МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

МЕЛЕШКО Єлизавета Владиславівна

УДК 004.89+004.942

МЕТОДОЛОГІЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ РЕКОМЕНДАЦІЙНИХ СИСТЕМ ДО ДЕСТАБІЛІЗУЮЧИХ ФАКТОРІВ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

05.13.05 – Комп'ютерні системи та компоненти

Автореферат
дисертації на здобуття наукового ступеня
доктора технічних наук

Черкаси – 2021

Дисертацією є рукопис.

Робота виконана на кафедрі обчислювальної техніки та програмування Національного технічного університету «Харківський політехнічний інститут» Міністерства освіти і науки України.

Науковий консультант: доктор технічних наук, професор
Семенов Сергій Геннадійович,
Національний технічний університет «Харківський політехнічний інститут», завідувач кафедри обчислювальної техніки та програмування.

Офіційні опоненти: доктор технічних наук, професор
Єременко Володимир Станіславович,
Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського», завідувач кафедри інформаційно-вимірювальної техніки.

доктор технічних наук,
старший науковий співробітник
Чемерис Олександр Анатолійович,
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, заступник директора з наукової роботи.

доктор технічних наук, професор
Можаєв Олександр Олександрович,
Харківський національний університет внутрішніх справ Міністерства внутрішніх справ України, професор кафедри інформаційних технологій.

Захист відбудеться «9» лютого 2021 року о $12^{\underline{00}}$ на засіданні спеціалізованої вченої ради Д 73.052.04 при Черкаському державному технологічному університеті за адресою: 18006, м. Черкаси, бул. Шевченка, 460, конференц-зала, 1 корпус.

З дисертацією можна ознайомитись в бібліотеці Черкаського державного технологічного університету за адресою: 18006, м. Черкаси, бул. Шевченка, 460.

Автореферат розісланий « 24 » грудня 2020 р.

Вчений секретар
спеціалізованої вченої ради
к.т.н., доцент Ю.Ю. Бондаренко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Актуальність дослідження зумовлена стрімким збільшенням у комп'ютерних мережах кількості контент-орієнтованих веб-ресурсів та віртуальних соціальних мереж, які використовують рекомендаційні системи. За допомогою рекомендаційних систем користувач швидше знаходить потрібний саме йому контент, а власник збільшує відвідуваність свого веб-ресурсу, а отже, і власний прибуток. Тому вони стають такою ж важливою частиною веб-сайтів, як і пошукові підсистеми, інколи доповнюючи їх, а інколи створюючи їм альтернативу.

В той же час, проведені дослідження показали, що рекомендаційні системи вразливі до ряду внутрішніх та зовнішніх дестабілізуючих факторів, що значно впливають на точність їх роботи, а отже, й ефективність використання як для користувачів, так і для власників веб-ресурсів. Прикладами внутрішніх дестабілізуючих факторів у рекомендаційних системах можуть бути проблема холодного старту та проблема недостатньої кількості і якості вхідних даних. Основним зовнішнім дестабілізуючим фактором у рекомендаційних системах є інформаційні атаки ін'єкцією профілів.

Найбільш важливими роботами в галузі дослідження, розробки та вдосконалення рекомендаційних систем є роботи зарубіжних та вітчизняних науковців, серед яких варто відзначити наступних: Річчі Ф., Рокач Л., Шапіра Б., Кантор П.Б., Джонс М., Берк Р., Мобашер Б., Вільямс Ч., Фанк С., Бернарді Л., Кастеллс П., Варгас С., Пасічник В.В., Артеменко О.І., Лобур М.В., Стех Ю.В.

Для тестування моделей та методів синтезу рекомендаційних систем досить важливим є створення програмних імітаційних моделей користувачів, об'єктів та інформаційних процесів веб-ресурсів та соціальних мереж для генерації навчальних і тестових вибірок даних, а також симуляції реакції користувачів на створені списки рекомендацій. Водночас для рекомендаційних систем таких моделей практично немає, переважно вони тестуються на відкритих наборах даних, що не дозволяє в повній мірі досліджувати реакцію користувачів на запропоновані рекомендації та вплив бот-мереж.

Найбільш важливими роботами у напрямку моделювання поведінки користувачів та інформаційних процесів у комп'ютерних мережах, спрямованими на широке застосування, є роботи зарубіжних та вітчизняних науковців, серед яких слід відзначити наступних: Барабаши А.-Л., Альберт Р., Трааг В., Губанов Д.О., Новіков Д.О., Чхартішвілі О.Г., Пасічник В.В., Ланде Д.В., Снарський А.О., Додонов О.Г.

Проведене дослідження відомих моделей та методів синтезу рекомендаційних систем показало, що на даний момент не в повній мірі вирішено питання забезпечення стійкості рекомендаційних систем до дестабілізуючих факторів, внаслідок чого вплив таких факторів значно знижує точність формування рекомендацій користувачам.

Таким чином, на сьогоднішній день в теорії і практиці функціонування рекомендаційних систем загострилося **протиріччя** між підвищенням вимог до точності пропозицій користувачам рекомендаційних систем, збільшенням ризиків впливу на цей процес внутрішніх і зовнішніх дестабілізуючих факторів та існуючим станом теоретичного обґрунтування, синтезу і практичної реалізації підсистем забезпечення стійкості до цих негативних впливів.

Подолати цю суперечність можна шляхом вирішення актуальної **науково-практичної проблеми** підвищення точності пропозицій рекомендаційних систем в умовах дестабілізуючих факторів у комп'ютерних мережах на основі розробки моделей та методів синтезу підсистеми забезпечення стійкості.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана у межах пріоритетних наукових напрямів, які охоплюють актуальні проблеми, відповідно до рішення Ради президентів академій наук України від 30 січня 2019 року «Про Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2019-2023 роки», «Інформатика» за темами: «Розроблення обчислювальних алгоритмів і процедур з метою вирішення практичних задач міждисциплінарного характеру для застосувань, що належать до науково-технічної та соціально-економічної сфер діяльності людини», «Розроблення математичних методів та систем моделювання об'єктів та процесів». Дисертаційну роботу виконано у межах зареєстрованих НДР Центральноукраїнського національного технічного університету: «Методи застосування штучних нейронних мереж в телекомунікаційних системах для обробки та аналізу даних» (ДР № 0116U008161) та «Моделювання та аналіз складних мереж та інформаційних систем» (ДР № 0119U003587), а також НДР Національного технічного університету «Харківський політехнічний інститут»: «Дослідження методів управління та захисту даних в комп'ютеризованих інформаційно-вимірювальних та розподілених системах» (ДР № 0119U002603).

Мета і задачі дослідження. Мета дисертаційної роботи – підвищення стійкості рекомендаційних систем соціальних мереж та веб-сервісів до внутрішніх та зовнішніх дестабілізуючих факторів у комп'ютерних мережах.

Мета дисертаційної роботи визначає необхідність розв'язання таких **основних задач:**

1. Дослідження моделей та методів синтезу рекомендаційних систем для соціальних мереж та контент-орієнтованих веб-сайтів у комп'ютерних мережах.
2. Розробка методу визначення динаміки ймовірностей перебування рекомендаційної системи в своїх можливих станах та методики отримання аналітичних співвідношень для безпосереднього розрахунку цих ймовірностей з метою створення на їх основі математичних моделей конкретних рекомендаційних систем.
3. Розробка математичної моделі динаміки ймовірностей перебування стійкої рекомендаційної системи в своїх можливих станах для створення на її основі методів формування списків рекомендацій, стійких до внутрішніх дестабілізуючих факторів.
4. Розробка методу та алгоритмів формування списків рекомендацій, стійких до внутрішніх дестабілізуючих факторів рекомендаційної системи.
5. Розробка математичної моделі динаміки ймовірностей перебування підсистеми інформаційної безпеки стійкої рекомендаційної системи в своїх можливих станах для створення на її основі методів формування списків рекомендацій, стійких до зовнішніх дестабілізуючих факторів.
6. Розробка методу та алгоритмів та способів програмного імітаційного моделювання користувачів, об'єктів та інформаційних процесів рекомендаційної системи для тестування алгоритмів її роботи.
7. Розробка методу та алгоритмів виявлення інформаційних атак на рекомендаційну систему.

8. Розробка методу, алгоритмів та способів ідентифікації профілів ботів і виявлення бот-мереж у рекомендаційних системах.

9. Обґрунтування достовірності одержаних результатів наукових досліджень.

Об'єктом дослідження є процес функціонування рекомендаційних систем соціальних мереж та веб-сайтів у комп'ютерних мережах.

Предметом дослідження є методологія забезпечення стійкості рекомендаційних систем в умовах дестабілізуючих факторів.

Методи дослідження. Для вирішення завдань математичного моделювання рекомендаційної системи використано теорію марківських та напівмарківських процесів, теорію графів, теорію складних мереж та теорію ймовірностей. Для створення програмної імітаційної моделі використано методи об'єктно-орієнтованого програмування та методи роботи з графовими базами даних. Для розробки методів синтезу рекомендаційних систем та підсистем забезпечення стійкості також було використано теорію статистичної обробки даних, теорію штучного інтелекту, теорію інформаційної безпеки та теорію технічного аналізу.

Наукова новизна одержаних результатів полягає у такому:

– *Вперше розроблено* метод визначення динаміки ймовірностей перебування рекомендаційної системи в своїх можливих станах з використанням математичного апарату марківських та напівмарківських процесів, що дає можливість встановлення зв'язку між набором щільності розподілу випадкових тривалостей перебування системи у цих станах і функціями опису динаміки ймовірностей станів для визначення ймовірностей перебування конкретної рекомендаційної системи в своїх можливих станах в довільний момент часу.

– *Вперше розроблено* математичну модель стійкої рекомендаційної системи на основі запропонованого методу визначення динаміки ймовірностей перебування системи в своїх можливих станах, що дозволило здійснити оптимізацію загальних витрат на обслуговування системи в умовах внутрішніх дестабілізуючих факторів.

– *Удосконалено* метод колаборативної фільтрації, який відрізняється від існуючих використанням продукційних правил для визначення подоби користувачів та використанням показників активності користувачів для формування рекомендацій, що дозволило підвищити стійкість системи у випадку недостатньої кількості вхідних даних та під час холодного старту.

– *Вперше розроблено* математичну модель підсистеми інформаційної безпеки стійкої рекомендаційної системи на основі запропонованого методу визначення динаміки ймовірностей перебування системи в своїх можливих станах, що дозволило визначити оптимальну частоту перевірки на наявність інформаційної атаки та профілів ботів.

– *Вперше розроблено* метод імітаційного програмного моделювання користувачів та об'єктів рекомендаційної системи соціальної мережі або веб-ресурсу на основі існуючих і розроблених методів моделювання структури складних мереж та методів моделювання поведінки користувачів, що дозволило генерувати вхідні дані для тестування якості роботи алгоритмів формування рекомендацій.

– *Вперше розроблено* метод виявлення інформаційної атаки на рекомендаційну систему на основі аналізу трендів рейтингів об'єктів, що дозволило знизити кількість

витрат на моніторинг безпеки системи за рахунок зняття необхідності пошуку ботів при відсутності ознак атаки.

– *Вперше розроблено* метод виявлення бот-мереж у рекомендаційній системі на основі графової кластеризації та аналізу дій користувачів, що дозволило виявляти бот-мережі та розрізняти їх за множинами об’єктів атаки.

Практичне значення одержаних результатів. Отримані в дисертаційній роботі результати дають змогу підвищити стійкість рекомендаційних систем до внутрішніх та зовнішніх дестабілізуючих факторів, що в свою чергу дозволяє забезпечити достатній рівень точності та інших показників якості формування списків рекомендацій.

Практична цінність роботи полягає у такому:

– розроблено алгоритми програмного імітаційного моделювання користувачів, об’єктів та інформаційних процесів рекомендаційної системи, які дозволяють генерувати вхідні дані для тестування алгоритмів формування списків рекомендацій;

– розроблено вдосконалені алгоритми колаборативної фільтрації даних для формування більш точних списків рекомендацій користувачам веб-ресурсів на основі продукційних правил та використання показників активності користувачів;

– розроблено алгоритми виявлення наявності інформаційної атаки на рекомендаційну систему на основі аналізу трендів рейтингів об’єктів системи;

– розроблено алгоритми виявлення окремих профілів ботів на основі нейронних мереж та алгоритми виявлення бот-мереж на основі графової кластеризації та аналізу дій користувачів у рекомендаційній системі;

– розроблено методику одержання аналітичних співвідношень для розрахунку ймовірностей перебування стійкої рекомендаційної системи в своїх можливих станах в довільний момент часу для оптимізації частоти перерахунку вхідних даних для формування списків рекомендацій;

– розроблено методику одержання аналітичних співвідношень для розрахунку ймовірностей перебування підсистеми інформаційної безпеки стійкої рекомендаційної системи в своїх можливих станах для визначення оптимальної частоти перевірки на наявність інформаційної атаки та ботів.

Практичне значення отриманих результатів підтверджено відповідними актами впровадження. Результати дисертації впроваджені і використовуються у діяльності Компанії «Line Up», Державного підприємства «Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості», Державного підприємства «Харківський науково-дослідний інститут технологій машинобудування», Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса», а також використано у навчальному процесі Центральноукраїнського національного технічного університету та Національного технічного університету «Харківський політехнічний інститут».

Особистий внесок здобувача. Усі наукові результати дисертаційної роботи автор отримав самостійно. У друкованих працях, опублікованих у співавторстві, здобувачеві належать: [1] – дослідження стійкості серверу комп’ютерної мережі до завантаженості даними; [2, 3, 6, 27, 35, 36, 38] – дослідження методів виявлення інформаційних атак та впливів на системи обробки даних; [5] – дослідження методів

тестування обчислювальних алгоритмів; [7, 11, 20, 45, 48, 49, 60, 67-69] – дослідження методів побудови рекомендаційних систем; [10, 17, 19, 31, 33, 37, 39, 41, 64, 72] – дослідження методів програмного імітаційного моделювання складних систем та інформаційних процесів; [16, 18, 21, 59, 61, 65, 66, 73] – дослідження інформаційних загроз та методів захисту від них у рекомендаційних системах; [22] – розробка методу визначення динаміки ймовірностей перебування системи в своїх можливих станах з використанням математичного апарату марківських та напівмарківських процесів; [23] – розробка способу програмного імітаційного моделювання рекомендаційних систем для проведення тестування якості роботи їх алгоритмів; [24, 63, 70] – розробка способу ідентифікації ботів у рекомендаційних системах на основі нейронних мереж; [25] – розробка математичної моделі підсистеми інформаційної безпеки стійкої рекомендаційної системи; [26] – розробка методу колаборативної фільтрації на основі продукційних правил; [32, 33, 53] – розробка способу формування тестових вибірок для систем аналізу даних; [40, 50, 55, 57, 62, 71, 74-76] – дослідження методів обробки інформації з соціальних мереж та контент-орієнтованих веб-сайтів.

З робіт, що опубліковані у співавторстві, у дисертаційній роботі використовуються виключно результати, отримані особисто здобувачем.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися на таких наукових конференціях та семінарах: IEEE International Conference on Computational Intelligence and Knowledge Economy ICCIKE-2019 (United Arab Emirates, Dubai, 2019 р.); Міжнародна науково-технічна конференція «Сучасні засоби зв’язку» (Республіка Білорусь, Мінськ, 2016 р.); Всеукраїнська науково-практична конференція «Інформаційна безпека держави суспільства та особистості» (Кіровоград, 2015 р.); Міжнародний науково-практичний семінар «Комбінаторні конфігурації та їх застосування» (Кропивницький, 2016-2020 рр.); Всеукраїнська науково-практична конференція «Кібербезпека в Україні: правові та організаційні питання» (Одеса, 2016 р.); Міжнародна науково-практична конференція «Інформаційна безпека та комп’ютерні технології» (Кропивницький, 2017-2018 рр.); Міжнародна наукова конференція «Інформація. Комунікація. Суспільство» (Львів, 2017-2020 рр.); Всеукраїнська науково-практична Інтернет-конференція "Автоматика та комп’ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті (АКІТ)", (Кропивницький, 2017-2018 рр.); Міжнародна науково-практична конференція «Актуальні питання забезпечення кібербезпеки та захисту інформації» (с. Верхнє Студене – Київ, 2017, 2020 рр.); Міжнародна науково-технічна конференція «ITSEC» (Київ, 2018 р.); Всеукраїнська науково-практична конференція «Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS’2018)» (Миколаїв-Коблево, 2018 р.); Міжнародна науково-практична конференція «Контроль і управління в складних системах (КУСС-2018)» (Вінниця, 2018 р.); Міжнародна науково-практична конференція «Інформаційні технології та взаємодії (IT&I)» (Київ, 2018 р.); Всеукраїнська науково-практична конференція «Перспективні напрямки сучасної електроніки, інформатики і комп’ютерних систем» (Дніпро, 2018 р.); Науково-практична конференція «Інформатика, математика, автоматика (ІМА)» (Суми, 2019 р.); Міжнародна науково-практична конференція «Комплексне забезпечення якості технологічних процесів та

систем» (Чернігів, 2019-2020 р.); Міжнародна науково-практична конференція «Обробка сигналів і негаусівських процесів» (Черкаси, 2019 р.); Міжнародна наукова конференція «Безпека в сучасному світі» (Дніпро, 2019 р.); Всеукраїнська науково-практична Інтернет-конференція «Перспективні напрямки інформаційних і комп'ютерних систем та мереж, комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті» (Кропивницький, 2019 р.); Міжнародна науково-практична конференція «Математичне та програмне забезпечення інтелектуальних систем» (Дніпро, 2019 р.); Всеукраїнська науково-практична конференція «Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем MEICS» (Дніпро, 2019 р.); Міжнародна науково-практична конференція «Інформаційна безпека та інформаційні технології» (Кропивницький, 2020 р.).

Публікації. Основні положення дисертації опубліковано в 76 наукових працях, у тому числі: в 25 наукових статтях (з них 4 проіндексовано у базі даних Scopus; 2 – опубліковані у закордонних рецензованих виданнях; 22 – опубліковані у вітчизняних фахових наукових журналах, з яких 7 статей одноосібні), а також у 51 тезі доповідей (з них 1 проіндексовано у базі даних Scopus).

Структура роботи та її обсяг. Дисертація складається із анотації, вступу, шести розділів, загальних висновків, списку використаної літератури та додатків і містить 300 сторінок основного тексту, 42 рисунки, 31 таблицю, 231 джерело у списку літератури та 23 сторінки додатків. Загальний обсяг роботи 323 сторінки.

ОСНОВНА ЧАСТИНА

У **вступі** подано загальну характеристику роботи, обґрунтовано актуальність, сформульовано мету і задачі досліджень, відображено наукову новизну і практичну цінність отриманих результатів, наведено дані щодо їх апробації та впровадження.

У **першому розділі** проведено аналіз наукової літератури за темою дисертаційної роботи.

Показано, що на сьогоднішній день у комп'ютерних мережах для просування контенту, товарів та послуг все частіше використовують рекомендаційні системи – інструменти автоматичної генерації рекомендацій на основі вивчення персональних потреб користувачів веб-сайтів. Найчастіше вони застосовуються в електронній комерції, контент-орієнтованих веб-сайтах та соціальних мережах, а також у пошукових системах.

