулій, В.М., Муляр І.В., Кльоц Ю.П., Джулій А.В., Жилевич М.Л. Контроль додатків трафіка комп'ютерних мереж методами машинного навчання. Вісник ХНУ. Технічні науки. 2021. № 5. С. 22-26.

6. Джулій, В.М. Метод класифікації додатків інтернет - трафіка комп'ютерних мереж в умовах невизначеності / В.М. Джулій, Л.В. Солодєєва, О.В. Мірошніченко, // Збірник наукових праць ВІКНУ ім. Т. Шевченка. – К.: ВІКНУ, 2022. –№74. – С. 73-82.

7. Джулій, В.М. Модель оцінки ймовірнісно-часових характеристик інтернет речей інформаційної взаємодії в мережі / В.М. Джулій, Б.М. Кізюн, О.В. Сєлюков, І.В. Муляр // Збірник наукових праць ВІКНУ ім. Т. Шевченка. – К.: ВІКНУ, 2019. –№ 63. – С.96-106

8. Довгий, С.О. Сучасні телекомунікації: управління, технології, мережі, регулювання, економіка / С.О. Довгий, П.П. Воробієнко, О.Я. Савченко – К.: УВЦ, 2014. – 521 с.

9. Дроб'язко, В. С. Охорона баз даних : регіональні, національні аспекти, міжнародні / В. С. Дроб'язко – К. : Л.-Поліграф, 2018. – 132 с.

10. Ермаков, А.М. Основы конфигурации корпоративных сетей Cisco. А.М. Ермаков – М.: ФГБОУ, 2015. — 458 с.

11. Зацепіна, О.О. Проблеми і задачі протидії та виявлення в соціальних мережах шкідливої інформації / В.М. Джулій, О.О. Зацепіна / Тези доповідей XVIII міжнародної наукової конференції молодих учених, аспірантів та студентів. / ред. кол. Д. Струнін – К., - 2022. –С.109

12. Кудінов, В.А. Основи протидії кіберзлочинності. / В. М. Смаглюк, В. Г. Хахановський, В.А. Кудінов. – К. : НАВС, 2016. – 104 с.

13. Кузьменко, Г.Н. Компьютерные сети и сетевые технологии/ Г. Н. Кузьменко– Л: Наука и техника, 2016. – 369 с.

14. Кутузов, О. И. Моделирование и оценка вероятностно-временных характеристик. Инфокоммуникационные сети. / Т. М. Татарникова, О. И. Кутузов - СПб. : РГГМУ, 2017. – 384 с

15. Кутузов, О. И. Моделирование сетей телекоммуникаций и систем / Т. М. Татарникова, О. И. Кутузов. СПб.: ГУАП, 2014–578с.

16. Лавров, Є. А. Математичні методи дослідження операцій. / В. В. Шендрик, Л. П. Перхун, Є. А. Лавров– Суми : СДУ, 2017. – 214 с.

17. Лєнков, С.В. Аналіз існуючих алгоритмів та методів виявлення атак передачі даних в бездротових мережах / С.В. Лєнков, С.О. Божук, Н.М. Берназ, В.М. Джулій // Збірник наукових праць ВІКНУ ім. Т. Шевченка. – К.: ВІКНУ, 2017. – № 56. – С.124-132

18. Ленков, С.В. Методы и средства защиты в сети информации. В 2-х томах / Д.А. Перегудов, В.А. Хорошко, С.В. Ленков–К: Арий, 2018.–467с.

19. Ленков, С.В. Модель безпеки поширення в інформаційно-телекомунікаційних мережах забороненої інформації / В.С. Орленко, С.В. Ленков, А.В. Атаманюк, О.В. Сєлюков, В.М.Джулій, // Збірник наукових праць ВІКНУ ім. Т. Шевченка. – К.: ВІКНУ, 2020. –№68. – С. 53-64.

20. Лук’янов, Б. В. Комп’ютерни аналіз даних / Б. В. Лук’янов – К. : Академія, 2017. – 345 с.

21. Олифер, Н.А. Компьютерные сети. Принципы, технологии, протоколы / Н. А. Олифер, В. Г. Олифер, - СПб.: РГГМУ, 2017. - 996 с.

22. Остапов, С. Е. Технології захисту інформації: навч. посіб. / С.П. Євсеєв, О.Г. Король, С.Е. Остапов – Харків : ХНЕУ, 2016. – 471 с.

23. Соболь, Б.В. Сети и телекоммуникации. / Г.А. Мани,н Е.Д. Герасименко, Б. В. Соболь – М.: Феникс, 2016. – 192 с.

24. Соціальні мережі – реальні загрози віртуального світу. [Електронний ресурс]. – Режим доступу : http://ogo.ua/ articles/view/011–02–23/26490.htm.

25. Суворов, Б. А. Основы технологий массовых телекоммуникаций. / Б.А. Суворов— СПб.: РГГМУ, 2015. — 507 с.

26. Трубачев, П. А. Оценка безопасности сетевых информационных технологий / П.А. Трубачев, ред. В. А. Галатенко – СПб.: РГГМУ, 2015. – 358 с.

27. Тарасюк, В. М. Защищенные информационные технологии / В. М. Тарасюк. – СПб.: РГГМУ, 2014. – 193 с.

28. Татт, Р.У. Теория графов / Р.У. Татт, пер. Г. П. Гаврилова – М.: Феникс, 2012. – 425 с.

29. Nadvarro, S.R. Cyberbullying Across the Globe: Mental Health, Gender, and Family / B.E. Larrañaga, S.R. Navarro, I.S. Yubero - Springer International Publishing Switzerland, 2016. 284 c.

ДОДАТОК А
(обовязковий)
Код (лістинг) програмних компонентів системи протидії та виявлення в соціальних мережах поширення шкідливої інформації

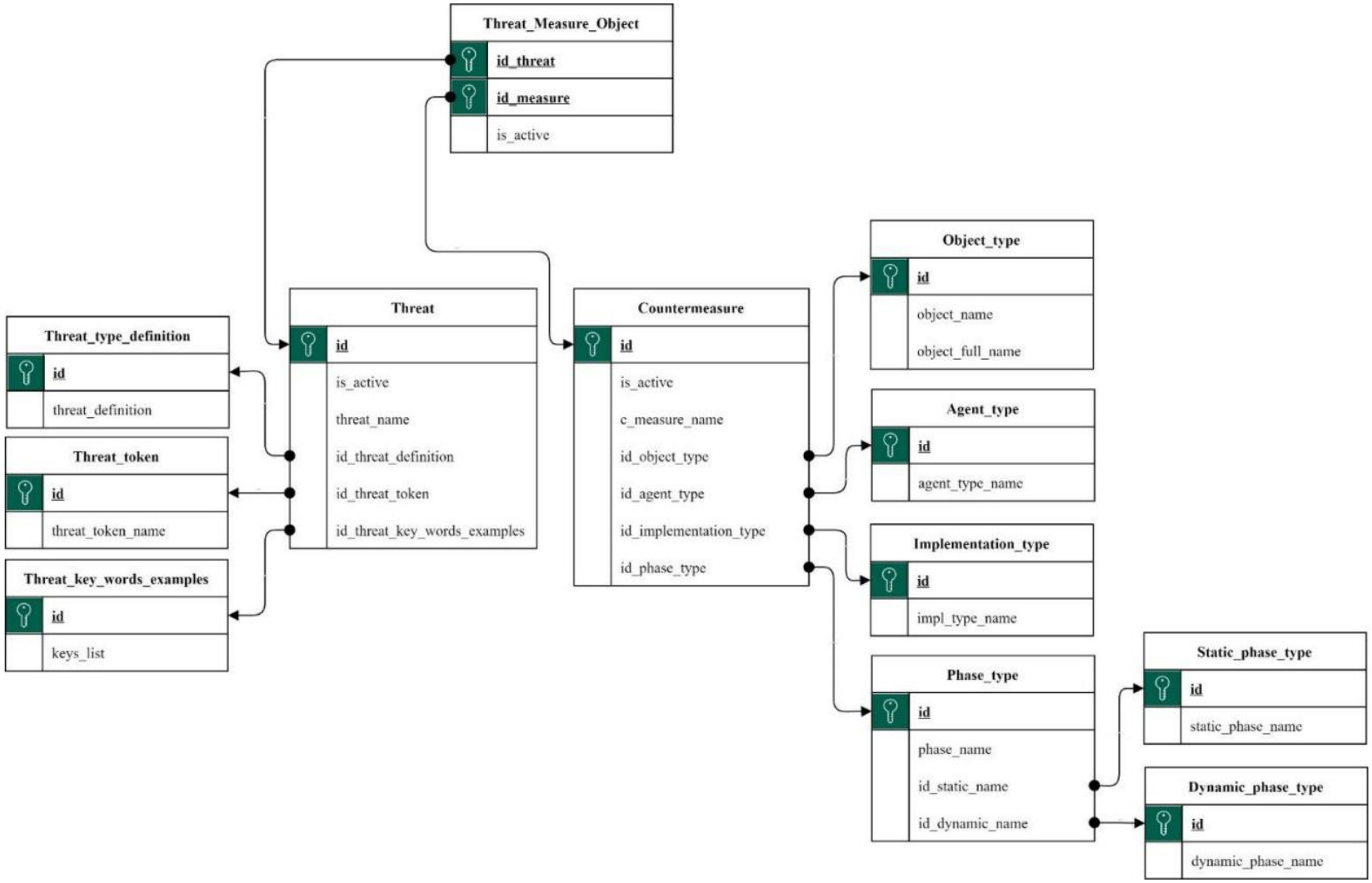
```
#Алгоритму оцінки джерел активності
#Крок 1 Обчислення суми повідомлень джерела
for (int) i in range (length(list(Sources_Potential_Calculation[URLmessage]))):
 Sources_Potential_Calculation.local[int i,potentialIndex]==0
 if Sources_Potential_Calculation[Type_message][i]= post: else
Sources_Potential_Calculation.local[i,potential_Index]=Sources_Potential_Calculation
[potentialIndex][i]+1
 if SourcesPotentialCalculation[Type_message][i] = comment: else
SourcesPotentialCalculation.loc[i,potentialIndex]=SourcesPotentialCalculation[potenti
alIndex][i]+0.5
 if SourcesPotentialCalculation [messageType][i]= reply to comment: else
SourcesCalculationPotential.loc[(int)i,potentialIndex]=SourcesCalculationPotential [
Indexpotential][i]+0.25
## Крок 2 Розрахунок джерела повідомлень потенціалу
## Розрахунок середнього
count = 0
firstAverage = 0
for int i in range (length(list(SourcesCalculationPotential [URLmessage]))):
 firstAverage = firstAverage + SourcesPotentialCalculation['potentialIndex'][i] else
 count = count + 1
firstAverage = firstAverage / count
# Розрахунок другого середнього
secondAverage = 0
count = 0
for i in range (len(list(SourcesPotentialCalculation['messageURL']))):
 if SourcesPotentialCalculation['potentialIndex'][i]>= firstAverage:
 secondAverage = secondAverage + SourcesPotentialCalculation['potentialIndex'][i]
 count = count + 1
secondAverage = secondAverage / count
# Формування результату
```

```
for i in range (len(list(SourcesPotentialCalculation['messageURL']))):
 if SourcesPotentialCalculation['potentialIndex'][i]<firstAverage:
 SourcesPotentialCalculation.loc[i,'potentialIndex']=0
 elif SourcesPotentialCalculation['potentialIndex'][i]>=firstAverage and
SourcesPotentialCalculation['potentialIndex'][i]<secondAverage:
 SourcesPotentialCalculation.loc[i,'potentialIndex']=1
 elif SourcesPotentialCalculation['potentialIndex'][i]>=secondAverage:
 SourcesPotentialCalculation.loc[i,'potentialIndex']=2
#Алгоритм оцінки джерел активності
Крок 1. Обчислення індексу активності
 if SourcesActivityCalculation['sourseId'][j]==subscriberCount['sourseId'][i]:
SourcesActivityCalculation.loc[j,'subscriberCount']=subscriberCount['subscriberCount']
[i]
urlCounter=0
for i in range (len(list(SourcesActivityCalculation['messageURL']))):
 for j in range (len(list(SourcesActivityCalculation['messageURL']))):
 if i!=j:
 if SourcesActivityCalculation['sourseId'][i]== SourcesActivityCalculation['sourseId'][j]:
 urlCounter=urlCounter+1
urlCounter=list(SourcesActivityCalculation['sourseId'])
urlCounter = len (set (urlCounter))
activityIndex = pd.DataFrame({
 'sourseId':[],
 'activityIndex': [], })
for i in range(len(list(SourcesActivityCalculation['sourseId']))):
 activityIndex.loc[i,'sourseId']= SourcesActivityCalculation['sourseId'][i]
activityIndex.loc[i,'activityIndex']=SourcesActivityCalculation['likesCount'][i]+Sources
ActivityCalcul
ation['commentCount'][i]+SourcesActivityCalculation['repostCount'][i]
for i in range(len(list(activityIndex['sourseId']))):
 if SourcesActivityCalculation['subscriberCount'][i]!=0:
activityIndex.loc[i,'activityIndex']=activityIndex['activityIndex'][i]/SourcesActivityCalc
ulation['subscr
iberCount'][i          ]
```

```
 else:
 activityIndex.loc[i,'activityIndex']=activityIndex['activityIndex'][i]/1
 activityIndex.loc[i,'activityIndex']=activityIndex['activityIndex'][i]/urlCounter
#Крок 2 Обчислення індексу перегляду джерела
viewIndex = pd.DataFrame({
 'sourseId':[],
 'viewIndex': [], })
for i in range(len(list(SourcesActivityCalculation['sourseId']))):
 viewIndex.loc[i,'sourseId']= SourcesActivityCalculation['sourseId'][i]
 viewIndex.loc[i,'viewIndex']= SourcesActivityCalculation['viewCount'][i]
for i in range(len(list(viewIndex['sourseId']))):
 if SourcesActivityCalculation['subscriberCount'][i]!=0:
viewIndex.loc[i,'viewIndex']=viewIndex['viewIndex'][i]/SourcesActivityCalculation['su
bscriberCount'
][i]
 else:
 viewIndex.loc[i,'viewIndex']=viewIndex['viewIndex'][i]/1
 viewIndex.loc[i,'viewIndex']=viewIndex['viewIndex'][i]/urlCounter
 # Крок 3 Обчислення індексу впливу джерела
 impactIndex = pd.DataFrame({
 'sourseId':[],
 'impactIndex': [], })
for i in range(len(list(SourcesActivityCalculation['sourseId']))):
 impactIndex.loc[i,'sourseId']= SourcesActivityCalculation['messageURL'][i]
 impactIndex.loc[i,'impactIndex']=
activityIndex['activityIndex'][i]+viewIndex['viewIndex'][i]
#Формування результату
InfluenceObjectSorting = pd.DataFrame({...})
```

