Original Research Article: full paper

(2019), «EUREKA: Physics and Engineering»
Number 5

METHOD FOR DETECTING SHILLING ATTACKS IN E-COMMERCE SYSTEMS USING WEIGHTED TEMPORAL RULES

Oksana Chala[1]
Department of Information Control Systems
Kharkiv National University of Radio Electronics
14 Nauka ave., Kharkiv, Ukraine, 61166
oksana.chala@nure.ua

Lyudmyla Novikova[1]
l.novikova@karazin.ua

Larysa Chernyshova[1]
Department of International Economics
Kharkiv State University of Food Technology and Trade
333 Klochkivska str., Kharkiv, Ukraine, 61051

[1]*Department of International Relations, International Information and Security*
V. N. Karazin Kharkiv National University
6 Svobody sq., Kharkiv, Ukraine, 61022
lach.2803@gmail.com

Abstract

The problem of shilling attacks detecting in e-commerce systems is considered. The purpose of such attacks is to artificially change the rating of individual goods or services by users in order to increase their sales. A method for detecting shilling attacks based on a comparison of weighted temporal rules for the processes of selecting objects with explicit and implicit feedback from users is proposed. Implicit dependencies are specified through the purchase of goods and services. Explicit feedback is formed through the ratings of these products. The temporal rules are used to describe hidden relationships between the choices of user groups at two consecutive time intervals. The method includes the construction of temporal rules for explicit and implicit feedback, their comparison, as well as the formation of an ordered subset of temporal rules that capture potential shilling attacks. The method imposes restrictions on the input data on sales and ratings, which must be ordered by time or have timestamps. This method can be used in combination with other approaches to detecting shilling attacks. Integration of approaches allows to refine and supplement the existing attack patterns, taking into account the latest changes in user priorities.

Keywords: e-commerce, recommendation system, temporal rules, shilling attack, feedback.

DOI: 10.21303/2461-4262.2019.00983

1. Introduction

E-commerce systems provide the sale of goods and services online on the Internet. Such systems offer a wider selection of objects than in ordinary stores, and also reduce the cost of users to select and purchase goods of interest to them. In particular, e-commerce systems are widely used in the activities of such large companies as Netflix, Amazon, and Google.

In order to simplify and support the choice of users, recommendation subsystems are used in e-commerce systems. The latter form the recommended list of objects for the current user of the e-commerce system based on the prediction of his interests, as well as taking into account the popularity of the offered goods and services. When formed recommendations use data of the selection of similar users, as well as information of the similarity of product characteristics [1].

In general, e-commerce systems have reactive behavior, as they formulate their proposals depending on the user's reaction. This feature leads to the problem of shilling attacks in such systems [2]. A shilling attack means that an attacker or a group of attackers artificially change the ratings of target goods or services. To do this, fake user profiles created automatically. Fake users further modify the ratings of specific products in order to increase (or decrease) their sales. Thus,

the goal of a shilling attack is to influence the formation of a personal list of goods and services offered to a user. Such a modified list does not meet in the user's interest [3].

Existing approaches to detecting shilling attacks are based on finding a pattern of behavior of attacking users [4]. Such patterns are formed on the basis of an analysis of the data array on the ratings assigned. [5]. To construction attack patterns, statistical methods are used, as well as Supervised learning, Unsupervised learning, and a Semi-supervised learning [6]. Supervised learning methods allow to detect known attacks, but they are not suitable for combined attacks [7]. To increase the efficiency of detecting attacks of various types, a convolutional neural network with deep learning is proposed in [8]. However, learning such a network requires significant computational costs, which makes it difficult to use it when dynamically changing user interests. Unsupervised learning methods [9] allow clustering attack patterns in the case of typical behavior of ordinary users. However, they do not distinguish between attackers and users with periodically changing interests, who occasionally purchase goods and services in e-commerce systems. In order to take into account the changing interests of users, a subset of the initial ratings is allocated for a given time interval [10].

The considered methods use rating information and do not use data on purchases of goods and services, corresponding to explicit feedback from users of the e-commerce system. Such data objectively reflects the interests of the user and is relevant, since it is entered into the database only after payment for a product or service.

