РЕФЕРАТ

Пояснювальна записка: ___ с., ___ рис., ___ табл., __ додатків, ___ джерел.

Об'єкт дослідження: методи класифікації користувачів соціальних мереж з метою детектування шкідливих акаунтів.

Мета роботи (проекту): розробка алгоритму детектування шкідливих акаунтів в соціальних мережах.

Методи дослідження: аналіз, системний підхід, методи, розпізнавання образів, кластеризація, класифікація.

У спеціальній частині проведено аналіз сучасних методів детектування, методів кластеризації з метою вибору найбільш ефективних. Сформульовано формальні вимоги до вибору методів детектування. Запропоновано метод поліпшення якості сортування, відстеження поведінки підозрілих акаунтів. Розроблено алгоритм детектування ботів на базі обраних методів.

В економічному розділі визначено економічну ефективність від розробки і реалізації запропонованого алгоритму.

Практичне значення роботи полягає в можливості інтеграції розробленого алгоритму в існуючу систему детектування шкідливих акаунтів в соціальних мережах для поліпшення аналізу та розпізнавання даних.

Результати проведених в дипломній роботі досліджень можуть бути використані для подальшої роботи над удосконаленням алгоритмів детектування шкідливих акаунтів.

Наукова новизна дослідження полягає в розробці комбінованого методу розпізнавання шкідливих акаунтів з мінімізацією кількості додаткових перевірок користувачів.

Напрямки подальших досліджень – тестування запропонованого алгоритму на прикладі реальних соціальних мереж.

Ключові слова: СОЦІАЛЬНІ БОТИ, ДЕТЕКТУВАННЯ, ШКІДЛИВІ АКАУНТИ, СОЦІАЛЬНІ МЕРЕЖІ, МЕТОДИ КЛАСИФІКАЦІЇ, КЛАСТЕРНИЙ АНАЛІЗ.

РЕФЕРАТ

Пояснительная записка: ___ с., ___ рис., ___ табл., __ приложений, ___ источников.

Объект исследования: методы классификации пользователей социальных сетей с целью детектирования вредоносных аккаунтов.

Цель работы (проекта): разработка алгоритма детектирования вредоносных аккаунтов в социальных сетях.

Методы исследования: анализ, системный подход, методы распознавания образов, кластеризации, классификация.

В специальной части проведен анализ современных методов детектирования и кластеризации для выбора наиболее эффективных. Сформулированы требования к выбору методов. Предложен метод улучшения качества сортировки, отслеживания поведения подозрительных аккаунтов. Разработан алгоритм детектирования ботов на базе выбранных методов.

В экономическом разделе определена экономическая эффективность от разработки и реализации предложенного алгоритма.

Практическое значение работы состоит в возможности интеграции алгоритма в существующую систему детектирования вредоносных аккаунтов в социальных сетях для улучшения анализа и распознавания данных.

Результаты проведенных в дипломной работе исследований могут быть использованы для дальнейшей работы над усовершенствованием алгоритмов детектирования вредоносных аккаунтов.

Научная новизна исследования – в разработке комбинированного метода распознавания вредоносных аккаунтов с минимизацией количества дополнительных проверок пользователей.

Направления дальнейших исследований – тестирование предложенного алгоритма на примере реальных социальных сетей.

Ключевые слова: СОЦИАЛЬНЫЕ БОТЫ, ДЕТЕКТИРОВАНИЕ, ВРЕДОНОСНЫЕ АКАУНТЫ, СОЦИАЛЬНЫЕ СЕТИ, МЕТОДЫ КЛАССИФИКАЦИИ, КЛАСТЕРНЫЙ АНАЛИЗ.

ABSTRACT

Explanatory note: ___ pages, ___ pics., ___tables, __ applications, ___ sources.

Project objectives: methods of classifying social networks users to detect malicious accounts.

Project purpose: Develop an algorithm for detecting malicious accounts in social networks.

Research methods: analysis, system approach, methods of: visualization, data collection, pattern recognition, clustering, algorithm development, classification.

In the technical part, existing methods of detecting social networks bots are analyzed and an improved algorithm is developed.

Analysis of existing modern detection methods which use various image recognition approaches and clustering methods is carried out. Requirements for the choice of appropriate detection methods are formulated. New method is proposed to improve quality of sorting, tracking suspicious accounts behavior in social networks. An algorithm for detecting bots based on selected methods is developed.

In the economic section, economic efficiency of proposed algorithm is assesed.

Practical value of this work is the ability to integrate developed algorithm into existing system for detecting malicious accounts in social networks to improve analysis and recognition of data.

Results of research carried out in the project can be used for further improvement of malicious account detection algorithms.

The scientific novelty of this research is: new method which combines malicious accounts recognition and minimization of additional user checks.

Keywords: SOCIAL BOT, DETECTION, MALICIOUS ACCOUNTS, SOCIAL NETWORKS, CLASSIFICATION METHODS, CLUSTER ANALYSIS.

ЗМІСТ

с.

ВСТУП

РОЗДІЛ 1. АНАЛІЗ ВПЛИВУ ШКІДЛИВИХ АКАУНТІВ У СОЦІАЛЬНИХ МЕРЕЖАХ

1.1 Загальна характеристика соціальних мереж

1.2 Вплив ботів на соціальні мережі

1.3 Класифікація соціальних ботів

1.4 Висновки до першої частини

РОЗДІЛ 2. АНАЛІЗ МЕТОДІВ ДЕТЕКТУВАННЯ ШКІДЛИВИХ АКАУНТІВ

2.1 Візуальне представлення соціальних мереж

2.2 Методи і засоби збору та класифікації даних

2.3 Методи розпізнавання образів для класифікації

2.3.1 Кластеризація

2.3.2 Класифікація

2.4 Існуючі методи виявлення шкідливих акаунтів

2.5 Математичний апарат

2.5.1 Наївний алгоритм Байєса

2.5.2 Дерева рішень

2.5.3 Випадковий ліс

2.6 Висновки до другого розділу

РОЗДІЛ 3. РОЗРОБКА АЛГОРИТМУ ДЕТЕКТУВАННЯ ШКІДЛИВИХ АКАУНТІВ В СОЦІАЛЬНИХ МЕРЕЖАХ

3.1 Визначення характеристики близькості об'єктів

3.2 Обґрунтування вибору методів кластеризації

3.6.1 Ієрархічні методи кластеризації

3.6.2 Неієрархічні методи кластеризації

3.6.3 Чіткі і нечіткі методи кластеризації

3.7 Розробка алгоритму обчислення кількості кластерів

3.7.1 Обґрунтування вибору методу для розрахунку оптимальної кількості кластерів
3.7.2 Алгоритм модуля визначення оптимальної кількості кластерів
3.8 Розробка алгоритму визначення шкідливих акаунтів
3.8.1 Обґрунтування вибору методу кластеризації для класифікації акаунтів
3.8.2 Визначення кластерів з підозрілими акаунтами
3.8.3 Алгоритм модуля прийняття рішень
3.9 Висновки до третього розділу
РОЗДІЛ 4. ЕКОНОМІЧНА ЧАСТИНА
4.1 Орієнтовний розрахунок капітальних витрат
4.1.1 Визначення трудомісткості розробки та опрацювання програмного забезпечення
4.1.2 Розрахунок витрат на створення програмного продукту
4.1.3 Розрахунок поточних (експлуатаційних) витрат
4.2 Економічне обґрунтування доцільності розробки
4.3 Висновки до четвертого розділу
ВИСНОВКИ
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ
ДОДАТОК А. Перелік документів на оптичному носії
ДОДАТОК Б. Відгук керівника економічного розділу
ДОДАТОК В. Відгук на дипломну роботу магістра.
ДОДАТОК Г. Зведена таблиця характеристик українських соціальних мереж.
ДОДАТОК Д. Приклад вибірки користувачів соціальної мережи з показниками.
ДОДАТОК Е. Схема роботи модуля прийняття рішень

ВСТУП

В даний час соціальні мережі – невід'ємна частина більшості сфер життя людини, інтегруюча практично всі існуючі інтернет-джерела. Вони ефективно структурують користувачів з політичних або релігійних поглядів, інтересів і захоплень, зачіпаючи практично всі верстви населення, і є потужним інструментом самоорганізації як окремих груп, так і суспільства в цілому. Соціальні мережі, які об'єднують 40% населення планети щодня, стали не тільки засобом спілкування, а й великим джерелом інформації, розважальним хостингом, комерційним майданчиком з набором ефективних інструментів для поширення послуг і товарів. Природно, що зацікавлені особи прагнуть використовувати такий безмежний потенціал для наживи і досягнення своїх, далеко не благородних цілей.

Одна з основних загроз – так звані «соціальні боти», що сприяють підвищенню недовіри до співрозмовників, сумнівам в їх реальності [1]. Це шкідливі програми, підроблені акаунти, здатні імітувати поведінку людей. На даний момент, боти створюють чимало проблем, як для звичайних користувачів, так і для тих, хто застосовує соціальні мережі для ведення маркетингової кампанії або проведення соціальних досліджень. За допомогою експлуатації бот-профілів в соціальних мережах сильно спотворюється інформація про дійсні переваги і інтереси користувачів порталів. Одна з основних цілей використання бот-програм – поширення інформації, як позитивної, так і негативної щодо просування ідеї, що заважає проведенню SMM-аналізу (Social media marketing – процес залучення трафіку чи уваги до бренду або продукту через соціальні платформи), за рахунок «накрутки» кількості учасників в спільнотах [4]. Тому слід визначати, які користувачі соціальної мережі є запрограмованими, і вміти розділяти потік даних на генерований ботами і людиною.

Як правило, масове поширення запрограмованих акаунтів застосовується для:

– організації інформаційних вкидань;
– масового розкрадання персональних даних;
– погіршення довіри в соціальних мережах;
– створення помилкових новин і голосувань;
– як засіб для легального бізнесу кіберзлочинності;
– створення проблем в соціальному маркетингу.

Так, наприклад, при SMM-просуванні в «Вконтакте» або «Facebook» частка цільової аудиторії це «мертві» акаунти або акаунти-двійники [4]. За даними дослідників тіньового ринку десятки сервісів пропонують ботів-читачів, продаючи їх великими партіями. При цьому обсяг ринку сягає $360 млн.

Загрозливі масштаби використання соціальних ботів вимагають створення ефективних алгоритмів їх детектування. Самі інтернет-платформи і соціальні сервіси не надто переймаються цією проблемою. В результаті страждають як звичайні користувачі, які організовують різні спільноти, так і компанії, які просувають через соціальні мережі товари, бренди, послуги. А статистичні данні при цьому: кількість лайків (позитивних оцінок), приріст учасників спільнот і кількість публікацій, мало пов'язані з кількістю реальних покупців.

Таким чином, завдання розпізнавання шкідливих акаунтів в соціальних мережах і боротьба з ними залишається актуальною в питанні кібербезпеки.

Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [21].

Рішенням проблеми стане розвиток методів мережевого аналізу, які призначені для виявлення і класифікації спільнот в соціальних мережах, оцінки їх зв'язності, ступеня довіри, а також розробка ефективних алгоритмів детектування шкідливих акаунтів.

Метою дипломної роботи є розробка вдосконаленого алгоритму детектування шкідливих акаунтів в соціальних мережах, який ґрунтується на дослідженні сучасних методів.

Для досягнення зазначеної мети дипломної роботи визначені завдання, необхідні для виконання:

- вивчити предметну область за темою дипломного проекту;
- провести аналіз сучасних методів детектування шкідливих акаунтів в соціальних мережах, а також їх ефективності;
- проаналізувати способи візуалізації та класифікації акаунтів в соціальних мережах за заданими ознаками;
- вибрати методи класифікації об'єктів для розробки алгоритму детектування;
- розробити алгоритм детектування шкідливих акаунтів в соціальних мережах;
- провести аналіз результатів роботи;
- довести економічну доцільність розробки.

Об'єкт дослідження проекту – процес класифікації користувачів з метою виявлення шкідливих акаунтів.

Предмет дослідження – методи розпізнавання образів, кластерного аналізу для виявлення шкідливих акаунтів в соціальних мережах.

Для вирішення завдань, поставлених у дипломній роботі, використані наступні методи: методи аналізу та синтезу (при розкритті теоретичних положень та уточненні категоріального апарату), історико-логічний метод (при групуванні теорії), методи візуалізації (для графічного представлення соціальних мереж), методи збору даних з різних інтернет-сервісів, математичні методи розпізнавання образів, методи ієрархічної кластеризації

(для визначення кількості груп користувачів при класифікації), методи нечіткої кластеризації (для проведення розподілу користувачів на групи з однаковими ознаками), методи теорії ймовірностей і математичної статистики, методи розробки алгоритмів (для розробки алгоритму детектування), імітаційне моделювання (при перевірці отриманих результатів).

Наукова новизна отриманих результатів:

- удосконалено метод детектування соціальних ботів, який поліпшує якість сортування акаунтів з подальшим аналізом результатів та прийняттям рішень по окремим групам користувачів;
- запропоновано комбінований метод відстеження поведінки підозрілих акаунтів в соціальній мережі, що дозволяє значно зменшити кількість додаткових перевірок.

Практична цінність дипломної роботи полягає в наступному: запропонований алгоритм може бути використаний для інтегрування в існуючу систему детектування шкідливих акаунтів в соціальних мережах для поліпшення аналізу та розпізнавання даних.

Основні положення дипломної роботи викладені в статті, розміщеній на п’ятій всеукраїнській науково-технічній конференції студентів, аспірантів і молодих учений «Молодь: наука та інновації». Секція 12. Автоматизація та інформаційні технології.

РОЗДІЛ 1. АНАЛІЗ ВПЛИВУ ШКІДЛИВИХ АКАУНТІВ У СОЦІАЛЬНІХ МЕРЕЖАХ

1.1 Загальна характеристика соціальних мереж

У житті людини суспільство відіграє важливу роль: з дитинства люди, що знаходяться поруч так чи інакше впливають на нас, відбувається безперервна взаємодія в соціальній сфері (в дитячому садку, школі, університеті, вдома, на роботі), без якої повноцінний розвиток особистості неможливий. З середини XX століття було опубліковано безліч робіт вчених-соціологів, в тому числі і вітчизняних, де пропонуються різні підходи аналізу в сфері суспільних відносин. У своїх працях під соціальною мережею вони розуміли структури людей, пов'язаних один з одним спільними відносинами або інтересами. Вже пізніше, з появою Інтернету, таким чином стали називати спеціалізовані електронні портали. Проте, поняття «соціальна мережа» має більш широкий зміст. Соціолог Градосельская Г. В. [26] запропонувала наступне визначення: «Соціальні мережі – це особлива реальність і особлива філософія аналізу даних, яка дозволяє інтегрувати різні математичні підходи – статистичні, системні, імітаційні – із сучасною соціальною теорією».

З розвитком інформаційних технологій з'явилися електронні портали, здатні відображати ті чи інші сторони активності людини в суспільстві, зберігати і накопичувати інформацію. Особливе місце займають віртуальні соціальні мережі, такі як «Вконтакте», «Facebook», «Twitter» та інші.

Таким чином, сьогодні популярне інше визначення соціальної мережі. Її ще називають віртуальною соціальною мережею. Під віртуальною (онлайн) соціальною мережею розуміється соціальна структура Інтернет-середовища, вузли якої складають організації або окремі люди, а зв'язки означають встановлені взаємодії (політичні, корпоративні, службові, сімейні, дружні, за інтересами).

Відразу після реєстрації нового учасника в мережі створюється профіль користувача, в якому спочатку міститься інформація з заповнених анкетних даних: вік, стать, сімейний стан, інтереси, освіта та інше. Цей профіль більш «розвинений» в порівнянні з аналогами в блогах і форумах, так як останні можуть бути лише частиною засобів спілкування в соціальній мережі.

Усередині соціальної мережі утворюються різні групи і спільноти за інтересами, наприклад, любителів музики, автомобілів, навчання, роботи. Зв'язки між учасниками таких об'єднань досить сильні, що дозволяє їх легко ідентифікувати. На рисунку 1.1 зображено приклад описаної ситуації. Усередині групи між учасниками зв'язків більше і вони сильніші, ніж з іншими членами соціальної мережі. У складі спільнот можуть з'являтися підгрупи і співтовариства, таким чином, утворюючи ієрархію [9].

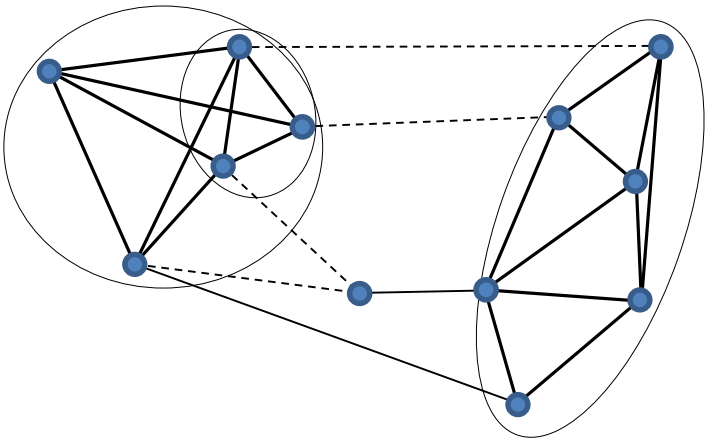


Рисунок 1.1 – Ієрархія груп в соціальних мережах

Інструментами, за допомогою яких відбувається спілкування в віртуальних соціальних мережах, є:

– блог – мережевий журнал, до якого регулярно додаються записи;

– чат – надає можливість обміну текстовими повідомленнями між кількома учасниками в режимі online;

– форуми, де користувач може створювати нову тему, доступну для інших. Інші користувачі можуть переглядати її та залишати свої коментарі [9].

1.2 Вплив ботів на соціальні мережі

Аналіз соціальних мереж (socialnetworkanalysis, SNA) – напрямок сучасної комп'ютерної соціології, який займається описом і аналізом зв'язків (мереж) різної щільності та інтенсивності, що виникають в ході соціальної взаємодії і комунікації [27].

Аналіз соціальних даних стрімко набирає популярність у всьому світі [1, 2] завдяки появі в 1990-х роках онлайнових сервісів соціальних мереж (SixDegrees, LiveJournal, Facebook, Twitter та інші). З цим пов'язаний феномен соціалізації персональних даних: стали публічно доступними факти біографії, листування, щоденники, фото-, відео-, аудіоматеріали, замітки про подорожі і т.і. Таким чином, соціальні мережі є унікальним джерелом даних про особисте життя і інтереси реальних людей. Це відкриває безпрецедентні можливості для вирішення дослідницьких та бізнес-задач (багато з яких до цього неможливо було вирішувати ефективно через брак даних), а також створення допоміжних сервісів і додатків для користувачів соціальних мереж.