ДОДАТОК Б

Діаграма бази даних контрзаходів та інформаційних загроз



ДОДАТОК В
(обовязковий)
Перелік наукових праць

Міжнародний науково-технічний журнал
«Вимірювальна та обчислювальна техніка в технологічних процесах»
ISSN 2219-9365

https://doi.org/10.31891/2219-9365-2022-71-3-8
УДК 004.056:621.397.3:004.942

ВОЛОДИМИР ДЖУЛІЙ
Хмельницький національний університет
https://orcid.org/0000-0003-1878-4301
e-mail: dg2303@ukr.net
ІГОР МУЛЯР
Хмельницький національний університет
https://orcid.org/0000-0002-6659-605X
muliariv@khmnu.edu.ua
ОРИСЛАВА ЗАЦЕПІНА
Хмельницький національний університет
e-mail: orysiia@gmail.com
ВАДИМ ПІЧУРА
Хмельницький національний університет
e-mail: vadimpichura007@gmail.com

ІНФОРМАЦІЙНО-ОЗНАКОВА МОДЕЛЬ ДЖЕРЕЛА ШКІДЛИВОЇ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

Розглянута актуальна задача побудови інформаційно-ознакової моделі джерела шкідливої інформації в соціальних мережах. Інформаційно-ознакова модель шкідливої інформації в соціальних мережах, дозволяє сформувати дані для виявлення та протидії поширенню шкідливої інформації в мережі. Комплекс моделей складається з моделі шкідливої інформації, інформаційно-ознакової моделі шкідливої інформації, моделі джерела інформації, моделі соціальної мережі. Кожна з моделей містить унікальні атрибути та відношення між інформаційними об'єктами, також комплекс моделей дозволяє сформувати відповідні вимоги до алгоритмів оцінки та аналізу джерел повідомлень та забезпечує вибір контрзаходів.

Ключові слова: моделі, алгоритми, модель шкідливої інформації, соціальні мережі, контрзаходи, джерела повідомлень.

VOLODYMYR DZHULIY, IGOR MULYAR,
ORYSLAVA ZACEPINA, VADYM PICHURA
Khmelnytskyi National University

AN INFORMATION-SIGN MODEL OF THE SOURCE OF HARMFUL INFORMATION IN SOCIAL NETWORKS

The problem of detecting and countering the spread of harmful information has an insufficient number of scientific and technical solutions. The available means of combating and detecting harmful information in social networks do not meet the requirements for adequacy, speed, accuracy and completeness of the decisions made. This is due to the following reasons: the systems are divided into two unrelated modules - monitoring, countermeasures, between which the operator is located. It is necessary to process extremely large flows of messages in real time, implement countermeasures in a short period of time, in manual mode the operator is unable to stop the spread of malicious information in the social network.

The task of the research is to develop: models of harmful information, source and social network; algorithms for analyzing the sources of messages spreading harmful information in social networks and ranking countermeasures.

Solving the set tasks will allow: to improve the quality of decisions made in the process of detecting and countering harmful information; sort information objects of influence for the operator by priority; set the input data for the configuration of the system for detecting and countering the spread of malicious information in networks.

The information-sign model of malicious information in social networks allows you to generate data for detecting and countering the spread of malicious information in the network. The complex of models consists of a model of malicious information, an information-sign model of malicious information, a model of the source of information, a model of a social network. Each of the models contains unique attributes and relationships between information objects, as well as a set of models allows for the formation of appropriate requirements for algorithms for the evaluation and analysis of message sources and provides a choice of countermeasures.

Keywords: models, algorithms, malicious information model, social networks, countermeasures, message sources.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

На сучасному етапі, глибина проникнення у повсякденне життя соціальних мереж є значною. Перевагою соціальних мереж є можливість учасникам комунікації висловлювати оперативно свою думку значній кількості групі людей, публікувати відео-, медіа файли. Соціальні мережі є не лише засобом спілкування групи людей, а й також інструментом поширення інформації, в тому числі шкідливої інформації. Необхідно зазначити, що злочинні та терористичні угруповання беруть на озброєння, дедалі частіше, засоби інформаційного впливу, розробляють та пишуть стратегії, спрямовані на залучення нових

Міжнародний науково-технічний журнал
«Вимірювальна та обчислювальна техніка в технологічних процесах»
ISSN 2219-9365

адептів та розширення сфери впливу через соціальні мережі. Таким чином, однією зі складових надійного забезпечення інформаційної безпеки держави є виявлення, моніторинг, аналіз та активна протидія розповсюдженню шкідливої інформації в соціальних мережах [1-3].

Проблема виявлення та протидії поширенню шкідливої інформації має не достатню кількість науково-технічних рішень. Доступні засоби протидії та виявлення шкідливої інформації в соціальних мережах не відповідають вимогам до адекватності, швидкості, точності та повноти прийнятих рішень. Це обумовлено наступними причинами: системи розділені на два незв'язаних модулі – моніторинг, протидія, між якими знаходиться оператор. Соціальні мережі мають складну структуру, до складу яких входять різнорідні повідомлення, що недостатньо враховується під час реалізації мети протидії – джерело, тип повідомлення, та інші характеристики. Необхідно обробляти у реальному масштабі часу надвеликі потоки повідомлень, в стислий термін реалізувати контрзаходи, в ручному режимі оператор не в змозі зупинити поширення шкідливої інформації в соцмережі [2-6].

Постановка задачі

Протидія поширенню шкідливої інформації у соцмережах є важливим елементом інформаційної безпеки особистості, суспільства, держави, проте більшість систем, на теперішній час не враховують простір функціональності системи виявлення та протидії шкідливій інформації, необхідна автоматизація процесу протидії. Соціальні мережі мають складну структуру, параметри повідомлень та джерел не в повній мірі враховуються під час виборів мети виявлення та протидії шкідливій інформації. При розробці методу протидії поширенню шкідливої інформації необхідно: в повній мірі враховувати кількість повідомлень на сторінці, характеристики джерела, зворотній зв'язок від джерела та аудиторії; підтримувати дві стадії: експлуатація, налаштування; ранжувати контрзаходи з урахуванням коефіцієнтів складності [4,7,8].

Задача дослідження полягає у розробці: моделей шкідливої інформації, джерела та соціальної мережі; алгоритмів проведення аналізу джерел повідомлень поширення шкідливої інформації у соціальних мережах та проведення ранжування контрзаходів; методу виявлення та протидії поширенню шкідливої інформації у соціальних мережах з урахуванням вимог до обґрунтованості; архітектури компонентів системи протидії поширеню шкідливої інформації в соцмережах [8,9].

Вирішення поставлених задач дозволить: підвищити якість прийнятих рішень у процесі виявлення та протидії шкідливій інформації; сортувати інформаційні об'єкти впливу для оператора по пріоритету; задати вхідні дані налаштування системи виявлення та протидії поширенню шкідливої інформації в мережах.

Основна частина

Моделі даних соціальних мереж характеризуються, незалежно від їх структури, загальними атрибутами - джерела, повідомлення, ознаки зворотного зв'язку на повідомлення суб'єкта. Наявність ознак зворотного зв'язку в моделі соцмережі дозволяє характеризувати джерело повідомлення. Нехай $ACTIVITY$ $\{countLike, countREpost, countComment, countView\}$ множина у повідомленнях від реципієнтів всіх ознак зворотного зв'язку інформації у соцмережі, де $countLike$ – кількість позначок, $countREpost$ – кількість копій з посиланням на джерело («репостів»), $countComment$ - кількість коментарів, $countView$ – кількість переглядів.