In general, the considered approaches do not take into account two significant factors that allow to quickly detect shilling attacks in the e-commerce system. Firstly, the comparison of the results of the explicit and implicit (rating) communications from the user is not performed in order to identify the discrepancy between them. Such discrepancy indicates a potential shilling attack. Secondly, the temporal aspect of the user selection process is not taken into account. Such a process consists of a sequence of decision-making on the purchase or assignment of a rating of goods. The hidden relationships between these solutions are described by a set of temporal dependencies [11]. The latter reflect typical user behavior patterns. In [12], it is proposed to apply temporal dependencies in the form of a multilayer graph when constructing recommendations online. According to [13], temporal restrictions can be used to solve the problem of cold start in a recommendation system. However, temporal rules were not used to solve the problem of detecting external influences on the e-commerce system.

Thus, the ability to use temporal rules to identify attacks on the ratings of goods and services can be implemented based on the search for discrepancies for selection processes with explicit and implicit feedback.

The aim of this research is development of a method for detecting shilling attacks in e-commerce systems based on a comparison of temporal dependencies that describe the change in user interests for the processes of purchasing goods and forming their ratings.

2. Method for detecting shilling attacks using temporal rules to describe the user's selection sequence

The developed method implements a three-stage scheme for detecting shilling attacks based on a comparison of temporal rules. These rules describe implicit time dependencies between the user's choices in the specified processes [14]. At the first two stages, a set of modified rules is constructed. Such rules describe the processes of buying and rating. At the third stage, rules differing for these two processes are revealed. A discrepancy between concurrently executed rules indicates a potential shilling attack.

The method uses a modified type of rules $r_{m,s}$ with a temporal operator X (Next) and a quantifier E (Exist). The operator X links the facts F_m and F_s purchases (rating settings) of the object i_j for a pair of consecutive time intervals $\Delta\tau_m$ and $\Delta\tau_s$. The quantifier E defines the ability to purchase an object i_j by multiple users u_k from multiple users U. The modification is in supplementing the rule with a parameter $\delta_{m,s}$, characterizing the change in the user's interest during the transition from the time interval $\Delta\tau_m$ to the interval $\Delta\tau_s$. The parameter accepts true in case of increase in sales (rating). The generalized rule has the following form:

$$r_{m,s} = F_m(EX\delta_{m,s})F_s. \quad (1)$$

The initial data of the method are: sales log$L$; time stamp Q ratings log; the analyzed object i_j; a subset of users U, selecting this object; an interval $\Delta\tau_s$, that sets the level of detail of time (hour, day, week, etc.).

The method includes the following stages and steps.

Stage 1. Construction of a subset of weighted temporal rules R^{α}. The rules describe the dependencies between entries in the sales log.

Step 1. 1. Selection of a subset L_1 from sales log entries for the selected object i_j and a given subset of users U.

At this stage, records of the sale to users of the object i_j (possible target attacks) are selected. A subset U includes users who could potentially carry out these attacks.

The resulting ordered subset L_1 has the form:

$$L_1 = \left\langle l_{1,1},...,l_{1,s-1},l_{1,s},...,l_{1,|L_1|} : \forall s\ \tau_{s-1} < \tau_s \right\rangle. \quad (2)$$

Each element l_{1s} of the subset L_1 contains information about the buyer u_k, object i_j, time of purchase τ_s and the number of purchased objects $n_{k,j}$:

$$l_{1,s} = \left\{(u_k, i_j, \tau_s, n_{k,j}) : n_{k,j} > 0, u_k \in U\right\}. \quad (3)$$

Step 1. 2. Integration of events $l_{1,s}$ from the set L_1 within a given level of time detail $\Delta\tau_s$. At this stage, the summation of the number $n_{j,s}$ of purchases of each object i_j for all users from the set U is performed.

The result of this stage is a set L_2 consisting of elements $l_{2,s}$:

$$l_{2,s} = \left\{(i_j, n_{j,s}, \tau_s) : n_{j,s} = \sum_{u_k \in U | \tau_s \in \Delta\tau_s} n_{k,j}\right\}. \quad (4)$$

Each element $l_{2,s}$ of the resulting set contains information about the event «purchase of an object i_j $\Delta\tau_s$».

Step 1. 3. Temporal rule prototyping. These rules link consecutive pairs of facts F_m^{α} and F_s^{α}, reflecting consecutive pairs of events $l_{2,m}$ and $l_{2,s}$.

The result of this stage is a set R_1 of prototypes of unweighted temporal rules. The parameter $\delta_{m,s}^{\alpha}$ is not defined for these rules:

$$R_1^{\alpha} = \left\{r_{m,s}^{\alpha}\right\}, r_{m,s}^{\alpha} = F_m^{\alpha}(EX\delta_{m,s}^{\alpha})F_s^{\alpha} : \forall F_s^{\alpha} \exists l_{2,s} \wedge F_m^{\alpha} \exists l_{2,m}. \quad (5)$$

Step 1. 4. Construction of the set R_2^{α} prototypes of weighted temporal rules.

