DOI: 10.20998/2079-0023.2025.02.20
УДК 004.8:004.9

О. В. ЧАЛА, доктор технічних наук, доцент, Харківський національний університет радіоелектроніки, завідувачка кафедри радіотехнічних та інформаційно-комунікаційних систем, м. Харків, Україна; e-mail: oksana.chala@nure.ua, ORCID: https://orcid.org/0000-0002-9982-9091
О. М. БІТЧЕНКО, кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри радіотехнічних та інформаційно-комунікаційних систем, м. Харків, Україна; e-mail: oleksandr.bitchenko@nure.ua, ORCID: https://orcid.org/0000-0002-4561-1046
Л. Ф. САЙКІВСЬКА, кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри радіотехнічних та інформаційно-комунікаційних систем, м. Харків, Україна; e-mail: liliia.saikivska@nure.ua, ORCID: https://orcid.org/0000-0002-4139-7732
А. Ю. КАЛЬНИЦЬКА, Харківський національний університет радіоелектроніки, асистент кафедри інформаційних управляючих систем, м. Харків, Україна; e-mail: angelika.kalnitskaya@nure.ua, ORCID: https://orcid.org/0000-0002-5613-4150

МЕТОД ВИЯВЛЕННЯ КОРОТКОЧАСНИХ ШИЛІНГ-АТАК У СИСТЕМАХ ЕЛЕКТРОННОЇ КОМЕРЦІЇ НА ОСНОВІ АДАПТИВНОЇ ДЕТАЛІЗАЦІЇ ЯВНИХ ТА НЕЯВНИХ ВІДГУКІВ КОРИСТУВАЧІВ

Предметом дослідження є процес виявлення короткочасних шилінг-атак у системах електронної комерції на основі аналізу темпоральних залежностей між явними та неявними відгуками користувачів. Мета роботи полягає у розробці підходу до виявлення шилінг-атак з використанням темпоральних правил та адаптивної деталізації як продажів, так і рейтингів у системі електронної комерції. Задачі дослідження включають: розробку підходу до виявлення короткочасних шилінг-атак на основі адаптивного порівняння темпоральних правил для продажів і рейтингів; розробку методу виявлення короткочасних шилінг-атак на основі адаптивної деталізації явних та неявних відгуків користувачів. Явні відгуки користувачів представлені рейтингами, а неявні відгуки фіксуються через продажі товарів. Розроблений метод включає такі етапи: попередню агрегацію даних щодо продажів; аналіз варіабельності продажів і рейтингів через відношення стандартного відхилення до середнього значення; виявлення інтервалів з потенційною можливістю атаки; формування набору фактів з різним рівнем деталізації; побудову темпоральних правил двох типів для продажів та рейтингів; виявлення інтервалів шилінг-атак на основі порівняння знаків ваг правил для продажів і рейтингів; виявлення користувачів-авторів атак на основі аналізу активності користувачів за виявленими інтервалами шилінг-атак. Метод забезпечує автоматизований вибір деталізації часу для визначення фактів продажів та формування рейтингів і, на цій основі, підвищення точності виявлення короткочасних атак порівняно з фіксованою деталізацією, а також можливість виявлення атак у режимі near-online. Практична значущість отриманих результатів полягає у можливості виявлення короткочасних спотворень рейтингів у системах електронної комерції, соціальних мережах і рекомендаційних системах для підвищення довіри користувачів до рекомендованих товарів та послуг.

Ключові слова: шилінг-атаки, системи електронної комерції, темпоральні правила, адаптивна деталізація, варіабельність продажів, виявлення атак, рекомендаційні системи, викиди.

Вступ. Шилінг-атаки використовують спотворені рейтинги продукції від підроблених профілів користувачів систем електронної комерції для зловмисного підвищення або зниження популярності цільових товарів. Рейтинги продукції від користувачів використовуються для побудови рекомендацій. Спотворення рекомендацій внаслідок шилінг-атак приводить до відмови користувачів до запропонованих товарів. Тому виявлення шилінг-атак є актуальною задачею, вирішення якої забезпечує підвищення довіри користувачів до рекомендованих товарів та послуг [1], [2].