Виходячи з поставлених задач, необхідно визначити атрибути множини $ACTIVITY$, а також відношення $R(SOURCE, MESSAGE)$, які в подальшому дозволять проводити аналіз повідомлення та джерела, що містять шкідливу інформацію та вибирати відповідний об'єкт для протидії. Наприклад, якщо сума елементів активності до повідомлення дає можливість обчислити індекс активності повідомлення, таким чином може бути отриманий, в даній ситуації, інтегральний показник індексу активності, який в свою чергу залежить від кількості повідомлень джерела, очевидно одним із атрибутів моделі даних джерела буде *index_active*. Якщо кількість переглядів повідомлення дозволяє обчислити індекс перегляду, таким чином можемо отримати інтегральний показник індексу перегляду для джерела інформації, отримаємо наступний атрибут моделі даних джерела - *index_viewability*. Функція $f: MESSAGE \to SOURCE$ задає область визначення, вхідні та вихідні значення (аргументи). Функція сюр'єктивна - є відображенням множини $MESSAGE$ на множину $SOURCE$, при відображенні кожен елемент множини $SOURCE$ є образом множини $MESSAGE$ (хоча б одного елемента). Таким чином, отримаємо:

$$\forall source \in SOURCE \exists message \in MESSAGE : source = f(message) \quad (1)$$

Повідомлення (аргументи) на стіні джерела можуть бути різного типу (відповідь, пост, коментар). Таким чином, для окремих аргументів (повідомлень) може бути заданий числовий коефіцієнт (рейтинг) у дереві повідомлень соціальної мережі (рис. 1).

Міжнародний науково-технічний журнал
«Вимірювальна та обчислювальна техніка в технологічних процесах»
ISSN 2219-9365

Рис. 1. Дерево повідомлень соцмережі

В залежності від кількості аргументів, джерело повідомлення можливо оцінити за потенціалом (potential): джерело із низьким потенціалом; джерело із середнім потенціалом; джерело із високим потенціалом. Якщо джерело повідомлень має атрибути: index_active, index_viewability, то можна задати індекс впливу - index_impact, який відображає рівень впливу джерела повідомлення на аудиторію.

Виділимо атрибути в кортежі, що характеризують *SOURCE* через елементи множини *ACTIVITY* і відношення $R(SOURCE, MESSAGE)$ - $\langle index_{active}, index_{viewability}, potential, index_{impact} \rangle$. Також, атрибутами моделі джерел повідомлень є: *social_network_type* – тип даних структури соцмереж; *followers* – кількість пов'язаних користувачів; *registration_time* - час реєстрації в мережі джерела інформації. Модель даних джерела повідомлень відрізняється наявністю нових атрибутів, класів, відношень.

Розглянемо модель шкідливої інформації в мережі Інтернет. Основою для формування поняття - шкідлива інформація виступають два терміни [10]: *I* – information (Інформація); *IO* – information object (Інформаційний об'єкт) –логічно цільний блок відповідної інформації, представлений у фіксованої формі, використовується та створений в ході інформаційної діяльності. Формально терміни пов'язані між собою, так, що $IO \subseteq I$ (рис. 2. а) - інформаційний об'єкт є елементом множини всієї інформації, над якою проводиться аналіз. Із терміном «інформація» також пов'язаний термін - *IA* – information area («інформаційний простір»), а множини I, IO є підмножинами інформаційного простору. Соціальні мережі представляють собою сукупність взаємозалежних вузлів: спільноти, акаунти, сторінки, вкладення, пости; зв'язки між об'єктами – однорівневі відношення (перебувають у співтоваристві, у друзях); відношення вкладеності (сторінка запису містить посилання на пост, стіна містить пост) [6-8]. Соціальні мережі можуть бути представленні графами: частина об'єктів - інформаційні, вершина графа, а зв'язки між об'єктами - ребра між вершинами. Таким чином, справедливо, що $IO \subseteq I \subseteq IA$, $SN \subseteq I \subseteq IA$, область перетину між *SN* (соцмережа) та *IO* є предметом дослідження у соціальних мережах розробки моделі шкідливої інформації (рис. 2. б).

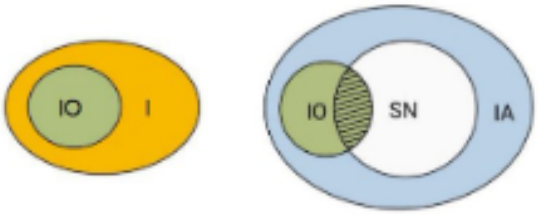


Рис. 2. Графічне представлення відношень множини інформаційного простору

Інформаційний об'єкт - *MIO* (шкідливий інформаційний об'єкт), містить відповідні ознаки, які дозволяють прийняти рішення, що інформація завдає шкоди державі, суспільству, бізнесу особистості. В залежності від умови експерт встановлює ознаки *Token* інформаційної загрози *T*. Наприклад, батько сам вибирає обмеження для дитини, у випадку використання система батьківського контролю. Якщо представник бізнес - компанії зацікавлений у захисті конфіденційного інформації бізнеса, в даній ситуації він їх сам задає. Таким чином, у соціальній мережі, теоретико-множинна модель шкідливої інформації, включає наступні базові елементи: *IO* - інформаційний об'єкт (Information Object); *T* - інформаційна загроза (Threat); *MIO* – шкідливий інформаційний об'єкт; *Token* – ознака інформаційної загрози, що знаходиться у шкідливому інформаційному об'єкті; *Feature* – ознака наявності інформаційного об'єкта [0,1]; зв'язок між інформаційними об'єктами.

Теоретико-множинна модель шкідливої інформації (2) формально представлена наступним чином:

Міжнародний науково-технічний журнал
«Вимірювальна та обчислювальна техніка в технологічних процесах»
ISSN 2219-9365

$$\begin{aligned} &IO = \{io\}; MIO = \{io\}; MIO_i = \{io\} \\ &MIO \subset IO; \forall io \in MIO : io \in IO \\ &MIO_i \subseteq MIO; \forall io \in MIO_i : io \in MIO \\ &Token_{mio_i} \subset T; Token_{mio_i} = \{t\} \\ &CheckFeature(io,t) = \{True; False\} \\ &io \in MIO_i \Leftrightarrow \exists Token_{mio_i} : checkFeature(io,t) = True \end{aligned} \quad (2)$$

де IO – множина інформаційних об'єктів, io – інформаційний об'єкт, T - множина ознак інформаційної загрози, t_i –*i* -а ознака інформаційної загрози, MIO – множина шкідливих інформаційних об'єктів мережі, MIO_i - *i*-й клас шкідливої інформації, $Token_{mio_i}$ - множина ознак загрози, що характеризують MIO.

Таким чином, для виявлення та протидії поширенню шкідливій інформації в мережі необхідно задати набір ознак, характерних для інформаційної загрози в соціальній мережі.

Особливістю моделі шкідливої інформації соціальної мережі є те, що модель допускає наявність дискретних ознак у множині ознак: зв'язок інформаційного об'єкта з іншими інформаційними об'єктами у соцмережі; частота повторення ознаки; дата створення інформаційного об'єкта.

Протидія поширенню шкідливого інформаційного об'єкта в соціальній мережі може здійснюватися лише на рівні джерел чи повідомлень. Таким чином, необхідно виділити такі інформаційні загрози та відповідні інформаційні ознаки повідомлення у соцмережі, що характеризують його як шкідливий об'єкт. Інформаційно-ознакова модель (табл.1) - впорядкована сукупність інформації про зв'язки повідомлень та їх ознак зі змістом повідомлень. Інформаційні ознаки повідомлень - окремі властивості повідомлень, їх зміст. Інформаційна загроза – задається оператором системи. Шкідлива інформація в соціальній мережі – задається оператором шляхом формування набору відповідних ключових слів. Інформаційні ознаки - формують множину усіх можливих інформаційних ознак *t*. На рис.3 наведено співвідношення, взаємозв'язок різних рівнів інформаційно-ознакової моделі шкідливої інформації Показано, що формується повідомлення, розміщується повідомлення в джерелі розповсюдження, на сторінці групи, облікового запису. Повідомлення можуть містити ознаки шкідливої, а також не містити ознаки шкідливої інформації. Інформаційні ознаки (табл. 1) формують рівень інформаційних загроз в соціальній мережі.

Таблиця 1

Інформаційно-ознакова модель шкідливої інформаціїсоціальної мережі

Інформаційні загрози	Шкідлива інформація у соцмережах	Інформаційні ознаки
Приклад Самогубство	Приклад Повідомлення, що містить прохання, пропозицію, наказ зробити самогубство, описує самогубство як спосіб вирішення проблем	t_1
	Приклад Повідомлення, що містить позитивну оцінку схвалення вчинення самогубства, дій, спрямованих на самогубство	t_2

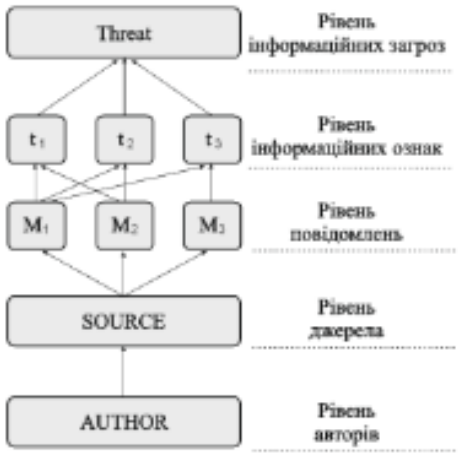


Рис. 3. Інформаційно-ознакова модель шкідливої інформації

Таким чином, зібравши відповідну інформацію на сторінці джерела можливо визначити, які з цих повідомлень інформаційної мережі належать до шкідливих повідомлень. Результатом виявлених загроз та їх кількості буде прийняте відповідне рішення про протидію джерелу, повідомленню.

Запропонована інформаційно-ознакова модель шкідливої інформації в соціальних мережах, дозволяє сформувати дані для виявлення та протидії поширенню шкідливої інформації в мережі. Комплекс моделей складається з моделі шкідливої інформації, інформаційно-ознакової моделі шкідливої інформації, моделі джерела інформації, моделі соціальної мережі. Кожна з моделей містить унікальні атрибути та відношення між інформаційними об'єктами, також комплекс моделей дозволяє сформувати відповідні вимоги до алгоритмів оцінки та аналізу джерел повідомлень та забезпечує вибір контрзаходів.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Запропонована модель соціальної мережі, що включає джерела, повідомлення, зв'язки (відношення) між інформаційними об'єктами, відрізняється наявністю нових рв'язків та структурних елементів. Розроблено модель джерела, в якій враховуються наступні параметри: індекс впливу, індекс активності, індекс перегляду, потенціал. Запропонована теоретико-множинна модель шкідливої інформації в соціальній мережі, складається з ознак шкідливої інформації та взаємопов'язаних об'єктів, що в сукупності формують шкідливо-інформаційні об'єкти в мережі Інтернет. Також розроблена інформаційно-ознакова модель шкідливої інформації в соціальних мережах, дозволяє сформувати дані для виявлення та протидії поширенню шкідливої інформації в соціальних мережах.