At this step, weights of temporal rules are calculated. The weights $w_{m,s}^{\alpha}$ correspond to changes in the number of sales between intervals $\Delta\tau_m$ and $\Delta\tau_s$. Normalized weights are calculated as follows:

$$w_{m,s}^{\alpha} = \frac{n_{j,s} - n_{j,m}}{\max\limits_{s}(n_{j,s})}. \quad (6)$$

The resulting set R_2^{α} contains the absolute values of the weights $w_{m,s}^{\alpha}$:

$$R_2^{\alpha} = \left\{\left(r_{m,s}^{\alpha}, \left|w_{m,s}^{\alpha}\right|\right)\right\}. \quad (7)$$

Step 1. 5. Construction of the set R^{α} of weighted temporal rules.

At this step, each prototype of the rule $r_{m,s}^{\alpha}$ is supplemented with a parameter value $\delta_{m,s}^{\alpha}$. This value is calculated based on the weight value as follows:

$$\delta^{\alpha}_{m,s} = \begin{cases} \text{true, if } w^{\alpha}_{m,s} > 0, \\ \text{false, othewise.} \end{cases} \quad (8)$$

The result of this stage is a set of weighted rules that objectively (financially) correspond to the needs of users.

Stage 2. Construction of a subset of estimated weighted temporal rules R^{β}, corresponding to implicit dependencies between entries in the rating log$Q$.

Step 2. 1. Selection of a subset Q_1 of rating journal entries, taking into account restrictions on the object i_j and a subset of users U.

Each element q_{1s} of the resulting ordered set contains a non-negative rating $\rho_{k,j}$ of a user u_k for the object i_j. This rating does not exceed the maximum value $\rho_{\max}$:

$$q_{1,s} = \left\{(u_k, i_j, \tau_s, \rho_{k,j}) : \rho_{\max} > \rho_{k,j} > 0, u_k \in U\right\}. \quad (9)$$

Step 2. 2. Integration of the events $q_{1,s \text{ of set } Q1}$ within a given level of time detail $\Delta\tau_s$ by averaging object i_j ratings set, by users from a subset U. The resulting set Q_2 consists of subsets $q_{2,s}$ with an average rating $\rho_{j,s}$ on the interval $\Delta\tau_s$:

$$q_{2,s} = \left\{(i_j, \rho_{j,s}, \tau_s) : \rho_{j,s} = \frac{\sum\limits_{u_k \in U | \tau_s \in \Delta\tau_s} \rho_{k,j}}{\left|q_{1,s}\right|}\right\}. \quad (10)$$

Step 2. 3. Construction of prototypes of the temporal rules linking sequential pairs of records $q_{2,m}$ and $q_{2,s}$.

The result of this step is a set $R^{\beta}_1 = \left\{r^{\beta}_{m,s}\right\}$ of prototypes of unweighted temporal rules, for which a parameter $\delta^{\beta}_{m,s}$ is not defined.

Step 2 .4. The construction of set R^{β}_2 prototypes of weighted temporal rules. Weights $w^{\beta}_{m,s}$ characterize the normalized change in rating between intervals $\Delta\tau_m$ and $\Delta\tau_s$:

$$w^{\beta}_{m,s} = \frac{\rho_{j,s} - \rho_{j,m}}{\rho_{\max}}. \quad (11)$$

The resulting set R^{β}_2 contains the absolute values of the weights $\left|w^{\beta}_{m,s}\right|$.

Step 2. 5. The construction of set R^{β} weighted temporal rules.

At this step, for each prototype's rule $r^{\beta}_{m,s}$ a parameter value $\delta^{\beta}_{m,s}$ is set. This value is calculated similarly to the value $\delta^{\alpha}_{m,s}$.

The result of this stage is a set of weighted rules that describe the change in ratings of goods.

Stage 3. Construction of an ordered subset of temporal rules $R^{\beta}_{attacked}$, fixing possible shilling attacks.