У даному розділі вводиться основна термінологія в області рекомендаційних систем, досліджено існуючі моделі та методи їх синтезу. Проведене дослідження показало, що на даний момент існують наступні моделі синтезу рекомендаційних систем: моделі сусідства, матричні факторизаційні моделі, моделі на основі класифікації та кластеризації даних, моделі на основі знань, моделі на основі даних про соціальні зв'язки користувачів, моделі зміни вподобань користувачів у часі та моделі робастних до інформаційних атак рекомендаційних систем. Існуючі методи синтезу рекомендаційних систем представлені наступними: методи колаборативної фільтрації, методи контентної фільтрації, методи фільтрації на основі знань про предметну область, методи соціальної фільтрації, методи на основі репутаційних систем, методи на основі асоціативних правил, методи контекстної фільтрації, гібридні методи тощо.

Також проведено дослідження внутрішніх та зовнішніх факторів, що можуть дестабілізувати роботу рекомендаційних систем. Виявлено, що до внутрішніх дестабілізуючих факторів відносяться: проблема холодного старту, проблема постійного холодного старту, проблема недостатньої кількості та якості вхідних даних, а також проблема бульбашки фільтрів. До зовнішніх дестабілізуючих факторів відносяться: інформаційні атаки для зміни рейтингів об'єктів системи та інформаційні атаки на приватність вподобань користувачів.

Проведено порівняльний аналіз існуючих моделей та методів синтезу рекомендаційних систем стосовно їх вразливості до дестабілізуючих факторів. Його результати показали, що переважна більшість відомих моделей та методів тією чи іншою мірою вразливі до дії внутрішніх та зовнішніх дестабілізуючих факторів. Підвищення стійкості рекомендаційних систем до дії негативних факторів дасть змогу підвищити й точність та інші показники якості їх роботи.

Таким чином, у першому розділі на основі проведеного аналізу визначено і обґрунтовано основні задачі дослідження, розв'язання яких необхідне для досягнення поставленої мети.

Другий розділ присвячений розробці методу визначення динаміки ймовірностей перебування рекомендаційної системи в своїх можливих станах на основі використання математичного апарату марківських та напівмарківських процесів. Даний метод може використовуватися для створення математичних моделей різних рекомендаційних систем та їх підсистем для оптимізації частоти періодичних планових дій у системі. Також у даному розділі обґрунтовано вибір підходів до забезпечення стійкості рекомендаційної системи в умовах дії зовнішніх та внутрішніх дестабілізуючих факторів у комп'ютерних мережах.

Рекомендаційна система є складною динамічною системою, яку можна розглядати з точки зору систем масового обслуговування. Виникнення зовнішніх чи внутрішніх дестабілізуючих факторів можна розглядати як вплив випадкового процесу. Тому для математичного моделювання динаміки ймовірностей станів рекомендаційної системи в процесі перебування під дією внутрішніх та зовнішніх дестабілізуючих факторів було запропоновано використати теорію марківських та напівмарківських процесів.

Етапи запропонованого методу визначення динаміки ймовірностей перебування рекомендаційної системи в своїх можливих станах:

Етап 1. Визначення скінченної множини станів конкретної рекомендаційної системи або її підсистеми, дослідження якої необхідно провести. Множину можливих станів та переходів між ними можна представити графічно у вигляді ланцюга Маркова.

Етап 2. Побудова системи інтегральних рівнянь, що пов'язує відомі щільності розподілу тривалостей перебування рекомендаційної системи в можливих станах і шукані функції, що описують ймовірнісну динаміку системи.

Етап 3. Розв'язання отриманої системи інтегральних рівнянь з використанням перетворення Лапласа. Результатом будуть співвідношення для розрахунку умовних ймовірностей знаходження системи в можливих станах в довільний момент часу t, якщо в початковий момент часу система знаходилася в стані H_0.

На основі запропонованого методу було розроблено методику отримання аналітичних співвідношень для розрахунку ймовірностей перебування рекомендаційної системи у двох можливих станах H_0 та H_1 в довільний момент часу t.

Для розробки методики було розглянуто загальний випадок для таких двох станів:

– Стан H_0 (назвемо його *Normal*) – нормальна робота системи, списки рекомендацій, що створюються користувачам, відповідають їх потребам та вподобанням.

– Стан H_1 (назвемо його *Problem*) – у цьому стані відбувається помітне зниження точності рекомендацій під впливом зовнішніх чи внутрішніх дестабілізуючих факторів.

Були введені наступні позначення: $f_{01}(t)$ – щільність розподілу тривалості перебування системи в стані H_0 до переходу в стан H_1; $f_{10}(t)$ – щільність розподілу тривалості перебування системи в стані H_1 до переходу в стан H_0; $G_{00}(t)$ – умовна ймовірність опинитися в стані H_0 в момент часу t, якщо в початковий момент часу об'єкт знаходиться в стані H_0; $G_{01}(t)$ – умовна ймовірність опинитися в стані H_1 в момент часу t, якщо в початковий момент часу об’єкт знаходиться в стані H_0; $G_{10}(t)$ – умовна ймовірність опинитися в стані H_0 в момент часу t, якщо в початковий момент часу об'єкт знаходиться в стані H_1; $G_{11}(t)$ – умовна ймовірність опинитися в стані H_1 в момент часу t, якщо в початковий момент часу об’єкт знаходиться в стані H_1.

Щільності розподілу тривалостей перебування в кожному із станів до переходу в інший стан для марківської системи:

$$f_{01}(t) = \lambda e^{-\lambda t}, \;\; f_{10}(t) = \mu e^{-\mu t}. \tag{1}$$

Щільності розподілу тривалостей перебування в кожному із станів до переходу в інший стан для напівмарківської системи:

$$f_{01}(t) = t\lambda^2 e^{-\lambda t}, \;\; f_{10}(t) = t\mu^2 e^{-\mu t}. \tag{2}$$

Система інтегральних рівнянь (4)-(7) утворює математичну модель, що пов’язує відомі щільності розподілу тривалостей перебування системи в можливих станах і шукані функції, що описують ймовірнісну динаміку системи.

$$G_{ij}(t) = \int_0^t f_{ik}(\tau) G_{kj}(t-\tau) d\tau, \;\; i = 1,2,\ldots,n, \;\; j = 1,2,\ldots,n. \tag{3}$$

$$G_{00}(t) = \left(1 - \int_0^t f_{01}(\tau) d\tau\right) + \int_0^t f_{01}(\tau) \cdot G_{10}(t-\tau) d\tau. \tag{4}$$

$$G_{01}(t) = \int_0^t f_{01}(\tau) \cdot G_{11}(t-\tau) d\tau. \tag{5}$$

$$G_{10}(t) = \int_0^t f_{10}(\tau) \cdot G_{00}(t-\tau) d\tau. \tag{6}$$

$$G_{11}(t) = \left(1 - \int_0^t f_{10}(\tau) d\tau\right) + \int_0^t f_{10}(\tau) \cdot G_{01}(t-\tau) d\tau. \tag{7}$$

Ця модель може бути використана для ймовірнісного аналізу будь-якої напівмарківської системи. Отриману систему рівнянь (4)-(7) можна розв’язати з використанням перетворення Лапласа.

Запропонований метод, на відміну від відомих, дозволяє не тільки розрахувати фінальний розподіл ймовірностей системи, але і значення ймовірності будь-якого стану в довільний момент часу t. Це дає можливість вирішувати задачі оцінки ефективності рекомендаційної системи в залежності від значень задаваємого набору її параметрів, а також здійснювати оптимізацію управління розподілом обмеженого ресурсу з метою підвищення ефективності рекомендаційної системи.

Також у даному розділі було проведено обґрунтування вибору шляхів забезпечення стійкості рекомендаційних систем до дестабілізуючих факторів. Під *стійкістю рекомендаційної системи* у даній роботі мається на увазі міра її здатності створювати релевантні та точні рекомендації користувачам, незважаючи на дію внутрішніх та зовнішніх дестабілізуючих факторів.

Було проведено дослідження існуючих показників стійкості рекомендаційних систем. Вони, як правило, використовуються для оцінки робастності системи до інформаційних атак. Як показало дослідження, після деякої адаптації, ці показники можна застосовувати і для визначення стійкості до внутрішніх негативних факторів.

Оцінити стійкість рекомендаційної системи можна вимірюючи показники її точності до та після виникнення дестабілізуючих факторів. Для оцінки стійкості рекомендаційної системи можна використовувати наступні показники.

Середній зсув прогнозування рейтингів об’єкта i для всіх користувачів:

$$\Delta_i = \sum_{u \in U_T} \frac{\Delta_{i,u}}{|U_T|}, \tag{8}$$

$$\Delta_{u,i} = p'_{u,i} - p_{u,i}, \tag{9}$$

де U_T – набір користувачів; $|U_T|$ – кількість елементів у наборі користувачів U_T; $\Delta_{i,u}$ – зсув прогнозування для кожної пари користувач-об’єкт (u, i); p і p' – прогнози до та після виникнення дестабілізуючого фактору відповідно.

Середній зсув прогнозування рейтингів для всіх об’єктів у тестовій виборці:

$$\overline{\Delta} = \sum_{i \in I_T} \frac{\Delta_i}{|I_T|}, \tag{10}$$

де I_T – набір об’єктів; $|I_T|$ – кількість елементів у наборі об’єктів I_T.

Зсув прогнозування дозволяє дослідити, як інформаційні атаки впливають на рейтинги цільових об’єктів. Однак навіть дуже сильні зміни у рейтингу об’єкту можуть не змінити його рекомендований статус. Наприклад, якщо початкова середня оцінка об’єкту дуже низька, навіть сильний її приріст недостатній для потрапляння у списки рекомендацій. Тому для оцінювання впливу інформаційної атаки на списки рекомендацій існує наступний показник – коефіцієнт звернень.

Коефіцієнт звернень для елементу i визначається як:

$$HitRatio_i = \sum_{u \in U_T} \frac{H_{i,u}}{|U_T|}, \tag{11}$$

де $H_{i,u}$ – функція оцінювання результату атаки, якщо цільовий об’єкт i потрапляє у список рекомендацій користувачу u вона приймає значення 1, інакше – 0.

Середнє значення коефіцієнту звернень може бути обчислене як:

$$\overline{HitRatio} = \sum_{i \in I_T} \frac{HitRatio_i}{|I_T|}. \tag{12}$$

Для оцінювання стійкості різних методів синтезу рекомендаційних систем формується два набори тестових даних: одні – в звичайному режимі роботи системи, інші – в умовах дії дестабілізуючих факторів. Для кожного набору даних створюються списки рекомендацій та обчислюються вищерозглянуті показники стійкості. Потім результати для тестових наборів порівнюються.

Якщо необхідно розробити стійку до дестабілізуючих факторів рекомендаційну систему, то задачу оптимізації можна сформулювати наступним чином:

$$d(R_n, R_a) \to \min, \tag{13}$$

де вектор R_n містить список прогнозованих оцінок (рекомендацій), сформований у нормальному режимі роботи системи; а вектор R_a містить список прогнозованих оцінок (рекомендацій), сформований під час дії дестабілізуючих факторів.

Вибір методів забезпечення стійкості рекомендаційної системи залежить від типу дестабілізуючих факторів та моделей і методів її синтезу. Основним шляхом забезпечення стійкості до внутрішніх дестабілізуючих факторів є гібридизація різних методів синтезу рекомендаційних систем, а до зовнішніх – розробка підсистем інформаційної безпеки для виявлення та нейтралізації діяльності бот-мереж.

Так як створити рекомендаційну систему, стійку до всіх видів інформаційних атак та внутрішніх помилок, складно та затратно, то раціональним кроком буде оцінити вартість збитків від виникнення дестабілізуючих факторів та вартість усунення цих факторів, щоб на основі отриманої інформації приймати рішення про доцільність внесення тих чи інших змін у систему, направлених на підвищення її стійкості.

У **третьому розділі** запропоновано математичну модель стійкої рекомендаційної системи для оптимізації загальних витрат на обслуговування системи та стійкі методи колаборативної фільтрації в умовах дії внутрішніх дестабілізуючих факторів. Досліджено показники якості роботи рекомендаційних систем. Наведено результати експериментів для визначення точності та стійкості розроблених методів та порівняння їх з відомими методами колаборативної фільтрації.

Математична модель стійкої рекомендаційної системи для оптимізації частоти перерахунку вхідних даних в умовах дії внутрішніх дестабілізуючих факторів для зменшення витрат на обслуговування системи представлена ланцюгом Маркова на рис. 1 та формулами (14)-(17) для марківських процесів і формулами (18)-(22) для напівмарківських процесів.

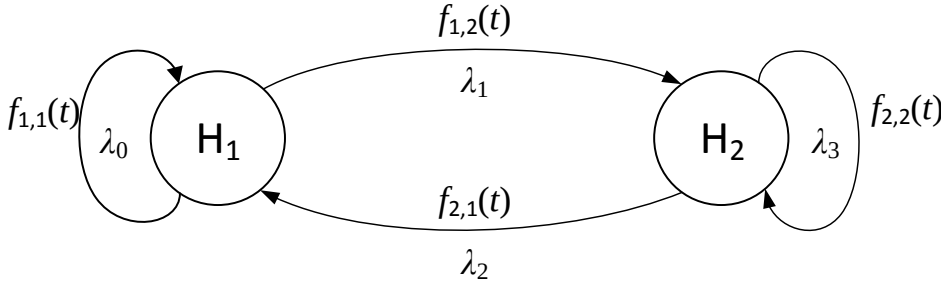

Рис. 1. Ланцюг Маркова для стійкої рекомендаційної системи в умовах внутрішніх дестабілізуючих факторів

Можливі стани рекомендаційної системи:

***H*₁** – Наявні дані актуальні: для прогнозування вподобань можна використовувати раніше отримані та обчислені дані (наприклад, раніше отримані коефіцієнти подоби користувачів, чи приховані фактори).

***H*₂** – Наявні дані більше не актуальні: треба завантажити нові дані користувачів та здійснити нові обчислення для визначення вхідних даних для рекомендаційної системи.

Використовуючи запропонований раніше у даній роботі метод визначення динаміки ймовірностей перебування рекомендаційної системи в своїх можливих

станах можна отримати наступні рівняння ймовірностей для марківських процесів:

$$G_{11}(t) = \frac{\lambda_0}{\lambda_1 + \lambda_0} + \frac{\lambda_1}{\lambda_1 + \lambda_0} \cdot e^{-(\lambda_1+\lambda_0)\cdot t}, \quad (14)$$

$$G_{12}(t) = \frac{\lambda_1}{\lambda_1 + \lambda_0} - \frac{\lambda_1}{\lambda_1 + \lambda_0} \cdot e^{-(\lambda_1+\lambda_0)\cdot t}, \quad (15)$$

$$G_{21}(t) = \frac{\lambda_3}{\lambda_2 + \lambda_3} - \frac{\lambda_3}{\lambda_2 + \lambda_3} \cdot e^{-(\lambda_2+\lambda_3)\cdot t}, \quad (16)$$

$$G_{22}(t) = \frac{\lambda_2}{\lambda_2 + \lambda_3} + \frac{\lambda_3}{\lambda_2 + \lambda_3} \cdot e^{-(\lambda_2+\lambda_3)\cdot t}. \quad (17)$$

Для напівмарківських процесів обчислення цих ймовірностей буде більш складним. Покажемо нижче спосіб визначення ймовірностей G_{11} та G_{12}.

$$D = \frac{(\lambda_0 + \lambda_1)^2}{4} - 2\lambda_0\lambda_1. \quad (18)$$

Якщо дискримінант $D > 0$, то:

$$G_{11}(t) = \alpha_0 + \alpha_1 e^{-(\lambda_1+\lambda_0)t} + \alpha_2 e^{-\left(\frac{\lambda_1+\lambda_0}{2}+\sqrt{D}\right)t} + \alpha_3 e^{-\left(\frac{\lambda_1+\lambda_0}{2}-\sqrt{D}\right)t}, \quad (19)$$

де $\alpha_0 = \frac{\lambda_0}{\lambda_1 + \lambda_0}, \alpha_1 = -\frac{\lambda_1(\lambda_1 - \lambda_0)}{2\lambda_0(\lambda_1 + \lambda_0)}, \alpha_2 = \alpha_3 = \frac{\lambda_1}{4\lambda_0} \mp \frac{\lambda_1(\lambda_1 - 3\lambda_0)}{4\lambda_0\sqrt{\lambda_1^2 - 6\lambda_1\lambda_0 + \lambda_0^2}}$.

Якщо дискримінант $D = 0$, то:

$$G_{11}(t) = \alpha_0 + \alpha_1 \cdot e^{-\frac{(\lambda_1+\lambda_0)}{2}t} + \left(\left(-\alpha_2 \cdot \frac{(\lambda_1 + \lambda_0)}{2} + \alpha_3\right)\cdot t + \alpha_2\right) \cdot e^{-\frac{(\lambda_1+\lambda_0)}{2}t}, \quad (20)$$

де $\alpha_0 = \frac{1}{2} - \frac{\sqrt{2}}{4}\ \alpha_1 = -\left(1 + \frac{3\sqrt{2}}{4}\right)\ \alpha_2 = \frac{2}{3} + \sqrt{2}\ \alpha_3 = \left(3 + 2\sqrt{2}\right)\lambda_0$.

Якщо, $D < 0$, то:

$$G_{11}(t) = \alpha_0 + \alpha_1 \cdot e^{-(\lambda_1+\lambda_0)\cdot t} + \alpha_2 \cdot \cos at \cdot e^{-\frac{(\lambda_1+\lambda_0)}{2}t} + \frac{\alpha_3 - \alpha_2 \cdot b}{a} \cdot \sin at \cdot e^{-\frac{(\lambda_1+\lambda_0)}{2}t}, \quad (21)$$

де $\alpha_0 = \frac{\lambda_0}{\lambda_1 + \lambda_0}$, $\alpha_1 = -\frac{\lambda_1(\lambda_1 - \lambda_0)}{2\lambda_0(\lambda_1 + \lambda_0)}, \alpha_2 = \frac{\lambda_1}{2\lambda_0}$, $\alpha_3 = \lambda_1$.

Ймовірність G_{12} буде визначатися за формулою (22):

$$G_{12}(t) = 1 - G_{11}. \quad (22)$$

На основі запропонованої математичної моделі було розроблено спосіб визначення загальних витрат рекомендаційної системи на завантаження та обчислення вхідних даних для формування списків рекомендацій.

Повні витрати рекомендаційної системи на збір та обробку вхідних даних для створення пропозицій користувачам пропонується визначати за формулою:

$$L = G_{1,1} \cdot K_1 \cdot \lambda_1 + G_{2,2} \cdot K_2 + (G_{2,2} + G_{2,1})K_3\lambda_2 \quad (23)$$

де K_1 – витрати на обслуговування системи у нормальному режимі роботи; K_2 – витрати (збитки) внаслідок неправильно створених рекомендацій; K_3 – витрати на

завантаження та перерахунок нових вхідних даних з інтенсивністю λ_2.