Література

1. Ленков, С.В. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах / С.В. Ленков, В.М. Джулій, В.С. Орленко, О.В. Селюков, А.В. Атаманюк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2020. – Вип. №68. – С. 53-64.

2. Соціальні мережі – реальні загрози віртуального світу. [Електронний ресурс]. – Режим доступу : http://ogo.ua/ articles/view/011–02–23/26490.htm.

3. Ленков, С.В. Методы и средства защиты информации. В 2-х томах /С.В. Ленков, Д.А. Перегудов, В.А. Хорошко –К: Арий, 2008.–464с

4. Остапов С. Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король–Харків : Вид-во ХНЕУ, 2016. – 476 с.

5. Лєнков, С.В. Аналіз існуючих методів та алгоритмів виявлення атак в бездротових мережах передачі даних / С.В. Ленков, В.М. Джулій, Н.М. Берназ, С.О. Божук // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 56. – С.124-132

6. Довгий, С.О. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / С.О. Довгий, О.Я. Савченко, П.П. Воробієнко – К.: Український Видатничій Центр, 2012. – 520 с.

7. Джулій, В.М. Модель оцінки ймовірнісно-часових характеристик інформаційної взаємодії в мережі інтернет речей / В.М. Джулій, І.В. Муляр, О.В. Селюков, Б.М. Кізюн // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2019. – Вип. № 63. – С.96-106

8. Джулій, В.М., Кльоц Ю.П., Муляр І.В., Жилевич М.Л., Джулій А.В. Контроль додатків інтернет-трафіка комп'ютерних мереж методами машинного навчання. Вісник Хмельницького національного університету. Технічні науки. 2021. № 5. С. 22-26.

9. Джулій, В.М. Метод класифікації додатків трафіка комп'ютерних мереж на основі машинного навчання в умовах невизначеності / В.М. Джулій, О.В. Мірошніченко, Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2022. – Вип. №74. – С. 73-82.

10. Лавров, Є. А. Математичні методи дослідження операцій : підручник / Є. А. Лавров, Л. П. Перхун, В. В. Шендрик – Суми : Сумський державний університет, 2017. – 212 с.

References

1. Lenkov, S.V. (2020), Model bezpeky poshyrennia zaboronenoi informatsii v informatsiino-telekomunikatsiinykh merezhakh / S.V. Lenkov, V.M. Dzhulii, V.S. ORLENKO, O.V. Sielniukov, A.V. Atamaniuk // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – №68. – pp. 53-64.

2. Cotsialni merezhi – realni zahrozy virtualnoho svitu. [Elektronnyi resurs]. – Rezhym dostupu : http://ogo.ua/ articles/view/011–02–23/26490.htm.

3. Lenkov, S.V. (2008), Metodyy sredstva zashchyty ynformatsyy. V 2-kh tomakh / S.V. Lenkov, D.A. Peregudov, V.A. Khoroshko – K: Aryi–464s.

4. Ostapov, S. E. (2016) Tekhnolohii zakhystu informatsii: navchalnyi posibnyk / S.E. Ostapov, S.P. Yevseiev, O.H. Korol–Kharkiv : Vyd-vo KhNEU. – 476 s.

ISSN 2219-9365

5. Lenkov, S.V. (2017), Analiz klasyuchih metodiv ta algoritmiv viyavlennya atak v bezdrotovih merezhah peredachI danih / S.V. Lenkov, V.M. Dzhuliy, N.M. Banasa, S.O. Bozinuk // Zbirnik naukovih prats Viyskovogo Institutu Kiyivskogo natsionalnogo universitetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vip. No 56. – p.124-132

6. Dovbyi, S.O. (2012). Suchasni telekommunikatsii: merezhi, tekhnolohii, ekonomika, upravlinnia, rehuliuvannia /S.O. Dovbyi, O.I. Savchenko, P.P. Vorobiienko – K.: Ukrainskyi Vydavnychii Tsentr. – 520p.

7. Dzhulii, V.M. (2019), Model otsinky ymovirnisno-chasovykh kharakterystyk informatsiinoi vzaiemodii v merezhi internet rechei / V.M. Dzhulii, I.V. Muliar, O.V. Sielinkov, B.M. Kizitun // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vyp. № 63. – p.96-106

8. Dzhulii V.M., Klots Yu.P., Muliar I.V., Zhylevych M.L., Dzhulii A.V. (2021), Kontrol dodatkiv internet-trafika kompiuternykh merezh metodamy mashynnoho navchannia. Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. – Khmelnytskyi. – №3. – pp. 22–26.

9. Dzhulii, V.M. (2022), Metod klasyfikatsii dodatkiv trafika kompiuternykh merezh na osnovi mashynnoho navchannia v umovakh nevyznachenosti / V.M. Dzhulii, O.V. Miroshnichenko, L.V. Solodiseva // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vyp. №74. – pp. 73-82.

10. Lavrov, Ye. A. (2017.), Matematychni metody doslidzhennia operatsii : pidruchnyk / Ye. A. Lavrov, L. P. Perkhun, V. V. Shendryk – Sumy : Sumskyi derzhavnyi universytet, – 212 p.

ПРОБЛЕМИ І ЗАДАЧІ ПРОТИДІЇ ТА ВИЯВЛЕННЯ В СОЦІАЛЬНИХ МЕРЕЖАХ ШКІДЛИВОЇ ІНФОРМАЦІЇ

к.т.н. Джулій В.М. *(ХмНУ),*
Зацепіна О.О. *(ХмНУ)*

На сучасному етапі залишається відкритим питання, як в інформаційному полі розпізнати шкідливу інформацію, як державі протидіяти окремим соціальним викликам (дитячий та підлітковий суїцид), як захистити суспільство від панічних настроїв у період змін і глобальних катастроф, можливим кольоровим революціям? Удосконалення систем протидії поширенню шкідливої інформації в мережах з боку держави, організацій, особистості можуть дати дійові результати. Конфлікти та процеси в інформаційному полі держави - відображення активності суб'єктів діяльності: інституційні, групові актори чи індивідуальні. Таким чином спостерігаємо зворотну тенденцію, коли процеси та конфлікти в інформаційному полі держави можуть породжувати конфлікти та події, що безпосередньо впливають на соціальну активність людей, їх життєвий шлях та захоплення, змінюють, при цьому, суспільство в цілому. Процеси, що породжують зміни стану безпеки суспільства та держави протікають у прихованій формі і результат впливу на інформаційне поле особистості, суспільства, держави виявляємо лише в момент її кульмінації.

Швидкість змін в інформаційному полі суспільства є досить великою, а уповільнена та невірна реакція з боку органів безпеки держави може призвести до катастрофи суспільства. Адаптація до змін в інформаційному полі держави, потребує на сучасному етапі значних і швидких коригувань у сфері захисту інформаційного поля держави. Необхідно бути більш здатним краще протидіяти та відновлюватися після кризи, більш обізнаними щодо характеру та потенціалу кризових ситуацій.

Аналіз результатів досліджень робіт в даній області показав, що вони здебільшого спрямовані на аналіз кількісних, якісних характеристик зв'язків пристроїв у соцмережах, систематизацію, кластеризацію отриманих даних, моніторинг інцидентів інформаційної безпеки, на забезпечення інформаційно-технічних, нормативно-правових аспектів інформаційної безпеки в просторі суспільства.

Залежно від задачі та мети протидії розробляються, змінюються моделі, методи, алгоритми, використовуються різні архітектури систем виявлення та протидії поширенню шкідливої інформації в соціальних мережах. На сучасному етапі постає питання підвищення ефективність протидії поширенню шкідливої інформації в соцмережах Інтернет.

ЛІТЕРАТУРА:

1. Соціальні мережі – реальні загрози віртуального світу. [Електронний ресурс]. – Режим доступу : http://ogo.ua/ articles/view/011–02–23/26490.htm.

2. Остапов С. Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король–Харків : Вид-во ХНЕУ, 2013. – 476 с.

ДОДАТОК Г
Презентація

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАЦЕПІНА Орислава Олександрівна

Метод протидії та виявлення в соціальних мережах шкідливої інформації

Науковий керівник
к.т.н., доцент Тітова В. Ю.

кафедра кібербезпеки

Тема Метод протидії та виявлення в соціальних мережах шкідливої інформації

Мета магістерської роботи - підвищення ефективності виявлення та протидії поширення в соціальних мережах шкідливої інформації за рахунок проведення аналізу та дослідження джерел шкідливої інформації в мережі та автоматизації вибору адекватних контрзаходів.

Наукова задача – розробка моделей, методу виявлення та протидії в соцмережах поширення шкідливої інформації

Об'єкт дослідження: Соціальні мережі, у яких можлива наявність поширення інформації із шкідливою інформацією («фейкові новини») та їх джерела.

Предмет дослідження: Моделі, алгоритми, методи виявлення та протидії в соцмережах шкідливої інформації.

Задачі досліджень у роботі формулюються наступним чином:

1. Аналіз існуючих моделей поширення в мережі шкідливої інформації та інформаційного обміну;
2. Аналіз існуючих методик та систем моніторингу виявлення та протидії в соціальних мережах шкідливої інформації;
3. Аналіз алгоритмів проведення оцінки в соцмережах джерел інформації;
4. Розробка моделей та алгоритмів аналізу соцмереж, джерела шкідливої інформації;
5. Розробка методу виявлення та протидії в соцмережах шкідливої інформації;
6. Розробка архітектури системи виявлення та протидії в соціальних мережах шкідливої інформації.

Наукова новизна роботи визначає:

1. Моделі шкідливої інформації, джерела повідомлень, соціальної мережі. Враховують в соціальній мережі структуру шкідливої інформації, інформаційних об'єктів та потоку інформаційного обміну на основі використання запропонованої класифікації в соцмерекжі інформаційних об'єктів. Модель шкідливої інформації в соцмережі, заснована на ознаках шкідливої інформації та взаємопов'язаних об'єктів, результатом якої є шкідливо-інформаційні об'єкти.

2. Метод виявлення та протидії в соціальних мережах шкідливої інформації -орієнтований на автоматизований вибір заходів виявлення та протидії шкідливої інформації в соцмережах зі списку контрзаходів та об'єктів впливу.

Методи дослідження. Для вирішення задач поставлених у магістерській роботі застосовувалися методи дослідження: системний та порівняльний аналіз; аналіз науково-технічної інформації про предметну область та систематизація -дозволили створити відповідні моделі; структурний синтез та об'єктно-орієнтований підхід - для оцінки джерел, проектування та розробки алгоритмів аналізу; експертні оцінки, методи ранжирування - запропоновано метод виявлення та протидії поширення в соцмережах шкідливої інформаціяїт, архітектуру системи протидії в соцмережах шкідливій інформації.