Step 3. 1. Definition of a set of values $\varphi_{m,s}$ based on pairwise comparison of parameters $\delta^{\alpha}_{m,s}$ and $\delta^{\beta}_{m,s}$. Values $\varphi_{m,s}$ indicate inconsistencies in user priority changes for rules $r^{\alpha}_{m,s}$ and $r^{\beta}_{m,s}$:

$$\varphi_{m,s} = \begin{cases} \text{true, if } \delta^{\alpha}_{m,s} \neq \delta^{\beta}_{m,s}, \\ \text{false, othewise.} \end{cases} \quad (12)$$

The result of this step is a subset of the rules R^{β}_3, that indicate a possible artificial change in the ratings in the interval $\Delta\tau_s$:

$$R^{\beta}_3 = \left\{r^{\beta}_{m,s} : \varphi_{m,s} = \text{true}\right\}. \quad (13)$$

Step 3. 2. Calculation of inconsistency of standardized rule weights $r^{\alpha}_{m,s}$ and $r^{\beta}_{m,s}$. Normalized weights $w^{\alpha}_{m,s}$ and $w^{\beta}_{m,s}$ show the relative degree of change in a parameter characterizing the objective and subjective interest of a group of users in the same object i_j. Since

$\varphi_{m,s} = \text{true}$, then the interest of users at the same intervals varies in different directions (for example, purchases are growing, but the rating is not increasing or falling). This enables possible to set priority the anomaly based on the sum $\Delta w_{m,s}$ of the modules of the normalized weights of these rules:

$$\Delta w_{m,s} = \left| w_{m,s}^{\alpha} \right| + \left| w_{m,s}^{\beta} \right|. \quad (14)$$

The value $\Delta w_{m,s}$ for $\varphi_{m,s} = \text{true}$ indicates an atypical change in the rating of the object i_j between the intervals $\Delta\tau_m$ and $\Delta\tau_s$: the higher $\Delta w_{m,s}$, the higher the probability of a shilling attack.

Step 3. 3. Ordering rules $r_{m,s}^{\beta}$ according to value $\Delta w_{m,s}$.

The resulting set $R_{attacked}^{\beta}$ of rules $r^{(k)}$, indicating a probable shilling attack is:

$$R_{attacked}^{\beta} = \left\langle r^{(1)}, r^{(2)}, ..., r^{(k-1)}, r^{(k)}, ... : \forall k \, \Delta w^{(k-1)} > \Delta w^{(k)} \right\rangle. \quad (15)$$

The ordered set $R_{attacked}^{\beta}$ obtained as a result of this stage contains the most likely attack objects at the top of the list.

The method allows an iterative implementation, in which at the first iteration all users are included in the subset. On following iterations, users who do not rate the rules from the set $R_{attacked}^{\beta}$ are deleted from the subset *U*. Iterative implementation of the method makes it possible to gradually reduce the subset of potential attacking users.

3. Experimental results

The experimental verification of the method was performed on two data sets. The first data set was formed from two files: ratings.csv and to_read.csv, which contain ratings and reading notes for several million books. This data is ordered in time, but there are no time stamps [15]. The purpose of the first experiment was to evaluate the possibility of applying the method to detected temporal dependencies in the absence of timestamps. Therefore, the combined events $l_{2,s}$ and $q_{2,s}$ were select by allocating a fixed number of records. The results of the method implementation for one book object are presented in **Table 1.**

The results of steps 1 and 2 in **Table 1** contain key rule elements.

For example, the temporal rule from the second line has the form:

$$r_{1,2}^{\alpha} = F_1 (E\,X\,\text{true}) F_2. \quad (16)$$

The parameter $\delta_{1,2}^{\alpha} = \text{true}$, since the number of sales (or book readings) increased from 7 to 11. The weight is $w_{1,2}^{\alpha}$ of this rule 0,108.

Rules $r_{6,7}^{\beta}$, $r_{10,11}^{\beta}$, $r_{14,15}^{\beta}$ and $r_{17,18}^{\beta}$, for which

$$\varphi_{m,s} = \text{true},$$

fix a possible shilling attack. The attack analysis priority is set based on the difference in weights $\Delta w_{m,s}$ for these rules.

Iterative method implementation for a rule $r_{10,11}^{\beta}$, with the first priority allowed to increase the value $\Delta w_{10,11}$ to 0,385. The number of users – potential attackers at the same time decreased by more than 5 times. Therefore, the iterative application of this method allows to highlight the group of users who have made the greatest contribution to the distortion of the rating of goods or services of the e-commerce system.

The second experiment was performed using the Online Retail dataset from the UCI repository. This set contains sales data with timestamps and does not contain ratings. Therefore, the set was artificially supplemented with 10 ratings for the same object, which did not correspond to the dynamics of its sales. The time interval was 1 day. Discrepancies for the rules were obtained only for adjacent time intervals (for pairs of consecutive days). This result indicates the need to use other types of rules to increase the accuracy of attack detection.

