ВІДГУК

офіційного опонента на дисертаційну роботу **Мелешко Єлизавети Владиславівни** "Методологія забезпечення стійкості рекомендаційних систем до дестабілізуючих факторів у комп'ютерних мережах" на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Актуальність теми дисертації.

Динамічний розвиток комп'ютерних систем та компонентів стимулюють створення нових інформаційних послуг серед яких можна виділити окремий вид програмного забезпечення – рекомендаційні системи.

Якість роботи рекомендаційних систем у великій кількості залежить від точності пропозицій, що надаються суб'єктам інформаційного простору. При цьому цей показник якості рекомендацій визначається як суб'єктивною оцінкою користувачів та замовників так і відповідними керівними документами, що визначають якість та ефективність роботи рекомендаційних систем. Цей фактор підкреслює актуальність та велику кількість розробок, що пов'язані с забезпеченням точності пропозицій рекомендаційних систем. Однак, на теперішній час рівень та різноманіття дестабілізуючих факторів впливу на існуючи рекомендаційні системи обумовлює втрати та ризики.

На даний час в теорії і практиці функціонування рекомендаційних систем загострилося протиріччя між підвищенням вимог щодо точності пропозицій суб'єктам рекомендаційних систем, збільшенням ризиків впливу на цей процес внутрішніх і зовнішніх дестабілізуючих факторів, та існуючим станом теоретичного обґрунтування, синтезу та практичної реалізації підсистем забезпечення стійкості до цих деструктивних впливів. Тому дисертаційна робота Мелешко Єлизавети Владиславівни що присвячена вирішенню наукової проблеми підвищення точності пропозицій рекомендаційних систем в умовах дестабілізуючих факторів у комп'ютерних мережах на основі розробки моделей та методів синтезу підсистеми забезпечення стійкості є актуальною.

Дисертаційна робота виконана відповідно до пріоритетних наукових напрямів, які охоплюють актуальні проблеми, перелічені в документі «Основні наукові напрямки та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2019–2023 роки наук України», затвердженою постановою Президії НАН України від 30 січня 2019 року, №30, розділ 1.2 «Інформатика», напрямки «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). в яких автор є співвиконавцем окремих етапів.

Основний зміст роботи.

У вступі обґрунтовано актуальність дисертації, визначено мету, об'єкт та предмет дослідження. Сформульовано проблему дисертаційного дослідження, наукові завдання, наведено основні наукові та практичні результати. Відзначено особистий внесок здобувача, апробацію результатів дисертаційної роботи на конференціях, наведено відомості про публікації та структуру роботи.

У першому розділі здобувачем проведене дослідження та порівняльний аналіз існуючих моделей і методів роботи рекомендаційних систем, розроблена їх класифікація. Розглянуто основні внутрішні та зовнішні дестабілізуючі фактори у роботі сучасних рекомендаційних систем.

Проведені дослідження та порівняльний аналіз відомих методів синтезу рекомендаційних систем показали, що одним з перспективних напрямків у розвитку даних методів є удосконалення існуючих методів формування рекомендацій та розробка підсистем забезпечення стійкості до холодного старту, вхідних даних низької якості та інформаційних атак.

У другому розділі дисертаційної роботи запропоновано метод визначення динаміки ймовірностей перебування рекомендаційної системи в своїх можливих станах. Основу методу становить модель динаміки ймовірностей станів системи. Модель містить набір інтегральних рівнянь щодо невідомих функцій, що описують ймовірнісну динаміку системи. В результаті рішення інтегральних рівнянь отримано шукане співвідношення для розрахунку умовної ймовірності знаходження рекомендаційної системи в стані H_0 в довільний момент часу t, якщо в початковий момент часу об'єкт знаходився в стані H_0. Підкреслю, що 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. Отримані співвідношення, по-перше, дають можливість вирішувати задачі оцінки ефективності системи в залежності від значень задаваємого набору її параметрів. По-друге, вони можуть бути використані для оптимізації управління розподілом обмеженого ресурсу з метою підвищення ефективності системи.

Також у даному розділі досліджено поняття стійкості рекомендаційних систем та способи її оцінювання. Обґрунтовано шляхи забезпечення стійкості рекомендаційної системи до внутрішніх та зовнішніх дестабілізуючих факторів.

У третьому розділі запропоновано математичну модель стійкої рекомендаційної системи для оптимізації загальних витрат на її обслуговування, розроблену на основі методу визначення динаміки ймовірностей перебування системи в своїх можливих станах. На основі розробленої математичної 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.

Також у даному розділі запропоновано гібридний метод колаборативної фільтрації, стійкий до внутрішніх дестабілізуючих факторів.

Було проведено експерименти для порівняння точності та стійкості розробленого гібридного методу з відомими методами колаборативної фільтрації. Експерименти показали, що розроблений гібридний метод, на відміну від методу колаборативної фільтрації на основі моделі сусідства, дозволяє забезпечити 100% покриття простору 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). Також розроблений гібридний метод, на відміну від існуючих методів колаборативної фільтрації, більш стійкий до дестабілізуючого фактору холодного старту користувачів. А саме, в 1.6 разів підвищується стійкість в порівнянні з методом на основі моделі сусідства та в 3.2 разів в порівнянні з методом на основі факторизації матриць.

У четвертому розділі розроблені математичні та програмні імітаційні моделі користувачів, об’єктів та інформаційних процесів рекомендаційної системи, що дозволяють одержувати набори даних для тестування алгоритмів рекомендаційних систем. Крім поведінки звичайних користувачів системи було здійснено моделювання також поведінки ботів на основі різних відомих

моделей інформаційних атак на рекомендаційні системи з метою формування наборів даних, що можна використати для тестування стійкості системи до зовнішніх дестабілізуючих факторів.

У п'ятому розділі запропоновано математичну модель підсистеми безпеки рекомендаційної системи на основі запропонованого раніше методу визначення динаміки ймовірностей перебування системи в своїх можливих станах, що дозволило визначати оптимальну частоту перевірки на наявність інформаційної атаки та профілів ботів. У межах математичної моделі розроблено набір можливих станів, у яких може перебувати рекомендаційна система в умовах інформаційних атак ін'єкцією профілів. Запропоновано три стани роботи рекомендаційної системи в умовах інформаційної атаки, а саме, «нормальний стан», «система атакована» та «система відбиває атаку». Визначено можливі переходи між цими станами. Розроблено аналітичні співвідношення для розрахунку ймовірностей перебування рекомендаційної системи в своїх можливих станах в довільний момент часу.

Розроблено спосіб визначення оптимальної частоти перевірки рекомендаційної системи на наявність інформаційної атаки та профілів ботів для оптимізації загальних витрат системи. В розглянутому дисертантом прикладі, використання оптимальної частоти перевірки системи на наявність атаки знижує загальні витрати власників системи на 30.7% в порівнянні з постійною перевіркою системи.

Запропоновано 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. Розроблений метод в середньому дозволяє виявити 76% об'єктів інформаційних атак у рекомендаційній системі. Об'єкти, які не зазнавали інформаційної атаки та помилково були визначені як такі, що зазнали атаки, в середньому складали 13%.

Запропоновано спосіб ідентифікації профілів ботів на основі нейронних мереж у рекомендаційних системах. При наявності 10 цілей у ботів, незалежно від моделі атаки, розроблений метод може ідентифікувати профілі ботів в середньому з точністю 0.97.

Основною метою шостого розділу є розроблення методу виявлення і нейтралізації зовнішніх дестабілізуючих факторів у рекомендаційній системі та дослідження достовірності отриманих результатів.

Розроблена підсистема інформаційної безпеки дозволяє забезпечити вищу стійкість рекомендаційної системи до зовнішніх дестабілізуючих факторів на відміну від існуючих методів. Вона в середньому показує в 2.5 рази кращі результати значення стійкості для випадкової та середньої атаки та в 1.7 разів 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 профілів користувачів за їх статистичними даними.

Наукова новизна дисертаційної роботи.

– *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.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, та їх достовірність.

Обґрунтованість та достовірність наукових положень, висновків і рекомендацій дисертації забезпечується аргументованими результатами досліджень та співставленням з результатами математичного моделювання.

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».

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: 25 наукових статей (з них 4 входять до бази даних Scopus; 2 – опубліковані у закордонних рецензованих виданнях; 22 – у вітчизняних фахових наукових журналах, з яких 7 статей одноосібні), а також 51 тези доповідей (з них 1 входять до бази даних Scopus).

Відповідність автореферату дисертації.

Зміст автореферату є ідентичним до змісту дисертації й повною мірою відображає основні завдання, наукову новизну, практичне значення, висвітлює всі отримані результати, висновки та запропоновані рекомендації.

Зауваження по роботі:

1. У другому розділі автор пояснює термінологію стійкості рекомендаційних систем а також перелічує способи її оцінювання. На мій погляд це загально відома інформація, яку можна було би довести у додатку.
2. У третьому розділі, підрозділ 3.2.1, автор пропонує використовувати показники: Precision, Recall, RMSE, покриття каталогу та покриття простору користувачів, як основні показники якості роботи рекомендаційних систем. Нажаль аргументації цього висновку у розділі не наведено.
3. У четвертому розділі автор пропонує метод програмного імітаційного моделювання поведінки звичайних користувачів та ботів у рекомендаційній системі на основі теорії складних мереж. Нажаль складових метода у дисертаційній роботі не наведено.
4. Також, у четвертому розділі на рис. 4.9-4.11 наведено графіки зміни випадкових характеристик частоти правильного прогнозування вподобань, частоти повного прогнозування вподобань та RMSE розпізнавання вподобань відповідно. Також на цих рисунках наведено допустимі межі коливання цих випадкових величин, що отримані в результаті проведеного моделювання.

Нажаль даних про методику визначення межі коливання досліджуваних випадкових величин автором не наведено.

5. На рис. 4.12. автором наведено діаграму частоти інтервалів стійкості вподобань від їх довжини та проведено ряд експериментальних досліджень цієї залежності. На мій погляд у цьому експерименті мають місце деякі неточності. Наприклад, при визначенні коефіцієнту, ще показує межу чутливості d автор неаргументовано пропонує величину, рівну 0.01, яка у подальшому суттєво впливає на результат. При апроксимації досліджуваних процесів експоненційним розподілом автор нехтує загально відомими методиками математичної формалізації та апроксимації. Крім того, на мій погляд, автор пропонує не дуже вдалий термін «частота інтервалів стійкості вподобань».

6. У п'ятому розділі автором розроблено спосіб визначення оптимальної частоти перевірки рекомендаційної системи на наявність інформаційної атаки та профілів ботів. При цьому як критерій оптимізації автор пропонує мінімум загальних збитків системи. На мій погляд у цьому випадку існує протиріччя між загальною науковою проблемою дослідження – підвищенням точності пропозицій рекомендаційних систем, та локальним завданням, що автор пропонує вирішити розробленим способом. Було би краще при розробці цього способу визначити обмеження, що акцентують увагу на покращенні показників точності.

7. В тексті дисертації та авторефераті присутні помилки та неточності. Зокрема, в авторефераті в розділі «Зв'язок роботи з науковими програмами, планами, темами» на стор.2 присутній текст «відповідно до рішення Ради президентів академій наук України» замість «…постанови Президії НАН України» при посиланні на документ «Про Основні наукові напрями та найважливіші проблеми фундаментальних досліджень …».

Відзначені зауваження не ставлять під сумнів основні наукові та практичні результати, і суттєво не впливають на загальну позитивну оцінку дисертаційної роботи.

Висновок.

Дисертаційна робота Мелешко Єлизавети Владиславівни представляє собою завершене актуальне наукове дослідження. В роботі отримано нові науково- обґрунтовані результати, які дозволяють розвинути методи та моделі забезпечення стійкості рекомендаційних систем до дестабілізуючих факторів у комп'ютерних мережах.

Вважаю, що докторська дисертація Мелешко Єлизавети Владиславівни за актуальністю теми, ступенем обґрунтованості наукових положень, рівнем апробації та публікацій, науковою новизною та практичною цінністю отриманих результатів відповідає вимогам, що висуваються до докторських дисертацій згідно п. 9, 10, 12 «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567, а сам автор заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент,

Заступник директора з наукової роботи
Інституту проблем моделювання в енергетиці
імені Г. Є. Пухова НАН України
доктор технічних наук,
старший науковий співробітник Олександр ЧЕМЕРИС