Також було розроблено спосіб визначення оптимальної частоти перерахунку вхідних даних. В рекомендаційній системі можна керувати частотою перерахунку вхідних даних v, що відповідає за значення параметру λ_2. Для того, щоб визначити оптимальну частоту перерахунку вхідних даних v_{opt}, треба знайти таке значення λ_2, при якому загальні збитки системи L будуть мінімальними. Тому, система має мінімальну збитковість при:

$$v_{opt} = \arg\min_{\lambda_2} L(\lambda_1,\lambda_2) = \arg\min_{\lambda_2} \left[G_{1,1} \cdot K_1 \cdot \lambda_1 + G_{2,2} \cdot K_2 + (G_{2,2} + G_{2,1}) K_3 \lambda_2\right]. \qquad (24)$$

Рівняння є нелінійним, тому його розв'язання в загальному випадку можливе лише за допомогою чисельних методів. Для прикладу, візьмемо наступні значення усіх видів витрат системи: K_1=1 *гр.од./хв*, K_2=5 *гр.од./хв*, K_3=3 *гр.од./хв*. Після проведемо табуляцію функції витрат для: λ_1 = 0.05, λ_2 = 0.05; 0.1; 0.15; 0.2; 0.25; 0.3; 0.35.

Таблиця 1. Приклад розрахунків для визначення оптимальної частоти перерахунку вхідних даних λ_2 для стійкої рекомендаційної системи

$v=\lambda_2$	0.05000	0.10000	0.15000	0.20000	0.25000	0.30000	0.35000	0.40000	0.45000
$G_{1,1}$	0.41770	0.41770	0.41770	0.41770	0.41770	0.41770	0.41770	0.41770	0.41770
$G_{2,2}$	1.00000	0.44440	0.34781	0.28571	0.24242	0.21052	0.18604	0.16666	0.15094
$G_{2,1}$	0.00000	0.55559	0.65218	0.71428	0.75757	0.78947	0.81395	0.83333	0.84905
L	5.02088	2.54293	2.20997	2.04945	1.98300	1.97351	2.00111	2.05421	2.12560

Графічне відображення побудованих точок, які поєднані плавною кривою показані на рис. 2. З графіку можна зробити висновок, що мінімальні витрати на повернення системи до стану H_1 зі стану H_2, а, отже, забезпечення необхідної точності її роботи при заданих параметрах, будуть при інтенсивності перерахунку даних λ_2 = 0.3, і витрати складатимуть L = 1.97351 умовних грошових одиниць за одиницю часу.

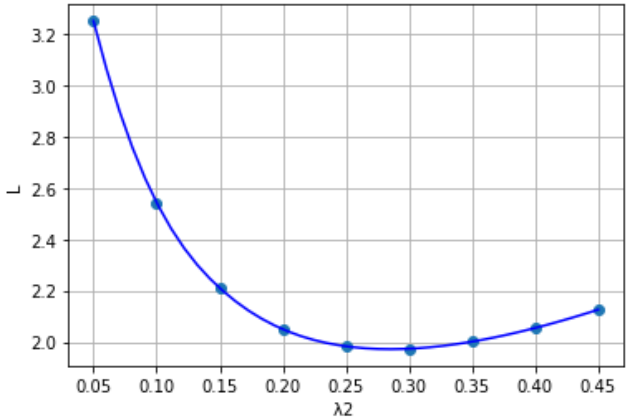

Рис. 2. Залежність розміру повних витрат рекомендаційної системи L від частоти перерахунку вхідних даних $v=\lambda_2$

У даному розділі також було розроблено метод колаборативної фільтрації на основі моделі сусідства, удосконалений за рахунок визначення відсутніх коефіцієнтів подоби користувачів за допомогою запропонованих продукційних правил.

Пропонується визначати відсутні коефіцієнти подоби для користувачів, у яких немає спільних дій для порівняння, за допомогою продукційних правил, заснованих на принципі транзитивності.

Продукційні правила – правила, які мають вигляд: **ЯКЩО** <умова>, **ТО** <подія>.

Запропоновані наступні продукційні правила (рис. 3-4):

1. **Якщо** коефіцієнт подоби користувачів *A* та *B* дорівнює *y* **та** коефіцієнт подоби користувачів *A* та *C* дорівнює *x*, **то** коефіцієнт подоби користувачів *B* та *C* дорівнює $z = [min(x, y), 1 – |x – y|]$.

2. **Якщо** для користувачів *C* та *B* є множина користувачів $\{A_1, A_1, \dots, A_n\}$, для яких відомі коефіцієнти подоби з користувачами *B* та *C*, **то** коефіцієнт подоби між *B* та *C* дорівнює: $z = z_1 \cap z_2 \cap \dots \cap z_n$.

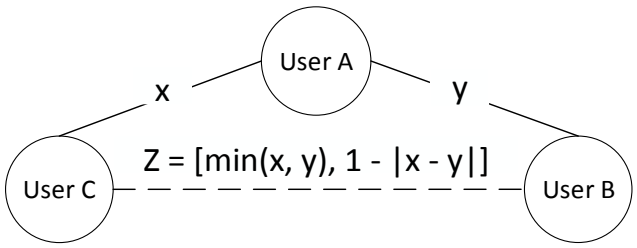

Рис. 3. Схематичне зображення продукційного правила 1

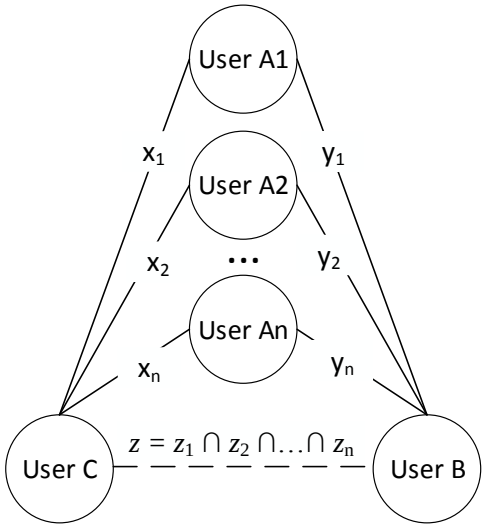

Рис. 4. Схематичне зображення продукційного правила 2

Було проведено серію експериментів для тестування розробленого методу з використанням відкритого набору даних MovieLens Datasets та розробленого на мові програмування Python програмного забезпечення з використанням графової СУБД Neo4j. Як показали експерименти, розроблений метод дозволяє збільшити загальну кількість рекомендацій в середньому для одного користувача у 1.8 разів та підвищити покриття каталогу в 2 рази без суттєвих коливань точності та повноти роботи системи.

Також було розроблено метод колаборативної фільтрації з врахуванням показників активності користувачів для підвищення стійкості системи до проблеми холодного старту.

Запропоновано у список рекомендацій користувачів, для яких не вдалося створити пропозиції іншими методами, додавати найпопулярніші об’єкти серед найактивніших користувачів. Такий підхід пропонується назвати експертно-орієнтованим, оскільки кожний користувач системи розглядається як експерт та має коефіцієнт експерта, що залежить від його активності, хоча може визначатися на основі й інших даних.

Етапи розробленого методу колаборативної фільтрації з врахуванням показників активності користувачів:

Етап 1. Вибираємо усіх користувачів, крім u_i, для якого формуються рекомендації.

Етап 2. Вибираємо всі об’єкти, яким поставили оцінки дані користувачі та розраховуємо для кожного об’єкту коефіцієнт його цікавості для користувача u_i:

$$k_{\text{int}}(o,u_i) = \sum_{j\geq 1,\, j\neq i}^{n} r_j \cdot k_{\text{exp}}(u_j), \tag{25}$$

де *o* – об’єкт, для якого розраховуємо коефіцієнт цікавості для u_i; *n* – кількість користувачів у рекомендаційній системі; k_{exp} – коефіцієнт експерта для *j*-того

користувача; r_j – оцінка, яку поставив j-тий користувач об'єкту o.

$$k_{\text{exp}}(u) = \frac{m_u}{\max(m_i)} \tag{26}$$

де m_u – кількість об'єктів, які оцінив u_j; $\max(m_i)$ – кількість об'єктів, які оцінив користувач, що оцінив найбільше об'єктів системи з поміж усіх користувачів.

Етап 3. Формуємо список усіх вибраних об'єктів, за необхідності, відкидаємо зі списку об'єкти, які вже оцінював користувач u_i.

Етап 4. Сортуємо список усіх об'єктів за спаданням коефіцієнту цікавості для u_i.

Етап 5. За необхідності, вибираємо TopN об'єктів з одержаного списку.

Проведено тестування розробленого методу. Запропонований метод на відміну від методу колаборативної фільтрації на основі моделі сусідства дозволяє створювати рекомендації для всіх користувачів системи, вирішуючи проблему холодного старту. Покриття простору користувачів в розробленому методі завжди 100%, а в існуючому – в середньому 56.1%. Покриття каталогу розроблений метод збільшує в 2.5 рази.

Також у рамках даної роботи було розроблено гібрид запропонованих методів з відомим методом колаборативної фільтрації на основі моделі сусідства.

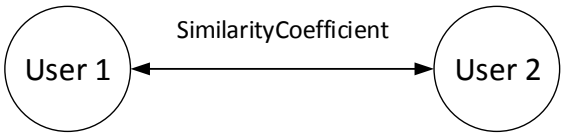

Рис. 5. Двонаправлені зв'язки типу «схожість» між користувачами

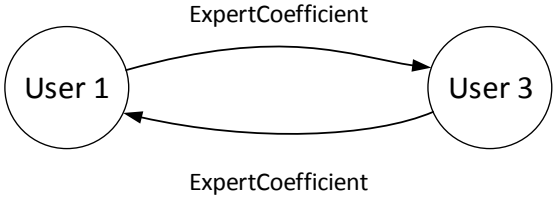

Рис. 6. Однонаправлені зв'язки типу «експерт» між користувачами

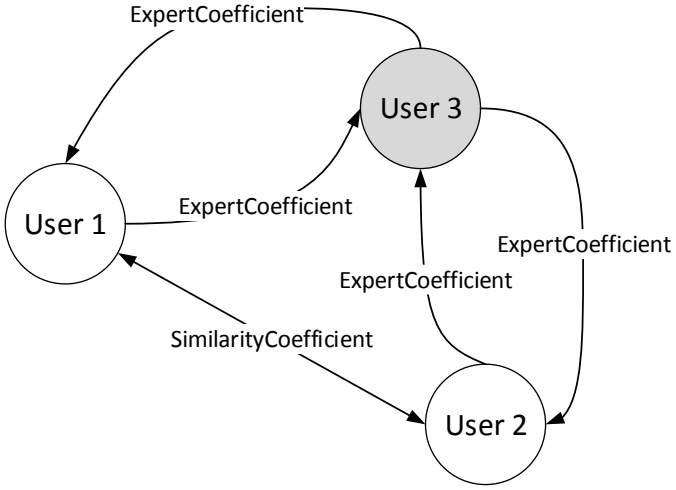

Рис. 7. Приклад побудови зв'язків типу «схожість» та «експерт» у гібридному методі

На рис. 5 наведено приклад зв'язків у базі даних між користувачами при використанні колаборативної фільтрації на основі моделі сусідства, на рис. 6 – при використанні запропонованого експертно-орієнтованого методу, а на рис. 7 – при використанні запропонованого гібриду цих двох методів. Гібридний метод формує зв'язки типу «експерт» тільки для користувачів, у яких немає коефіцієнтів подоби з іншими користувачами системи (рис. 7, User3).

Розроблено гібридний метод, що поєднав: 1) існуючий метод колаборативної фільтрації на основі моделі сусідства; 2) запропонований метод колаборативної фільтрації з використанням продукційних правил; 3) запропонований метод колаборативної фільтрації з врахуванням показників активності користувачів. Була застосована послідовна стратегія гібридизації, тобто, алгоритми на основі даних методів запускалися по черзі у порядку, наведеному вище. Проведені експерименти для тестування показників якості розробленого гібриду, результати наведені у табл. 2, де використані скорочення: МС – колаборативна фільтрація на основі моделі сусідства; ФМ – колаборативна фільтрація на основі факторизації матриць; Г+ – розроблений гібрид.

Розроблений гібридний метод на відміну від методу колаборативної фільтрації на основі моделі сусідства дозволяє забезпечити 100% покриття користувачів та 99% покриття каталогу товарів без зменшення точності формування рекомендацій, а на відміну від методу колаборативної фільтрації на основі матричної факторизації дозволяє отримати вищі значення точності і повноти на 5% і 17% відповідно та менше в 1.9 разів значення помилки прогнозування рекомендацій (RMSE).

Таблиця 2. Результати тестування показників якості роботи гібриду запропонованих методів колаборативної фільтрації та порівняння його з існуючими методами

№ експ.	**Точність (Precision)**			**Повнота (Recall)**			**Покриття користувачів (User space Coverage),%**			**Покриття каталогу товарів (Item space Coverage), %**			**RMSE**		
	МС	**ФМ**	**Г+**	**МС**	**ФМ**	**Г+**	**МС**	**ФМ**	**Г+**	**МС**	**ФМ**	**Г+**	**МС**	**ФМ**	**Г+**
1	0.8731	0.8420	0.8873	0.8058	0.6398	0.8221	77.89	100.0	100.0	96.50	100.0	99.00	0.954	1.796	0.952
2	0.8932	0.8456	0.8970	0.7243	0.6506	0.7316	77.89	100.0	100.0	97.50	100.0	99.50	0.826	1.691	0.841
3	0.9178	0.8557	0.9173	0.8265	0.6452	0.8200	91.57	100.0	100.0	97.50	100.0	98.50	0.919	1.765	0.911
…	…							…							
20	0.9419	0.8998	0.9365	0.8326	0.6696	0.8400	84.21	100.0	100.0	98.5	100.0	99.50	0.848	1.736	0.859
С.з.	**0.8877**	**0.8444**	**0.8926**	**0.8129**	**0.6413**	**0.8132**	**83.62**	**100.0**	**100.0**	**97.55**	**100.0**	**99.32**	**0.923**	**1.774**	**0.926**

Також були проведені експерименти для оцінки стійкості розробленого гібриду до внутрішніх дестабілізуючих факторів на прикладі проблеми холодного старту.

Було запропоновано консолідований показник стійкості рекомендаційної системи:

$$persistence = \sum k_i x_i \,, \tag{27}$$

$$persistence = \overline{\Delta}_u + HitRatio_u + \overline{\Delta}_i + HitRatio_i \,, \tag{28}$$

де $\overline{\Delta}_i = \left| \frac{\sum_{i=1}^{n} \frac{\Delta_{i,u}}{m_i}}{n} \right|, \overline{\Delta}_u = \left| \frac{\sum_{u=1}^{m} \frac{\Delta_{i,u}}{n_u}}{m} \right|, HitRatio_i = \frac{\sum_{i=1}^{n} \frac{H_{i,u}}{m_i}}{n}, HitRatio_u = \frac{\sum_{u=1}^{m} \frac{H_{i,u}}{n_u}}{m},$

у наведених формулах m_i – кількість користувачів, що оцінили *i*-тий об’єкт, n – кількість об’єктів у системі, n_u – кількість об’єктів оцінених *u*-тим користувачем, m – кількість користувачів у системі.

Результати тестування стійкості розробленого гібриду наведені у табл. 3. Чим менше значення консолідованого показника стійкості (суми зсувів у формуванні рекомендацій, викликаних дестабілізуючим фактором) тим вища стійкість системи.

Таблиця 3. Результати тестування стійкості гібриду розроблених методів та порівняння з існуючими методами колаборативної фільтрації

№ експ.	Стійкість. консолідований показник		
	ВМ	**ФМ**	**Г+**
1	0.134	0.1382	0.1179
2	0.0967	0.1728	0.0501
3	0.0776	0.1786	0.0404
…	**…**		
20	0.0724	0.1974	0.0298
Сер. знач.:	**0.0937**	**0.1802**	**0.0558**

Розроблений гібридний метод, на відміну від існуючих методів колаборативної фільтрації, більш стійкий до дестабілізуючого фактору холодного старту користувачів, в 1.6 разів підвищена стійкість в порівнянні з методом на основі моделі сусідства та в 3.2 разів – в порівнянні з методом на основі факторизації матриць.

Четвертий розділ присвячено розробці програмної імітаційної моделі користувачів та об'єктів рекомендаційної системи для генерації наборів даних, що можна використовувати у тестуванні алгоритмів рекомендаційних систем. Крім поведінки звичайних користувачів системи моделюється також поведінка ботів для різних відомих моделей атак, що дає змогу формувати набори даних, які можна використати для тестування стійкості рекомендаційної системи до атак.

Для програмного імітаційного моделювання користувачів та об'єктів рекомендаційної системи було використано теорію складних мереж. *Складні мережі* –стохастичні мережі з нетривіальною топологією, зокрема, з наявністю невеликої кількості вузлів з великим числом зв'язків (такі вершини називаються хабами).

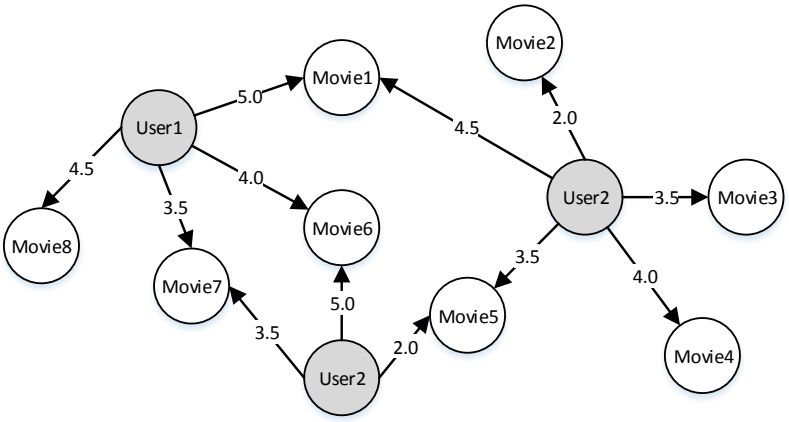

Рис. 8. Приклад складної мережі для моделювання в рамках даної роботи

Генерація зв'язків між користувачами та об'єктами рекомендаційної системи здійснювалася на основі модифікації відомого методу Барабаши-Альберт (АБА), створеного для генерації складних соціальних мереж. Цей метод дозволяє створювати безмасштабні мережі на основі 2 умов:

Ріст. Починаючи з невеликого числа n_0 вузлів, на кожній новій часовій ітерації додається один новий вузол з n зв'язками (де $n <= n_0$), які з'єднують новий вузол з n різними уже існуючими вузлами.

Бажане приєднання. Ймовірність P, з якою новий вузол утворить зв'язок з деяким уже існуючим вузлом i, тим вища, чим більше зв'язків у i-го вузла:

$$P_i = \frac{k_i}{\sum_j k_j} \tag{29}$$

де k_i – степінь i-го вузла, а в знаменнику підраховується сума всіх степенів існуючих у мережі вузлів.

У процесі моделювання використано наступні підграфи: 1) Users-Friends, Users-Followers, Posts-Published, Posts-Viewed та Posts-Liked – що створюються генератором графу соціальної мережі, 2) Users-Similarity, Posts-Similarity та Posts-Recommended – що створюються рекомендаційною системою. Серед користувачів генерувалися й боти, їх поведінка моделювалася на основі відомих базових моделей атак.

Етапи розробленого методу програмного імітаційного моделювання користувачів та об’єктів рекомендаційної системи:

Етап 1. Генерується неорієнтований підграф Users-Friends на основі АБА.

Етап 2. Генерується неорієнтований підграф Users-Friends АБА.

Етап 3. Підграфи Users-Friends та Users-Followers об’єднуються в один граф.

Етап 4. Генерується орієнтований підграф Posts-Published на основі модифікованого методу АБА. На першій ітерації випадковим чином обираються n_0 користувачів, які "створюють" m_0 постів. Ймовірність опублікування посту деяким користувачем на наступних ітераціях визначається за формулою:

$$P_i = \frac{k_{1i} + k_{2i} + k_{3i}}{\sum_j (k_{1j} + k_{2j} + k_{3j})} \tag{30}$$

де k_{1i} – кількість друзів у i-го вузла, k_{2i} – кількість підписників у i-го вузла, k_{3i} – кількість постів у i-го вузла, а в знаменнику підраховується сума всіх цих значень для усіх існуючих у мережі вузлів.

Етап 5. Підграф Posts-Published приєднується до загального графу.

Етап 6. Генерується орієнтований підграф Posts-Viewed на основі АБА. Ймовірність, що пост буде переглянутий, визначається за формулою:

$$P_i = \frac{q_{1i} + q_{2i} + q_{3i}}{\sum_j (q_{1j} + q_{2j} + q_{3j})} \tag{31}$$

де q_{1i} – кількість друзів у автора i-го поста, q_{2i} – кількість підписників у автора i-го поста, q_{3i} – кількість переглядів у i-го поста, а в знаменнику підраховується сума всіх цих значень для усіх існуючих у мережі вузлів.

Етап 7. Підграф Posts-Viewed приєднується до загального графу.

Етап 8. Генерується підграф Posts-Liked. Ймовірність того, що деякий пост отримає лайк, визначається за формулою:

$$P_i = \frac{q_{1i} + q_{2i} + q_{3i} + q_{4i}}{\sum_j (q_{1j} + q_{2j} + q_{3j} + q_{4j})} \tag{32}$$

де q_{1i} – кількість друзів у автора i-го поста, q_{2i} – кількість підписників у автора i-го поста, q_{3i} – кількість переглядів у i-го поста, q_{4i} – кількість лайків у i-го поста, а в знаменнику підраховується сума всіх цих значень для усіх існуючих у мережі вузлів.

Етап 9. Підграф Posts-Liked приєднується до загального графу.

Етап 10. Підграфи Users-Similarity, Posts-Similarity та Posts-Recommended генеруються методами рекомендаційної системи та приєднуються до загального графу.

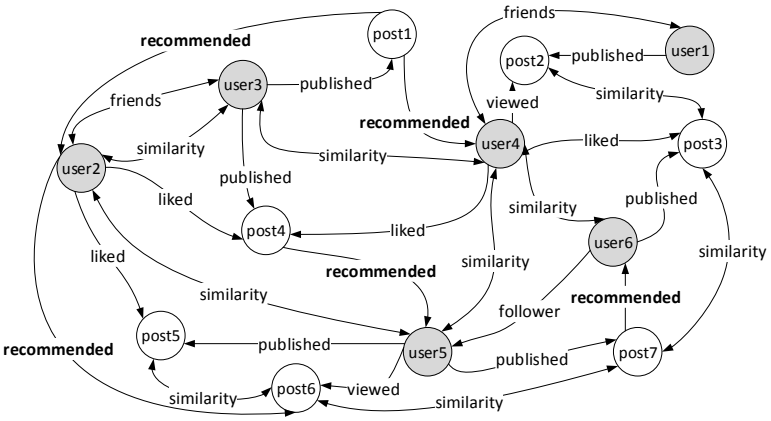

Рис. 9. Схема соціальних зв'язків у розробленій програмній імітаційній моделі

Середні значення параметрів згенерованих у запропонованій програмній імітаційній моделі соціальних графів рекомендаційної системи, які були обчислені за допомогою додатку Gephi: середня степінь вузлів – 5.7, діаметр мережі – 4.0, щільність графу – 0.22, середній коефіцієнт кластеризації – 0.61, середня довжина шляху – 1.98. Вони відповідають параметрам реальних соціальних мереж.

Рис. 10. Приклад частини соціального графу рекомендаційної системи, одержаного в результаті моделювання (скриншот з менеджера СУБД Neo4j Desktop)

Дана імітаційна програмна модель дозволяє генерувати вхідні набори даних для тестування роботи алгоритмів рекомендаційної системи.

Також було здійснено моделювання поведінки користувачів на основі генерації динамічного графу Users-Ratings-Items.

Розроблена програмна імітаційна модель також містить: модель користувача системи, модель об'єкту системи та модель інформаційних процесів у рекомендаційній системі.

Модель користувача системи має наступні параметри:

– *Id* – ідентифікаційний номер користувача, містить цифру;

– *Активний* – значення True – ставить багато оцінок, False – мало оцінок;

– *Бот* – значення True – якщо бот та False – якщо аутентичний користувач;

– *Тип* – приймає значення «Звичайний», якщо користувач не бот, інакше містить

назву застосованої до рекомендаційної системи атаки;

– *Характер* – містить тип характеру користувача стосовно стилю виставлення оцінок: «Звичайний», «Частіше ставить хороші оцінки», «Ставить тільки хороші оцінки». «Звичайний» ставить і позитивні, і негативні оцінки. Інші типи користувачів можуть не виставляти оцінку, якщо оцінили об’єкт негативно;

– *Час реєстрації* – містить час реєстрації користувача у системі;

– *Час останньої активності* – містить час останньої активності користувача;

– *Час зупинки активності* – час, коли користувач перестав користуватися системою;

– *Приховані фактори* – список випадкових змінних, які приймають значення від -1 до 1, довжиною *K*, моделює набір вподобань користувача до різних ознак об’єктів;

– *Зсув користувача* – випадкова величина в діапазоні від -1.0 до 1.0, що моделює схильність користувача занижувати чи завищувати оцінки об’єктам;

– *Час останньої зміни вподобань* – для моделювання змін вподобань користувачів у часі, містить час останнього перезапису списку прихованих факторів користувача.

Модель об’єкту системи має наступні параметри:

– *Id* – ідентифікаційний номер об’єкту, містить цифру;

– *Популярний* – значення True – якщо отримує багато оцінок, False – мало оцінок;

– *Тип для ботів* – приймає значення «Цільовий» – якщо боти повинні змінити рейтинг об’єкту в певну сторону та False – в протилежному випадку;

– *Тип атаки* – приймає значення «Немає», якщо об’єкт не цільовий, або містить тип атаки «На зменшення рейтингу», «На збільшення рейтингу»;

– *Час додавання* – містить час додавання об’єкту до бази даних системи;

– *Приховані фактори* – список випадкових змінних, які приймають значення від -1 до 1, довжиною *K*, що моделює вираженість тих чи інших характеристик у даного об’єкту, які впливають на рівень інтересу до нього користувачів;

– *Зсув об’єкту* – випадкова величина в діапазоні від -1.0 до 1.0, що моделює загальну якість об’єкту, призводить до отримання частіше низьких оцінок через низьку якість, або частіше високих оцінок через високу якість об’єкту.

Модель інформаційних процесів у системі має наступні параметри:

– *Матриця рейтингів* – містить оцінки поставлені користувачами об’єктам.

– *Матриця часу* – містить час виставлення оцінок у матриці рейтингів.

– *Набір можливих оцінок* – містить набір оцінок, які користувачі можуть виставляти об’єктам, представлений наступним списком [0.5, 1.0, 1.5, 2.0, 2.5, 3.0, 3.5, 4.0, 4.5, 5.0], що означає можливість поставити оцінку у вигляді кількості зірочок, зірочок максимум 5, можна вибирати половинку зірочки.

– *Список користувачів* – містить список користувачів системи, екземплярів класу Користувач.

– *Список об’єктів* – містить список об’єктів системи, екземплярів класу Об’єкт.

– *Початковий час роботи моделі* – містить час у форматі Unix time stamp.

– *Поточний час роботи моделі* – містить час у форматі Unix time stamp, що вказує на час останньої дії у системі.

– *Список ботів* – містить список ботів у розроблюваній моделі.

– *Список цілей* – містить список цілей атаки ботів у розроблюваній моделі.

– *Кількість кластерів* – містить задану кількість кластерів, на яку можна буде розділити елементи системи на основі даних про їх приховані фактори.

– *Шаблони кластерів* – містить список шаблонів для моделювання прихованих факторів користувачів/об’єктів. Всього у моделі було створено 19 випадкових шаблонів для генерації елементів, що можуть належати 19 різним кластерам.

Було реалізовано наступні функції для моделювання поведінки користувачів і об’єктів та інформаційних процесів рекомендаційної системи:

– *Запуск моделі* – запускає процес моделювання.

– *Збереження даних моделі у файл* – зберігає усі дані та параметри моделі у файл.

– *Генерація елементів системи* – створення заданої кількості користувачів та об’єктів системи і привласнення їм параметрів.

– *Генерація шаблонів кластерів елементів* – створює різні шаблони набору прихованих факторів для елементів, що будуть відноситися до різних кластерів.

– *Генерація прихованих факторів елементів на основі шаблонів кластерів* – на вході одержує шаблон кластера, на виході надає список прихованих факторів, що випадковим чином на деякі величини відрізняються від даних у шаблоні, щоб не виходити за межі кластеру, але мати свої унікальні значення факторів.

– *Генерація прихованих факторів елементів за межами кластерів* – генерація списку прихованих факторів елемента випадковим чином без використання шаблонів.

– *Генерація «Зерна» соціального графу* – створює початковий соціальний граф на основі заданої початкової кількості користувачів, об’єктів та щільності графу.

– *Ітеративна побудова моделі* – дозволяє моделювати зміну часу у моделі.

– *Одна ітерація моделі* – всередині даної функції викликаються всі функції, що реалізують поведінку користувачів та роботу системи в поточний момент часу.

– *Генерація поточного часу роботи моделі* – генерація часового проміжку між двома подіями у системі – випадкової величини, що лежить в заданому діапазоні.

– *Додавання користувача до системи* – моделювання процесу реєстрації користувача у рекомендаційній системі, користувач отримує час реєстрації та можливість переглядати об’єкти та ставити їм оцінки.

– *Додавання об’єкту до системи* – моделювання процесу додавання об’єкту до бази даних рекомендаційної системи, об’єкт одержує час додавання до бази даних та можливість одержувати перегляди та оцінки.

– *Визначення ймовірності перегляду об'єкту* – на основі принципу «бажаного приєднання» визначається ймовірність перегляду об’єкту користувачем.

– *Визначення ймовірності появи оцінки* – на основі принципу «бажаного приєднання» визначається ймовірність виставлення оцінки об’єкту користувачем.

– *Генерація оцінки на основі прихованих факторів* відповідного об’єкту та користувача. Оцінка для пари користувач-об’єкт визначається за формулами:

$$d_{u,m} = \frac{\sum_{i=0}^{n} \left| f_{u,i} - f_{m,i} \right|}{n}, \tag{33}$$

$$r_{u,m} = \Psi\left(5 d_{u,m} + b_u + b_m\right), \tag{34}$$

де $d_{u,m}$ – дистанція між користувачем u та об’єктом m у багатомірному просторі прихованих факторів, може приймати значення від 0 до 1; n – кількість прихованих факторів у системі; $f_{u,i}$ – i-тий прихований фактор користувача u; $f_{m,i}$ – i-тий прихований фактор об’єкту m; b_u – зсув користувача у оцінюванні об’єктів (рівень

вимогливості до контенту); b_m – зсув об'єкту у одержанні оцінок (рівень якості контенту); Ψ() – функція, що перетворює одержане дробове число у дискретне число з набору оцінок [0.5, 1.0, 1.5, 2.0, 2.5, 3.0, 3.5, 4.0, 4.5, 5.0], наприклад, якщо число лежить в діапазоні від (4.000 – k) до (4.500 – k), де k деяке невелике число (у моделі було взято k = 0.05), то воно перетворюється на оцінку 4.0.

– *Рішення поставити оцінку та її коригування.* Після того як користувач «переглянув» об'єкт, і на основі прихованих факторів, було визначено, яка оцінка для даного об'єкту відповідає його вподобанням, дана функція, визначає факт того, що користувач прийме рішення поставити переглянутому об'єкту оцінку, а також можливе незначне коригування оцінки на основі випадкових чинників.

– *Визначення ймовірності зміни вподобань* – визначає ймовірність того, що у поточний момент часу вказаний користувач змінить свої вподобання, якщо відомий час, коли він останній раз змінював вподобання (використовується опціонально).

– *Зміна вподобань користувача* – здійснює заміну прихованих факторів вказаного користувача.

Також в моделі розроблені генератори оцінок ботів для різних видів атак.

– *Генерація оцінки для випадкової атаки* – створює оцінки для пар бот-об'єкт, де бот здійснює випадкову атаку на систему. Відбувається наступним чином:

$$r_{u,m} = \begin{cases} \text{randomPattern}(), \textit{якщо об'єкт} - \text{"}\textit{звичайний}\text{"} \\ 5.0, \textit{якщо об'єкт} - \text{"}\textit{цільовий}\text{"} \end{cases}, \quad (35)$$

де randomPattern() – функція, що генерує випадкові оцінки для випадково обраних об'єктів з заданими значеннями ймовірності появи кожного значення оцінки.

– *Генерація оцінки для середньої атаки* – створює оцінки для пар бот-об'єкт, де бот здійснює середню атаку на систему. Відбувається наступним чином:

$$r_{u,m} = \begin{cases} \textit{average}\,\text{Pattern}(), \textit{якщо об'єкт} - \text{"}\textit{звичайний}\text{"} \\ 5.0, \textit{якщо об'єкт} - \text{"}\textit{цільовий}\text{"} \end{cases}, \quad (36)$$

де *average* Pattern() – функція, що генерує для випадково обраного об'єкту його середньостатистичну оцінку.

– *Генерація оцінки для популярної атаки* – створює оцінки для пар бот-об'єкт, де бот здійснює популярну атаку на систему. Відбувається наступним чином:

$$r_{u,m} = \begin{cases} \textit{popular}\,\text{Pattern}(), \textit{якщо об'єкт} - \text{"}\textit{звичайний}\text{"} \\ 5.0, \textit{якщо об'єкт} - \text{"}\textit{цільовий}\text{"} \end{cases}, \quad (37)$$

де *popular* Pattern() – функція, що генерує для випадково обраного об'єкту з множини популярних об'єктів його середньостатистичну оцінку.

Також у даному розділі була запропонована модель зміни вподобань користувачів рекомендаційної системи у часі. Для визначення як саме змінюються вподобання реальних користувачів у часі було проведено експерименти з використанням набору даних MovieLens. В проведених експериментах значення коефіцієнтів подоби між парами користувачів перераховувалися через певні проміжки часу та порівнювалися з попередніми з метою визначення періодів незмінності коефіцієнтів їх подоби. Отримані дані дозволили побудувати діаграму частоти подій появи проміжків стабільності коефіцієнтів подоби для пар користувачів $N(n)$ (рис. 11) та визначити залежність кількості користувачів, які не змінили своїх вподобань, від часу (рис. 12).

Рис. 11. Діаграма частоти інтервалів стійкості вподобань від їх довжини,
де: n – довжина інтервалу часу стабільності коефіцієнта подоби пари користувачів;
N – кількість часових інтервалів стабільності коефіцієнтів подоби довжиною n

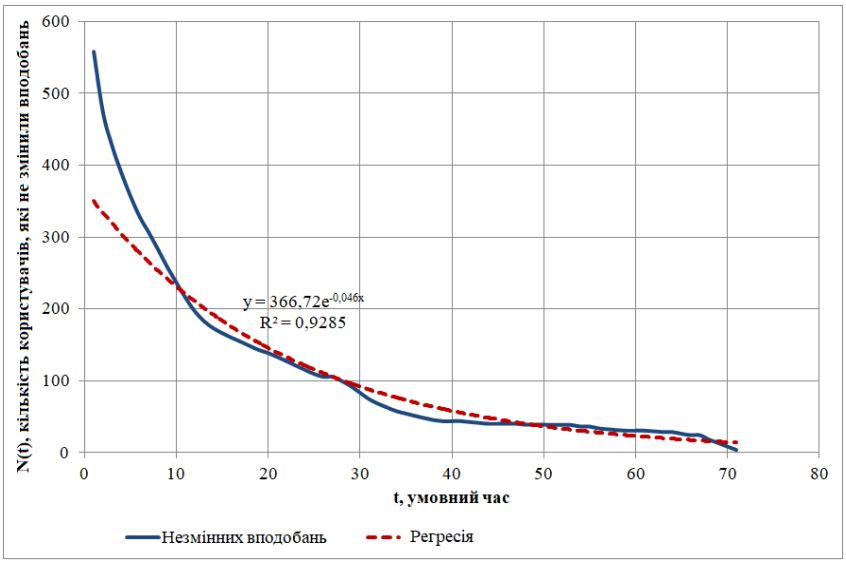

Рис. 12. Залежність кількості користувачів, які не змінили своїх вподобань, від часу,
де: t – умовний час; k – кількість пар користувачів, які не змінили свого коефіцієнту подоби за певний час t

Для даних з рис. 12 були побудовані регресії, які відповідають популярним спадаючим розподілам. Найкращі наближення дала показникова регресія $N(n) \approx 80e^{-0.17n}$ з середнім квадратичним відхиленням $S \approx 19$. В той же час, якщо прийняти наявність розподілу Парето, то матимемо наближення $N(n) \approx 79n^{-0.93}$ з середнім квадратичним відхиленням $S \approx 24$. Отримані дані дають перевагу екпоненційному розподілу, бо його використання дало змогу отримати менше середньоквадратичне відхилення результату апроксимації від експериментальних даних. За прийнятою гіпотезою про експонентний закон розподілу зміни вподобань користувачів у часі, можна до даного процесу застосувати закони радіоактивного розпаду елементів, з причини співпадіння прийнятих базових законів розподілу.

Для моделювання процесу зміни вподобань користувачів у часі було визначено наступні величини, як аналог закономірностей радіоактивного розпаду елементів:

Середній час життя вподобання $\tau = 1/\lambda$.

Період напіврозпаду – час, за який у половини пар користувачів зміняться коефіцієнти подоби: $T_{1/2} = \tau \cdot \ln 2$

Ймовірність зміни вподобань за час t: $p(t) = 1\text{-}e^{-\lambda t}$.

Ймовірність залишити вподобання незмінними за час t**:** $q(t) = e^{-\lambda t}$.

Запропоновані у даному розділі метод та спосіб дозволяють генерувати набори даних для тестування алгоритмів роботи рекомендаційних систем. Це особливо актуально для тестування стійкості рекомендаційних систем до інформаційних атак бот-мереж, адже немає відкритих наборів даних, у яких відображена діяльність ботів.

П’ятий розділ присвячено розробці математичної моделі підсистеми інформаційної безпеки рекомендаційної системи та методу виявлення інформаційних атак на рекомендаційну систему.

Існуючі методи виявлення атак на рекомендаційні системи тотожні знаходженню профілів ботів і потребують постійних періодичних перевірок профілів користувачів. Було запропоновано розділити задачу захисту системи від інформаційних атак на дві частини: 1) виявлення атаки, 2) ідентифікація та нейтралізація профілів ботів.

Виявлення атаки може бути менш ресурсозатратною задачею, ніж пошук ботів, і полягати у відслідковуванні динаміки рейтингів об’єктів системи, усіх або тільки критично важливих з точки зору інформаційної безпеки. Якщо рейтинги деяких об’єктів починають стрімко змінюватися під впливом великої кількості нових оцінок, статистичні дані появи яких є аномальними для системи, то пропонується перевіряти профілі користувачів, причетних до виставлення таких оцінок. Цей підхід скоротить кількість перевірок профілів користувачів. По-перше, тому що перевіряти їх буде потрібно тільки при виявленні підозри на атаку. А, по-друге, тому що треба буде перевіряти профілі не всіх користувачів, а тільки тих, що здійснюють підозрілі дії.

Була розроблена математична модель підсистеми інформаційної безпеки рекомендаційної системи, що має наступні можливі стани:

H_1 – Нормальна робота: атак немає, здійснюється моніторинг стану системи.

H_2 – Система атакована: атака не виявлена, збитки від атаки, моніторинг системи.

H_3 – Система відбиває атаку: атака виявлена, пошук ботів, нейтралізація їх дій.

Можливі переходи між станами системи: 1) здійснення атаки (перехід $H_1 \rightarrow H_2$, інтенсивність потоку λ_1); 2) втрата актуальності дій ботів ($H_2 \rightarrow H_1$, λ_2); 3) виявлення атаки ($H_2 \rightarrow H_3$, λ_3), λ_3 – частота перевірок системи на наявність атаки; 4) виявлення та нейтралізація ботів ($H_3 \rightarrow H_1$, λ_4).

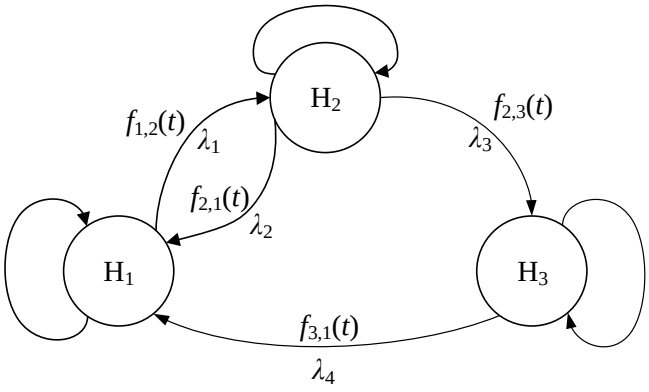

Рис. 13. Граф динаміки станів підсистеми інформаційної безпеки рекомендаційної системи в умовах інформаційної атаки

Система інтегральних рівнянь ймовірностей системи опинитися у різних станах:

$$\begin{cases} G_{1,1}(t)=\left(1-\int f_{1,2}(\tau)d\tau-\int f_{1,3}(\tau)d\tau\right)+\int f_{1,2}(\tau)\cdot G_{2,1}(t-\tau)d\tau+ \\ \qquad +\int f_{1,3}(\tau)\cdot G_{3,1}(t-\tau)d\tau \\ G_{2,1}(t)=\int f_{2,1}(\tau)\cdot G_{1,1}(t-\tau)d\tau+\int f_{2,3}(\tau)\cdot G_{3,1}(t-\tau)d\tau \\ G_{3,1}(t)=\int f_{3,1}(\tau)\cdot G_{1,1}(t-\tau)d\tau+\int f_{3,2}(\tau)\cdot G_{2,1}(t-\tau)d\tau \\ G_{1,2}(t)=\int f_{1,2}(\tau)\cdot G_{2,2}(t-\tau)d\tau+\int f_{1,3}(\tau)\cdot G_{3,2}(t-\tau)d\tau \\ G_{2,2}(t)=\left(1-\int f_{2,1}(\tau)d\tau-\int f_{2,3}(\tau)d\tau\right)+\int f_{2,1}(\tau)\cdot G_{1,2}(t-\tau)d\tau+. \\ \qquad +\int f_{2,3}(\tau)\cdot G_{3,2}(t-\tau)d\tau \\ G_{3,2}(t)=\int f_{3,1}(\tau)\cdot G_{1,2}(t-\tau)d\tau+\int f_{3,2}(\tau)\cdot G_{2,2}(t-\tau)d\tau \\ G_{1,3}(t)=\int f_{1,2}(\tau)\cdot G_{2,3}(t-\tau)d\tau+\int f_{1,3}(\tau)\cdot G_{3,3}(t-\tau)d\tau \\ G_{2,3}(t)=\int f_{2,1}(\tau)\cdot G_{1,3}(t-\tau)d\tau+\int f_{2,3}(\tau)\cdot G_{3,3}(t-\tau)d\tau \\ G_{3,3}(t)=\left(1-\int f_{3,1}(\tau)d\tau-\int f_{3,2}(\tau)d\tau\right)+\int f_{3,1}(\tau)\cdot G_{1,3}(t-\tau)d\tau+ \\ \qquad +\int f_{3,2}(\tau)\cdot G_{2,3}(t-\tau)d\tau \end{cases} \quad (38)$$

Так як аналітичне рішення даної системи рівнянь є досить складним та громіздким, то краще використати чисельні методи. Наявні конкретні значення дозволяють знайти корені або точно, або наближено, тому, для прикладу, використаємо наступні параметри: λ_1=0.01; λ_2=0.01; λ_3=0.1; λ_4=0.1; p_{21}=0.2; p_{23}=0.8. Тут λ є інтенсивностями подій, дані значення можуть бути визначені власниками рекомендаційної системи на основі аналізу статистичних даних, доступних адміністраторам системи.

Шукані ймовірності після підстановки вказаних значень у загальному випадку для марківських процесів можна визначити за наступними формулами:

$$G_{1,1}=\frac{\lambda_2\lambda_3\lambda_4}{Z},\ G_{1,2}=\frac{\lambda_1\left(p_{2,3}(\lambda_2-\lambda_3)+\lambda_3\right)\lambda_4}{Z},\ G_{1,3}=\frac{p_{2,3}\lambda_1\lambda_2\lambda_3}{Z}, \quad (39)$$

де $Z=(\lambda_1+\lambda_2)\lambda_3\lambda_4+p_{2,3}\lambda_1(\lambda_2(\lambda_3+\lambda_4)-\lambda_3\lambda_4)$.

На основі запропонованої моделі було розроблено спосіб визначення загальних витрат, що зазнає рекомендаційна система внаслідок моніторингу власної інформаційної безпеки та внаслідок інформаційних атак.

Повні витрати на інформаційний захист рекомендаційної системи:

$$L=\left(G_{1,2}+G_{1,3}\right)\cdot K_1+\left(G_{1,1}+G_{1,2}\right)\cdot K_2\lambda_3+G_{1,3}\ K_3, \quad (40)$$

де K_1 – фінансові витрати власника системи внаслідок вдалої атаки мережі ботів; K_2 – фінансові витрати власника системи на використання додаткових обчислювальних ресурсів для перевірок на наявність інформаційних атак; K_3 – фінансові витрати власника системи на ідентифікацію та нейтралізацію окремих профілів ботів.

Також було розроблено спосіб визначення оптимальної частоти перевірки рекомендаційної системи на наявність інформаційної атаки та профілів ботів.

В підсистемі інформаційної безпеки рекомендаційної системи можна керувати частотою перевірок на наявність атаки v, що відповідає за значення параметру λ_3. Для того, щоб визначити оптимальну частоту перевірки системи на наявність атаки v_{opt}, треба знайти таке λ_3, при якому загальні збитки системи L будуть мінімальними:

$$v_{opt}=\arg\min_{\lambda_3} L(\lambda_3)=\arg\min_{\lambda_3}\left[\left(G_{1,2}+G_{1,3}\right)\cdot K_1+\left(G_{1,1}+G_{1,2}\right)\cdot K_2\lambda_3+G_{1,3}\ K_3\right]. \quad (41)$$

Це рівняння є нелінійним, з причини впливу значення λ_3 на коефіцієнти G. Тому

його розв'язок в загальному випадку можливий лише за допомогою чисельних методів або методів оптимізації. Для прикладу, візьмемо наступні значення усіх видів витрат рекомендаційної системи: K_1=5 *гр.од./хв*, K_2=1 *гр.од./хв*, K_3=2 *гр.од./хв*. Такі значення витрат взяті з наступних міркувань, збитки від діяльності ботів K_1, як правило більші, ніж витрати на моніторинг стану системи K_2 та на ідентифікацію і нейтралізацію профілів ботів K_3. А також витрати на моніторинг системи з метою виявлення наявності атак K_2 менші, ніж витрати на ідентифікацію та нейтралізацію окремих профілів ботів K_3. Значення решти констант залишається тим самим, що й раніше. Визначимо ν_{opt} за допомогою проведення табуляції функції витрат (41) для λ_3=0; 0.05; 0.1; 0.15; 0.2; 0.25; 0.3, де значення ймовірностей $G_{1,1}$, $G_{1,2}$ та $G_{1,3}$ отримані з (39), результати наведено у табл. 4. Вираз для функції витрат при вказаних значеннях параметрів має вигляд:

$$L(\lambda_3) = \frac{0.000195 + 0.0389\lambda_3 + 1.231\lambda_3^2 + 0.9375\lambda_3^3}{0.0000391 + 0.0125\lambda_3 + \lambda_3^2}. \qquad (42)$$

Графічне відображення побудованих точок для значень повних збитків рекомендаційної системи L при різних значеннях частоти перевірок на наявність інформаційних атак ν, які поєднані плавною кривою, показані на рис. 14.

Таблиця 4. Приклад розрахунків для визначення оптимальної частоти перевірки рекомендаційної системи на наявність інформаційних атак ботів ν_{opt}

$\nu=\lambda_3$	0.00	0.05	0.10	0.15	0.20	0.25	0.3
$G_{1,1}$	1/2	25/36	25/34	75/100	25/33	125/164	75/98
$G_{1,2}$	1/2	9/36	7/34	19/100	6/33	29/164	17/98
$G_{1,3}$	0	2/36	2/34	6/100	2/33	10/164	6/98
L	2.5	1.67	1.54	1.51	1.52	1.55	1.58

З рис. 14 та табл. 4 можна зробити висновок, що мінімальними загальні витрати системи будуть L_{min} = 1.51 *гр.од./хв* при частоті перевірки на наявність інформаційних атак ν_{opt} = 0.16 *1/хв*, це відповідає періодичності перевірок $T = 1/\lambda_3$ = 6.25 *хв*.

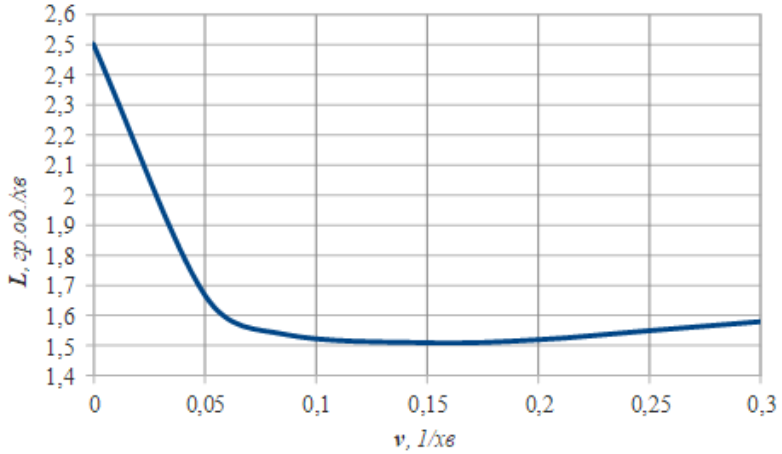

Рис. 14. Залежність розміру повних витрат рекомендаційної системи L від частоти її перевірки на наявність інформаційних атак ν

Якщо пошук наявного втручання у рекомендаційну систему проводити з більшою інтенсивністю, витрати зростуть за рахунок додаткових обчислень; якщо виявляти активність ботів з меншою інтенсивністю – матимемо ситуацію зі збільшенням

витрат за рахунок неправильної роботи системи під впливом ботів. Якщо б інтенсивність перевірок для розглянутого прикладу була максимальною $\nu = \lambda_3 = 1$, тобто перевірки відбувалися би безперервно, то загальні збитки системи сягнули б $L = 2.18$ *гр.од./хв*. Тож, при застосуванні оптимальної частоти перевірок рекомендаційної системи на наявність інформаційних атак, загальні витрати системи у розглянутому прикладі зменшилися на (2.18–1.51)/2.18 = 30.7%.

Таким чином, застосування способу визначення оптимальної частоти перевірки рекомендаційної системи на наявність інформаційної атаки дозволить власникам веб-ресурсів мінімізувати свої фінансові витрати на забезпечення інформаційної безпеки рекомендаційних систем.

У даному розділі також був розроблений метод виявлення інформаційної атаки на рекомендаційну систему на основі аналізу трендів рейтингів об'єктів.

Була запропонована наступна множина показників наявності інформаційної атаки на об'єкт рекомендаційної системи:

$$Q_{a,i} = \{tr, pr, d_r, d_t, n_r, n_{tr}, n_{rec}\} \quad (43)$$

де tr – тренд динаміки рейтингів об'єкту, приймає значення $\{-1, 0, 1\}$; pr – прогнозування збереження тренду для об'єкту i, наприклад, на основі показника Херста; d_r – дисперсія оцінок виставлених об'єкту; d_t – дисперсія часу виставлення цільових оцінок об'єкту; n_r – кількість оцінок у об'єкта на деякому проміжку часу; n_{tr} – кількість цільових оцінок у об'єкта на деякому проміжку часу; n_{rec} – кількість потраплянь об'єкта у списки рекомендацій на деякому проміжку часу.

Розроблений метод виявлення інформаційної атаки на рекомендаційну систему складається з наступних етапів:

Етап 1. Формуємо множину об'єктів $I = \{i_1, i_2, \dots i_m\}$ для перевірки на наявність атаки на них.

Етап 2. Визначаємо для усіх $i_j \in I$ наявність та напрямок тренду tr на проміжку часу τ.

Етап 3. Визначаємо на основі R/S-аналізу для кожного $i_j \in I$ індекс Херста H на проміжку часу τ.

Етап 4. Визначаємо для усіх $i_j \in I$ на проміжку часу τ дисперсію оцінок d_r, дисперсію часових проміжків між виставленням цільових оцінок d_t, та їх середньостатистичні значення у системі $d_{\tau,cep}$ та $d_{t,cep}$.

Етап 5. Визначаємо для усіх $i_j \in I$ на проміжку часу τ кількість виставлених йому цільових n_{tg}, усіх оцінок n_r, середньостатистичну кількість цільових $n_{tg,cep}$ та усіх оцінок $n_{r,cep}$ для об'єктів системи.

Етап 6. Визначаємо для усіх $i_j \in I$ на проміжку часу τ кількість потраплянь у списки рекомендацій n_{rec} та середньостатистичну кількість потраплянь у списки рекомендацій $n_{rec,cep}$ для всіх об'єктів.

Етап 7. Визначаємо наявність та тип атаки за наступними правилами:

Правило 1. Якщо у об'єкта наявні будь-які 5 ознак з: $tr_\tau = 1$, $H > 0.73$, $d_\tau \le d_{\tau,cep}$, $d_t \le d_{t,cep}$, $n_r > n_{r,cep}$, $n_{tg} > n_{tg,cep}$, $n_{rec} > n_{rec,cep}$, то існує висока ймовірність атаки на підвищення рейтингу для нього.

Правило 2. Якщо у об'єкта наявні будь-які 5 ознак з: $tr_\tau = -1$, $H > 0.73$, $d_\tau \le d_{\tau,cep}$, $d_t \le d_{t,cep}$, $n_r > n_{r,cep}$, $n_{tg} > n_{tg,cep}$, $n_{rec} < n_{rec,cep}$, то існує висока ймовірність атаки на зниження рейтингу для нього

Етап 8. Формуємо множину *G* ймовірних цілей інформаційної атаки.

Для тестування розробленого методу було реалізовано програмне забезпечення на мові програмування Python з використанням СУБД Neo4j. Вхідні дані для експериментів генерувалися у розробленій програмній імітаційній моделі рекомендаційної системи. Атаки моделювалися за допомогою відомих моделей атак. Було проведено серію експериментів, результати яких наведені у таблиці 5.

Таблиця 5. Результати тестування розробленого методу виявлення інформаційної атаки на рекомендаційну систему та об'єктів атаки

№ експ.	Модель інформаційної атаки	Кількість об'єктів у системі	Кількість об'єктів атаки ботів	Вірно розпізнані об'єкти атаки, %	Помилково розпізнані як об'єкти атаки, %	RMSE
1	Випадкова атака	200	20	100.00	5.55	0.223
2		200	10	80.00	23.68	0.484
3		200	5	40.00	22.05	0.479
4		200	1	100.00	16.58	0.406
5	Середня атака	200	20	90.00	0.00	0.100
6		200	10	50.00	13.68	0.393
7		200	5	60.00	13.84	0.380
8		200	1	100.00	12.06	0.346
9	Популярна атака	200	20	75.00	0.00	0.158
10		200	10	80.00	12.63	0.360
11		200	5	40.00	17.94	0.435
12		200	1	100.00	15.57	0.393
Середні значення:				**76.25**	**12.79**	**0.346**

Як показали результати експериментів, розроблений метод в середньому дозволяє виявити 76% об'єктів інформаційних атак у рекомендаційній системі. Об'єкти, які помилково були визначені як цілі атаки, в середньому складали 13%. Розроблений метод формує множину ймовірних цілей атаки ботів, яку можна використати для подальшого пошуку їх профілів. Це дозволить при пошуку бот-мереж перевіряти не всі профілі системи, а тільки ті, які взаємодіяли з ймовірними об'єктами атаки.

Також було розроблено спосіб ідентифікації окремих профілів ботів у рекомендаційній системі на основі багатошарової нейронної мережі прямого поширення. Як вхідні дані для нейронної мережі було обрано кількості різних оцінок у профілі користувача. Використану нейронну мережу зображено на рис. 15.