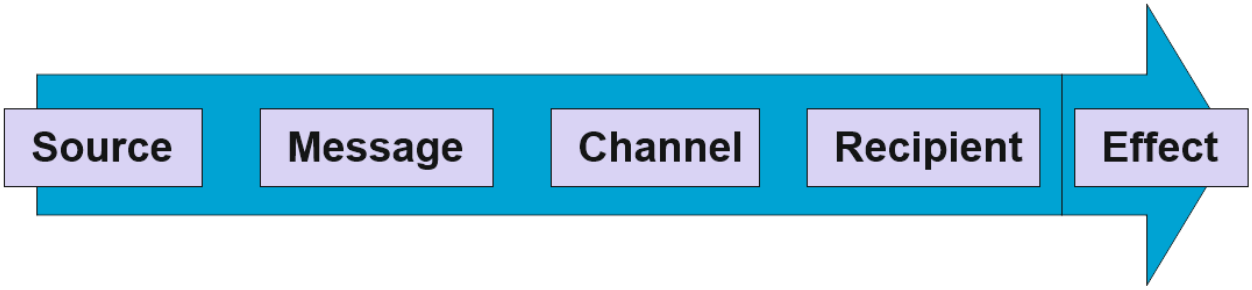
Практична цінність Запропоновані моделі, алгоритми, архітектура системи виявлення та протидії в мережі поширення шкідливої інформації можуть бути використані як окрема складова системи підтримки прийняття рішень на користь протидії шкідливій інформації в соцмережі оператором. Запропонований підхід до вирішення завдач, пов'язаних з аналізом та виявлення в соціальних мережах джерела шкідливої інформації, а також повязаних з протидією інформації та її джерелом, дозволяє формулювати адекватні науково-обґрунтовані вимоги.

Апробація роботи. Наукові результати і основні положення магістерської роботи доповідались і обговорювались на всеукраїнських та міжнародних науково-технічних конференціях,

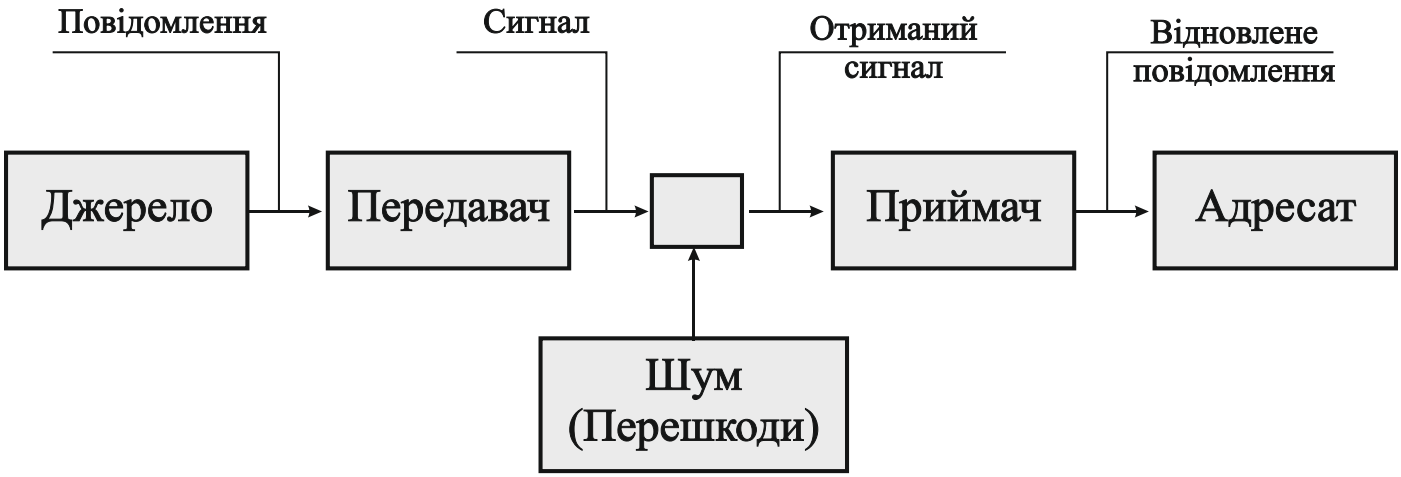
Публікації. За темою дипломної роботи ОКР «Магістр» опубліковано 1 теза доповідей, 1 фахова стаття.

Моделі комунікації протидії та виявлення
в соціальних мережах шкідливої інформації

Лінійна модель комунікації SMCRE



Модель комунікації Уівера – Шеннона



Множинна модель Френка Басса проникнення нововведень

$$n_t = \left(p + q \times \frac{N_t}{M} \right) \times \left(M - N_t \right),$$

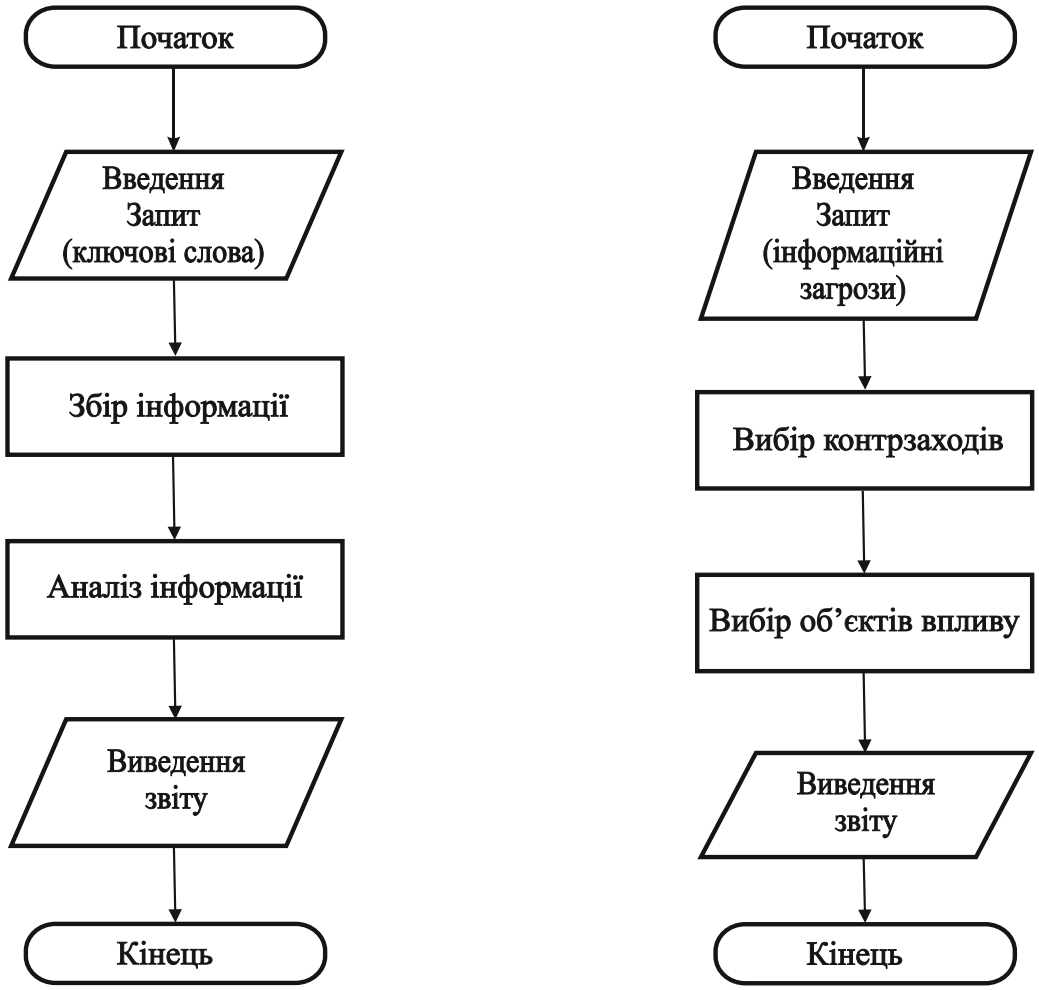
n_t - кількість прийнятих іновацій, в момент часу t; N_t - сумарна кількість інновацій; M- потенціал ринку; q – коефіцієнт внутрішнього впливу

Порогова модель Грановеттера

$$F_0\left(r\left(t\right)\right) = \begin{cases} r(t) < 0, \text{ то агент "не діє"} \\ r(t) \geq 0, \text{ то агент "діє"} \end{cases},$$

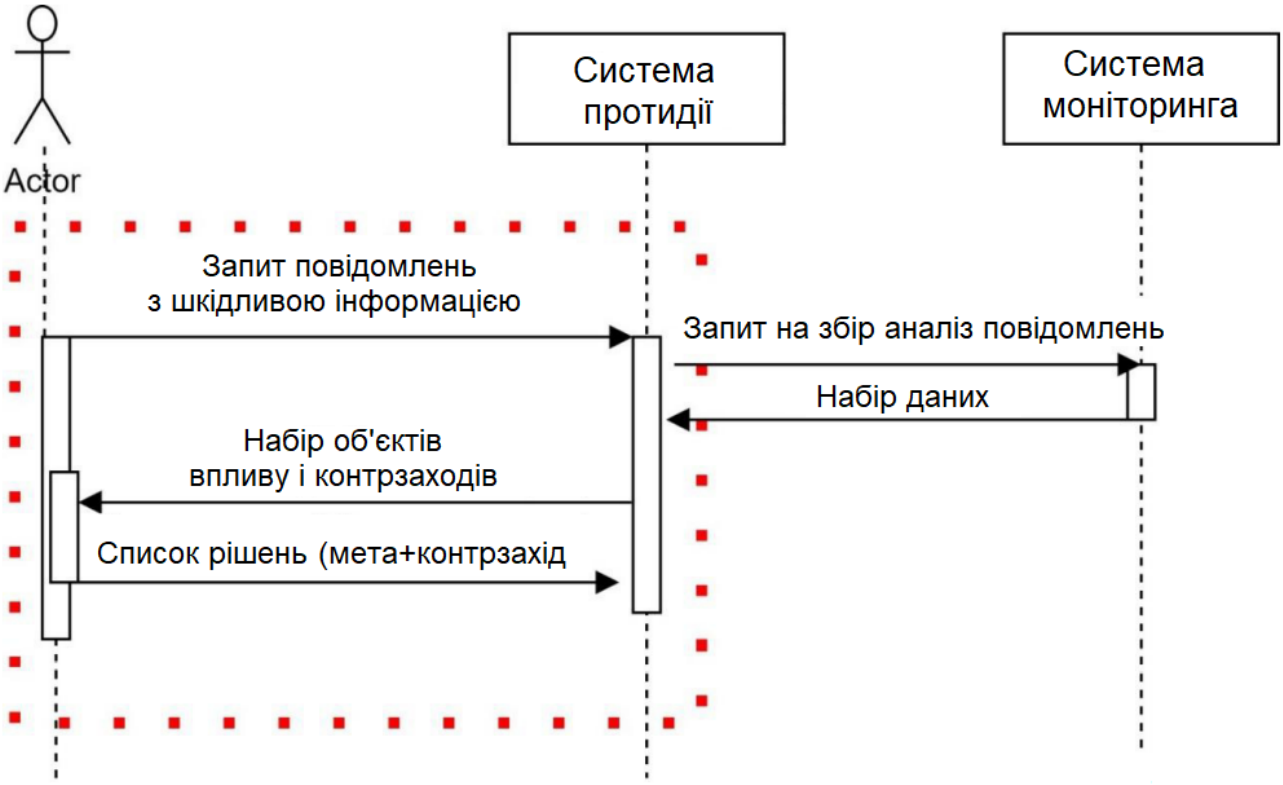
$F_0\left(r\left(t\right)\right)$ - функція розподілу порогів; t:$r(t)$ - частка агентів, що діють, в момент часу