Table 1
Method implementation results

	Stage 1			Stage 2				Stage 3	
s	$n_{j,s}$	$\lvert w^{\alpha}_{m,s}\rvert$	$\delta^{\alpha}_{m,s}$	$\rho_{j,s}$	$\lvert w^{\beta}_{m,s}\rvert$	$\delta^{\beta}_{m,s}$	$\varphi_{m,s}$	$\Delta w_{m,s}$	Attack analysis priority
1	7								
2	11	0.108	True						
3	18	0.189	True						
4	17	0.027	False						
5	20	0.081	True	5.000					
6	15	0.135	False	4.833	0.033	False	False		
7	21	0.162	True	4.500	0.067	False	True	0.229	2
8	30	0.243	True	4.641	0.028	True	False		
9	17	0.351	False	4.386	0.051	False	False		
10	22	0.135	True	4.457	0.014	True	False		
11	35	0.351	True	4.405	0.011	False	True	0.362	1
12	26	0.243	False	4.388	0.003	False	False		
13	37	0.297	True	4.491	0.021	True	False		
14	31	0.162	False	4.436	0.011	False	False		
15	31	0.000	False	4.466	0.006	True	True	0.006	4
16	26	0.135	False	4.357	0.022	False	False		
17	28	0.054	True	4.445	0.018	True	False		
18	25	0.081	False	4.446	0.000	True	True	0.081	3
19	13	0.324	False	4.350	0.019	False	False		

4. The discussion of the results

The result of this research is a method for detecting shilling attacks by means of a comparative analysis of the choice of users of an e-commerce system using temporal rules. Temporal rules describe changes in user interests over time, for example, by day, week, etc. At the first stage, the method creates temporal rules that describe the growth or decline in sales of the selected product. The implicit feedback used at this stage, objectively reflects a change in the interests of users, since they have already paid for the purchase of the specified product. At the second stage, the method uses explicit feedback to form temporal rules that reflect changes in the rating of the same product. At the third stage, the comparison of the obtained rules is performed. Inconsistency of the rules, for example, an increase in sales of a product and a drop in its rating at the same time intervals, indicates a possible shilling attack. The list of conflicting rules is ordered by the sum of the values of their weights, since weights characterize the normalized change in purchases and ratings at the same time intervals. With the growing discrepancy between the scales of temporal rules for purchases and ratings, the likelihood of a shilling attack also increases.

The ordered list of weighted temporal rules obtained as a result of the method characterizes the most probable attacks, taking into account the list of potential attackers.

The difference of the proposed method is the use of temporal dependencies to identify differences in the processes of purchasing goods and forming their ratings as a necessary condition for a shilling attack.

The advantage of the method is the ability to iteratively clarify the composition of the user group that had the greatest impact on the artificial change in product ratings. This change is a sign of a shilling attack.

The disadvantage of this method is that the temporal rules used in detecting attacks specify dependencies only between adjacent time intervals. This approach does not allow to search for attacks at various levels of granulation time of the process of user selection.

The method has a limit on the source data, which should be ordered by time. The presence of time stamps is also desirable, which allows to group the source records at the required level of detail.

The developed method is designed to detect attacks and then interactively refine the list of attacking users. The method can be used to quickly refine the results of existing resource-intensive approaches to identify shilling attacks, taking into account recent changes in user priorities. Additional scope of application of the method includes predicting the anomalous states of discrete processes. An example of such tasks is the calculation of the peaks of Internet traffic information system [16].

5. Conclusions

The problem of the prompt detection of shilling attacks, consisting in artificially changing the ratings of goods and services in the e-commerce system in order to influence their sales, is considered. The recommended personal list of objects obtained after such attacks will not meet the user's needs.

A method is proposed for detecting attacks on the rating of goods and services in e-commerce systems based on a comparison of weighted temporal rules that describe the user's selection sequence. The method includes the steps of forming rules describing the temporal dependencies between sales of goods and between their ratings, as well as constructing an ordered subset of temporal rules that fix possible shilling attacks.

This method differs from the existing ones by using discrepancies between purchases objectively reflecting user preferences and subjective ratings to identify shilling attacks.

The proposed method allows increasing the efficiency of prompt detection of shilling attacks, taking into account the constant preferences of users in the e-commerce system.