Крім того, цим обумовлюється підвищений інтерес до збору та аналізу соціальних даних з боку компаній і дослідницьких центрів. Аналітичне агентство Gartner опублікувало звіт під назвою "Цикл ажіотажу для технологій, що розвіваються" [6]. Згідно зі звітом, технології "Соціальна аналітика" і "Великі дані" в даний час знаходяться на "піку завищених очікувань". Зокрема, дослідженнями соціальних даних активно займаються університети Карнегі-Меллон, Стенфорд, Оксфорд, INRIA, а також компанії Facebook, Google, Yahoo!, LinkedIn і багато інших. Компанії-власники сервісів онлайнових соціальних мереж (Facebook, Twitter) активно інвестують в розробку вдосконалених інфраструктурних (Cassandra, Presto, FlockDB, Thrift) і алгоритмічних (нові алгоритми пошуку і рекомендації

користувачів, товарів і послуг) рішень для обробки великих масивів даних користувачів. Разом з тим, при роботі з соціальними даними потрібно брати до уваги такі фактори як нестабільність якості користувацького контенту (спам і неправдиві акаунти), проблеми із забезпеченням приватності особистих даних користувачів при зберіганні і обробці, а також часті оновлення користувальницької моделі та функціоналу. Все це вимагає постійного вдосконалення алгоритмів розв'язання різних аналітичних і бізнес-задач.

Так, група фахівців з канадського Університету Британської Колумбії у Ванкувері провела дослідження можливостей так званих «соціальних ботів» (англ. Socialbot), які широко використовують зловмисники і маркетологи для дій в соціальних мережах. Двомісячне дослідження проводилося з метою визначити, наскільки вразливі соціальні мережі і їх користувачі перед обличчям великомасштабних операцій, пов'язаних з викраденням особистих даних. Експериментальна частина дослідження тривала два місяці. За цей час канадські дослідники в одній лише «Facebook» за допомогою «соціо-ботів» отримали майже 250 гігабайт інформації про користувачів цієї соціальної мережі. Уже з одного цього можна зрозуміти, що сучасні мережі дуже уразливі для ботів.

За словами авторів дослідження, «соціальні» механізми захисту в «Facebook» та інших соц.мережах існують, але вони недостатньо інтелектуальні і поки не можуть відрізнити справжнього користувача від бота, навіть якщо останній діє повністю на автоматі і без участі живої людини. Також в дослідженні зазначено, що в майбутньому на базі цієї або подібної методики кіберзловмисниками можуть бути реалізовані справжні кампанії по крадіжці даних у десятків або навіть сотень тисяч людей.

Рішенням даної проблеми є розвиток методів мережевого аналізу. Дослідницькі лабораторії по даній темі створені в багатьох світових університетах. Ці методи можуть дати набагато більш детальну інформацію – виявити і кластеризувати спільноти, оцінити зв'язність таких спільнот,

ступінь взаємної довіри, лідерів думок. Разом з контент аналізом оцінити тональність висловлювань і більш точно окреслити портрет клієнта, його інтереси і цінності. В результаті в 2011 році з'явився ще один термін – socialmarketinganalysis (SMM), який зараз пропонує кілька метрик, заснованих на мережевому аналізі.

SMM – процес залучення трафіку або уваги до бренду або продукту через соціальні мережі. Це комплекс заходів щодо використання соціальних медіа в якості каналів для просування компаній і вирішення інших бізнес-завдань. На світовому ринку зараз з'являються SMM-інструменти, засновані на мережевому аналізі, програмні продукти, призначені для підвищення ефективності маркетингових кампаній, що проводяться в соціальних мережах, розробки і проведення маркетингових кампаній, їх аналізу в режимі реального часу.

При аналізі соціальних мереж особлива увага приділяється зв'язкам, а не самим дійовим особам. Як правило, соціальна мережа описується графом або матрицею взаємин (рисунок 1.2) [27].

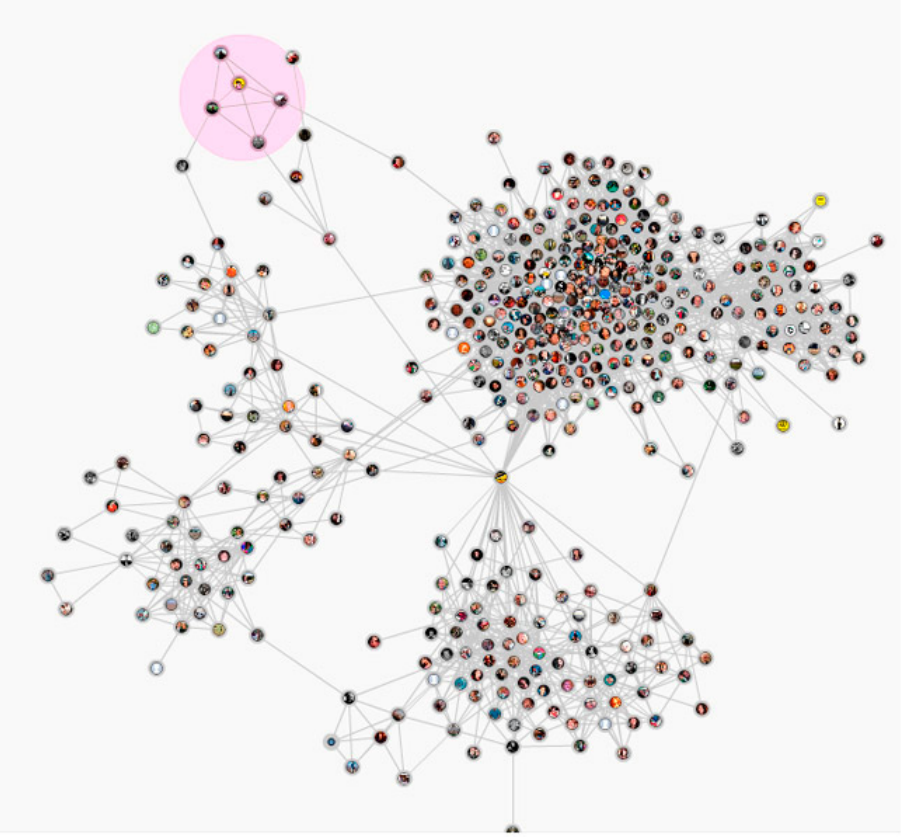


Рисунок 1.2 – Приклад графа соціальної мережі

Одним з основних модулів системи аналізу соціальних мереж є модуль детектування ботів в соціальних мережах. Багато з груп «Вконтакте» і «Facebook» більш ніж на 40% складаються з шкідливих акаунтів (рис 1.3). Підсумком цього є загальне зниження ефективності дій в соціальних медіа до 35%. Наприклад, при виконанні робіт по SMM просуванню в групу замість цільової аудиторії теж можуть бути притягнуті «мертві» акаунти і акаунти-двійники [4].

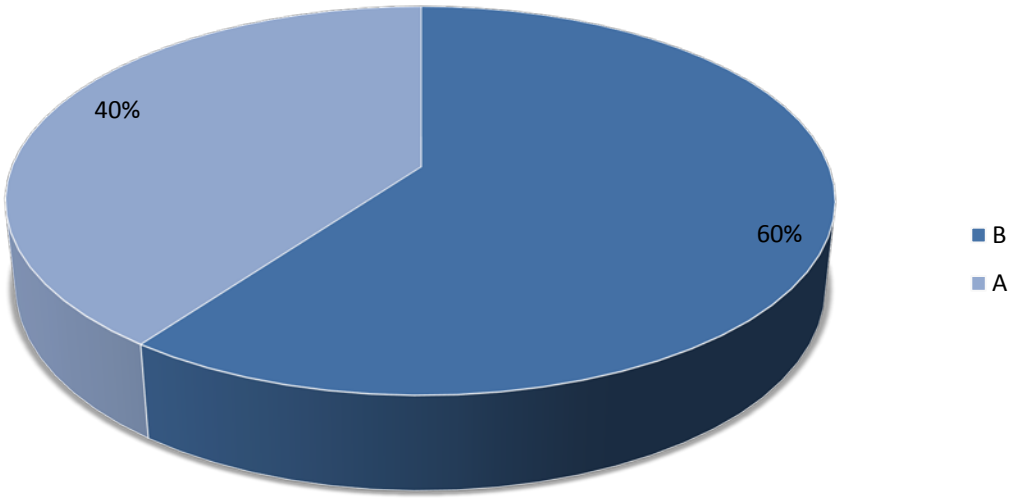


Рисунок 1.3 – Співвідношення шкідливих акаунтів (A) до нешкідливих (B)

1.3 Класифікація соціальних ботів

Соціальні боти – частина програмного забезпечення, призначена для імітації поведінки живої людини в соціальній мережі. Шкідливі програми використовуються щоб видати себе за реального користувача шляхом викрадання його персональних даних або для досягнення інших цілей, таких як просування ідеї, бренду, поширення реклами, створення інтересу до обговорення якоїсь теми великої кількості людей.

Помилковою є думка, що всі боти ідентичні і створені для однакових цілей. Прості користувачі, як правило, не намагаються визначити послідовність їх дій. Провівши аналіз поведінки бот-програм, їх можна розділити на 2 типи:

– автоматичні, що виконують прості, задані заздалегідь дії;

– керовані – боти, контрольовані оператором, який бере участь в обговореннях в напівавтоматичному режимі (ставить лайки, робить репости і т.п.).

Просунуті програми можуть в автоматичному режимі вступати в співтовариства, заповнювати профіль, навіть додавати користувачів в друзі. Вони найчастіше використовуються для поширення спаму або накрутки показників. До керованих ботів також відносяться клоновані сторінки реальних, часто відомих людей.

За типом боти також діляться на наступні категорії:

– аватари – профілі, якими користуються і реальні люди і боти. Такий вид ботів ще називають кіборгами [13]. Зазвичай мають добре налагоджені соціальні зв'язки;

– новинні боти – боти, що розміщують останні новини у себе в профілі. Потрібні в основному для поширення цих новин. Шкоди не несуть, якщо новини не є дезінформацією;

– боти, які розповсюджують повідомлення реальних користувачів. Роблять це для того, щоб бути схожими на людей. Одна з основних цілей існування – інформаційні вкидання;

– ігрові боти. Беруть участь в іграх або інших додатках соціальних мереж, спілкуються з реальними людьми від імені реальних людей. Найчастіше використовуються для накрутки згадуваності додатків;

– боти, які беруть участь в накручуванні репутації, – збільшення кількості друзів та зв’язків. Дозволяють заробляти гроші на репостах;

– акаунти, що публікують тільки перепости та чужі новини.

По сусідству з ботами розташувалися штучно створені акаунти, розвитком і веденням яких займаються реальні люди. Залежно від призначення, часу і зусиль, витрачених на ведення акаунта, сторінки віртуальних особистостей можуть бути як схожими на ботів, так і не відрізнятись від живих людей. Їх можна розділити на кілька типів:

– акаунти з бірж лайків. На профільних біржах можна купити практично все – лайки, шери, коментарі, підписи на сторінки. Незважаючи на те, що біржі гарантують, що у них працюють реальні люди, багато з них є агрегаторами міні-ботоферм;

– акаунти з шаблонним прокачуванням – за їх розвиток відповідає скрипт або реальна людина. Їх якість вище, але якщо придивитися, то пости в стрічці з'являються приблизно в один і той же час, під постами немає взаємодій або присутні самотні коментарі;

– акаунт з нешаблонним прокачуванням – бот з поведінкою, схожою на дії живої людини. Тут використовуються різні типи постів, під якими зустрічаються самотні лайки або коментарі;

– «жива людина» – акаунти, що створюються складною програмою, яка переконливо імітує дії людини в соціальній мережі. Завдяки цьому вони не викликають підозри, наприклад у «Facebook», так як невидимі для алгоритмів виявлення ботів. «Живі люди» акумулюють в друзях і підписаних користувачах активну аудиторію і регулярно взаємодіють з нею;

– боти-ломи – так звані лідери громадської думки. Вершина ланцюжка соціальних ботів. Створені вручну і старанно підтримувані акаунти. Кожен з них має своє позиціонування і свою аудиторію. У багатьох з них дійсно цікавий і унікальний контент. Таких акаунтів мало і вони використовуються для вкидань необхідної замовнику інформації, а не для її масштабування;

– люди та інші публічні майданчики. Звинувачуючи в інформаційному спамі ботів, не слід забувати про реальних людей, які не мають ніякого відношення до ботів, але працюють в соціальних мережах в чиїх інтересах. Це можуть бути експерти, журналісти, публічні персоналії чи просто люди,

чиї акаунти знайшли масову популярність. За гроші, інші форми винагороди або просто за покликом серця пишуть про те, що цікаво замовнику;

Через таке розмаїття програм-ботів основною проблемою при розробці методів їх детектування є створення алгоритму, який міг би відрізнити реальних користувачів, які своїми діями нагадують ботів, від самих ботів.

1.4 Висновки до першої частини

Соціальні мережі є невід'ємною частиною сучасного суспільства, що не мають вікових чи професійних обмежень. На базі соціальних мереж проводять різні дослідження, рекламні та маркетингові компанії. Все частіше інтернет можливості активно використовуються для формування громадської думки, що, в свою чергу, може впливати на якість життя, політичні процеси в країні та світі. Тому особливої уваги потребує питання безпеки інформації в соціальних мережах.

Одна з головних проблем – соціальні боти або шкідливі акаунти. Вони можуть грати позитивну роль (наприклад, новинні боти), але частіше за все є інструментом для зниження довіри в соціальних мережах, масового розкрадання даних, організації інформаційних вкидань і таке інше.

Постійно зростаючі загрози використання шкідливих акаунтів роблять завдання їх ефективного детектування особливо актуальним та пов’язаним з кібербезпекою.

РОЗДІЛ 2. АНАЛІЗ МЕТОДІВ ДЕТЕКТУВАННЯ ШКІДЛИВИХ АККАУНТІВ

2.1 Візуальне представлення соціальних мереж

Значимість соціальних мереж обумовлена тим, що, з одного боку вони є предметом соціалізації людей, а з іншого – найбільш потужним і доступним політичним, ідеологічним та економічним інструментом [5]. Дослідженню соціальних мереж як систем, що містять дані надвеликого обсягу, присвячений ряд робіт в цій області [2, 3]. Величезні обсяги даних, а також залежності (зв'язки) між ними необхідно представити у вигляді, зручному для сприйняття. Дані соціальних мереж можуть бути представлені в різних видах: хмара тегів, діаграми, історичні потоки [4], однак найчастіше для цієї мети використовують графи.

В основному, коли мова йде про об'єкти, що представляють собою мережу, наприклад, соціальну, поняття візуалізації даних тісно пов'язане з поняттям графів. Важливим завданням є представлення зв'язку в соціальних мережах для виявлення різного роду залежності.

Граф являє собою сукупність непорожньої множини вершин і множини ребер: $G(X,U)$ (X – множина вершин, U – множина ребер). Вершинами в графі, що описує соціальну мережу, є акаунти користувачів, а ребрами – зв'язки між ними, наприклад, підписка в мережах twitter і ставлення типу «дружба» в соціальній мережі Facebook (рисунок 2.1).

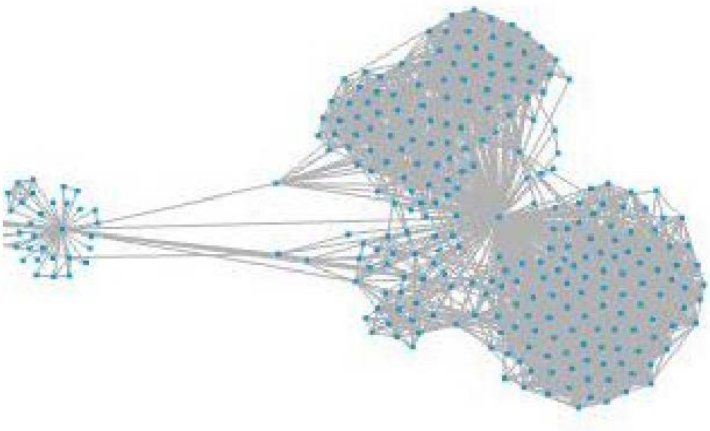


Рисунок 2.1 – Фрагмент графа соціальної мережі «ВКонтакте»

Однією з важливих пов'язаних характеристик, яку слід розглянути, є метрика. Метрика графа заснована на понятті відстані.

Відстанню $d(x_i, x_j) = d_{ij}$ між вершинами x_i і x_j графа $G(X, U)$ називається довжина найкоротшого ланцюга, що з'єднує ці вершини. Під довжиною ланцюга розуміється число ребер, що входять до неї.

Тоді функція $d(x_i, x_j)$, певна на множині ребер U графа G, називається метрикою графа.

Ступенем вершини $x_i \in X$ графа є кількість ребер, які інцидентні даній вершині – $d(x_i)$.

Дослідним шляхом доведено, що статечне розподілення різних сегментів переважної більшості користувачів в соціальних мережах має такий вигляд (рис. 2.2).

f_k – це частка вершин графа $G(X, U)$, що мають ступінь $d(x_i) = k$.

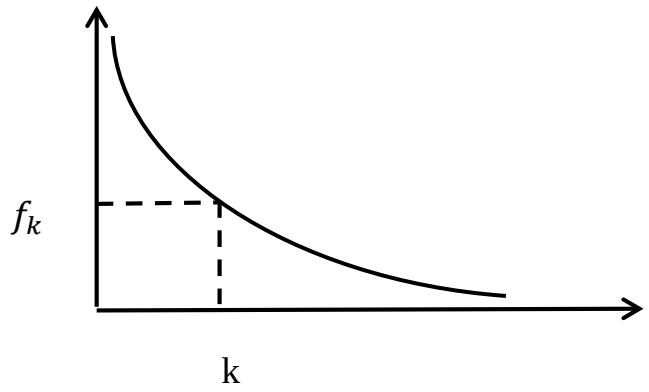


Рисунок 2.2 – Розподіл ступеня вершин графа

Для моделювання даного розподілу як правило підходять функції виду [5]:

$$p(k) = Ck^{-\alpha} \tag{2.1}$$

де α – коефіцієнт находження сегмента мережі;

C – коефіцієнт;

k – ступінь розподілу;

$p(k)$ – функція розподілу.