Алгоритми моніторингу (*а*) та протидії (*б*) поширенню шкідливої інформації у процесі обробки мережевого контенту в соцмережах

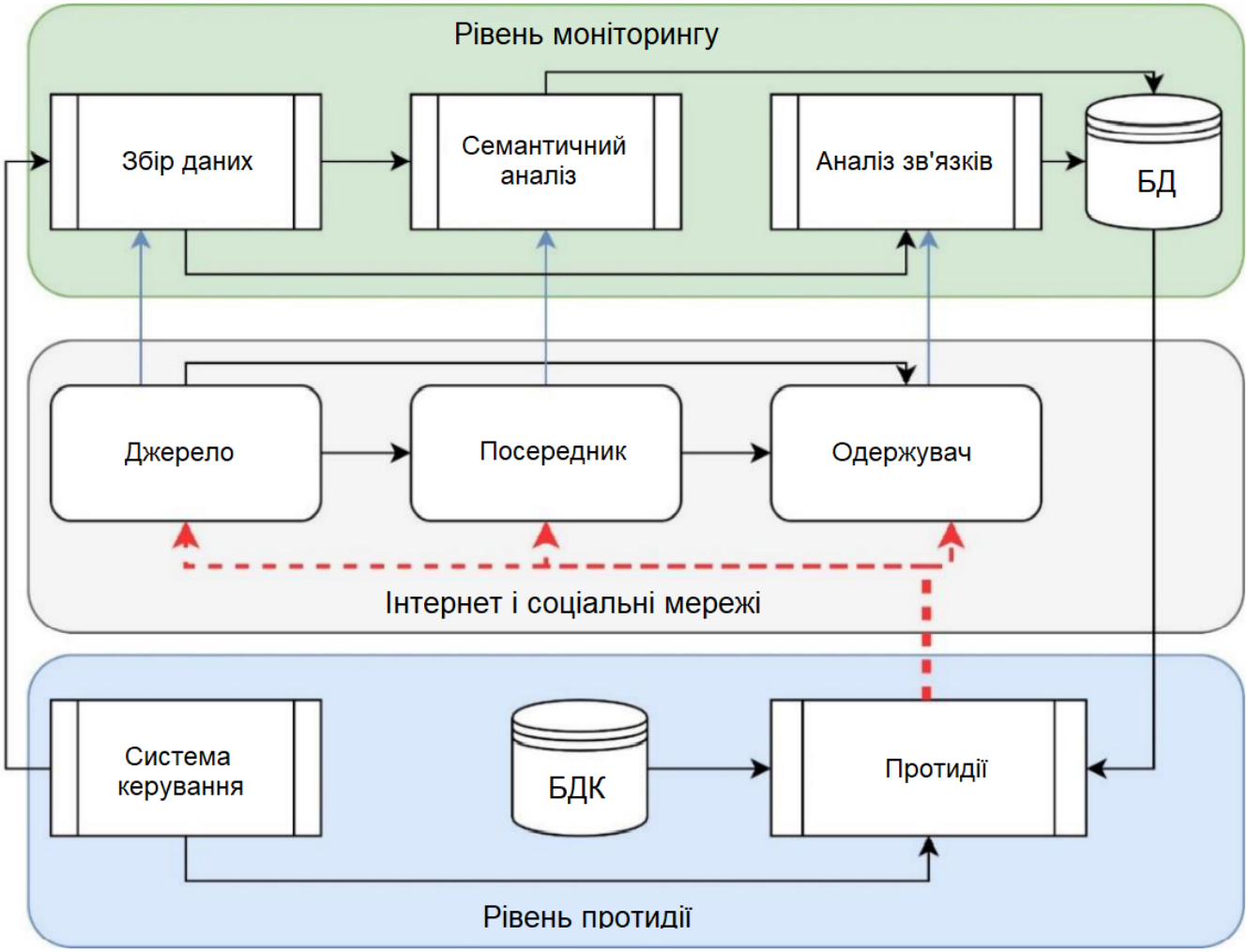


а) б)

Фундамент функціональності системи виявлення та протидії шкідливій інформації у соцмережах



Концептуальна модель системи виявлення та протидії поширенню шкідливої інформації у соцмережах



Теоретико-множинна модель шкідливої інформації

$$IO = \{io\}; MIO = \{io\}; MIO_i = \{io\}$$

$$MIO \subset IO; \forall io \in MIO : io \in IO$$

$$MIO_i \subseteq MIO; \forall io \in MIO_i : io \in MIO$$

$$Token_{mio_i} \subset T; Token_{mio_i} = \{t\}$$

$$CheckFeature(io,t) = \{True; False\}$$

$$io \in MIO_i \Leftrightarrow \exists Token_{mio_i} : checkFeature(io,t) = True$$

IO – множина інформаційних об'єктів, io – інформаційний об'єкт, T - множина ознак інформаційної загрози, t_i –*i -а* ознака інформаційної загрози, MIO – множина шкідливих інформаційних об'єктів мережі, MIO_i - *i-й* клас шкідливої інформації, $Token_{mio_i}$ - множина ознак загрози, що характеризують MIO.

Ранжування джерел повідомлень соціальних мережі

Залежно від кількості повідомлень на стіні, джерела соціальних мереж можуть бути розділені потенціалами:

1. Потенціал джерела низький (low index) - $P_{LI} = 0,$ відповідає нерівності (1):

$$f_1\left(S_p\right) \le \overline{X_1} = \frac{\sum_{i=1}^{n} x_i}{n}, \tag{1}$$

де $\sum_{i=1}^{n} x_i$ – сума числових коефіцієнтів повідомлень соцмережі на стіні джерела, $\overline{X_1}$ - середньоарифметичне у наборі даних для DATASET, n – кількість повідомлень джерела.

2. Потенціал джерела середній (medium index) - $P_{MI} = 1,$ відповідає нерівності (2):

$$f_2\left(S_p\right) \le \overline{X_2} = \frac{\sum_{i=1}^{n} x_i}{n} \tag{2}$$

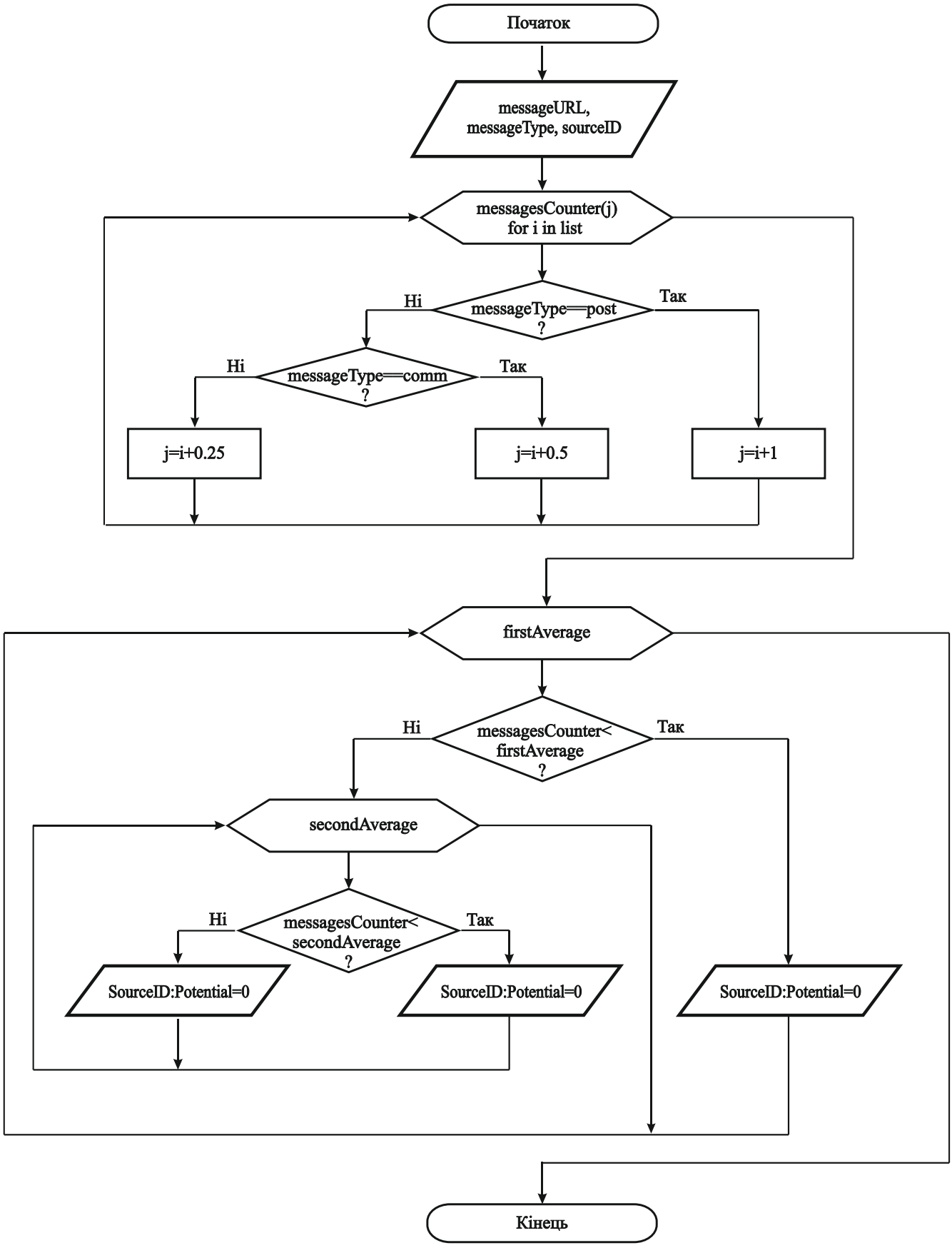
де $\overline{X_2}$ - середньоарифметичне значення у наборі даних для DATASET, отримане після видалення джерел із низьким потенціалом P_{LI}.