Шилінг-атаки часто мають неритмічний характер, коли атакуючі профілі користувачів системи електронної комерції здійснюють координовані дії протягом короткого інтервалу часу, наприклад декількох годин. Після атаки профілі користувачів зазвичай видаляються. Така тактика мінімізує ризик виявлення традиційними методами, оскільки нові профілі не встигають виконати суттєву кількість транзакцій для подальшої класифікації атаки [3]. Якщо при виявленні шилінг-атак використовується фіксована деталізація продажів та рейтингів на основі фіксованих довгих інтервалів часу, то короткотривалі викиди внаслідок дій атакуючих можуть бути замасковані у масиві звичайних операцій у системі електронної комерції, що приводить до зниження точності виявлення атак. З іншого боку, при використанні постійних коротких інтервалів часу для виявлення атак суттєво збільшуються обчислювальні витрати. Таким чином, актуальною є проблема виявлення шилінг-атак з використанням адаптивної деталізації продажів та рейтингів у системі електронної комерції.

Аналіз останніх досліджень і публікацій.

Сучасні методи виявлення шилінг-атак класифікуються за типом навчання та особливостями використання параметру часу. Методи навчання з учителем використовують розмічені набори даних для виявлення сигнатур атакуючих профілів [4], [5]. Однак даний підхід потребує використання збалансованих навчальних вибірок. Перевагою методів навчання без вчителя є досягнення достатньо високої точності виявлення атак. Однак чутливість такого підходу є низькою внаслідок узагальнення короткочасних змін у поведінці користувачів [6], [7]. Використання графів для виявлення групових шилінг-атак у соціальних рекомендаційних системах запропоновано в [8]. Однак запропонований метод має високу обчислювальну складність, що обме-

жує використання графів для виявлення атак. У роботах [9], [10] запропоновано методи виявлення шилінг-атак на основі використання зважених темпоральних правил та аналізу часових рядів із рейтингів товарів та послуг. Однак ці методи використовують фіксовані інтервали часу і тому не орієнтовані на виявлення короткочасних шилінг-атак. Прогнозний та реконструктивний підходи дають можливість виявити концептульний дрейф в рекомендаційних системах, що створює умови для виявлення шилінг-атак, однак потребують попередніх даних за великий період часу, що обмежує швидке виявлення атак [11]. У [12] запропоновано виявлення атак з використанням динамічних інтервалів, проте метод потребує апріорного знання про типову тривалість атак.

Таким чином, існуючі методи виявлення шилінг-атак орієнтовані переважно на фіксовану деталізацію даних систем електронної комерції, що суттєво утруднює виявлення швидких атак і свідчить про важливість використання адаптивної деталізації часу для вирішення цієї задачі.

Мета та задачі дослідження.

Метою роботи є розробка підходу до виявлення шилінг-атак з використанням темпоральних правил та адаптивної деталізації як продажів, так і рейтингів в системі електронної комерції.

Вирішення цієї задачі створює умови для підвищення точності виявлення короткочасних шилінг-атак.

Для досягнення даної мети вирішуються такі задачі дослідження: розробка підходу до виявлення короткочасних шилінг-атак на основі адаптивного порівняння темпоральних правил; розробка методу виявлення короткочасних шилінг-атак в системах електронної комерції на основі адаптивної деталізації явних та неявних відгуків користувачів.

Підхід до виявлення короткочасних шилінг-атак на основі адаптивного порівняння темпоральних правил.