2.2 Методи і засоби збору та класифікації даних

Оскільки сценарії використання інтерфейсів соціальних мереж не передбачають автоматичного збору даних безлічі користувачів з метою побудови соціального графа, то виникає ряд проблем:

– приватність даних – часто доступ до даних користувачів дозволений тільки для зареєстрованих і авторизованих учасників мережі, що вимагає підтримки емуляції користувальницької сесії за допомогою спеціальних облікових записів (акаунтів);

– слабка структурованість даних – у багатьох випадках програмні інтерфейси (API) соціальних мереж мають обмежений функціонал, що вимагає підтримки отримання за допомогою призначеного для користувача веб-інтерфейсу статичних копій HTML-сторінок, коректної обробки їх динамічної частини (включаючи виконання асинхронних запитів до сервера соціальної мережі), вилучення потрібних даних за допомогою алгоритму і / або шаблону і побудови їх структурованого уявлення, зручного для подальшої автоматичної обробки;

– обмеження доступу і блокування – з метою запобігання несанкціонованому автоматичного збору даних і обмеження навантаження на інфраструктуру сервісу соціальної мережі власники сервісів часто вводять явні чи приховані обмеження на допустиму кількість запитів від одного користувача акаунта і / або IP-адреси в одиницю часу, що вимагає врахування кількості запитів, що посилаються, а також підтримки динамічної ротації використовуваних для збору даних акаунтів користувача і IP-адрес;

– розмірність даних обумовлює необхідність в паралельному методі збору даних, а також в методах отримання репрезентативної вибірки користувачів соціальної мережі (семплірування).

У зв'язку з постійною необхідністю отримання великих наборів даних з соціальних мереж, розроблений фреймворк для збору даних з різних інтернет-сервісів. Інструмент підтримує скачування даних з соціальних мереж Facebook, Twitter, Hunch. Реалізовано кілька способів отримання репрезентативних вибірок користувачів соціальних мереж: семплірування методом обходу в ширину (breadth-first search, BFS) [1], по МетрополісуГастінгсу (Metropolis-Hastings Random Walk, MHRW) [3] та методом «лісової пожежі» (Forest Fire , FF) [2]. Реалізовано механізм автоматичного вибору облікового запису соціальної мережі для кожного запиту, а також підтримки проксі-з'єднань. Це забезпечує стійкість до блокування по IP-адресам і обліковим записам. Крім того, фреймворк підтримує багатопотокове скачування. Однією з ключових особливостей розробленого фреймворка є можливість швидко реалізувати нові сценарії скачування і методи семплінгу. Для оцінки продуктивності фреймворка були проведені експерименти, в яких скачували профілі користувачів соціальних мереж Twitter, Facebook і Hunch. В результаті досягнуті наступні показники:

- Facebook: більше 500 профілів на годину (один потік);
- Twitter: більше 3000 профілів на годину (один потік);
- Hunch: понад 100 профілів на годину (один потік).

2.3 Методи розпізнавання образів для класифікації

В основі вирішення задачі дипломної роботи – розробки алгоритму детектування шкідливих акаунтів лежить принцип розпізнавання образів. Це науковий напрямок, пов'язаний з розробкою принципів та побудовою систем, призначених для визначення приналежності об'єкта до одного з класів об'єктів. Під об'єктами в розпізнаванні образів розуміють різні предмети і явища, процеси і ситуації, сигнали і т. п. [2].

Системи розпізнавання мають наступну типову функціональну схему: вхідні дані, що підлягають розпізнаванню, подаються на вхід системи і піддаються попередній обробці з метою їх перетворення в необхідний для наступного етапу вид або для виділення з них необхідних характерних ознак. Далі на етапі прийняття рішення над опрацьованим масивом даних проводиться ряд обчислень і на основі їх результатів формується відповідь, що містить очікувані від системи відомості про вхідні данні. Зміст вхідних і вихідних даних визначається призначенням системи [3].

Системи розпізнавання мають наступну типову функціональну схему, представлену на рисунку 2.3.

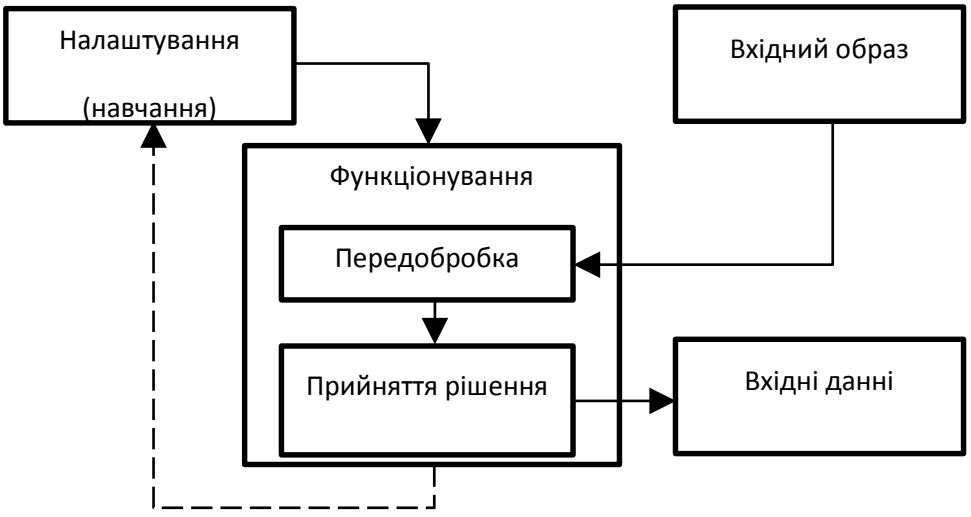


Рисунок 2.3 – Система розпізнавання образів

Класифікація ґрунтується на прецедентах. Прецедент це образ, правильна класифікація якого відома, – раніше класифікований об'єкт, який приймається як зразок при вирішенні задач класифікації. Ідея прийняття рішень на основі прецедентного – основоположна в природно-науковому світогляді.

Будемо вважати, що всі об'єкти або явища розбиті на кінцеве число класів. Для кожного класу відомо і вивчено кінцеве число об'єктів – прецедентів. Завдання розпізнавання образів полягає в тому, щоб віднести новий об'єкт, що розпізнається, до якого-небудь класу.

Системи розпізнавання передбачають і свою настройку на безліч можливих вхідних даних: цей етап називають етапом навчання системи. Метою навчання системи є формування в її пам'яті набору відомостей, необхідних для розпізнавання передбачуваного класу вхідних даних. Залежно від специфіки розв'язуваної задачі навчання може бути виражено процедурою одноразового ручного завдання параметрів роботи системи її розробником, автоматичною процедурою визначення оптимальних значень параметрів в результаті проведення навчальних циклів розпізнавання або процесом безперервного підстроювання параметрів в результаті аналізу відповідей, що виробляються системою. Як правило, має місце комбінація названих підходів.

Виходячи з наявності або відсутності прецедентної інформації, розрізняють завдання розпізнавання з навчанням і без навчання. Завдання розпізнавання на основі наявної множини прецедентів називається класифікацією з навчанням (або з учителем).

У тому випадку, якщо є безліч векторів ознак, отриманих для деякого набору образів, але правильна класифікація цих образів невідома, виникає задача поділу цих образів на класи за подібністю відповідних векторів ознак. Ця задача називається кластеризацией або розпізнаванням без навчання.

2.3.1 Кластеризация

Кластеризація – це об'єднання об'єктів або спостережень в непересічні групи, які називаються кластерами, на основі близькості значень їх атрибутів (ознак). В результаті в кожному кластері будуть знаходитися об'єкти, схожі за своїми властивостями один на одного і відрізняються від тих, які розташовані в інших кластерах. При цьому, чим більше подібність об'єктів всередині кластера і чим сильніше їх несхожість на об'єкти в інших кластерах, тим краще кластеризація.

Формальна постановка задачі кластеризації виглядає наступним чином.

Нехай задані множини об'єктів $X = (x_1, x_2, \dots, x_n)$ та номерів (імен, міток) кластерів $Y = (y_1, y_2, \dots, y_k)$. Для X визначена деяка функція відстані між об'єктами $D(x, x')$, наприклад, метрика *L2*. Крім цього, є кінцева вибірка навчальних прикладів $X_m = (x_1, x_2, \dots, x_m)$ з множини X, яку потрібно розбити на X_m непересічні підмножини (кластери) так, щоб кожна з них складалася б лише з елементів, близьких за метрикою D. При цьому кожному об'єкту x_i з множини X_m присвоюється номер кластера y_j.

Тоді завдання полягатиме в пошуку функції f, яка будь-якому об'єкту x з множини X ставить у відповідність номер кластера y з множини Y, яка сама по собі буває відома заздалегідь. Однак в більшості випадків доводиться визначати оптимальне число кластерів виходячи з особливостей розв'язуваної задачі.

2.3.2 Класифікація

Завдання розбиття множини об'єктів або спостережень на апріорно задані групи, звані класами, всередині кожної з яких вони передбачаються схожими один на одного, мають приблизно однакові властивості і ознаки. При цьому рішення виходить на основі аналізу значень атрибутів (ознак). Якщо число класів обмежено двома, то має місце бінарна класифікація, до якої можуть бути зведені багато складних завдань.

Для класифікації використовується безліч різних моделей: нейронні мережі, дерева рішень, машини опорних векторів, метод k-найближчих сусідів, алгоритми покриття та ін., при побудові яких застосовується навчання з учителем, коли вихідна змінна (мітка класу) задана для кожного спостереження. Формально класифікація проводиться на основі розбиття простору ознак на області, в межах кожної з яких багатовимірні вектори розглядаються як ідентичні. Іншими словами, якщо об'єкт потрапив в область простору, асоційовану з певним класом, він до нього і відноситься [9].
Класифікувати об'єкт – значить вказати номер (або найменування) класу, до якого належить даний об'єкт.

2.4 Існуючі методи виявлення шкідливих акаунтів

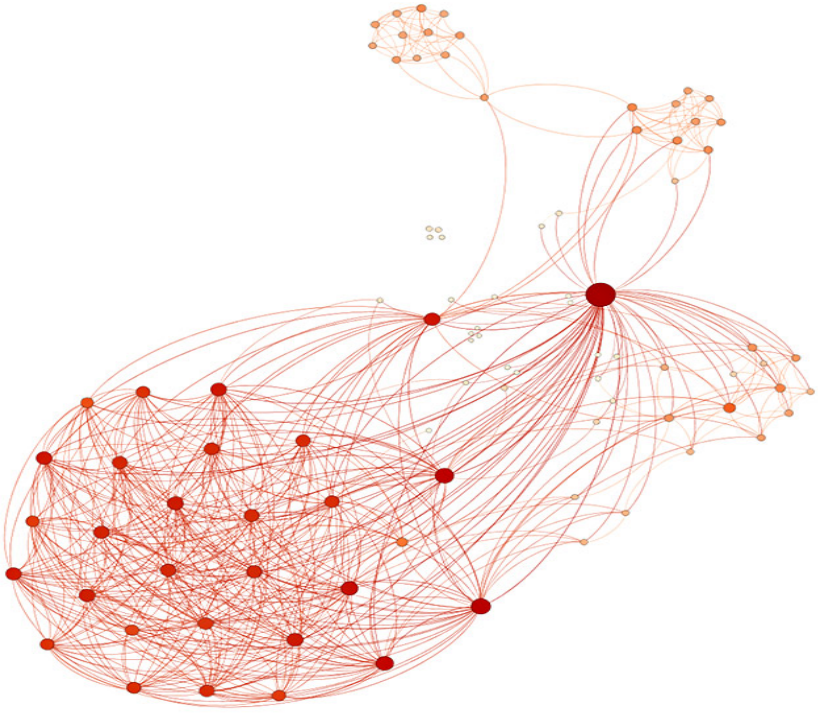
Самі соціальні мережі не надають активного опору шкідливим акаунтам. В основному всі дії по захисту від ботів є профілактикою:

– Captcha – повністю автоматизований публічний тест Тьюринга, комп'ютерний тест, який використовується для того, щоб визначити, ким є користувач системи: людиною або комп'ютером;

– SMS-verification – перевірка справжності користувача за допомогою відправки йому на номер смс з кодом підтвердження, який він повинен потім ввести в потрібне поле при реєстрації або вході в систему;

– Ratelimit (обмеження пропускної здатності) – обмеження числа запитів до системи за певний час.

В роботі [6] і [14] на прикладі популярної соціальної мережі досліджується проблема виявлення спам-ботів. Розрізняти звичайних користувачів від шкідливих програм пропонується за допомогою класифікації методом машинного навчання. Для цього використовуються традиційні алгоритми класифікації: дерева рішень, нейронні мережі, машина опорних векторів, наївний байєсовський класифікатор. В якості ознак були взяті кількість користувачів, що підписались та читаються, а також граф-орієнтовані взаємозв'язки користувачів (рис 2.4). Дані класифікатори натреновані і протестовані на великому наборі даних (25000 акаунтів) і



виявлено найбільш продуктивний алгоритм.

Рисунок 2.4 - Граф взаємозв'язків користувачів в соціальній мережі Facebook

Для оцінки продуктивності спочатку складена матриця (рис 2.5), потім обчислювані значення показників precision (точність) $P = a/(a + c)$, $recall\ R = a/(a + b)$, $F\text{-}measure\ \ F = a/(a + c)$. В результаті отримана зведена таблиця (рис 2.6), по якій визначено, що байєсовський наївний алгоритм найбільш точно класифікував спам-ботів (найбільше значення F).

Таблиця 2.5 – Таблиця контингентні

		Prediction	
		Spam	Not Spam
True	Spam	a	d
	Not Spam	c	b

Таблиця 2.6 – Метрики ефективності

Classifier	Precision	Recall	F-measure
Decision Tree	0.667	0.333	0.444
Neural Networks	1	0.417	0.588
Support Vector Machines	1	0.25	0.4
Naïve Bayesian	0.917	0.917	0.917

Робота [7] описує проектування фреймворка (системи) [19] для виявлення ботів в соціальній мережі. У ній розглянуто загальний підхід для всіх соціальних мереж, який полягає в наступному:

– збір даних. Перша проблема, яка постає при вирішенні задачі виявлення ботів – це збір інформації про користувачів;

– виявлення ознак (або метрик), на основі яких буде працювати алгоритм класифікації;

– вибірка вже класифікованих даних для навчання класифікатора. Тобто необхідна вибірка профілів-ботів і вибірка профілів – не ботів. На цих даних буде навчатися класифікатор. Чим більше вибірка, тим точніше буде працювати надалі класифікатор;

– навчання класифікатора на даній вибірці.

В роботі розглядалися три алгоритму класифікації: наївний байесовский алгоритм, дерево рішень і машина опорних векторів.

Робота фреймворка полягає в наступному:

1) вибирається алгоритм класифікації і подаються на вхід метрики з навчальної вибірки;

2) запускається алгоритм на тестовій вибірці для перевірки. На виході виходить розподіл вибірки на два класи. Якщо якісь об'єкти були класифіковані неправильно, повідомляється про це алгоритму;

3) повторюються пункти 2 і 3 до тих пір, поки точність роботи алгоритму буде не нижче заданої планки (напр. 97% чітко визначених профілів) (рис 2.7).

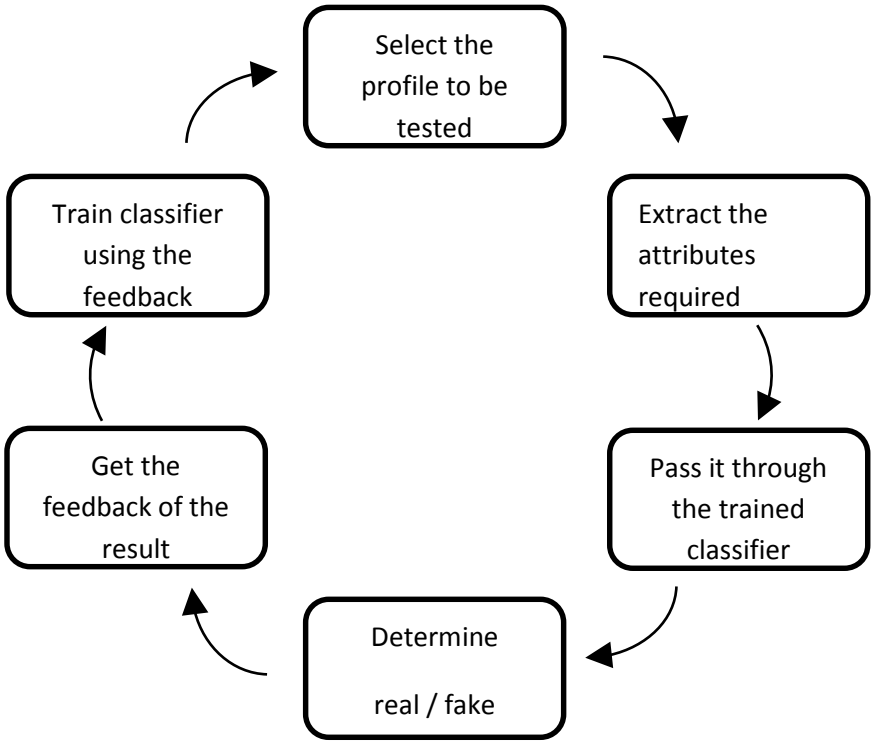
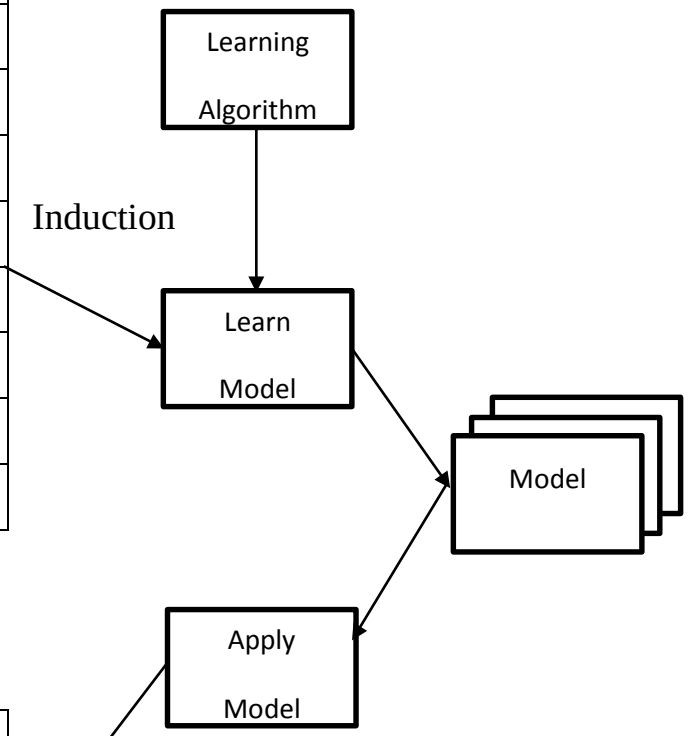


Рисунок 2.7 – Схема функціювання системи

Класифікація – знаходження такої цільової функції f, яка є набором ознак з визначенним класом. Модель роботи класифікатора представлена на рисунку 2.8.

Training Set				
Tid	Attrib1	Attrib1	Attrib1	Class
1	Yes	Large	125K	No
2	No	Medium	100K	No
3	No	Small	70K	No
4	Yes	Medium	120K	No
5	No	Large	95K	Yes
6	No	Medium	60K	No
7	Yes	Large	220K	No
8	No	Small	85K	Yes
9	No	Medium	75K	No
10	No	Small	90K	Yes



Test Set				
Tid	Attrib1	Attrib1	Attrib1	Class
11	No	Small	55K	?
12	Yes	Medium	80K	?
13	Yes	Large	110K	?
14	No	Small	95K	?
15	No	Large	67K	?