3. Потенціал джерела високий (high index) - $P_{HI} = 2,$ відповідає нерівності (3):

$$f_3\left(S_p\right) > \overline{X_2} = \frac{\sum_{i=1}^{n} x_i}{n} \tag{3}$$

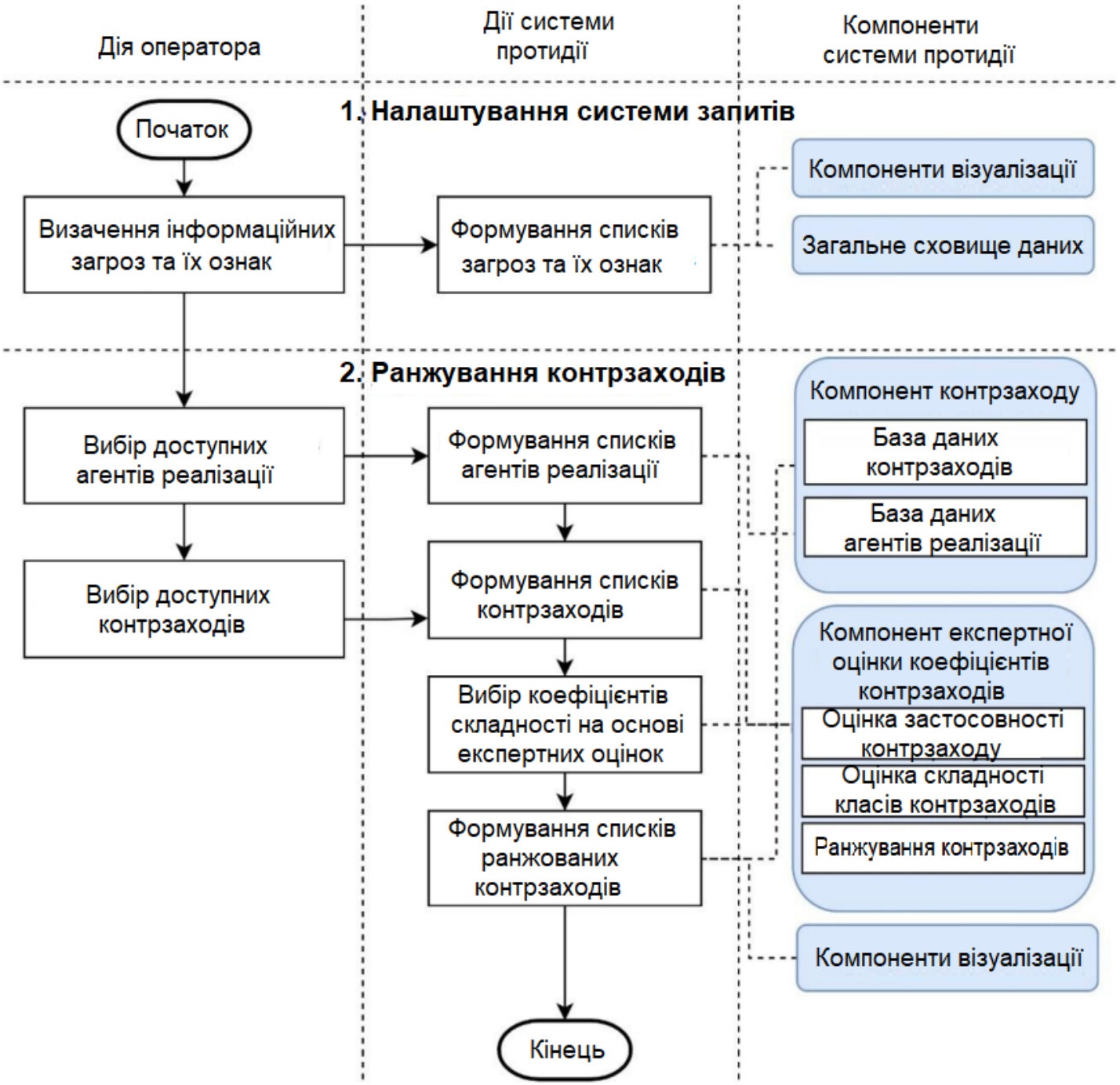
Всі джерела повідомлень в наборі даних DATASET можуть бути ранжовані за потенціалом в залежності від глибини та кількості на стіні джерела повідомлень.

Алгоритм ранжування джерел повідомлень за потенціалом



Алгоритм ранжування за потенціалом джерел повідомлень враховує: глибину розташування на сторінці в соцмережі повідомлень, кількість опублікованих повідомлень.

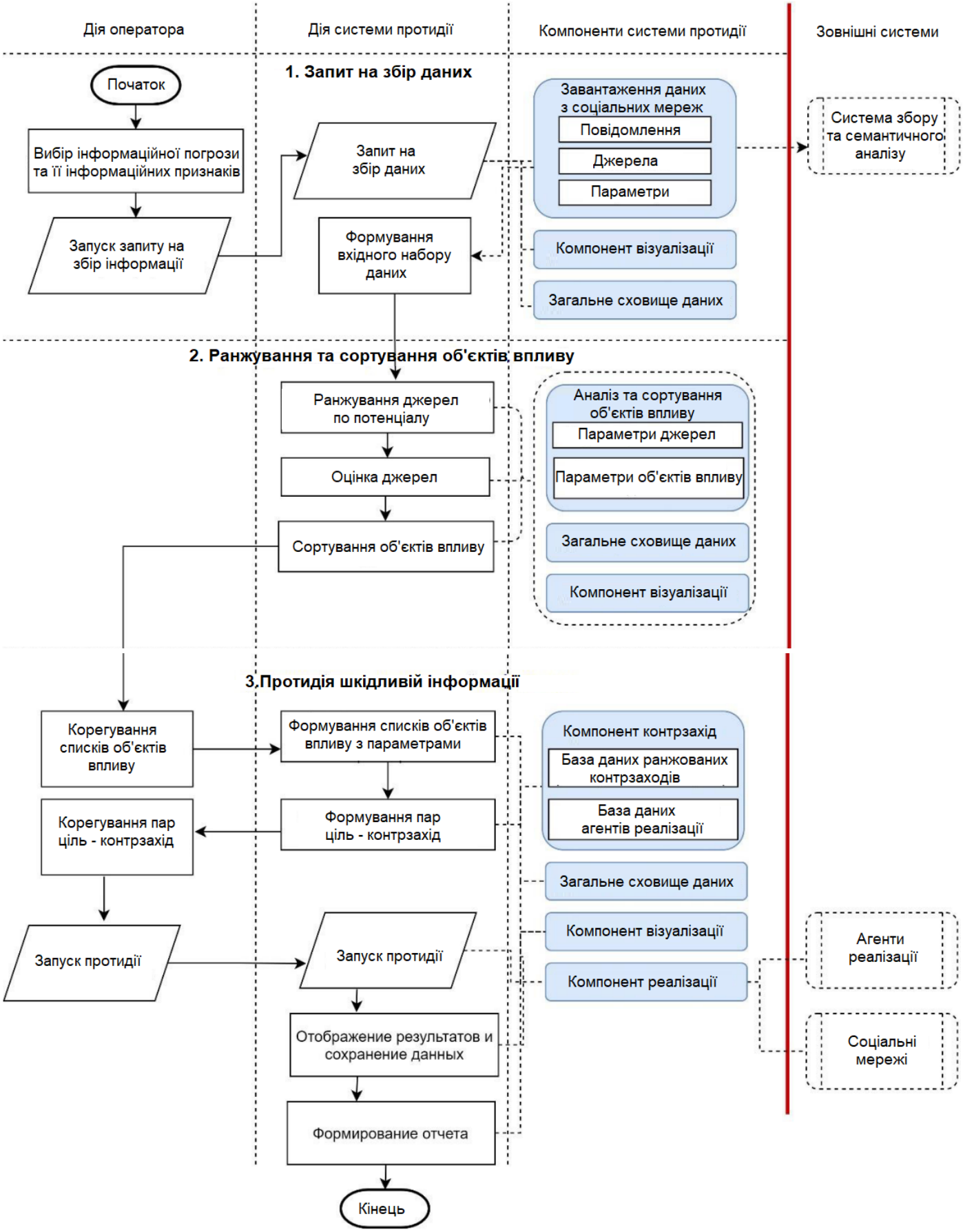
Метод протидії в соціальних мережах поширенню та виявлення шкідливої інформації



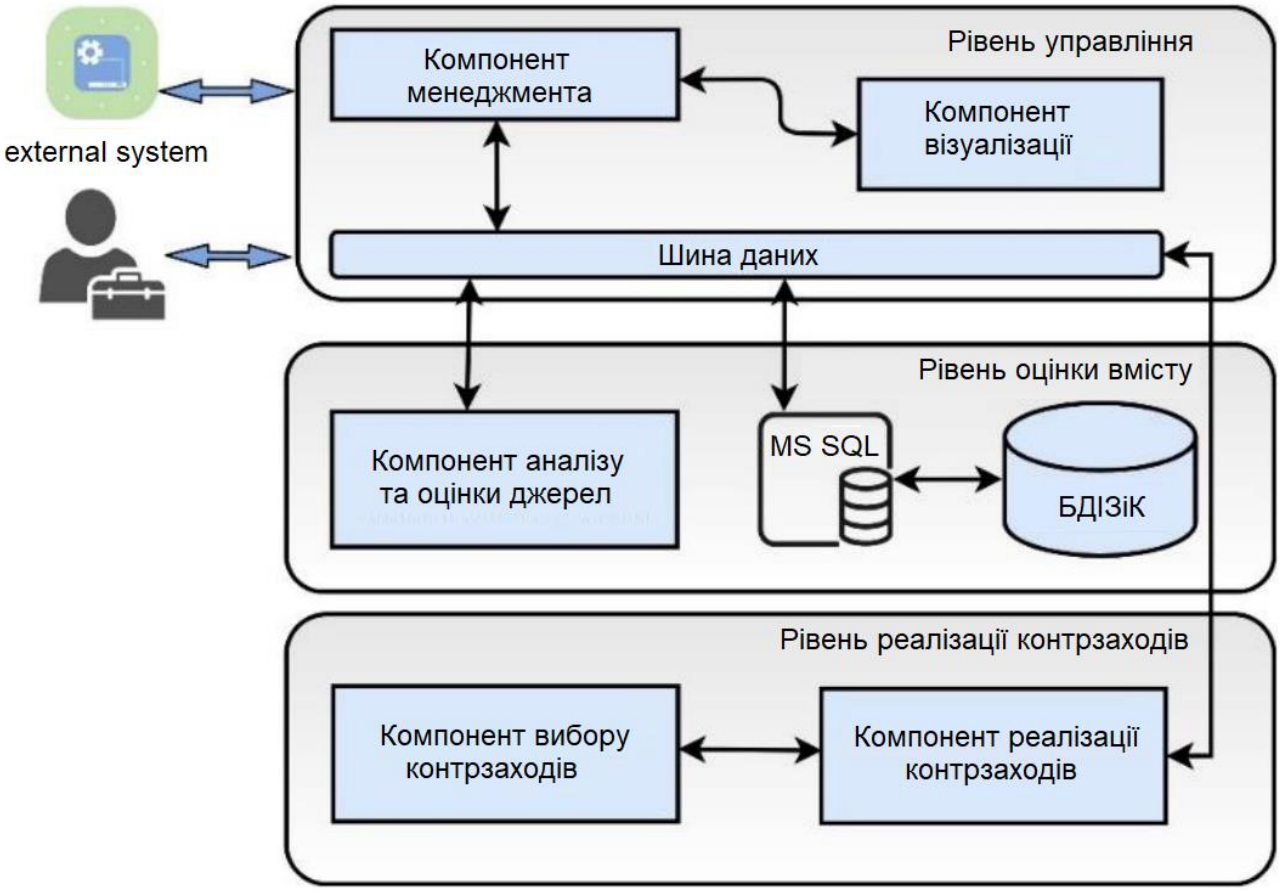
1. Налаштування системи запитів. Оператор, відповідно до інформаційно-ознакової моделі загроз, формує список інформаційних загроз та їх ознак.

2. Ранжування контрзаходів. Оператор вибирає доступні агенти реалізації. Формується та зберігається список доступних агентів реалізації. Вибирає доступні контрзаходи. Формується список контрзаходів протидії.