Further improvement of the method involves the use of rules with the "Future" temporal operator. This operator associates the current user selection with a selection at one of the following time intervals. The combination of the Next and Future operators will make it possible to compare the change in user choice for an arbitrary pair of intervals and thereby ensure the detection of attacks at different levels of time granulation.

References

[1] Aggarwal, C. C. (2016). Recommender Systems. Springer. doi: https://doi.org/10.1007/978-3-319-29659-3

[2] Gunes, I., Kaleli, C., Bilge, A., Polat, H. (2012). Shilling attacks against recommender systems: a comprehensive survey. Artificial Intelligence Review, 42 (4), 767–799. doi: https://doi.org/10.1007/s10462-012-9364-9

[3] Mobasher, B., Burke, R., Bhaumik, R., Williams, C. (2007). Toward trustworthy recommender systems. ACM Transactions on Internet Technology, 7 (4). doi: https://doi.org/10.1145/1278366.1278372

[4] Wu, Z., Cao, J., Mao, B., Wang, Y. (2011). Semi-SAD: applying semi-supervised learning to shilling attack detection. Proceedings of the fifth ACM conference on Recommender systems, 289–292. doi: https://doi.org/10.1145/2043932.2043985

[5] Burke, R., Mobasher, B., Bhaumik, R. (2005). Limited knowledge shilling attacks in collaborative filtering systems. Proceedings of the 3rd IJCAI Workshop in Intelligent Techniques for Personalization, 1–36.

[6] Wang, Y., Qian, L., Li, F., Zhang, L. (2018). A Comparative Study on Shilling Detection Methods for Trustworthy Recommendations. Journal of Systems Science and Systems Engineering, 27 (4), 458–478. doi: https://doi.org/10.1007/s11518-018-5374-8

[7] Wang, Y., Zhang, L., Tao, H., Wu, Z., Cao, J. (2015). A comparative study of shilling attack detectors for recommender systems. 2015 12th International Conference on Service Systems and Service Management (ICSSSM). doi: https://doi.org/10.1109/icsssm.2015.7170330

[8] Tong, C., Yin, X., Li, J., Zhu, T., Lv, R., Sun, L., Rodrigues, J. J. P. C. (2018). A shilling attack detector based on convolutional neural network for collaborative recommender system in social aware network. The Computer Journal, 61 (7), 949–958. doi: https://doi.org/10.1093/comjnl/bxy008

[9] Patel, K., Thakkar, A., Shah, C., Makvana, K. (2016). A State of Art Survey on Shilling Attack in Collaborative Filtering Based Recommendation System. Smart Innovation, Systems and Technologies, 377–385. doi: https://doi.org/10.1007/978-3-319-30933-0_38

[10] Xia, H., Fang, B., Gao, M., Ma, H., Tang, Y., Wen, J. (2015). A novel item anomaly detection approach against shilling attacks in collaborative recommendation systems using the dynamic time interval segmentation technique. Information Sciences, 306, 150–165. doi: https://doi.org/10.1016/j.ins.2015.02.019

[11] Levykin, V., Chala, O. (2018). Development of a method for the probabilistic inference of sequences of a business process activities to support the business process management. Eastern-European Journal of Enterprise Technologies, 5 (3 (95)), 16–24. doi: https://doi.org/10.15587/1729-4061.2018.142664

[12] Chalyi, S., Pribylnova, I. (2019). The method of constructing recommendations online on the temporal dynamics of user interests using multilayer graph. EUREKA: Physics and Engineering, 3, 13–19. doi: https://doi.org/10.21303/2461-4262.2019.00894

[13] Chalyi, S., Leshchynskyi, V., Leshchynska, I. (2019). Method of forming recommendations using temporal constraints in a situation of cyclic cold start of the recommender system. EUREKA: Physics and Engineering, 4, 34–40. doi: https://doi.org/10.21303/2461-4262.2019.00952

[14] Kalynychenko, O., Chalyi, S., Bodyanskiy, Y., Golian, V., Golian, N. (2013). Implementation of search mechanism for implicit dependences in process mining. 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS). doi: https://doi.org/10.1109/idaacs.2013.6662657

[15] Zajac, Z. (2017). Goodbooks-10k: a new dataset for book recommendations. FastML. Available at: http://fastml.com/goodbooks-10k

[16] Kuchuk, N., Mozhaiev, O., Mozhaiev, M., Kuchuk, H. (2017). Method for calculating of R-learning traffic peakedness. 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). doi: https://doi.org/10.1109/infocommst.2017.8246416

Received date 19.07.2019
Accepted date 15.08.2019
Published date 17.09.2019