Розроблений підхід до виявлення шилінг-атак на основі порівняння темпоральних правил використовує різницю у зміні вподобань користувачів за основі порівняння як явних відгуків, так і неявних відкликів від користувачів. Явні відгуки задаються через виставлення рейтингів. Неявні відклики задаються через продажі товарів в системі електронної комерції. Останні потребують фінансових витрат і тому краще відображають справжні наміри користувачів. Розроблений підхід використовує темпоральні правила для фактів продажів та виставлення рейтингів. Ці факти формуються на визначених інтервалах часу, які, в залежності від цільової деталізації, можуть становити годину, день, тиждень, місяць, рік. Кожен факт продажів відображає сумарний продаж цільового товару (нормовану кількість або суму продажів) на визначеному інтервалі часу. Кожен факт виставлення рейтингів відображає середній нормований рейтинг цільового товару на аналогічному інтервалі часу.

Для кожної пари інтервалів часу визначаються темпоральні правила типів *Next* та *Future*. Перше правило встановлює порядок в часі для двох послідовних інтервалів, а друге – для двох довільних інтервалів, між якими є інші інтервали. Для правил розраховуються ваги, як визначають зміни в продажах товарів або зміни в рейтингах для пари інтервалів, на яких визначено темпоральне правило. Тобто ваги відображають зміни інтересу користувачів у аспекті продажів та рейтингів: позитивні ваги свідчать про збільшення продажів/підвищення рейтингів, а негативні – про зменшення продажів/зниження рейтингів. Тому невідповідність знаків ваг для темпоральних правил продажів і правил, що сформовані для однієї й тієї ж пари інтервалів, є ознакою можливої шилінг-атаки. Однак фіксовані тривалі інтервали можуть усереднити короткі атаки, наприклад в межах 2-4 годин.

Для того, щоб оцінити такий локальний викид внаслідок атаки, в рамках розробленого підходу використовується показник варіабельності продажів, який визначається як відношення стандартного відхилення до середнього значення покупок/рейтингів на визначеному інтервалі.

Такий показник розраховується для підінтервалів основного інтервалу часу. Підінтервали виділяються за наступною меншою одиницею вимірювання часу. Тобто якщо стандартний цільовий інтервал становить одну добу, то тоді підінтервал становитиме одну годину. Відповідно, перевищення показником варіабельності продажів порогового значення свідчить про наявність викидів у продажах, що потребує виділення підінтервалів часу та розрахунку темпоральних правил на цих підінтервалах.

Загальна послідовність кроків запропонованого підходу включає, по перше, розрахунок фактів продажів та рейтингів на апріорно визначених стандартних інтервалах часу. По-друге, для кожного інтервалу визначаються субінтервали і розраховується показник варіабельності продажів/рейтингів. По-третє, формується набір інтервалів часу для побудови темпоральних правил в залежності від значень показника варіабельності. У випадку, якщо показник варіабельності перевищує порогове значення, то використовуються підінтервали. В іншому випадку – базові інтервали часу. Учетверте, формуються зважені темпоральні правила та визначаються можливі інтервали шилінг-атак й потенційні користувачі – автори атак.

Метод виявлення короткочасних шилінг-атак в системах електронної комерції на основі адаптивної деталізації явних та неявних відгуків користувачів.

Розроблений метод використовує аналіз варіабельності продажів та рейтингів й подальший розрахунок необхідного рівня деталізації часу для виявлення короткочасних шилінг-атак.

Метод використовує вхідні дані щодо продажів в системі електронної комерції: журнал системи L, який включає множину записів про продажі; кожен запис містить мітки часу, що дає можливість відбирати дані для заданих темпоральних інтервалів; журнал рейтингів Q, що включає виставлені користувачами системи рейтинги продукції; цільовий об'єкт z (наприклад, певний товар або послуга), для якого виконується аналіз щодо шилінг-атак; набір $U = \{u_j\}$ користувачів

системи електронної комерції; даний набір містить дані потенційних атакуючих; початковий (типовий для системи електронної комерції, наприклад, день або тиждень) рівень деталізації часу t_{init}; мінімальний рівень деталізації часу $t_{\min}$ для аналізу атак (наприклад, година); період аналізу шилінг-атак T.