Deduction

Рисунок 2.8 – Схема роботи класифікатора

В роботі [13] розглядається проблема розрізнення ботів і звичайних людей – класифікація акаунтів в Twitter на людину, бота та кіборга. Кіборг визначається як середнє між ботом і людиною. Була зібрана база з 500 000 акаунтів соціальної мережі Twitter. Різниця визначається за такими ознаками: поведінка, зміст твітів і характеристик профілю. На основі результатів досліджень запропонована система класифікації, що складається з 4 частин:

– компонент ентропії (entropycomponent) – аналізує інтервал між твітами (повідомленнями) акаунта для визначення його поведінки;

– компонент виявлення спаму (spamdetectioncomponent) – аналізує вміст твіттів по заздалегідь заготовленим шаблонами для визначення приналежності даного контенту до спам контенту;

– компонент аналізу профілю (accountpropertiescomponent) – аналізує ознаки, що відносяться до профілю;

– компонент класифікації (decisionmarkercomponent) – використовує результати роботи трьох попередніх компонентів для класифікації облікового запису за допомогою одного з алгоритмів класифікації.

Компоненти аналізу профілю.

При аналізі профілю автором використовується 8 характеристик акаунта. Розглянемо кожну з них.

Таблиця 2.3 – Характеристики акаунтів 1

Top 10 Tweeting Devices				
Rank	Human	Bot	Cyborg	All
1	Web (50,53%)	API (42,39%)	Twitterfeed (31,29%)	Web (46,78%)
2	TweetDeck (9,19%)	Twitterfeed (26,11%)	Web (23,00%)	TweetDeck (9,26%)
3	Tweetie (6,23%)	twitRobot (13,11%)	API (6,94%)	Twitterfeed (7,83%)
4	UberTwitter	RSS2Twitter	Assetize (5,74%)	API (6,23%)

	(3,64%)	(2,66%)		
5	Mobile web (3,02%)	Twitter Tools (1,24%)	HootSuite (5,22%)	Echofon (2,80%)
6	Txt (2,56%)	Assetize (1,17%)	WP to Twitter (2,40%)	Tweetie (2,50%)

Продовження таблиці 2.3

7	Echofon (2,22%)	Proxifeed (1,08%)	TweetDeck (1,54%)	Txt (2,13%)
8	TwitterBerry (2,10%)	TweetDeck (0,99%)	UberTwitter (1,19%)	HootSuite (2,10%)
9	Twitterrific (1,96%)	bit.ly (0,91%)	RSS2Twitter (1,18%)	UberTwitter (1,71%)
10	Seesmic (1.64%)	Twitme for WordPress (0,84%)	Twaitter (0,86%)	Mobile web (1,53%)

– кількість нескорочених твітів – боти використовують більше нескорочених посилань в своїх твітах;

– з якого пристрою створюються твіти. В таблиці 2.1 наведено 10 найпопулярніших засобів, з яких можуть створюватися повідомлення і яка категорія найбільш часто використовується людьми та ботами. Як видно з таблиці, люди найчастіше використовують вебсайт, а боти API;

– метрика, яка називається репутацією акаунта. Тобто співвідношення читачів і тих, кого читають. Люди мають або однакову кількість читачів і тих, кого читають, або читачів більше, ніж тих, кого читають. Боти ж навпаки, мають більшу кількість читаних, ніж читачів;

– чи містяться в твітах даного користувача посилання на ресурси з чорних списків. Є сервіси, які можуть детектувати підозрілі сайти. Наприклад, GoogleSafeBrowsing, PhishingTank, URIBL, SURBL, Spamhaus.

Дані сервіси надають API для використання їх можливостей в своїх програмах;

– наявність верифікації від Twitter. Це стосується, в основному, акаунтів відомих людей;

– відношення кількості хештегів до загальної кількості твітів;

– кількість репоста з даного облікового запису.

Також в роботі використовуються наступні характеристики акаунту:

– число читачів та що читаються;

– освіта, робота;

– стать;

– число символів в «Про себе»;

– сімейний статус;

– число фотографій, на яких відзначений користувач;

– число постів у аккаунта;

– число завантажених фото.

В роботі розглянуто фреймворк, що складається з 4 модулів. Кожен модуль аналізує свою групу характеристик. Найбільш вагомий внесок у результат детектування показаний в таблиці 2.3.

Таблиця 2.3 – Характеристики акаунтів 2

Feature Weights	
Feature	Accuracy (%)
Entropy	82,8
URL Ratio	74,9
Automated Device %	71,0
Bayesian Spam Detection	69,5
Manual Device %	69,2
Registration Date	62,9
Mention Ratio	56,2
Link Safety	49,3

Hashtag Ratio	47,0
Followers to Friends Ratio	45,3
Account Verification	35,0

Автори статті [18] досліджують вплив ботів на політичні кампанії в інтернеті. Розробляється метод з використанням технології машинного навчання, який враховує особливості контенту, краудсорсінг і топологію мереж для детектування спам-ботів на ранніх стадіях розвитку політичної кампанії.

Нову методику виявлення шкідливих акаунтів висунули автори статті [15]. Вона полягає в побудові та аналізі маштабограм (scalogram) [16], що відображають взаємодію користувачів в соціальній мережі. Масштабограми виявляють багато прихованої інформації про природу нестаціонарних процесів. Вони застосовуються в різних областях: прогнозування наслідків під час землетрусу, аналізу руху землі, аналіз стійкості будівель до ураганів і бурь, аналіз стійкості мостів і т.п. Приклад масштабограми представлений на рисунку 2.9. Вона відображає кількість постів і активність користувачів в соціальній мережі протягом 20 днів.

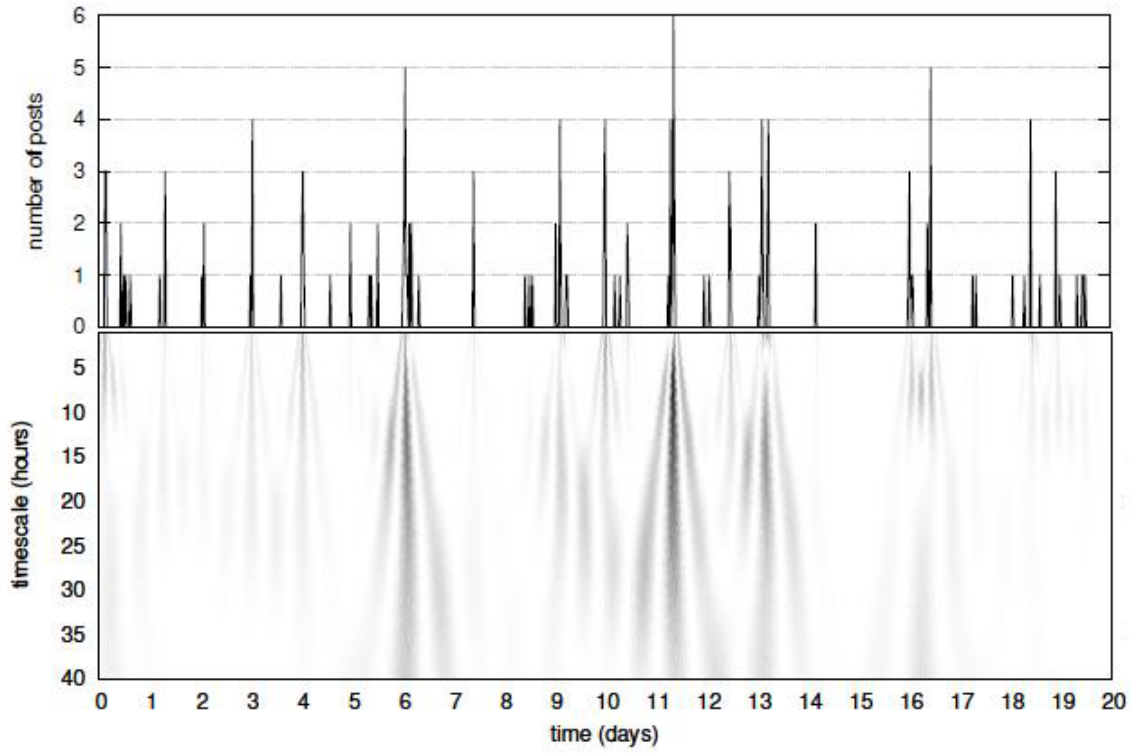


Рисунок 2.9 – Приклад масштабограми

Відрізняється від попередніх алгоритм приманки (Honeypot) [12]. Технологія Honeypot – ресурс безпеки, призначення якого полягає в тому, щоб стати дослідженим або зазнали нападу. Це означає, що незалежно від того, яку структуру має засіб Honeypot, мета полягає в тому, щоб даний ресурс був досліджений, атакований і використаний зловмисником. Не має значення, чим є ресурс: імітованим сервісом або повноцінною операційною системою. Головне, що сенс функціонування ресурсу полягає в нападі на нього.

У мережі інтернет знайдена інформація лише про теорію використання цього алгоритму разом з технологією машинного навчання. Технологія Honeypot має один суттєвий недолік – обмежена область видимості. Вона може бути використана як мала частина комплексного алгоритму, що включає в себе кілька алгоритмів детектування.

2.5 Математичний апарат

Для вирішення задачі детектування ботів повинен бути використаний відповідний математичний апарат. Джерела, які були проаналізовані, пропонують: наївний алгоритм Байєса, дерева рішень, випадковий ліс Randomforest.

2.5.1 Наївний алгоритм Байєса

Наївний байєсовський класифікатор заснований на теоремі Байєса [20]. Теорема Байєса – одна з основних теорем теорії ймовірностей, яка дозволяє визначити ймовірність якої-небудь події за умови, що сталося інша, взаємозалежна з ним подія. Теорема Байєса виражається наступною формулою:

$$P(A|B) = \frac{P(B|A)*P(A)}{P(B)} \quad (2.1)$$

де $P(A|B)$ – ймовірність гіпотези А при настанні події В,

$P(B|A)$ – ймовірність настання події В при вірності гіпотези А,

$P(A)$ – апріорна (безумовна) ймовірність події А,

$P(B)$ – ймовірність настання події В.

У наївному байєсовському класифікаторі висувається гіпотеза (А – користувач є ботом), після чого рахується ймовірність істинності цієї гіпотези.

Алгоритм називається наївним, тому що заснований на теоремі Байеса із суворим (наївним) припущенням про незалежність від атрибутів.

Наприклад, є об'єкт Sk зі значеннями атрибутів $(A_1 = v_2,\ A_2 = v_2, \dots A_m = v_m)$з максимальною вірогідністю $Prob\big(C_i\big|(v_1, v_2, \dots v_m)\big)$. Тоді ймовірність приналежності до класуC_i або C_j обчислюється таким чином:

Імовірність приналежності Sk до класу C_i:

$$Prob\big(C_i\big|(v_1, v_2, \dots, v_m)\big) = \frac{P((v_1,v_2,\dots,v_m)|C_i)P(C_i)}{P((v_1,v_2,\dots,v_m))}$$

(2.2)

Імовірність приналежності Sk до класу C_j:

$$Prob\left(C_j\middle|(v_1, v_2, \dots, v_m)\right) = \frac{P((v_1,v_2,\dots,v_m)|C_j)P(C_j)}{P((v_1,v_2,\dots,v_m))} \qquad (2.3)$$

Таким чином, щоб порахувати вірогідність $Prob\big(C_i\big|(v_1, v_2, \dots, v_m)\big)$ і $Prob\left(C_j\middle|(v_1, v_2, \dots, v_m)\right)$необхідно обчислити значення виразів $P((v_1, v_2, \dots, v_m)|C_i)P(C_i)$ і $P((v_1, v_2, \dots, v_m)|C_j)P(C_j)$.

З огляду на припущення про незалежність атрибутів:

$$P\left((v_1, v_2, \dots, v_m)\middle|C_j\right) = P\big(A_1 = v_1\big|C_j\big) * P\big(A_2 = v_2\big|C_j\big) \dots P\big(A_m = v_m\big|C_j\big) =$$

$\prod_{h=1}^{m} P(A_h = v_h|C_j)$

(2.4)

$$P(C_i) = \frac{no.of\ training\ samples\ belonging\ to\ C_j}{total\ no.of\ training\ samples} \quad (2.5)$$

2.5.2 Дерева рішень

Дерево прийняття рішень (також можуть називатися деревами класифікації або регресійними деревами) – використовується в області статистики та аналізу даних для прогнозних моделей.

Структура дерева являє собою наступне:

- нелістовая вершина - одна з ознак;
- ребро - значення ознаки;
- листова вершина – значення цільової функції (клас).

Структура дерева являє собою «листя» і «гілки» (рис 2.10). На ребрах («гілках») дерева рішення записані атрибути, від яких залежить цільова функція, в «листі» записані значення цільової функції, а в інших вузлах – атрибути, за якими розрізняються випадки. Щоб класифікувати новий випадок, треба спуститися по дереву до листа і видати відповідне значення. Подібні дерева рішень широко використовуються в інтелектуальному аналізі даних. Мета полягає в тому, щоб створити модель, яка передбачає значення цільової змінної на основі декількох змінних на вході [30].

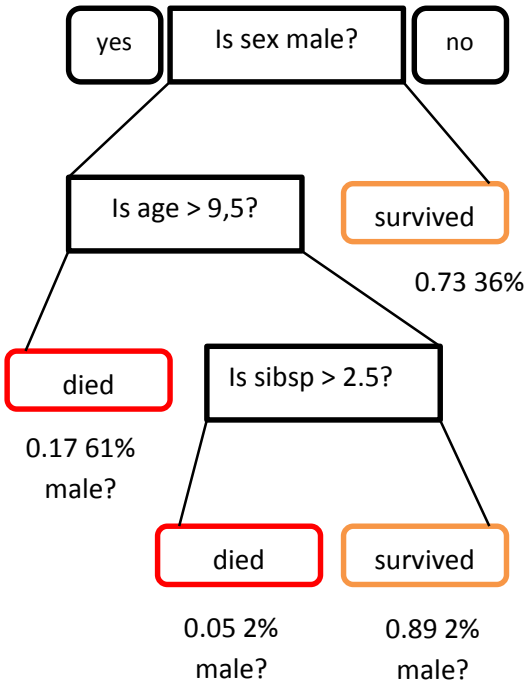


Рисунок 2.10 – Приклад схеми дерева рішень

Загальна схема побудови дерева рішень:

1) вибрати чергову ознаку P, помістити її в поточну вершину;

2) для кожного значення вибраної ознаки v:

– з тестових даних залишити тільки ті, у яких P = v;

– рекурсивно побудувати дерево обраних ознак, розглядаючи ознаки, що залишилися.

3) зупинитися, якщо всі тестові об'єкти належать одному класу, якщо закінчилися ознаки або по іншим заданим критеріям.

2.5.3 Випадковий ліс Randomforest

Алгоритм машинного навчання, що полягає у використанні комітету (ансамблю) вирішальних дерев. Особливості алгоритму випадковий ліс:

– використання комітету дерев;

– обробка даних з великою розмірністю;

– вбудована оцінка якості передбачення;

– високий ступінь розпаралелювання і масштабованості.

Випадковий ліс – ансамбль B дерев: $\{T_1(X), T_2(X), \dots, T_b(X)\}$, X – вектор розмірності p.

Ансамбль повертає B пророкувань: $\{Y_1 = T_1(X), \ldots, Y_b = T_b(X)\}$, Y_b– повертається клас. З Y_b обирається самий часто використовуваний клас.

2.6 Висновки до другого розділу

Аналіз існуючих методів детектування шкідливих акаунтів показав, що більшість з них засновано на класифікації. Кожен з методів в якійсь мірі вирішує завдання поділу даних на групи з однаковими ознаками. Але поряд з цим вони мають і деякі недоліки, такі як:

– робота з обмеженим обсягом даних;

– використовуються для вирішення певної задачі;

– для деяких методів потрібен великий обсяг експериментальних початкових даних;

– характерні істотні похибки;

– вимагають складних математичних розрахунків і т.п.

Тому існує необхідність розробки альтернативного методу детектування шкідливих акаунтів, який буде більш адаптивним і універсальним.

Для вирішення завдань, поставлених у дипломній роботі необхідно:

1) грунтуючись на проведених дослідженнях та аналізі, розробити вдосконалений алгоритм детектування шкідливих акаунтів з урахуванням переваг і недоліків розглянутих методів;

2) вибрати інструменти для ефективної реалізації алгоритму;

3) розробити і протестувати алгоритм детектування ботів на прикладі конкретних соціальних мереж.

РОЗДІЛ 3. РОЗРОБКА АЛГОРИТМУ ДЕТЕКТУВАННЯ БОТІВ В СОЦІАЛЬНИХ МЕРЕЖАХ

3.1 Структура алгоритму детектування

На підставі аналізу алгоритмів детектування шкідливих акаунтів, які застосовуються в сучасних соціальних мережах, в даній роботі прийнято рішення використовувати методи теорії розпізнавання образів.

В роботі прийняті наступні терміни:

– клас – безліч об'єктів, що мають спільні властивості. Класів може бути необмежена кількість;

– класифікація – процес призначення міток класу об'єктам, відповідно до деякого опису властивостей цих об'єктів;

– класифікатор – пристрій, який в якості вхідних даних отримує набір ознак об'єкта, а в якості результату видає мітку класу;

– верифікація – процес зіставлення примірника об'єкта з однією моделлю об'єкта або описом класу;

– ознака – кількісний опис тієї чи іншої властивості досліджуваного предмета або явища;

– простір ознак – це N-мірний простір, певний для даної задачі розпізнавання, де N – фіксоване число вимірюваних ознак для будь-яких об'єктів. Вектор з простору ознак x, відповідний об'єкту завдання поширення це N-мірний вектор з компонентами $(x_1, x_2, \dots, x_n)$, які є значеннями ознак для даного об'єкта.

Таким чином, вся задача розпізнавання зводиться до виділення істотних ознак для кожного класу і, в кінцевому рахунку, віднесення вхідних даних до одного з них за допомогою виявлення ключових ознак. Тобто розпізнавання образів можна розділити на наступні завдання (рис 3.1):

– отримання вхідних даних. Завдання генерації ознак – вибір ознак, які з достатньою повнотою описують образ;

– первинна обробка, така як відбір найбільш інформативних ознак для класифікації, нормалізація даних;

– формування векторів ознак за допомогою вибору найбільш значущих ознак, за допомогою яких можна виділити непересічні множини класів;

– класифікація чи припущення на основі отриманих даних про клас;

– завдання якісної оцінки системи (вибрані ознаки + класифікатор) з точки зору правильності або помилковості класифікації.

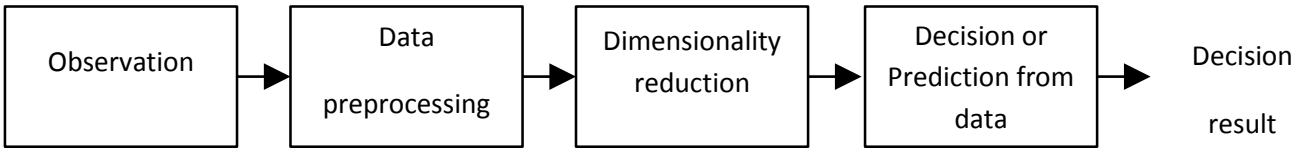


Рисунок 3.1 - Етапи розпізнавання образів

Залежно від наявності або відсутності прецедентної інформації розрізняють завдання розпізнавання з навчанням і без навчання. Завдання розпізнавання на основі наявної множини прецедентів називається класифікацією з навчанням (або з учителем). У тому випадку, якщо є безліч векторів ознак, отриманих для деякого набору образів, але правильна класифікація цих образів невідома, виникає задача поділу цих образів на класи за подібністю відповідних векторів ознак. Це завдання називається кластеризацією або розпізнаванням без навчання.

Системи розпізнавання передбачають свою настройку на безліч можливих вхідних даних; цей етап називають етапом навчання системи. Метою навчання системи є формування в її пам'яті набору відомостей, необхідних для розпізнавання передбачуваного класу вхідних даних. Залежно від специфіки розв'язуваної задачі навчання може бути виражено процедурою одноразового ручного завдання параметрів роботи системи її розробником, автоматичною процедурою визначення оптимальних значень параметрів в результаті проведення навчальних циклів розпізнавання цим процесом безперервного підстроювання параметрів в результаті аналізу

відповідей, що виробляються системою. Як правило, має місце комбінація названих підходів.

3.2 Обґрунтування вибору ознак, що характеризують об'єкти

За основу для розробки алгоритму, зокрема збору необхідної інформації про користувачів, використані дані мереж «Facebook» і «Вконтакте».

Загальний вигляд запропонованого алгоритму представлений на рисунку 3.2

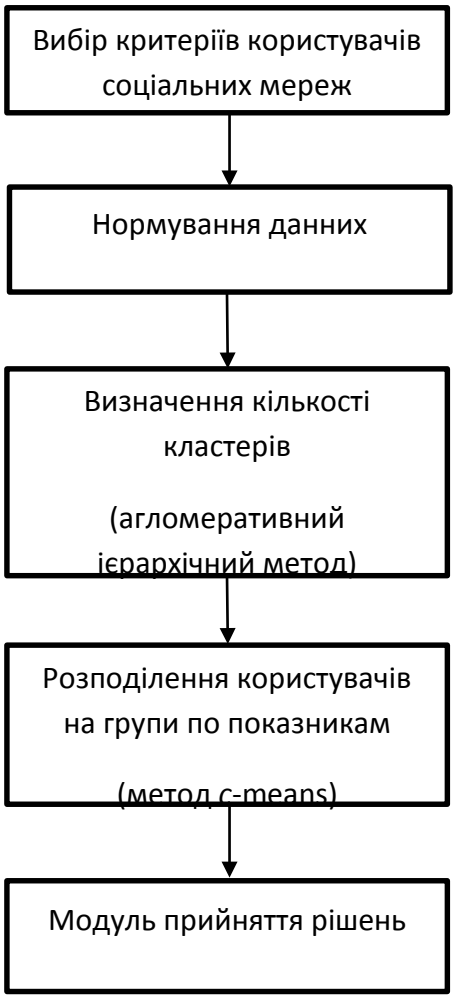


Рисунок 3.2 – Загальний алгоритм детектування шкідливих акаунтів

Вибір ознак користувачів зроблений за наступними критеріями:

– відкритість вихідних даних. Максимальна кількість інформації про користувачів соціальних мереж (вміст профілю, інформація про підписаних

користувачив , активності користувача і т.п.) знаходиться у відкритому доступі. Це дозволяє без особливих проблем зібрати вихідні дані для створення моделі соціальної мережі, їх класифікації та аналізу;

– кількість користувачів. Обробка соціальних даних вимагає також розробки відповідних алгоритмічних і інфраструктурних рішень, що дозволяють враховувати їх розмірність. Наприклад, база даних соціальної мережі Facebook на сьогоднішній день містить більше 1 мільярда користувальницьких акаунтів і більше 100 мільярдів зв'язків між ними. Кожен день користувачі додають більше 200 мільйонів фотографій і залишають більше 2 мільярдів коментарів до різних об'єктів мережі. На сьогоднішній день більшість існуючих алгоритмів, що дозволяють ефективно вирішувати актуальні завдання, не здатні обробляти дані подібної розмірності за прийнятний час;

– спосіб реєстрації. Деякі соціальні мережі, особливо корпоративні, дозволяють вводити користувачам обмежений обсяг інформації в процесі реєстрації. При цьому наявність адміністратора в таких мережах практично виключає втручання ботів ззовні. У великих популярних соціальних мережах відсутній такий контроль, що дозволяє використовувати їх для дослідження та перевірки ефективності розробленого алгоритму.

Данні про українські мережі розміщені в додатку Б.

Однією з основних проблем при детектуванні соціальних ботів є визначення, чи є користувач ботом, що зробити однозначно неможливо. Виходячи з цього, доводиться оперувати поняттями нечіткої логіки. Проектована система оцінки близька, по суті, до скорингової системи, прийняття рішень в якій здійснюється за сукупністю деяких, заздалегідь визначених, ознак, а не по одному показнику. Реалізувати саму систему необхідно тільки після визначення переліку показників, нормування, оцінки їх вагомості в сумарній оцінці критеріїв визначення бот-профілів.

Методи визначення ботів можна розділити на 2 категорії – аналіз інформації, отриманої під час присутності користувача на сторінках

соціальної мережі (онлайн аналіз), і на аналіз даних, розміщених користувачем в своєму профілі (оффлайн аналіз). Відповідно всі отримані ознаки аккаунта будуть поділятися на статичні і поведінкові.

3.2.1 Статичні ознаки визначення ботів

До статичним ознак належать характеристики даних, що використовуються для оформлення аккаунта, а також особливості його ведення – повнота заповнення і т.п. Це можуть бути фотографії, публічні повідомлення, персональна інформація, така як місце проживання, дата народження та інше.

Для даної роботи передбачається розглянути наступні статичні ознаки:

– заблокований профіль – блокування акаунта практично завжди пов'язане з використанням сторонніх спам-програм;

– верифікований профіль з галочкою біля імені – ознака акаунта відомої особистості, реальної людини;

– кількість друзів, яка в середньому у користувача соціальної мережі складає 20-200 «друзів». У ботів ж ця цифра може досягати декількох тисяч або спостерігається повна відсутність друзів, але активна участь в обговореннях, листуванні;

– кількість підписок у передбачуваного бота;

– повнота заповнення профілю. При реєстрації ботів щоб прискорити процес заповнюється мінімум даних. Якщо використовуються програмні засоби, поля заповнюються повністю;

– некоректне ім'я може служити непрямою ознакою бот-активності, яка використовується в комплексі з іншими характеристиками;

– публікації користувача. Якщо користувач нічого не пише, а тільки репостить або коментує або публікує не унікальні повідомлення для імітації активності, це може бути ознаками ботів. В цьому випадку береться показник співвідношення записів, зроблених користувачем, до загальної кількості постів на його сторінці;

– активність користувача – різкі скачки активності по наповненню профілю контентом. Показником ботів може бути співвідношення активності до тривалості існування акаунта. Для виявлення подібних випадків розраховується середня активність користувача, періоди активності, співвідношення активності до тривалості існування акаунта і т.і.;

– кількість коментарів від інших користувачів – їх відсутність служить ознакою акаунта-бота;

– шкідливі посилання – наявність в контактах або статусі посилань на ресурси з чорного списку пошукових сервісів.

3.2.2 Поведінкові ознаки визначення ботів

До поведінкових ознак відносять особливості поведінки користувача, не характерні для людей [10]. Наприклад, штучне просування контенту. Подібними характеристиками можуть бути:

– швидкість коментування – реальна людина не в змозі писати по коментарю в секунду. Для більшої точності використовується співвідношення швидкості написання до довжини коментаря;

– коментарі декількох акаунтів з одного IP за короткий проміжок часу є явною вказівкою, що управляються ці акаунти-боти з одного комп'ютера або проксі-сервера;

– поведінка на сторінці. Якщо користувач переходить за посиланням, а вона не активна, то людина скоріше спробує ще раз, тоді як бот не стане цього робити;

– пристрої, якими користується користувач мережі;

– кількість відправлених повідомлень за певний проміжок часу.

У даній роботі для ідентифікації ботів в соціальній мережі «Вконтакте» застосовується наступний набір ознак:

– блокований профіль;
– кількість друзів;
– заповненість профілю (%);

– публікації профілю (відношення своїх постів до загальної кількості постів);

– час існування акаунта;

– шкідливі посилання;

– скарги на акаунт;

– активність користувача (активність / час існування акаунта);

– кількість коментарів від інших користувачів;

– швидкість коментування;

– коментування з декількох акаунтів при однаковому IP в один і той же час;

– кількість відправлених повідомлень за проміжок часу;

– відношення кількості друзів до кількості повідомлень, що відправляються.

На підставі запропонованого переліку ознак була створена база з 100 користувачів, 30% яких містять характерні ознаки ботів. На рисунку 3.2 представлена частина вибірки користувачів мережи з різними показниками. В повному обсязі таблиця представлена в електронному вигляді на диску, частково – в додатку Б.

Таблиця 3.1 – Фрагмент таблиці з показниками даних

Користувач	**Заблокований профіль**	**Кількість друзів**	**Заповненність профілю (%)**	**Публікації користувача (посты свої/до загальному числу постів)**
Дмитро Гвоздецький	0	67	100	0,77
Рита Іщенко	1	461	100	0,07
Микита Кот	0	120	60	0,97
Юрій Стасюк	0	78	80	0,99
Маша Леонова	0	560	90	0,68
Игор Белкин	0	1012	100	0,43
Іван Лазебников	0	71	50	0,83

Миша Рудой	0	0	20	0,01
Анастасія Ковш	1	2	10	0,33
Аліна Юрченко	0	603	100	0,97

Надалі для перевірки ефективності необхідно виконати тестування алгоритму на більшій кількості користувачів.

3.3 Нормування даних

В мережевому аналізі (кластерному зокрема) ефективне розбиття на класи істотно залежить від абсолютних значень вихідних даних. Проблему вирішують за допомогою нормування (стандартизації). Залежно від завдання дослідження використовують різні способи нормування. Одним із стандартних варіантів є віднімання з усіх значень по кожному фактору вибіркове середнє цього фактора і отримані різниці ділять на середнє відхилення.

$$x^* = \frac{x - \bar{x}}{S_H} \qquad (3.1)$$

де x – вихідне дане (показник користувача);

$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$ - вибіркове середнє;

$S_H = \sqrt{\frac{1}{n-1}}\sum_{i=1}^{n}(x_i - \bar{x})^2$ - середньоквадратичне відхилення.

При цьому стандартизовані значення матимуть вибіркові середні рівні нулю, а вибіркові дисперсії – рівні одиниці. Іншими словами, всі фактори зводяться в одну вагову категорію. Поряд зі стандартизацією змінних, існує варіант додання кожної з них певного коефіцієнта важливості, або ваги, який би відображав значимість відповідної змінної. За основу можуть виступати експертні оцінки, отримані в ході опитування експертів – фахівців предметної області. Отримані результати перемноження нормованих змінних на відповідні ваги дозволяють отримувати відстані між точками в

багатовимірному просторі з урахуванням неоднакової ваги змінних. В ході експериментів можливо порівняння результатів, отриманих з урахуванням експертних оцінок і без них, і вибір кращого з них.

3.4 Розробка класифікатора

В якості методу, використовуваного для моделювання класифікатора, обрана кластеризація – розпізнавання без навчання. Переваги кластерного аналізу в тому, що він дозволяє здійснювати розбиття об'єктів не по одному параметру, а по цілому набору ознак. Крім того, кластерний аналіз, на відміну від більшості математико-статистичних методів, не накладає ніяких обмежень на вид розглянутих об'єктів і дозволяє розглядати безліч вихідних даних практично довільної природи.

Кластерний аналіз дозволяє розглядати досить великий обсяг інформації і різко скорочувати, стискати великі масиви інформації, робити їх компактними і наочними. До того ж кластеризація може використовуватися циклічно. У цьому випадку дослідження проводиться до тих пір, поки не будуть досягнуті необхідні результати. При цьому кожен цикл може давати інформацію, яка здатна сильно змінити спрямованість і підходи подальшого застосування кластерного аналізу.

Завдання кластерного аналізу полягає в тому, щоб на підставі даних, що містяться у множині X, розбити безліч об'єктів G на m (m – ціле) кластерів (підмножин) $Q_1, Q_2, \dots, Q_m$ так, щоб кожен об'єкт Q_j належав одній і тільки одній підмножині розбиття. А об'єкти, що належать одному і тому ж кластеру, були подібними, в той час як об'єкти, що належать різним кластерам, були різнорідними. Рішенням задачі кластерного аналізу є розбиття, що задовольняють деякому критерію оптимальності.

Кластер має наступні математичні характеристики: центр, радіус, середньоквадратичне відхилення, розмір кластера.

Центр кластера – це середнє геометричне місце точок у просторі змінних.

Радіус кластера – максимальна відстань точок від центру кластера. Кластери можуть бути такими, що перекриваються. Така ситуація виникає, коли виявляється перекриття кластерів. У цьому випадку неможливо за допомогою математичних процедур однозначно віднести об'єкт до одного з двох кластерів. Такі об'єкти називають спірними.

Спірний об'єкт – це об'єкт, який у міру подібності може бути віднесений до кількох кластерів з певною ймовірністю.

Розмір кластера може бути визначений або по радіусу кластера, або по середньоквадратичному відхиленню об'єктів для цього кластера. Об'єкт відноситься до кластера, якщо відстань від об'єкта до центру кластера менше радіуса кластера. Якщо ця умова виконується для двох і більше кластерів, об'єкт є спірним.

Робота кластерного аналізу спирається на два припущення. Перше припущення – ознаки об'єкта, що розглядаються, в принципі допускають бажане розбиття пулу (сукупності) об'єктів на кластери. Друге припущення – правильність вибору масштабу або одиниць вимірювання ознак.

Вимоги, що пред'являються до виявлення кластерів в досліджуваній сукупності об'єктів:

– представлення кожного кластера має бути виражене однорідної категорією, що містить схожі об'єкти по близьким значенням властивостей або ознак;

– досліджувана сукупність всіх об'єктів повинна бути розподілена по всім кластерам, іншими словами, бути вичерпною;

– кожен об'єкт досліджуваної сукупності не повинен належати одночасно двом різним кластерам.

У загальному вигляді алгоритм кластеризації складається з наступних кроків:

1) вибір методів кластеризації;

2) визначення характеристики близькості об'єктів;

3) вибір методу розрахунку мінімальної відстані між кластерами;

4) об'єднання даних, що входять в групи по заданих ознаках;

5) виявлення спірних об'єктів, що знаходяться на кордоні кластерів;

6) виконання функції по аналізу траєкторії спірних акаунтів за певний період часу;

7) прийняття рішень виходячи з отриманих результатів.

3.5 Визначення характеристики близькості об'єктів

Важливим етапом кластеризації є вибір метрики, за якою визначається близькість об'єктів. Метрика вибирається залежно від:

– простору, в якому розташовані об'єкти;
– неявних характеристик кластерів.

Критерій для визначення схожості та відмінності кластерів – відстань між точками на діаграмі розсіювання. Цю схожість можна "виміряти", вона дорівнює відстані між точками на графіку.

Існує безліч метрик, ось лише основні з них

Евклідова відстань.

Найбільш поширена функція відстані. Являє собою геометричну відстань в багатовимірному просторі:

$$\rho(x, x') = \sqrt{\sum_i^n (x_i - x_i')^2} \quad (3.2)$$

Квадрат евклідової відстані.

Застосовується для додання більшої ваги більш віддаленим один від одного об'єктів. Це відстань обчислюється таким чином:

$$\rho(x, x') = \sum_i^n (x_i - x_i')^2 \quad (3.3)$$

Відстань міських кварталів (манхеттенська відстань).

Ця відстань є середнім різниць по координатах. У більшості випадків ця міра відстані приводить до таких же результатів, як і для звичайної

відстані Евкліда. Однак для цієї міри вплив окремих великих різниць (викидів) зменшується (тому що вони не зводяться в квадрат). Формула для розрахунку манхеттенського відстані:

$$\rho(x, x') = \sum_i^n |x_i - x_i'| \tag{3.4}$$

Відстань Чебишева.

Це відстань може виявитися корисною, коли потрібно визначити два об'єкти як «різні», якщо вони розрізняються за якоюсь однією координатою. Відстань Чебишева обчислюється за формулою:

$$\rho(x, x') = \max(|x_i - x_i'|) \tag{3.5}$$

Статечна відстань.

Застосовується в разі, коли необхідно збільшити або зменшити вагу, що відноситься до розмірності, для якої відповідні об'єкти сильно відрізняються. Статечна відстань обчислюється за такою формулою:

$$\rho(x, x') = \sqrt[r]{\sum_i^n (x_i - x_i')^p} \tag{3.6}$$

де r і p - параметри, що визначаються користувачем.

Параметр p відповідальний за поступове зважування різниць за окремими координатами, параметр r відповідальний за прогресивне зважування великих відстаней між об'єктами. Якщо обидва параметри – r і p дорівнюють двом, то ця відстань збігається з відстанню Евкліда.

У даній дипломній роботі використовується метод «Евклідова відстань». Приклад графічного представлення відстані між об'єктами в тривимірному просторі представлений на рисунку 3.3.

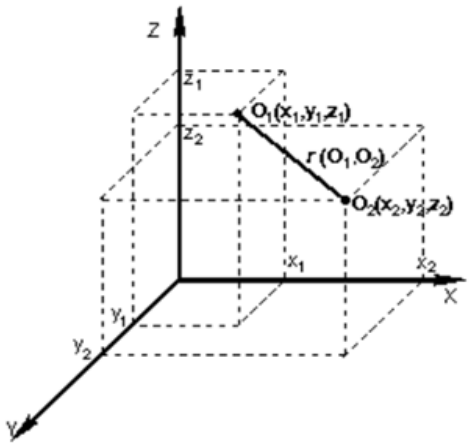


Рисунок 3.3 – Відстань між точками в тривимірному просторі

3.6 Обґрунтування вибору методів кластеризації

Головною причиною розробки великого різноманіття алгоритмів і методів кластеризації послужила можливість використання різних підходів до формального визначення кластерів. Алгоритми і методи кластерного аналізу як інструмент попереднього аналізу даних незамінні при пошуку закономірностей у великих наборах багатовимірних даних, таких як сховища даних [9]. Саме тому для розподілу акаунтів соціальних мереж за категоріями в даній роботі запропоновано метод кластерного аналізу. Незважаючи на те, що на сьогоднішній день відомі сотні алгоритмів і методів кластеризації, не існує «універсального рішення», оскільки специфіка поставленого завдання характеризується специфікою об'єкта кластеризації.

Виходячи з того, що об'єктом кластеризації є дані про користувачів соціальних мереж, вимоги, яким повинен задовольняти використовуваний метод кластеризації, сформульовані наступним чином:

– висока розмірність простору даних – об'єкти описуються великою кількістю атрибутів, отже, повинна бути пристосованість алгоритму до роботи в просторах даних високої розмірності;

– великий обсяг даних – в зв'язку з тим, що інформація про користувачів постійно оновлюється, збільшуючи тим самим вихідну вибірку, необхідно, щоб алгоритм був таким, що масштабується для роботи з великим обсягом даних;

– змішаний тип вимірювань – опис поведінки користувачів мережі включає в себе кількісні та якісні характеристики, тому алгоритм повинен бути пристосований до використання різних типів вимірювань.

За способом обробки даних методи кластерного аналізу підрозділяються на ієрархічні і неієрархічні.

За кількістю застосувань алгоритмів кластеризації виділяють методи з одноетапною і з багатоетапною кластеризацією.

По можливості розширення обсягу оброблюваних даних розрізняють методи масштабовані і немасштабовані.

За часом виконання кластеризації методи можна розділити на потокові (on-line) і непотокові (off-line) [11].

За способом аналізу даних методи кластеризації поділяють на чіткі і нечіткі.

На підставі аналізу методів для даної роботи обрані ієрархічний і нечіткий методи кластеризації.

3.6.1 Ієрархічні методи кластеризації

Суть ієрархічної кластеризації полягає в послідовному об'єднанні менших кластерів в великі або розподіду великих кластерів на менші.

Дівізімні (подільні) методи (DIvisive ANAlysis, DIANA). На початку роботи алгоритму дівізімного методу всі об'єкти належать одному кластеру, який на наступних кроках ділиться на менші кластери, в результаті утворюється послідовність груп, що розщеплені.

Агломеративні методи (Agglomerative Nesting, AGNES). Ця група алгоритмів характеризується послідовним об'єднанням вихідних елементів і

відповідним зменшенням числа кластерів. Принцип роботи описаних вище груп методів у вигляді дендрограмми показаний на рисунку 3.4

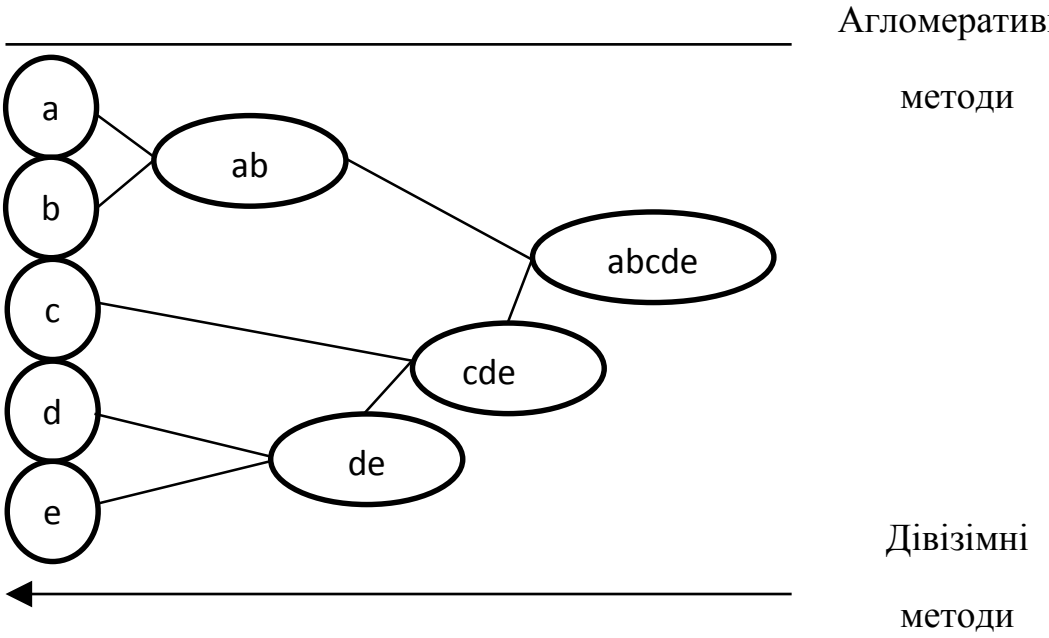


Рисунок 3.4 – Принцип роботи дівізімних і агломеративних методів кластеризації

Ієрархічні алгоритми пов'язані з побудовою дендрограмм (від грецького dendron – "дерево"), які є результатом ієрархічного кластерного аналізу. Дендрограмма описує близькість окремих точок і кластерів один до одного, представляє в графічному вигляді послідовність об'єднання (поділу) кластерів.

Дендрограмма (dendrogram) – деревоподібна діаграма, що містить n рівнів, кожен з яких відповідає одному з кроків процесу послідовного укрупнення кластерів.

Дендрограмму також називають деревовидною схемою, деревом об'єднання кластерів, деревом ієрархічної структури.

Дендрограмма – вкладене угруповання об'єктів, яке змінюється на різних рівнях ієрархії.

Існує багато способів побудови дендрограмм. У дендрограмі об'єкти можуть розташовуватися вертикально або горизонтально. Приклад вертикальної дендрограмми наведено на рисунку 3.5

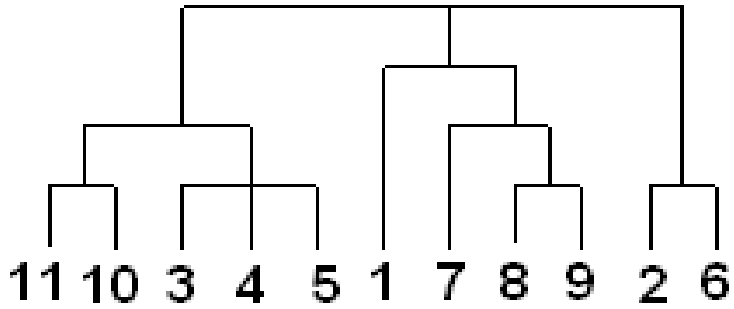


Рисунок 3.5 – Приклад дендограмми

До недоліків ієрархічних алгоритмів можна віднести систему повного розбиття, яке може бути зайвим в контексті розв'язуваної задачі.

3.6.2 Неієрархічні методи кластеризації

У неієрархічних або ітеративних методах кластери формуються в залежності від поставлених умов розбиття з можливістю зміни користувачем з метою досягнення бажаного результату. До таких методів належать: k-середніх (k-means), CLOPE, PAM, карти Кохонена, що самоорганізуються та ін.

Завдання кластеризації можна розглядати і як побудову оптимального розбиття об'єктів на групи. При цьому оптимальність може бути визначена як вимога мінімізації середньоквадратичної помилки розбиття:

$$e^2(X, L) = \sum_{j=1}^{K} \sum_{i=1}^{n_j} ||x_i^{(j)} - c_j||^2 \qquad (3.7)$$

де c_j – «центр мас» кластера,

j (точка з середніми значеннями характеристик для даного кластера).

Алгоритми квадратичної помилки відносяться до типу плоских алгоритмів. Найпоширенішим алгоритмом цієї категорії є метод k-середніх.

Метод k-середніх – досить простий і швидкий у використанні, алгоритм прозорий і зрозумілий, але дуже чутливий до викидів, на великих

базах даних повільний в роботі. Недоліком його є неможливість застосування на пересічних кластерах і необхідність завдання кількості кластерів.

Даний алгоритм складається з наступних кроків:

– випадково вибрати k точок, які є початковими «центрами мас» кластерів (будь-які k з n об'єктів або взагалі k випадкових точок);

– віднести кожен об'єкт до кластеру з найближчим «центром мас»;

перерахувати «центри мас» кластерів відповідно до поточного членства;

– якщо критерій зупинки алгоритму не задовільний, повернутися до кроку два.

Як критерій зупинки зазвичай вибирають або відсутність переходу об'єктів з кластера в кластер на кроці 2 або мінімальну зміну середньоквадратичної помилки.

PAM – так само, як і k-means, простий і швидкий у використанні, алгоритм менш чутливий до викидів, проте присутня необхідність завдання кількості кластерів і повільна робота на великих базах даних.

Алгоритми, засновані на теорії графів. Суть таких алгоритмів полягає в тому, що вибірка об'єктів представляється у вигляді графа $G = (V, E)$, вершинам якого відповідають об'єкти, а ребра мають вагу, рівну «відстані» між об'єктами. Перевагою графових алгоритмів кластеризації є наочність, відносна простота реалізації і можливість внесення різних удосконалень, заснованих на геометричних міркуваннях.

Основними алгоритмами є алгоритм виділення зв'язкових компонент, алгоритм побудови мінімального покривного (остовного) дерева та алгоритм пошарової кластеризації.

Алгоритм виділення зв'язкових компонент.

В алгоритмі виділення зв'язкових компонент задається вхідний параметр R і в графі видаляються всі ребра, для яких «відстані» більше R. Сполученими залишаються тільки найбільш близькі пари об'єктів. Сенс

алгоритму полягає в тому, щоб підібрати таке значення R, що лежить в діапазоні всіх «відстаней», при якому граф «розвалиться» на кілька зв'язкових компонент. Отримані компоненти і є кластерами.

Для підбору параметра R зазвичай будується гістограма розподілів попарних відстаней. У завданнях з добре вираженою кластерної структурою даних на гістограмі буде два піки – один відповідає внутрікластерним відстаням, другий – межкластерним відстаням. Параметр R підбирається із зони мінімуму між цими піками. При цьому управляти кількістю кластерів за допомогою порога відстані досить важко.

Алгоритм мінімального покривного дерева.

Алгоритм мінімального покривного дерева спочатку будує на графі мінімальне покривне дерево, а потім послідовно видаляє ребра з найбільшою вагою. На рисунку 3.6 зображено мінімальне покривне дерево, отримане для дев'яти об'єктів.

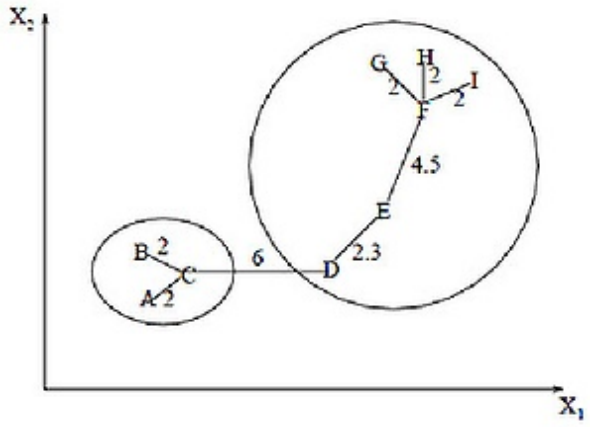


Рисунок.3.6 – Мінімальна покривне дерево

Шляхом видалення зв'язку з позначкою CD, з довжиною рівною 6 одиницям (ребро з максимальною відстанню), отримуються два кластери: {A, B, C} і {D, E, F, G, H, I}. Другий кластер в подальшому може бути розділений ще на два кластери шляхом видалення ребра EF, яке має довжину рівну 4,5 одиницям.

Пошарова кластеризація.

Алгоритм пошарової кластеризації заснований на виділенні зв'язкових компонент графа на деякому рівні відстаней між об'єктами (вершинами). Рівень відстані задається порогом відстані c. Наприклад, якщо відстань між об'єктами $0 \leq \rho(x, x') \leq 1$, то $0 \leq c \leq 1$.

Алгоритм пошарової кластеризації формує послідовність підграфів графа G, які відображають ієрархічні зв'язки між кластерами.

Карти Кохонена, що самоорганізуються, використовують універсальний апроксіматор – нейронну мережу, метод простий у реалізації, але має деякі особливості:

– штучні нейронні мережі легко працюють в розподілених системах з великою паралелізацією в силу своєї природи;

– нейронні мережі оперують числами, тому можуть проводити розбиття на класи тільки для об'єктів з чисельними векторами характеристик;

– оскільки штучні нейронні мережі підлаштовують свої вагові коефіцієнти, грунтуючись на вихідних даних, це допомагає зробити вибір значущих характеристик менш суб'єктивним.

3.6.3 Чіткі і нечіткі методи кластеризації

Чіткі методи кластеризації розбивають початкову множину об'єктів X на кілька непересічних підмножин. При цьому будь-який об'єкт з X належить тільки одному кластеру. В результаті використання нечітких методів кластеризації можлива одночасна приналежність кількома або навіть всім кластерам, але з різним ступенем приналежності. У багатьох ситуаціях нечітка кластеризація більш «природна», ніж чітка, наприклад, для об'єктів, розташованих на кордоні кластерів [6].

Нечітка кластеризація отримала широке застосування і розвиток завдяки Бездеку і його методу нечітких с-середніх (Fuzzy c-means – FCM), який дозволяє виділяти в кластер об'єкти, що знаходяться на кордоні кластера, для нього характерна менша чутливість до викидів, проте присутня необхідність завдання кількості кластерів, обчислювальна складність

кластеризації, а також виникає невизначеність з об'єктами, віддаленими від усіх центрів кластерів [12].

Вимога знаходження однозначної кластеризації елементів досліджуваної проблемної області є досить грубою і твердою, особливо при вирішенні погано або слабо структурованих задач. Методи нечіткої кластеризації послаблюють цю вимогу. При введенні в розгляд нечітких кластерів і відповідних їм функцій приналежності, що приймають значення з інтервалу [0,1], відбувається ослаблення цієї вимоги. А елементи матриці ступенів належності чіткого розбиття приймають значення з двоелементної множини {0,1}, а не з інтервалу [0,1].

Найбільш популярним алгоритмом нечіткої кластеризації є алгоритм c-середніх (c-means). Він являє собою модифікацію методу k-середніх.

Кроки роботи алгоритму:

– вибирається початкове нечітке розбиття n об'єктів на k кластерів шляхом вибору матриці приналежності U розміру $n \times k$;

– використовуючи матрицю U , знаходиться значення критерію нечіткої помилки:

$$E^2(X,U) = \sum_{i=1}^{N} \sum_{k=1}^{K} U_{ik} ||x_i^{(k)} - C_k||^2 \quad (3.8)$$

де C_k - «центр мас» нечіткого кластера k

$$C_k = \sum_{i=1}^{N} U_k x_i \quad (3.9)$$

– перегрупувати об'єкти з метою зменшення цього значення критерію нечіткої помилки.

– повертатися в п. 2 до тих пір, поки зміни матриці U не стануть незначними.

Цей алгоритм може не підійти, якщо заздалегідь невідомо число кластерів, або необхідно однозначно віднести кожен об'єкт до одного

кластеру. Тому для визначення кількості кластерів, на які буде розбита множина користувачів соціальних мреж, використовується ієрархічний метод кластеризації.

3.7 Розробка алгоритму обчислення кількості кластерів

3.7.1 Обґрунтування вибору методу для розрахунку оптимальної кількості кластерів.

Для визначення оптимальної кількості кластерів в дипломній роботі обраний агломеративний ієрархічний метод, в якому спочатку кожен об'єкт (аккаунт користувача з вибіркою ознак) вважається окремим кластером. Для одноелементних кластерів природним чином визначається функція відстані:

$$R(\{x_i\},\{x_j\}) = \rho(x_i, x_j) \tag{3.10}$$

де x_i, x_j – ознаки акаунта користувача.

Потім запускається процес злиття. На кожній ітерації замість пари найближчих кластерів U і V утворюється новий кластер $W = U \cup V$. Відстань від нового кластера W до будь-якого іншого кластера S обчислюється по відстанях $R(U,V)$, $R(U,S)$ и $R(V,S)$, які до цього моменту вже повинні бути відомі:

$$R(U \cup V, S) = \alpha U R(U,S) + \alpha V R(V,S) + \beta R(U,V) + \gamma |R(U,S) - R(V,S)| \tag{3.11}$$

де αU, αV, β, γ – числові параметри.

Ця універсальна формула узагальнює практично всі способи визначення відстаней між кластерами. Вона була запропонована Лансом і Вільямсом.

На практиці застосовуються такі методи обчислення відстаней $R(W,S)$ між кластерами W и S. Для кожного з них доведено відповідність формулі Ланса-Вільямса при певних поєднаннях параметрів.

Коли кожен об'єкт являє собою окремий кластер, відстані між цими об'єктами визначаються обраної мірою. Існують різні правила, звані методами об'єднання або зв'язку для двох кластерів.

Метод ближнього сусіда або одиночний зв'язок.

Тут відстань між двома кластерами визначається відстанню між двома найбільш близькими об'єктами (найближчими сусідами) в різних кластерах. Цей метод дозволяє виділяти кластери як завгодно складної форми за умови, що різні частини таких кластерів з'єднані ланцюжками близьких один до одного елементів. В результаті роботи цього методу кластери представляються довгими "ланцюжками" або "волокнистими" кластерами, "зчепленими разом" тільки окремими елементами, які випадково опинилися ближче інших один до одного.

$$R^{б}(W,S) = \min_{w \in W, s \in S} \rho(w,s) \qquad (3.12)$$

де $\alpha_U = \alpha_V = \frac{1}{2}$,

$\beta = 0, \gamma = -\frac{1}{2}$

Метод найбільш віддалених сусідів або повний зв'язок

Тут відстані між кластерами визначаються найбільшою відстанню між будь-якими двома об'єктами в різних кластерах (тобто "найбільш віддаленими сусідами"). Метод добре використовувати, коли об'єкти дійсно з різних "гаїв". Якщо ж кластери мають в деякому роді подовжену форму або їх природний тип типу "ланцюжка", то цей метод не слід використовувати.

$$R^{д}(W,S) = \max_{w \in W, s \in S} \rho(w,s) \qquad (3.13)$$

де $\alpha_U = \alpha_V = \frac{1}{2}$,

$\beta = 0, \gamma = \frac{1}{2}$

Метод Уорда (Ward's method)

За відстань між кластерами береться приріст суми квадратів відстаней об'єктів до центрів кластерів, що отримується в результаті їх об'єднання. На відміну від інших методів кластерного аналізу, для оцінки відстаней між кластерами тут використовуються методи дисперсійного аналізу. На кожному кроці алгоритму об'єднуються такі два кластери, які призводять до мінімального збільшення цільової функції, тобто внутрішньогрупової суми квадратів. Цей метод направлений на об'єднання близько розташованих кластерів.

$$R^y(W,S) = \frac{|S||W|}{|S|+|W|}\rho^2\left(\sum_{w\in W}\frac{w}{|W|}, \sum_{s\in S}\frac{s}{|S|}\right) \quad (3.14)$$

де $\alpha_U = \frac{|S|+|U|}{|S|+|W|}$,

$\alpha_V = \frac{|S|+|U|}{|S|+|W|}$,

$\beta = \frac{-|S|}{|S|+|W|}, \gamma = 0$

Метод невиваженого попарного середнього (метод невиваженого попарного арифметичного середнього – unweighted pair-group method using arithmetic averages, UPGMA (Sneath, Sokal, 1973)).

За відстань між двома кластерами береться середня відстань між усіма парами об'єктів в них. Цей метод слід використовувати, якщо об'єкти дійсно з різних "гаїв", у випадках присутності кластерів типу "ланцюжка", при припущенні нерівних розмірів кластерів.

$$R^c(W,S) = \frac{1}{|W||S|}\sum_{w\in W}\sum_{s\in S}\rho(w,s) \quad (3.15)$$

де $\alpha_U = \frac{|U|}{|W|}$,

$\alpha_V = \frac{|V|}{|W|}$,

$\beta = \gamma = 0$

Невиважений центроїдний метод (метод невиваженого попарного центроїдного усереднення – unweighted pair-group method using the centroid average (Sneath and Sokal, 1973)). За відстань між двома кластерами в цьому методі береться відстань між їх центрами тяжкості.

$$R^{\text{ц}}(W,S) = \rho^2\left(\sum_{w\in W}\frac{w}{|W|}, \sum_{s\in S}\frac{s}{|S|}\right) \tag{3.16}$$

де $\alpha_U = \frac{|U|}{|W|}$,

$\alpha_V = \frac{|V|}{|W|}$,

$\beta = -\alpha_U\alpha_V, \gamma = 0$

З додаткових властивостей, які характеризують якість кластеризації, виділені наступні.

Властивість монотонності.

Позначимо через R_t відстань між найближчими кластерами, обраними на t-му кроці злиття. Кажуть, що функція відстані R має властивість монотонності, якщо при кожному злитті відстань між кластерами, що об'єднуються тільки збільшується: $R_2 <= R_3 <= \cdots <= R_{l.}$ Якщо кластеризация монотонна, то дендрограмма не має самоперетинів.

Властивості розтягування і стиснення.

Деякі відстані мають властивість розтягування. У міру того, як кластер росте, відстані від нього до інших кластерів збільшуються, як ніби простір навколо кластера розтягується. Властивість розтягування вважається бажаним, так як воно сприяє більш точному відділенню кластерів. З іншого боку, при занадто сильному розтягуванні можливо знайти кластери там, де їх

спочатку не було. Відстанями, що розтягують є відстані $R_д$і $R_у$. Деякі відстані, навпаки, мають властивість стиснення. У міру зростання кластера відстані від нього до інших кластерів зменшується, і здається, що простір навколо кластера стискається. Природна кластеризація при цьому розмазується. Відстань ближнього сусіда $R_б$ є такою, що сильно стискається. Кластеризація стискає, якщо $R_t <= \rho(\mu U, \mu V)$, де $R_t = R(U, V)$.

Кластеризація розтягується, якщо $R_t >= \rho(\mu U, \mu V)$, де $R_t = R(U, V)$, а μU и μV – центри цих кластерів.

R_c і $R_ц$ не є тими, що стискають ані тими, що розтягують. Про них говорять, що вони зберігають метрику простору.

Висновок: Кожна з відстаней, перерахованих вище, має свої недоліки. Метод ближнього сусіда володіє ланцюжковим ефектом, коли незалежно від форми кластера до нього приєднуються найближчі до кордону об'єкти. У деяких випадках це призводить до того, що кластери відрощують щупальця. Метод ближнього сусіда добре підходить для виділення кластерів стрічкової форми. Метод далекого сусіда ланцюжкового ефекту не має, але на ранньому етапі може об'єднувати досить несхожі групи. Відстань між центрами мас не є однорідним і не редуктивним.

Метод Уорда, обраний для дипломної роботи, виявився найкращим за результатами експериментального порівняння на представницькому наборі модельних задач [5]. Він частіше за інших методів відновлює інтуїтивно найкращу кластеризацію.

З метою оптимізації алгоритму приймається, що користувачі, які зареєстровані менше місяця, не розглядаються, так як не мають достатньої інформації для виконання кластеризації. Даний період може бути скоректований за результатами проведення подальших випробувань.

3.7.2 Алгоритм модуля визначення оптимальної кількості кластерів

1) спочатку всі кластери одноелементні:

$$t \coloneqq 1;\ C_t \coloneqq \{x_1\}, \dots, \{x_l\};$$
$$R(\{x_i\}, \{x_j\}) = \rho(x_i, x_j)$$

2) вибрати початкове значення параметра δ

$$P(\delta) \coloneqq \{(U,V) | U,V\} \in C_t,\ R(U,V) <= \delta;$$

3) для всіх $t = 2, \dots, l$ (t - номер ітерації);

4) якщо $P(\delta) = 0$, то збільшувати δ так, щоб $P(\delta) \neq 0$

5) знайти в $C_t - 1$ два найближчих кластера:

$$(U,V) \coloneqq \underset{(U,V) \in P(\delta)}{\operatorname{argmin}}\ R(U,V)$$
$$R_t \coloneqq R(U,V)$$

6) вилучити кластери U і V, додати злитий кластер $W = U \cup V$:

$$C_t \coloneqq C_t - 1 \cup \{W\} \backslash \{U,V\}$$

7) для всіх $S \in C_t$ обчислити відстань $R(W,S)$ за формулою Ланса-Вільямса.

8) якщо $R(W,S) <= \delta$ то $P(\delta) \coloneqq P(\delta) U \{(W,S)\}$.

3.8 Розробка алгоритму визначення шкідливих акаунтів

3.8.1 Обґрунтування вибору методу кластеризації для класифікації акаунтів

Поділ акаунтів користувачів соціальної мережі з великою кількістю нерівнозначних критеріїв на групи складно уявити двома ступенями приналежності 0 або 1. Більш природним є використання часткової належності в діапазоні від 0 до 1, що дозволить користувачам,

характеристики яких знаходяться на кордонах між декількома кластерами, належати їм з різною ступенем. Тому в якості основного методу розбиття акаунтів користувачів на групи обраний метод нечіткої кластеризації – нечітких с-середніх.

Вихідною інформацією для кластеризації є матриця спостережень $l \times n$

$$X = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ x_{l1} & x_{l2} & \cdots & x_{ln} \end{bmatrix}$$

де l – число користувачів,

n – число ознак [6, 7].

Задача кластеризації полягає в розбитті множини об'єктів на групи (кластери) «схожих» між собою об'єктів. У n-вимірному метричному просторі ознак мірою «подібності» двох об'єктів вважається відстань між ними (Евклідова відстань).

Число кластерів c визначено на попередньому кроці алгоритму детектування.

Кластерна структура задається матрицею приналежності ($c \times l$ матриця):

$$M = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1l} \\ m_{21} & m_{22} & \cdots & m_{2l} \\ \cdots & \cdots & \cdots & \cdots \\ m_{c1} & m_{c2} & \cdots & m_{cl} \end{bmatrix}$$

де m_{ij} – ступінь приналежності,

j – го елемента i-го кластеру.

Відзначимо, що матриця приналежності повинна задовольняти наступним умовам:

$$m_{ij} \in [0,1],\ i = \overline{1,c},\ j = \overline{1,l},$$

$$\sum_{i=1}^{c} m_{ij} = 1,\ j = \overline{1,l}$$

тобто кожен об'єкт повинен бути розподілений між усіма кластерами,

$$0 < \sum_{j=1}^{l} m_{ij} < l, i = \overline{1,c}$$

тобто жоден кластер не повинен бути порожнім або містити всі елементи.

Для оцінки якості розбиття використовується критерій розкиду, який показує суму відстаней від об'єктів до центрів кластерів з відповідними ступенями приналежності:

$$J = \sum_{i=1}^{c} \sum_{j=1}^{l} (m_{ij})^{w} d(v_i, x_j) \quad (3.17)$$

де $d(v_i, x_j)$ – Евклідова відстань між j -м об'єктом $x_j = (x_{j1}, x_{j2}, \dots, x_{jn})$і i -м центром кластера $v_i = (v_{i1}, v_{i2}, \dots, v_{in})$;

$w \in (1, \infty)$ – експонентна вага, яка визначає нечіткість, розмитість кластерів;

$V = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \vdots & v_{2n} \\ \cdots & \cdots & & \cdots \\ v_{c1} & v_{c2} & \cdots & v_{cn} \end{bmatrix}$ – $c \times n$ матриця координат центрів кластерів, елементи якої обчислюються за формулою:

$$v_{ik} = \frac{\sum_{j=1}^{l} (m_{ij})^{w} x_{jk}}{\sum_{j=1}^{l} (m_{ij})^{w}}, k = \overline{1,n}(v) \quad (3.18)$$

Завданням є знаходження матриці M, що мінімізує критерій j.

У дипломній роботі для цієї мети використовується алгоритм нечітких с-середніх, в основі якого лежить метод множників Лагранжа. Він дозволяє знайти локальний оптімум, тому для різних запусків можуть вийти різні результати.

Алгоритм нечітких c-середніх

1) на першому етапі матриця належності M, яка задовольняє умовам, генерується випадковим чином;

2) далі запускається ітераційний процес обчислення центрів кластерів та перерахунку елементів матриці ступенів належності;

$$m_{ij} = \frac{1}{(d_{ij})^{\frac{2}{w-1}} \sum_{k=1}^{c} \frac{1}{(d_{kj})^{\frac{2}{w-1}}}} \tag{3.19}$$

де $d_{ij} > 0,$

$m_{kj} = \begin{cases} 1, k = i \\ 0, k \neq i' \end{cases}$

$d_{ij} = 0, d_{ij} = d(v_i, x_j),$

$i = \overline{1, c},$

$j = \overline{1, l}$.

3) обчислення тривають до тих пір, поки зміна матриці M, яка характеризується величиною $||M - M^*||^2$, де $||M - M^*||^2$– матриця на попередній ітерації, не стане менше заздалегідь заданого параметра зупинки ε.

Збіжність алгоритму нечітких с-середніх доведена в [8]

Зупинимося на виборі значення w – експоненціального ваги. Чим більше це значення, тим матриця приналежності більш розмазана і при $w \to \infty$ елементи будуть виглядати як $m_{ij} = \frac{1}{c}$, що є поганим рішенням, тому що всі об'єкти з однаковим ступенем розподілені по всьому кластерам. Теоретично обґрунтованого правила вибору ваги поки не існує і зазвичай встановлюють $w = 2.$

Результат кластеризації акаунтів, виконаної за алгоритмом нечітких *C*-середніх, показав правильне визначення центрів кластерів, що дозволяє зробити висновок про перспективність використання даного методу. (Рис 3.6)

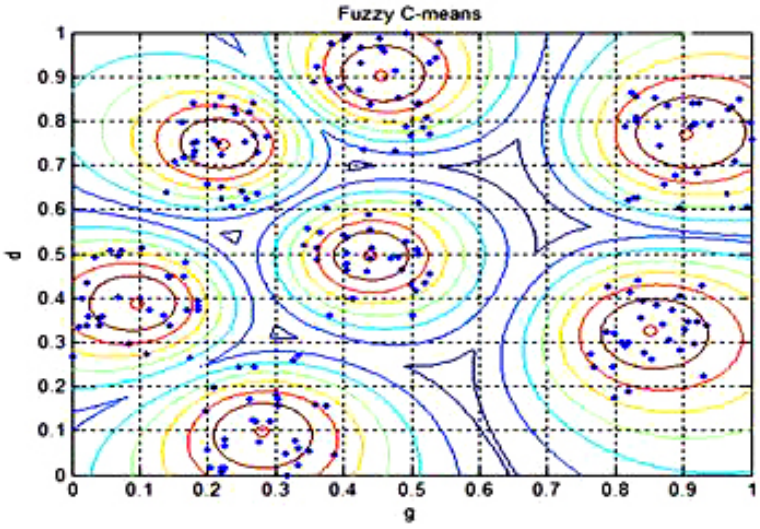


Рисунок 3.6 – Результат кластеризації методом нечітких *c*-середніх

3.8.2 Визначення кластерів з підозрілими акаунтами

В результаті кластеризації утворилося *c* кластерів. Ступінь приналежності акаунтів до кожного з кластерів відображена в отриманій матриці приналежності.

Для визначення кластерів з підозрілими акаунтами повинна бути сформована вибірка еталонних користувачів, в які входять:

– акаунти з максимальними характеристиками реального людини – мають максимально заповнені поля профілю, які пройшли всі необхідні перевірки, не помічені в розсилці спаму і т.і.;

– акаунти з ознаками шкідливих програм – мінімальна інформація про користувача, піддавалися блокування тощо.

На наступному етапі виконується перевірка приналежності всіх еталонних акаунтів до отриманих кластерів. Залежно від результату кластери можуть розподілитися на:

– лояльні, з акаунтами реальних користувачів;

– підозрілі – ті, яким належать акаунти з ознаками шкідливих програм;

– кластери, в які не потрапив жоден з еталонних користувачів, тобто спірні.

3.8.3 Алгоритм модуля прийняття рішень

На вхід модуля подається матриця приналежності і класифікація кластерів, отримана на попередньому кроці.

Алгоритм прийняття рішень складається з наступних етапів:

1) для кластерів, до яких не належить жоден з акаунтів з еталонної вибірки, необхідно вибрати групу користувачів з максимальними показниками приналежності (розташовані в центрі кластера). Їм пропонується додаткова перевірка. За результатами приймається рішення про те, чи можна вважати об'єкти шкідливими акаунтами чи ні. Перевірені користувачі заносяться в еталонну вибірку.

2) перевірка акаунтів, розташованих на кордоні кластерів.

– на першому етапі визначаються акаунти з коефіцієнтами приналежності, наближеними до 0.5, а також номери кластерів, від центру яких вони рівновіддалені (на кордоні з якими знаходяться);

– на наступному кроці визначається часовий інтервал ΔT, протягом якого система відстежує траєкторію руху спірних об'єктів – зміну показників приналежності в матриці. Також задається максимальна відстань об'єкта від центру кластера (межа належності), в межах якого він не є спірним;

– якщо об'єкт, що перевіряється розташовується на кордоні двох не підозрілих кластерів, перехід до наступного кроку;

– якщо об'єкт знаходиться на кордоні двох підозрілих кластерів, то він не вважається;

– якщо об'єкт знаходиться на кордоні між підозрілим і «лояльним» кластерами, то запускається функція відстеження його вектору руху протягом ΔT. Для цього після кожного виконання алгоритму порівнюються його показники приналежності до суміжних кластерів в матриці.

Якщо показник приналежності об'єкта до «лояльному» кластеру збільшується (вектор руху спрямований в бік кластера, що не є підозрілим) і менше значення кордону приналежності, то спостереження триває. А якщо

значення показника приналежності перевищує значення кордону приналежності, то він перестає бути спірним.

Якщо показник приналежності об'єкта до підозрілого кластеру збільшується (вектор руху спрямований в бік підозрілого кластера) і менше значення кордону приналежності, то аккаунт піддається додатковій перевірці (верифікації). У разі успішного проходження верифікації за аккаунтом триває спостереження. Якщо користувач не пройшов верифікацію, застосовується тимчасове блокування. А якщо значення показника приналежності перевищує значення кордону приналежності, то він перестає бути спірними та стає підозрілим.

Схематичне зображення алгоритму модуля прийняття рішень в додатку В.

3.9 Висновки до третього розділу

У третьому розділі дипломної роботи проаналізовано основні напрямки теорії розпізнавання образів, зокрема кластерного аналізу, методів класифікації об'єктів з навчанням і без вчителя.

Проведено аналіз методів кластеризації з метою вибору найбільш ефективних для вирішення завдань, поставлених у дипломній роботі. Кожен з них має свої переваги і недоліки. На підставі результатів аналізу було визначено, що кластерний аналіз є уніфікованим засобом розвідувального аналізу даних і статистичних досліджень в будь-якій предметній області, зокрема для вирішення задачі детектування ботів. Для коректного застосування методів та отримання найбільш достовірних результатів запропоновано використовувати комбінацію з двох методів кластерного аналізу – ієрархічного та нечіткого.

Розроблений алгоритм детектування шкідливих акаунтів має наступні переваги в порівнянні з існуючими:

1) покращено якість сортування користувачів соціальних мереж завдяки використанню комбінації двох методів кластеризації;

2) мінімізація кількості зайвих перевірок (верифікації).

У діючих на сьогоднішній день системах визначення соціальних та пошукових роботів виконується за жорсткими алгоритмами і умовами. Підозрілі акаунти користувачів або блокуються або піддаються додатковій верифікації, що може стати причиною відходу користувачів з соціальної мережі або переходу в іншу соціальну мережу. У розробленому алгоритмі спочатку до всіх нових акаунтів система лояльна, а для класифікації підозрілих користувачів використовуються додаткові аналітичні методи. Це дозволяє підозрілі акаунти з неоднозначними показниками піддавати додатковій класифікації через певний проміжок часу, після збору статистики і спостереження за їх поведінкою і тільки після підтвердження належності до шкідливим акаунтів пропонувати перевірочну верифікацію.

РОЗДІЛ 4. ЕКОНОМІЧНА ЧАСТИНА

Метою дипломної роботи є розробка алгоритму детектування шкідливих акаунтів (соціальних ботів) в соціальних мережах. В цьому розділі надається економічне обґрунтування доцільності розробки та орієнтовна економічна ефективність від її впровадження.

4.1 Орієнтовний розрахунок капітальних витрат

Розрахунки капітальних витрат, які спрямовані на розробку програмного забезпечення по розробленому в дипломній роботі алгоритму детектування соціальних ботів, складаються з:

– визначення трудомісткості розробки та опрацювання програмного забезпечення;

– витрат на створення програмного продукту;

– оцінки швидкодії та надійності роботи ПЗ.

4.1.1 Визначення трудомісткості розробки та опрацювання програмного забезпечення

Умовна кількість оперантів у програмі:

$$Q = q * c(1 + p) \qquad (4.1)$$

де q – очікувана кількість оперантів;

c – коефіцієнт складності програми;

p – коефіцієнт корекції програми в процесі її опрацювання.

$$Q = 7200 * 1{,}7(1 + 0{,}06) = 12974{,}4$$

Тривалість вивчення технічного завдання, опрацювання довідкової літератури з урахуванням уточнення ТЗ і кваліфікації програміста

$$t_{\text{в}} = \frac{Q*B}{(75...85)*k} \quad (4.2)$$

де В – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання,

k – коефіцієнт, що враховує кваліфікацію програміста і визначається стажем роботи за фахом.

$$t_{\text{в}} = \frac{12974,4*1,3}{80*1,4} = \frac{16866,72}{112} = 150,6, \text{ годин}$$

Тривалість розробки блок-схеми алгоритму:

$$t_a = \frac{Q}{(20...25)*k} \quad (4.3)$$

$$t_a = \frac{12974,4}{25*1,4} = 370, \text{ годин}$$

Тривалість складання програми за готовою блок-схемою:

$$t_{np} = \frac{Q}{(20...25)*k} \quad (4.4)$$

$$t_{np} = \frac{12974,4}{22*1,4} = 421,2, \text{ годин}$$

Тривалість опрацювання програми на ПК:

$$t_{onp} = \frac{1,5*Q}{(4...5)*5} \quad (4.5)$$

$$t_{onp} = \frac{1,5*12974,4}{25} = 778,4, \text{ годин}$$

Тривалість підготовки технічної документації на ПЗ:

$$t_{\text{д}} = \frac{Q}{(15...20)*k} + \frac{Q}{(15...20)} * 0,75 \quad (4.6)$$

$$t_д = \frac{12974,4}{20*1,4} + \frac{12974,4}{20} * 0,75 = 463,4 + 648,7 * 0,75 = 949,9, \text{ годин}$$

Трудомісткість створення ПЗ

$$t = t_д + t_{опр} + t_{пр} + t_а + t_в + t_о \quad (4.7)$$

де $t_о$ – принимается 50

$$t = 949,9 + 778,4 + 421.2 + 370 + 150,6 + 50 = 2720,1, \text{ годин}$$

4.1.2 Розрахунок витрат на створення програмного продукту

Витрати на створення програмного продукту Кпз складаються з витрат на заробітну плату виконавця програмного забезпечення Ззп і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК Змч:

$$К_{пз} = З_{зп} + З_{мч} \quad (4.8)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби

$$З_{зп} = t * З_{пр} \quad (4.9)$$

де t – загальна тривалість створення ПЗ, годин,

$З_{пр}$– средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

Середня зарплата програміста, потрібного кваліфікаційного рівню в Україні, складає 25600 в місяць. Що в свою чергу складає 160 грн/годину.

$$З_{зп} = 2720,1 * 160 = 435216, \text{ гривень.}$$

Вартість машинного часу для налагодження програми на ПК

$$З_{мч} = t * C_{мч} \quad (4.10)$$

Вартість 1 години машинного часу ПК визначається за формулою

$$C_{мч} = P * t * C_e + \frac{Ф_{зал} * 0,5}{F_p} + \frac{К_{лпз} * H_{апз}}{F_p}$$

$$C_{мч} = 1,5 * 1 * 0,9 + \frac{113280*0,5}{2080} + \frac{22000*0,5}{2080} = 1,35 + 27,2 + 5,3 = 33,85,$$

гривень

$$З_{мч} = 33,85 * 2720,1 = 920755,3, \text{ гривень}$$

$$K_{пз} = 920755,3 + 435216 = 527291,3, \text{ гривень}$$

4.1.3 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

Таблиця 4.1 - Поточні витрати на експлуатацію

Назва комплектуючих	Вартість грн.
Процесор: IntelXeonE5-2660	50 000
Материнская плата: Asus Prime Z370-P	5000
Оперативная память Kingston DDR4-2666	50 000

16384MB PC4-21300 HyperX Fury Black (8шт)	

Продовження таблиці 4.1

Жесткий диск: Western Digital Blue	1280
Корпус для сервера Chieftec UNC-310RS-B	7000
Разом	113280

Ліцензійне програмне забезпечення IntelliJ IDEA Ultimate – 11000грн за рік.

Річні поточні (експлуатаційні) витрати на функціонування системи

$$C = C_{\text{в}} + C_{\text{к}} + C_{\text{ак}} \tag{4.11}$$

де $C_{\text{в}}$ – витрати на Upgrade-відновлення й модернізацію системи

$$C_{\text{в}} = 58{,}5, \text{ тис. гривень}$$

$C_{\text{к}}$ – витрати на керування системою

$$C_{\text{к}} = C_{\text{н}} + C_{\text{з}} + C_{\text{ел}} + C_{\text{тос}} + C_{o} \tag{4.12}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації тощо (Сн).

$$C_{\text{н}} = 3\ 500, \text{ гривень}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему

$$C_{\text{з}} = 144000, \text{ гривень}$$

Вартість електроенергії, що споживається апаратурою системоюпротягом року ($C_{ел}$)

$$C_{ел} = P * F_p * Ц_е \quad (4.13)$$

$$C_{ел} = 1{,}5 * 2080 * 0{,}9 = 2808, \text{ гривень}$$

Витрати на технічне й організаційне адміністрування та сервіс системи (Стос)

$$C_{тос} = 8500, \text{ гривень}$$

Витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу (Со)

$$C_o = 10550, \text{ гривень}$$

$$C_к = 169358, \text{ гривень}$$

де $C_{ак}$ – витрати, викликані активністю користувачів системи.

$$C_{ак} = 128\ 180, \text{ гривень}$$

Річні поточні (експлуатаційні) витрати на функціонування системи

$$C = 128\ 180 + 169358 + 58500 = 356038, \text{ гривень}$$

4.2 Економічне обґрунтування доцільності розробки

85% доходу соціальної мережі доводиться на розміщення реклами, в тому числі доходи від кампаній, що запускаються найбільшими брендами.

Решта приносять платежі від підприємств, які на платформі соціальної мережі розробляють платні програми (наприклад, ігри).

На сьогодні майданчик найбільших мереж використовує понад 3 млн. активних рекламодавців для розміщення оголошень хоча б один раз протягом 28 днів.

Середня ціна за текстове оголошення із зображенням:

– CPC: оплата за клік – 8,6 гривень:
– CPM: оплата за 1000 показів – 5,4 гривень.

Мінімальний бюджет на добу – 27 гривень або 837 гривень на місяць.

В середньому на кожному зі своїх користувачів великі мережі заробляють 135 гривень на рік.

З огляду на те, що кількість користувачів тільки однієї мережі на сьогодні досягає 2 млрд., її дохід становить 270 млрд. гривень на рік.

Використання алгоритму детектування шкідливих акаунтів в соціальних мережах, розробленого в дипломній роботі, робить мережу більш стабільною та безпечною. Це сприяє залученню нових рекламодавців і, відповідно, збільшення доходу соціальної мережі.

4.3 Висновки до економ розділу

Під час розрахунків було підраховано витрати на створення програмного продукту які склали:

- капітальні витрати склали: 527291,3 грн
- поточні витрати склали: 356038 грн

Було розраховано витрати на розроблення та інтеграцію програмної системи для виявлення шкідливих акаунтів у соціальних мережах, а також доцільність створення та використання.

ВИСНОВКИ

У дипломній роботі запропоновано актуальне для кібербезпеки соціальних мереж рішення, що стосується розробки нового методу детектування шкідливих акаунтів (ботів). В ході вирішення поставленого завдання були отримані наступні аналітичні та практичні результати:

1) виконано аналіз сучасних методів детектування з використанням різних підходів розпізнавання образів, математичних моделей. Проведено порівняння результатів тестування існуючих методів, яке показало, що в більшості з них робота здійснюється з певним обсягом даних, характерні істотні похибки, потрібні складні математичні розрахунки, відсутня варіативність прийняття рішень. У зв'язку з цим виникла необхідність в розробці нового алгоритму детектування шкідливих акаунтів, що дозволяє зменшити кількість зайвих перевірок користувачів;

2) проведено аналіз методів кластеризації, враховуючи їхні переваги і недоліки, з метою вибору найбільш ефективних для вирішення завдань, поставлених у дипломній роботі;

3) сформульовано формальні вимоги до вибору методів детектування, визначені критерії, за якими визначається ступінь приналежності аккаунту до соціальних ботів;

4) запропоновано метод для поліпшення якості сортування акаунтів з подальшим аналізом результатів і прийняттям рішень по окремих групам користувачів;

5) запропоновано комбінований метод відстеження поведінки підозрілих акаунтів в мережі, що дозволяє значно зменшити кількість додаткових перевірок;

6) розроблено алгоритм детектування шкідливих акаунтів на базі методів, що обрані для вирішення поставлених завдань;

7) доведено економічну доцільність розробки і впровадження розробленого алгоритму.

З практичної точки зору запропонований алгоритм може бути використаний для інтегрування в існуючу систему детектування шкідливих акаунтів в соціальних мережах для поліпшення аналізу та розпізнавання даних.

Для остаточного висновку про ефективність розробленого алгоритму необхідно проведення ретельного тестування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, Matei Ripeanu. The Socialbot Network: When Bots Socialize for Fameand Money / University of British Columbia Vancouver, Canada, 2011. – 1 с.
2. Korrespondent.net – Продажа ботов в Twitter стала многомиллионным бизнесом – исследование. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: https://korrespondent.net/business/web/1540808-prodazha-botov-v-twitter-stala-mnogomillionnym-biznesom-issledovanie (дата обращения 15.11. 2017)
3. Carlo De Micheli, Andrea Stroppa. Twitter and the underground market / 11th Nexa Lunch Seminar, May, 2013.— 5–9 с.
4. Topmarketing.by – Честное SMM-продвижение, выявляем аккаунты-боты в социальных сетях. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://topmarketing.by/internet-marketing/chestnoe-smm-prodvizhenie-vyyavlyaem-akkaunty-boty-v-socialnyx-setyax.html (дата обращения 14.11. 2017)
5. Cossa.ru – Использование ботов (технических аккаунтов) в работе с отзывами. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://www.cossa.ru/155/12121/ (дата обращения 12.11. 2017)
6. Alex Hai Wang. Detecting Spam Bots in Online Social Networking Sites: A Machine Learning Approach / College of Information Sciences and Technology The Pennsylvania State University, USA, 2010. — 2–10 с.
7. R. Nithin Reddy, Nitesh Kumar. Automatic Detection of Fake Proles in Online Social Networks / Department of Computer Science and Engineering National Institute of Technology Rourkela, Orissa, India, May, 2012. — 10–15 с.
8. Inosmi.ru – Бот в твиттере оказался настолько убедительным, что люди начали сочувствовать «ей». [Электронный ресурс] : [Веб-сайт]. – Режим

доступа: http://inosmi.ru/world/20120627/194149517.html (дата обращения 15.11. 2017)

9. Basegroup.ru, BasegroupLabs – Введение в SocialMining. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://www.basegroup.ru/library/web_mining/introduction_in_social_mining (дата обращения 16.11. 2017)
10. Wikipedia.org. Сводная энциклопедия – Кластерный анализ. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://ru.wikipedia.org/wiki/Кластеризация (дата обращения 15.11. 2017)
11. Wikipedia.org. Сводная энциклопедия – Задача классификации. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://ru.wikipedia.org/wiki/Задача_классификации (дата обращения 15.11. 2017)
12. Securitylab.ru SecurityLab – Технология Honeypot. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://www.securitylab.ru/analytics/275420.php (дата обращения 13.11. 2017)
13. Zi Chu, Steven Gianvecchio, Haining Wang, SushilJajodia. Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg? / IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, 2012. – 2-10 с.
14. Alex Hai Wang. DON'T FOLLOW ME: SPAM DETECTION IN TWITTER / College of Information Sciences and Technology, The Pennsylvania State University, Dunmore, USA, 2012. – 2-7 с.
15. Wikipedia.org. Сводная энциклопедия – Scaleogram. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://ru.wikipedia.org/wiki/Scaleogram (дата обращения 11.11. 2017)

16. Wikipedia.org. Сводная энциклопедия – JSON. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://ru.wikipedia.org/wiki/JSON (дата обращения 11.11. 2017)
17. J. Ratkiewicz, M. D. Conover, M. Meiss, B. Gonc¸alves, A. Flammini, F. Menczer. Detecting and Tracking Political Abuse in Social Media / Center for Complex Networks and Systems Research School of Informatics and Computing Indiana University, Bloomington, IN, USA, 2011. — 2-5 с.
18. Wikipedia.org. Сводная энциклопедия – Теорема Байеса. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://ru.wikipedia.org/wiki/Теорема_Байеса (дата обращения 12.11. 2017)
19. Ibm.comПрограммное обеспечение IBM – Анализ социальных сетей – техническая публикация. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://public.dhe.ibm.com/software/dw/ru/download/ZZW03070.pdf (дата обращения 15.11. 2017)
20. Haijian Shi**.** Best-first Decision Tree Learning / The university of Waikato, Hamilton, NewZealand, 2007. — 5 с.
21. Wikipedia.org. Сводная энциклопедия – Дерево принятия решений. [Электронный ресурс] : [Веб-сайт]. – Режим доступа: http://ru.wikipedia.org/wiki/ Дерево_принятия_решений (дата обращения 12.11. 2017)

ДОДАТОК А

Перелік документів на оптичному носії

1. Титульна сторінка.doc
2. Завдання.doc
3. Реферат.doc
4. Зміст.doc
5. Вступ.doc
6. Розділ 1.doc
7. Розділ 2.doc
8. Розділ 3.doc
9. Розділ 4.doc
10. Висновки.doc
11. Список використаної літератури.doc
12. Додаток А.doc
13. Додаток Б.doc
14. Додаток В.doc
15. Презентація.pptx

ДОДАТОК Б

ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник розділу доц. Волотковська Ю.О.

(підпис) (ініціали, прізвище)

ДОДАТОК В

ВІДГУК
на дипломну роботу магістра

студента Смолича Дмитра Сергійовіча гр. 125м-16-1

(прізвище, ім’я)

на тему: ***Методи детектування шкідливих акаунтів в соціальних мережах***

Мета дипломної роботи – підвищення ефективності методів детектування шкідливих акаунтів в соціальних мережах.

Тема дипломної роботи безпосередньо пов’язана з об’єктом діяльності фахівця за спеціальністю 125 Кібербезпека – розвиток методів детектування акантів в соціальних мережах.

Задачі дипломної роботи (класифікація акантів в соціальних мережах, аналіз впливу ботів на соціальні мережі, аналіз методів і засобів збору та класифікації даних, аналіз методів виявлення шкідливих акантів, обґрунтування вибору методів кластеризації, розробка алгоритму детектування шкідливих акаунтів в соціальних мережах) віднесені в освітньо-кваліфікаційній характеристиці магістра до класу евристичних, вирішення яких основане на знаково-розумових уміннях фахівця.

Оригінальність запропонованих рішень полягає у розробці адаптованого алгоритму детектування акантів у випадках неоднозначної класифікації.

Практичне значення результатів проектування полягає у підвищенні лояльності до користувачів при забезпечені безпеки соціальних мереж.

До недоліків дипломної роботи відносяться:

– недостатньо обґрунтовано вибір базових методик;

– не в повному обсязі проведено випробування запропонованої методики.

Оформлення пояснювальної записки до дипломного проекту виконано з деякими відхиленнями від стандартів.

Ступінь самостійності виконання дипломної роботи висока.

За час дипломування Смолич Д.С. виявив себе фахівцем, здатним самостійно, на високому рівні вирішувати поставлені задачі.

В цілому дипломна робота виконана у відповідності до вимог, що ставляться до дипломної роботи магістра, заслуговує оцінки “добре”, а Смолич Д.С. присвоєння йому кваліфікації професіонал із організації інформаційної безпеки.

Керівник спеціальної частини
дипломної роботи магістра,
старший викладач _____ О.В. Кручінін

Керівник дипломної
роботи магістра,
д.ф-м.н., професор _____ Т.С. Кагадій

“____”_____201__р.

ДОДАТОК Г

Зведена таблиця характеристик українських соціальних мереж

Соц. сеть	Год начала рабоы	Оценка экспертами	Количество пользователей
https://www.facebook.com/	2006	Хорошо оптимизирован	На апрель 2017 года месячная аудитория сети составляет 1,968 миллиарда человек
http://www.vk.com	2006	Хорошо оптимизирован	на август 2017 среднесуточная аудитория составляет более 80 миллионов посетителей
http://www.yachudo.com/	(бета тест 2010) релиз 2017	- Большое время отклика сервера - Код подключения JavaScript и CSS, блокирующий отображение верхней части страницы. Страница начинает отображаться, только после загрузки этих файлов	Информация не предоставляется
Ц.укр	Информация не предоставляется	Сайт блокируется браузером (рис.1.1)	Информация не предоставляется
https://ukropen.net/	2015	- Большое время отклика сервера - не оптимизирован под устройства разного типа	80 000 пользователей
http://ukrainci.org.ua/home.php	2009	-	50 000 пользователей
http://ukrface.com.ua/	2014	- Оценка сайта 68% (по версии pr-cy) - Большое время отклика сервера - не оптимизирован под устройства разного типа	100 000 пользователей

ДОДАТОК Д

Приклад вибірки користувачів соціальної мережі з показниками

Пользователь	**Блоированный профиль**	**Количество друзей**	**Заполненность профиля (%)**	**Публикации пользователя (посты свои/к общему числу постов)**
Дмитрий Гвоздецкий	0	67	100	0,77
Рита Ищенко	1	461	100	0,07
Никта Кот	0	120	60	0,97
Юра Стасюк	0	78	80	0,99
Маша Леонова	0	560	90	0,68
Игорь Белкин	0	1012	100	0,43
Иван Лазебников	0	71	50	0,83
Миша Рудой	0	0	20	0,01
Анастасия Ковш	1	2	10	0,33
Алина Юрченко	0	603	100	0,97

Пользователь	**Время существования аккаунта**	**Вредоносные ссылки**	**Жалобы на аккаунт**	**Активность пользователя (активност/ t существоваания аккаунта)**
Дмитрий Гвоздецкий	68424	0	0	0,13
Рита Ищенко	70124	0	20	0,25
Никта Кот	50624	0	0	0,17
Юра Стасюк	21345	0	0	0,10
Маша Леонова	76101	0	0	0,20
Игорь Белкин	80131	0	0	0,10
Иван Лазебников	30154	0	0	0,10
Миша Рудой	10087	0	0	0,12
Анастасия Ковш	5678	1	26	0,34
Алина Юрченко	59456	0	0	0,10

Пользователь	Время существования аккаунта	Вредоносные ссылки	Жалобы на аккаунт	Активность пользователя (активност/ t существоваания аккаунта)
Дмитрий Гвоздецкий	68424	0	0	0,13
Рита Ищенко	70124	0	20	0,25
Никта Кот	50624	0	0	0,17
Юра Стасюк	21345	0	0	0,10
Маша Леонова	76101	0	0	0,20
Игорь Белкин	80131	0	0	0,10
Иван Лазебников	30154	0	0	0,10
Миша Рудой	10087	0	0	0,12
Анастасия Ковш	5678	1	26	0,34
Алина Юрченко	59456	0	0	0,10

ДОДАТОК Г

Схема роботи модуля прийняття рішень