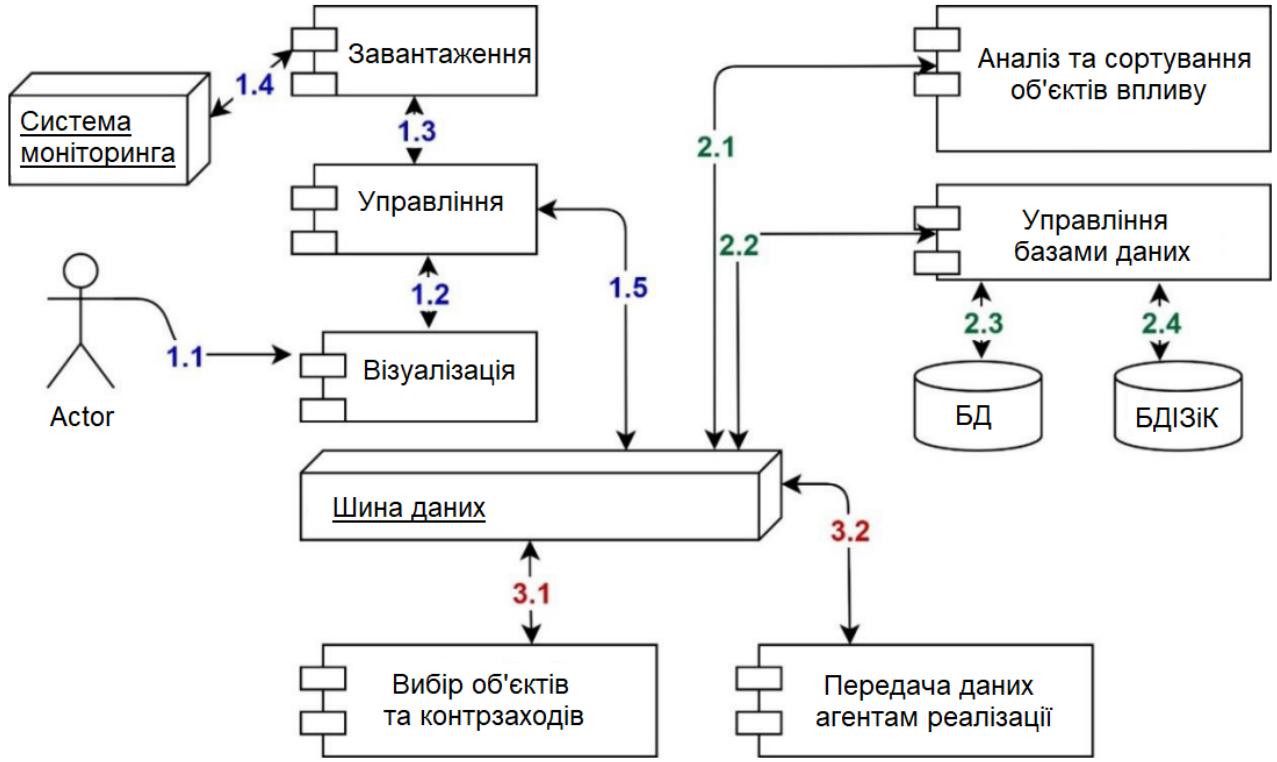
Метод протидії в соціальних мережах поширенню та виявлення шкідливої інформації на стадії експлуатації



Архітектура системи протидії шкідливій інформації в соціальній мережі



Функціональна структура системи протидії шкідливій інформації в соціальній мережі



ВИСНОВКИ

У магістерській роботі з метою підвищення ефективності системи протидії у соціальних мережах вирішена задача підвищення обґрунтованості прийнятого рішення на протидію шкідливій інформації за рахунок збільшення числа параметрів, що враховуються при виборі інформаційного об'єкта впливу та дійових контрзаходів. Вирішення поставленої задачі, досягається за рахунок проведення ранжування контрзаходів та аналізу джерел мережі шкідливої інформації. В результаті виконання магістерської роботи отримані наступні результати:

1. Запропоновані моделі джерела поширення шкідливої інформації, соціальної мережі та шкідливої інформації.
2. Запропоновані алгоритми проведення аналізу джерел поширення шкідливої інформації, ранжування контрзаходів протидії.
3. Розроблено метод протидії та виявлення в соціальних мережах поширення шкідливої інформації.
4. Розроблена архітектура та програмні прототипи компонентів системи протидії в соціальних мережах поширення шкідливої інформації.

Розроблені моделі шкідливої інформації, соціальної мережі, джерела повідомлень, відрізняється від аналогів, доданих нових атрибутів, елементів, зв'язків між ними, які більш детально характеризують інформаційні об'єкти в соціальних мережах. Запропоновані алгоритми проведення аналізу джерел поширенню шкідливої інформації та проведення ранжування контрзаходів, відрізняється від наявних, врахуванням залежних атрибутів інформаційних об'єктів та зв'язків у соцмережі. Як результат роботи алгоритму проведення аналізу джерел поширення шкідливої інформації формується відсортований список інформаційних об'єктів впливу. Алгоритм проведення ранжування контрзаходів протидії, враховує рівні складності та коефіцієнти для проведення кожного контрзаходу. Метод протидії та виявлення в соціальних мережах поширення шкідливої інформації, орієнтований на автоматизований та автоматичний вибір інформаційних об'єктів впливу та контрзаходів протидії поширенню в мережах шкідливої інформації зі списку контрзаходів та підтримку прийняття рішення про обрану протидію загрозам. Запропоновано архітектуру системи протидії та програмні компоненти системи протидії поширенню шкідливої інформації, яка містить оригінальні компоненти проведення оцінки та аналізу джерела поширення шкідливої інформації, ранжує контрзаходи протидії, база даних – містить інформацію про контрзаходи протидії, інформацію про агентів реалізації, з використанням яких будуть реалізовані контрзаходи.

Сформульовано відповідні рекомендації щодо використання результатів роботи для захисту інтересів організації, забезпечення інформаційної безпеки суспільства та особистості у соцмережах. Запропоновані підходи в магістерській роботі можуть бути використанні в міських та державних ситуаційних центрах для протидії тероризму та екстремізму, запобіганню розповсюдженню в мережах фейкових новин, інформації суїциду чи закликів до нього. Результати роботи можуть бути використані для систем керування репутацією бренду, вдосконалення систем батьківського контролю.

За темою роботи опубліковано 1 теза та 1 наукова стаття.

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Метод протидії та виявлення в соціальнихмережах шкідливої інформації

Автор: Зацепіна Орислава Олександрівна
Спеціальність: 123 – Комп'ютерна інженерія
Освітня програма: Програмування та захист комп`ютерних систем і мереж
Науковий керівник: Тітова В.Ю., к.т.н, доц.
Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 3,6% з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Віра ТІТОВА

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

Дата: 06.12.2022р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА ДИПЛОМНУ РОБОТУ

освітнього ступеня «магістр»

Магістр Зацепіна Ориславa Олександрівна

Тема Метод протидії та виявлення в соціальних мережах шкідливої інформації

Спеціальність 123 «Комп'ютерна інженерія»
спеціалізація «Комп'ютерні системи та мережі»

Обсяг дипломної роботи освітнього ступеня «магістр»:

кількість листів креслень 11; кількість сторінок записки 75

1. Короткий зміст ДР та прийнятих рішень В рамках магістерської роботи вирішена задача підвищення рівня ефективності виявлення та протидії поширення в соціальних мережах шкідливої інформації за рахунок проведення аналізу та дослідження джерел шкідливої інформації в мережі та автоматизації вибору адекватних контрзаходів, та отримані основні результати: моделі шкідливої інформації, джерела повідомлень, соціальної мережі. Враховують в соціальній мережі структуру шкідливої інформації, інформаційних об'єктів та потоку інформаційного обміну. Модель шкідливої інформації в соцмережі, заснована на ознаках шкідливої інформації та взаємопов'язаних об'єктів, результатом якої є шкідливо-інформаційні об'єкти. Метод виявлення та протидії в соціальних мережах шкідливої інформації - орієнтований на автоматизований вибір заходів виявлення та протидії шкідливої інформації в соцмережах зі списку контрзаходів та об'єктів впливу. Для вирішення задач поставлених у магістерській роботі застосовувалися методи дослідження: системний та порівняльний аналіз; аналіз науково-технічної інформації про предметну область та систематизація.

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

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обгрунтовується актуальність теми роботи, надається аналіз досліджуваної проблеми і обгрунтовується застосовуваний підхід до її вирішення, формулюються цілі і завдання дослідження, описується наукова новизна і практична значимість отриманих результатів. У першому розділі якісно та в повній мірі проаналізовано сучасний стан протидії та виявлення в соціальних мережах шкідливої інформації. Наступні розділи присвячені розробці моделі та методу виявлення та протидії поширенню шкідливої інформації у соціальних мережах, архітектурі компонентів системи протидії. Розглянуто питання оцінки методу протидії.

4. Позитивні сторони проекту Дипломна робота містить ряд інноваційних рішень, зокрема, в розробці моделей і алгоритмів, до вирішення задач пов'язаних з аналізом та виявленням в соціальних мережах джерел шкідливої інформації, а також з протидією інформації та її джерелом, дозволяє формулювати адекватні науково-обгрунтовані вимоги.

5. Негативні сторони проекту Як показано в роботі система протидії виявленню та поширенню шкідливої інформації в соцмережах орієнтована на більш загальні підходи поширенню інформації в мережах. Як покаже себе система при використанні специфічних методів при поширенні шкідливої інформації в соцмережах?

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми дипломної роботи з дотриманням стандартів. В загальному графічне оформлення виконане на достатньому рівні. Пояснювальна записка відповідає нормам для її оформлення.

7. Відгук про роботу в цілому В загальному дипломна робота заслуговує позитивної оцінки. Весь матеріал дипломної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики дипломної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі.

8.Інші зауваження

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

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)

Лисенко Сергій Миколайович, д.т.н., професор, кафедра комп'ютерної інженерії та інформаційних систем, Хмельницького національного університету

« 1 » 12 2022р. _____ (підпис)

ХНУ. Зам. 54, тир. 6000, 2007.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльощу Ю.П.
Зацепіної Орислави Олександрівни
ПІБ здобувача вищої освіти

студента ФІТ, 2 курсу, групи КІм-21-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

5.12.2022
дата

підпис

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1013208400

Дата перевірки:
06.12.2022 12:02:09 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
06.12.2022 14:15:43 EET

ID користувача:
100008300

Назва документа: **Зацепіна_О_О_Магістерська**

Кількість сторінок: **77** Кількість слів: **13773** Кількість символів: **111360** Розмір файлу: **11.86 MB** ID файлу: **1012824874**

14.6%
Схожість

Найбільша схожість: **11.4%** з Інтернет-джерелом (http://elar.khmnu.edu.ua/jspui/bitstream/123456789/12636/1/VOTTP_3.

11.7% Джерела з Інтернету | 12 ..... Сторінка 79

3.31% Джерела з Бібліотеки | 13 ..... Сторінка 79

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

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

Замінені символи | 10

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 0.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 10%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 108800 Название: Метод протидії та виявлення в соціальних мережах шкідливої інформації Добавлено в БД: 2022-11-28 Авторы: Зацепіна О.О. Руководители: Тітова В.Ю. Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	101276	734	774 (1%)	15 (2%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы