Міністерство освіти і науки України
Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА
Дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній рівень ***магістр***
(назва освітнього рівня)

кваліфікація
(код і назва кваліфікації)

на тему: *Удосконалений метод виявлення недостовірної інформації в інформаційному просторі*

Виконавець: студент *2* **курсу, групи** *КБм-21*

(підпис) *Швець Дар'я Юріївна* (прізвище ім'я по-батькові)

	Прізвище, ініціали	Оцінка	Підпис
Науковий керівник	*Лаптєв О. А.*		
Рецензент			
Нормоконтроль	*Фесенко А. О.*		

Київ 2022

Міністерство освіти і науки України

Київський Національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту інформації

_____ Лукова-Чуйко Н.В.

«_____»_____20___року

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту *КБм-21* (група) *Швець Дар'ї Юріївній* (прізвище ім'я по-батькові)

Тема дипломного *Удосконалений метод виявлення недостовірної інформації в інформаційному просторі.*

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 29.10.2021

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт *Процес оцінки достовірності повідомлень в просторі під час передачі інформації від першоджерела до користувача.*

Предмет досліджень *Метод визначення достовірності повідомлень в інформаційному просторі під час передачі інформації від першоджерела до користувача.*

Мета *Підвищення ефективності виявлення недостовірної інформації та припинення її розповсюдження в умовах інформаційного протиборства.*

Вихідні дані для проведення роботи *Методи виявлення недостовірної інформації в інформаційному просторі.*

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *Удосконалення виявлення недостовірної інформації в інформаційному просторі за допомогою методу бджолиної колонії.*

Практична цінність *Покращення системи боротьби з недостовірною інформацією.*

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Розробка плану для досягнення мети роботи.	29.10.2021 – 31.10.2021
Збір даних для кваліфікаційної роботи.	01.11.2021 – 15.11.2021
Аналіз літературних джерел.	16.11.2021 – 01.12.2021
Розробка методу виявлення недостовірної інформації в інформаційному просторі.	02.12.2021 – 02.01.2022
Розробка і написання програмного коду.	03.01.2022 – 02.02.2022
Написання першого розділу роботи.	03.02.2022 – 02.03.2022
Написання другого розділу роботи.	03.03.2022 – 02.04.2022
Написання третього розділу роботи.	03.04.2022 – 02.05.2022
Підготовка ілюстративного матеріалу.	03.05.2022 – 10.05.2022
Оформлення і друк пояснювальної записки.	11.05.2022 – 14.05.2022

Завдання видав _____ *Лаптєв О. А.*
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ *Швець Д. Ю.*
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____
Термін подання дипломної роботи до ЕК _____

УДК 004.492.2

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Удосконалений метод виявлення недостовірної інформації в інформаційному просторі»: 72 сторінок, 11 рисунків, 10 додатків та 3 таблиці, 36 літературних джерел.

Об’єкт дослідження – процес оцінки достовірності повідомлень в інформаційному просторі під час передачі інформації від першоджерела до користувача.

Мета роботи – підвищення ефективності виявлення недостовірної інформації та припинення її розповсюдження в умовах інформаційного протиборства.

Методи дослідження – біоінспіровані методи, метод бджолиної колонії.

У роботі досліджено сучасні загрози та методи протидії недостовірної інформації. Проведено аналіз ринку рішень, завдяки яким можна підвищити якість інформаційного простору. Запропоновано удосконалений метод виявлення недостовірної інформації. Написаний код методу бджолиної колонії, який пропонується як удосконалений.

Наукова новизна: удосконалено метод виявлення недостовірної інформації у інформаційному просторі за допомогою біонсіпрованих методів, а саме методу бджолиної колонії, що дозволяє підвищити якість мережі Інтернет.

Актуальність теми: проблеми масової комунікації та доступніть ЗМІ впливають на суспільне життя і майбутнє самої держави загалом і реалізуються у вигляді маніпуляції свідомістю. Існує багато різних теорій про способи та методи управління свідомістю мас. Саме це обумовлює актуальність роботи щодо виявлення недостовірної інформації.

Ключові слова: метод бджолиної колонії, алгоритм оптимізації, генетичні алгоритми, безпека інформаційного простору.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ГА	–	Генетичні алгоритми
ЗМІ	–	Засоби масової інформації
ІБ	–	Інформаційна безпека
ІТС	–	Інформаційно-телекомунікаційні системи
ЦФ	–	Цільова функція
ABC	–	Artificial Bee Colony
ACO	–	Ant Colony Optimization
IDS	–	Intrusion Detection System
TACS	–	Trust Ant Colony System
PR	–	Public Relations

ВСТУП

Актуальність. Масова комунікація грає у розвитку сучасного суспільства величезну роль. Дедалі більше інформації приймає людина від засобів. В даний час вони взяли на себе значну частину функцій щодо формування свідомості людей, виховання їх ціннісних орієнтацій, смаків, поглядів, звичок, уподобань.

ЗМІ у вигляді інформації впливають як свідомість і думка особистості, а й свідомість мас, т. е. ставлення різних груп людей до подій і процесам, що відбуваються в суспільному житті і зачіпають їх інтереси та потреби. Вони є одним з основних факторів, здатних вплинути на народні настрої.

Саме через такі великі можливості ЗМІ стали називати «четвертою владою». В умовах величезного впливу ЗМІ на суспільну свідомість стала гостро відчуватиметься сукупність низки проблем інформаційної безпеки, таких як: існування особистостей, переважно політично значимих, зацікавлених у маніпулюванні масовою свідомістю та рухом народних мас, та наявність журналістів, готових допомогти їм із реалізацією цієї мети.

ЗМІ грають чималу роль формуванні політичної свідомості громадян. За допомогою грамотної PR-компанії політичні партії та їхні лідери здатні значною мірою вплинути на хід та результат народного голосування, а оскільки є можливість отримання недостовірної інформації про кандидатів на вибори, постає і небезпека того, що люди можуть зробити неправильний вибір, що вплине на подальший перебіг розвитку держави.

Всі ці проблеми значною мірою впливають на суспільне життя і майбутнє самої держави загалом і реалізуються у вигляді маніпуляції свідомістю. Існує багато різних теорій про способи та методи управління свідомістю мас. Саме це обумовлює актуальність роботи.

З плином часу виникає необхідність пошуку нових методів та вдосконалення існуючих методів виявлення недостовірної інформації. З цим завдання можуть

впоратись також біоінспіровані методи, до яких відноситься і метод бджолиної колонії.

Метою роботи є підвищення ефективності виявлення недостовірної інформації та припинення її розповсюдження в умовах інформаційного протиборства.

Об'єктом роботи є процес оцінки достовірності повідомлень в інформаційному просторі під час передачі інформації від першоджерела до користувача.

Предметом роботи є метод визначення достовірності повідомлень в інформаційному просторі під час передачі інформації від першоджерела до користувача.

В ході роботи необхідно вирішити наступні **завдання**:

- визначити роль достовірності інформації і її значення в інформаційному просторі;
- дослідити відомі біоінспіровані методи;
- дослідити можливість використання методу бджолиної колонії до вирішення поставленного завдання;
- розробити алгоритм методу бджолиної колонії для виявлення недостовірної інформації в інформаційному просторі;
- провести удосконалення алгоритму;
- зробити аналіз отриманих результатів.

Перелік **питань**, які розроблені під час роботи:

- здійснити порівняльний аналіз існуючих моделей щодо оцінювання достовірності інформації;
- дослідження існуючих методів щодо оцінювання достовірності інформації;
- розробити методику виявлення недостовірної інформації та припинення її розповсюдження в інформаційному просторі.

РОЗДІЛ 1
ІНФОРМАЦІЙНИЙ ПРОСТІР І ЗАБЕЗПЕЧЕННЯ ЙОГО БЕЗПЕКИ

1.1 Значення інформаційного простору у формуванні громадської думки

Протягом другої половини XX ст. багато економічно розвинених країн поступово перейшли до того, що отримало назву «інформаційне суспільство», «століття інформації» або «постіндустріальна епоха». Цей перехід складається з ряду взаємопов'язаних елементів. В економіці виробництво як джерело багатства все більшою мірою замінює сфера обслуговування. Роль інформації та інтелекту, втілених як у людях, так і у все більш розумних машинах, стає всеосяжною, а розумова праця все більше замінює фізичну. Виробництво глобалізується в міру того, як недорогі інформаційні технології роблять усе більш легким поширення інформації через національні кордони, а засоби швидкого зв'язку – телебачення, радіо, факс та електронна пошта – розмивають кордони стійко існуючих протягом тривалого часу культурних спільнот. Суспільство, що базується на інформації, усе більшою мірою сприяє зростанню свободи і рівності – двох речей, які люди в сучасній демократія цінують найбільше [12, с. 157].

Доводячи тезу про «Третю хвилю», Е. Тоффлер зазначає, що зараз ми не отримуємо готову ментальну модель реальності, а змушені постійно формувати її і переформовувати. Це є для нас важким тягарем, але водночас веде до більшої індивідуальності, демасифікації як особистості, так і культури. Демасифікація цивілізації, відображенням і посиленням якою є засоби інформації, тягне за собою значне збільшення обсягу інформації, якою ми обмінюємося один з одним. І це зростання пояснює, чому ми стаємо «інформаційним суспільством» [11, с. 180, с. 89].

В інформаційному суспільстві кардинально змінюються всі сфери життя: від технологічної та виробничої до економічної і культурної. Істотно змінюються форми мислення та світогляду. Швидкість технічного та концептуального

оновлення технічних засобів і управління ними зростає за експоненційною кривою. У той самий час уніфікуються технологічні стандарти, що дозволяє збільшити конкурентний відбір як у сфері власне технічній, так і у сфері виробництва програмного забезпечення. Інформаційне суспільство – це технокомунікаційна частина постіндустріального суспільства, таке суспільство, де сфера послуг має пріоритетне значення щодо промислового виробництва і аграрного сектору. Головними продуктами виробництва і споживання є інформація і знання [15, с. 440, с. 219].

Цифрові інформаційні потоки та комунікативні технології необхідні для ефективної роботи вузлів і частин мережевого суспільства. Поняття «мережеве суспільство» стає все більш затребуваним у міру прискорення інформаційної революції. Це пов'язано з перманентною модернізацією економіки і ускладненням соціальної структури постіндустріального суспільства. З появою радіо і телебачення виникли необхідні інфраструктурні та організаційні передумови для формування комплексних інформаційних мереж. Створення і експоненціальне зростання мережі Інтернет, її інтеграція з радіомережами і телебаченням, економічні ефекти мережевої діяльності спровокували наукові та філософські суперечки про значущість мереж для сучасного суспільства.

Усе більш широке використання мережевих комунікацій може стати причиною виникнення якісно іншої суспільно-політичної системи. Особливим результатом телекомунікаційної революції стала заміна однолінійного зв'язку між відправником і одержувачем інформації багатофункціональним і діалоговим зв'язком, що створює нові можливості для участі в інформаційному обміні. Аналіз політичних технологій у західних країнах підтверджує, що подібні нововведення розцінюються як спосіб демократії. Цей феномен одержав назву «телеполітика», «теледемократія», «відеодемократія». Апологети такої системи підкреслюють можливість громадян самим вирішувати всі політичні і соціальні проблеми, що їх цікавлять, а не делегувати свої права обраним представникам (депутатам) [5, с. 10].

Якщо природна інформація, автором якої є природа, створює можливості для творчості, а людина на базі цих можливостей розробляє практичні варіанти

застосування природної інформації у вигляді знань, то соціальна інформація і є основою соціально-економічного прогресу, а людина є в цьому процесі творчим посередником між інформацією і знаннями, перетворюючи загальнонаукове на індивідуальне, яке або привласнює собі, або перетворює на суспільне надбання у вигляді навої, але вже соціальної інформації. Такий підхід до розуміння термінів «інформація» і «знання» відкриває нові методологічні можливості трактування методів організації трудових процесів людини в сучасних умовах [10, с. 16-20].

Для перетворення суспільства на сучасне інформаційне суспільство важливим є не лише обсяг інформації, не лише інтенсивність обігу інформації та обміну інформацією, але й її якісні показники. Інформаційне суспільство відрізняється від суспільства, засміченого спотвореною інформацією, перш за все тим, що визначальний вплив на розвиток різних галузей та сфер здійснює саме обіг інформаційно-інтелектуальних ресурсів. Коли ж обіг інформації зростає, але відсоток інтелектуальних знань у її загальному обсязі не збільшується або ж навіть скорочується, тоді таке суспільство навряд чи зможе утриматися на шляху до формування сучасного інформаційного суспільства.

Для становлення інформаційного суспільства дуже важливою є якість інформації, а також те, наскільки складно чи просто здобути повну, всебічну та об'єктивну інформацію серед величезної кількості спотворених, напівправдивих, неповних та перекручених даних. Зрозуміло, що спотворена та перекручена інформація становить слабку основу для обговорення в суспільстві найбільш актуальних та важливих тем і проблем. Рішення та нормативно-правові акти, створені на основі такої низькоякісної та неповної інформації та й до того ж без загального, фахового та експертного обговорення, будуть неоптимальними, вкрай неефективними і такими, що неадекватно відображають реальний стан та рівень розвитку певної сфери суспільних відносин. Зрозуміло, що й коефіцієнт корисної дії таких рішень, такого правового врегулювання буде вкрай низьким, якщо взагалі буде позитивний ефект [4, с. 17-21].

Водночас основна моральна проблема інформаційного суспільства полягає в тому, що комунікація перестала бути справжньою. Інтенсивність інформаційних

потоків, швидка зміна ціннісних і ідеологічних пріоритетів, ставка на фактичність і сенсаційність, байдужість до духовних цінностей призводять до того, що комунікація стає формальною і вихолощеною, позбавленою людського начала.

Інформаційна картина світу з властивими їй ціннісними настановами радикально відрізняється від картини світу традиційної моралі. Більше того, основні духовно-етичні кризові процеси, що відбуваються в сучасній інформаційній цивілізації, пов'язані якраз із гіпертрофованим технічним розвитком людства, і далеко не в останню чергу – з безконтрольним і хаотичним зростанням інформації в сучасному суспільстві. Можна сказати, що стало аксіоматичним таке положення: сучасна моральна ситуація утворилася внаслідок дистанцій, яка дедалі збільшується, між науково-технічним прогресом і етичним станом суспільства.

Сьогодні доступ до інформації – фундамент соціальності, основа громадянського суспільства. Це виявляється у володінні світовим контентом, свободі знати, оцінювати, голосувати, керувати, приймати рішення. Сучасна людина отримала більш широкі права й реальну можливість заволодіти світовою увагою, втрутитися у світові сценарії, оцінювати їх і транслювати світові свою оцінку того, що відбувається, створювати власні версії, діяти і закликати до соціальної дії. Для цього немає необхідності бути формально організованим представником громадянського суспільства.

Однак необхідно зазначити, що до інформаційної революції специфіка комунікативних технологій, які здійснювали найвагоміший вплив на свідомість людей (радіо, телебачення), характеризувалась односторонньою спрямованістю від суб'єкта до об'єкта контролю та мала лінійний характер. За такого типу інформаційної дії відбувається розподіл, доведення інформації з центру до периферій, тоді як її рух іншими напрямами і назад до центру є надзвичайно ускладненим. Протягом історії розвитку комунікативних технологій, особливо в індустріальному суспільстві, панував саме такий тип траєкторії руху інформації в соціальних системах.

За такого – лінійного характеру поширення інформації носієм інформаційної влади в суспільстві є ЗМІ, інформаційні та рекламні агентства, піар-компанії, а

також інститути соціалізації. Інформаційний контроль виявляється через управління комунікаціями, їх змістом і спрямованістю за допомогою інформації. Інформаційна влада відрізняється від звичайного інформаційного впливу силою та стійкістю впливу суб'єкта на об'єкт, високою мірою контролю його поведінки. Зазначимо, що комунікації здійснюють визначальний вплив, у тому числі й на політичну поведінку [6, с. 138-146].

Глобальна мережа Інтернет як принципово новий засіб масової комунікації увійшла в життя людей відносно недавно – наприкінці минулого сторіччя. За короткий час ця новітня інформаційна технологія поширилася настільки, що стала активно застосовуватися у всіх сферах життєдіяльності людини та суспільства. Мережа Інтернет стала невід'ємною складовою частиною інформаційного простору сучасної культури, причому її значущість постійно зростає. Спеціалізована інформаційна комп'ютерна мережа за короткий термін набула рис соціальної системи, основною функцією якої є комунікація.

Мережа Інтернет формує віртуальні спільноти, стирає кордони між державами, елімінує відстані, що роз'єднують людей і, в остаточному підсумку, створює навколо себе специфічну форму культури – кіберкультуру. У цьому специфічному інформаційному середовищі діють особливі етичні принципи та засновані на них правила поведінки. Сучасні інформаційні технології, які лежать в основі функціонування засобів масової комунікації та стали новим щаблем відносин «людина – техніка – суспільство», створюють новий культурний простір. Однією з його особливих рис є трансформація традиційних поведінкових стереотипів, головним чином у тих сферах соціокультурного життя, що пов'язані зі спілкуванням.

Необхідно зазначити, що перехід до нових можливостей комунікативної взаємодії можна розглядати у двох аспектах – позитивному, або демократичному, та негативному. Соціальний контроль у демократичних суспільствах зазнає істотної зміни з приходом ери мережі Інтернет; нові потужні інформаційні засоби для здійснення політичних цілей роблять актуальними такі поняття, як інформаційна

безпека та інформаційна війна; поряд з цим набувають нового поширення можливості використання нових демократичних методів соціального контролю.

Інформація, як властивість об’єктивної реальності, забезпечує процес пізнання цієї реальності у всіх її проявах. Саме ця властивість, поряд з властивістю відображення, забезпечує об'єктивний і необхідний зв'язок між об'єктивним світом, тобто постійно рухається в просторі й часі матерією і її породженням – ідеальною свідомістю, остаточно замикає ланцюжок процесу пізнання, представляючи її у вигляді: матерія – інформація – комунікація – пізнання.

Зазначимо також ще одну особливість соціальної інформації. Оскільки вона є властивістю, породженням високоорганізованої матерії (індивіда, особистості як соціального суб'єкта), то тільки цей індивід може визначити спосіб її подальшого використання: передача іншим соціальним суб'єктам або особисте споживання.

Передачу добутої соціальної інформації індивід може здійснювати за безпосередньої особистої взаємодії (комунікації) з іншими соціальними суб'єктами або за допомогою різних допоміжних технічних засобів: засобів індивідуальної або масової комунікації (у тому числі ЗМІ). Тобто засоби індивідуальної та масової комунікації не є самостійними джерелами соціальної інформації, а є лише її передавачами. А саму соціальну інформацію формують певні особи і (або) спільності людей.

Доступність засобів масової комунікації, зрозумілість знань про світ забезпечили можливість відносного вирівнювання різних за соціально-статусними характеристиками груп щодо рівня інформованості про життя суспільства. Відповідно до соціальної стратифікації суспільства склалося дві основні наукові парадигми бачення впливу засобів масової комунікації як виразника соціальної структури суспільства, системи суспільної свідомості: 1) парадигма тотального впливу на інертну, пасивну аудиторію з метою реалізації інтересів престижних соціальних груп (таких, що володіють значною частиною різних типів капіталу, зокрема капіталу символічного); 2) парадигма часткового впливу на соціокультурно-гетерогенну і диференційовану аудиторію.

Більш перспективним є підхід до соціальних медіа як до довгострокових інструментів, що можуть зміцнити громадянське суспільство та громадську сферу. Прагнучі ініціювати наукову полеміку щодо проблеми, дослідник К. Ширкі висуває два заперечення ідеї про те, що соціальні медіа впливають на національну політику. По-перше, ці інструменти самі по собі неефективні, а по- друге, вони несуть стільки ж шкоди для демократизації, скільки й користі, тому що репресивні уряди вчаться використовувати їх для придушення інакомислення. К. Ширкі зазначає, що активісти різних режимів, як демократичних, так і авторитарних, використовуватимуть соціальні медіа для досягнення змін у своїх державах. І можливості впливу або керування цим процесом обмежені. Для досягнення довгострокових переваг від соціальних медіа необхідно переключитись від інструментального до середовищного підходу, хоча це й може призвести до розчарування у короткостроковій перспективі [11, с. 180, с. 79-85].

Однією із сучасних технологій впливу на людину є хай-х'юм-технології, тобто високі соціогуманітарні технології, основне призначення яких полягає у впливі на свідомість індивідів або груп з метою зміни їх поведінки і взаємин. Технології хай-х'юм є результатом конвергенції соціальних та інформаційних технологій, а також новітніх досягнень у галузі психології, нейрофізіології, етології та інших наук.

І. В. Лисак зауважує, що до хай-х'юм-технологій можна віднести маркетингові та бізнес-технології, також до хай-х'юм-технологій вона відносить піар-технології, високі політтехнології, технології інформаційних війн. Хай-х'юм-технології дозволяють ефективно прогнозувати соціально-політичні зміни і керувати ними. Однією з ефективних технологій інформаційної війни є, наприклад, руйнування механізмів традиційної самоідентифікації (етнонаціональної, культурної, конфесійної та ін.) через проектування в інформаційному просторі штучних варіантів ідентифікації, зокрема «мультикультурної ідентичності» [8, с. 258-263].

Наслідки застосування хай-х'юм-технологій двоїсті. З одного боку, вони дозволяють ефективно управляти соціальними процесами, дають можливість довільно перебудовувати масову та індивідуальну свідомість, що в економічній сфері дозволяє отримати суттєвий матеріальний прибуток, а у сфері політичний –

ефективно керувати великими масами людей. З іншого боку, хай-х'юм-технології здатні чинити деструктивний вплив на людину і суспільство, руйнувати механізми їх саморегуляції. Причому ці технології можуть негативно вплинути не тільки на об'єкти їх безпосереднього впливу, але й на осіб, які їх застосовують [8, с. 258-263].

Ще однією небезпечною технологією масофікації інформаційного продукту є резонансні технології, бо саме вони застосовуються з урахуванням позиції і реакції отримувача інформації, тобто аудиторії. Використання резонансних технологій зумовлює різке зростання довіри до повідомлення, у якому зміст (і, імовірно, форма) зовнішнього впливу наближався би до змісту (і форми) того, що саме очікує отримувач інформації. Силу резонансу в масовій комунікації можна відчути тоді, коли змодельоване спеціалістом у теорії комунікації повідомлення потрапляє в масові очікування. Сила резонансної технології не в тому, що вона подає нову інформацію, а в тому, що вона відповідає тим уявленням, які вже сформувалися в масовій свідомості. Резонансні технології – це приклад так званої м’якої сили, що використовується у демократичних суспільствах та враховує когнітивні, комунікативні та власне резонансні схеми, за якими живе аудиторія.

О. Соловйов доводить, що для суспільств, у яких відсутні сталі демократичні традиції, виникає справді хаотичне переплетення інформаційних потоків, яке знецінює механізми комунікації влади і громадянського суспільства, котре народжується, і в результаті цього суспільство поступово втрачає знаряддя інформаційного впливу на позиції влади.

В. Ф. Чешко говорить про новий феномен впливу на людину – біовладу. Розглядаючи роботу П. Д. Тіщенко, він доходить висновку, що прогрес інформаційних технологій перетворив саме психоматичне буття людини – зміст її свідомості та генетичної програми – на об'єкт технологічного маніпулювання, а отже – соціально-політичного контролю і управління. Людина розглядається як елемент з відповідною програмою, яку можна запрограмувати відповідним чином. Також В. Ф. Чешко зазначає, що одним із найбільш істотних і потужних системоутворюючих чинників еволюції сучасної цивілізації стає глобальна біополітика. Предмет біополітики як міждисциплінарної галузі дослідження можна

визначити як дослідження феномену біовлади. Його в сучасній соціологічній і політологічній літературі розуміють як здатність (безпосередню або опосередковану громадською думкою, ЗМІ, масовою культурою і ментальністю) владних структур соціуму контролювати і маніпулювати відправленням біологічних функцій окремих індивідуумів [14, с. 440].

Потрібні дослідження і тактики протидії «тонкому» маніпулюванню. Усе більше сигналів надходить про те, що конструювання починає застосовуватися на високих і тонких рівнях людської свідомості. Комп'ютери вчаться за енцефалограмами розпізнавати і моделювати рух аксонів і нейронів у людському мозку. З'являються дисципліни з галузі «хай-х'юм» – тобто щось, що високотехнологічно працює з тим, що становить особливість власне людського («х'юм») – пам'яттю, свідомістю, переконаннями, здатністю прийняття рішень, уявою. І хоча основним способом протидії такому маніпулюванню є безпосередньо виховання людини, потрібні також техніки культурної інтелігенції, методи проти управління сприйняттям, гіпнозу і зомбування. Першим кроком до створення таких технік буде інформація про те, як усе це діє.

Найбільш ефективними, порівняно з іншими чинниками формування ціннісної системи, є мас-медіа, які впливають на формування ціннісних орієнтацій суспільства. Медіа задають певні аксіологічні моделі поведінки, з якими реципієнти співвідносять свої моральні принципи, ціннісні орієнтири і навіть виробляють стереотипи мислення під впливом трансльованих зразків. За дослідженням А. Кавалерова, 82% респондентів зазначають, що найбільш потужно на їхні ціннісні орієнтації впливає не навчальний процес, а телебачення [3, с. 99].

Таку ситуацію можна пояснити тим, що сприймання медійних продуктів є невіддільною частиною повсякденного життя сучасних людей, яка за кількістю витраченого на неї часу перебуває на другому місці серед усіх видів активності, поступаючись лише праці. В інформаційну епоху саме засоби масової комунікації стають основним каналом отримання інформації, способом залучення реципієнта до реальної дійсності та її подій. Сьогодні зростає доступність і значущість інформаційних потоків. Мас-медіа поступово перетворюються на основне джерело

інформації, що активно збільшує діапазон свого вияву. Нещодавно події реальної дійсності транслювали друковані, радіо- й телевидання. Нині цю місію активно виконує комп'ютерна мережа. В інформаційну епоху засоби масової комунікації спроможні вести діалог з будь-яким респондентом: комунікаційні технології «стирають» просторово-часові кордони, завдяки чому інформація стає все більш доступною. Практично кожний член інформаційного суспільства має можливість споживати інформацію за власними інтересами й потребами.

Перебування людей під постійним впливом небезпечної інформації викликає трансформацію психіки, зміну поглядів, думок, відносин, ціннісних орієнтацій, мотивів, стереотипів, реакції, поведінки, дії особистості, призводить до формування викривленого світогляду та ціннісної дезінформації, провокує розвиток шкідливих звичок, викликає агресію, ненависть, роздратованість, стан невизначеності, сприяє виникненню психологічного дискомфорту у споживачів інформаційної продукції, нарешті, ставить під загрозу збереження соціально-психологічного балансу та користі здорових, продуктивних сил суспільства, життєспроможної соціальної адаптації його різних верств і може завдати громадянам країни моральної, а державі політичної шкоди.

Недостатній контроль з боку держави за дотриманням законів України політичними силами, ЗМІ та окремими особами, які займаються підприємницькою діяльністю в інформаційній сфері, призводить до того, що нині трапляються непоодинокі випадки надання ефірного часу теле- та радіопрограмам, спрямованим на руйнування моральних цінностей, свідомості української нації, підривання морального і фізичного здоров'я громадян. Певна залежність ЗМІ від держави, контроль з боку фінансових чи політичних груп перетворюють вітчизняні ЗМІ на знаряддя маніпуляції суспільною свідомістю, провідників певної ідеології і, що є найнебезпечнішим, часто сприяють упровадженню чужих, не властивих суспільству духовно-моральних і політичних цінностей, що руйнує духовний фундамент її існування. Час від часу відвертаючи увагу споживачів від реальності, ЗМІ створюють для них специфічний інформаційний світ, формують певні ціннісно-

смислові моделі для засвоєння суспільством і таким чином змінюють аксіологічну картину світу соціуму.

1.2 Роль виявлення недостовірної інформації в інформаційному просторі

Інформація – це джерело влади, і демократичні системи здатні розподіляти цю владу. В цьому відношенні можливість громадян відкрито поширювати, отримувати та порівнювати інформацію сприяє свободі, оскільки це фактично є використанням фундаментальних прав: свободи слова, збори та об'єднання.

Крім того, однією з опор демократії є активна участь громадян у суспільному житті, наприклад участь у політичних процесах, таких як регулярні, Конкурентні вибори, що визначають склад уряду. У свою чергу, участь залежить від віри в інститути, що працюють на користь суспільства. Цей взаємозв'язок є «громадським договір» між громадянами та державою. Певною мірою цей договір залежить від потоку достовірної інформації, що дозволяє громадянам розуміти дії уряду та обирати варіанти дій залучення уряду до відповідальності.

Достовірність інформації життєво необхідна здоровій демократії. Хибна чи неточна інформація може негативно вплинути на громадське обговорення питань та політичні рішення громадян призводячи до порушення коректної політичної дискусії та перешкоджаючи досягненню угод. Можливість поінформованого та поважного обговорення громадянами політичних ідей та суспільно-політичних питань є ключовим аспектом збереження демократії у довгостроковій перспективі. Це повною мірою відноситься також до діалогу всередині уряду та між політиками.

Аналогічним чином, громадяни повинні розуміти роботу уряду та мати у своєму розпорядженні необхідну інформацію, щоб урядовці несли відповідальність перед ними за рішення. Поширення помилкової інформації, що вводить в оману та її використання для підриву довіри суспільства, посилення розколу та обмеження можливості громадян діяти за окремо чи спільно можна розглядати як загрозу для демократії.

Дезінформація може мати особливу руйнівну силу в період виборів, за наявності значних, що укорінилися протиріч у пріоритетах та політичних принципах. У такі періоди дезінформація може маніпулювати перевагами виборців, порушувати нормальний перебіг виборного процесу, підживлювати невдоволення та розчарування громадськості. Зрозуміло, не кожна спроба впровадження дезінформації пов'язано з особливою подією, такою як вибори.

Дезінформація також може застосовуватись для зміни загального інформаційного поля, в якому люди обговорюють питання, формують погляди та приймають політичні рішення. У деяких випадках метою дезінформації є поступове формування ширшої інформаційної картини чи перешкоджання суспільної дискусії за рахунок розбіжностей чи цинізму.

Авторитарні політичні діячі часто вдаються до різних хитрощів, щоб вплинути на розповсюдження інформації. Вони можуть закривати доступ до незалежних джерел інформації та зривати громадське обговорення, контролювати канали ЗМІ та склад трансльованої інформації, навмисно розповсюджувати дезінформацію з метою обману громадськості. Такі діячі отримують величезну вигоду від зниження суспільної довіри до своїх демократичних конкурентів та ізолювання їхню відмінність від політичних процесів.

Технічний прогрес спричинив цілий ряд тектонічних змін у процесах виробництва та споживання інформації. Інтернет, стаючи все поширенішим, швидшим і дешевшим, дав мільярдам людей можливість ділитись інформацією як ніколи легко.

Ще одним наслідком прогресу став розвиток соціальних мереж, які зробили процес споживання інформації в мережі підконтрольним кільком великим компаніям і винесли їх у громадський простір.

Зростання кількості мобільних пристроїв та скорочення циклу виробництва новин збільшили швидкість поширення інформації. Прискорений обмін інформацією, що відбувається в реальному часі між учасниками мережі в деяких випадках знижує ймовірність того, що достовірність отриманої інформації буде

поставлено під сумнів. В інших випадках потік вхідної інформації настільки величезний, що стає все складніше відрізняти достовірні відомості від брехні.

Оскільки цифрові середовища стають все більш індивідуалізованими за рахунок алгоритмів, що підбирають інформаційне вміст під смаки та переваги користувачів, недолік критичного аналізу приймає виражений характер. Ці фактори, що характеризують цифрову революцію, знизили стійкість громадськості до маніпуляцій неточною інформацією.

«Оцифрування» інформаційного простору ускладнюється тим, що людям складно пристосовуватися до швидкості технологічних змін. Обробка інформації людиною визначається психологічними факторами, та різні типи інформації викликають або раціональну, або емоційну реакцію.

Електронні ЗМІ а особливо платформи соціальних мереж, через які інформація поширюється надзвичайно швидко, можуть заохочувати емоційну обробку інформації, а не раціональні реакції, засновані на ретельній перевірці. [26, с. 477]

Зрозуміло, що маніпуляція інформацією не є чимось новим для демократичних суспільств, але цифрові технології збільшили масштаб проблеми через те, що зловмисні особи отримали можливість анонімно впливати на громадську думку та загрожувати достовірності інформації. Соціальні мережі посилюють наслідки через відносно низьку вартості та високої швидкості донесення інформації до великої аудиторії. Процесу часто сприяють автоматизовані системи, наприклад боти, просувають матеріали користувачам згідно з даними про їх демографію та особисті переваги.

Фальшиві новини - це термін, який використовують взаємозамінно з терміном «дезінформація» та, іншими словами, що позначають інші порушення інформаційної екосистеми. Зараз його застосовують у загальному сенсі щодо неточних чи сфабрикованих новин. В той же час термін «фальшиві новини» недостатньо точно відображає складність дезінформації, недостовірної інформації та шкідливоїінформації. Його часто використовують авторитарні та інші політичні

діячі у тому, щоб девальвувати неугодні факти, вплітаючи у яких хибні установки. [16, с. 12]

Дезінформація - це повідомлення помилкової інформації, створеної з наміром заподіяти шкоду фізичній особі, соціальній групі, організації чи країні. Дезінформація не обов'язково полягає у подачі відвертої брехні. У ній можуть використовуватись факти, відірвані від вихідного контексту, або факти, змішані з неправдивою інформацією.

Приклад

Каліфорнійська агенція з кібербезпеки FireEye виявила багаторічну дезінформаційну кампанію, спрямовану на Латинську Америку, Ближній Схід, Великобританію та Сполучені Штати. У соціальних мережах було створено понад 600 облікових записів користувачів із Ірану, через які здійснювали дезінформацію у глобальному масштабі. У 2018 році FireEye поділилася цією інформацією з Facebook, внаслідок чого було видалено 652 фіктивні облікові записи та сторінки за «координовану неавтентичну поведінку».

Недостовірна інформація - це помилкова інформація, яка була створена без мети завдати шкоди.

Приклад

У 2017 році після вибуху в Манчестері, Великобританія, місцева газета помилково розмістила в Twitter інформацію про те, що поруч із місцевою лікарнею помічено озброєна людина. Пізніше виявилось, що інформація не відповідала насправді, і газета видалила попереднє повідомлення. [23, с. 1006-1023]

Наявність наміру при поширенні хибної інформації є ключовою відмінністю дезінформації від повідомлення недостовірної інформації Як правило, дезінформація є «Тисячоліттями політичні діячі використовували дезінформацію для власної вигоди. При цьому швидкість поширення та обсяг дезінформації у сучасному інформаційному полі тільки підвищує її ефективність і провокує неухильне зростання роздратування, страху та оман у багатьох членів суспільства. В результаті громадськість стає ще вразливішою до подальших маніпуляцій, та

відбувається цикл падіння довіри людей до об'єктивних джерел інформації. Деякі аналітики називають такою процес «вимиванням правди».

Шкідлива інформація - це достовірна інформація, яка була навмисно використана для того, щоб завдати шкоди фізичній особі, організації чи країні.

Приклад

У 2016 році під час первинних виборів у США, повідомлення електронної пошти Національного комітету Демократичної партії (DNC) були вибірково опубліковані у спільному доступі з метою підкріплення заяв про ангажованості цього комітету під час кампанії.

Пропаганда - це кампанії з поширення інформації, призначеної для маніпулювання аудиторією шляхом формування потрібного відношення чи провокування певних дій. [23, с. 1006-1023]

Приклад

Північна Корея відома своєю пропагандою, спрямованою на ідеологічну обробку населення. Практично всі інформаційні засоби, включаючи музику, мистецтво та фільми, спрямовані на роздмухування національної гордості. Обмежений доступ до інтернету та цензура соціальних мереж полегшують уряду Північної Кореї завдання щодо встановлення політичного вектора.

Громадська інформаційна кампанія - це організована діяльність з донесення інформації до великих груп людей, формування суспільної думки, цінностей або поведінки у надії домогтися будь-якого позитивного соціального результату. Це поняття слідує відокремлювати від поняття пропаганди, яка передбачає намір маніпулювати чи дурити.

Приклад

2016 року на грецькому острові Сірос було розгорнуто громадську інформаційна кампанія з метою поінформувати людей про шкідливих наслідки забруднення. Як показали дослідження, кампанія успішно змінила суспільне ставлення до поводження зі сміттям, що призвело до зниження забруднення пластиком місцевого морського середовища.

Існує безліч форм недостовірної інформації та дезінформації. Клер Вордл із First Draft News розділила всі типи недостовірної інформації та дезінформації на сім чітких категорій, що охоплюють весь спектр проблемного матеріалу в інтернеті та засобах масової інформації. Ця класифікація подана у табл. 1.1 і 1.2.

Таблиця 1.1.

Поширені типи недостовірної інформації

Тип	Опис	Приклад
Сатира	відсутня мета заподіяння шкоди, але є ризик введення в оману	гумористична передача або громадська критика
Хибний зв'язок	коли заголовки, візуальні матеріали або супровідні написи не відповідають змісту	«Клікбейт» для статті новин у мережі, наприклад шокуюча або суперечлива назва
Тип	Опис	Приклад
Матеріал, що вводить в оману	використання інформації, щоб роздмухати проблему або очорнити людину	фотографія, яка змушує аудиторію думати, що якась людина знаходилася в певному місці, в той час як насправді його там не було

Таблиця 1.2.

Поширені типи дезінформації

Тип	Опис	Приклад
Хибний контекст	коли достовірний матеріал подається з хибною контекстною інформацією	неправильне зіставлення один одному достовірною інформації та справжніх фотографій

Матеріал із хибним авторством	коли хтось видає себе за справжнє джерело інформації	хибна інформація, яку подають так, наче вона походить від великого, заслуговує на довіру джерела новин
Сфабрикований матеріал	це повністю сфабрикований матеріал, призначений для введення в оману або заподіяння шкоди	зображення, оброблені в графічному редакторі, або сфабрикована інформація, яку видають за факти
Підтасований матеріал	коли здійснюють підтасовування достовірної інформації або візуальних матеріалів з метою введення в оману	справжня фотографія, що супроводжується сфабрикованим текстом

Значний розвиток електронних ЗМІ різко збільшує кількість способів розповсюдження дезінформації. Одним із ключових інструментів дезінформаційних кампаній стали соціальні мережі. Це пояснюється їх популярністю у всьому світі та легкістю поширення інформації через закриті групи та приватні мережі.

Ключовою відмінністю дезінформації від повідомлення недостовірної інформації є намір. Мотиви, якими керуються дійові особи при розробці, створенні та розповсюдженні дезінформації, дозволяють вивчити це ще глибше. Мотиви поділяються на чотири категорії: фінансові, політичні, соціальні та психологічні. Дезінформацію можуть використовувати з метою маніпулювання думкою чи поглядами цільової аудиторії як державні, так та недержавні політичні діячі. Політики можуть поширювати дезінформацію про установи чи політичні супротивники як усередині своєї країни, так і за кордоном з метою заглушити їх голоси і відвести дискурс у потрібне русло. Подібні політичні діячі можуть як мати зв'язок з урядами, так і діяти самостійно та координувати свої дії з іншими особами на підтримку загальної ідеологічної концепції.

Інші діячі, які займаються дезінформацією, можуть керуватися неполітичними мотивами, наприклад, бажанням розважитися або збільшити прибуток. На сьогоднішній день реклама в Інтернеті виступає фінансовим стимулом для дезінформації, здатної швидко поширюватися та залучати відвідувачів на певний веб-сайт. Корпоративні та незалежні діячі, які прагнуть збільшити прибуток за рахунок нарощування відвідуваності ресурсу можуть маніпулювати внутрішніми механізмами (алгоритмами) соціальних мереж, призначеними для надання інформації, а також самої інформацією. Оскільки в соціальних мережах розваги та новини співіснують у тісному сусідстві один з одним, введення в оману споживачів у мережі може бути побічним результатом основний мети — отримання прибутку.

Інші незалежні діячі можуть керуватися іншими мотивами, наприклад можливістю просувати особисті питання, славою чи навіть простим бажанням позлити або «потролити» людей.

Зрозуміло, соціальні мережі мають законне застосування, але їх також можна використовувати й інших цілей.

Взаємозв'язок традиційних ЗМІ та соціальних мереж у загальній картині інформаційного забезпечення відрізняється складною динамікою. Соціальні мережі можуть служити для спотворення та роздування сюжетів, поширених через традиційні ЗМІ, а традиційні ЗМІ часто повідомляють та відображають тенденції, що спостерігаються у соціальних мережах. В результаті утворюється порочне коло дезінформації, який множить неточну інформацію. Навіть просте повторення інформації чи опис результатів перевірки відомостей у мережі часто є ненавмисною допомогою надалі поширення хибної інформації.

1.3 Система забезпечення інформаційної безпеки в світі і в Україні

Інформаційна безпека відіграє важливу роль у забезпеченні життєво важливих інтересів будь-якої держави.

Створення розвиненого та захищеного інформаційного середовища є обов'язковою умовою розвитку суспільства та держави.

Інформаційна безпека досягається шляхом балансу між інформаційними правами та свободами різноманітних суб'єктів права та захистом національного інформаційного суверенітету. Питання інформаційної безпеки та національної безпеки взагалі – це насамперед питання балансу між правами та інтересами людини та компетенцією та інтересами державної влади, балансу, який можна встановити лише з допомогою правових норм.

Усі країни зацікавлені у розвитку глобального інформаційного суспільства та використанні нових можливостей, які відкриваються завдяки покращенню доступу до інформації та кращому забезпечення інформацією. Особливої уваги інформаційні ресурси набувають у сучасних умовах швидкої глобалізації інформаційних процесів та прагнення розвинених країн досягти безперечного інформаційного домінування задля вирішення своїх національних завдань. Саме тому стає необхідним ретельне дослідження теоретичних та практичних проблем інформаційної безпеки у сучасному глобалізованому світі.

За умов швидкого розвитку глобального інформаційного суспільства, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливе значення набуває проблема інформаційної безпеки. Український дослідник О. Марущак наводить таке визначення інформаційної безпеки: «Інформаційна безпека – стан захищеності життєво важливих інтересів людини, за якої запобігає заподіянню шкоди через неповноту, несвоєчасність та недостовірність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання та порушення цілісності, конфіденційності та доступності інформації» [9, с. 107].

У практиці формування інформаційного суспільства у різних країнах виділяють три основні моделі:

- європейську;
- американську;
- азіатську.

Європейська модель розвитку інформаційного суспільства характеризується соціальною орієнтованістю та активним залученням держави та міжнародних інституцій. Органи ЄС реалізують низку програм розвитку інформаційного суспільства та створення єдиного європейського інформаційного простору Ці програми орієнтовані забезпечення прав і свобод громадян, розвитку інформаційної інфраструктури, вільного доступу до неї та інформованості товариства, створення пільгових умов для розвитку підприємництва у сфері інформаційних технологій.

Ознакою європейської моделі інформаційного суспільства є варіативність політичної спрямованості програм побудови та розвитку національних складових об'єднаної Європи, зумовлених новою регіональною геополітикою, становленням інформаційної (інтелектуальної) економіки держав, інформаційного законодавства, різними можливостями постіндустріального розвитку [13, с. 19].

Американська модель відрізняється тим, що основне навантаження щодо інформатизації, розвитку інформаційної інфраструктури посідає приватний сектор. Держава забезпечує регулювання інформаційної діяльності, вільну конкуренцію, бере участь у реалізації найбільш масштабних проектів Враховуючи передову роль приватного сектора, ця модель є більш комерціалізованою, тобто орієнтованою на насичення ринку комерційними інформаційними продуктами та послугами.

Для азіатської моделі характерно те, що більшість питань інформатизації вирішуються в межах взаємодії держави та великих корпорацій. Крім цього, приділяється увага також забезпечення повсякденних потреб суспільства, доступності інформаційних продуктів та послуг.

Сучасна міжнародна інформаційна діяльність визначається як одна з провідних напрямів в умовах становлення глобального інформаційного суспільства, глобальної інформаційної цивілізації, глобального міжнародного інформаційного порядку, інформаційної безпеки міжнародної співдружності.

Особливої уваги інформаційні ресурси набувають у сучасних умовах швидкої глобалізації інформаційних процесів та прагнення розвинених країн досягти інформаційного домінування заради власних національних інтересів, завдань тощо.

необхідним дослідження проблем забезпечення інформаційної безпеки у сучасному глобалізованому світі.

Інформаційна безпека розглядається як глобальна проблема захисту інформації, інформаційного простору та інформаційного суверенітету. Практичне вирішення проблем інформаційної безпеки, притягнення до відповідальності за її порушення чи загрозу їй у кожному державі здійснюється у порядку, передбаченому нормами міжнародного права, що відповідають міждержавними договорами, а також внутрішнім законодавством. Інформаційна безпека регулюється певними нормами міжнародного права, які зафіксовані у документах ООН та ЮНЕСКО, у документах європейських міжнародних організацій, а також у нормативних актах окремих держав. Кожна розвинена країна має закони про захист інформації у різних галузях. Наприклад, Франція має закон «Про інформацію, інформаційні файли та права людини», Німеччина, Австрія, Бельгія, Данія, Ірландія – закон «Про захист інформації», Фінляндія, Ісландія – закон «Про захист інформації про особу», Люксембург – закон « Про використання інформації у процесі роботи з комп'ютером» [7, с. 55].

Стан інформаційного простору України характеризується наявністю суперечності між потребами суспільства у розширенні вільного обміну інформацією та необхідністю окремих обмежень на її поширення. Рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, тому що найчастіше реалізація інформаційних загроз – це завдання шкоди у політичній, військовій, економічній, соціальній, екологічній сферах.

На сучасному етапі в Україні немає реальних гарантів інформаційної безпеки країни, відсутній комплекс нормативно-правових актів із захисту інформаційних ресурсів та інформаційної інфраструктури.

Процес інформатизації має стихійний, некерований характер, з переважним ухилом у бік використання засобів інформатизації іноземного виробництва.

Безсистемність процесів формування інформаційної інфраструктури України зумовлює складність вирішення проблеми інформаційної безпеки, захисту

інформаційних ресурсів. Специфіка цих проблем полягає в тому, що об'єктивно достатній рівень захищеності інформаційної інфраструктури та інформаційних ресурсів може бути досягнутий лише внаслідок чіткого визначення об'єктів інформаційної безпеки України, забезпечення надійного функціонування державних та громадських інституцій для реалізації практичних заходів забезпечення інформаційної безпеки.

При аналізі стану інформаційної безпеки України та визначенні основних проблем у цій галузі слід враховувати політичні, соціально-економічні та організаційно-технічні фактори, що безпосередньо впливають на безпеку країни.

Реалізація інформаційних загроз на рівні особи призводить до порушення чи обмеження доступу громадян до інформації загального користування. Це створює загрозу інформаційній безпеці особистості як з боку органів влади, так і сторонніх осіб або угруповань, порушує баланс відносин між особистістю, суспільством і державою.

Наслідком впливу інформаційних загроз на соціальну спільність є ускладнення суспільних процесів, що виявляється в загостренні протиріч між різними соціальними верствами, загостренні політичної боротьби, розпалюванні релігійних та етнічних протиріч, зниженні загальної культури населення, розвитку бездуховності, зростанні злочинності, поширенні антигуманних ідей.

Наслідки інформаційних злочинів в економічній сфері можуть призвести до економічних втрат за рахунок знецінення та втрати товарної частини інформаційного ресурсу – промислових та інформаційних технологій. Вплив інформаційних загроз на структури державної влади, відповідальні за підготовку та прийняття рішень, реалізація яких безпосередньо впливає на безпеку, може сприяти виникненню надзвичайних ситуацій у державі та суспільстві, значним збиткам через порушення функціонування систем зв'язку, контролю та управління, витік інформації, яка містить державну таємницю.

Для запобігання та ліквідації загроз інформаційній безпеці використовують правові, програмно-технічні та організаційно-економічні методи.

Правові методи – передбачають розробку комплексу нормативно-правових актів та положень, що регламентують інформаційні відносини у суспільстві, керівних та нормативно-методичних документів щодо забезпечення інформаційної безпеки.

Тема захисту та розвитку національного інформаційного простору вже кілька десятиліть є приводом для затятих наукових дискусій. її розробляли такі зарубіжні фахівці, як М. Кастельс, А. Моль, З. Бжезінський, Д. Томпсон, Ф. Вільямсі багато інших. Аналіз чинної нормативної бази показує, що поняття "інформаційна безпека України" достатньо широко застосовується у Конституції України та низці інших нормативно-правових актів, підлеглих та затверджених Верховною Радою, Президентом України, Кабінетом Міністрів, центральними органами виконавчої влади.

Так, ст. 17 Конституції наголошує, що забезпечення інформаційної безпеки є "однією та найважливішою функцією держави, справа всього українського народу", а Закон України "Про Концепцію Національної програми інформатизації" проголошує, що "інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших содових національної безпеки”.

У ст. 23 "Військової доктрини України "прямо вказується, що" здійснення заходів щодо забезпечення інформаційної безпеки є одним із основних завдань Збройних сил України у мирний час". На ст. 20 наголошується, що характерними рисами сучасної збройної боротьби, серед іншого, є "зростання ролі та значущості протистояння в інформаційній сфері, використання новітніх інформаційних технологій".

У ст. 13 Закону України «Про основні засади розвитку інформаційного суспільства в Україні 2007-2015 роки "дається визначення поняття" інформаційна безпека "- це" ... через: неповноту, несвоєчасності та негативний інформаційний вплив; негативні наслідки застосування інших технологій; несанкціоноване поширення, використання та порушення цілісності, конфіденційності та доступність інформації ".

Водночас у Законі України "Про інформацію" визначення "інформаційна безпека" взагалі ні.

А у Законі України "Про основи національної безпеки України", який є основним орієнтиром забезпечення безпеки нашої держави, сутність "інформаційної безпеки" представлена як невід'ємна складова національної безпеки України без точного визначення цього поняття.

Так, наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 10.06.2008 р. № 94 затверджено "Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ та організацій незалежно від форм власності щодо попередження, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах".

Метою цього Порядку є організація координації діяльності з питань попередження скоєння порушень безпеки інформації в ІТС, виявлення та усунення наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в ІТС, а також запровадження єдиної процедури надання суб'єктами координації інформації про скоєння та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в ІТС.

Вагомим зрушенням у нормативно-правовому регулюванні національної безпеки в інформаційній сфері в цілому та на інформаційно-психологічному напрямі зокрема стала розробка та запровадження дія Доктрини інформаційної безпеки України (далі- Доктрина), який був підготовлений на виконання Указу Президента України "Про рішення Ради національної безпеки та оборони України від 21 березня 2008 року «Про невідкладні заходи щодо забезпечення інформаційної безпеки України» від 24.04.2008 р. № 377.

Слід зазначити, що Доктрина стала першим вітчизняним нормативно-правовим документом. якому проголошується особливе місце інформаційної безпеки в системі забезпечення національної безпеки, а саме з одного боку – як невід'ємного компонента кожної із сфер забезпечення національної безпеки та як

важливої самостійної сфери забезпечення національної безпеки – з іншого боку. Останнім часом розроблено низку нових законопроектів з інформаційної безпеки держави, а саме "Про основи інформаційної безпеки України", "Про кібернетичну безпеку України", "Про внесення змін до деяких законів України щодо заохочення кібернетичної безпеки України". В цих законопроектах частково враховано зазначені недоліки вітчизняного законодавства.

Таким чином, хоча основи інформаційного законодавства України у сфері інформаційної безпеки вже є, проте вона потребує подальшого розвитку та вдосконалення з багатьох аспектів у відповідних законах та Доктрині інформаційної безпеки України.

При цьому забезпечення інформаційного суверенітету та забезпечення інформаційної безпеки України з правового погляду має включати:

- визначення та уніфікації загальних положень законодавства;
- основи та норми регулювання інформаційних відносин у різних сферах суспільної діяльності та сферах національної безпеки;
- визначення та забезпечення державою стратегічних напрямів розвитку та захисту національного інформаційного простору, цілісної державної інформаційної політики;
- визначення норм, принципів та меж діяльності вітчизняних та зарубіжних суб'єктів інформаційних відносин у національному інформаційному просторі України;
- визначення основ, принципів, методів захисту національних інтересів України як у вітчизняному, так і у світовому інформаційному просторі та міжнародних інформаційних відносинах.

Пошуки адекватних відповідей на виклики міжнародного розвитку є основою багатосторонньої співпраці України в галузі інформації та комунікації, свободи вираження та розвитку нових інформаційних технологій. Україна здійснює реформування інформаційної сфери для забезпечення національної участі у міжнародних програмах становлення інформаційного суспільства та європейської інтеграції, для вирішення внутрішніх державно-творчих проблем, трансформації

економіки та використання глобального інтелектуального придбання. Наразі суспільство переживає етап проникнення інтелектуальних інформаційних технологій. у різні сфери діяльності. Усі країни життєво зацікавлені у розвитку глобального інформаційного суспільства та використанні нових можливостей. Україна має можливість зробити свій великий внесок у формування міжнародної політики забезпечення інформаційної безпеки.

Висновки до прешого розділу

Доступність засобів масової комунікації, зрозумілість знань про світ забезпечили можливість легкого доступу до будь-якої інформації, але виникла проблема з надто великою кількістю інформації, яка ще й не завжди достовірна. ЗМІ та інші відкриті джерела інформації наразі мають дуже великий вплив на людей та їх свідомості у нашому житті, завдяки чому можуть змінювати поведінку та мислення. Перебування людей під постійним впливом небезпечної інформації викликає трансформацію психіки, зміну поглядів, думок, відносин, ціннісних орієнтацій, мотивів, стереотипів, реакції, поведінки, дії особистості, призводить до формування викривленого світогляду та ціннісної дезінформації, провокує розвиток шкідливих звичок, викликає агресію, ненависть, роздратованість, стан невизначеності, сприяє виникненню психологічного дискомфорту у споживачів інформаційної продукції. Саме тому є важливим для людей, компаній та держав вчасно виявляти недостовірні джерела та блокувати їх.

РОЗДІЛ 2
ВІДОМІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ

2.1 Дослідження можливості застосування біоінспірованих методів для реалізації криптоаналізу

В даний час при розробці комп'ютерних технологій, що забезпечують інформаційну безпеку та захист інформації, широке застосування знаходять криптографічні методи захисту. Для вирішення цього завдання, що відноситься до класу NP-повних, в останні роки застосовуються алгоритми, засновані на природних системах. До них відносяться методи моделювання відпалу, генетичні алгоритми (ГА), еволюційні методи, алгоритми роєвого інтелекту тощо.

У моделях та алгоритмах еволюційних обчислень ключовим елементом є побудова початкової моделі та правил, за якими вона може змінюватися (еволюціонувати). Протягом останніх років було запропоновано різноманітні схеми еволюційних обчислень, зокрема, генетичний алгоритм, генетичне програмування, еволюційні стратегії, еволюційне програмування.

Однією з задач є задача криптоаналізу класичних криптографічних алгоритмів з використанням методів еволюційної оптимізації та генетичного пошуку для симетричних шифрів перестановок. Розрізняють такі шифри перестановок: прості таблиці, що шифрують; шифруючі таблиці з одиночною перестановкою по ключу; шифруючі таблиці з подвійною перестановкою по ключу; магічні квадрати. Зазначимо, що методи шифрування за допомогою простих шифруючих таблиць, за допомогою одиночної перестановки за ключом, подвійний перестановки.

При використанні шифруючих таблиць ключем є перестановка (p1, p2, ... pn), тому хромосома у ГА має також ставити перестановку. Основне питання при цьому - як здійснити уявлення окремих генів особи. У найпростішому випадку шифрування здійснюється шляхом присвоєння окремим генів відповідних елементів ключа, тобто. і -м геном хромосоми P рахувати елемент pi. Незважаючи на недоліки

такого підходу, наприклад, гени виходять залежними один від друга, що призводить до можливості отримання нелегальних рішень, таке визначення генів інтуїтивно зрозуміле і не вимагає додаткових витрат на їх формування.

Альтернативним підходом є використання деякого проміжного уявлення, при якому набір генів задає деяке правило або об'єкт, з якого формується ключ. При цьому основним завданням є знаходження проміжного рішення, що задається в бітового рядка для застосування стандартних генетичних операторів. Зазначимо, що з реалізації ГА криптоаналізу використовувався перший підхід, тобто. як гени особи розглядаються елементи ключа. Для запобігання одержанню нелегальних рішень при десятковому кодуванні хромосом використовується правило: при появі в хромосомі однакових генів другий повторюваний ген замінюється на відсутній. Як функцію пристосованості особин використовувався факт збігу відкритого тексту і шифртексту при реалізації криптоаналізу 2-го типу для визначення секретного ключа. Як цільову функцію пропонується використовувати функцію Якобсена про розподіл частот біграм у відкритих текстах. Результати експерименту свідчать про можливість застосування еволюційних методів для криптоаналізу шифрів, що використовують шифруючі таблиці для стовпцевих та малих перестановок.

Сутність методів простої заміни зводиться до заміни символів тексту, що шифрується. символами того ж чи іншого алфавіту із заздалегідь встановленим правилом заміни. Відома реалізація криптоаналізу шифрів одноалфавітної заміни на прикладі афінного шифру Цезаря та системи Цезаря з ключовим словом при відомій та невідомій довжині ключа, шифрів блокової заміни на прикладі шифру Плейфейра та шифру «подвійний квадрат» Вітсона за відомої та невідомої довжині кодового слова, і навіть шифру багатоалфавітної заміни з прикладу шифру Вижинера.

Поняття «біоінспіровані алгоритми» можна докладніше пояснити, як алгоритми, натхненні процесами живої природи. Інакше висловлюючись, це використання алгоритмів методів оптимізації, заснованих на елементах живої природи для моделювання будь-яких явищ та пошуку найефективніших рішень.

Існує такий підклас біоінспірованих алгоритмів як генетичні алгоритми. Вони імітують деякі фундаментальні аспекти еволюційного процесу неодарвіністської

теорії. Алгоритм проводить одночасно пошук з набором популяцій (рішень) кандидатів і пов'язує з ними об'єктивну оцінку як визначальне значення для кожного з них. Потім алгоритм вибирає з отриманих значень серед популяцій ті рішення, що є найбільш підходящими. Наступне покоління (тобто нова популяція) складається з повторів відповідних значень, які були генетично мутовані і перейшли до наступної біологічної фази: значення змінних були отримані таким чином, що вони успадковували характери своїх батьків, а також змінювалися випадково. Розмір цієї проміжної популяції в ході роботи алгоритму зменшується до розміру популяції батьків за рахунок виключення найменш підходящих під визначальне значення рішень.

Структури генетичних алгоритмів є "сліпими" пошуковими структурами з властивим їм рядом недоліків. Тому цікаве застосування евристичних методів, ідеї яких запозичені у живої природи або фізичних процесів і в яких розв'язання задачі будується поетапно шляхом додавання нового компонента до частково побудованого рішення. До методів цього виду відносять і мурашині алгоритми. Зазначимо, що мурашині алгоритми досліджуються з середини 90-х років, і на сьогоднішній день відомі їх застосування: задачі про комівояжер, квадратичну задачу про призначення, задачі про розмальовку графа, задачі маршрутизації в комутаційних мережах. Застосування алгоритму «мурашиних колоній» для реалізації криптоаналізу шифрів перестановки показує, як ця проблема може бути зведена до класичної задачі про призначення, що вирішується за допомогою алгоритму мурашиних колоній. Важливою особливістю застосування алгоритмів «мурашиних колоній» є необхідність представлення завдання у вигляді графової моделі, на якій мурахи можуть будувати рішення.

Однією з останніх розробок у галузі роєвого інтелекту є алгоритм бджіл, який досить успішно використовується для знаходження екстремумів складних багатовимірних функцій.

Структура його включає такі основні етапи:

1. Формування простору пошуку.
2. Оцінка цільової функції (ЦФ) бджіл у популяції.

3. Пошук агентами-розвідниками перспективних позицій для пошуку в околицях.
4. Вибір бджіл із найкращими значеннями ЦФ з кожної ділянки.
5. Надсилання бджіл-фуражиров для випадкового пошуку та оцінка їх ЦФ.
6. Формування нової популяції бджіл.
7. Якщо умови закінчення роботи алгоритму виконуються, то перехід до 8, інакше до 2.
8. Кінець.

2.2 Відомі біоінспіровані методи в кібербезпеці

Пошук рішення в різноманітних системах необхідний завдяки зауваженню, що кіберпростір за своєю суттю є складним. В інших сферах, наприклад робототехніці, аналогії з імунною системою використовуються для розробки механізмів самоорганізації [24, с. 66-83].

Біологічні концепції були взяті за основу і сприяли надійності кібербезпеки. Їх принцип та алгоритми знайшли застосування та перспективи реалізації в ряді областей, включаючи обчислення, фінансове моделювання і робототехніку тощо.

Основні переваги біологічних систем полягають в їх розподіленості архітектури, де автономні організації приймають локальні рішення з глобальними наслідками.

Для, наприклад, імунної системи існує здатність адаптуватися і самозахищатися, динамічно відтворюватись і руйнувати мутовані або інфіковані клітини організму, оскільки він дізнається про нові загрози і захищає себе та свій захист. Оскільки віртуалізація є звичним явищем у кіберпросторі, програмно визначені платформи та мережі в значній мірі покладаються на нього, однак моніторинг безпеки стає складнішим, оскільки методологічно атаки стають важче і ширше.

Таким чином, надійність кібертехнологій та інфраструктур визначається якістю базової віртуалізації, а складність технології впливає на рівень реалізації [23, с. 1006-1023].

Природа ефективно демонструє самоорганізацію, адаптивність, стійкість та інші властивості. Сильні сторони природних систем полягають у здатності бути автономними суб'єктам для прийняття локальних рішень, безперервної координації та обміну інформацією для підтримки між елементами системи [11, с. 1800]. Наприклад, динаміка хижак-здобич підкреслює важливість і наслідки взаємодії між двома видами та те, як залежать функції спільноти від її особливостей.

Біологічні системи були предметом досліджень у всьому обчислювальному континуумі починаючи з 1980-х років [11, с. 1801]. За останні роки кілька опитувань [11, с. 1802] присвятили свої зусилля оцінці біологічно інспірованих алгоритмів у обчислювальній сфері додатків. Зі зростанням попиту на мережеві системи та залежністю від Інтернету зв’язок, що забезпечується за допомогою асортименту пристроїв та інфраструктур, є обов’язковим, а обчислювальні системи є адаптивними, стійкими, масштабованими та достатньо надійними, щоб протистояти збоям, досить динамічним, щоб справлятися із змінами. Вважається, що підходи, натхненні біотехнологією, забезпечують послідовність у продуктивності протягом тривалого періоду часу, і насправді мають спільну складність атрибутів та відносний успіх міжмережевих середовищ. Наприклад, атрибут самоорганізації біосистем, які використовуються в бездротових мережах, означає, що кластеризація вузлів маршрутизації підвищує масштабованість протоколів пересилання даних. Таким чином, мережа стає надійною і може адаптуватися до частих топологічних змін.

На рисунку 2.1 представлено таксономічну систему прикладів біоінспірованих підходів, розрізнених відповідно до їх фізіологічних та екологічних властивостей. Таке явище, як еволюційні наслідки хижацтва для адаптацію та контрпристосування, визначають поведінку видів. Поведінка в тому числі «Ризик хижацтва» та оцінка вартості кормових видів, змінює результати взаємодії між сутностями та їх середовищем [11, с. 1803].

На основі взаємодії та поведінки, які існують між хижаком та його жертвою були розроблені інновації. З цією метою застосовується динаміку хижак-жертва. Звичайна безпека підходи зосереджені на виконанні комплексного аналізу

обмежених наборів даних, тоді як нетрадиційні механізми обробляють невеликі обсяги даних «простим розподіленим способом» у широкому діапазоні входів. Показано, що існує багато форм біоінспірованих систем штучного інтелекту, причому генетичні алгоритми (ГА) є особливо успішними.

Автори представляють всебічний огляд біоінспірованих мережевих протоколів, посилаючись на значну кількість джерел, які вказують на той факт, що імунні алгоритми становлять основу мережевої безпеки; виявлення аномалій і неправильної поведінки. Автори пов’язують епідеміологію з поширенням контенту в комп’ютерних мережах, у тому числі аналіз недостовірної інформації, що поширюються в Інтернеті. Також запропоновані траст і модель репутації (BTRM-WSN), натхненна колонією мурашок, як стратегія для використання довіри за пріоритетним шляхом. Розумно припустити, що базову модель довіри можна поширити на обчислювальні середовища шляхом адаптації системи мурашиних колоній, в якій визначені шляхи виконання умови, із залишками феромонів, щоб мурахи, що йдуть, могли слідувати за довіреним маршрутом. Інші моделі, включаючи систему Trust Ant Colony System (TACS), засновану на алгоритмі AntRep про динамічний інтелект, моделі динамічної довіри на основі часу (TBDTM). Тим не менш, необхідно наголосити на необхідності комплексного тестування та оцінці перед їх використанням у середовищах.

Модель на основі сімейних генів для Cloud Trust (FBCT) включає обмеження, властиві системам на основі PKI, які включають проблеми з ідентифікацією вузлів у середовищах, контролю доступу та системі аутентифікації сторонніх розробників. Взявши до уваги біологічні принципи в сімейних генах, їх модель забезпечує рішення для довіри в області хмарних обчислень. Використання біологічних метафор як основи для проектування, моделювання та впровадження хмарного сервісу, який здатний впоратися з проблемами стабільності, які виникають внаслідок довготривалих процесів, і атаки безпеки. Запропонований підхід, натхненний стадом зебр, не лише спростив складні технічні завдання, але також покращив нові проекти для автоматизованих процесів самокерування для системних адміністраторів. Таблиця 2.1 підсумовує деякі біосистеми, класифікуючи їх

відповідно до сфери застосування, а також підкреслює сильні сторони і слабкості кожної системи.

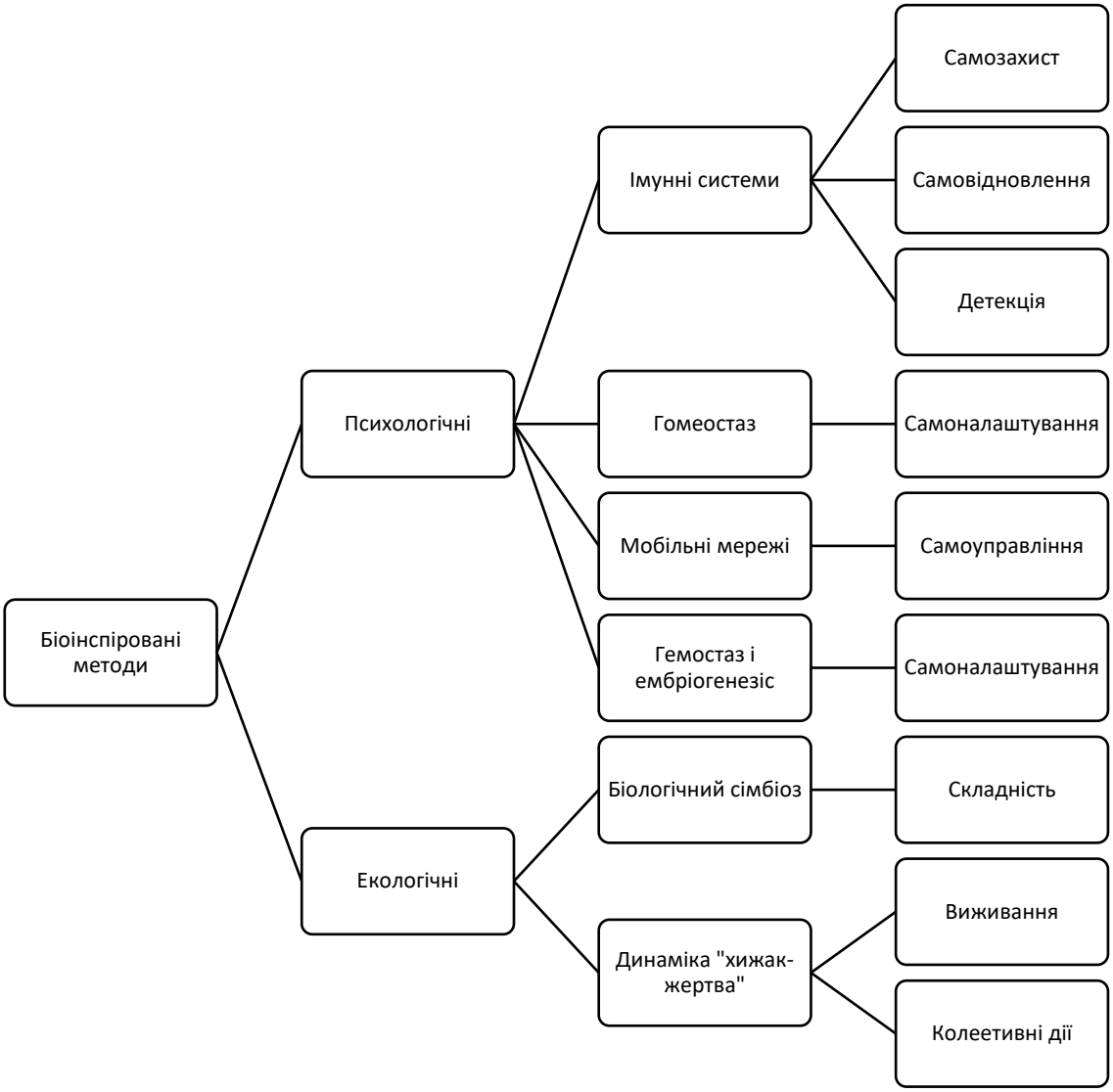

Рисунок 2.1. Таксономічна система прикладів біоінспірованих підходів

Зіткнувшись із поєднанням наполегливих віжливі контрзаходи кібербезпеки розробляються на основі видобутої з природи основи.

Традиційні контрзаходи безпеки успішні відповідно лише в традиційних мережах. Це призводить до зростання популярності підходів адаптивного кіберзахисту (ACD), таких як біоінспірованих методів, щоб на основі їх можливостей оптимізувати непередбачуваність і максимізувати адаптивні конфігурації атаки, і тим самим підвищити вартість атаки для супротивника.

Складність, масштабна віртуалізація та надзвичайно розподілений характер кіберпростору означає, що підзвітність, контроль і довіра до таких середовищ стає ключовим.

Таблиця 2.1.

Біоінспіровані методи в кіберсередовищі

Алгоритм	Опис	Застосування
Множина послідовність вирівнювання (MSA)	Структура білка	Класифікація веб-трафіка та впорядкування послідовності
Алгоритм оптимізації з соеволюцією	Спільна еволюція в населення	Оптимізація IDS виявлення вторгнення
Стратегія безпеки даних	Імунна система	Безпека збережених даних
Безпечне зберігання даних	Фізіологічні і поведінкові моделі	Біометрична аутентифікація хмарного збереження даних
AIS для виявлення фішингу	Життєвий цикл Т-лімфоцитів	Виявлення фішингу в електронних листах
Інтегральна циклічна метріка (ICMetrics)	Властивості людини та її особливості	Висока ентропія Відкритий/приватний ключ Схема генерації
Біоінспірована стійкість	Клітини та організми (морський хамелеон)	Керування хмарною безпекою
Приховування даних на основі спільного використання ресурсів ДНК	Послідовності ДНК	Приховування даних для конфіденційності і цілісності хмарних даних
Органічна стійкість Підхід до забезпечення стійкості до атак і невдач	Імунологія (запалення і імунізація)	Виявлення загроз, Автоматизована реорганізація
Безпека на основі розпізнавання обличчя	Риси обличчя	Аутентифікація і авторизація
Модель на основі сімейних генів (FBCT)	Ідентифікація генів	Аутентифікація користувача, управління доступом, і авторизація

Продовження таблиці 2.1.

Алгоритм	Опис	Застосування
Агент мережі Оцінка небезпеки	Імунна система:	
Навчання під наглядом класифікатора з режимом реального часу (UCSSE)	Генетична машина навчання	Автоматичне виявлення підпису в IDS
Виявлення шахрайства та нелегтимне використання комп'ютерних систем і мобільних телекомунікацій	Імунна система	Моніторинг і виявлення шахрайських злочинів
Розширення моделі хижака-здобичі	Хижак-здобич-спільнота	Запобігання дії шкідливого програмного забезпечення в мережі
Комп’ютерна імунна система	Фаза вродженого імунітету	За допомогою імітації імунітета створення антигенів рядків підпису
Мурав’їнні колонії	Колонія мурах, алгоритм оптимізації	Одночасний обмін інформації агентами в мережі

Сучасні приклади класичних біоінспірованих підходів у обчислювальному середовищі включають теорії та алгоритми. Алгоритми корисні для опису систем з дискретного простору станів. Наприклад, на основі алгоритмів про механізми, що регулюють поведінку колоній мурах, імунну систему людини, роїння бджіл, взаємодію у спільноті риб, хижаків і здобичі тощо, були змодельовані високопродуктивні, ефективні, складні та розподілені системи. Застосовані алгоритми включають, але не обмежуються ними: автономні обчислення, штучне життя, біоміметичні, органічні обчислення та генетичні алгоритми. Крім того, такі

теорії, як «Я» і «Не-я» та «Теорія небезпеки», були створені і передумовлені біоінспірацією. Подальші розробки біоінспірованих підходів також викликають необхідність формалізації теорії паралельності як формальної основи для моделювання паралельних, розподілених та мобільних систем.

Штучні природні імунні системи застосовуються в різних сферах, і особливо їх хвалять за успіх у IDS. Ефективність виявлення визначають імунні детектори, що характеризуються як основний компонент імунної системи. Виявлення фішингу AIS надихається частиною механізму реакції імунної системи на патогенні мікроорганізми. Створюючи детектори пам'яті зі статичного навчального набору даних і незрілих детекторів шляхом мутації, пропонована система виявляє вхідні фішингові електронні листи через детектори пам'яті, тоді як незрілі детектори виявляють фішингові листи з невідомими підписами.

Генетичні алгоритми (ГА) — це стохастичні методи пошуку, біоінспіровані методи, де вирішення проблем відбувається опосередковано через еволюцію рішень. Наступні покоління рішень, у свою чергу, дають найкраще рішення проблеми. Подібний алгоритм GTAP для аутентифікації користувачів, які з «сім'ї», а також ідентифікуються за допомогою унікального генного сертифіката (синонімом унікальних підписів). Користувачі аутентифікуються після позитивного аналізу їх генного коду. Результати моделювання для GTAP продемонстрували перевагу в безпеці та захищеності шляхом протидії недолікам безпечних паролів та неоднозначності предметної інформації в представлених сертифікатах у традиційних механізмах.

Окрім того, генетичні алгоритми реалізовані в криптографії для оцінки та підвищення складності систем шифрування. У криптоаналізі, де реалізовано механізм атаки для оцінки міцності системи шифрування, ГА є дуже успішним у підстановці шифрів та транспозиції шифрів. Хоча нейронні мережі, як правило, використовуються, наприклад, для розпізнавання та класифікації, а також фільтрації, вони корисні в інших областях, включаючи використання біометрики в безпеці. Ключ до їхнього успіху — це точність вилучення ознак і ефективність класифікації, тобто низький рівень відхилень і висока позитивна класифікація.

Колонії мурах застосовуються для оптимізації маршрутизації трафіку, оцінюють алгоритм оптимізації. Мурашині колонії, в яких агенти одночасно здійснюють мережевий обмін інформацією, що є синонімом стигмерії у комах. Цей алгоритм запропоновагий FBeeAd-Hoc як фреймворк безпеки для проблем маршрутизації в мобільних мережах (MANET) з використанням теорії нечітких множин та цифрового підпису.

2.3 Метод бджолиної колонії і його переваги у порівнянні з конкурентними методами

В класичній теорії штучного інтелекту для визначенної задачі створюється одна інтелектуальна система, що має всі необхідні ресурси для її рішення. В теорії багатоагентних систем використовується протилежний принцип. Вважається, що один агент має неповне представлення про глобальну проблему, тому створюється безліч агентів і забезпечується ефективна взаємодія між ними. В рамках «колективного» інтелекту розглядається глобальна поведінка всієї системи, як результат взаємодії ряда простих агентів. Прихильники напряму «інтелекта роя», зокрема, Р. Брукс, Ж. Денебург, Л. Стиль та ін. опираються на наступні положення:

- багатоагентна система – це популяція простих і залежних друг від друга агентів;
- кожен агент самостійно визначає свої реакції на події в локальному середовищі та взаємодії з іншими агентами;
- зв’язки між агентами є горизонтальними, тобто не існує агента-супервізора, керуючого взаємодією інших агентів;
- немає точних правил, щоб визначити глобальну поведінку агентів;
- поведінка, властивості та структура на колективному рівні породжуються тільки локальними взаємодіями агентів.

Для визначення переваг методу бджолиної колонії порівняємо його з методами мурашиної колонії і рою частинок.

«Мурашині» алгоритми пошуку. Основою для цього алгоритму є імітація колективної поведінки мурах. Система мурашиної колонії заснована на простих

правилах автономної поведінки кожної мурахи. Незважаючи на примітивність дій мурахи, діяльність всієї колонії розумна, тобто мурашина колонія, по суті, є природною багатоагентною системою.

Непрямий обмін – стигмержі (stigmergy), є рознесеною у часі взаємодією, при якій одна особина змінює деяку область довкілля, інші використовують цю інформацію пізніше, як у неї потрапляють. Біологи встановили, що така відкладена взаємодія відбувається через спеціальну хімічну речовину – феромон (pheromone), секрет спеціальних заліз, що відкладається при переміщенні мурахи. Концентрація феромону на шляху визначає перевагу руху по ньому. Адаптивність поведінки реалізується випаром феромону, що у природі сприймається мурахами протягом кількох діб. Ми можемо провести деяку аналогію між розподілом феромону в навколишньому колонію просторі і «глобальної» пам'яттю мурашника, що має динамічний характер.

Будь-який мурашиний алгоритм, незалежно від модифікацій, може бути представлений у такому вигляді:

поки (умови виходу не виконані), реалізуються наступні кроки алгоритму:

1. «створюємо мурах»;
2. знаходимо рішення;
3. оновлюємо феромон;
4. робимо додаткові дії.

Для того щоб побудувати відповідний мурашиний алгоритм для вирішення будь-якого завдання, необхідно:

1. уявити завдання як набір компонент і переходів чи набір не орієнтованих зважених графів, у яких мурахи можуть будувати рішення;
2. визначити значення сліду феромону;
3. визначити евристику поведінки мурахи, коли будуємо або знаходимо рішення;
4. якщо можливо, реалізувати ефективний локальний пошук;
5. вибрати специфічний ACO (Ant Colony Optimization) алгоритм і застосувати для вирішення задачі;
6. настроїти параметри ACO-алгоритму.

Також визначальними є такі параметри:

- кількість мурах;
- баланс між вивченням простору пошуку та використанням оптимального шляху;
- поєднання із жадібними евристиками або локальним пошуком;
- момент часу, коли оновлюється феромон.

«Мурашині» алгоритми є ефективним способом вирішення задач пошуку та оптимізації, що допускають графову інтерпретацію, що підтверджується експериментальними дослідженнями. До переваг варто віднести можливість застосування до широкого спектру завдань та гарантовану збіжність. З недоліків можна відзначити сильну залежність від початкових настроювальних параметрів алгоритму, які підбираються тільки виходячи з практичного досвіду.

Бджолині алгоритми. Засновані на поведінці колонії бджіл у природному середовищі. Існує два основних алгоритми – бджолиний алгоритм (Bee Algorithm) та алгоритм колонії бджіл (Artificial Bee Colony). Бджолиний алгоритм заснований на методі пошуку бджолами елітних ділянок. Основна перевага даного алгоритму – бджоли досліджують також ділянки, що знаходяться на околицях елітних, що дозволяє наблизити рішення до оптимального.

Найпростіший алгоритм бджіл можна представити формально таким чином:

1. «створення бджіл»;
2. визначення ЦФ (значення цільових функцій) бджіл;
3. вибір ділянок для пошуку;
4. відправлення бджіл-розвідників;
5. вибір бджіл з найкращими ЦФ;
6. відправлення робочих бджіл для випадкового пошуку та визначення їх ЦФ;
7. створення нової популяції бджіл;
8. 8 доти, доки (умови виходу не виконані), повторюємо пункти 2-7.

Алгоритм колонії бджіл було запропоновано Д. Карабога у 2005 р. [11, с. 1804]. Основна ідея – імітація діяльності бджіл у вулику під час пошуку нектару. Використовується фіксоване розбиття бджіл на групи – робочі бджоли, бджоли-розвідники, бджоли-дослідники

Основні кроки алгоритму колонії бджіл такі:

1. визначення розташування джерел нектару;
2. пошук робочими бджолами нових джерел та дослідження кращого;
3. вибір джерела бджолою-дослідником, залежно від якості;
4. повтор пунктів 1-3 доти, доки рішення не перестане покращуватися;
5. запам'ятовуємо найкраще джерело;
6. заповнюємо частину популяції, що залишилася;
7. повторюємо пункти 2-6, доки не буде досягнуто умови виходу.

Методи «бджолиного» рою підтверджують свою ефективність як евристичні мультиагентні методи випадкового пошуку [1, с. 19]. До недоліків даного методу варто віднести велику кількість вільних параметрів, від значення яких часто залежить результат, з іншого боку, відсутні підстави вибору цих значень.

Метод рою частинок. У методі рою частинок (Particle Swarm Optimization) агентами є частинки, які у кожний момент часу мають у просторі параметрів задачі деяке положення та швидкість. Правила, за якими частинка змінює своє положення та швидкість, визначаються на основі обчислення цільової функції частки. Канонічний метод рою частинок був запропонований в 1995 р. в роботі J. Kennedy, R. Eberhart [11, с. 1806], в основі якого лежить наступний принцип: кожної ітерації визначення наступного положення частки враховується інформація про найкращу частинку від «сусідів» та інформація про цю частинку на тому кроці, коли цій частинці відповідало найкраще значення цільової функції. Так само існує модифікації канонічної моделі, які враховують значення ЦФ всіх частинок рою, в деяких моделях частинки групуються в кілька роїв тощо.

У канонічному методі рою частинок, що використовує метричне шкалування, нова позиція частинки і визначається за такою формулою:

$$x_i(t+1)= x_i(t)+ v_i(t+1), \qquad (2.1)$$

де $v_i(t+1)$ – швидкість перемещіння частинок із позиції $x_i(t)$ в позицію $x_i(t+1)$. Початковий стан визначається як: $x_i(0)$, $v_i(0)$. Наведена формула представлена у векторній формі. Найкращі частки з точки зору цільової функції оголошується

«центром тяжіння». Вектори швидкостей всіх частинок спрямовуються до цих центрів.

Алгоритм рою частинок широко застосовується, серед інших, у задачах машинного навчання (зокрема, для навчання нейромереж та розпізнавання зображень), параметричної та структурної оптимізації (форм, розмірів та топологій) в галузі проектування, в галузях біохімії та біомеханіки. За ефективністю він може змагатися з іншими методами глобальної оптимізації, а низька алгоритмічна складність сприяє простоті реалізації.

Найбільш перспективними напрямками подальших досліджень у даному напрямку слід вважати теоретичні дослідження причин збіжності алгоритму рою частинок та пов'язаних з цим питань з областей роєвого інтелекту та теорії хаосу, комбінування різних модифікацій алгоритму для вирішення складних завдань, розгляд алгоритму рою частинок як багатоагентної обчислювальної системи, а також дослідження можливостей включення до нього аналогів складніших природних механізмів.

Висновки до другого розділу

Для покращення інформаційного простору необхідні методи виявлення недостовірної інформації та вчасне їх покращення, адже зловмисники також розвиваються і шукають шляхи передачі своєї інформації. Для розробки алгоритму виявлення недостовірної інформації обраний удосконалений метод бджолиної колонії. Цей метод заснований на поведінці колонії бджіл у природному середовищі. Існує два основних алгоритми – бджолиний алгоритм (Bee Algorithm) та алгоритм колонії бджіл (Artificial Bee Colony). Бджолиний алгоритм заснований на методі пошуку бджолами елітних ділянок. Основна перевага даного алгоритму – бджоли досліджують також ділянки, що знаходяться на околицях елітних, що дозволяє наблизити рішення до оптимального.

РОЗДІЛ 3
ЗАСТОСУВАННЯ УДОСКОНАЛЕНОГО МЕТОДУ ВИЯВЛЕННЯ НЕДОСТОВІРНОЇ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

3.1 Задача пошуку алгоритму виявлення недостовірної інформацій в інформаційному просторі

З математичної точки зору, щоб вирішити завдання виявлення недостовірної інформації з використанням алгоритмів обчислювального інтелекту, нам знадобиться математичне уявлення нашої проблеми. Це уявлення називається цільовою функцією, яка є математичним правилом, що описує проблему і всі змінні рішення в цій проблемі.

Завдання визначається простором пошуку, тобто областю, в якій ми шукатимемо рішення, набором змінних рішень, що включає всі параметри, що впливають на наше завдання, і, звичайно ж, цільовою функцією, яка визначається математичними правилами, вирішує проблему, а також дає нам оцінку якості рішення-кандидата.

Мета завдання полягає в тому, щоб знайти найкраще рішення з усіх можливих рішень. Зазвичай це означає, що ми хочемо мінімізувати чи максимізувати цільову функцію. Іншими словами, ми хочемо знайти набір вхідних змінних рішень, який мінімізує або максимізує значення нашої цільової функції, яка також називається значенням придатності.

Алгоритм штучної бджолиної колонії (ABC) є алгоритмом оптимізації, який імітує поведінку бджолиної сім'ї.

У цій математичній моделі наша бджолина сім'я складається з трьох типів бджіл: бджоли-співробітники, які будуть працювати над збиранням їжі у вулик із певного джерела їжі; бджоли - спостерігачі, які будуть патрулювати співробітників, щоб перевірити, коли конкретне джерело їжі більше не варте того; бджоли-розвідники, які будуть шукати нові місця для джерел їжі.

В алгоритмі ABC джерело їжі визначається як позиція у просторі пошуку (варіант вирішення поставленої), і спочатку кількість джерел їжі дорівнює кількості бджіл у вулику. Якість джерела їжі визначається значенням цільової функції цієї позиції (значенням придатності).

Емерджентну інтелектуальну поведінку бджіл можна резюмувати кількома етапами:

Бджоли починають випадково досліджувати довкілля у пошуках хороших джерел їжі (значення придатності).

Знайшовши джерело їжі, бджола стає найманою бджолою і починає видобувати їжу з виявленого джерела.

Службова бджола повертається у вулик із нектаром і вивантажує нектар.

Після вивантаження нектару вона може повернутися безпосередньо до свого джерела або поділитися інформацією про своє джерело, виконавши танець на танцювальному майданчику.

Якщо джерело їжі вичерпано, бджола-службовець стає розвідником і починає випадково шукати нове джерело їжі.

Бджоли-спостерігачі, які очікують у вулику, спостерігають за тим, як бджоли-службовці збирають свої джерела їжі, і вибирають джерело серед більш прибуткових джерел.

Вибір джерела їжі є пропорційним якості джерела (значенню придатності).

Незважаючи на те, що ми описали три типи бджіл, на рівні реалізації ми розуміємо, що є лише два типи: працівники та спостерігачі. Бджола-розвідник насправді є дослідницькою поведінкою, яку можуть виконувати як співробітники, так і бджоли-спостерігачі.

В ході роботи ми будемо використовувати Python, тому що його ефективність у чисельних обчисленнях стає все більш очевидною, і він спрощує реалізацію набору об'єктивних тестів для повторного використання наших алгоритмів інтелектуального аналізу рою.

3.2 Опис алгоритму методу бджолиної колонії

ABC починається з колонії штучних бджіл з метою виявлення місця джерел їжі з великою кількістю нектару, і, нарешті, вибирається той, у якого найбільше нектару.

Штучна бджола

Є три основні загальні функції, якими повинна мати будь-яка бджола. По-перше, коли через дослідницьку поведінку бджола виходить за межі нашого рішення, вона повинна мати можливість повернутися у вулик. Другий – це можливість оновлювати статус фактичного джерела їжі, над яким працює бджола, та оцінювати, чи є новий сусідній регіон найкращим джерелом їжі. І останній розуміє, коли джерело їжі вичерпано, і тепер бджола має шукати нові джерела їжі.

Реалізація класу ArtificialBee в Python надана в Додатку А.

Бджола-службовець

Основна поведінка бджоли, що служить, полягає в тому, щоб видобувати їжу з джерела їжі, над яким працює службовець, який виснажується. На рівні реалізації цю поведінку можна розглядати як створення нової позиції поруч із місцем, де знаходиться бджола-службовець, та оцінку того, чи є на цій новій позиції більша кількість їжі. Службова бджола завжди запам'ятовуватиме найкраще становище джерела їжі, досягнуте досі, поки воно не буде вичерпане.

Реалізація класу EmployeeBee надана в Додатку Б.

Бджола-спостерігач

Бджоли-спостерігачі патрулюватимуть роботу бджіл-службовців. Вони літатимуть над вуликом, перевірятимуть хід своєї роботи та оцінюватимуть, хто зі співробітників успішніше збирає їжу. Бджоли-спостерігачі завжди будуть націлюватися на кращих співробітників, використовуючи ймовірнісний підхід, як «місце зустрічі», де інші бджоли повинні прийти до цієї успішної позиції, сподіваючись отримати більше їжі. На рівні реалізації бджоли-спостерігачі переглядатимуть кращих співробітників та намагатимуться покращити це джерело їжі. Після певної кількості випробувань бджола-спостерігач скаже вул'ю, що це

джерело їжі вичерпане і його необхідно викинути. Реалізація класу OnlookerBee надана в Додатку В.

Після реалізації основних типів агентів, які використовуватимуться, настав час фактично реалізувати всі кроки, описані раніше. У роботі було реалізовано кожен крок алгоритму в окремих методах. Спочатку скидаються внутрішні параметри алгоритму ABC та ініціалізуються бджоли-співробітники та бджоли-спостерігачі у випадкових позиціях. Стратегія за умовчанням, яка дуже добре зарекомендувала себе у реальних проблемах, полягає в тому, щоб ініціалізувати половину всього вулика як бджіл-службовців, а іншу половину – як бджіл-спостерігачів.

Після цього ми починаємо з того, що відправляємо наших бджіл-співробітників збирати їжу в їхніх відповідних первинних джерелах їжі, завжди шукаючи найкращі місця навколо них. Як тільки фаза бджіл-службовців завершена, ми відправляємо бджіл-спостерігачів патрулювати їхню роботу та оцінювати, наскільки добре відбувається видобуток їжі з кожного джерела їжі. Нарешті, настав час перевірити, чи не вичерпано якесь джерело їжі, у цей момент будь-який співробітник чи спостерігач може стати бджолою-розвідником і розпочати процес дослідження у пошуках нового джерела їжі.

Повний алгоритм ABC можна реалізувати так:

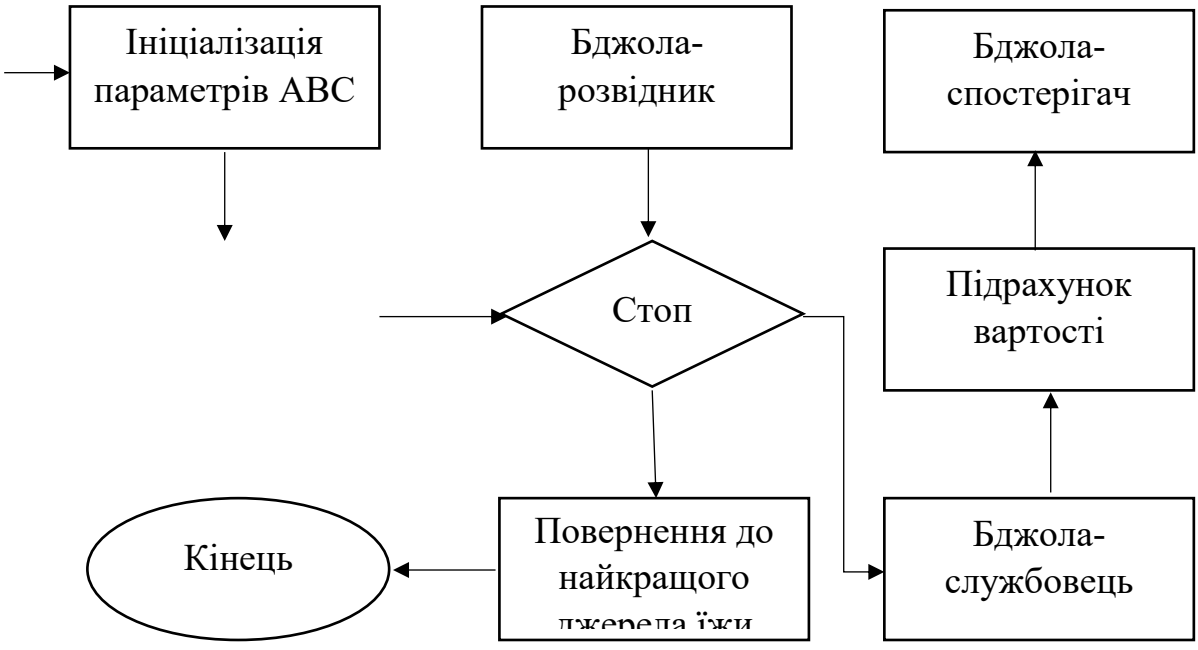

Рисунок 3.1. Блок-схема ABC

Реалізація повного алгоритму ABC надана в додатку Г.

3.3 Застосування алгоритму удосконаленого методу бджолиної колонії для реалізації виявлення недостовірної інформації в інформаційному просторі

Використаємо реалізацію алгоритма ABC на Python для виконання виявлення недостовірної інформації. В нашому випадку запропоновано використати кластерізацію як спосіб виявлення і відокремлення достовірної, недостовірної, а також сумнівної інформації.

Проблема кластеризації – це нечітко визначене NP-складне завдання, основна ідея якого полягає в тому, щоб знайти приховані закономірності наших даних. Формального визначення того, що таке кластер не існує, але воно пов'язане з ідеєю угруповання елементів таким чином, щоб ми могли розрізняти елементи в окремі групи.

Існують різні сімейства алгоритмів, які по-різному визначають проблему кластеризації. Класичний спосіб визначення проблеми кластеризації, що часто зустрічається в літературі, полягає в тому, щоб звести її до математичного завдання, відомого як знаходження k-розбиття вихідних даних.

Пошук k-розбиття множини S визначається як пошук k підмножин S , які підпорядковуються двом правилам:

Перетин будь-якої окремої з цих підмножин дорівнює порожній множині. Об'єднання всіх k підмножин дорівнює S.

По суті, в кінці цієї процедури секційної кластеризації ми хочемо знайти окремі підмножини нашого вихідного набору даних таким чином, щоб жоден екземпляр не належав більш, ніж до однієї групи. Це можна проілюструвати на рисунку 3.2.

Результатом процедури кластеризації є набір центроїдів. Центроіди в основному є репрезентативними об'єктами кожної групи, тому якщо ми хочемо k-розбиття наших даних, то у нас буде k центроїдів.

Використання центроїдів подано на рисунку 3.3.

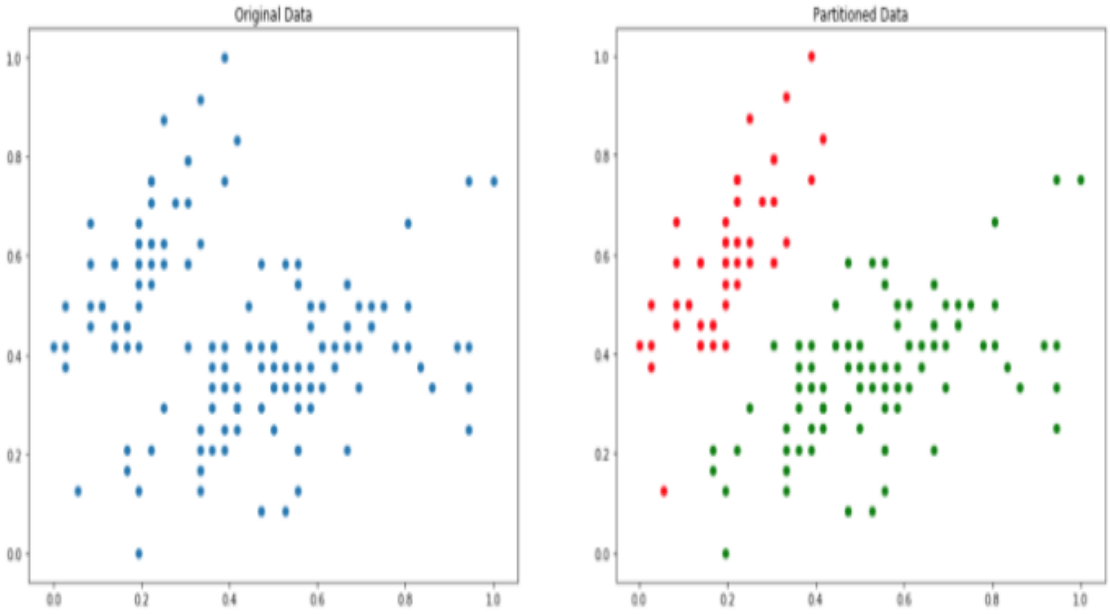

Рисунок 3.2. Вихідний і розподілений набір даних

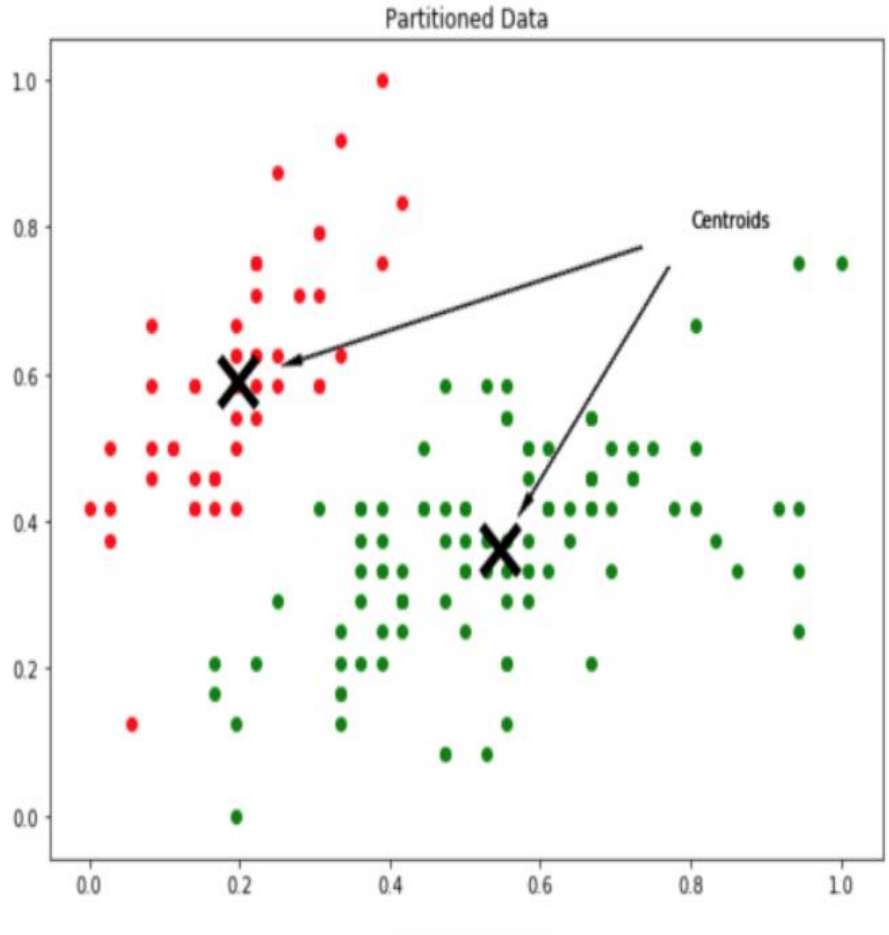

Рисунок 3.3. Використання центроїдів для розподіленя даних

Центроїди також є точками в просторі пошуку, що визначається нашими даними, і, оскільки кожен центроїд визначає групу, кожна точка даних буде призначена найближчому центроїду.

Тепер можна розглянути проблему кластеризації інформаційних повідомлень та перетворити її на завдання оптимізації.

Для чітко визначеної задачі оптимізації потрібен простір пошуку , набір d-вимірних вхідних змінних рішень і цільова функція. Якщо ми подивимося на кожну бджолу в штучній колонії як на цілісне вирішення проблеми кластеризації, то кожна бджола може являти собою повний набір центроїдів-кандидатів! Якщо ми працюємо з d-вимірним простором і хочемо виконати k-розбиття нашого набору даних, то кожна бджола буде k · d-вимірним вектором!

Тепер, коли ми визначили, як представляти наші вхідні змінні рішення, нам просто потрібно з'ясувати, як визначити межі простору пошуку та якою буде наша цільова функція.

Ми можемо нормалізувати весь набір даних із інтервалом [0, 1] і визначити нашу цільову функцію як межі від 0 до 1, де 0 – достовірна інформація, 1 – недостовірна інформація.

У підході роздільної кластеризації ми хочемо максимізувати відстань між двома окремими групами та мінімізувати внутрішню відстань усередині групи. Є кілька цільових функцій, які використовуються в літературі, але найвідоміша і використовується називається Sum of Squared Errors (SSE) – яка обчислюється за формулою:

$$SSE = \sum_{k=1}^{k} \sum_{\forall x_i \in C_k} \left|| x_i - \mu_k || \right|^2, \quad (3.1)$$

Сума квадратичних помилок (SSE) - це метрика кластеризації, і ідея, що стоїть за нею, дуже проста. По суті це числове значення, яке обчислює квадрат відстані кожного екземпляра в наших даних до його найближчого центроїду. Метою нашого оптимізаційного завдання буде мінімізація цієї функції.

Ми можемо використати нашу попередню структуру цільових функцій для реалізації суми квадратичних помилок.

Реалізація суми квадратичних помилок подана у Додатку Д.

В якості вихідного використаємо набір даних, що містить інформацію з характеристиками трьох об’єктів. З метою візуалізації ми будемо використовувати лише два виміри цього набору даних. Давайте перевіримо взаємозв'язок між двома вимірами цього набору даних:

Реалізація програмного коду подана в Додатку Е.

Вихідний розподіл даних поданий на рисунку 3.4.

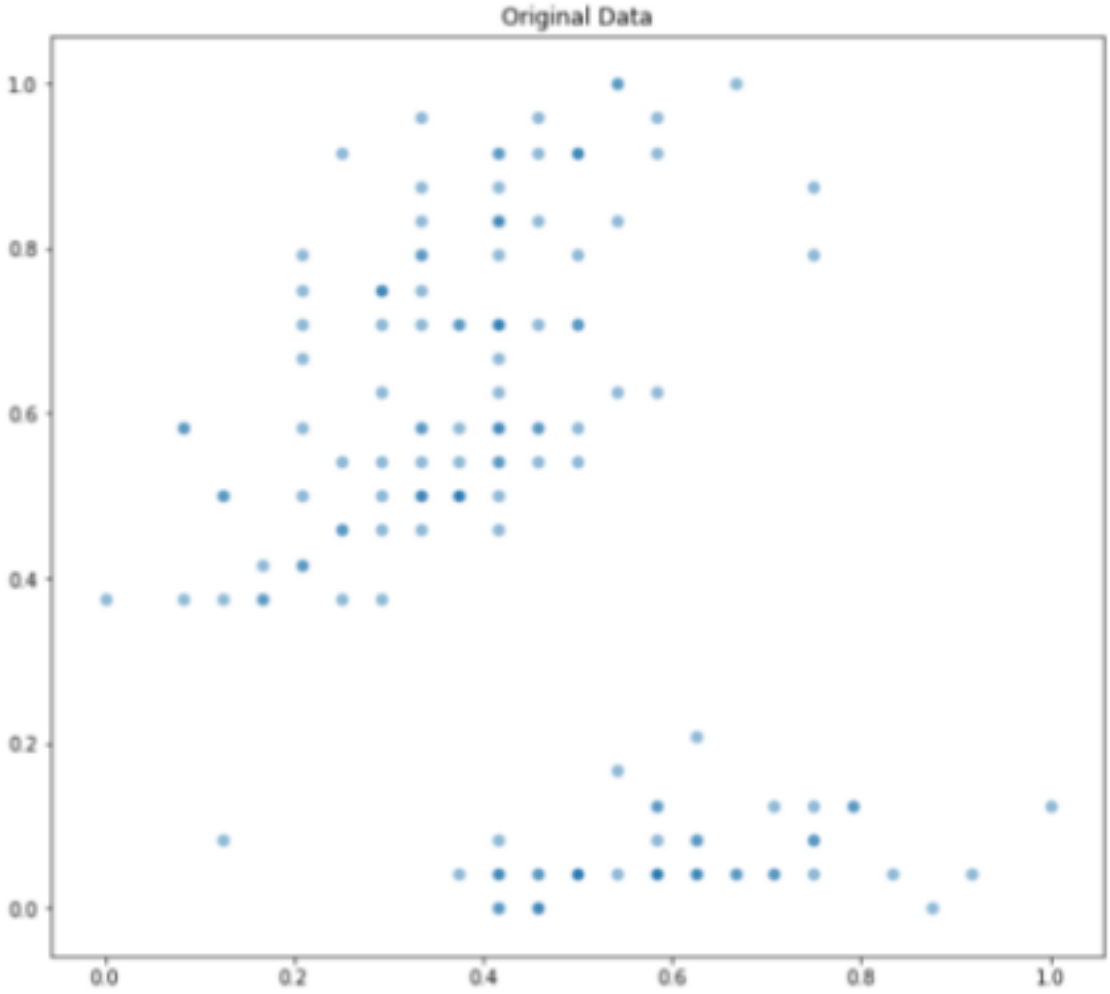

Рисунок 3.4. Вихідний розподіл даних

Оскільки ми будемо використовувати ці дані як еталонного тесту, ми вже знаємо, який їхній оптимальне розподіл, і воно визначається вихідним розподілом трьох типів кольорів (достовірна інформація, сумнівна, недостовірна інформація).

Ми можемо візуалізувати вихідний оптимальний розділ набору даних за допомогою коду, поданого в Додатку Є.

Отримаємо наступний розподіл, який зображено на рисунку 3.5.

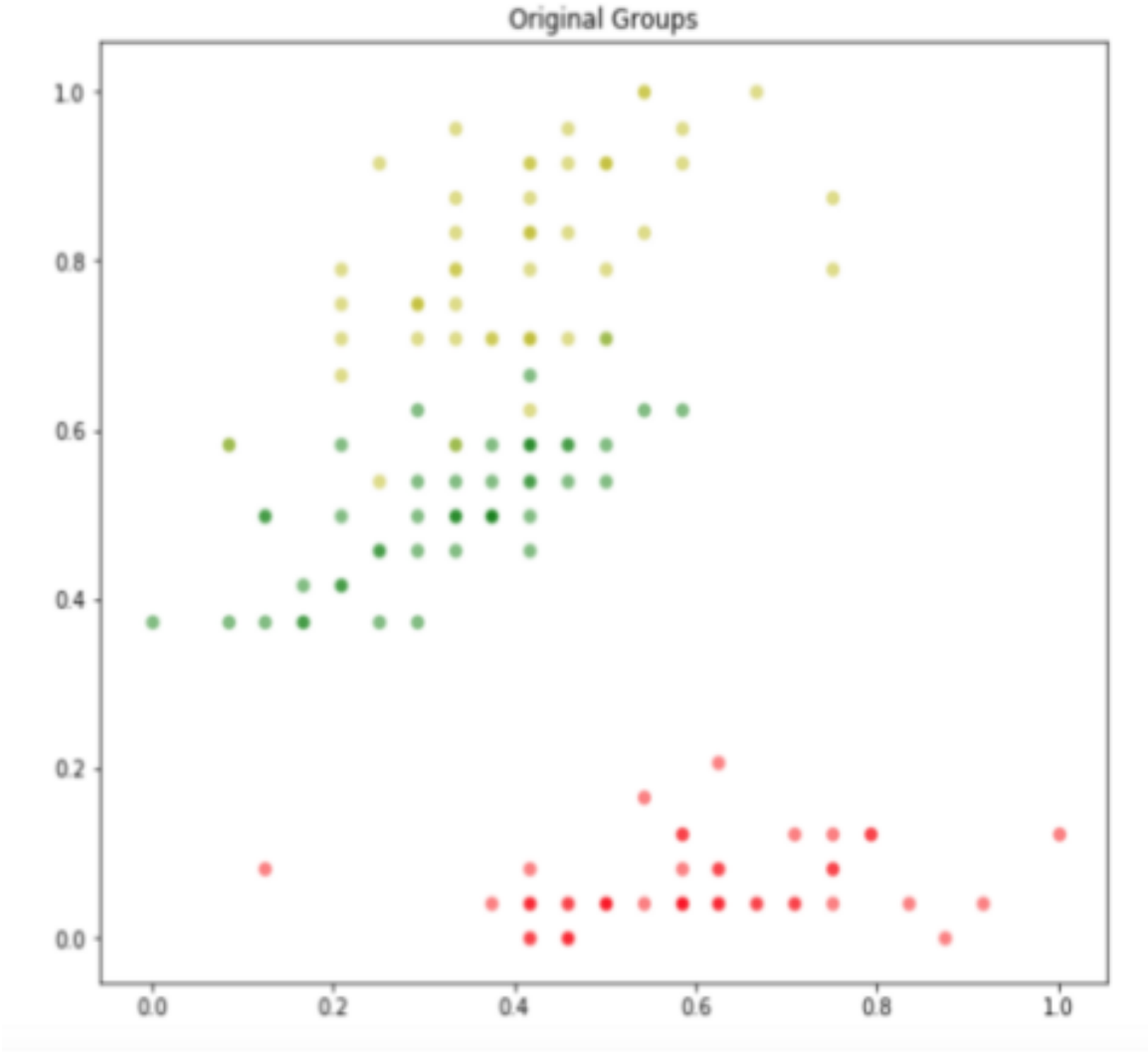

Рисунок 3.5. Вихідні групи в наборі даних

Тепер, коли ми знаємо, яким є вихідне оптимальне розбиття для цієї вибірки даних, з'ясуємо, чи здатний алгоритм ABC знайти дуже точне вирішення цієї проблеми.

Використаємо нашу цільову функцію Sum of Squared Errors – формула 3.1 – та встановимо кількість розділів рівним трьом.

Оскільки ініціалізація є випадковою, ймовірно, що порядок згенерованих центроїдів не збігається з порядком класів. Тому при побудові нашого висновку для алгоритму ABC кольори груп можуть не збігатися. Це не має великого значення, оскільки звертаємо увагу на те, наскільки добре виглядатимуть відповідні секційовані групи.

Відповідний код поданий в додатку Ж.

Розподіл, знайдений алгоритмом поданий на рисунку 3.6.

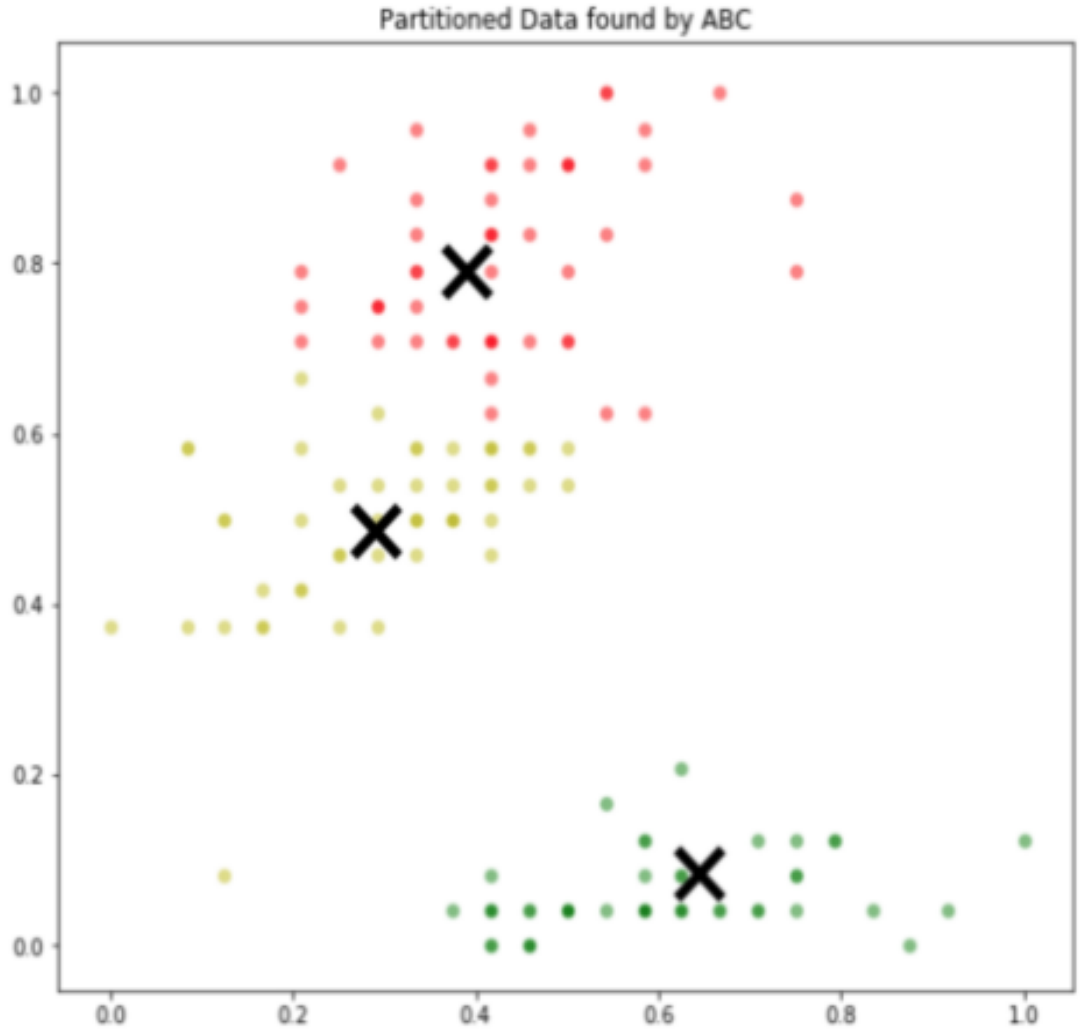

Рисунок 3.6. Розподіл, знайдений алгоритмом

Якщо ми подивимося на вихідний розділ і той, який був згенерований нашим алгоритмом ABC, ми побачимо, що він зміг знайти розділ, наближений до

оптимального. Це доводить, наскільки потужним є модифікований алгоритм ABC для кластеризації.

3.4 Дослідження отриманих результатів

Перевага алгоритмів біоінспірованих методів у порівнянні з класичними та градієнтними методами полягає у здатності дуже добре працювати з недиференційованими функціями, а також з мультимодальними функціями.

Щоб протестувати нашу структуру та перевірити, чи працює наш алгоритм ABC так, як очікувалося, ми можемо реалізувати наступний тестовий код та побудувати значення придатності для ітерацій та оцінити, наскільки добре пройшов процес мінімізації для кожної з функцій.

Тестовий код наданий у додатку З.

Ми можемо перевірити результати, проаналізувавши графік придатності в залежності від кількості ітерацій для кожної з наших еталонних функцій, ви також можете перевірити виведення оптимізатора і переконатися, що ABC отримав дуже хороше приблизне значення для оптимальної точки для наших еталонних функцій.

На рисунку 3.7 проілюстровано тестування роботи алгоритму із функцією «Sphere».

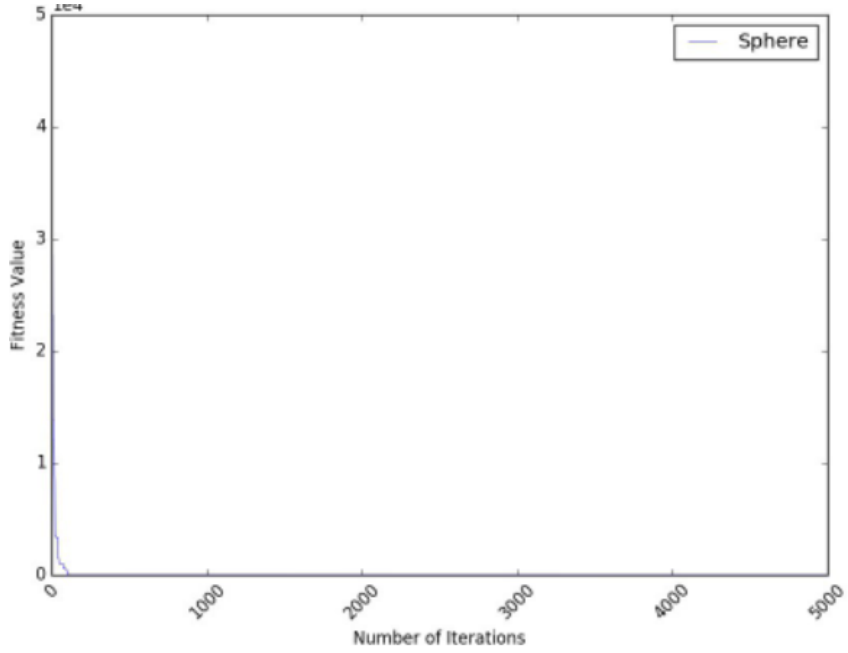

Рисунок 3.7. Тестування роботи алгоритму із функцією «Sphere»

На рисунку 3.8 проілюстровано тестування роботи алгоритму із функцією Розенброка.

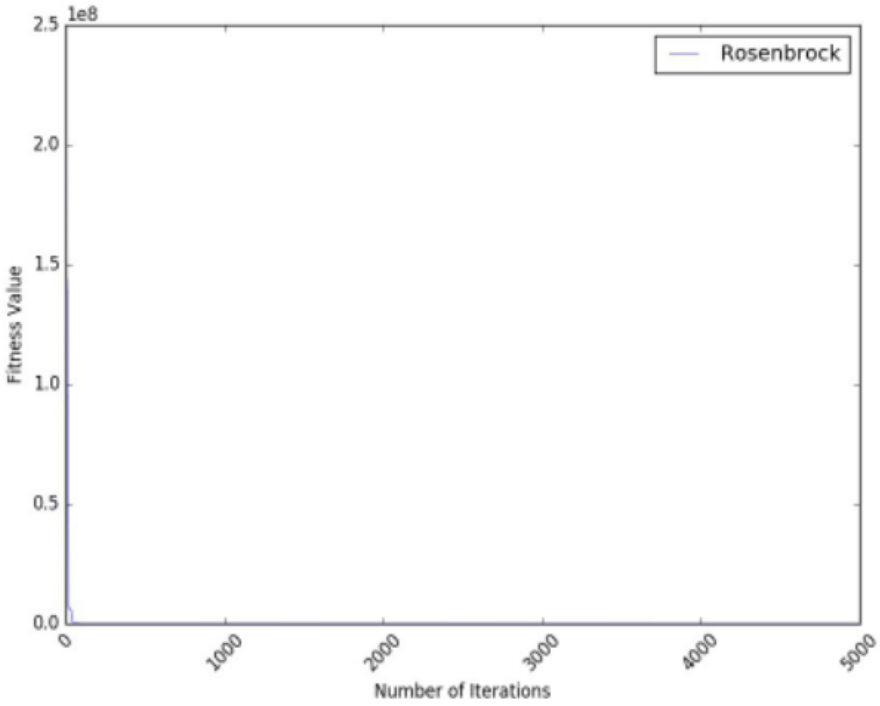

Рисунок 3.8 Тестування роботи алгоритму із функцією Розенброка

На рисунку 3.9 проілюстровано тестування роботи алгоритму із функцією Растригіна.

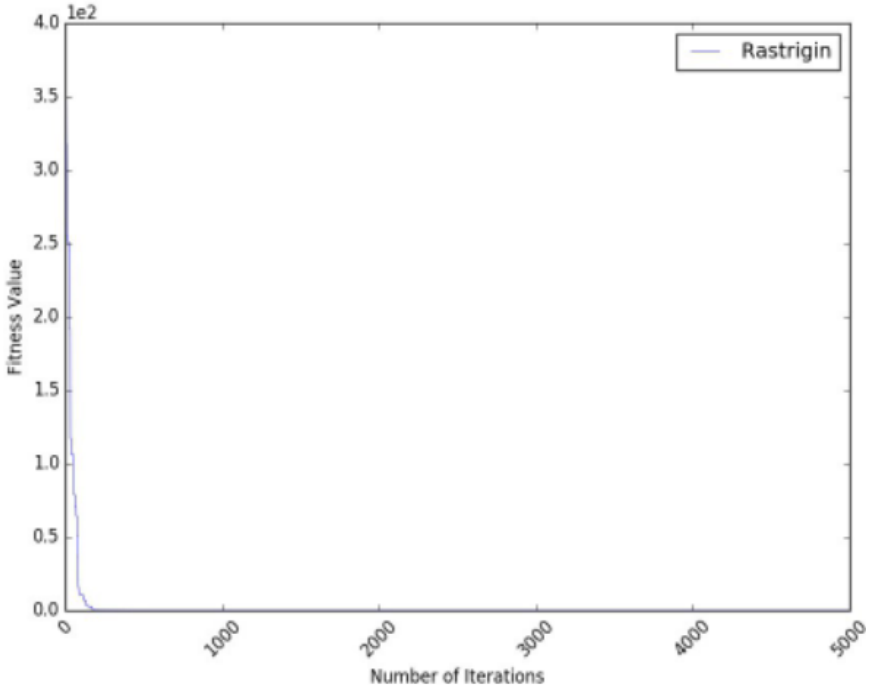

Рисунок 3.9. Тестування роботи алгоритму із функцією Растригіна

Ми також можемо подивитись, як пройшов процес удосконалення нашого алгоритму ABC.

Для цього звернемо увагу на атрибут absoluteity_tracking алгоритму (рисунок 3.10).

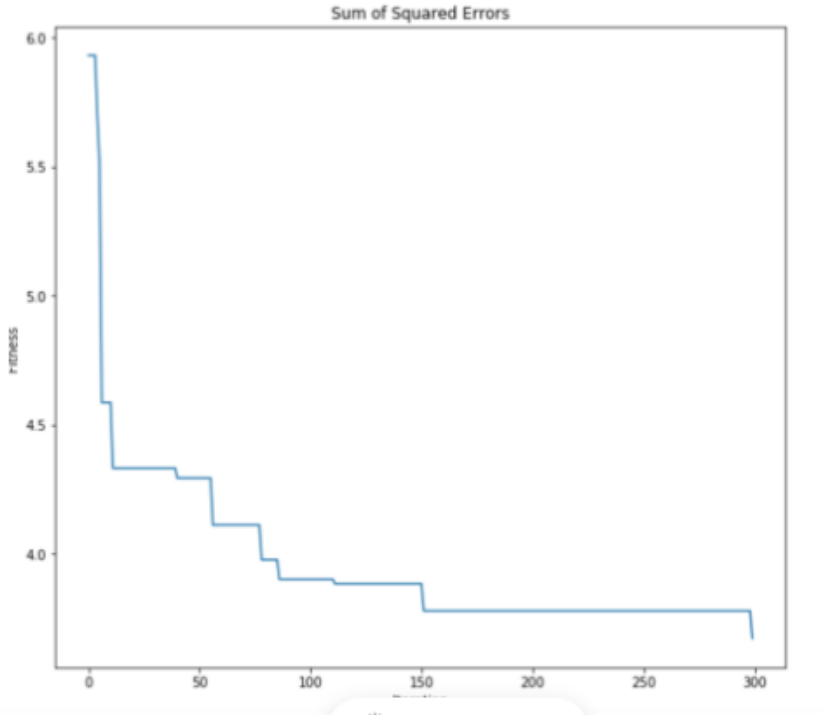

Рисунок 3.10. Тестування роботи удосконаленого алгоритму

Як і очікувалося, алгоритм дійсно ефективно мінімізував цільову функцію SSE. Ми бачимо, що він має деякі потужні механізми для вирішення задач оптимізації, і адаптація цих алгоритмів для вирішення реальних завдань, таких як виявлення недостовірної інформації — це лише питання того, як ми можемо звести ці проблеми до завдання оптимізації.

Висновки до третього розділу

В ході роботи поставлене завдання було представлено у вигляді функції, яку необхідно мінімізувати, а також застосовано кластерізацію інформації в інформаційному просторі. Проведено удосконалення алгоритму.

Аналіз результатів роботи алгоритму показав його високу ефективність.

ВИСНОВКИ

Доступність засобів масової комунікації, зрозумілість знань про світ забезпечили можливість відносного вирівнювання різних за соціально-статусними характеристиками груп щодо рівня інформованості про життя суспільства. Відповідно до соціальної стратифікації суспільства склалося дві основні наукові парадигми бачення впливу засобів масової комунікації як виразника соціальної структури суспільства, системи суспільної свідомості.

Однією із сучасних технологій впливу на людину є хай-х'юм-технології, тобто високі соціогуманітарні технології, основне призначення яких полягає у впливі на свідомість індивідів або груп з метою зміни їх поведінки і взаємин. Технології хай-х'юм є результатом конвергенції соціальних та інформаційних технологій, а також новітніх досягнень у галузі психології, нейрофізіології, етології та інших наук.

Найбільш ефективними, порівняно з іншими чинниками формування ціннісної системи, є мас-медіа, які впливають на формування ціннісних орієнтацій суспільства. Медіа задають певні аксіологічні моделі поведінки, з якими реципієнти співвідносять свої моральні принципи, ціннісні орієнтири і навіть виробляють стереотипи мислення під впливом трансльованих зразків.

Перебування людей під постійним впливом небезпечної інформації викликає трансформацію психіки, зміну поглядів, думок, відносин, ціннісних орієнтацій, мотивів, стереотипів, реакції, поведінки, дії особистості, призводить до формування викривленого світогляду та ціннісної дезінформації, провокує розвиток шкідливих звичок, викликає агресію, ненависть, роздратованість, стан невизначеності, сприяє виникненню психологічного дискомфорту у споживачів інформаційної продукції.

Технічний прогрес спричинив цілий ряд тектонічних змін у процесах виробництва та споживання інформації. Інтернет, стаючи все поширенішим, швидшим і дешевшим, дав мільярдам людей можливість ділитись інформацією як ніколи легко.

Ще одним наслідком прогресу став розвиток соціальних мереж, які зробили процес споживання інформації в мережі підконтрольним кільком великим компаніям і винесли їх у громадський простір.

Зростання кількості мобільних пристроїв та скорочення циклу виробництва новин збільшили швидкість поширення інформації. Прискорений обмін інформацією, що відбувається в реальному часі між учасниками мережі в деяких випадках знижує ймовірність того, що достовірність отриманої інформації буде поставлено під сумнів. В інших випадках потік вхідної інформації настільки величезний, що стає все складніше відрізняти достовірні відомості від брехні.

Для розробки алгоритму виявлення недостовірної інформації обраний удосконалений метод бджолиної колонії.

Цей метод заснований на поведінці колонії бджіл у природному середовищі. Існує два основних алгоритми – бджолиний алгоритм (Bee Algorithm) та алгоритм колонії бджіл (Artificial Bee Colony). Бджолиний алгоритм заснований на методі пошуку бджолами елітних ділянок. Основна перевага даного алгоритму – бджоли досліджують також ділянки, що знаходяться на околицях елітних, що дозволяє наблизити рішення до оптимального.

Засновані на поведінці колонії бджіл у природному середовищі. Існує два основних алгоритми – бджолиний алгоритм (Bee Algorithm) та алгоритм колонії бджіл (Artificial Bee Colony). Бджолиний алгоритм заснований на методі пошуку бджолами елітних ділянок. Основна перевага даного алгоритму – бджоли досліджують також ділянки, що знаходяться на околицях елітних, що дозволяє наблизити рішення до оптимального.

Бджолина сім'я складається з трьох типів бджіл: бджоли-співробітники, які будуть працювати над збиранням їжі у вулик із певного джерела їжі; бджоли - спостерігачі, які будуть патрулювати співробітників, щоб перевірити, коли конкретне джерело їжі більше не варте того; бджоли-розвідники, які будуть шукати нові місця для джерел їжі.

В алгоритмі ABC джерело їжі визначається як позиція у просторі пошуку, і спочатку кількість джерел їжі дорівнює кількості бджіл у вулику. Якість джерела їжі визначається значенням цільової функції цієї позиції.

В ході роботи поставлене завдання було представлено у вигляді функції, яку необхідно мінімізувати, а також застосовано кластерізацію інформації в інформаційному просторі. Проведено удосконалення алгоритму.

Аналіз результатів роботи алгоритму показав його високу ефективність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cormen, Thomas H.; Leiserson, Charles E.; Rivest, Ronald L.; Stein, Clifford (2001). "Section 24.3: Dijkstra's algorithm". Introduction to Algorithms (Second ed.). MIT Press and McGraw–Hill. pp. 595–601. ISBN 0-262-03293-7.

2. Жугай Н. Огляд статті Клея Ширкі «Політична сила соціальних медіа: технології, публічна сфера і політичні зміни», Комунікація: наук.- практ. зб. – 2012. – № 2. – С. 79 – 85.

3. Кавалеров А. А. Цінність у соціокультурній трансформації, — О.: Астропринт, 2011. — 224 с.

4. Колісник В. П. Становлення сучасного інформаційного суспільства та поширення спотвореної інформації, Інформаційне суспільство і держава: проблеми взаємодії на сучасному етапі: зб. наук. ст. та тез наук. повідомл. за матеріалами міжнар. наук.-практ. конф, м. Харків, 26 жовт. 2018 р., редкол.: С. Г. Серьогіна [та ін.]. – Х. : НДІ держ. буд-ва та місц. самоврядування, 2018. – С. 17 –21.

5. Коляденко В. А. Інфокомунікаційні технології як чинник політичної модернізації: автореф. дис. канд. політ. наук: 23.00.12 , Одес. нац. юрид. акад. – О., 2012. – 16 с.

6. Кондов К. В. Особливості реалізації соціального контролю в соціологічних теоріях інформаційного суспільства, Укр. інформац. простір: наук. журн. – К.: КНУКІМ, 2013. – С. 138 – 146.

7. Кудрявцева С. П., Колос В. В. Міжнародна інформація: навчальний посібник. Київ, 2015.

8. Лисак І. В. HI-HUME технологии и последствия их применения, Соврем. исслед. соц. проблем. – 2010. – № 4(04) – С. 259 – 263.

9. Марущак А. І. Інформаційне право: регулювання інформаційної діяльності: навчальний посібник. Київ, 2018.

10. Пархоменко О. В. Соціальна інформація як чинник інноваційного розвитку, Теоретичні і практичні аспекти економіки та інтелектуальної власності: зб. наук. пр. ПДТУ. – Маріуполь, 2010. – Т. 1. – С. 16 – 20.

11. Тофлер Е. Третя хвиля, пер. с англ. під ред. П. С. Гуревич. – М.: АСТ, 2009. – 261 с.

12. Фукуяма Ф. Великий розрив, пер. с англ. під заг. ред. А. В. Олександрової.: АСТ, 2008. – 474 с.

13. Цимбалюк В. С. Інформаційне право (основи теорії і практики): монографія. Київ, 2019

14. Чешко В. Ф. Стабильная адаптивная стратегия Homo sapiens. Биополитические альтернативы. Проблема Бога: монография, ИНЖЭК, 2016. – 596 с.

15. Baase, S. (2018). A Gift of Fire: Social, Legal, and Ethical Issues for Computing and the Internet. Publisher: Prentice Hall.

16. Commission High Level Group on Fake News and Online Disinformation, "A Multi-Dimensional Approach to Disinformation: Report of the Independent High-Level Group on Fake News and Online Disinformation," опубліковано в 2017 р., стр. 12.

17. N. DiRienzo, J. N. Pruitt, and A. V Hedrick, "The combined behavioural tendencies of predator and prey mediate the outcome of their interaction," Anim. Behav., vol. 86, no. 2, pp. 317–322, 2018.

18. F. Dressler and O. B. Akan, "A survey on bio-inspired networking," Comput. Networks, vol. 54, no. 6, pp. 881–900, 2020.

19. Dean Jackson, "Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and 'Fake News,'" [Електронний ресурс]. – Режим доступу: https://www.ned.org/issue-briefdistinguishing-disinformation-from-propaganda-misinformation-and-fake-news

20. Natalie Jomini Stroud и др., "Making Sense of Information and Judging its Credibility," Understanding and Addressing the Disinformation Ecosystem,

Annenberg School for Communication, [Електронний ресурс]. – Режим доступу: https://firstdraftnews.org/wp-content/

21. Karaboga D. An idea based on honey bee swarm for numerical optimization, Technical Report TR06, Erciyes University, Engineering Faculty, Computer Engineering Department, 2005.

22. Kennedy J, Eberhart R. Particle swarm optimization, Proceedings of IEEE International conference on Neural Networks. – 2005. – P. 1942-1948

23. C. Low, Y. Chen, and M. Wu, “Understanding the determinants of cloud computing adoption,” Ind. Manag. Data Syst., vol. 111, no. 7, pp. 1006–1023, 2021.

24. F. A. C. Polack, “Self-organisation for survival in complex computer architectures,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6090 LNCS, pp. 66–83, 2020.

25. C. Priami, “Algorithmic systems biology,” Commun. ACM, vol. 52, no. 5, pp. 80–88, 2019.

26. A. H. Sayed, “Adaptive networks,” Proc. IEEE, vol. 102, no. 4, pp. 460–497, 2014.

27. M. Dorigo and L. M. Gambardella, ―Ant colony system: A cooperative learning approach to the traveling salesman problem,‖ IEEE Transactions on Evolutionary Computation, vol. 1, no. 1. – 1997. – PP. 53-66.

28. T. Stützle and H. H. Hoos, ―MAX-MIN ant system‖ Future Generation Computer Systems, vol. 16, no. 9. – 2000. – PP. 889-914.

29. Y. Zhou, ―Runtime analysis of an ant colony optimization algorithm for TSP instances,‖ IEEE Transactions on Evolutionary Computation, vol. 13, no. 5. – 2009. – PP. 1083-1092.

30. G. Reinelt. Tsplib. Heidelberg University. Germany. [Online]. Available: http://comopt.ifi.uniheidelberg.de/software/TSPLIB95

31. T. Stützle. Acotsp. (Software package). [Online]. Available: http://www.acometaheuristic.org/acocode/public-software.html

32. Seyedali Mirjalili, Seyed Mohammad Mirjalili, Andrew Lewis. Grey Wolf Optimizer, 2014.

33. Eren T., Belhumeur P., Anderson B. et al. A framework for maintaining formation based on rigidity, Proc. of the 15th IFAC World Congress. Vol. 15. Barcelona: International Federation of Automatic Control, 2002. P. 1306–1306.

34. Olfati-Saber R., Fax J. A., Murray R. M. Consensus and Cooperation in Networked Multi-Agent Systems, Proceedings of the IEEE. 2007. Vol. 95, N 1. P. 215–233.

35. Lalish E., Morgansen K., Tsukamaki T. Formation tracking control using virtual structures and deconfliction, Proceedings of the 2006 IEEE Conference on Decision and Control. San Diego: IEEE, 2006. P. 5699–5705.

36. Lewis M. A., Tan K. High precision formation control of mobile robots using virtual structures, Autonomous Robots. 1997. Vol. 4, N 4. P. 387–403.

ДОДАТОК А.

Реалізація класу ArtificialBee в Python

```
import
numpy
as np


    from scipy import optimize
    from deap.benchmarks import schwefel


    from abc import ABCMeta
    from abc import abstractmethod
    from six import add_metaclass



    @add_metaclass(ABCMeta)
    class ObjectiveFunction(object):


        def __init__(self, name, dim, minf, maxf):
            self.name = name
            self.dim = dim
            self.minf = minf
            self.maxf = maxf


        def sample(self):
            return np.random.uniform(low=self.minf, high=self.maxf, size=self.dim)


        def custom_sample(self):
            return np.repeat(self.minf, repeats=self.dim) \
                   + np.random.uniform(low=0, high=1, size=self.dim) *\
                   np.repeat(self.maxf - self.minf, repeats=self.dim)


        @abstractmethod
        def evaluate(self, x):
            pass
```

```
class Sphere(ObjectiveFunction):

    def __init__(self, dim):
        super(Sphere, self).__init__('Sphere', dim, -100.0, 100.0)

    def evaluate(self, x):
        return sum(np.power(x, 2))



class Rosenbrock(ObjectiveFunction):

    def __init__(self, dim):
        super(Rosenbrock, self).__init__('Rosenbrock', dim, -30.0, 30.0)

    def evaluate(self, x):
        return optimize.rosen(x)



class Rastrigin(ObjectiveFunction):

    def __init__(self, dim):
        super(Rastrigin, self).__init__('Rastrigin', dim, -5.12, 5.12)

    def evaluate(self, x):
        return 10 * len(x)\
               + np.sum(np.power(x, 2) - 10 * np.cos(2 * np.pi * np.array(x)))



class Schwefel(ObjectiveFunction):

    def __init__(self, dim):
        super(Schwefel, self).__init__('Schwefel', dim, -500.0, 500.0)
```

```
def evaluate(self, x):
    return schwefel(x)[0]
```

ДОДАТОК Б.

Реалізація класу EmployeeBee

```
import
numpy
as np


    from copy import deepcopy
    from abc import ABCMeta
    from six import add_metaclass



    @add_metaclass(ABCMeta)
    class ArtificialBee(object):

        TRIAL_INITIAL_DEFAULT_VALUE = 0
        INITIAL_DEFAULT_PROBABILITY = 0.0

        def __init__(self, obj_function):
            self.pos = obj_function.custom_sample()
            self.obj_function = obj_function
            self.minf = obj_function.minf
            self.maxf = obj_function.maxf
            self.fitness = obj_function.evaluate(self.pos)
            self.trial = ArtificialBee.TRIAL_INITIAL_DEFAULT_VALUE
            self.prob = ArtificialBee.INITIAL_DEFAULT_PROBABILITY

        def evaluate_boundaries(self, pos):
            if (pos < self.minf).any() or (pos > self.maxf).any():
                pos[pos > self.maxf] = self.maxf
                pos[pos < self.minf] = self.minf
            return pos

        def update_bee(self, pos, fitness):
            if fitness <= self.fitness:
                self.pos = pos
                self.fitness = fitness
                self.trial = 0
            else:
```

```
            self.trial += 1


    def reset_bee(self, max_trials):
        if self.trial >= max_trials:
            self.__reset_bee()


    def __reset_bee(self):
        self.pos = self.obj_function.custom_sample()
        self.fitness = self.obj_function.evaluate(self.pos)
        self.trial = ArtificialBee.TRIAL_INITIAL_DEFAULT_VALUE
        self.prob = ArtificialBee.INITIAL_DEFAULT_PROBABILITY
```

ДОДАТОК В.

Реалізація класу OnlookerBee

```
lass
OnLookerBee(ArtificialBee):


                    def onlook(self, best_food_sources, max_trials):
                        candidate = np.random.choice(best_food_sources)
                        self.__exploit(candidate.pos, candidate.fitness, max_trials)


                    def __exploit(self, candidate, fitness, max_trials):
                        if self.trial <= max_trials:
                            component = np.random.choice(candidate)
                            phi = np.random.uniform(low=-1, high=1, size=len(candidate))
                            n_pos = candidate + (candidate - component) * phi
                            n_pos = self.evaluate_boundaries(n_pos)
                            n_fitness = self.obj_function.evaluate(n_pos)


                            if n_fitness <= fitness:
                                self.pos = n_pos
                                self.fitness = n_fitness
                                self.trial = 0
                            else:
                                self.trial += 1
```

ДОДАТОК Г.

Реалізація повного алгоритму ABC

```
class
ABC(object):

                def __init__(self, obj_function, colony_size=30, n_iter=5000, max_trials=100):
                    self.colony_size = colony_size
                    self.obj_function = obj_function


                    self.n_iter = n_iter
                    self.max_trials = max_trials


                    self.optimal_solution = None
                    self.optimality_tracking = []


                def __reset_algorithm(self):
                    self.optimal_solution = None
                    self.optimality_tracking = []


                def __update_optimality_tracking(self):
                    self.optimality_tracking.append(self.optimal_solution.fitness)


                def __update_optimal_solution(self):
                    n_optimal_solution = \
                        min(self.onlokeer_bees + self.employee_bees,
                            key=lambda bee: bee.fitness)
                    if not self.optimal_solution:
                        self.optimal_solution = deepcopy(n_optimal_solution)
                    else:
                        if n_optimal_solution.fitness < self.optimal_solution.fitness:
                            self.optimal_solution = deepcopy(n_optimal_solution)


                def __initialize_employees(self):
                    self.employee_bees = []
                    for itr in range(self.colony_size // 2):
                        self.employee_bees.append(EmployeeBee(self.obj_function))
```

```
def __initialize_onlookers(self):
    self.onlokeer_bees = []
    for itr in range(self.colony_size // 2):
        self.onlokeer_bees.append(OnLookerBee(self.obj_function))


def __employee_bees_phase(self):
    map(lambda bee: bee.explore(self.max_trials), self.employee_bees)


def __calculate_probabilities(self):
    sum_fitness = sum(map(lambda bee: bee.get_fitness(), self.employee_bees))
    map(lambda bee: bee.compute_prob(sum_fitness), self.employee_bees)


def __select_best_food_sources(self):
    self.best_food_sources =\
        filter(lambda bee: bee.prob > np.random.uniform(low=0, high=1),
               self.employee_bees)
    while not self.best_food_sources:
        self.best_food_sources = \
            filter(lambda bee: bee.prob > np.random.uniform(low=0, high=1),
                   self.employee_bees)


def __onlooker_bees_phase(self):
    map(lambda bee: bee.onlook(self.best_food_sources, self.max_trials),
        self.onlokeer_bees)


def __scout_bees_phase(self):
    map(lambda bee: bee.reset_bee(self.max_trials),
        self.onlokeer_bees + self.employee_bees)


def optimize(self):
    self.__reset_algorithm()
    self.__initialize_employees()
    self.__initialize_onlookers()
    for itr in range(self.n_iter):
        self.__employee_bees_phase()
        self.__update_optimal_solution()


        self.__calculate_probabilities()
        self.__select_best_food_sources()
```

```
self.__onlooker_bees_phase()
self.__scout_bees_phase()


self.__update_optimal_solution()
self.__update_optimality_tracking()
print("iter: {} = cost: {}"
      .format(itr, "%04.03e" % self.optimal_solution.fitness))
```

ДОДАТОК Д.

Реалізація суми квадратичних помилок

```
@add_metaclass(ABCMeta)
class PartitionalClusteringObjectiveFunction(ObjectiveFunction):


    def __init__(self, dim, n_clusters, data):
        super(PartitionalClusteringObjectiveFunction, self)\
            .__init__('PartitionalClusteringObjectiveFunction', dim, 0.0, 1.0)
        self.n_clusters = n_clusters
        self.centroids = {}
        self.data = data


    def decode(self, x):
        centroids = x.reshape(self.n_clusters, self.dim)
        self.centroids = dict(enumerate(centroids))


    @abstractmethod
    def evaluate(self, x):
        pass

class SumOfSquaredErrors(PartitionalClusteringObjectiveFunction):


    def __init__(self, dim, n_clusters, data):
        super(SumOfSquaredErrors, self).__init__(dim, n_clusters, data)
        self.name = 'SumOfSquaredErrors'


    def evaluate(self, x):
        self.decode(x)


        clusters = {key: [] for key in self.centroids.keys()}
        for instance in self.data:
            distances = [np.linalg.norm(self.centroids[idx] - instance)
                         for idx in self.centroids]
            clusters[np.argmin(distances)].append(instance)


        sum_of_squared_errors = 0.0
        for idx in self.centroids:
            distances = [np.linalg.norm(self.centroids[idx] - instance)
```

```
                for instance in clusters[idx]]
            sum_of_squared_errors += sum(np.power(distances, 2))
        return sum_of_squared_errors
```

ДОДАТОК Е.

Реалізація програмного коду

```
import
matplotlib.pyplot
as plt
```

```
from abc import ABC
from objection_function import SumOfSquaredErrors


from sklearn.datasets import load_iris
from sklearn.preprocessing import MinMaxScaler


data = MinMaxScaler().fit_transform(load_iris()['data'][:, [1,3]])
plt.figure(figsize=(9,8))
plt.scatter(data[:,0], data[:,1], s=50, edgecolor='w', alpha=0.5)
plt.title('Original Data')
```

ДОДАТОК Є.

Код вихідного оптимального розділу набору даних

```
colors
=
['r',
'g',
'y']
      target = load_iris()['target']


      plt.figure(figsize=(9,8))
      for instance, tgt in zip(data, target):
          plt.scatter(instance[0], instance[1], s=50,
                      edgecolor='w', alpha=0.5, color=colors[tgt])
      plt.title('Original Groups')
```

ДОДАТОК Ж.

Реалізація удосконаленого алгоритму

```
objective_function      =
SumOfSquaredErrors(dim=6,
n_clusters=3, data=data)
                        optimizer = ABC(obj_function=objective_function, colony_size=30,
                                        n_iter=300, max_trials=100)
                        optimizer.optimize()


                        def decode_centroids(centroids, n_clusters, data):
                            return centroids.reshape(n_clusters, data.shape[1])

                        centroids = dict(enumerate(decode_centroids(optimizer.optimal_solution.pos,
                                                                    n_clusters=3, data=data)))


                        def assign_centroid(centroids, point):
                            distances = [np.linalg.norm(point - centroids[idx]) for idx in centroids]
                            return np.argmin(distances)

                        custom_tgt = []
                        for instance in data:
                            custom_tgt.append(assign_centroid(centroids, instance))


                        colors = ['r', 'g', 'y']
                        plt.figure(figsize=(9,8))
                        for instance, tgt in zip(data, custom_tgt):
                            plt.scatter(instance[0], instance[1], s=50, edgecolor='w',
                                        alpha=0.5, color=colors[tgt])


                        for centroid in centroids:
                            plt.scatter(centroids[centroid][0], centroids[centroid][1],
                                        color='k', marker='x', lw=5, s=500)
                        plt.title('Partitioned Data found by ABC')
```

ДОДАТОК З.

Тестовий код

```
import
numpy
as np
      import matplotlib.pyplot as plt


      from algorithm.abc import ABC


      from matplotlib.style import use


      from objection_function import Rastrigin
      from objection_function import Rosenbrock
      from objection_function import Sphere
      from objection_function import Schwefel




      use('classic')




      def get_objective(objective, dimension=30):
          objectives = {'Sphere': Sphere(dimension),
                        'Rastrigin': Rastrigin(dimension),
                        'Rosenbrock': Rosenbrock(dimension),
                        'Schwefel': Schwefel(dimension)}
          return objectives[objective]




      def simulate(obj_function, colony_size=30, n_iter=5000,
                   max_trials=100, simulations=30):
          itr = range(n_iter)
          values = np.zeros(n_iter)
          box_optimal = []
          for _ in range(simulations):
              optimizer = ABC(obj_function=get_objective(obj_function),
                              colony_size=colony_size, n_iter=n_iter,
```

```
                    max_trials=max_trials)
        optimizer.optimize()
        values += np.array(optimizer.optimality_tracking)
        box_optimal.append(optimizer.optimal_solution.fitness)
        print(optimizer.optimal_solution.pos)
    values /= simulations


    plt.plot(itr, values, lw=0.5, label=obj_function)
    plt.legend(loc='upper right')



def main():
    plt.figure(figsize=(10, 7))
    simulate('Rastrigin')
    plt.ticklabel_format(axis='y', style='sci', scilimits=(-2, 2))
    plt.xticks(rotation=45)
    plt.show()



if __name__ == '__main__':
    main()
```