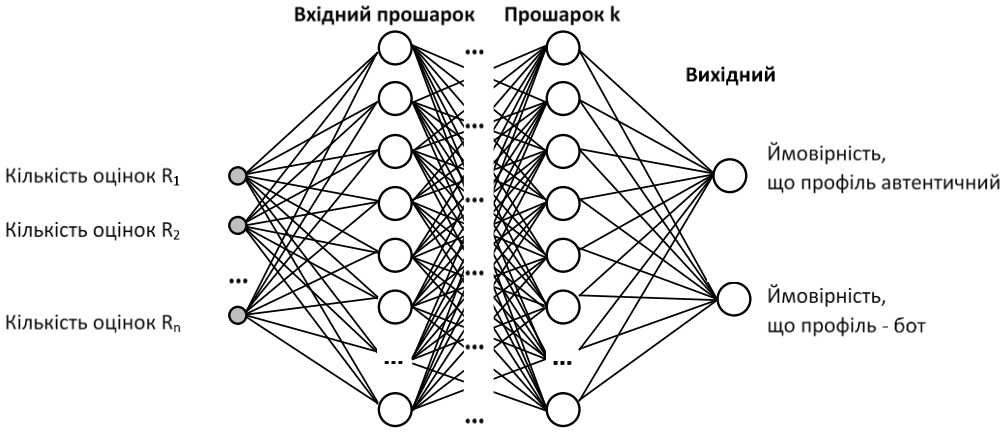

Рис. 15. Запропонована загальна архітектура нейронної мережі для ідентифікації профілів ботів у рекомендаційній системі

Для реалізації нейронної мережі використана бібліотека TensorFlow та мова Python. Експериментальним шляхом було виявлено, що баланс між точністю та складністю нейромережі вдається досягнути при параметрах, що наведені у табл. 6.

Таблиця 6. Параметри розробленої конкретної нейронної мережі

Прошарок	Тип	Кіл-ть нейронів	Кіл-ть входів на нейроні	Функція активації
1	вхідний	100	10	sigmoid
2	прихований	100	100	sigmoid
3	прихований	100	100	sigmoid
4	вихідний	2	100	softmax

Для проведення експериментів було використано набір даних, згенерований у розробленій програмній імітаційній моделі рекомендаційної системи.

Результати експериментів наведено у таблиці 7. Позначення використані у таблиці: RA – випадкова атака, AA – середня атака, PA – популярна атака.

Таблиця 7. Результати тестування розробленого способу ідентифікації профілів ботів на основі нейронних мереж

№ експ.	Кіл-ть ботів, %	Кіл-ть цілей у ботів, шт.	Помилка I роду, %			Помилка II роду, %			Точність (Precision)			Повнота (Recall)			F-міра, %		
			RA	AA	PA	RA	AA	PA	RA	AA	PA	RA	AA	PA	RA	AA	PA
1	5	1	0.001	0.002	0.002	0.023	0.049	0.047	0.95	0.12	0.25	0.52	0.006	0.006	0.67	0.013	0.013
2	10	1	0.0006	0.001	0.0006	0.036	0.099	0.099	0.98	0.25	0.33	0.63	0.003	0.003	0.77	0.006	0.006
3	20	1	0.002	0.001	0.002	0.080	0.199	0.197	0.98	0.28	0.14	0.59	0.003	0.001	0.74	0.006	0.003
4	30	1	0.0006	0.002	0.002	0.116	0.297	0.296	0.99	0.25	0.30	0.61	0.002	0.003	0.75	0.004	0.006
Середні значення:			**0.001**	**0.001**	**0.001**	**0.063**	**0.161**	**0.159**	**0.97**	**0.22**	**0.25**	**0.58**	**0.003**	**0.003**	**0.73**	**0.007**	**0.007**
5	5	10	0.002	0.001	0.001	0.001	0.024	0.009	0.96	0.93	0.97	0.98	0.50	0.81	0.97	0.65	0.88
6	10	10	0.001	0.001	0.002	0.002	0.045	0.014	0.98	0.98	0.96	0.97	0.55	0.85	0.98	0.70	0.90
7	20	10	0.001	0.001	0.001	0.005	0.047	0.013	0.99	0.99	0.99	0.97	0.76	0.93	0.98	0.86	0.96
8	30	10	0.001	0.001	0.002	0.005	0.024	0.006	0.99	0.99	0.99	0.98	0.92	0.97	0.98	0.95	0.98
Середні значення:			**0.001**	**0.001**	**0.001**	**0.003**	**0.035**	**0.010**	**0.98**	**0.97**	**0.97**	**0.97**	**0.68**	**0.89**	**0.97**	**0.79**	**0.93**

За допомогою запропонованого способу найлегше виявити ботів, що здійснюють випадкову атаку, їх можна виявити навіть якщо ціль у ботів одна з точністю 97%. Значно тяжче виявити середню та популярну атаку, їх вдавалося виявити з достатньою точністю, якщо у бота було декілька цілей. Для підвищення точності роботи нейромережі, можна враховувати й інші параметри профілів користувачів, зокрема, час виставлення кожної оцінки, характеристики об’єктів атаки тощо.

Шостий розділ присвячено розробці методу виявлення та нейтралізації мережі ботів у рекомендаційній системі на основі графової кластеризації та аналізу дій користувачів. Проведено експерименти для визначення показників точності його роботи та стійкості методів рекомендаційних систем з його застосуванням. Здійснене обґрунтування достовірності одержаних у роботі результатів наукових досліджень.

Якщо у системі виявлені об’єкти з аномальною зміною рейтингів, що могло виникнути внаслідок атаки, пропонується перевірити профілі користувачів, які вплинули своїми діями на цю зміну та з’ясувати, чи не належать вони до бот-мережі.

Запропонований метод виявлення мережі ботів на основі графової кластеризації та аналізу дій користувачів складається з наступних етапів:

Етап 1. Формуємо множину підозрілих профілів користувачів S, в яку поміщаємо профілі, що ставили цільові оцінки r_t об’єктам з множини G.

Етап 2. Привласнюємо кожному користувачу з множини G мітку *:suspicious* та коефіцієнт недовіри, розрахований за наступною формулою:

$$k_{d,i} = \sum_{j \in G} \frac{E_{r_{t,i,j}}}{n_g} \tag{44}$$

де $E_{rt,i,j}$ – наявність цільової оцінки r_t від користувача u_i об'єкту $g_j \in G$, приймає значення $\{0, 1\}$; n_g – кількість об'єктів у множині G.

Етап 3. Для кожної пари користувачів i_1 та i_2 з множини S, де $k_{d,i1} \geq q$ та $k_{d,i2} \geq q$, створюємо ребро між ними з міткою *:BotNet.*

Етап 4. Виконуємо графову кластеризацію для підграфу, що містить вершини з мітками *:User* і *:suspicious* та ребра з міткою *:BotNet.* Боти з високою ймовірністю потраплять до одного великого кластеру (якщо бот-мережа одна) або до декількох великих кластерів (якщо бот-мереж декілька), аутентичні користувачі з високою ймовірністю потраплять у різні кластери, кожний з таких кластерів буде містити одного користувача, або невелику кількість користувачів.

Етап 5. Визначити найбільші кластери, що складаються з ($N_{cr} – e$) користувачів, де N_{cr} – мінімальна кількість користувачів, що може вплинути на результати роботи рекомендаційної системи (залежить від параметрів конкретної системи), e – приблизне значення похибки при розділенні профілів користувачів на кластери. Такий кластер (або кластери) вважати можливою бот-мережею (бот-мережами). У користувачів, що не потрапляють до даних кластерів прибрати ребра з міткою *:BotNet*. Користувачів, що потрапили до підграфу *BotNet* треба додатково перевірити, проаналізувавши статистичні характеристики їх профілів, наприклад, за допомогою запропонованого у попередньому розділі способу з використанням нейронних мереж.

Етап 6. Скорегувати множину G після аналізу оцінок користувачів з підграфу *BotNet*. Слід перевірити, яким об'єктам користувачі з бот-мережі скоординовано виставляли цільові оцінки. Видалити з G об'єкти, які не одержували взагалі, або одержали незначний процент цільових оцінок від користувачів, ідентифікованих як боти. Додати до множини G об'єкти, які одержали цільові оцінки від усіх ботів (або великого проценту ботів).

Була розроблена підсистема інформаційної безпеки рекомендаційної системи, що складається з методу виявлення інформаційної атаки на основі аналізу трендів рейтингів об'єктів та методу виявлення бот-мереж на основі графової кластеризації та аналізу дій користувачів. Проведено серію експериментів для визначення точності роботи розробленої підсистеми інформаційної безпеки. Результати наведені у табл. 8.

Як показала серія експериментів з табл. 8, точність розпізнавання ботів розробленим методом в середньому становить 0.72 для випадкової атаки, 0.81 для середньої атаки, а також 0.71 для популярної атаки.

Також було більш детально досліджено точність розпізнавання ботів розробленим методом для популярної моделі атаки (табл. 9). Як показали проведені експерименти, точність розпізнавання ботів розробленим методом для популярної атаки в середньому становить 0.71, повнота 0.82, а RMSE – 0.22. Найгірші результати одержувалися, коли ціль для атаки ботів була одна, тоді точність розробленого методу падала до 0.57 у середньому. Найвища точність спостерігалася, коли цілей атак було 25-30 шт., в такому разі вона сягала значення 0.78.

Таблиця 8. Результати тестування розробленої підсистеми інформаційної безпеки для різних моделей атак та різної кількості ботів і цілей атаки

№ експ.	Частка ботів серед усіх профілів, %	Кіль-ть цілей у кожного бота, шт.	Тип атаки	Кіль-ть вірно розпізнаних цілей	Кіль-ть невірно розпізнаних як цілі	Точність розпізнавання ботів	Повнота розпізнавання ботів	Частка помилок першого роду	Частка помилок другого роду	RMSE для розпізнавання ботів
1	5	1	RA	1.000000	0.241206	0.666666	0.800000	0.021052	0.200000	0.173205
2	5	5	RA	0.400000	0.220513	0.571428	0.800000	0.031578	0.200000	0.200000
…	…									
12	30	10	RA	0.800000	0.236842	0.884615	0.766666	0.042857	0.233333	0.316227
Середні значення:				**0.741666**	**0.246085**	**0.723953**	**0.773611**	**0.039476**	**0.226388**	**0.245681**
13	5	1	AA	1.000000	0.180905	0.625000	1.000000	0.000000	0.032608	0.173205
14	5	5	AA	1.000000	0.210257	0.555555	1.000000	0.000000	0.043956	0.200000
…	…									
24	30	10	AA	0.600000	0.115789	0.925925	0.833333	0.028571	0.166666	0.264575
Середні значення:				**0.808333**	**0.200986**	**0.813037**	**0.945833**	**0.023611**	**0.067028**	**0.192739**
25	5	1	PA	0.758793	0.241206	0.714285	1.000000	0.021052	0.021052	0.141421
26	5	5	PA	0.400000	0.179488	0.625000	1.000000	0.031578	0.031578	0.173205
…	…									
36	30	10	PA	1.000000	0.173684	0.892857	0.833333	0.042857	0.166666	0.282842
Середні значення:				**0.788232**	**0.225498**	**0.715251**	**0.811111**	**0.037990**	**0.188889**	**0.246043**

Таблиця 9. Результати тестування розробленої підсистеми інформаційної безпеки для популярної моделі атаки та різної кількості цілей атаки

Кількість цілей у кожного бота	Точність (Precision) розпізнавання ботів	Повнота (Recall) розпізнавання ботів	RMSE
1	0.571391191	0.843750000	0.240591404
5	0.750070242	0.925000000	0.208735147
10	0.751688997	0.937500000	0.208005683
15	0.757313520	0.950000000	0.194432974
20	0.759444202	0.931250000	0.191765580
25	0.780512370	0.925000000	0.189773836
30	0.781431763	0.875000000	0.192072089
35	0.684367195	0.737500000	0.242168980
40	0.676923250	0.581250000	0.267032399
45	0.641781656	0.568750000	0.274543689
Сер. знач.:	**0.715492439**	**0.827500000**	**0.220912178**

Було проведено серію експериментів для визначення стійкості розробленого гібриду колаборативної фільтрації з запропонованою підсистемою безпеки в умовах дії зовнішніх дестабілізуючих факторів у вигляді інформаційних атак ін’єкцією профілів.

Розроблений гібрид містить у собі: 1) існуючий метод колаборативної фільтрації на основі моделі сусідства; 2) запропонований метод колаборативної фільтрації з використанням продукційних правил для визначення відсутніх коефіцієнтів подоби між користувачами; 3) запропонований метод колаборативної фільтрації з врахуванням показників активності користувачів.

Розроблена підсистема безпеки рекомендаційної системи складається з наступних елементів: 1) метод виявлення інформаційної атаки на рекомендаційну систему на основі аналізу трендів рейтингів об’єктів; 2) метод виявлення бот-мереж у

рекомендаційній системі на основі графової кластеризації та аналізу дій користувачів; 3) спосіб ідентифікації профілів ботів на основі нейронних мереж.

Результати проведеної серії експериментів наведені у таблицях 10-12. У таблицях були використані наступні скорочення: МС – колаборативна фільтрація на основі моделі сусідства; ФМ – колаборативна фільтрація на основі факторизації матриць; Г+ – розроблений гібридний метод колаборативної фільтрації; ІМЗ – існуючий метод захисту (виявлення ботів і нейтралізації у рекомендаційній системі); РМЗ – розроблений метод захисту (виявлення ботів і нейтралізації у рекомендаційній системі).

Показник стійкості визначався за формулою (28). Чим менше значення суми зсувів у роботі системи (консолідованого показника стійкості) тим вища стійкість системи.

Таблиця 10. Консолідовані показники стійкості для існуючого та розробленого методів виявлення ботів при випадковій атаці

№ експ.	**Стійкість. Консолідований показник зсувів прогнозувань вподобань**					
	МС		**ФМ**		**Г+**	
	ІМЗ	**РМЗ**	**ІМЗ**	**РМЗ**	**ІМЗ**	**РМЗ**
1	0.08551	0.00000	0.05895	0.05720	0.21870	0.01411
2	0.06115	0.03092	0.06426	0.05703	0.10668	0.06413
3	0.02793	0.01161	0.05930	0.05930	0.08601	0.01693
…	**…**					
10	0.19909	0.17904	0.07470	0.12697	0.33420	0.29953
Сер. знач.:	**0.100669**	**0.037728**	**0.069779**	**0.067715**	**0.152068**	**0.060975**

Таблиця 11. Консолідовані показники стійкості для існуючого та розробленого методів виявлення ботів при середній атаці

№ експ.	**Стійкість. Консолідований показник зсувів прогнозувань вподобань**					
	МС		**ФМ**		**Г+**	
	ІМЗ	**РМЗ**	**ІМЗ**	**РМЗ**	**ІМЗ**	**РМЗ**
1	0.08647	0.00000	0.05794	0.05699	0.21520	0.01362
2	0.06510	0.02700	0.06414	0.05702	0.11236	0.05954
3	0.03728	0.01206	0.05839	0.05820	0.08889	0.01216
…	**…**					
10	0.20517	0.18101	0.07489	0.06312	0.34032	0.29071
Сер. знач.:	**0.10267**	**0.03632**	**0.06930**	**0.06403**	**0.15287**	**0.05800**

Таблиця 12. Консолідовані показники стійкості для існуючого та розробленого методів виявлення ботів при популярній атаці

№ експ.	**Стійкість. Консолідований показник зсувів прогнозувань вподобань**					
	МС		**ФМ**		**Г+**	
	ІМЗ	**РМЗ**	**ІМЗ**	**РМЗ**	**ІМЗ**	**РМЗ**
1	0.08976	0.00485	0.05830	0.05730	0.06378	0.01886
2	0.06133	0.02844	0.06510	0.05795	0.05773	0.06171
3	0.02956	0.01179	0.05907	0.05902	0.06424	0.01381
…	**…**					
10	0.19852	0.18482	0.07480	0.06310	0.05996	0.29571
Сер. знач.:	**0.09977**	**0.03919**	**0.06971**	**0.06143**	**0.06076**	**0.06194**

Розроблена підсистема виявлення інформаційної атаки та профілів ботів (РМЗ) дозволяє забезпечити вищу стійкість рекомендаційної системи до зовнішніх дестабілізуючих факторів на відміну від існуючих методів (ІМЗ). Вона в середньому

показує в 2.5 рази кращі результати значення стійкості для випадкової та середньої атаки та в 1.7 рази кращі результати для популярної атаки, якщо застосовувалася до методу колаборативної фільтрації на основі сусідства та до розробленого гібридного методу. Для методу на основі матричної факторизації вона показує практично такі ж результати як у існуючого методу на основі кластеризації статистичних даних з профілів користувачів.

У **висновках** сформульовані основні результати дисертаційного дослідження.

У **додатках** наводяться акти про практичне впровадження результатів проведеного дисертаційного дослідження та список публікацій за темою дисертації.

ВИСНОВКИ

В дисертаційній роботі вирішена науково-практична проблема підвищення точності пропозицій рекомендаційних систем в умовах дестабілізуючих факторів у комп'ютерних мережах на основі розробки моделей та методів синтезу підсистеми забезпечення стійкості.

Проведено дослідження та порівняльний аналіз моделей та методів рекомендаційних систем соціальних мереж та контент-орієнтованих веб-сайтів, який показав, що переважна більшість існуючих моделей і методів вразливі до дії внутрішніх та зовнішніх дестабілізуючих факторів у комп'ютерних мережах. Показано, що забезпечення стійкості рекомендаційних систем до дії дестабілізуючих факторів є важливою умовою для підвищення точності їх роботи.

Основні наукові та практичні результати дисертаційної роботи:

1. Розроблено метод визначення динаміки ймовірностей перебування рекомендаційної системи в своїх можливих станах з використанням математичного апарату марківських та напівмарківських процесів, що дає можливість встановлення зв'язку між набором щільності розподілу випадкових тривалостей перебування системи у цих станах і функціями опису динаміки ймовірностей станів для визначення ймовірностей перебування конкретної рекомендаційної системи в своїх можливих станах в довільний момент часу. На основі запропонованого методу було розроблено методику отримання аналітичних співвідношень для розрахунку ймовірностей перебування системи у своїх можливих станах в довільний момент часу.

2. Розроблено математичну модель стійкої рекомендаційної системи на основі запропонованого методу визначення динаміки ймовірностей перебування системи в своїх можливих станах, що дозволило здійснити оптимізацію загальних витрат на обслуговування системи в умовах внутрішніх дестабілізуючих факторів. На основі розробленої моделі запропоновано спосіб визначення повних витрат підсистеми збору та перерахунку вхідних даних, а також спосіб визначення оптимальної частоти перерахунку вхідних даних, при яких система має мінімальну збитковість.

3. Удосконалено метод колаборативної фільтрації, який відрізняється від існуючих використанням продукційних правил для визначення подоби користувачів та використанням показників активності користувачів для формування рекомендацій, що дозволило підвищити стійкість системи у випадку недостатньої кількості вхідних даних та під час холодного старту. Розроблено та реалізовано відповідні алгоритми, використання яких дозволило в 1.6 разів підвищити стійкість системи в порівнянні з відомим методом колаборативної фільтрації на основі моделі сусідства та в 3.2 разів – в

порівнянні з відомим методом колаборативної фільтрації на основі факторизації матриць.

4. Розроблено математичну модель підсистеми інформаційної безпеки стійкої рекомендаційної системи на основі запропонованого методу визначення динаміки ймовірностей перебування системи в своїх можливих станах, що дозволило визначити оптимальну частоту перевірки на наявність інформаційної атаки та профілів ботів. Розроблено методику отримання аналітичних співвідношень для розрахунку ймовірностей перебування підсистеми інформаційної безпеки в своїх можливих станах в довільний момент часу. На основі запропонованої математичної моделі розроблено спосіб визначення повних витрат, що зазнає рекомендаційна система внаслідок моніторингу власної інформаційної безпеки, нейтралізації діяльності бот-мереж та внаслідок інформаційних атак ін'єкцією профілів. Також розроблено спосіб визначення оптимальної частоти перевірки рекомендаційної системи на наявність інформаційної атаки та профілів ботів для оптимізації загальних витрат системи.

5. Розроблено метод імітаційного програмного моделювання користувачів та об'єктів рекомендаційної системи соціальної мережі або веб-ресурсу на основі існуючих і розроблених методів моделювання структури складних мереж та методів моделювання поведінки користувачів, що дозволило генерувати вхідні дані для тестування якості роботи алгоритмів формування рекомендацій. Розроблено спосіб моделювання змін вподобань у часі користувачів системи, що дозволяє генерувати тестові набори даних, більш схожі за статистичними характеристиками на реальні. Спосіб засновано на математичній моделі нециклічних змін вподобань користувачів у часі з використанням експоненційного закону розподілу та закону радіоактивного розпаду. Розроблено та реалізовано відповідні алгоритми та програмну імітаційну модель користувачів, об'єктів, бот-мереж та інформаційних процесів у рекомендаційній системі. За допомогою розробленої програмної моделі сформовано набори даних для тестування методів рекомендаційних систем та підсистем їх інформаційної безпеки.

6. Розроблено метод виявлення інформаційної атаки на рекомендаційну систему на основі аналізу трендів рейтингів об'єктів, що дозволило знизити кількість витрат на моніторинг безпеки системи за рахунок зняття необхідності пошуку ботів при відсутності ознак атаки. Розроблено та реалізовано відповідні алгоритми, які дозволили виявляти в середньому 76% об'єктів атак у рекомендаційній системі. Це дозволило при пошуку бот-мереж перевіряти не всі профілі користувачів рекомендаційної системи, як у відомих методах, а тільки ті, які взаємодіяли з ймовірними цілями атаки.

7. Розроблено метод виявлення бот-мереж у рекомендаційній системі на основі графової кластеризації та аналізу дій користувачів, що дозволило виявляти бот-мережі та розрізняти їх за множинами об'єктів атаки. Також розроблено спосіб ідентифікації окремих профілів ботів на основі нейронних мереж для уточнення результатів запропонованого методу. Розроблено відповідні алгоритми та реалізовано підсистему інформаційної безпеки рекомендаційної системи. Розроблена підсистема інформаційної безпеки дозволяє забезпечити вищу стійкість системи до зовнішніх дестабілізуючих факторів на відміну від існуючих методів. Вона дозволяє підвищити стійкість системи в середньому у 2.5 рази до випадкової та середньої

атаки та в 1.7 разів – до популярної атаки, якщо застосовується для методу колаборативної фільтрації на основі моделі сусідства або для запропонованого гібридного методу колаборативної фільтрації.

Проведена оцінка достовірності та ефективності запропонованих методів і моделей підвищення стійкості рекомендаційних систем.

Практичне значення отриманих результатів підтверджено відповідними актами впровадження. Результати дисертації впроваджені і використовуються у діяльності Компанії «Line Up», Державного підприємства «Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості», Державного підприємства «Харківський науково-дослідний інститут технологій машинобудування», Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса», а також використано у навчальному процесі Центральноукраїнського національного технічного університету та Національного технічного університету «Харківський політехнічний інститут».

Таким чином, сукупність отриманих у дисертаційній роботі наукових результатів і одержана в ході проведення експериментальних досліджень оцінка їх ефективності, дозволяють вважати сформульовану наукову проблему підвищення точності пропозицій рекомендаційних систем в умовах дестабілізуючих факторів у комп'ютерних мережах на основі розробки моделей та методів синтезу підсистеми забезпечення стійкості – вирішеною, а поставлену мету підвищення стійкості рекомендаційних систем соціальних мереж та веб-сервісів до внутрішніх та зовнішніх дестабілізуючих факторів у комп'ютерних мережах – досягнутою.

ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Дрєєв О.М., Смірнов О.А., Мелешко Є.В., Коваленко О.В. Метод прогнозування завантаженості серверу телекомунікаційної мережі // Системи обробки інформації. – 2012. – Вип. 3(2). – С. 181-187.
2. Смірнов О.А., Даниленко Д.О., Мелешко Є.В. Метод обнаружения вредоносного программного обеспечения. Часть 1. Корреляционный анализ сетевого трафика // Науково-технічний журнал «Інформаційно-керуючі системи на залізничному транспорті». – 2012. – № 4(95). – С. 8-14.
3. Даниленко Д.О., Смірнов О.А., Мелешко Є.В. Дослідження методів виявлення вторгнень в телекомунікаційні системи та мережі // Системи озброєння і військова техніка. – 2012. – № 1. – С. 92-100.
4. Мелешко Е.В. Метод встраивания двухуровневых цифровых водяных знаков в медиафайлы для защиты авторских прав // Збірник наукових праць Харківського університету Повітряних сил. – 2013. – Вип. 4. – С. 127-131.
5. Лысенко И.А., Смирнов А.А., Мелешко Е.В. Исследование уровней тестирования программного обеспечения инфотелекоммуникационных систем // Наука і техніка Повітряних Сил Збройних Сил України. – 2014. – № 4. – С. 79-81.
6. Шингалов Д.В., Мелешко Є.В., Минайленко Р.М., Резніченко В.А. Методи автоматичного аналізу тональності контенту у соціальних мережах для виявлення інформаційно-психологічних впливів // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – 2017. – Вип. 30. – С. 196-202.

7. Мелешко Є.В., Семенов С.Г., Хох В.Д. Дослідження методів побудови рекомендаційних систем в мережі Інтернет // Збірник наукових праць "Системи управління, навігації та зв’язку". Випуск 1(47). – Полтава: ПНТУ ім. Ю. Кондратюка. – 2018. – С. 131-136.

8. Мелешко Є.В. Методи оцінки якості роботи рекомендаційних систем // Системи управління, навігації та зв'язку. – Полтава: ПНТУ, 2018. – Вип. 5 (51). – С. 92-97.

9. Мелешко Є.В. Проблеми сучасних рекомендаційних систем та методи їх рішення // Системи управління, навігації та зв’язку. Збірник наукових праць. – Полтава: ПНТУ, 2018. – Т. 4 (50). – С. 120-124.

10. Улічев О.С., Мелешко Є.В. Програмне моделювання поширення інформаційно-психологічних впливів у віртуальних соціальних мережах // Сучасні інформаційні системи. – 2018. – Т. 2, № 2. – С. 35-39.

11. Шингалов Д.В., Мелешко Є.В., Минайленко Р.М., Резніченко В.А. Математична модель рекомендаційної системи з врахуванням емоційного забарвлення коментарів у якості контексту // Збірник наукових праць Кіровоградського національного технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кропивницький: ЦНТУ, 2018. – Вип. 31. – С. 181-186.

12. Meleshko Ye. Method of collaborative filtration based on associative networks of users similarity // Advanced information systems. – 2018. – Vol. 2, Iss. 4. – P. 55-59.

13. Мелешко Є.В. Методи кластеризації графів соціальних мереж для побудови рекомендаційних систем // Системи управління, навігації та зв’язку. Збірник наукових праць. – Полтава: ПНТУ, 2019. – Т. 2 (54). – С. 129-134.

14. Meleshko Ye. Method of generating recommendations lists with considering activity indexes of users in a recommendation system // Advanced information systems. – 2019. – Vol. 3, Iss. 1. – P. 43-47.

15. Meleshko Ye. Computer model of virtual social network with recommendation system // Innovative technologies and scientific solutions for industries. – 2019. – №2(8). – P. 80-85.

16. Мелешко Є.В., Хох В.Д., Улічев О.С. Дослідження робастності рекомендаційних систем з колаборативною фільтрацією до інформаційних атак // Електронне фахове наукове видання Кібербезпека: освіта, наука, техніка.– Київ: КУБГ, 2019. – Т.1, № 5. – С. 95-104.

17. Ulichev O.S., Meleshko Ye.V., Sawicki D., Smailova S. Computer modeling of dissemination of informational influences in social networks with different strategies of information distributors // Proc. SPIE 11176, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments, Wilga, Poland (ISSN: 0277-786X). – 2019. – 111761T. **(SCOPUS)**

18. Мелешко Є.В., Хох В.Д., Улічев О.С. Дослідження відомих моделей атак на рекомендаційні системи з колаборативною фільтрацією // Збірник наукових праць Системи управління, навігації та зв’язку. Збірник наукових праць. – Полтава: ПНТУ, 2019. – №. 5 (57). – С. 67-71.

19. Ulichev O., Meleshko Y., Khokh V. The computer simulation method of a social network structure for the research of dissemination processes of informational influences // Scientific and Practical Cyber Security Journal (SPCSJ), 4(3). – Georgia, Tbilisi, 2019. – P. 34-47.

20. Мелешко Є.В., Хох В.Д., Босько В.В. Дослідження матричних факторизаційних моделей рекомендаційних систем // Системи управління, навігації та зв’язку. Збірник наукових праць. – Полтава: ПНТУ, 2019. – Т. 6 (58). – С. 58-62.

21. Ulichev O., Meleshko Ye., Smirnov O., Khokh V., Goncharenko Iu. Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process // CEUR-WS, Vol 2588, Lviv, Ukraine (ISSN: 1613-0073). – 2019. – P. 215-227. **(SCOPUS)**

22. Meleshko Ye., Raskin L., Semenov S., Sira O. Methodology of probabilistic analysis of state dynamics of multi-dimensional semi-Markov dynamic systems // Eastern-European Journal of Enterprise Technologies (ISSN: 1729-3774). – 2019. – Vol. 6, No 4(102). – P. 6-13. **(SCOPUS)**

23. Міхав В.В., Мелешко Є.В., Якименко М.С. Метод зберігання даних рекомендаційної системи на основі бінарних діаграм рішень // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2020. – Т. 2 (60). – С. 85-89.

24. Meleshko Ye., Drieiev O., Drieieva H. Method of identification bot profiles based on neural networks in recommendation systems // Advanced Information Systems. – 2020. – Vol. 4, No. 2 – C. 24-28.

25. Meleshko Ye., Drieiev O., Yakymenko M., Lysytsia D. Developing a model of the dynamics of states of a recommendation system under conditions of profile injection attacks // Eastern-European Journal of Enterprise Technologies (ISSN 1729-3774). – 2020. – Vol. 4, No. 4(106). – P. 14-24. **(SCOPUS)**

26. Mohammed A.S., Meleshko Y., Balaji S.B., Semenov S. Collaborative filtering method with the use of production rules // Proceedings of ICCIKE, Amity University Dubai; United Arab Emirates. – 2019. – P. 387-391. **(SCOPUS)**

27. Мелешко Е.В., Смирнов А.А. Исследование методов структурного анализа социальных сетей с точки зрения информационной безопасности // Материалы XXI Международной научно-технической конференции "Современные средства связи", 20-21 октября 2016 года, Минск, Республика Беларусь – Минск: Белорусская государственная академия связи. – 2016. – С. 175-177.

28. Мелешко Є.В. Методи протидії деструктивним інформаційним впливам в соціальних мережах в умовах інформаційної війни // Збірник тез Всеукраїнської науково-практичної конференції «Інформаційна безпека держави суспільства та особистості», м. Кіровоград, 16 квітня 2015 р. – Кіровоград: КНТУ. – 2015. – С. 139-142.

29. Мелешко Є.В. Аналіз структури соціальної мережі з точки зору інформаційної безпеки // Збірник тез XVIII міжнародного науково-практичного семінару "Комбінаторні конфігурації та їх застосування", м. Кіровоград, 15-16 квітня 2016. – Кіровоград: Кіровоградський національний технічний університет. – 2016. – С. 93-97.

30. Мелешко Є.В. Дослідження методів динамічного аналізу віртуальних соціальних мереж з точки зору інформаційної безпеки // Матеріали Всеукраїнської науково-практичної конференції "Кібербезпека в Україні: правові та організаційні питання", м. Одеса, 21 жовтня 2016 р. – Одеса: ОДУВС. – 2016. – С. 154-155.

31. Мелешко Є.В., Шингалов Д.В., Минайленко Р.М. Методи автоматизації побудови графових структур спільнот у соціальних мережах // Матеріали XIX Міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування» присвяченого пам'яті д.ф.-м.н., професора Петренюка Анатолія Яковича, м. Кропивницький, 7-8 квітня 2017 року. – Кропивницький: КЛА НАУ. – 2017. – С. 162-164.

32. Охотний С.М., Мелешко Є.В. Збирання даних про користувачів віртуальної соціальної мережі за допомогою web-кроулера // Збірник тез II Міжнародної науково-

практичної конференції «Інформаційна безпека та комп’ютерні технології», м. Кропивницький, 20-22 квітня 2017 р. – Кропивницький: ЦНТУ. – 2017. – С. 157-159.

33. Улічев О.С., Мелешко Є.В. Моделювання розповсюдження інформаційно-психологічних впливів у сегменті соціальної мережі // Збірник тез VI міжнародної наукової конференції "Інформація. Комунікація. Суспільство", м. Львів, 18-20 травня 2017 р. – Львів: Національний університет "Львівська політехніка". – 2017. – С. 29-30.

34. Охотний С.М., Мелешко Є.В., Константинова А.А. Розробка бота для соціальної мережі Facebook на основі фреймворка Selenium // Збірник тез Всеукраїнської науково-практичної Інтернет-конференції "Автоматика та комп’ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті", м. Кропивницький, 16-17 листопада 2017 р. – Кропивницький: ЦНТУ. – 2017. – С. 202-203.

35. Мелешко Є.В., Гермак В.С. Дослідження впливу структури соціальної мережі на захищеність від поширення вірусної інформації // Збірник тез доповідей III Міжнародної науково-практичної конференції "Актуальні питання забезпечення кібербезпеки та захисту інформації". с. Верхнє Студене, 22-25 лютого 2017 р. – Київ: Видавництво Європейського університету. – 2017. – С. 118-119.

36. Улічев О.С., Мелешко Є.В. Математична модель розповсюдження інформації в сегменті соціальної мережі // Матеріали XX Міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування», м. Кропивницький, 13-14 квітня 2018 р. – Кропивницький: КЛА НАУ. – 2018. – С. 68-72.

37. Улічев О.С., Мелешко Є.В. Програмна модель розповсюдження інформаційно-психологічних впливів в сегменті соціальної мережі // Збірник тез VIII Всеукраїнської науково-практичної конференції «Безпека інформаційних технологій (ITSec 2018)», м. Київ, 16-18 травня 2018 р. – Київ: НАУ. – 2018. – С. 34-35.

38. Мелешко Є.В., Хох В.Д., Сидоренко В.В. Розробка автоматизованої системи виявлення, оцінки та розробки заходів по усуненню загроз в інформаційних системах // Збірник тез VIII Всеукраїнської науково-практичної конференції «Безпека інформаційних технологій (ITSec 2018)», м. Київ, 16-18 травня 2018 р. – Київ: НАУ. – 2018. – С. 38-39.

39. Улічев О.С., Мелешко Є.В. Моделювання розповсюдження інформаційно-психологічних впливів у сегменті соціальної мережі // Збірник тез VII Міжнародної наукової конференції «Інформація. Комунікація. Суспільство (ICS-2018)», 17-19 травня 2018 р., Україна, смт. Чинадієво. – Львів: НУ «Львівська політехніка». – 2018. – С. 29-30.

40. Охотний С.М., Мелешко Є.В. Визначення центральностей у соціальному графі засобами графової бази даних Neo4j // Збірник тез III Міжнародної науково-практичної конференції «Інформаційна безпека та комп’ютерні технології», м. Кропивницький. 19-20 квітня 2018 р. – Кропивницький: ЦНТУ. – 2018. – С. 247-248.

41. Улічев О.С., Мелешко Є.В. Програмна модель соціальної мережі та стратегій поширення інформаційно-психологічних впливів // Збірник тез III Міжнародної науково-практичної конференції «Інформаційна безпека та комп’ютерні технології», м. Кропивницький, 19-20 квітня 2018 р. – Кропивницький: ЦНТУ. – 2018. – С. 136-220.

42. Мелешко Є.В. Дослідження методів побудови рекомендаційних систем заснованих на фільтрації контенту // Збірник тез III Міжнародної науково-практичної конференції «Інформаційна безпека та комп’ютерні технології», м. Кропивницький, 19-20 квітня 2018 р. – Кропивницький: ЦНТУ. – 2018. – С. 234-237.

43. Мелешко Є.В. Методи оцінки якості роботи рекомендаційних систем //

Матеріали XX Міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування», м. Кропивницький, 13-14 квітня 2018 р. – Кропивницький: КЛА НАУ. – 2018. – С. 68-72.

44. Мелешко Є.В. Загрози інформаційній безпеці у рекомендаційних системах соціальних медіа // Збірник тез VIII Всеукраїнської науково-практичної конференції «Безпека інформаційних технологій (ITSec 2018)», м. Київ, 16-18 травня 2018 р. – Київ: НАУ. – 2018. – С. 24-25.

45. Мелешко Є.В., Дреєва Г.М. Дослідження проблем сучасних рекомендаційних систем // Збірник тез VII Міжнародної наукової конференції «Інформація. Комунікація. Суспільство (ICS-2018)», 17-19 травня 2018 р., Україна, смт. Чинадієво. – Львів: НУ «Львівська політехніка». – 2018. – С. 31-32.

46. Мелешко Є.В. Методи оцінки точності прогнозування вподобань користувачів веб-ресурсів рекомендаційними системами // Збірник тез X Всеукраїнської науково-практичної конференції «Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2018)», с. Коблево, 21-23 червня 2018 р. – Миколаїв: НАУ та МІПРО. – 2018. – С. 58-61.

47. Мелешко Є.В. Дослідження проблем сучасних рекомендаційних систем та методів їх рішення // Збірник тез Міжнародної науково-практичної конференції «Контроль і управління в складних системах (КУСС-2018)», м. Вінниця, 15-17 жовтня 2018 р. – Вінниця: ВНТУ. – 2018. – С. 126.

48. Мелешко Є.В., Босько В.В., Резніченко В.А. Застосування асоціативних мереж для побудови рекомендаційних систем // Збірник тез Міжнародної науково-практичної Інтернет-конференції «Автоматика, комп'ютерно-інтегровані технології та проблеми енергоефективності в промисловості і сільському господарстві (АКІТ-2018)», м. Кропивницький, 15-16 листопада 2018 р. – Кропивницький: ЦНТУ. – 2018. – С. 165-166.

49. Мелешко Є.В., Босько В.В., Резніченко В.А. Розробка рекомендаційної системи на базі СУБД Neo4j // Збірник тез V Міжнародної науково-практичної конференції «Інформаційні технології та взаємодії (IT&I – 2018)», м. Київ, 20-21 листопада 2018 р. – Київ: КНУ. – 2018. – С. 351-352.

50. Шингалов Д.В., Мелешко Є.В., Минайленко Р.М. Дослідження програмних засобів для аналізу та візуалізації соціальних графових структур // Збірник тез V Міжнародної науково-практичної конференції «Інформаційні технології та взаємодії (IT&I-2018)», м. Київ, 20-21 листопада 2018 р. – Київ: КНУ. – 2018. – С. 159-160.

51. Мелешко Є.В. Розробка програмного забезпечення для виділення співтовариств у соціальній мережі // Збірник тез III Всеукраїнської науково-практичної конференції «Перспективні напрямки сучасної електроніки, інформатики і комп'ютерних систем», м. Дніпро, 21-23 листопада 2018 р. – Дніпро: ДНУ. – 2018. – С. 42-43.

52. Мелешко Є.В. Метод визначення подоби між користувачами у рекомендаційних системах з колаборативною фільтрацією // Збірник тез Науково-практичної конференції «Інформатика, математика, автоматика (ІМА-2019)», м. Суми, 23-26 квітня 2019 р. – Суми: СДУ. – 2019. – С. 213-214.

53. Мелешко Є.В., Охотний С.М., Босько В.В. Розробка програмного забезпечення для збору та аналізу даних із соціальних мереж // Збірник тез IX Міжнародної науково-практичної конференції «Комплексне забезпечення якості технологічних процесів та систем», Т.2, м. Чернігів, 14-16 травня 2019 р. – Чернігів: ЧНТУ. – 2019. – С. 225-226.

54. Мелешко Є.В. Метод побудови рекомендаційних систем на основі асоціативних мереж користувачів // Збірник тез XXI Міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування», м. Кропивницький, 17-18 травня 2019 р. – Кропивницький: КЛА НАУ. – 2019. – С. 91-95.

55. Мелешко Є.В., Босько В.В., Резніченко В.А. Дослідження методів комп'ютерної лінгвістики для аналізу контенту веб-сайтів // Збірник тез XXI Міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування», м. Кропивницький, 17-18 травня 2019 р. – Кропивницький: КЛА НАУ. – 2019. – С. 96-100.

56. Мелешко Є.В. Дослідження засобів кластеризації графів у графовій СУБД Neo4j для виявлення співтовариств у соціальних мережах // Збірник тез VIII Міжнародної наукової конференції «Інформація. Комунікація. Суспільство», смт. Чинадієво, 16-18 травня 2019 р. – Львів: Видавництво Львівської політехніки. – 2019. – С. 19-20.

57. Мелешко Є.В., Чабан О.О. Дослідження засобів парсингу веб-сайтів // Збірник тез VIII Міжнародної наукової конференції «Інформація. Комунікація. Суспільство», смт. Чинадієво, 16-18 травня 2019 р. – Львів: Видавництво Львівської політехніки. – 2019. – С. 168-20.

58. Мелешко Є.В. Методи кластеризації графів для побудови рекомендаційних систем соціальних медіа // Збірник тез VII Міжнародної науково-практичної конференції «Обробка сигналів і негаусівських процесів», присвячена пам'яті професора Кунченка Ю.П., м. Черкаси, 23-24 травня 2019 р., – Черкаси: ЧДТУ. – 2019. – С. 100-102.

59. Мелешко Є.В., Дрєєва Г.М. Дезінформаційні атаки на рекомендаційні системи // Збірник тез Міжнародної наукової конференції «Безпека в сучасному світі», м. Дніпро, 27-28 вересень 2019 р. – Дніпро: ДНУ ім. Олеся Гончара. – 2019. – С. 51-53.

60. Мелешко Є.В., Чабан О.О., Міхав В.В. Способи побудови рекомендаційних систем для соціальних мереж з врахуванням репутації користувачів // Збірник тез Всеукраїнської науково-практичної конференції «Перспективні напрямки інформаційних і комп'ютерних систем та мереж, комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті», м. Кропивницький, 13-14 листопада 2019 р. – Кропивницький: ЦНТУ. – 2019. – С. 86-87.

61. Мелешко Є.В., Хох В.Д., Улічев О.С. Методи тестування робастності рекомендаційних систем з колаборативною фільтрацією // Збірник тез Всеукраїнської науково-практичної конференції «Перспективні напрямки інформаційних і комп'ютерних систем та мереж, комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті», м. Кропивницький, 13-14 листопада 2019 р. – Кропивницький: ЦНТУ. – 2019. – С. 88-89.

62. Мелешко Є.В., Охотний С.М., Резніченко В.А. Дослідження методів визначення спільнот у соціальному графі // Збірник тез Всеукраїнської науково-практичної конференції «Перспективні напрямки інформаційних і комп'ютерних систем та мереж, комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті», м. Кропивницький, 13-14 листопада 2019 р. – Кропивницький: ЦНТУ. – 2019. – С. 92-93.

63. Мелешко Є.В., Хох В.Д., Минайленко Р.М. Розробка експертної системи для виявлення атак на рекомендаційні мережі // Збірник тез XVII Міжнародної науково-практичної конференції «Математичне та програмне забезпечення інтелектуальних систем», м. Дніпро, 20-22 листопада 2019 р. – Дніпро: ДНУ. – 2019. – С. 176-177.

64. Шингалов Д.В., Мелешко Є.В., Улічев А.С. Дослідження Баєсових мереж довіри як засобів для моделювання динамічних процесів у складних мережах // Збірник тез XVII Міжнародної науково-практичної конференції «Математичне та програмне забезпечення інтелектуальних систем», м. Дніпро, 20-22 листопада 2019 р. – Дніпро: ДНУ. – 2019. – С. 284-285.

65. Мелешко Є., Хох В., Резніченко В., Босько В. Дослідження методів оцінювання робастності рекомендаційних систем до атак накручування рейтингів // Збірник тез IV Всеукраїнської науково-практичної конференції «Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем MEICS-2019», м. Дніпро, 27-29 листопада 2019 р. – Дніпро: ДНУ. – 2019. – С. 10-11.

66. Мелешко Є.В., Дрєєва Г.М., Гермак В.С., Резніченко В.А., Шевченко О.О. Методи визначення ботів серед користувачів соціальних мереж // Збірник тез II Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології", м. Кропивницький, 2-3 квітня 2020 р. – Кропивницький: ЦНТУ. – 2020. – С. 44.

67. Мелешко Є.В., Хох В.Д. Дослідження моделей рекомендаційних систем на основі прихованих факторів // Збірник тез II Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології", м. Кропивницький, 2-3 квітня 2020 р. – Кропивницький: ЦНТУ. – 2020. – С. 46.

68. Міхав В.В., Мелешко Є.В. Метод оптимізації швидкодії бінарних діаграм рішень при представленні даних рекомендаційної системи // Збірник тез II Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології", м. Кропивницький, 2-3 квітня 2020 р. – Кропивницький: ЦНТУ. – 2020. – С. 17.

69. Шингалов Д.В., Мелешко Є.В., Босько В.В. Дослідження моделей репутації користувачів соціальної мережі // Збірник тез II Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології", м. Кропивницький, 2-3 квітня 2020 року. – Кропивницький: ЦНТУ. – 2020. – С. 29.

70. Мелешко Є.В., Дрєєв О.М., Дрєєва Г.М. Розробка методу ідентифікації ботів у рекомендаційних системах // Матеріали X міжнародної науково-практичної конференції "Комплексне забезпечення якості технологічних процесів та систем", м. Чернігів, 29-30 квітня 2020 р. – Чернігів: ЧНТУ. – 2020. – С. 165-166.

71. Міхав В.В., Мелешко Є.В. Порівняння стратегій редагування бінарних діаграм рішень для роботи з графовими даними // Матеріали IX Міжнародної наукової конференції "Інформація. Комунікація. Суспільство", м. Львів, 21-23 травня 2020 р. – Львів: Видавництво Львівської політехніки. – 2020. – С. 17-18.

72. Мелешко Є.В., Дрєєва Г., Якименко М., Хох В. Методи моделювання складних мереж // Матеріали 9-ої Міжнародної наукової конференції "Інформація. Комунікація. Суспільство", м. Львів, 21-23 травня 2020 р. – Львів: Видавництво Львівської політехніки. – 2020. – С. 29-30.

73. Мелешко Є.В., Хох В.Д., Улічев О.С. Дослідження методів підвищення робастності рекомендаційних систем до інформаційних атак // Матеріали VI Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації», 19-22 лютого 2020 р. – м. Київ: Вид-во Європейського університету, 2020. – С. 65-70.

74. Мелешко Є.В., Дрєєва Г.М., Дрєєв О.М. Метод кластеризації користувачів соціальної мережі на основі нейронних мереж // Збірник тез XXII Міжнародного

науково-практичного семінару «Комбінаторні конфігурації та їх застосування» імені А.Я. Петренюка, м. Запоріжжя, 15-16 травня 2020 р. – Запоріжжя-Кропивницький: КЛА НАУ. – 2020. – С. 87-90.

75. Мелешко Є.В., Якименко М.С., Резніченко В.А. Методи оцінки якості роботи алгоритмів машинного навчання // Збірник тез XXII Міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування» імені А.Я. Петренюка, м. Запоріжжя, 15-16 травня 2020 р. – Запоріжжя-Кропивницький: КЛА НАУ. – 2020. – С. 90-94.

76. Шингалов Д.В., Мелешко Є.В., Босько В.В. Методи нормалізації даних для моделей машинного навчання // Збірник тез XXII Міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування» імені А.Я. Петренюка, м. Запоріжжя, 15-16 травня 2020 р. – Запоріжжя-Кропивницький: КЛА НАУ. – 2020. – С. 197-200.

АНОТАЦІЯ

Мелешко Є.В. Методологія забезпечення стійкості рекомендаційних систем до дестабілізуючих факторів у комп'ютерних мережах – Рукопис.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – Комп'ютерні системи та компоненти. – Черкаський державний технологічний університет, Черкаси, 2021.

Дисертаційна робота присвячена розв'язанню актуальної науково-практичної проблеми підвищення точності пропозицій рекомендаційних систем в умовах дестабілізуючих факторів у комп'ютерних мережах на основі розробки моделей та методів синтезу підсистеми забезпечення стійкості. У роботі проведено аналіз сучасних моделей та методів синтезу рекомендаційних систем для соціальних мереж та контент-орієнтованих веб-сервісів, який показав, що переважна більшість існуючих моделей і методів вразливі до дії внутрішніх та зовнішніх дестабілізуючих факторів у комп'ютерних мережах. Показано, що забезпечення стійкості рекомендаційних систем до дії дестабілізуючих факторів є важливою умовою для підвищення точності їх роботи. Розроблено метод визначення динаміки ймовірностей перебування рекомендаційної системи в своїх можливих станах з використанням математичного апарату марківських та напівмарківських процесів. Розроблено математичну модель стійкої рекомендаційної системи, що дозволило здійснити оптимізацію загальних витрат на обслуговування системи в умовах внутрішніх дестабілізуючих факторів. Удосконалено метод колаборативної фільтрації, який відрізняється від існуючих використанням продукційних правил та показників активності користувачів, що дозволило підвищити стійкість системи в умовах холодного старту, розроблено відповідні алгоритми. Розроблено математичну модель підсистеми інформаційної безпеки стійкої рекомендаційної системи, що дозволило визначити оптимальну частоту перевірки на наявність інформаційної атаки та профілів ботів у системі, розроблено відповідні алгоритми. Розроблено метод імітаційного програмного моделювання користувачів та об'єктів рекомендаційної системи, що дозволило генерувати вхідні дані для тестування якості роботи алгоритмів формування рекомендацій, розроблено відповідну програмну імітаційну модель. Розроблено метод виявлення інформаційної атаки на рекомендаційну систему на основі аналізу трендів рейтингів об'єктів, що дозволило знизити кількість

витрат на моніторинг безпеки системи за рахунок зняття необхідності пошуку ботів при відсутності ознак атаки, розроблено відповідні алгоритми. Розроблено метод виявлення бот-мереж у рекомендаційній системі на основі графової кластеризації та аналізу дій користувачів для забезпечення стійкості системи до зовнішніх дестабілізуючих факторів, розроблено відповідні алгоритми.

Ключові слова: рекомендаційні системи, комп'ютерні мережі, проблема холодного старту, колаборативна фільтрація, аналіз даних, кластеризація, моделювання складних мереж, інформаційні атаки, бот-мережі, соціальні мережі, веб-ресурси

АННОТАЦИЯ

Мелешко Е.В. Методология обеспечения устойчивости рекомендательных систем к дестабилизирующим факторам в компьютерных сетях – Рукопись.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.05 – Компьютерные системы и компоненты. – Черкасский государственный технологический университет, Черкассы, 2021.

Диссертация посвящена решению актуальной научно-практической проблемы повышения точности предложений рекомендательных систем в условиях дестабилизирующих факторов в компьютерных сетях на основе разработки моделей и методов синтеза подсистемы обеспечения устойчивости. В работе проведен анализ современных моделей и методов синтеза рекомендательных систем для социальных сетей и контент-ориентированных веб-сервисов, который показал, что подавляющее большинство существующих моделей и методов уязвимы к действию внутренних и внешних дестабилизирующих факторов в компьютерных сетях. Показано, что обеспечение устойчивости рекомендательных систем к действию дестабилизирующих факторов является важным условием для повышения точности их работы. Разработан метод определения динамики вероятностей пребывания рекомендательной системы в своих возможных состояниях с использованием математического аппарата марковских и полумарковских процессов. Разработана математическая модель устойчивой рекомендательной системы, что позволило осуществить оптимизацию общих затрат на обслуживание системы в условиях внутренних дестабилизирующих факторов. Усовершенствован метод коллаборативной фильтрации, который отличается от существующих использованием продукционных правил и показателей активности пользователей, что позволило повысить устойчивость системы в условиях холодного старта, разработаны соответствующие алгоритмы. Разработана математическая модель подсистемы информационной безопасности устойчивой рекомендательной системы, что позволило определить оптимальную частоту проверки на наличие информационной атаки и профилей ботов в системе, разработаны соответствующие алгоритмы. Разработан метод имитационного программного моделирования пользователей и объектов рекомендательной системы, что позволило генерировать входные данные для тестирования качества работы алгоритмов формирования рекомендаций, разработана соответствующая программная имитационная модель. Разработан метод выявления информационной атаки на рекомендательную систему на основе анализа трендов рейтингов объектов, что позволило снизить количество

затрат на мониторинг безопасности системы за счет снятия необходимости поиска ботов при отсутствии признаков атаки, разработаны соответствующие алгоритмы. Разработан метод выявления бот-сетей в рекомендательной системе на основе графовой кластеризации и анализа действий пользователей для обеспечения устойчивости системы к внешним дестабилизирующим факторам, разработаны соответствующие алгоритмы.

Ключевые слова: рекомендательные системы, компьютерные сети, проблема холодного старта, коллаборативная фильтрация, анализ данных, кластеризация, моделирование сложных сетей, информационные атаки, бот-сети, социальные сети, веб-ресурсы

ABSTRACT

Meleshko Ye. The methodology of ensuring the stability of recommendation systems to destabilizing factors in computer networks – Manuscript.

Dissertation for the degree of Doctor in Technical Sciences, specialty 05.13.05 – Computer systems and components. – Cherkasy State Technological University, Cherkasy, 2021.

The thesis is devoted to solution of an actual scientific and practical problem of accuracy increasing for propositions of recommendation systems in the conditions of destabilizing factors in computer networks on the basis of development of models and methods of synthesis of a subsystem of stability ensuring.

The object of research is process of functioning of recommendation systems of social networks and websites in computer networks.

The subject of research is methodology of stability ensuring of recommendation systems in the conditions of destabilizing factors.

It is shown that today recommendation systems in computer networks are increasingly used for promotion of content, goods and services. Such systems are tools for automatic generation of recommendations based on study of personal needs of website users. They are most often used in e-commerce, content-oriented websites, social networks and search engines.

Analysis of modern models and methods of synthesis of recommendation systems for social networks and content-oriented web services is carried out. The analysis showed that the vast majority of existing models and methods are vulnerable to internal and external destabilizing factors in computer networks. Ensuring the stability of recommendation systems to the action of destabilizing factors is an important condition for improving their accuracy.

Examples of internal destabilizing factors in recommendation systems would be cold start problem, constant cold start problem, filter bubble problem of and problem of insufficient quantity and quality of input data, as well as problem of permanent change of user preferences over time. The main external destabilizing factor in recommendation systems is injection profile attacks.

A method for determining the dynamics of probabilities of recommendation system in its possible states using the mathematical apparatus of Markov and semi-Markov processes is developed. This allows to determine the probabilities of staying specific recommendation system in its possible states at any moment of time.

A mathematical model of a stable recommendation system is developed on the basis of the proposed method of determining the dynamics of probabilities of staying the system in its possible states, allowing to optimize the total cost of system maintenance in the

conditions of internal destabilizing factors.

The method of collaborative filtering is improved. This method differs from the existing ones in using production rules to determine user similarity and using user activity indicators to form recommendations. This allowed to increase system stability in conditions of insufficient input and cold start.

A mathematical model of information security subsystem of a stable recommendation system is developed on the basis of the proposed method of determining the dynamics of probabilities of staying the system in its possible states, this allowed to determine the optimal frequency of checking for information attack and bot profiles in the system.

A method of software simulation modeling of users and objects of the recommendation system of a social network or web resource based on existing and developed methods of modeling the structure of complex networks and methods of modeling user behavior is developed. This allowed to generate input data for testing the quality of algorithms for forming recomendations.

A method of detecting an information attack on the recommendation system based on the analysis of trends of the ratings of objects is developed. This allowed to reduce the cost on monitoring system security by eliminating the need of search for bots in the absence of signs of attack.

A method of detecting botnets in the recommendation system based on graph clustering and analysis of user actions for ensuring stability of the system to external destabilizing factors is developed. This allowed to detect botnets and differ them using sets of attack objects.

The practical value of the work is as follows. Algorithms for software simulation modeling of users and objects of the recommendation system are developed. These algorithms allowed generating input data for testing algorithms that form recommendation lists. Improved collaborative data filtering algorithms are developed to generate more accurate lists of recommendations for web-resource users based on production rules and the use of user activity metrics. Algorithms for detecting the presence of an information attack on the recommendation system based on the analysis of trends in the ratings of system objects are developed. Algorithms for detecting separate bot profiles based on neural networks and algorithms for detecting bot networks in the recommendation system based on graph clustering and analysis of user activities are developed. A technique for obtaining analytical relations for calculating the probabilities of a stable recommendation system in its possible states at any time to optimize the frequency of recalculation of input data for the formation of recommendations are developed. A technique for obtaining analytical relations for calculating the probabilities of a stable recommendation system in its possible states at any time to optimize the frequency of recalculation of input data for determining the optimal frequency of checking for information attacks and bots presence.

The assessment of credibility and efficiency of the proposed methods and models for increasing the stability of recommendation systems was carried out.

Thus, the results obtained in the dissertation allow to increase stability of recommendation systems to internal and external destabilizing factors and this allows to increase accuracy and other quality indicators of recommendation lists creating.

Keywords: recommendation systems, computer networks, cold start problem, collaborative filtering, data analysis, clustering, modeling of complex networks, information attacks, bot networks, social networks, web resources