Розроблений метод виявлення короткочасних шилінг-атак включає наступні етапи.

Етап 1. Попередня агрегація даних щодо продажів в межах початкового рівня деталізації часу t_{init}.

При виконанні даного етапу формуються факти продажів та надання рейтингів товарам з рівнем деталізації t_{init}.

Для кожного i – інтервалу t_i обчислюються агреговані факти продажів s_i^z як сума кількості покупок z – товару та рейтингів r_i^z як усереднений рейтинг на інтервалі.

Результатом етапу 1 є набори фактів продажів $\left\{s_1^z, s_2^z, ..., s_i^z, ..., s_I^z\right\}$ та рейтингів $\left\{r_1^z, r_2^z, ..., r_i^z, ..., r_I^z\right\}$ для періоду аналізу T.

Етап 2. Аналіз варіабельності продажів в рамках t_i – інтервалів.

Для кожного інтервалу t_i виконується розбиття на k підінтервалів $t_{i,k}$ тривалістю $t_i = \frac{t_{\text{init}}}{k}$. Наприклад, якщо виконується розбиття на годинні підінтервали в рамках добового інтервалу, то $k = 24$. Для кожного підінтервалу $t_{i,k}$ обчислюються та нормалізуються факти продажів $s_{i,k}^z$ та рейтингів $r_{i,k}^z$.

Для отриманих інтервалів $t_{i,k}$ та фактів $s_{i,k}^z$ і $r_{i,k}^z$ обчислюється варіабельність продажів через стандартне відхилення $\sigma\left(s_{i,k}^z\right)$ та середнє значення $\mu\left(s_{i,k}^z\right)$:

$$V_i^{\text{Sales}} = \frac{\sigma\left(s_{i,k}^z\right)}{\mu\left(s_{i,k}^z\right) + \varepsilon}. \quad (1)$$

Варіабельність рейтингів обчислюється аналогічно. Для уникнення ділення на нуль використовується константа ε:

$$V_i^{\text{Ratings}} = \frac{\sigma\left(r_{i,k}^z\right)}{\mu\left(r_{i,k}^z\right) + \varepsilon}. \quad (2)$$

На практиці константа ε може приймати значення 0,001–0,01.

Великі значення V_i^{Sales} або V_i^{Ratings} відображають короткочасні сплески активності користувачів в рамках інтервалу t_i.

Етап 3. Виявлення інтервалів з потенційною можливістю атаки $t_i \in \text{T}^{\text{Attack}}$ для подальшого аналізу зі збільшеною деталізацією часу.

Умовою потенційної можливості атаки на інтервалі t_i є перевищення V_i^{Sales} та V_i^{Ratings} порогового значення варіабельності θ:

$$t_i \in \text{T}^{\text{Attack}} \left| \left(V_i^{\text{Sales}} > \theta\right) \wedge \left(V_i^{\text{Ratings}} > \theta\right). \right. \quad (3)$$

На практиці порогове значення може бути вибрано в інтервалі від 0,8 до 1,2.

Для інтервалів з потенційною можливістю атак вибираються інтервали $t_{i,k}$, для всіх інших залишається вибір інтервалів t_i. Такий вибір дає можливість обмежити обчислювальну складність та забезпечити чутливість до короткочасних шилінг-атак.

Етап 4. Формування набору фактів з різним рівнем деталізації інтервалів часу.

На даному етапі формується повний набір фактів продажів та рейтингів з урахування різного рівня деталізації часу.

Для інтервалів, для яких виконується умова (3), використовуються факти $s_{i,k}^z$ та $r_{i,k}^z$. Для всіх інших інтервалів використовуються факти продажів s_i^z та рейтингів r_i^z.

Результуючий набір фактів продажу має вигляд:

$$S^{\text{Adapt}} = \left\{\left\{s_{i,k}^z \left| t_i \in \text{T}^{\text{Attack}}\right.\right\}, \left\{s_i^z \left| t_i \notin \text{T}^{\text{Attack}}\right.\right\}\right\}. \quad (4)$$

Аналогічно, адаптивний набір фактів виставлення рейтингів має вигляд:

$$R^{\text{Adapt}} = \left\{\left\{r_{i,k}^z \left| t_i \in \text{T}^{\text{Attack}}\right.\right\}, \left\{r_i^z \left| t_i \notin \text{T}^{\text{Attack}}\right.\right\}\right\}. \quad (5)$$

Етап 5. Побудова темпоральних правил з урахуванням змінної деталізації інтервалів часу.

Темпоральні правила типів *Next* та *Future* формуються для послідовних інтервалів часу та інтервалів, між якими є інші інтервали за запропонованим в роботі [9] методом. Тобто темпоральні правила відображають збільшення/зменшення продажів та рейтингів між інтервалами часу: для пар послідовних інтервалів у випадку правила *Next* та для пар інтервалів, між якими я інші інтервали у випадку правила *Future*.

Ваги цих правил обчислюються як нормовані різниці у продажах/рейтингах між інтервалами часу, які тепер мають змінну деталізацію і тому враховують короткочасні сплески продажів/рейтингів. Відповідно, для темпоральних правил, що були сформовані для кожної із множин S^{Adapt} та R^{Adapt} обчислюються послідовності ваг W_S^{Adapt} та W_R^{Adapt}. Ваги правил відображають збільшення (позитивні ваги $w_i^{S+}, w_{i,k}^{S+} \in W_S^{\text{Adapt}}$; $w_i^{R+}, w_{i,k}^{R+} \in W_R^{\text{Adapt}}$) або зменшення (негативні ваги $w_i^{S-}, w_{i,k}^{S-} \in W_S^{\text{Adapt}}$; $w_i^{R-}, w_{i,k}^{R-} \in W_R^{\text{Adapt}}$) продажів та рейтингів відповідно.

Етап 6. Виявлення інтервалів шилінг-атак

На даному етапі порівнюються ваги темпоральних правил для рейтингів та для продажів з відповідних інтервалів t_i або $t_{i,k}$. У випадку неспівпадіння знаків ваг

інтервал t_i або $t_{i,k}$ маркується як інтервал ймовірної шилінг-атаки.

Етап 7. Виявлення користувачів-авторів атак.

На даному етапі на основі даних із журнала подій за часовими мітками встановлюється, хто із авторів виставляв рейтинги на інтервалах шилінг-атак. Результатом етапу є перелік потенційних атакуючих.

Розроблений метод дає можливість виявити короткочасні шилінг – атаки без апріорного визначення рівня деталізації часу, оскільки адаптація виконується на основі аналізу варіабельності в рамках кожного інтервалу t_i. Обчислювальна складність методу залежить від кількості інтервалів I та кількості підінтервалів k і становить $O(I \cdot k)$, що забезпечує можливість виявлення атак у режимі онлайн.

Експериментальна перевірка розробленого методу.

Експериментальна перевірка методу виконана на реальних даних MovieLens 100 K, що містить рейтинги фільмів, з емуляцією шилінг-атак.

Порівняння виконано з методом виявлення шилінг-атак [9] із фіксованим рівнем деталізації 24 години. Запропонований метод використовує початковий рівень деталізації 24 години, мінімальний рівень деталізації 1 година. Пороговий коефіцієнт варіабельності становить 1,0. Метрики якості включають Precision (точність), Recall (чутливість) та F1-score для виявлення інтервалів атак.

Результати експериментальної перевірки методу наведено в табл. 1 та табл. 2.

Таблиця 1 – Виявленням атак на основі темпоральних правил для незмінних та адаптивних інтервалів

Метрика	Незмінні інтервали	Адаптивні інтервали	Різниця
F1-score	0,79	0,87	+8 %
Recall	0,78	0,89	+11 %
Precision	0,85	0,84	–1 %

Таблиця 2 – Виявлення атак з урахуванням її тривалості

Тривалість атаки	Точність: незмінні інтервали	Точність: адаптивні інтервали	Різниця
2 години	0,63	0,84	+21 %
4 години	0,72	0,84	+12 %

Експериментальні дані показують збільшення метрики F1-score детектування для раптових атак для розробленого методу у порівнянні з використанням фіксованих інтервалів, що свідчить врахування короткочасних сплесків активності користувачів. Precision знижується на 1 %. Таке зниження може бути наслідком виявлення змін у активності легітимних користувачів на інтервалах пікового навантаження системи. Порівняння точності виявлення коротких атак – 2 та 4 години показало переваги адаптації інтервалів при зменшенні кількості годин атаки.

Аналіз обчислювальної складності методу показав, що середній час обробки одного добового інтервалу для запропонованого методу становить 1,8 секунди та 0,9 секунди для базового методу з фіксованими інтервалами. Реалізація виконана на Python 3.9 на комп'ютері з процесором Intel Core i7-9700K. Збільшення часу обробки є наслідком аналізу підінтервалів. Час оброки свідчить про можливість роботи в near-online режимі у системах електронної комерції.

Висновки.

Розроблено підхід до виявлення шилінг-атак на основі адаптивного порівняння темпоральних правил. Адаптація в рамках підходу виконується на основі показника варіабельності продажів/рейтингів, який розраховується через відношення стандартного відхилення до середнього значення покупок/рейтингів.

Запропоновано метод виявлення короткочасних шилінг-атак в системах електронної комерції на основі адаптивної деталізації явних та неявних відкликів користувачів. Метод містить етапи адаптивного формування фактів продажів/рейтингів в залежності від значення показника варіабельності, формування потенційних інтервалів шилінг-атак та виявлення потенційних атакуючих користувачів. Метод дає можливість виявити короткочасне спотворення рейтингів/продажів в системах електронної комерції в режимі near-online.

Список використаної літератури

1. Zhou W., Wen J., Qu Q., Zeng J., Cheng T. Shilling attack detection for recommender systems based on credibility of group users and rating time series. *PLOS ONE*. 2018. Vol. 13, no. 5. Art. e0196533. DOI: doi.org/10.1371/journal.pone.0196533.
2. Cai H., Huang J., Liu B. Detecting shilling attacks in recommender systems based on analysis of user rating behavior. *Knowledge-Based Systems.* 2019. Vol. 177. P. 22–43. DOI: doi.org/10.1016/j.knosys.2019.03.041.
3. Pote M., Elmas T., Flammini A., Menczer F. Coordinated reply attacks in influence operations: characterization and detection. *Proc. of the Int. Conf. on Web and Social Media (ICWSM).* 2025. arXiv:2410.19272. DOI: doi.org/10.1609/icwsm.v19i1.35889.
4. Zhou W., Wen J., Xiong Q., Gao M., Zeng J. SVM-TIA: a shilling attack detection method based on SVM and target item analysis in recommender systems. *Neurocomputing.* 2016. Vol. 210. P. 197–205. DOI: doi.org/10.1016/j.neucom.2016.01.197.
5. Shao C., Sun Y. Z. Shilling attack detection for collaborative recommender systems: a gradient boosting method. *Mathematical Biosciences and Engineering.* 2022. Vol. 19, no. 7. P. 7248–7271. DOI: doi.org/10.3934/mbe.2022342.
6. Hao Y., Zhang F. An unsupervised detection method for shilling attacks based on deep learning and community detection. *Soft Computing.* 2020. Vol. 24. P. 18677–18688. DOI: doi.org/10.1007/s00500-020-05162-6.
7. Zhang F., Zhou Q. Unsupervised approach for detecting shilling attacks in collaborative filtering recommender systems. *IET Information Security.* 2019. Vol. 13, no. 6. P. 625–634. DOI: doi.org/10.1049/iet-ifs.2018.5131.
8. Gunes I., Kaleli C., Bilge A., Polat H. Shilling attacks against recommender systems: a comprehensive survey. *Artificial Intelligence Review.* 2014. Vol. 42, no. 4. P. 767–799. DOI: doi.org/10.1007/s10462-012-9364-9.
9. Chala O., Novikova L., Chernyshova L. Method for detecting shilling attacks in e-commerce systems using weighted temporal rules. *EUREKA: Physics and Engineering.* 2019. Vol. 5. P. 29–36. DOI: doi.org/10.21303/2461-4262.2019.00983.
10. Xu Y., Zhang F. Detecting shilling attacks in social recommender systems based on time series analysis and trust features. *Knowledge-Based Systems.* 2019. Vol. 178. P. 25–47. DOI: doi.org/10.1016/j.knosys.2019.04.035.

11. Yuan W., Guan D., Lee Y. K., Lee S. Detection of shilling attacks based on T-distribution on the dynamic time intervals. *IEEE Access.* 2019. Vol. 7. P. 121308–121319. DOI: doi.org/10.1109/ACCESS.2019.2937164.
12. Yang Z., Xu L., Cai Z. Re-scale AdaBoost for attack detection in collaborative filtering recommender systems. arXiv:1506.04584 [cs.IR]. 2015. DOI: doi.org/10.48550/arXiv.1506.04584.

References (transliterated)

1. Zhou W., Wen J., Qu Q., Zeng J., Cheng T. Shilling attack detection for recommender systems based on credibility of group users and rating time series. *PLOS ONE.* 2018, vol. 13, no. 5, article e0196533. DOI: doi.org/10.1371/journal.pone.0196533.
   Cai H., Huang J., Liu B. Detecting shilling attacks in recommender systems based on analysis of user rating behavior. *Knowledge-Based Systems.* 2019, vol. 177, pp. 22–43. DOI: doi.org/10.1016/j.knosys.2019.03.041.
3. Pote M., Elmas T., Flammini A., Menczer F. Coordinated reply attacks in influence operations: characterization and detection. *Proc. of the Int. Conf. on Web and Social Media (ICWSM).* 2025. arXiv:2410.19272. DOI: doi.org/10.1609/icwsm.v19i1.35889.
4. Zhou W., Wen J., Xiong Q., Gao M., Zeng J. SVM-TIA: a shilling attack detection method based on SVM and target item analysis in recommender systems. *Neurocomputing*. 2016, vol. 210, pp. 197–205. DOI: doi.org/10.1016/j.neucom.2016.01.197.
5. Shao C., Sun Y. Z. Shilling attack detection for collaborative recommender systems: a gradient boosting method. *Mathematical Biosciences and Engineering.* 2022, vol. 19, no. 7, pp. 7248–7271. DOI: doi.org/10.3934/mbe.2022342.
6. Hao Y., Zhang F. An unsupervised detection method for shilling attacks based on deep learning and community detection. *Soft Computing.* 2020, vol. 24, pp. 18677–18688. DOI: doi.org/10.1007/s00500-020-05162-6.
7. Zhang F., Zhou Q. Unsupervised approach for detecting shilling attacks in collaborative filtering recommender systems. *IET Information Security.* 2019, vol. 13, no. 6, pp. 625–634. DOI: doi.org/10.1049/iet-ifs.2018.5131.
8. Gunes I., Kaleli C., Bilge A., Polat H. Shilling attacks against recommender systems: a comprehensive survey. *Artificial Intelligence Review.* 2014, vol. 42, no. 4, pp. 767–799. DOI: doi.org/10.1007/s10462-012-9364-9.
9. Chala O., Novikova L., Chernyshova L. Method for detecting shilling attacks in e-commerce systems using weighted temporal rules. *EUREKA: Physics and Engineering.* 2019, vol. 5, pp. 29–36. DOI: doi.org/10.21303/2461-4262.2019.00983.
10. Xu Y., Zhang F. Detecting shilling attacks in social recommender systems based on time series analysis and trust features. *Knowledge-Based Systems.* 2019, vol. 178, pp. 25–47. DOI: doi.org/10.1016/j.knosys.2019.04.035.
11. Yuan W., Guan D., Lee Y. K., Lee S. Detection of shilling attacks based on T-distribution on the dynamic time intervals. *IEEE Access.* 2019, vol. 7, pp. 121308–121319. DOI: doi.org/10.1109/ACCESS.2019.2937164.
12. Yang Z., Xu L., Cai Z. Re-scale AdaBoost for attack detection in collaborative filtering recommender systems. arXiv:1506.04584 [cs.IR]. 2015. DOI: doi.org/10.48550/arXiv.1506.04584.

Надійшла (received) 14.11.2025

UDC004.8:004.9

O. V. CHALA, Doctor of Technical Sciences, Associate Professor, Head of the Department of Radio Engineering and Information-Communication Systems, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine; e-mail: oksana.chala@nure.ua, ORCID: https://orcid.org/0000-0002-9982-9091
O. M. BITCHENKO, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Radio Engineering and Information-Communication Systems, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine; e-mail: oleksandr.bitchenko@nure.ua, ORCID: https://orcid.org/0000-0002-4561-1046
L. F. SAIKIVSKA, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Radio Engineering and Information-Communication Systems, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine; e-mail: liliia.saikivska@nure.ua, ORCID: https://orcid.org/0000-0002-4139-7732
A. Y. KALNITSKA, Assistant of the Department of Information Control Systems, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine; e-mail: angelika.kalnitskaya@nure.ua, ORCID: https://orcid.org/0000-0002-5613-4150

DETECTION METHOD FOR SHORT-TERM SHILLING ATTACKS IN E-COMMERCE SYSTEMS USING ADAPTIVE GRANULARITY OF USER FEEDBACK

The subject of research is the process of detecting short-term shilling attacks in e-commerce systems based on analysis of temporal dependencies between explicit and implicit user feedback. The aim of the work is to develop an approach to detecting shilling attacks using temporal rules and adaptive granularity of both sales and ratings in e-commerce systems. Research tasks include: development of an approach to detecting short-term shilling attacks based on adaptive comparison of temporal rules for sales and ratings; development of a method for detecting short-term shilling attacks based on adaptive granularity of explicit and implicit user feedback. Explicit user feedback is represented by ratings, while implicit feedback is captured through product sales. The developed method includes the following stages: preliminary aggregation of sales data; analysis of sales and ratings variability through the ratio of standard deviation to mean value; identification of intervals with potential attack possibility; formation of a fact set with different granularity levels; construction of temporal rules of two types for sales and ratings; detection of shilling attack intervals based on comparison of rule weight signs for sales and ratings; identification of attacking users based on analysis of user activity across detected shilling attack intervals. The method provides automated selection of time granularity for determining sales facts and forming ratings and thereby improves the accuracy of detecting short-term attacks compared to fixed granularity, as well as enables attack detection in near-online mode. The practical significance of the obtained results lies in the possibility of detecting short-term rating distortions in e-commerce systems, social networks, and recommender systems to increase user trust in recommended products and services.

Keywords: shilling attacks, e-commerce systems, temporal rules, adaptive granularity, sales variability, attack detection, recommender systems, outliers.

Повні імена авторів / Author's full names

Автор 1 / Author 1: Чала Оксана Вікторівна / Chala Oksana Viktorivna
Автор 2 / Author 2: Бітченко Олександр Миколайович / Bitchenko Oleksandr Mykolaiovych
Автор 3 / Author 3: Сайківська Лілія Федорівна / Saikivska Liliia Fedorivna
Автор 4 / Author 4: Кальницька Анжеліка Юріївна / Kalnitska Anzhelika Yuriivna